JYVÄSKYLÄ STUDIES IN COMPUTING

170

Jari Kellokoski

Managing Mobility in an Always-Best-Connected IP Network

JYVÄSKYLÄN YLIOPISTO

JYVÄSKYLÄ STUDIES IN COMPUTING 170

Jari Kellokoski

Managing Mobility in an Always-Best-Connected IP Network

Esitetään Jyväskylän yliopiston informaatioteknologian tiedekunnan suostumuksella
julkisesti tarkastettavaksi yliopiston Agora-rakennuksen auditoriossa 2
elokuun 9. päivänä 2013 kello 12.

Academic dissertation to be publicly discussed, by permission of
the Faculty of Information Technology of the University of Jyväskylä,
in building Agora, auditorium 2, on August 9, 2013 at 12 o'clock noon.

UNIVERSITY OF JYVÄSKYLÄ

JYVÄSKYLÄ 2013

Managing Mobility in an Always-Best-Connected IP Network

JYVÄSKYLÄ STUDIES IN COMPUTING 170

Jari Kellokoski

Managing Mobility in an Always-Best-Connected IP Network

UNIVERSITY OF JYVÄSKYLÄ

JYVÄSKYLÄ 2013

Editors
Timo Männikkö
Department of Mathematical Information Technology, University of Jyväskylä
Pekka Olsbo, Sini Tuikka
Publishing Unit, University Library of Jyväskylä

URN:ISBN:978-951-39-5268-6
ISBN 978-951-39-5268-6 (PDF)

ISBN 978-951-39-5267-9 (nid.)
ISSN 1456-5390

Jyväskylä University Printing House, Jyväskylä 2013

ABSTRACT

Kellokoski, Jari
Managing Mobility in an Always-Best-Connected IP Network
Jyväskylä: University of Jyväskylä, 2013, 70 p.(+included articles)
(Jyväskylä Studies in Computing
ISSN 1456-5390; 170)
ISBN 978-951-39-5267-9 (nid.)
ISBN 978-951-39-5268-6 (PDF)
Finnish summary
Diss.

This thesis concentrates on access network selection and mobility management in a heterogeneous network environment. There are three main themes which are investigated. The first theme is about Always-Best-Connected access network where the network selection process is improved by taking into account factors such as link quality, application or service used, link cost, location data and bandwidth. The network selection also follows 3GPP EPC ANDSF information whenever it is available, and the performance of a network selection algorithm implementation is evaluated. The second theme is about challenges and problems of the standards and implementations used for the presented solutions. As the solutions and ideas presented in this thesis were implemented and their performance evaluated, a number of challenges, modifications and configurations in the Android and Maemo frameworks and Linux operating system were found. Finally, the third theme addresses one possible path toward multihomed user equipments, where network access may occur simultaneously over multiple network interfaces. The main motivation for this is the performance evaluation from the first theme, which indicated that real-time communication cannot be handed over -without compromises in user experience -between access technologies if the network interfaces are not used simultaneously. With simultaneous connections there is a trade-off with power efficiency which is also evaluated.

Keywords: Mobility Management, Handover, Always-Best-Connected, 3GPP EPC, Multihoming

Author Jari Kellokoski
Department of Mathematical Information Technology
University of Jyväskylä
Finland

Supervisor Professor Timo Hämäläinen
Department of Mathematical Information Technology
University of Jyväskylä
Finland

Reviewers Professor Tien Van Do
Department of Networked Systems and Services
Budabest University of Technology and Economics
Hungary

Associate Professor František Jakab
Department of Computers and Informatics
Technical University of Košice
Slovakia

Opponent Professor Hannu Jaakkola
Industrial applications of IT / Software Systems
Tampere University of Technology, Pori
Finland

ACKNOWLEDGEMENTS

This dissertation has taken and given a lot work from me. But it would not have been possible just by me. First of all, I would like to thank my supervisor Professor Timo Hämäläinen for all the inspiration and guidance during my years in university after Nokia faded away from the Jyväskylä. My research was part of projects founded by Tekes, Department of Mathematical Information Technology and privately held companies, and would not have been possible without them. In addition, I would like to thank my people who I worked with and specially Joonas Koskinen and Janne Villikka for their help in my publications. My thanks go also to the TeliaSonera foundation which helped me to completing this thesis with its funding.

I am grateful to the reviewers of my thesis Professor Tien Van Do and Associate Professor František Jakab for their constructive comments and Professor Hannu Jaakkola for being my opponent. I also would like to thank Steve Legrand for translating my language to proper English. I would also like to thank all you people on the 5th floor coffee room who had coffee or tea with me while discussing non-work related things.

Finally, I would like to thank my parents and brother for their full support my whole life. My sincerest gratitude goes to my loving wife Heli for her patience, support and encouragement and to my wonderful daughters Iina and Enni for reminding me about the life outside the telecommunication laboratory.

GLOSSARY

3GPP	3rd Generation Partnership Project
AAA	Authentication, Authorization and Accounting
ABC	Always-Best-Connected
ANDSF	Access Network Discovery and Selection Function
CAGR	Compound Annual Growth Rate
CoA	Care of Address
eNodeB	E-UTRAN Node B
EPC	Evolved Packet Core
EPS	Evolved Packet System
E-UTRAN	Evolved-Universal Terrestrial Radio Access
GSM	Global System for Mobile
HA	Home Agent
HBM	Host-Based Mobility
HetNet	Heterogeneous Network
HSPDA	High Speed Packet Data Access
HSS	Home Subscriber Server
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IFOM	IP Flow Mobility
IoT	Internet of Things
IP	Internet Protocol
LMA	Local Mobility Anchor
LTE	Long Term Evolution
M2M	Machine to Machine
MAG	Mobile Access Gateway
MAPCON	Multi Access PDN Connectivity
MIP	Mobile IP
MME	Mobility Management Entity
MN	Mobile Node
MPTCP	Multipath Transmission Control Protocol
NA	Neighbor Advertisement
NBM	Network-Based Mobility
NS	Neighbor Solicitation
PCRF	Policy and Charging Rule Function
PDN	Packet Data Network
PDN-Gw	Packet Data Network Gateway
PMIPv6	Proxy Mobile IPv6
QoS	Quality of Service
RTP	Real-Time Protocol
SAE	System Architecture Evolution

SCTP	Stream Control Transport Protocol
SGw	Serving Gateway
SSL	Secure Socket Layer
SW	Software
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UE	User Equipment
UMTS	Universal Mobile Telecommunications System
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
VoIP	Voice over IP
VPN	Virtual Private Network

LIST OF FIGURES

FIGURE 1 User movement in a heterogeneous network environment........ 15
FIGURE 2 The relation between publications and main themes of thesis.... 19
FIGURE 3 Mobile IPv6 network... 23
FIGURE 4 Proxy Mobile IPv6 network 24
FIGURE 5 3GPP Access Network Discovery and Selection Function in action 26
FIGURE 6 ABC algorithm Proof-of-concept test setup............................ 29
FIGURE 7 The ABC application permission page (Google Talk)............... 29
FIGURE 8 PMIPv6 test environment 32
FIGURE 9 RTP traffic with a 100-ms buffer in Linux during handovers 34
FIGURE 10 History-based location awareness for ABC application............ 36
FIGURE 11 Context- and location-aware ABC application proof-of-concept test setup 36
FIGURE 12 Vertical handover test setup for VPN-based mobility............... 45
FIGURE 13 HTTP download consumption 48
FIGURE 14 Handover power consumption 48
FIGURE 15 Energy efficiency during handovers 49
FIGURE 16 Multihoming download over WLAN and 3G 49
FIGURE 17 Energy efficiency trade-off in idle state 55
FIGURE 18 Handover delay.. 55
FIGURE 19 UDP-based multihoming between 3G and WLAN interfaces. The arrows are pointing at handover points 56
FIGURE 20 SCTP-based multihoming between 3G and WLAN interfaces. The arrows are pointing at the handover points and the interface used.. 57
FIGURE 21 Multipath TCP vertical handover performance........................ 61

LIST OF TABLES

TABLE 1 Network-change delay in open access.................................... 30
TABLE 2 SSL and IPsec handshake times over TCP 31
TABLE 3 Handovers with Linux UE.. 33
TABLE 4 Vertical Handover and EPC delays 45
TABLE 5 Standby current consumption 47

CONTENTS

ABSTRACT
ACKNOWLEDGEMENTS
GLOSSARY
LIST OF FIGURES AND TABLES
CONTENTS
LIST OF INCLUDED ARTICLES

1 INTRODUCTION 13
  1.1 Heterogeneous Networks 14
  1.2 Research Motivation 15
  1.3 The Thesis Outline and Main Contribution 16

2 ALWAYS-BEST-CONNECTED HETEROGENEOUS NETWORK 20
  2.1 Mobility and Mobility Management 20
    2.1.1 Handover Types 21
    2.1.2 IP version 6 22
    2.1.3 Host- and network-Based mobility management 22
  2.2 Evolved Packet System and Core 24
    2.2.1 User-centric approach 25
    2.2.2 A novel approach to Always-Best-Connected IP network .. 27
    2.2.3 Algorithm design for Always-Best-Connected application. 27
    2.2.4 Proof-of-Concept performance environment for ABC algorithm 28
    2.2.5 Network-change performance results for ABC algorithm .. 30
    2.2.6 Android device in a simulated EPC heterogeneous network environment 31
    2.2.7 Seamless mobility in PMIPv6 environment 31
    2.2.8 Seamless Handovers 32
  2.3 Need for Mobility Management 33
    2.3.1 Context and its relations to services 34
    2.3.2 Algorithm with context and location awareness 35
    2.3.3 Proof-of-concept implementation 36
    2.3.4 Results without context and location awareness 36
    2.3.5 Results with context and location awareness 37
  2.4 Summary 38

3 CHALLENGES FOR THE MOBILE USERS 40
  3.1 3GPP Evolved Packet System and Its Challenges for the User Equipment 40
  3.2 Implementation Challenges and Workarounds 42
    3.2.1 Android framework modification 42
    3.2.2 IP version 6 and Proxy Mobile IPv6 support in Android framework 43

3.2.3 Authentication challenges with Evolved Packet Core 44
3.2.4 Workaround for the lack of simultaneous connections 44
3.3 Power Consumption 46
3.3.1 Energy-efficient Always-Best-Connected user equipment .. 46
3.3.2 Implementation and measurements 47
3.4 Summary 48

4 TOWARDS MULTIHOMED MOBILES 51
4.1 Simultaneous Connections with Application Framework 52
4.1.1 Handover concept and implementation 52
4.1.2 Framework modification 53
4.1.3 User Datagram Protocol based multihoming in Android framework 54
4.2 Stream Control Transmission Protocol as a standalone application 56
4.3 Multipath TCP as a part of Evolved Packet Core 58
4.3.1 Multipath TCP and Evolved Packet Core in Android environment 58
4.3.2 Measurements on vertical handover performance 60
4.4 Summary 62

5 CONCLUSION 64

YHTEENVETO (FINNISH SUMMARY) 66

REFERENCES 67

INCLUDED ARTICLES

LIST OF INCLUDED ARTICLES

PI	Jari Kellokoski and Timo Hämäläinen. User-Centric Approach to Always-Best-Connected Networks. *ICUMT 2011, 3rd International Congress on Ultra Modern Telecommunications and Control Systems and Workshops*, 2011.
PII	Jari Kellokoski, Joonas Koskinen and Timo Hämäläinen. Real-life Performance Analysis of Always-Best-Connected Network. *NTMS 2012, New Technologies, Mobility and Security*, 2012.
PIII	Jari Kellokoski, Joonas Koskinen and Timo Hämäläinen. Power Consumption Analysis of the Always-Best-Connected User Equipment. *NTMS 2012, New Technologies, Mobility and Security*, 2012.
PIV	Jari Kellokoski. Challenges of the Always-Best-Connected Enablers for User Equipment in Evolved Packet System. *ICUMT 2012, 4th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops*, 2012.
PV	Jari Kellokoski, Joonas Koskinen and Timo Hämäläinen. Context and Location Aware Always-Best-Connected Concept for Heterogeneous Network. *Wireless Days 2012*, 2012.
PVI	Jari Kellokoski, Joonas Koskinen, Riku Nyrhinen and Timo Hämäläinen. Efficient Handovers for Machine-to-Machine Communications Between IEEE 802.11 and 3GPP Evolved Packet Core Networks. *iThings 2012, The IEEE International Conference on Internet of Things*, 2012.
PVII	Jari Kellokoski. Real-life Multipath TCP based Make-Before-Break Vertical Handover. *ISCC 2013, The Eighteenth IEEE Symposium on Computers and Communications*, 2013.

1 INTRODUCTION

Mobile internet data will grow 13-fold between 2012 and 2017, with nearly half of the traffic offloaded to fixed or Wi-Fi networks by 2017. Monthly global mobile data traffic is forecasted to reach 11.2 exabytes by 2017. With mobile data traffic at 885 petabytes per month in 2012, the 2017 figure represents a compound annual growth rate (CAGR) of 66 per cent. In order to deal with the increase in data, operators will increasingly seek to offload traffic from their mobile networks to Wi-Fi and fixed networks. By 2017, 46 per cent of traffic will be offloaded compared to 33 per cent in 2012, according to Cisco [1]. Mobile data traffic will outpace fixed data traffic by a factor of three as the number of mobile users increases to 5.2 billion by 2017, compared to 4.3 billion in 2012. There will be more than 10 billion mobile connections in 2017, including more than 1.7 billion M2M connections, up from 7 billion in 2012 [1]. This has created challenges for existing networks and enhancements of network performance in many respects including the system capacity and network coverage. These enhancements can be accomplished by heterogeneous networks where access is created via different access technologies.

In the context of this thesis, mobility is related to user and particularly to the management of User Equipment (UE) movement. A key concept with user movement is known as the handover, where an active UE changes its point of attachment to the network. There are different types of handovers, which are classified according to different aspects involved in the handover. From the point-of-view of this thesis, the most important are horizontal handover, which involves UEs moving between access points of the same type (inside cellular access basestations for example), and vertical handover, which involves UEs moving between access points of different type (cellular access to wireless local area network (WLAN) for example). The handover control has two main options, mobile-controlled handover or network-controlled handover, where either the UE or the network has the primary control over the handover process.

This dissertation discusses the design, implementation, functionality and the challenges of the Always-Best-Connected IP network, especially in a heterogeneous network environment. The real-life approach is present all the way through the discussion. Three main themes are present: the discussion begins from mobility and access management in heterogeneous networks, is followed by challenges caused by implementation and test environment, and finally leads to simultaneous usage of more than one network interface and to multihoming where there are multiple communication paths between the UE and the services used.

1.1 Heterogeneous Networks

Integration of heterogeneous access networks and efficient use of available communication systems are some of the key challenges for the next generation mobile communication. Today's mobile devices come with various network interfaces. Even the cheaper smartphones support at least two wireless technologies, for example the Universal Mobile Telecommunications System (UMTS) and IEEE 802.11 (WLAN). Over the past years, the number of heterogeneous access networks that are available at a specific location grew dramatically. Other technologies such as Long Term Evolution (LTE) [2] or Worldwide Interoperability for Microwave Access (WiMAX) [3] are being deployed currently.

All of these networks show different communication characteristics, e.g. in terms of throughput, delay, availability and costs, and in combination they offer a high communication performance. In an environment of multiple access technologies, the concept of being always connected becomes Always Best-Connected. This refers to being not only always connected, but also being connected in the best possible way [4]. A high uptake of mobile handheld devices and their associated data create a need for dense high data-rate networks. The trend is towards high traffic levels in indoor and urban areas. This clearly calls for ubiquitous coverage, mobility management and high throughputs. One way of meeting this demand is the deployment of heterogeneous networks [5]. This involves improving and densifying urban coverage, as well as adding small cells. In other words, smarter usage of the frequency spectrum is required: that is if more spectrum is available it should be utilized instead of consuming the crowded part of the spectrum. This is true for example in most homes and offices where an IEEE 802.11 WLAN coverage is available. To put it in other way, heterogeneous networks are already here, and they should be exploited.

FIGURE 1 shows one example of a real-life heterogeneous network environment and UE movement in it. In the figure, operator has presence in the form of cellular access (High Speed Packet Data Access - HSPDA and LTE) coverage and through trusted WLAN. Trusted and untrusted non-3GPP access networks are IP access networks that use access technology, the specification of which is out of the scope of the 3rd Generation Partnership Project (3GPP) [6]. Whether a non-3GPP IP access network is trusted or untrusted is not defined as an access network characteristic. The trust relationship of a non-3GPP access network is made known to the UE, if a non-3GPP access supports 3GPP-based access authentication, the

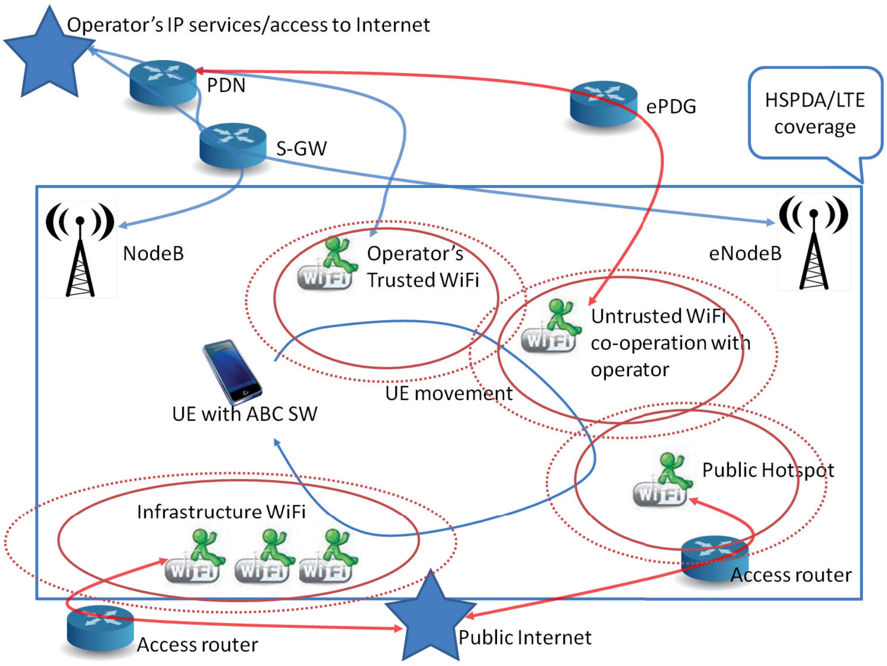


FIGURE 1 User movement in a heterogeneous network environment

UE discovers the trust relationship during the 3GPP-based access authentication or the UE operates on the basis of a pre-configured policy in the UE. Other access networks in FIGURE 1 are the hotspot WLAN and the infrastructure WLAN: the hotspot offers a single and limited-in-range point-of attachment to services, and the infrastructure WLAN can cover larger geographical areas e.g. offices, campuses or shopping centers. The user with UE is moving in range of these networks and has the opportunity to connect with them to initiate a service session or handover it from other access network.

1.2 Research Motivation

The previous section described generally the need for a network capacity increase and outlined challenges for heterogeneous networks. This thesis concentrates on access network selection and mobility management in a heterogeneous network environment. Access network selection aim at finding the most suitable access network. There are numerous factors to be taken into account when selecting a suitable network. Examples of these factors are; link quality, Quality of Service (QoS), cost and power efficiency. Since the introduction of the Always-Best-Connected term [4] there have been multiple strategies to decide which network is the best at any one moment. In their early work Gustafsson et al. made the first proper definitions for the Always-Best-Connected network. Their definition of the best connected network came with an estimate of complexity. It was stated that the choises available for a person selecting the best available access network and device at any point in time, will generate great complexity and a number of requirements. The first of the three main themes of this thesis is to simplify access network selection based on user experience, implement it and conduct performance measurements on the developed algorithm and, additionally, to examine how this simplified access network selection could improve mobility management.

Although today's mobile devices are not supporting the latest 3GPP or IETF standards yet, they have multiple radio interfaces such as IEEE 802.11 and cellular access. At the same time, many of the software (SW) environments including Linux, Android and Maemo, are open source and in many ways open to modifications for trialing of standards that are currently being developed. It is clear that the implementations of these actively developed new standards have challenges and problems. These implementation challenges and problems form the second main research problem.

The third and final problem area is the effective usage of multiple interfaces of UE. The real-time communication such as Voice over IP (VoIP) or video calls over IP have a generally accepted maximum delay requirement from 150 to 200 ms. If the delay is above this, the end user finds it unpleasant. This delay requirement is challenging for handovers, especially for the vertical ones, since another network interface is initialized and then connected to the network. In many cases the user authentication, authorization and possibly accounting (AAA) is mandatory before network access is complete. These facts make it difficult to achieve seamless vertical handovers that could serve real-time services. One solution to address the problem is multihoming where the UE has multiple network interfaces active at the same time and multiple IP addresses that can be reached. In this thesis, the solutions cover Android and Linux environment changes to enable simultaneous usage of interfaces and protocols such as Stream Control Transmission Protocol (SCTP) and Multipath TCP-(MPTCP)-based solutions. The network traffic here is both connectionless User Datagram Protocol (UDP) traffic and connection-oriented Transmission Control Protocol (TCP) traffic.

1.3 The Thesis Outline and Main Contribution

The main contributions relate to the three main themes of the thesis:

- Always-Best-Connected Heterogeneous Network where access network selection and mobility management in a heterogeneous network environment is examined. Access network selection aims for simplifying the selection process so that suitable connection is found based on well-defined preferences. The network selection algorithm is implemented in various SW environments and its performance is measured. Network selection is then used in vertical handovers. This problem is investigated in Chapter 2.

- Challenges for the Mobile Users gathers most important problems and workarounds that were encountered and solved during the research. The section covers implementation challenges with Linux and Android and the required changes to them to enable access network selection and mobility management. It also covers the network environment needed for emulations in performance measurements. One key challenge is power efficiency, which is introduced in this Chapter. These issues are looked at in Chapter 3.
- Towards Multihomed Mobiles aims for enhancing the probability that realtime communication may be handovered without compromising user experience. The Chapter introduces solutions for simultaneous connections where network interfaces are active at the same time. These solutions range from Android framework modifications and exploitation of Linux routing changes to the usage of multihoming-enabled protocols such as SCTP or MPTCP. The handover performance and power efficiency trade-off is also examined. Multihoming related challenges are studied in Chapter 4.

Proxy Mobile IPv6 is one of the key enabler standards for the 3GPP EPS based mobility management. Due to this reason the thesis presents the use of Proxy Mobile IPv6 in handovers with Linux and Android SW environments outside of the listed publications. This analysis acts as the background for presented research in the thesis. The author analyzed the results for handover performance and contributed to the implementation challenges as well as to the test environment setup. The Stream Control Transport Protocol provides a way to switch between streams which are connected to different network interfaces. To examine this multihoming enabler protocol, Linux under the Android Framework was modified to support SCTP and used to manage mobility between two network interfaces. The SCTP research provided a way to trial multihoming with existing protocol; it provided valuable information about handover performance and energy efficiency measurements. It can be seen as an evolutionary path from modified Android framework for single application to MPTCP which handles multipath as part of the protocols routine action for all applications.

During the work on the subject of this dissertation, the author produced and co-authored several publications. The relations of these publications to the main themes are presented in FIGURE 2. Publication **PI** considers the user’s role and opportunities for choosing the best possible connection in a heterogeneous network environment. For and ABC application the author proposed an idea that could take care of the network selection on behalf of the user. The research investigates how to build an Always-Best-Connected application that works with the EPS standard and what kind of user preferences should be taken into account when making network selection more user-centric. Additionally, the proof-of-concept implementation of this user-centric approach to Always-Best-Connected model is illustrated. The author was responsible for the implementation requirements regarding EPS as well as the performance evaluation setup.

In Publication **PII** the research started on **PI** is carried further to develop a device-based simple algorithm for the user and a service that will work with the existing EPS standard and with other known networks such as WLAN hotspots and cellular networks, to make performance measurements of this developed algorithm implementation and to show that the idea works in a real-life mobile environment. The author was responsible for design of the network selection algorithm and for the performance evaluations design and setup. The author was also responsible for introducing three separate SW environment that were used in the implementation and for the performance measurements. The SW environments were Android, Maemo and Linux.

One of the key factors with mobile devices is power consumption. Publication **PIII** is the first of the publications to cover power consumption by analyzing the energy efficiency of the Always-Best-Connected application presented in Publications **PI** and **PII**. The author was responsible for defining real-life use-cases for energy-efficiency measurements. The author was also responsible for the analysis of the results. The power consumption analysis is revisited in Publication **PVI**, where power consumption trade-off is analyzed when using more than one network interface at the same time to make efficient handovers between two connected networks. The author was responsible for the idea of examining power consumption efficiency and defined the use-cases and implementation of the measurements. The author also presented the idea of a test client and server for handover-time measurements. This was used in SCTP protocol analysis and in Publication **PVII** which examined the power efficiency of the MPTCP protocol.

As many of the subjects of this dissertation are closely related to real-life implementations and their accompanying measurements, Publication **PIV** focus on the Android framework and analyzes its clearly missing functionality to support EPS. As the EPS standard gives room for workarounds in the implementation, the publication introduces solutions such as the use of Virtual Private Network (VPN) and Secure Socket Layer [7] (SSL) instead of Proxy Mobile IPv6 and IPsec [8] and presents the implementation and performance measurements of these solutions. The publication also gives an overview of the Voice Call Continuity based on IP Multimedia Subsystem, Unlicensed Mobile Access, Media Independent Handover mobility management protocols and systems. Publication **PIV** was produced solely by the author.

Publication **PIV** showed that even though many mobility management systems have been developed, a commercial breakthrough is missing. The question about the need for mobility management with today's services is then brought to the focus. Publication **PV** investigates the problem, starting from The Third Generation Partnership Project (3GPP) Quality of Service (QoS) classes: conversional, streaming, interactive and background. The publication then investigates today's services corresponding to the classes. The author was responsible for service matching to the classes and for the modification of the ABC algorithm to make it take into account context and location information. The context is in the form of used bandwidth, and the location is based on the last five cell-ids visited.

As off-the-shelf solutions could not provide a feasible solution to handovers with real-time applications such as Voice over IP, the research focused on untapping more than one network interface. Publication **PVI** presents a way to modify

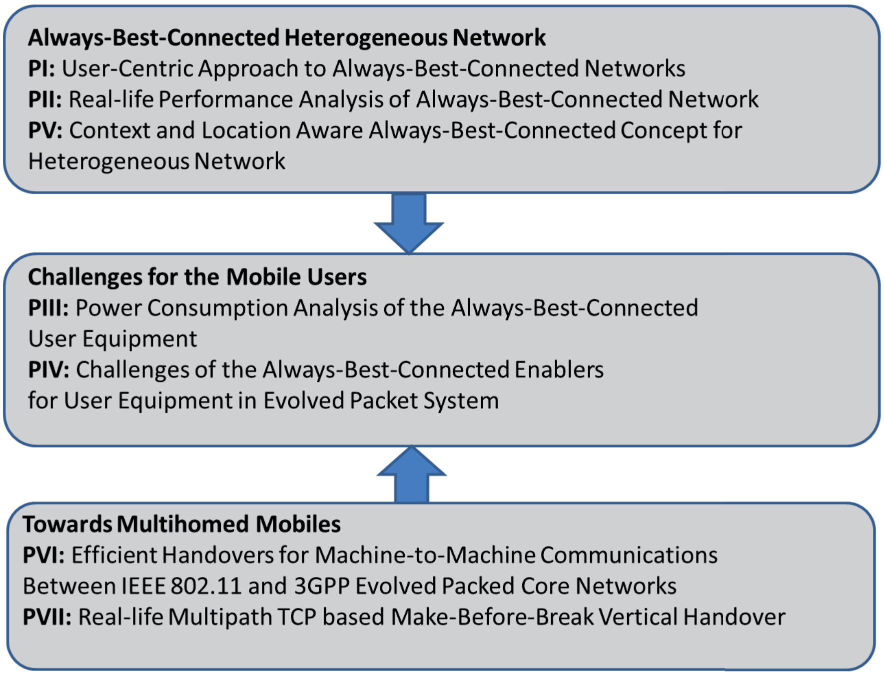


FIGURE 2 The relation between publications and main themes of thesis

the Android Framework so that two simultaneous connections are possible. The author was responsible of the idea of modifying the Android Framework and designing its modifications as well as defining and setting up the performance measurements. The author also analyzed the handover performance results.

In Publication **PVII**, the author contributes to the combining of EPS and Multipath TCP from the standard point-of-view and fitting MPTCP to the Android framework. The main contribution is the use of Multipath TCP as a part of EPS to enable make-before-break vertical handovers. An Android-based implementation and performance measurement in a real network environment are presented.

2 ALWAYS-BEST-CONNECTED HETEROGENEOUS NETWORK

Mobile Internet has rapidly evolved in the past years with an ever increasing number of novel technologies and services as well as a variety of access technologies being deployed along side. Today's mobile devices often support multiple communication technologies for accessing Internet services. However, they all do not tap the full potential of these capabilities as users often have to manually select the networks and only one network is used at a time. The concept of Always Best Connected allows a person to connect applications using the devices and access technologies that best suit to his or her needs, thereby combining the features of access technologies to provide an enhanced user experience of future Internet. However, an Always-Best-Connected scenario generates great complexity and a number of requirements, not only for the technical solutions, but also in terms of business relationships between operators and service providers, and in subscription handling. The 3GPP standardized the Evolved Packet System (EPS) where one of the key features is a support access system selection based on a combination of operator policies, user preference and access network conditions (**PI**). Still the standard focuses mainly on the operator point-of-view, and the user is considered to as following this approach. Yet, the standard offers a number of possibilities where the user centric approach can improve the ABC scenario over the one predefined by the operator.

2.1 Mobility and Mobility Management

A prospective next generation wireless network is expected to integrate harmoniously into an IP-based core network. It is widely anticipated that IP-layer handover is a feasible solution to global mobility. However, the performance of IP-layer handover based on basic Mobile IP (MIP) cannot support real-time services very well due to long handover delay. The Internet Engineering Task Force (IETF) Network-based Localized Mobility Management (NETLMM) working group developed a network-based localized mobility management protocol called Proxy Mobile IPv6 (PMIPv6) to reduce the handoff latency of MIPv6. Moreover, PMIPv6 provides the IP with the mobility to support User Equipments (UEs) without it being required to participate in any mobility-related signaling. This was one of the reasons why the 3GPP chose PMIPv6 as one of the mobility management protocols when defining the Evolved Packet System (EPS). One of the key features of the standard is its support for access system selection based on a combination of operator policies, user preference and access network conditions.

2.1.1 Handover Types

There are many types of mobility cases where the point of attachment can change in an IP network. This is why also handovers have been categorized based on the type of the handover. The "Mobility Related Terminology" (RFC 3753) [9] gives the following definitions for handover variations: there is a horizontal handover: when a mobile node moves between access points which use the same technology; a vertical handover takes place when a mobile node changes the point-of-attachment technology used, for example in research applications, from WLAN to UMTS. In addition to these definitions, there is one more mobility type, which the from point-of-view of IP network it is not a handover, just a normal connectivity-related action. This might be called between-session-mobility: first the equipment with the required connectivity is used in some location, then all connections are closed or at least not used while moving to another location where, the user starts using the connectivity again. A good example of this is a laptop/netbook/tablet user, with scheduled meetings and with all the necessary connections for the device: he/she closes the lid of the device and stops all connections before moving back to a desk or to another meeting room where the needed connections are started again. During the switch, the user is not actively expecting connectivity; it might or might not work. Nevertheless, the actual communication will take place later, once the user is ready to start communicating. This is not directly comparable to smartphone usage although there are similarities when excluding the real-time communication. The usage of smartphone will mostly take place when stationary, as in web browsing, video consuming and messaging.

In addition to horizontal and vertical handover, there are finer grades of handover such as the proactive handover, the reactive handover and the seamless handover. To minimize the effects, such as packet loss and/or delays caused by handovers, there is usually signaling in a proactive handover before the handover process in initiated. A reactive handover, on the other hand, takes place suddenly, and no signaling can be done before the handover has taken place. In seamless handover applications, the user cannot see any changes in the normal operation.

2.1.2 IP version 6

IP version 6 (IPv6) [10] is a new version of the Internet Protocol, designed as the successor to IP version 4 (IPv4) RFC 791 [11]. The major changes are: expanded addressing capabilities, header format simplification and improved support for extensions and options.

IPv6 increases the IP address size from 32 bits to 128 bits to support more addressing hierarchy levels and to provide, a much greater number of addressable nodes, and simpler auto-configuration of addresses. The scalability of multicast routing is improved by adding a "scope" field to multicast addresses. The following scopes and scope field values are defined: 1 Node-local, 2 Link-local, 8 Organization-local, E Global. For example, traffic with the multicast address of FF02::2 has a link-local scope. An IPv6 router never forwards this traffic beyond the local link. A new type of address, "anycast address" is defined. It is used to send a packet to any one of a group of nodes. An anycast address identifies multiple interfaces, and is used for one-to-one-of-many communication, with delivery to a single interface. With an appropriate routing topology, packets addressed to an anycast address are delivered to a single interface. In terms of routing distance, a packet addressed to an anycast address is delivered to the nearest interface identified by the address. That is, anycast addresses are used only as destination addresses and are assigned only to routers.

2.1.3 Host- and network-Based mobility management

Over the years there have been a number of investigations on host-based versus network-based mobility management. The Internet Engineering Task Force (IETF) proposed a host-based mobility management protocol, called the Mobile IPv6 (MIPv6) protocol RFC 3775, for UE to maintain continuous service when moving among different foreign networks. However, MIPv6 does not provide good service for real-time applications because it causes long disruptions during handoff.

The basic idea with Mobile IP is that UEs are able to change the point of attachment to the network and their location can be tracked. The Mobile IP has two versions for both IPv4 and IPv6. The key entity is the home agent (HA). HA is the node which should always know the current location of the UE and is located in the UE’s home network. Home network defines the primary IP address which the UE is using for communication. This address is called Home Address (HoA). When a UE moves and gets connected to a new network it needs a way to communicate in that network. For this purpose, the UE uses a new IP address called Care of Address (CoA). With this address, the UE is able to communicate in the new network. For updating the current location, the UE registers the CoA with an HA by using a binding update message. The HA forwards the packets destined to the UE HoA to the current location (and the CoA used) by tunneling them with IP encapsulation within IP [12]. Mobile IPv6 benefits from the functionality of IPv6 and from the experience learned from MIPv4. The MIPv6

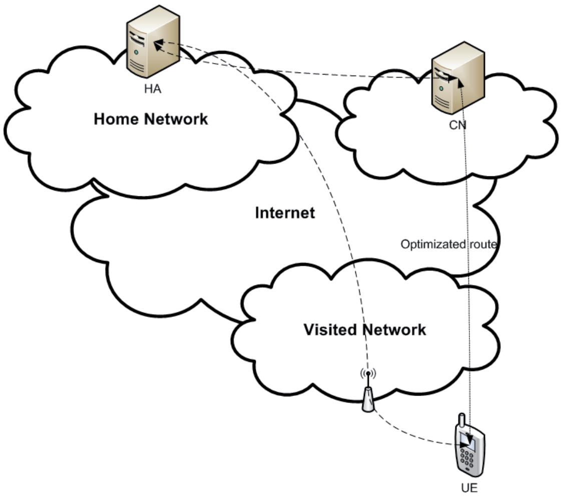


FIGURE 3 Mobile IPv6 network

network topology is depicted in FIGURE 3. MIPv6 still has the HA, and the location is also updated to the HA by using binding update messages. In a similar way, the UE may get a CoA from the visited network, but the protocol uses IPv6 neighbor discover and the address auto-configuration mechanism. MIPv6 has an optimization mechanism which allows UE to register the current CoA directly with the correspondent node. This enables direct IP flows between the two nodes without routing them via the HA. MIPv6 may also use IPv6 headers for routing instead of tunneling, which will reduce the overhead of sent packets.

PMIPv6, a network-based localized mobility management protocol, reduces the handoff latency compared to MIPv6. Moreover, PMIPv6 provides IP with the mobility to support UEs without requiring its participation in any mobility related signaling. The network architecture of PMIPv6 contains two network entities: a mobile access gateway (MAG) and a local mobility anchor (LMA). The MAG is responsible for detecting the movements of an MN and performs mobility-related signaling with the LMA in place of the Mobile Node (MN). The LMA acts in a way similar to the home agent (HA) in MIPv6 and maintains the binding cache entries for currently registered UEs. The network topology of PMIPv6 is shown in FIGURE 4.

The analytical models as in [13], [14] and [15] show that the handoff latency of PMIPv6 is much lower than that of the MIPv6, Hierarchical Mobile IPv6 Mobility Management (HMIPv6) [16] and Mobile IPv6 Fast Handovers (FMIPv6) [17] host-based mobility management protocols. Similar results are shown by Guan et al [18] in their implementation of protocols: their results show that PMIPv6 has lower handoff latency than the other schemes. This fact has inspired researchers to further improve PMIPv6. A Fast Handoff Scheme in PMIPv6 [19] and Optimized-PMIPv6 [20] present analytical models that perform better than plain PMIPv6. Despite these results, the real numerical and user experience data on handover delay in PMIPv6 managed networks with real UEs is minimal.

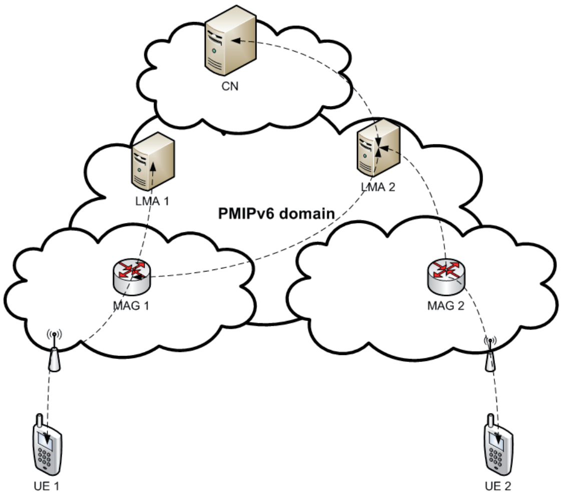


FIGURE 4 Proxy Mobile IPv6 network

2.2 Evolved Packet System and Core

This section outlines one of the major network technologies, namely the Evolved Packet System, which has the potential to become the next common baseline for all IP-based services. The Evolved Packet System, formerly known as the System Architecture Evolution (SAE), was standardized by 3GPP and consists of a radio part: (Evolved URTAN (E-UTRAN)) and a network part: (Evolved Packet Core (EPC)) [21]. The main objectives of the Evolved Packet System (EPS) are to:

- provide higher data rates, low latency, high level of security, support of variable bandwidth and Quality of Service (QoS)
- support a variety of different access systems (existing and future ones) and ensure mobility and service continuity between these access systems
- support access system selection based on a combination of operator policies, user preference and access network conditions as an operator-based ABC
- provide capabilities for co-existence with legacy systems and migration to the Evolved Packet System

This section focuses on the core network part (EPC), as it plays the key role in providing the IP connectivity. The section also describes the components of EPC, highlights their major functionalities and outlines their mobility support. The EPC architecture that interconnects 3GPP and non-3GPP access networks consists of several main subcomponents, namely eNodeB, Mobility Management Entity (MME), Serving Gateway (SGw) and Packet Data Network Gateway (PDN-Gw). In addition to these, there are several other components which inter-operate with non-3GPP access. These include WLAN/WiMAX (ePDG, ANGw) for access gateways and the Access Network Discovery and Selection Function (ANDSF). The PDN Gateway provides connectivity from User Equipment (UE) to one or multiple external PDNs simultaneously. The PDN-Gw acts also as a mobility anchor between 3GPP and non-3GPP technologies, and, in addition, performs packet filtering and charging. The Home Subscriber Server (HSS) is the central database in the EPC that stores user-related information. The Policy and Charging Rule Function (PCRF) encompasses the two main functions of flow-based charging: charging and QoS controls (e.g. QoS control and signaling, etc.). The ANDSF, a new EPC element in Release 8, performs data management and controls the functionality to assist the UE on the selection of an optimal access network in a heterogeneous scenario via the S14 interface. S14 is the logical interface between the ANDSF and the UE [22]. The Evolved Packet Data Gateway (ePDG) attaches un-trusted non-3GPP access networks like WLANs to the EPC and performs important security functions such as tunnel authentication/authorization and IPSec encapsulation/decapsulation of packets. The Access Gateway (Access GW) interconnects trusted non-3GPP access networks like WiMAX with the EPC. The components for the UE mobility support have the role of interacting with the core network mobility management components and providing a seamless experience for applications running on UE devices to allow operations such as network attachment or handover be transparently handled. To perform these operations, the UE would require an application component, as the background application running on the mobile device that will orchestrate the normal network management procedures. Such devices with the required software are not yet commercially available. The interfaces from the core network side are defined, but actual implementations on the UE side are largely missing. To provide value-added functionality, the ANDSF situated in the core network assists the UE with information and operator-pushed policies. The ANDSF component has the purpose of communicating with a UE mobility application running on the mobile endpoint device and exchanging information. That enhances both of the Always-Best-Connected cases and also allows the network operator to manage and enhance connectivity on a multi-access environment. The behavior of ANDSF, which uses the S14 interface with the ANDSF Management Objects, [22] is described in 3GPP TS23.402 chapter 4.8 [6]. FIGURE 5 gives a good overview of the existing core network elements and their relation to access management. A Working Policies Policy Engine can co-operate with the ANDSF, which allows for the delivery of dynamic and subscriber-specific Inter-System UE mobility policies. The operator can configure dynamic behavior by checking various conditions (e.g. subscriber category, access point names, access restrictions, etc.) and, accordingly, by providing parameterized action (e.g. time-based) to reorder and to indicate its prioritized access network hand-over policies to the UE.

2.2.1 User-centric approach

This research stresses the importance of user’ choices over the operator’s predefined preferences. This means that 3GPP access through a Serving Gateway works as the operator has defined it. Handovers and other mobility-related functionalities are not affected. However, non-3GPP networks, such as trusted and

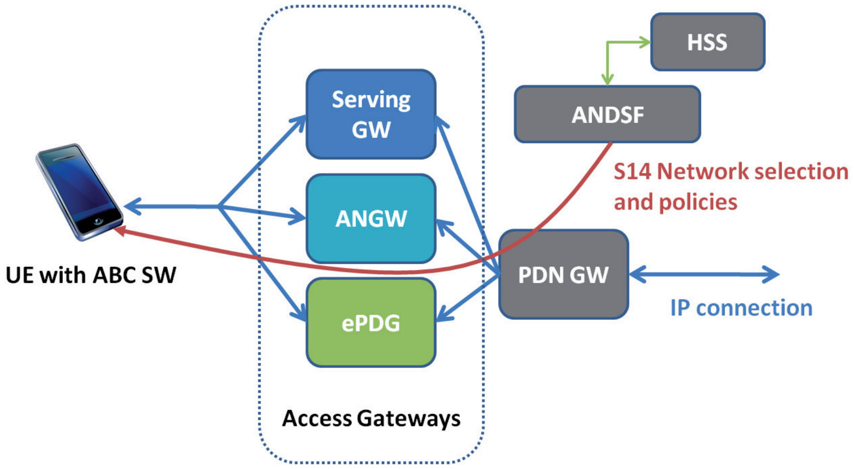


FIGURE 5 3GPP Access Network Discovery and Selection Function in action

untrusted IP access networks, are within the scope of user preferences. Next, existing standard-based mobility support is discussed, followed by the properties of a more user-centric approach.

Further, the parameters of the Inter-System Mobility Policy can be for example, validity areas, time intervals, etc. Once the UE receives a set of such policies, it will apply its current parameters to find a matching policy with the highest priority. From this, the UE can directly extract, for access networks, an operator-ordered list that indicates the operators' suggested solution for the given client's profile, location and the time of the day.

Among the parameters ease of use is the one that fits the operator-based model. In there, all the preferences are defined by the operator, and no extra effort is required before or during the usage. The same applies to services in case the services are something that the operator is offering. However, quality, common Internet services and especially the cost may not be the best for the user. In terms of quality, the WLAN can, in most cases, provide better bandwidth and latency compared to widely deployed 3GPP networks (UMTS, GSM), and WLAN networks are available in homes, offices and various hotspots. This means that they should be utilized whenever possible. Costs of mobile broadband have been dropping due to service provider competition and/or regulations. Still the mindset is that of avoiding costs whever possible. Flat rate contracts on mobile broadband are reducing the importance of cost. These user preferences can be taken into account in UE-based application, and the same application could also take care of network selection defined by the operator through EPC. This application could be called an ABC application. Its role is that of orchestrating the mobile client attachment/detachment procedures during the hand-over operations from one Access Network to another. As such, it allows for a seamless experience for the EPC UE clients, by managing the IP connectivity layer operations. It provides wrapper functions to connect and disconnect from each individual access network available, by reusing the client device's standard Layer 2 and 3 attachments.

For orchestrating smooth hand-over’s, the actual connection and final selection of a connection are provided with a fine-grain control mechanism to be used from the application layers, or managed transparently by the ABC application based on the Inter-System Mobility Policies, received from the ANDSF. The ABC application implements the ANDSF S14 interface, which allows for exchange of information between the core network and the clients. With this mechanism in place, the ABC application can provide the ANDSF its updated network location and connectivity information and it can also receive from the ANDSF coverage maps in the form of Access Network Discovery Information and hand-over indications in the form of Inter-System Client Mobility Policies. Based on the operator-pushed Inter-System Mobility Policies, the ABC application can transparently handle (if configured by the subscriber) the operator’s indications and requests. Besides this network-triggered hand-over mechanism, manually triggered hand-over’s on subscriber’s request are, of course, supported and have the highest priority over the network-triggered ones. For performing all these operations and for retrieving IP connectivity information, the ABC application should have an API towards the client application layer, which allows for easy integration with existing and future applications.

2.2.2 A novel approach to Always-Best-Connected IP network

In this research the network selections are designed to be simple and straightforward. There should not be any need for complex calculations. The justification for this comes from real-life. When we look at today’s devices, we discern mainly two possibilities for connectivity to Internet services: one through the operator’s cellular access and another one through WLAN (IEEE 802.11b/g/n). The 3GPP TS 23.402 standard’s chapter III referred to above gives information about how cellular and WLAN access could be combined by the operator [6]. This must be taken into account when designing a network selection algorithm for an Always-Best-Connected application.

2.2.3 Algorithm design for Always-Best-Connected application

The main goal of algorithm design is to get support for the EPC system and, if it is not available, find the most suitable connection for each application. In the approach used the following basic assumptions are made: 1. The user is in control: if some connectivity is set up, specifically by the user, for some application, then it must be respected. 2. Operator provided information (ANDSF) will be used if the information provided has heterogeneous networks defined. If it contains something else, then just cellular networks are used. 3. Otherwise the ABC algorithm is applied. The algorithm itself is, as far as possible, simple and straightforward. Complexity is avoided by making direct choices based on predefined preferences. The idea is to have either/or choices, that is, some condition is either true or false. This choice has to be made always when an Internet access is requested for a particular application. The main question/decision steps (True/False choices) for access point selection in the algorithm are:

1. Is there valid ANDSF information available?
2. The application is a part of a profile; is the profile active/valid?
3. Is the application real-time? Always ask for the used accesspoint
4. Is there a known protected WLAN connection available?
5. Is there an open WLAN connection available?
6. Use cellular IP connection.

Profiles are user-defined groups of applications and access points made to ease configuration. For example, the user can create home and work profiles where the access points are known. Thus, in the user's home profile the connections are through a home WLAN and in the work profile through a company WLAN. For real-time applications (as in FIGURE 7), it is better to have them in the always-ask mode, where the user equipment asks the access point when the application is launched or signed in. The always-ask mode enables the user to rationalize access point usage. During working hours or at home it is reasonable to a have connection through WLAN. For any other application one should just check if there is a protected or an open WLAN available and, if not, then fall back to a cellular IP connection. The algorithm needs to be revisited if the user equipment is moving and the network environment changes. In case of EPC (valid ANDSF information is available), it should not be any problem, as EPC supports seamless vertical handovers. There might be delays in packet routing and possibly packet loss, but connections should still remain. However, outside EPC the case is problematic from the mobility point-of-view. There is no other choice then but to drop the existing connections and form a new one, based on steps 2 to 6. Thus, there is no real mobility, as connections need to be rebuilt. It is up to the specific application to deal with connection loss.

2.2.4 Proof-of-Concept performance environment for ABC algorithm

In this section, a user and device-centric Always-Best-Connected proof-of-concept implementation and performance measurements are presented. The scenario shows how an ABC application, in the UE side, is able to handle user mobility between access networks. The application is functioning, in agreement with the operator information from EPC, based on the ABC algorithm. Initial performance measurements without the novel ABC algorithm are presented in **PI**. The network-change times in the open network were around one to ten seconds, depending on network conditions and on whether the measurement environment was Android or Maemo. The link quality and load affect the change of network, especially in case of real-time traffic [23]. In this research, two main scenarios were implemented: one with EPC mobility and another one without it. The implementation was done in the Android software environment. FIGURE 6 shows the test setup. The test bed consisted of simulated Evolved Packet Core WLAN accesspoints: one of these was operator-trusted and the other one was untrusted.

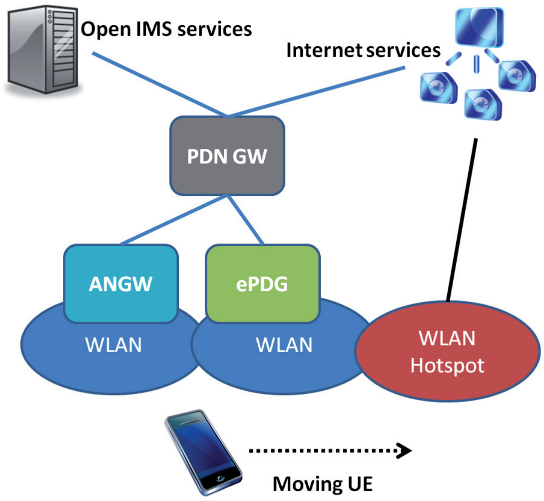
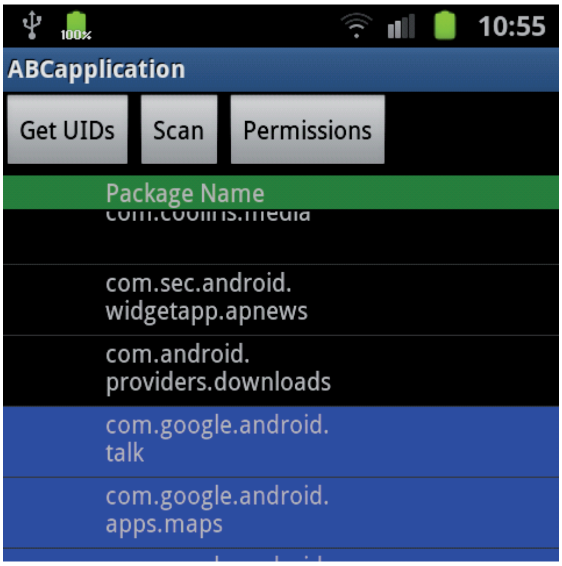


FIGURE 6 ABC algorithm Proof-of-concept test setup



com.sec.android.
widgetapp.apnews

com.android.
providers.downloads

com.google.android.
talk

com.google.android.
apps.maps

FIGURE 7 The ABC application permission page (Google Talk)

TABLE 1 Network-change delay in open access

	WLAN (msec)	σ	UMTS (msec)	σ
Android	941	203	2546	1001
Maemo	4125	394	5424	175

Besides the EPC, there were two other WLAN networks: one of the hotspot style, with only one WLAN base station, and another one with the WLAN infrastructure network with multiple basestations. Cellular access was through UMTS bases tations to live network. However, since there was no control over the live network, the results against the live network are to be considered as informative only. The following scenarios were defined: 1. network change between a public hotspot and an infrastructure WLAN network. 2. authentication overhead in a network change within EPC from a trusted WLAN to an untrusted one. In this scenario, the UE needed to authenticate itself before a connection could be made.

2.2.5 Network-change performance results for ABC algorithm

Network-change times between a public hotspot and an infrastructure WLAN are presented in Table 1. The table results show that network change can happen in about one second with a small standard deviation. During the measurements, the WLAN network was not used by other users. Clearly, the performance was not sufficient for real-time traffic, as gaps such as this are not acceptable (over 200 ms, which is generally kept as the limit for real-time communication). Informative measurements against a live network are also shown in the same table. There is notable delay in the live network when compared to WLAN. In contrast, Table 2 depicts the measurement results with the second scenario where authentication was required by the EPC. Three different approaches were examined: SSL tunnel in a Virtual Private Network style, SSL tunnel (only as in Browser) and IPsec tunnel. As the table shows, creating a real SSL tunnel was time-consuming. The advantage of this approach is that the VPN hides the IP change. That again makes mobility from the application point-of-view possible if the connection properties otherwise allow it. For example, keep-alive messages will not go through during a network change. The SSL tunnel only solution was clearly faster than complete tunneling but not suitable for real-time traffic when one adds the delay expected from an EPC network (over 200 ms just for authentication and EPC processing). IPsec provided a slightly faster response than real SSL tunneling. Still, even that solution was causing problems for real-time communication.

To summarize, off-the-shelf solutions cannot provide suitable real-time network change performance. For EPC authentication requirements, there were no standard-based solutions available at all, and the modified solutions did not work fast enough. The IPsec-based solution based on Linux gave hints that performance will improve with increasing computing power in mobile devices.

TABLE 2 SSL and IPsec handshake times over TCP

	WLAN (msec)	σ
SSL with VPN (Android)	2690	172
SSL tunnel only (Android)	109	47
IPsec in Linux	2083	189

2.2.6 Android device in a simulated EPC heterogeneous network environment

This section dealt with real-life long-delay problems when performing network changes in heterogeneous networks. These delays can be perceived by end users as service blockers in real-time communication. A simple and straightforward network selection algorithm was presented. Evolved Packet Core support was added, so that the algorithm can utilize ANDSF information when it is available. Through two user scenarios, network-change performance and a selection algorithm were evaluated in an Android-based implementation. Due to challenges in the Android environment, some of the measurements were done in Maemo and Linux-based systems. The measurements did show the difficulty of real-time communication when a network change occurs in a heterogeneous network. All the measurement times were too high to maintain continuous real-time communications. These facts defend the use a of simple and straightforward network-change algorithm. The proposed algorithm makes straightforward either/or choices based on predefined preferences. The algorithm proposes the use of a multibearer solution to handle real-time and non-real-time traffic through different connections. At this point, it was not possible in the Android environment as there could be only one connection at a time. Also, the lack of IPsec tunnels leads to workarounds with SSL tunneling. The results from these measurements further illustrate that the existing devices are not ready for real-time communication within EPC. Tunneling itself was able to make application-level tunneling possible where the communication path could handle lengthy delays during a network change.

2.2.7 Seamless mobility in PMIPv6 environment

The test environment was Proxy Mobile IPv6 based on UMIP OpenAirInterface [24]. The user equipment consisted of Samsung Galaxy SI and II and Linux Lubuntu laptops. The test environment is shown in FIGURE 8. The MAGs and the LMA are Linux desktops connected with a virtual network by HP ProCurve 2650 switch. Cisco Aironet 120s were used as the basestations. In the test setup, the mobility was managed by an LMA based on MAG information. When a PMIP device contacts a WLAN basestation the Media Access Control (MAC) information of the UE is used in the authentication. There is a Freeradius-based authentication server where a syslog service informs the MAG when a UE connects to the WLAN basestation. This information is then forwarded to the LMA which checks wheather the UE is known or not. If known, it returns the network prefix

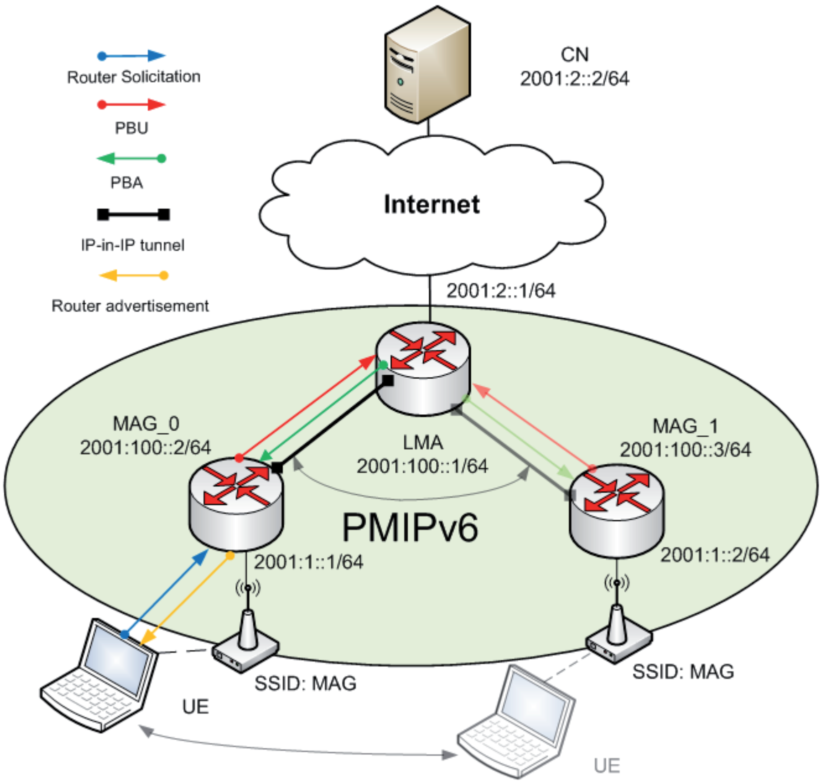


FIGURE 8 PMIPv6 test environment

to the UE that is used in IPv6 address creation.

2.2.8 Seamless Handovers

Two test scenarios were defined for handover tests. The first scenario was UE, where an address outside of a PMIPv6 domain was pinged while a handover between two WLAN networks was taking place. Real-time protocol (RTP RFC 3550) traffic between CN and UE was tested during the handovers. In this scenario, the traffic used 64 byte packets with a 0.5 second interval. The ping was initiated stationary close to the WLAN base station connected to the MAG_0, as FIGURE 8 shows. From there, the UE was moved closer to the MAG_1 WLAN base station causing the MAG_1 to notify the LMA that the UE had moved. As a result of this, the existing tunnel was torn down and a new tunnel was created between the LMA and the MAG_1. The second scenario concerned RTP protocol traffic similar to that in the first scenario but with different buffer sizes and flavors of the streaming protocol. The results are from the case where the bitrate is 96 kbits/second with 200-ms buffer 16-bit monaural audio stream. The measurements with an Android device show one complete session drop (starting around 50 second) that lasted around 20 seconds. Other handovers are visible when the bitrate drops below 40 kbits/second. The second problem is the high packet loss

TABLE 3 Handovers with Linux UE

Sent/Received Packets	12800/12527
Packet Loss	2.1 % 273 Packets
RTT Handover (min, avg, max)	1.27 / 7.69 / 202.00 ms
RTT No Handover (min, avg, max)	1.27 / 5.40 / 20.00 ms

of 23.8 % during the measurements (275 seconds). The average jitter was 20.44 ms. Based on these results, the Android UEs may operate with IPv6 addresses and under PMIPv6 mobility management. However, there are challenges to their suitability in real-time communication.

Both of these scenarios were run also under a Linux environment to compare them with the results from the Android environment. The Linux environment consisted of a Linux Lubuntu distribution with kernel 3.4.4 and the IPv6 options including mobility, IPsec and multiple routing tables. The network used the Zyxel USB wireless card as its interface card. The ping scenario results are shown in Table 3. The packet loss is visible: only about 2 %, and the average round-trip-time is higher where handovers occur. The test was repeated 50 times. The RTP streaming results are depicted in FIGURE 9. As with the Android UE, the handover points are clearly visible when the transfer bitrate drops significantly from 96 kbits/second to 20 or less kbits/second. Unlike with the Android UE, there are no total connection drops. The buffer size is 100 ms (16-bit monaural audio stream). The packet loss is 8.1 % and the jitter average is 20.99 ms during 600-second measurement period. Due to the fact that the handovers were successful with the Linux UE, additional tests with RTP streaming were conducted. The tests were similar but conducted with different stream protocols such as MPEG-1 Audio and MPEG-2 Audio, and with buffer values from 100 to 300 ms. These results show zero jitter, as the jitter was eliminated by the buffer and lower bitrate (16/24 kbits/second). The packet loss was within the range of 4.3% to 6.6%. Video testing was done purely for user experience: a 480p video was streamed from CN to UE while executing handovers. With a 200-ms buffer there was no visible or audible indication that the handover would have occurred. As a summary, the Linux UE was able to achieve seamless handovers in a PMIPv6 controlled network environment. The packet loss was there as expected but its effect on real-time communication remained non-existent with the executed bitrates and content.

2.3 Need for Mobility Management

The classical definition of traffic classes has a connection to 3GPP Universal Mobile Telecommunications System (UMTS) QoS classes, which have been defined since the 3GPP release 99 in the Quality of Service Concept and Architecture [25]. There are four different classes:

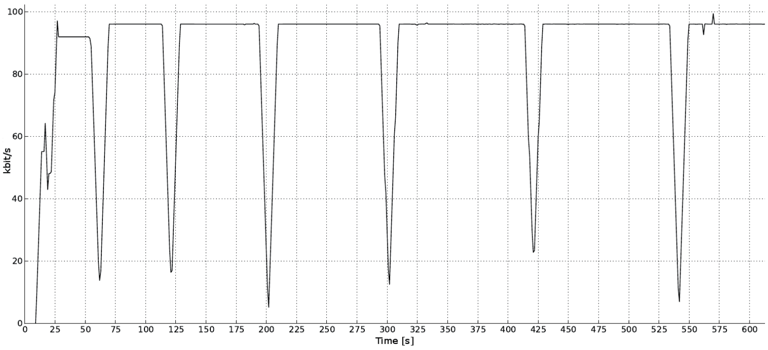


FIGURE 9 RTP traffic with a 100-ms buffer in Linux during handovers

- conversational
- streaming
- interactive
- background

The main distinguishing factor between these classes is the delay-sensitivity of their traffic. The conversational class is targeted for traffic which is very delay sensitive while the background class is the most delay insensitive traffic class. What are the real use cases of today in different traffic classes? And what, in these real services, is the effect of missing mobility management?

2.3.1 Context and its relations to services

The most well-known use of the conversational class is telephony speech. However, in this research the focus is on IP traffic and in this case the natural counterpart is the Voice over IP (VoIP) speech. Real-time conversation is always performed between peers (or groups) of live (human) end-users. This is the only scheme where the required characteristics are strictly related to human perception. In the streaming class, the real-time data flow is always aimed at a live (human) destination. On the other hand, it is a one-way transport, as responses are not expected, not at least in real time. It is important to preserve time relations between the information entities of the stream. The interactive class end user is either an online machine or a human requesting data from a remote equipment such as a server. Overall, this type of communication is characterized by the end users' request response pattern. At the message destination, there is an entity expecting the message (response) within a certain time. The key attributes are round-trip delay and low-bit error rate. Finally, in the background class the end user is typically a computer, usually sending and receiving data files in the background. The scheme is more or less delivery-time insensitive. The conversational class is perhaps the most demanding, as it deals with real-time communications between human end-users. The obvious use case is Voice over IP (VoIP) and one of the best known services is Skype. Streaming, on the other hand, has remained as specified in the traffic class. Services based on video streaming, for example YouTube, have gained popularity both in the desktop and mobile world. Streamed videos are usually buffered as far as possible. The most obvious use case for the interactive traffic class would be web-browsing. This usage exhibits the request response pattern, and although there are no hard latency values, the user expects fluent response and transmission without errors. The background class, on the other hand, uses cases related to activities taking place in the background beyond the user's immediate attention. Good examples of that are weather widgets, an email-fetch and file uploads or downloads.

2.3.2 Algorithm with context and location awareness

Bringing along context and location awareness assumes for more intelligence from the ABC algorithm. When the traffic classes and their real-life counterpart applications were examined, it became obvious that simple detection and classification of applications would be challenging. For example, the proprietary protocol of Skype was not trivial to detect nor was the YouTube streaming based on Flash player. Equally, highly context-sensitive bulk data transfer, such as FTP that cannot recover from a connection change, could be identified easily but without any mobility management could not be properly managed. Context sensitiveness was related to actual transfer of data, the idea being that when there is enough traffic there is also context that must be respected. An additional step was added to monitor network traffic. By doing this, the algorithm can keep the existing connection whenever there is a homogeneous network available. Location-based data were utilized in an ABC application context in the form of cell ID. This way, the preferred access network could use the visited network history as a clue for discovery of the preferred connection. The history data was a cell ID list of five most recently visited cells. The idea was that when the current cell ID is found on the preferred connection list, no network change will occur unless the UE runs out of coverage as in FIGURE 10. A clear advantage of this is that when the UE camps on an everyday geographical area then the preferred access network will be able to keep the preferred connection. Equally, when cell ID is not found on the list, then the UE is either travelling or orienting back to an everyday geographical area. The main steps of inquiry for access point selection are:

1. Has a valid preferred connection been selected and cell ID found from the history list?
2. Network traffic is above threshold: no changes to access point unless connection lost?
3. Is there a known protected WLAN connection available?
4. Is there a open WLAN connection available?
5. Use cellular IP connection.

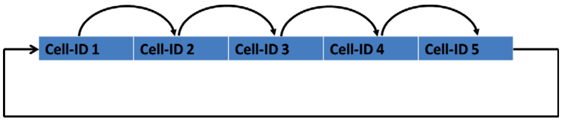


FIGURE 10 History-based location awareness for ABC application

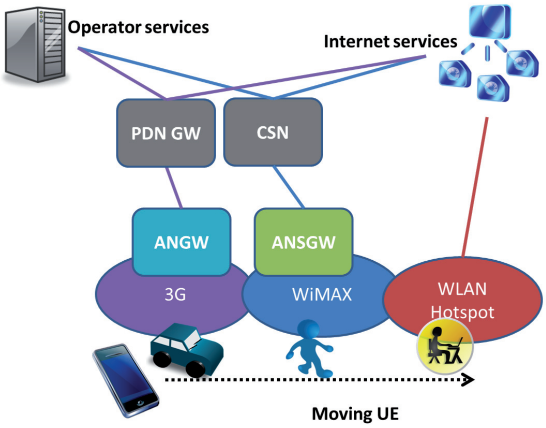


FIGURE 11 Context- and location-aware ABC application proof-of-concept test setup

2.3.3 Proof-of-concept implementation

The functionality and real-life performance was evaluated through use case scenarios. The classes and their equivalent services were: Conversational - Voice Over IP call by Skype, Streaming - YouTube, Interactive - Facebook and Google Chat as a social media service, Dropbox as a cloud service, Background - File Transfer Protocol (FTP) and Flickr as a bulk and background data transfer. Initial performance measurements without any particular ABC algorithm were done earlier in **PI**. The link quality and load influence the timing of network change, especially in case of real-time traffic [23]. FIGURE 11 depicts the test setup, where three access networks, each with a different technology, were available: WiMAX, UMTS 3G, and hotspot WLAN. Each of the networks is operated by a different operator. The test run was repeated, with service derived from the traffic class. The ABC application did take care of network change by selecting the best access network. The ABC application was developed on top of Linux.

2.3.4 Results without context and location awareness

The route was the same always. Testing started from the 3G coverage area. The UE moved under the WiMAX coverage and finally under the WLAN coverage, where the UE camped stationary until the test scenario ended. First, the UE was in a vehicle, which started moving closer to a WiMAX base station at an approximate speed of 40 km/h for a distance of roughly 1.2 km until it stopped on a parking area, where the UE was removed from the vehicle. At this point, the

WiMAX coverage was excellent and the UE camped there for a minute. After that, the UE started moving, at a walking speed, inside the cafeteria where the WLAN coverage was available. The walking distance was 300 meters and the starting point was outside the WLAN coverage. Finally, inside the cafeteria the UE was stationary for 2 minutes until scenario ended.

The Results for the services were:

- Conversational Skype: the call was interrupted each time when the underlying network connection changed. However, the call itself was not terminated, instead the connection continued when it was re-established.
- Streaming YouTube: streaming was started before the test execution began. During network change, the buffered stream was consumed and the view paused. After an access network change, the streaming was continued by manually selecting a time beyond the previously buffered stream section.
- Interactive Google and Facebook chats: these were nearly unaffected by the network change. With the Facebook, there had a short period of unavailability during the network change. Still, the messages were buffered during that time and delivered when the user got back online.
- Background Flickr and FTP: the data transfer was started before the test execution. In both cases the data transfer was disconnected when access network was changed.

2.3.5 Results with context and location awareness

The scenarios were run with two different sets: (a) one with empty location information and (b) one with known WiMAX location information where WiMAX was set as the preferred connection. In the conversational class with the Skype call (case a), there was so much data traffic that the algorithm considered it to be real-time traffic and kept the original connection (3G) until the call was terminated by the user in the cafeteria. After that the connection was changed to WLAN. In case b, the operation was similar otherwise, but in the cafeteria the connection was changed to WiMAX, as the cell ID was in the location list and it was considered to be a preferred connection. Functionality was similar in the streaming class with YouTube in both of the sub-cases. In the interactive class, the Facebook and Google chat did not create enough traffic for the algorithm to keep the connection fixed. In case (a) the change was first to WiMAX and then to WLAN. However, the chat session was not affected any more than in the original case without context and location awareness. In case (b), the UE changed to WiMAX once it became available. It was found from the last visited list, and it camped there until the test ended, as it was the preferred connection. The Dropbox case created so much traffic that the ABC algorithm considered it a real-time application and did not change the access network until synchronization was complete. As with the conversational class in case a, the connection in the cafeteria was changed to WLAN and in case b to WiMAX. The background class had the same functionality as the Skype call and Dropbox synchronization. The ABC application considered continuous traffic as a real-time traffic and kept the existing connection. The connection was changed once the data transfer was complete.As the results show, straightforward context and location awareness has clear advantages from the user point-of-view. The services consumed by the user are not interfered by the network changes and the preferred connection works well when the user moves around in a geographically restricted area, for example between home and work. Equally, there are challenges with the context and location awareness. At this point the traffic is not classified only the amounts of traffic are monitored. There is no cost optimization, although the preferred connection selection can assist in cost reduction. Location awareness is not effective for highly mobile users. It is based on visited cells and has no ability to predict future movements.

2.4 Summary

This chapter illustrates a user-centered approach to the Always-Best-Connected model by coupling the state-of-the-art telecommunication technologies, next generation network domain and user preferences. A generalized connection aware service architecture enabling mediation between network and services access was presented. The components of the architecture were discussed. There was a special focus on the user-centric mobility management enhanced with the operator predefined preferences. The ABC application is a key component in the architecture. The application manages the standard way as defined in EPC and also takes into account user preferences. This paper dealt with real-life long-delay problems when performing network changes in heterogeneous networks. These delays might be perceived by end users as service blockers in real-time communication. The paper presented a simple and straightforward network selection algorithm. Evolved Packet Core support was added, so that the algorithm can utilize ANDSF information when it is available. Through two user scenarios network-change performance and a selection algorithm were evaluated in an Android-based implementation. Due to challenges in the Android environment, some of the measurements were done in Maemo and Linux-based systems. The measurements did show the difficulty of real-time communication when a network change occurs in a heterogeneous network. All the measurement times were too high, to maintain continuous real-time communications. These facts defend the use of a simple and straightforward network-change algorithm. The proposed algorithm makes straightforward either/or choices based on predefined preferences. The algorithm proposes the use of a multibearer solution to handle real-time and non-real-time traffic through different connections. At this point, it was not possible in the Android environment, as there could be only one connection at a time. Also, the lack of IPsec tunnels leads to workarounds with SSL tunneling. The results from these measurements further illustrate that the existing devices are not ready for real-time communication within EPC. Tunneling itself was able to make application-level tunneling possible where the communication path could handle lengthy delays during a network change. To improve real-time communication, the context and location awareness information was added as a preference for ABC application. The algorithm uses network data traffic monitoring to identify ongoing context and avoids tearing down these contexts if network coverage allows it. Location awareness was included in the form of history location data by storing cellIDs of the preferred network. The proposed algorithm was implemented and tested in a real-life heterogeneous network environment. The test setup was derived from the four 3GPP traffic classes: conversational, streaming, interactive and background. The tests did show that from the user's point-of-view the experience can be maintained and the most suitable network will get selected once the service allows it. Location data will work as enforcing policy for the preferred connection in a geographically most visited area. Still, it is clear that without mobility management conversational traffic will remain outside all-IP communication solutions.

Finally, the chapter dealt with seamless handovers in a Proxy Mobile IPv6 managed network environment with Android and Linux User Equipment. Although the IPv6 is not officially supported by the Android operating system, enabling it was possible. The limitations were that the network manager requires an IPv4 address to keep the connection alive, routing of IPv6 addresses was limited, and, as the framework was not supporting the IPv6, it is up to the particular application to support IPv6. The PMIPv6 support in the Android and Linux UE is coming from the kernel support to the various IPv6 options that can be included into UE. The chapter presented a test-bed for PMIPv6-based mobility management. With the help of two user scenarios handover performance and its effect on user experience were evaluated in an Android UE. Due to the challenges in the Android environment, the same measurements were repeated in a Linux UE as well. The measurements did show some challenges with the existing Android UEs, for example dormant WLAN-roaming there resulted in bigger packet loss than with the Linux UE. On the other hand, with the Linux UE, measured handovers were successful and packet loss had a minimum or no effect on the user experience. These facts defend the use of PMIPv6 on mobility management in EPC, and Android may support it once the challenges presented have been solved.

3 CHALLENGES FOR THE MOBILE USERS

This dissertation examines the problem domain in a practical way, if possible: all ideas presented are tested in real-life environment. This is challenging since the Android framework is not supporting many of the standards used. However, Android is Linux-based, and there are open source alternatives to stock Android versions. It is possible to enable many of the missing standards and features. Furthermore, the heterogeneous network environment was setup through the research. 3GPP EPC was not commercially available during the research, thus the an own network setup was needed. Depending on the research topic, different features were built up, including user authentication, IPv6 network, PMIPv6 mobility management or some cases the network was considered as a predefined constant, for example as a delay. For user experience, one of the key factor related to user mobility is power efficiency. Sooner or later the mobile devices need to charged and that is why it is beneficial to have knowledge of power efficiency related to network selection, mobility and other choices that are made.

This chapter presents some of the challenges faced, which were related to UE and heterogeneous network, and workarounds that were used to overcome these challenges. In addition, the basic principles of power measurements and efficiency are presented in this chapter.

3.1 3GPP Evolved Packet System and Its Challenges for the User Equipment

The 3GPP TS23.402 architecture enhancements for non-3GPP accesses [6] and 3GPP TS access to the 3GPP Evolved Packet Core (EPC) via non-3GPP access networks [26] are specifying requirements toward UE. One of the basic definitions is that for IP Flow Mobility (IFOM) and another one for Multi Access PDN Connectivity (MAPCON) where the packet data connections are going through different access networks. This is not currently supported by the Android environment. When changing connection, the existing connection is disconnected before a new one is created.

The IP Mobility Management Selection (IPMS) principles state, naturally, that UE and network must support the same mobility management mechanism. The two main choices are network-based mobility (NBM) and host-based mobility (HBM). In case of HBM the defined protocols are Dual Stack Mobile IPv6 (DSMIPv6) [27] and Mobile IPv4 (MIPv4) [28]. Another critical fact is whether the IP address preservation can be utilized to gain session mobility during vertical handover. Upon initial attachment to 3GPP access, no IMPS is necessary since connectivity to PDN GW (see FIGURE 5) is always established with network-based mobility. Upon initial attachment to a trusted non-3GPP access or handover to it, IMPS is performed before an IP address is allocated and provided to UE. When applying NBM the session continuity can take place according to Proxy Mobile IPv6 RFC 5213 or by the legacy GPRS tunneling protocol [29]. In contrast with HBM the session continuity which can take place in case the network is aware of the UE capabilities to support DSMIPv6 or MIPv4. Unfortunately, Android does not support Proxy Mobile IPv6, so at this point the only solution would be to rely on GTP for non-3GPP access. However, GTP is a proprietary legacy protocol that is not currently supported by WLAN setup boxes.

Another challenge is the UE authentication. Trusted/untrusted non-3GPP access network detection has the following options: non-3GPP must support 3GPP-based authentication to enable the UE discover the trust relationship during 3GPP authentication. Or, the UE operates on the basis of a pre-configured UE policy. The user authentication is based on Network Access Identifier [30], where the International Mobile Subscriber Identity (IMSI) is used as identifier. This information can be constructed in Android environment. Authentication procedure itself takes place through Extensible Authentication Protocol Authentication and Key Agreement EAP-AKA [31], which can be handled in an Android environment, as it is the basis for UMTS Authentication. However, the connection from untrusted non-3GPP access to ePDG must be secured and this is done via the IPSec tunnel. This is something that is not supported by default in the Android platform.

As stated in previous section, the ANDSF situated in the core network assists the UE with information and operator-pushed policies. ANDSF management objects are XML-based, and the challenge is to provide this information to UE. The specification defines push and pull types to receive or get ANDSF data. In the pull type, the discovery can happen over a DNS query to a predefined address or with the help of a DHCP query as specified in RFC 6153 [32]. A push type message exchange can take place over OMA Device Management [33] via WAP push but only in 3GPP access networks. In Android environment, DHCP query as specified in RFC 6153 is not supported, and also OMA Device Management is not so clear. Support is not promoted but since the basic idea is the same in multimedia messaging it's likely that the support is there. On the other hand the EPC specification is somewhat loosely written, and it might be possible to deliver the ANDSF information other ways, too. As a summary, the Android software environment as such (versions 3.2 and 4.0) cannot support all the requirements specified by EPC. The biggest challenges are:

- Lack of simultaneous connections
- Lack of IPSec
- Lack of PMIPv6
- Lack of DHCP query as specified in RFC 6153

It is clear that these limitations are software related and can change at any given time when they get implemented. However, at the present time existing terminals are not compatible with the off-the-shelf Evolved Packet Core. As simultaneous connections and IPSec support are the ones that are handy with existing networks, (my personal expectation is that) they will be implemented first.

3.2 Implementation Challenges and Workarounds

This section presents modifications to the Android framework which were done during this thesis. The authentication challenges with 3GPP EPC and enabling the PMIPv6 protocol support are also discussed. Finally, a workaround for lack a of simultaneous connections is presented.

3.2.1 Android framework modification

During the research, the Android framework had to be modified for implementing features or enabling protocols outside the default off-of-shelf Android. The default Android environment had to go through the following changes:

- CyanogenMOD software as a baseline for software development: for example, CyanogenMOD 9 is based on Google's Android 4.0 Ice Cream Sandwich
- Semaphore Kernel: for example, version 1.3.0 and Linux 3.0.17 for multipath support in the kernel
- A wpa_supplicant for WLAN authentication
- Busybox for a test setup

where CyanogenMOD is an open source replacement firmware for smart phones and tablet computers based on the Android framework. Semaphore [1] kernel can be used with CyanogenMOD, and as an open source product it may be combined to the include required features in the kernel. wpa_supplicant is a free software implementation of the IEEE 802.11i standard and specifies security mechanisms for wireless networks. Finally, Busybox is a single binary including many stripped-down Linux tools. It is specifically created for embedded operating systems with limited resources. In this thesis context it is used to configure and execute test setups such as routing table changes and to execute test programs and timers.

---

[1] http://www.semaphore.gr/

3.2.2 IP version 6 and Proxy Mobile IPv6 support in Android framework

Android is a Linux-based operating system, mostly for portable devices such as smartphones and tablets [34]. At the moment, it is the most popular smartphone operating system. However, IPv6 is not officially supported by Android. Despite this, the Linux kernel in Android is supporting IPv6. This allows an IPv6 traffic if the network provides an IPv6 address and the application on top of Android can support it. Some challenges remain, however. The Android network manager can only manage IPv4 addresses. If the network is not providing an IPv4 address, the network manager considers the address faulty even when a valid IPv6 address is provided. Another challenge relates to stateless autoconfiguration of IPv6 addresses [35] where IPv6 addresses that use MAC address hiding might not be routed correctly by the Android system. Finally, by default the Android kernel is lacking mobility management protocol support such as PMIPv6.

Workarounds for these challenges are available. The IPv6 address can be manually setup to 0.0.0.0 as a non-routable address. After this, the Android network manager is contented and can keep the access connected and IPv6 addresses can be used in communication. The routing problems with a MAC address-based IPv6 address can be avoided by prohibiting the use of temporary addresses. This can be done with sysctl (an interface for examining and dynamically changing parameters in Linux). By the prohibition of temporary addresses the network interface obtains only the global and link-local address that are suitable for communication. PMIPv6 itself does not require any action from the applications using it. On the other hand, the kernel needs to support basic mobility-related options such as: Mobility, IPsec, Multiple Routing Tables, and source-address-based routing. These need to be included into the UE kernel. Further details about how to compile and install the kernel can be found from the Cyanogen MOD 9 [2] setup pages. With these modifications the Android UE can be put to handover tests.

During the test, in addition to IPv6 configuration challenges, there was a lack of functionality with the Internet Control Message Protocol (ICMPv6 [36]) and WLAN roaming. An ICMPv6 challenge was encountered when connecting to a PMIPv6 network via the MAG and authenticating with the LMA by sending a router solicitation message to the MAG, the responses being a router advertisement message. After that, the MAG and the LMA created an IP-in-IP tunnel between them for UE traffic. The UE and the MAG kept the connection and the tunnel alive with the help of neighbor solicitation (NS) and neighbor advertisement (NA) messages. The tunnel and the connection were kept alive while producing traffic, e.g. pinging to the correspondent node. In other cases, the tunnel was torn down. There is a relevant issue reported on the web [3].

Another challenge was a WLAN roaming problem related to the fact that the Android UE did not change its WLAN accesspoint as expected. Instead, the UE kept the existing connection until the connection was dropped due to poor signal level. The UE did not change from MAG_0 to MAG_1 until it was too late

---

[2] Android version 4.0.4

[3] http://code.google.com/p/android/issues/detail?id=32662

to achieve a seamless handover. There is an issue reported about it on the web [4].

3.2.3 Authentication challenges with Evolved Packet Core

For EPC authentication, the aim was to use IPsec [8] tunneling as defined in the standard. The idea was that the UE-related actions would be done in as realistic manner as possible. Nevertheless, this was not possible within the Android software environment. Instead, the SSL tunnel, which is widely used in web browsers was employed. This was considered to be the next best choice. IPsec tunnel creation times were tested in the Linux environment to get an idea of the performance of a real-life implementation. Additional challenges in the Android environment were the lack of Mobile IP and multibearer connections. This prevented truly seamless handovers between simulated EPC access points since only one connection was possible at a time. All the applications in the UE had to use the same connection.

3.2.4 Workaround for the lack of simultaneous connections

One of the key features for ABC in a heterogeneous network environment is its ability to make vertical handovers. These handovers are the ones where the existing connection is changed from one technology to another. They have been considered complex and as generating a number of requirements. The performance of vertical handover with an Android-based Virtual Private Network implementation is examined in a real-life heterogeneous network environment. FIGURE 12 depicts the test setup. Performance of vertical handover from legacy 3GPP (UMTS live network in Finland) to a simulated EPC network is measured and its suitability to real-time and non-real-time communication is discussed. The EPC network access is considered as an untrusted and non-3GPP type, being in this case a WLAN hotspot. Unfortunately, there is no real EPC core environment available, so the network elements are modeled as delays in the communication path. The estimated delay for EPC in this research is 100 ms. There is research using lower values, such as 10 ms, for legacy 3GPP networks [23]: this however feels very optimistic. A secure connection is created between UE and EPC via a WLAN hotspot. Since there are known limitations in the available Android environment, these needs to be handled in a different manner. The lack of PMIPv6, simultaneous connections and IPSec are covered by using a Virtual Private Network (VPN) in Android UE. This way, the applications using the VPN connection get an internal IP address that they use all the time. The IP address changes in network access do not affect this internal IP address. Delay and packet loss is occasioned by network access change. However, in this research the author considers only the time delay caused by the vertical handover. Its effect on individual applications is out of the scope. The same applies to the packet loss if it depends on the bitrate of used application. Overall, the usage of VPN can cover PMIPv6 for a single application. In a similar way, VPN hides the network

---

[4] http://code.google.com/p/android/issues/detail?id=12649

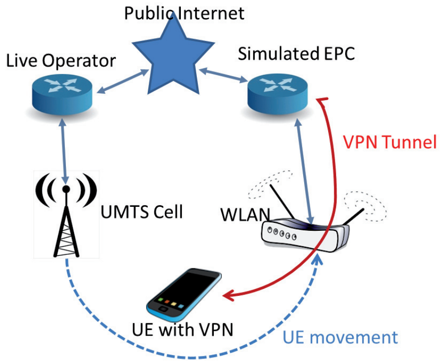


FIGURE 12 Vertical handover test setup for VPN-based mobility

TABLE 4 Vertical Handover and EPC delays

All values in ms	
Action	3G to WLAN
UE Authentication (VPN)	6893
Estimated EPC delay	100
Total time	6993

access changes from an individual application using VPN even the VPN has to re-create the tunnel after the previous network has been disconnected and the new network connection is made. The lack of IPSec is also covered by VPN: as IPSec is not supported, a VPN can be created by a Secure Sockets Layer (SSL) which is widely used in web browsers. This was considered to be the next best thing. Finally, the last missing functionality, the DHCP query as specified in RFC 6153 for ANDSF information availability, is covered by the assumption that either the Android UE used supports OMA DM or an XML file is made available by other means. In this performance evaluation it is available (in the UE), and it only shows that a WLAN hotspot is available for connections. The real-life measurement are shown in Table 4, (the standard deviation for UE Authentication was 1943 ms). As the table shows, real VPN tunnel creation and network change was time-consuming. Clearly, the performance was not sufficient for real-time traffic, as gaps such as this are not acceptable (over 200 ms which is generally seen as a limit for real-time communication). A complete analysis of the details about what is generating this delay is still unclear. Nevertheless, the delay might be shared nearly equally between the disconnection and connection of network access and re-recreation of the VPN tunnel. To summarize, this solution cannot provide suitable performance for real-time applications during vertical handover.

3.3 Power Consumption

Mobile Internet has rapidly evolved in the past years with an ever-increasing number of novel technologies and services and with a variety of access technologies for them. Indeed, today's mobile devices often support multiple communication technologies for accessing Internet services. For users, accessing these data hungry services means that the mobile device has to be charged more often. Energy efficiency in mobile device communication has been considered to be out of the users hands. The concept of Always-Best-Connected (ABC) allows a person to connect applications while using the devices and access technologies that best suit to his or her needs, thereby allowing a combination of the features of access technologies to provide an enhanced user experience for future Internet. This Always-Best-Connected scenario can make a mobile device more energy efficient by using always the most energy-efficient connection.

Mobile communication networks and connected devices consume a small fraction of the global energy supply. However, meeting the rapidly increasing demand for more capacity in wireless broadband access will further increase energy consumption. For example Cisco Visual Networking Index: Global Mobile Data Traffic Forecast 2010-2015 expects a compound annual growth rate of 92 percent during 2010 to 2015 Operators are now facing the need to invest in denser and denser networks while facing increased energy costs. Current cellular systems based on Universal Mobile Telecommunications System (UMTS) and Long Term Evolution (LTE) are characterized by high spectrum efficiency combined with low energy efficiency. In urban areas as well as in homes and offices alongside cellular networks and WLAN networks are available. In this heterogeneous network environment communication energy efficiency can make a significant difference when considering how often the user has to recharge the mobile device.

3.3.1 Energy-efficient Always-Best-Connected user equipment

In this research the network selections are designed to be energy efficient but still providing the most suitable connection so that the user experience is not compromised. The network environment in this research is a combination of existing networks such as WLAN, GSM and UMTS and prediction of the future in the shape of Evolved Packet Core. The EPC is there because it changes the way how network mobility is managed and the kind of networks the can be managed under an EPC operator. The main goal of the algorithm design is to achieve the most suitable and energy efficient connection for each application with the help of EPC ANDSF information and, if it is not available, find the most suitable connection otherwise. In the approach used, the following basic assumptions are made:

1. The user is in control: if some connectivity is setup, specifically by the user, for some application, then it must be respected
2. Operator provided information (ANDSF) will be used if the information provided has heterogeneous networks defined

TABLE 5 Standby current consumption

Measurement	Consumption (mA)	Error of the mean
WLAN idle, min. bright.	0.1273	0.0004
WLAN idle, max. bright.	0.2175	0.0007
3G idle, min. bright	0.1265	0.0003
3G idle max. bright	0.2122	0.0004
No mob. Data, Min. bright	0.1261	0.0006

3. Otherwise the ABC algorithm is applied.

3.3.2 Implementation and measurements

In this section, the energy efficiency of Always-Best-Connected application is discussed. The ABC application makes the choices of connection network in a heterogeneous network environment, where we have UMTS cells against live network as well as WLAN and simulated EPC+WLAN network coverage. Test cases were selected from real-life examples but simplified so that measurements could be done reliably. The test cases were: 1. Power consumption when attached to UMTS or WLAN. 2. Handover from UMTS to WLAN and from WLAN to UMTS. 3a. connection creation in UMTS or WLAN and downloading email with an attachment. 3b. Connection creation in UMTS or WLAN and HTTP download. The ABC application did choose either WLAN connection or an EPC+WLAN connection depending on the availability of ANDSF information. The first test case shows the base power consumption when UE camps in that particular network. The second test case indicates the penalty paid if the ABC application decides to change an existing connection in order to save energy in future communication. Test case 3 is there to show the difference in energy efficiency when actually transferring data.

The user equipment was the Android smartphone Samsung Galaxy S II with CyanogenMod firmware[5]. During the measurements the UE had a maximum screen brightness. The power supply was Agilent E3648A. During the measurements, the voltage level was set to 4.0 V (max error 0.05 percent). The power supply was connected to a laptop via a serial cable. A simple application under Windows XP was created to track power consumption over time. The current consumption measurement frequency was once in every 100 ms. The results of test case 1. are shown in Table 5, which shows that there are no significant differences over different connections. It is great importance in which network the UE camps. The second test case results are shown in FIGURE 14 according to which the handover was a consuming operation from the energy consumption point-of-view. However, it was not lengthy operation, so the overall energy consumption remained low. This means that a handover is feasible if there are better and more energy-efficient connections available. On the other hand, the seamless handover was not available, which has an effect on user experience for example in

---

[5] version 7.1

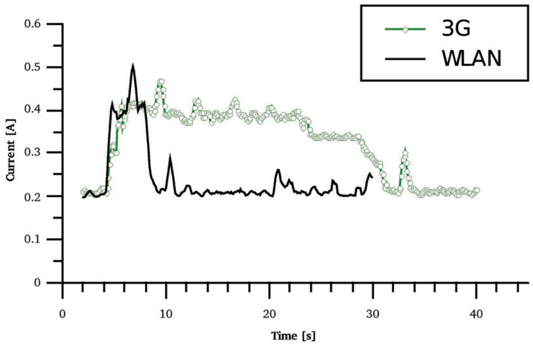


FIGURE 13 HTTP download consumption

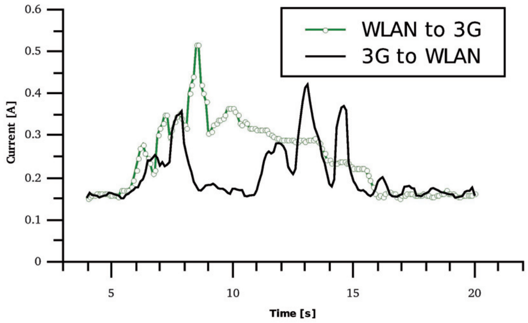


FIGURE 14 Handover power consumption

case the application in use cannot handle connection loss and recreation properly. The third test case was the most significant from energy-efficiency point-of-view. FIGURE 13 show the results from downloads with small and large data amounts. The maximum current consumption is about the same for all the communication methods, but the amount of time used in data transfers makes the difference. The WLAN performance was superior compared to that of UMTS.

3.4 Summary

This chapter dealt with challenges and requirements for User Equipment to enable the Always-Best-Connected IP connectivity. The Evolved Packet System and Evolved Packet Core specification were considered as the latest attempt to enable always-best connectivity to IP network. The specification was examined in detail and its UE requirements were analyzed against the Android 3.0 and 4.0 framework. The examined versions of Android were found to lack the essential features of EPC. The most significant of these lacking features were: simultaneous connections, PMIPv6, IPSec and support for DHCP queries as specified in RFC

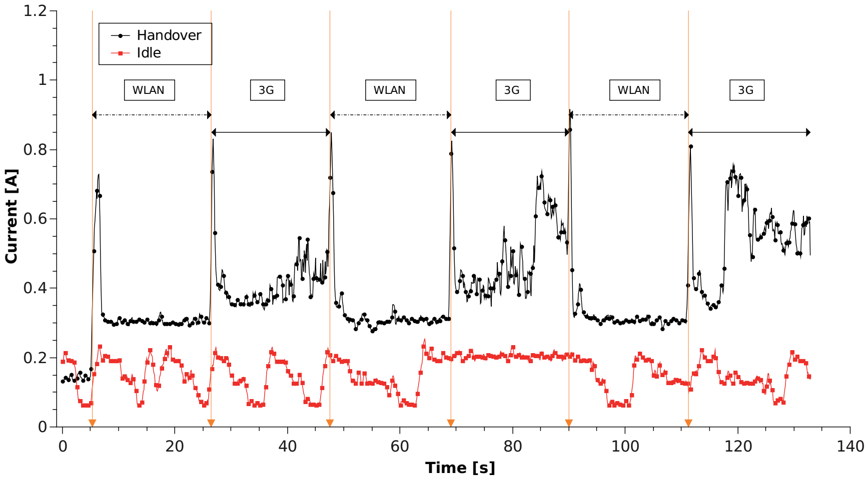


FIGURE 15 Energy efficiency during handovers

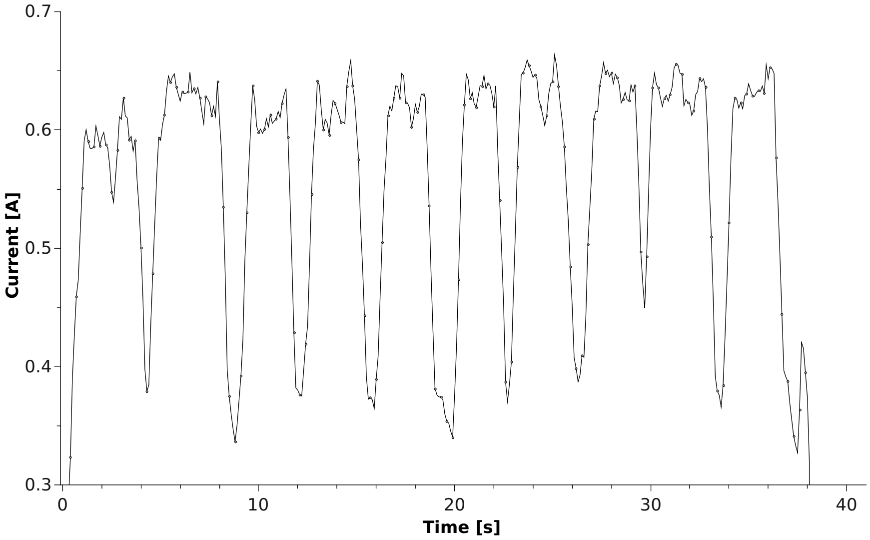


FIGURE 16 Multihoming download over WLAN and 3G

6153. Despite this, a vertical handover performance evaluation was conducted in the Android environment against a simulated EPC network. Android limitations were overcome with the help of VPN tunneling. The result was a successful implementation of mobility management for a single application level in an EPC network environment. However, the delays were too large (almost 7 seconds from UMTS to WLAN) for any real-time communication.

Additionally this chapter dealth with an analysis of energy-efficiency communication within IP data communication in a heterogeneous network. Energy-efficient communication is important for users since all mobile devices have to be charged eventually. The important thing is how often this is needed. Information technology advisory and telecommunication operators also predict that the amount of mobile data will grow significantly. The paper presented a straightforward network selection algorithm. Evolved Packet Core support was added, so that the algorithm can utilize ANDSF information when it is available. In other case, it used WLAN connections over cellular access, which is considered to be the last resort if no other connections are available. Network selection took place each time when some application wanted to access the network. Existing connections were handovered to this, partially due to the limitations of the existing Android implementation. The implementation of the algorithm were an ABC application that was used in near real-life measurements in a heterogeneous network environment. The results showed that energy efficiency favors the fastest connection, which in this research was WLAN over anything else. The reason for this is clear: data transfer action is over faster, and the device can reduce current consumption (slower connections use more time with nearly equally high current consumption). Handovers did cause high 1-2 second current consumption peaks, but the overall energy consumption remained low. Based on energy efficiency, the handovers were justified, as they enable more efficient communication in the best case. In future, when seamless handovers are possible, it would be interesting to make more detailed calculations, and measurements about how to optimize further network change for better energy efficiency and then create implementations based on the resulting values. These implementations might include triggers, such as signal-to-noise ratio, to indicate the start of a network change.

4 TOWARDS MULTIHOMED MOBILES

In IP networks, a node is considered multihomed when it is reachable via multiple different paths by other nodes in the network. Equally, not only single nodes but entire networks can be multihomed, when there are multiple paths leading to the network from outside nodes. Multihoming can become essential for providing robustness in the face of network failures for connection-oriented services. It can provide load balancing and fault tolerance, but most of all it can help performing make-before-break handovers during node mobility. The general motivations for multihoming are [37]:

- Fault tolerance, redundancy: if a path goes down, the terminals should still be reachable on alternative paths
- Transport layer survivability: established transport connections should not break when an underlying path changes
- Performance: reduction of jitter, delay and loss
- Load sharing: utilization of multiple paths at the same time

All this should be done with minimal changes to routers and hosts. Originally, the Internet was not designed with multihoming nodes in mind. Multihoming was added and engineered in along the way. However, it had a negative impact on global routing [38]. To solve this, a new approach to multihoming was developed with IPv6. Instead of burdening the core network with additional logic of knowledge of multiple paths, the logic was pushed to the end-nodes. This is done by allowing UE's to have multiple IP addresses. The approach is called host centric multihoming. In this approach, the UE is responsible for managing the available multiple paths from source to destination. On a high level, this includes selecting a proper source IP and interface for outbound datagrams and instructing peers about the desired destination IP addresses for inbound datagrams. Multihoming itself can be handled at different layers of the network stack. When doing so at lower layers, at the Network Layer for example, transparent upper layer protocols can provide the solution. This transparency is useful from the viewpoint of application development and legacy applications since multihoming needs no attention. On the other hand, the upper layer protocols could have more knowledge about the type and characteristics of network traffic. This means that as one ascends the network stack one can make better decisions about what a particular datagram needs with regard to QoS. The solutions revisited here consider host-centric multihoming in relation to routing updates and UDP traffic as well as the Stream Control Transmission Protocol, SCTP [39] (RFC 4960) and Multipath TCP [40] (RFC 6824).

4.1 Simultaneous Connections with Application Framework

Advances in wireless communication technologies are driving the evolution toward ever faster networks in terms of throughput and latency. At the same time, machine-to-machine (M2M) communications is expected to have considerable potential with millions of devices connected within the following years. M2M communications is one of the key capabilities for implementation of the Internet of Things (IoT). Due to this potential, several standard organizations are now focusing on developing enhancements into their standards to support M2M communications. As there is no consensus for the architecture of a general scenario for M2M communications, the heterogeneous mobile ad hoc network (HetMANET) can generally be considered suitable for the M2M challenges. Hence, this calls for the IP mobility management, allowing a device to connect to services and access technologies that are best suited for that need. To examine how-to improve the HetMANET concept using existing standards such as IEEE 802.11 and 3GPP Evolved Packed Core (EPC) this paper introduces a straightforward and energy efficient algorithm for vertical handovers. A reference implementation of the handover concept in Android based vehicular-to-infrastructure is introduced. This reference implementation examines energy and performance efficiency in heterogeneous network environment. In addition, real-life use cases with real-life services on top of WLAN and cellular network environments are presented next.

4.1.1 Handover concept and implementation

The Android framework was modified to allow simultaneous connections over different access technologies. It enabled simultaneous connections for accessing networks in a heterogeneous network environment. Handover complexity was avoided by making direct choices based on a set of predefined preferences. The idea is to have either/or choices, that is, a single condition that is either true or false. This choice is made always when an Internet access is requested for a particular application or when connection has been lost. The main decision question and steps of an inquiry for access point selection in the concept are: 1. Is valid ANDSF information available? 2. Is there any known protected WLAN connection available? 3. Is there an open WLAN connection available? 4. Use cellular IP connection.

In case a valid ANDSF is available, the algorithm follows this, as it plays the essential role in the compatibility with the EPC. The concept considers each connection request as separate, and in this way the algorithm is triggered over each time a connection is required. If the selection turns out the same as the existing connection, the data is multiplexed over the same connection. In the case of a different choice, the heterogeneous network support allows the use of simultaneous connections.

Functionality and real-life performance was evaluated through the use case scenarios. These scenarios were derived from the M2M scenarios and four traffic classes defined by the 3GPP. The classes and their equivalent services were:

- Conversational - Voice Over IP (VoIP) - Secured Access and Surveillance
- Streaming - YouTube, - Consumer Devices, Retail
- Interactive - Facebook and Google as a social media service - Consumer Devices, Retail
- Background - File Transfer Protocol (FTP) as bulk data transfer - Remote Maintenance and Control, Metering

The VoIP call simulates the case where a vehicle is being tampered with and gives an alert to the user by calling to the UE and delivering information on the real-time location. The YouTube streaming, Facebook and Google's interactive social media services are considered as possible infotainment provided by the retailers. FTP can provide background-type data transfer for the Remote maintenance and Control and the Metering service. The testing took place in a heterogeneous network environment, where WLAN and cellular networks were available. Link quality and load influence the timing of network change, especially in case of real-time traffic [23].

4.1.2 Framework modification

Currently, the Android framework does not support simultaneous connections. The connectivity service ([1]) manages connectivity, and it was modified to make simultaneous connections possible. The implementation was based on Samsung Galaxy SII, but the original software was replaced with CyanogenMod 9 [2]. The reason for this was that Samsung offers the source code for Galaxy SII. However, there were some hardware-related drivers missing. The common network access management process handles the event_state_changed event with the DISCONNECT event. When it is triggered, the framework tries to connect to some other known network as a failover. If a failover network is found, the framework is reconnected. After the reconnect event, the previous connection is terminated by flushing the Domain Name System (DNS) and the routing information and then tearing down the existing connections. While connected to the failover network, the corresponding interface is powered up and a new entity with an empty DNS and with routing information is created. The precondition for this is that both

---

[1] com.android and server.ConnectivityService

[2] firmware dated 6.8.2012

networks (WLAN and 3G) are known and previously used; thus DNS information is available in both of the cases. Therefore, when the DISCONNECT event is received the flush of DNS data is prevented, the otheraccess network is set immediately as an active network and the state is changed to CONNECTED.

The network-change times between a public cellular network and an infrastructure WLAN are presented in FIGURE 18. The results show that the handover times are around 204 ms. During the measurements,the WLAN network was not used by other users. This is significantly better than the approximitely one second without any modifications (**PII**). The handover measurements started from the DISCONNECT event, and the handover time itself was unaffected by the previous network. The handover time is within limits of suitability for real-time communication. Times around 200 ms are generally regarded as a limit for real-time communication. On the other hand, as the handover concept did not offer any solution for mobility management, it's up to the service to deal with the connection change. As a result of simultaneous connections, the tradeoff is energy efficiency. For the idle state, without any communication, the difference in energy consumption is presented in FIGURE 17. It shows that although the base consumption can be near the same level as with a single connection, the mandatory keep-alive signaling will result higher energy consumption. In the conversational class the VoIP call was interrupted each time the underlying network connection changed. However, the call itself was not terminated, instead the call continued once the connection was re-established. The user was notified about the connection error. In the streaming class during the network change, the buffered stream was consumed and the video paused. After an access network change, the YouTube streaming could be continued by manually selecting a time beyond the previously buffered stream section. For the interactive class, the scenario was browser-based and consisted of continuous usage of the Facebook and Google chat. In case of the chat the online/offline status of the user and message delivery were monitored. Messages were exchanged every 15 seconds. The Facebook and Google chat were unaffected by the network change from the user's point-of-view. With the background class, the test scenario was bulk data transfer with FTP. The data transfer was disconnected when access to the network was changed.

4.1.3 User Datagram Protocol based multihoming in Android framework

UDP and traffic routing changes offer a simple and straightforward way to enable multihoming in a heterogeneous network environment. UDP sends datagrams to other hosts on the IP network without any setup of transmission channels or data paths. It has no handshaking, and by default it is unreliable and not protected for ordering failure or duplicates. Our idea utilizes these communication characteristics of the UDP. The implementation environment was Samsung Galaxy S i9000, a smartphone where multihoming was implemented between the cellular and WLAN access. The solution has a client-server architecture where the server, guided by the client, can send UDP datagrams to various destinations. Rout-

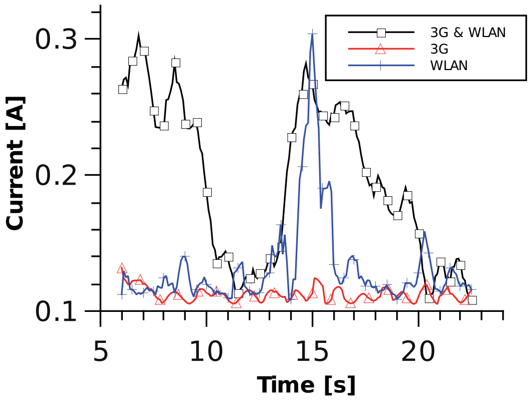


FIGURE 17 Energy efficiency trade-off in idle state

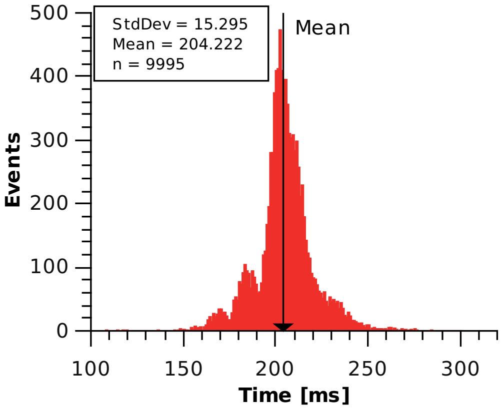


FIGURE 18 Handover delay

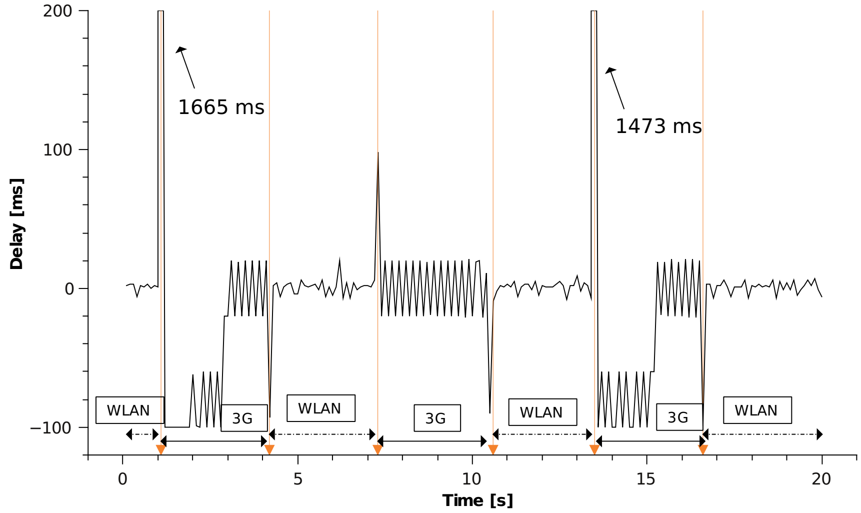


FIGURE 19 UDP-based multihoming between 3G and WLAN interfaces. The arrows are pointing at handover points

ing table and Dynamic Name Server (DNS) configuration changes were required. The routing table and DNS changes were made according to the connection in use. Both of the interfaces (in this case cellular access and then WLAN) are initialized and their route and DNS information is stored. Then, depending on the chosen path, the routing table and DNS are updated for outbound datagrams. For inbound datagrams, both of the interfaces are available.

The results show (FIGURE 19) packet delay between two consecutive packets without a transmission interval (100 ms). The negative values derive from the protocol buffers where the packets were read (as fast as possible) after a connection change. In case of 3G, the transmission delay resulted in a variation in reception. A handover is time-consuming when a 3G interface is powered up or awakening from the sleep state (around 1-13 seconds), but in other cases it causes a maximum of 100-ms spikes between two consecutive packets. The near zero delay packets after handover are derived from the connectionless nature of UDP when packets arrive out of order or are read from the buffer. These results indicate that "home-made" solutions to multihoming are possible and that they can be efficient enough for real-time communication.

4.2 Stream Control Transmission Protocol as a standalone application

The SCTP protocol is a reliable transport protocol operating on top of a connectionless packet network such as IP [39]. The basic service offered by SCTP is

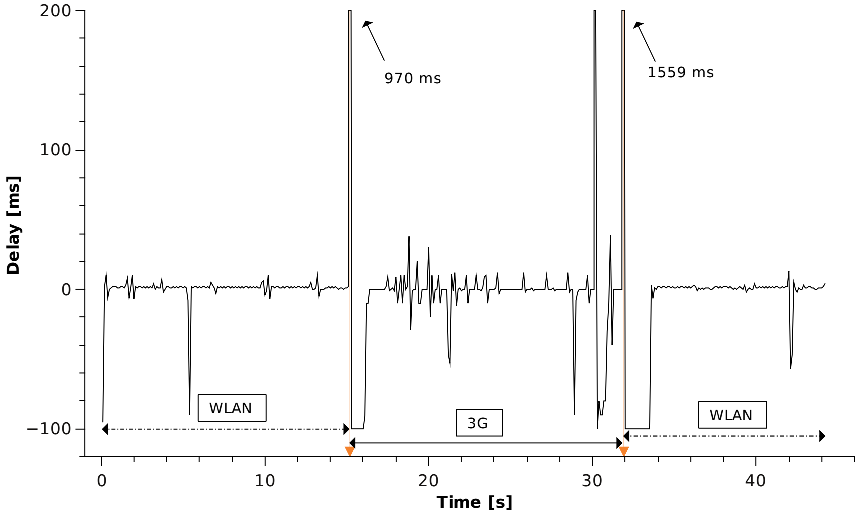


FIGURE 20 SCTP-based multihoming between 3G and WLAN interfaces. The arrows are pointing at the handover points and the interface used

reliable transfer of user messages between SCTP peer users. The service is performed within the context of an association between two SCTP endpoints. During the association startup, SCTP provides the means for each SCTP endpoint to provide the other endpoint with a list of transport addresses, for example multiple IP addresses, in combination with an SCTP port through which that endpoint can be reached and from which it will originate SCTP packets. The Android device (Samsung Galaxy S i9000) did not support the SCTP protocol out of the box, so we compiled and installed the Semaphore kernel with SCTP support enabled as a kernel module. Also libsctp.so was cross-compiled [3]. The same toolchain was used to cross-compile the UDP and SCTP client programs. The server programs were compiled using with gcc [4]. The performance results show (FIGURE 20) the constant "on/off" nature of the protocol implementation. The figure excludes the transmission interval of 100 ms. The handover is always time-consuming operation during which the data is buffered and delivered afterwards as big chunks. The behavior poses challenges for communication: the packets are not lost, but the handover delay itself is problematic from the viewpoint of real-time communication.

---

[3] lksctp-tools-1.0.11 for ARMv7 using arm-linux-gnueabi-gcc version 4.6.3-1ubuntu5

[4] version 4.6.3-1ubuntu5

4.3 Multipath TCP as a part of Evolved Packet Core

The 3GPP standardized the EPS, where one of the key features is a support access system selection based on a combination of operator policies, user preference and access network conditions [21]. The non-3GPP access networks are also covered by the standard. The EPS is under active development by 3GPP and the Internet Engineering Task Force (IETF) working groups such as Network-Based Mobility Extensions (netext). One of the key working item is the multiple interface support for a seamless handover. Multipath TCP (one of the most recent protocol standards of IETF), which is a modified version of TCP (RFC 793) [11] implements a multipath transport achieve this by pooling multiple paths within a transport connection, transparently to the application [41].

Although today's mobile devices are not supporting the EPS standard yet, they have multiple radio interfaces such as IEEE 802.11 and cellular access. Meanwhile, TCP is still only single-path. To gain robustness and smooth vertical handovers advantages, a transport protocol engineered to utilize multiple paths is needed. MPTCP is an extension of the TCP protocol to perform this. The first proposal dates back to 1995 [42]. However, the existence of middleboxes greatly constrains the design choices. The challenge is to make MPTCP to path failures as well as robust to failures in the presence of middleboxes that attempt to optimize single-path TCP flows [43]. MPTCP operates at the transport layer and aims to be transparent to both higher and lower layers. It is a set of additional features on top of standard TCP. MPTCP is designed to be usable by legacy applications with no changes [44]. The key terms of MPTCP are:

- Path: a sequence of links between the sender and the receiver, defined in this context by a 4-tuple of source and destination address/port pairs
- Subflow: a flow of TCP segments operating over an individual path, which forms part of a larger MPTCP connection. A subflow is started and terminated similarly to a regular TCP connection
- MPTCP Connection: a set of one or more subflows, over which an application can communicate between two hosts. There is a one-to-one mapping between the connection and an application socket
- Token: a locally unique identifier given to a multipath connection by a host. It may also be referred to as a "Connection ID"

The suitability MPTCP for make-before-break handovers is examined. The results show that, by nature, multipath has strong potential to act as an enabler for vertical handovers [45].

4.3.1 Multipath TCP and Evolved Packet Core in Android environment

The 3GPP TS23.402 architecture enhancements for non-3GPP accesses [6] and 3GPP TS access to 3GPP Evolved Packet Core (EPC) via non-3GPP access networks [26] are specifying requirements for UE. One of the basic definitions is IP

Flow Mobility (IFOM) and Multi Access PDN Connectivity (MAPCON), where the packet data connections are going through different access networks. This is not currently supported by the Android environment. When changing connection, the existing connection is disconnected before a new one is created.

The IP Mobility Management Selection (IPMS) principles state, naturally, that the UE and the network must support the same mobility management mechanism. The two main choices are network-based mobility (NBM) and host-based mobility (HBM). In case of HBM the defined protocols are DSMIPv6 and MIPv4. A critical question is whether the IP address preservation can be utilized to gain session mobility during vertical handover. Upon initial attachment to a 3GPP access, no IMPS is necessary since connectivity is always established with network-based mobility. Upon initial attachment to a trusted non-3GPP access or handover to it, IMPS is performed before the IP address is allocated and provided to the UE. When applying NBM, the session continuity can take place according to PMIPv6 [46] or by the legacy GPRS tunneling protocol [29]. In contrast with HBM, the session continuity can take place in case the network is aware of the UE capabilities to support DSMIPv6 or MIPv4. However, GTP is a proprietary legacy protocol that is not supported in large scale outside 3GPP access for example by WLAN setup boxes. The support for UE having multiple interfaces is described in the Internet draft “Proxy Mobile IPv6 Extensions to Support Flow Mobility” [47].

The NBM with Proxy Mobile IPv6 is being actively developed by the 3GPP and IETF Network-Based Mobility Extension (netext) working group. At the time of writing, there are three active Internet-Drafts to address multihoming and Proxy Mobile IPv6 challenges. The challenge is clear: network-based mobility management by Proxy Mobile IPv6 versus the host-centric approach by MPTCP. These protocols might possibly work together to complement each other: PMIPv6 as a way for the network operator to manage mobility and authentication in the core network and MPTCP as a UE to control its interfaces and communication effectively.

“PMIPv6 Multihoming Support Extensions for Flow Mobility” [48] proposes changes to local mobility anchor (LMA) and Mobility Access Gateway (MAG) behavior so that flow mobility can seamlessly be supported in PMIPv6. Flow mobility enables distribution of specific traffic flows on different physical interfaces. Instead of creating an independent mobility session for each interface, the bindings from each simultaneously active interface are kept together so that the flows can be moved among interfaces. The change is done in the home network prefix options where a new flag is introduced. The flag distinguishes, firstly or only, the connected interface from other possible interfaces.

“Seamless Handover for Multiple-Access Mobile Node in PMIPv6” [49] introduces an idea similar to the above scheme but with new mobility header messages Streamless Handover Initiate (SHI) and Streamless Handover Acknowledge (SHAck).

“Fault Tolerant Support for The Multihomed MN in Proxy Mobile IPv6” [50] has yet another nuance for multihomed UE support. In PMIPv6, Binding

Cache Entry (BCE) is created in the LMA to bind the MAG with the UE. The solution extends the multihoming flag, and the Status flag should be included in the new BCE entry. The multihoming flag is used to identify whether the MN is multihomed. When a multihomed MN joins the network, the MAG is used to communicate with the LMA to register the location information for an MN and to send the Proxy Binding Update (PBU) message to the LMA, which creates a BCE entry for each MN interface. If the received PBU messages from different MAGs come with the same UE-ID, the multihoming flag is set to 1, otherwise the value is set to 0. The status flag is used to identify whether the interface that the BCE entry corresponds to is available, or whether the state of the interface is in use.

All the reviewed Internet drafts assume operation in a single-domain PMIPv6 network, which may not be the case in a real-life heterogeneous network environment. However, this consideration is out of scope in this research. Another challenge is authentication. EPC requires IPsec-based security associations between untrusted access nodes which in many cases are WLAN access points. The IPsec has not been designed for nodes with multiple interfaces [51]. It may configure another IP address through MOBIKE [52] (RFC 5266) with the additional IP address [5] Notify Payloads. These payloads are only provided for the interface used by the IPsec. The main reason is that MOBIKE has been designed for a single interface.

As a summary, multipath communication was not originally engineered to EPC, which, at least at the moment, is promoting network base mobility. On the other hand, based on a comprehensive research on multipath communication, it must be host-centric mostly due to the vast number of middleboxes around Internet [38, 53]. To overcome this challenge, changes to NBM and particularly to PMIPv6 are explored by the IETF working groups. The authors proposal for multipath TCP utilization within EPC environment includes taking into use the proposed home network prefix option [48] as well as additioanl IP address field in IPsec. In this way, multihoming may be utilized at least between two interfaces with one flow in each interface. This would bring multihoming to EPC in a straightforward way and would require only minimal changes to the existing protocols. The changed protocol would be PMIPv6 and its home network prefix options.

4.3.2 Measurements on vertical handover performance

To examine MPTCP's suitability to vertical handovers in an Evolved Packet Core environment the following test setup (FIGURE 1) was constructed. It consisted of a simulated Evolved Packet Core WLAN accesspoint and a Cellular access over UTMS in a live network. The WLAN accesspoint was untrusted and the UE required IPsec connection to EPC. During the measurements the WLAN network was not used by other users. For EPC authentication, the aim was to use IPsec tunneling as defined in the standard. Nevertheless, this was not possible within the Android software environment [54]. Instead, the Secure Sockets Layer (SSL)

---

[5] ADDITIONAL_IP*_ADDRESS

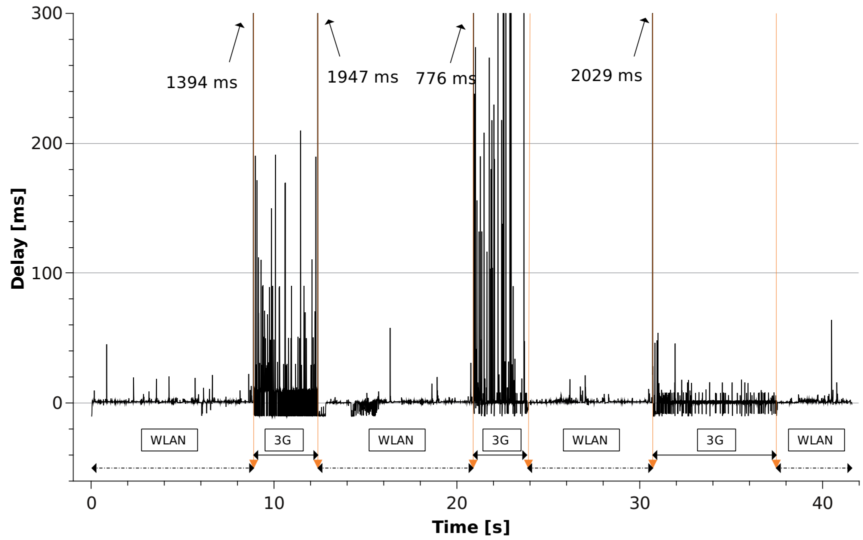


FIGURE 21 Multipath TCP vertical handover performance

tunnel, which is widely used in web browsers was employed. This was considered to be the next best choice. The authentication result was (SSL tunnel only) 109 ms, with a 47 ms standard deviation. Further details of this measurement can be found in **PII**. The UE implementation was done in the Android software environment but with modifications to the off-the-shelf firmware to support MPTCP. The following changes were made: the CyanogenMOD 9 (Android version 4.0.4) software as a baseline for software development [6]. The following scenarios were defined: file download (around 20 MB) through a single path as well as through multipath and handovers between WLAN and cellular access with corresponding energy consumption during the tests.

The vertical handover times between a public cellular network and a WLAN are presented in FIGURE. 21. The results show a packet delay between two consecutive packets without a transmission interval (10 ms). The handover was done by setting the network device that was currently in use to the backup state. MPTCP started using the other interface automatically. A moving window average filter (using 5 points) was applied to the results during the analysis. The results show that, with the current implementation, the connection change is a time-consuming operation, although interfaces were up and running during the tests. The link quality and load has its effect on when it would be effective to change the network, especially in the case of real-time traffic [23]. This poses challenges for make-before-break handovers in real-time traffic. Although packets were not lost and mobility is managed for the application, there is bound to be a short break in the communication. It is up to the corresponding applica-

---

[6] Kernel version 3.0.32-CM-ge9cef6c-dirty with MPTCP changes from https://github.com/mptcp-galaxys2

tion to handle the delay between two consecutive packets. Another result visible in FIGURE 21 is the delay in the communication path on the 3G network. There were temporary congestions, which appeared as detectable delays between packets, in the live network. After congestion, the delays were as low as seen in third round with 3G. Despite the fact that delays on the 3G path were temporary, the handover time remained high in every handover between WLAN and 3G.

4.4 Summary

The growth of mobile data, which is driven by the high number of devices and data-hungry services, has created a need for dense high-throughput networks. One generally accepted way of dealing with this is to introduce smaller cells and/or route the traffic through different access technologies, depending on service requirements. Both of the solutions require mobility management and vertical handovers capability in a heterogeneous network. The results from Chapter 2 show that without any modifications the prevailing handover performance is not suitable for real-time communication. For enabling make-before-break handovers, simultaneous connections in the Android framework were examined. This resulted in an Android implementation, where the handover times were close to 200 ms and could be considered to be within the acceptable limits for real-time communication. To find out whether handover times could be improved further, multihoming protocols were researched. Multihoming devices may have multiple interfaces providing multiple IP addresses to handle traffic. This enables transport layer survivability so that the established transport connections should not break when the underlying path changes a key feature for mobility management and usage of heterogeneous network. The implementations on top of Android operated with the UDP and SCTP protocols. The UDP solution utilized this protocol's connectionless characteristic with which multihoming was achieved simply by changing the routing of datagrams between the interfaces used. These results were impressive, the handover times being around 100 ms. Similarly, the SCTP protocol, which was originally designed for multipath communications, showed results of the same magnitude as the simple UDP solution. The trade-off was that neither of the presented solutions was suitable for Internet-wide communication because the numerous middleboxes in the transmission path would change or block random UDP or SCTP packets. After this the handover performance and energy efficiency of MPTCP protocol-based communication in IP networks was assessed. Additionally, the MPTCP suitability as a part of the 3GPP Evolved Packet Core network was examined. ECP promotes network-based mobility management whereas MPTCP is host-centric. This creates a challenge for MPTCP utilization in an EPC network. Clear advances in multipath communication have pushed the 3GPP and the IETF to work to overcome the challenges. The author proposes to take into use the proposed home network prefix option to the PMIPv6 and use the additional IP address [7] field in the IPsec. Thus multihoming may be utilized at least between two interfaces, with one flow in each interface. The Android framework was modified and tested against a live and partly simulated EPC network. The results show that MPTCP may be used for vertical handovers although make-before-break handovers suffer a communication break within around 750 to 2200 ms. However, from the application point-of-view the mobility works and overall energy efficiency is not compromised.

---

[7] ADDITIONAL_IP*_ADDRESS

5 CONCLUSION

This dissertation deals with research and implementation challenges caused by the heterogeneity of networks. Its main focus is to enable Always-Best Connectivity for existing and future UE devices under the umbrella of the 3GPP Evolved Packet Core standard. This standard allows, for the first time in 3GPP history, network access and mobility management over non-3GPP-specified access technology. As the selected research approach was aiming for real implementation, the dissertation deals with various challenges related to the specification and actual implementation of network access and mobility management. The limitations and lack of specification support resulted in creative solutions and a workaround. These included network interface management, user authentication and multihoming protocol support. At the same time, test setups were built to simulate EPC and other heterogeneous network environments. Finally, as the performance results showed that, at the moment, single interface could not provide seamless handovers for real-time communication, the research investigated the utilization of simultaneous connections for handover. The related multihoming challenges were researched and implemented both by own and protocol-based solutions.

The first main topic in this dissertation is the algorithm design for Always-Best-Connected heterogeneous network. The straightforward network selection algorithm in an Android framework is presented. The performance results show the network-change time being around one second. However, for EPC support, user authentication is required. This performance was about 110 ms. When this was combined with pure network-change delay, it was clear that seamless handovers were not possible with real-time communication. Similar results were obtained when using the PMIPv6 protocol for network change and mobility under the Linux and the Android framework. The network was homogeneous in both cases, and the handovers occurred between WLAN BSs. User experience under Linux was not compromised when using a buffer size within the limits of real-time communication (200 ms) although packet loss was detectable. However, under the Android framework there were problems that were specific (most likely) to network drivers. These caused the connection to disconnect before reconnecting to the adjacent BS.

The second topic of this dissertation, presents challenges and problems and resulted in solutions and workarounds in the involved standards and implementations for real devices and networks. Standards such as IPSec and, PMIPv6 were not supported off-the-shelf in the Android environment. Both of these standards are required as the EPC enabler for user authentication and seamless handover. The dissertation presents ways to enable the missing standards in the Android framework or to provide an alternative solution based on the existing features of the Android framework. The power efficiency of presented solutions was examined.

The final topic of this thesis enhances the probability of seamless vertical handovers with real-time communication. These solutions range from Android framework modifications and exploiting Linux routing changes to the usage of multihoming-enabled protocols such as SCTP or MPTCP. One solution is to modify the Android framework to allow simultaneous connections over different network adapters; in our case, connectionless UDP traffic could be used in a multihomed way. While connection oriented TCP works existing multihoming enabled protocols such as SCTP and MPTCP. The handover performance and power efficiency trade-off are also examined.

Although the dissertation utilized Android and Linux systems in the solution implementations, the results on straightforward network selection in a heterogeneous network are not restricted to presented systems. The main ideas of straightforward network selection based on profiles, known networks, history location information and knowledge of used services and bandwidth can be reused in other SW frameworks. On the other hand, the encountered challenges will be different with other SW frameworks. Due to the challenges, the real-life results may not be as good as expected, and the functionality may be faulty when solutions are other than those in the most popular use case. Also, the engineered simultaneous connections may provide the needed handover performance without any additional protocol support.

YHTEENVETO (FINNISH SUMMARY)

Tämä väitöskirja, Liikkuvuuden hallinta aina parhaiten kytketyssä IP-verkossa, tutkii sopivinta liityntää IP-verkkoon heterogeenisessa verkkoympäristössä ja tapoja miten päätelaitteen liikkuvuus näissä verkoissa voidaan toteutaa niin että siitä on mahdollisimman vähän haittaa käyttäjän palveluille. Väitöskirjassa on kolme pääteemaa, ensimmäinen näistä on verkonvalinta heterogeenisessä verkkoympäristössä. Tähän väitöskirja esittää algoritmia, joka toimii sekä 3GPP Evolved Packet Core -standardin kanssa että ottaa huomioon monia tekijöitä kuten signaalin tason, hinnan, käytetyt palvelut, palveluiden käyttämän kaistanleveyden ja virran käytön. Saavutettua verkonvaihdon suorituskykyä mitataan sekä oikeassa että simuloidussa verkkoympäristössä. Tuloksena huomattiin verkonvaihdon viiveen olevan niin suuri että reaaliaikaisten palveluiden kuten IP-puheluiden siirto toiseen verkkoteknologiaan on vaikeaa ilman että käyttäjä huomaa joko palvelun heikentyneen tai estyvän. Toinen väitöskirjan pääteema on käytettyjen standardien ja kehitysympäristöjen haasteet. Tutkimuksen lähestymistapa oli käytännönläheinen, kaikki uudet ideat pyrittiin toteuttamaan käytännössä. Käytettyinä päätelaiteympäristöinä oli Android- ja Maemo-ohjelmistopinoja ja Linux -käyttöjärjestelmä. Väitöskirjassa esitettyjen ratkaisujen todentaminen mittauksilla vaati muutoksia käytettyihin ohjelmistopinoihin tai Linux-käyttöjärjestelmään. Näitä ja muutosten vaikutuksia virrankulutukseen tarkastellaan toisessa pääosassa. Kolmannessa ja viimeisessä väitöskirjan osassa käsitellään yhtäaikaisten yhteyksien mahdollisuuksia reaaliaikaisen palvelun siirtämisestä eri verkkoteknologioiden välillä. Väitöskirjassa esitellään ratkaisuja, joissa hyödynnetään yhtäaikaisia yhteyksiä verkonvaihdossa, sekä niiden suorituskykyä nykyisillä päätelaitteilla. Osa ratkaisuista on yksittäiskäyttöön sopivia ratkaisuja, joilla yhteydet saadaan käyttöön yhtäaikaisesti ja verkonvaihdot voidaan suorittaa niin nopeasti että palvelun laatu ei heikkene. Toinen osa ratkaisuista hyödyntää yhtäaikaisia yhteyksiä tukevia protokollia kuten Stream Control Protocol tai Multipath TCP ja verkonvaihdon suorituskykymittausten perusteella näiden protokollien mukaiset ratkaisut voivat parhaimmillaan toimia niin että käyttäjän kokeman palvelun laatu ei heikkene. Haittapuolena on kuitenkin lisääntynyt virrankulutus verkkorajapintojen ollessa yhtäaikaisessa käytössä.

REFERENCES

[1] Cisco, "Cisco visual networking index: Global mobile data traffic forecast update, 2012 to 2017." http://www.cisco.com/en/US/netsol/ns827/networking_solutions_sub_solution.html, Feb. 2013.

[2] 3GPP TS 36.300 v10.8.0, *Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN)*, July 2012.

[3] IEEE 802.16-2012, *IEEE Standard for Air Interface for Broadband Wireless Access Systems*, Aug. 2012.

[4] E. and D. Jonsson, "Always best connected," *Wireless Communications, IEEE*, p. 49, Feb. 2003.

[5] Ericsson, "Ericsson mobility report." http://www.ericsson.com/ericsson-mobility-report, Dec. 2012.

[6] 3GPP TS 23.402 v10.8.0, *Architecture enhancements for non-3GPP accesses*, Sept. 2012.

[7] T. Dierks and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2." RFC 5246 (Proposed Standard), Aug. 2008. Updated by RFCs 5746, 5878, 6176.

[8] S. Kent and K. Seo, "Security Architecture for the Internet Protocol." RFC 4301 (Proposed Standard), Dec. 2005. Updated by RFC 6040.

[9] J. Manner and M. Kojo, "Mobility Related Terminology." RFC 3753 (Informational), June 2004.

[10] S. Deering and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification." RFC 2460 (Draft Standard), Dec. 1998. Updated by RFCs 5095, 5722, 5871, 6437, 6564.

[11] J. Postel, "Internet Protocol." RFC 791 (INTERNET STANDARD), Sept. 1981. Updated by RFCs 1349, 2474.

[12] B. Briscoe, "Tunnelling of Explicit Congestion Notification." RFC 6040 (Proposed Standard), Nov. 2010.

[13] K. Kong, W. Lee, Y.-H. Han, M.-K. Shin, and H. You, "Mobility management for all-IP mobile networks: mobile IPv6 vs. proxy mobile IPv6," *IEEE Wireless Communications, vol*, vol. 15 issue 2, pp. 36–45, Apr. 2008.

[14] K. Kong, W. Lee, Y.-H. Han, and M.-K. Shin, "Handover Latency Analysis of a Network-Based Localized Mobility Management Protocol," in *IEEE International Conference on Communications (ICC)*, pp. 5838–5843, May 2008.

[15] J. Lei and X. Fu, "Evaluating the Benefits of Introducing PMIPv6 for Localized Mobility Management," in *Wireless Communications and Mobile Computing Conference,IWCMC '08*, pp. 74–80, Aug. 2008.

[16] H. Soliman, C. Castelluccia, K. ElMalki, and L. Bellier, "Hierarchical Mobile IPv6 (HMIPv6) Mobility Management." RFC 5380 (Proposed Standard), Oct. 2008.

[17] G. Camarillo, A. Niemi, M. Isomaki, M. Garcia-Martin, and H. Khartabil, "Referring to Multiple Resources in the Session Initiation Protocol (SIP)." RFC 5368 (Proposed Standard), Oct. 2008.

[18] J. Guan, H. Zhou, W. Xiao, Z. Yan, Y. Qin, and H. Zhang, "Implementation and Analysis of Network-based Mobility Management Protocol in WLAN Environments," in *ACM Mobility Conference - MobiWorld Workshop*, Sept. 2008.

[19] M.-C. Chuang and J.-F. Lee, "FH-PMIPv6: A Fast Handoff Scheme in Proxy Mobile IPv6 Networks," in *International Conference on Consumer Electronics, Communications and Networks (CECNet)*, pp. 1297–1300, Apr. 2011.

[20] A. Rasem, M. St-Hilaire, and C. Makaya, "A comparative analysis of predictive and reactive mode of optimized PMIPv6," in *International Wireless Communications and Mobile Computing Conference (IWCMC)*, pp. 722–727, Aug. 2012.

[21] 3GPP TS 23.203 vV10.8.0, *Policy and charging control architecture*, Sept. 2012.

[22] 3GPP TS 24.312 v10.6.0, *Access Network Discovery and Selection Function (ANDSF) Management Object (MO)*, July 2012.

[23] E. Boysen and J. Flathagen, "Using sip for seamless handover in heterogeneous networks," in *Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)*, pp. 1–8, Oct. 2011.

[24] Eurecom, "Openairinterface proxy mobile ipv6." http://www.openairinterface.org/openairinterface-proxy-mobile-ipv6-oai-pmipv6, Jan. 2013.

[25] 3GPP, "Quality of Service (QoS) concept and architecture," TS 23.107, 3rd Generation Partnership Project (3GPP), Dec. 2011.

[26] 3GPP TS 24.302 Stage 3, *Access to the 3GPP Evolved Packet Core (EPC) via non-3GPP access networks*, Mar. 2012.

[27] J. White, "Responses to critiques of the proposed mail protocol." RFC 555, July 1973.

[28] C. Perkins, "IP Mobility Support for IPv4, Revised." RFC 5944 (Proposed Standard), Nov. 2010.

[29] 3GPP TS 29.060 v10.7.0, *GPRS Tunnelling Protocol (GTP) across the Gn and Gp interface*, Dec. 2012.

[30] B. Aboba, M. Beadles, J. Arkko, and P. Eronen, “The Network Access Identifier.” RFC 4282 (Proposed Standard), Dec. 2005.

[31] J. Arkko and H. Haverinen, “Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA).” RFC 4187 (Informational), Jan. 2006. Updated by RFC 5448.

[32] S. Das and G. Bajko, “DHCPv4 and DHCPv6 Options for Access Network Discovery and Selection Function (ANDSF) Discovery.” RFC 6153 (Proposed Standard), Feb. 2011.

[33] OMA, “Enabler Release Definition for OMA Device Management,” ERELD 1.2, Open Mobile Alliance, July 2008.

[34] Google Inc., “Android developers.” http://developer.android.com/, Jan. 2013.

[35] S. Thomson, T. Narten, and T. Jinmei, “IPv6 Stateless Address Autoconfiguration.” RFC 4862 (Draft Standard), Sept. 2007.

[36] A. Conta, S. Deering, and M. Gupta, “Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification.” RFC 4443 (Draft Standard), Mar. 2006. Updated by RFC 4884.

[37] J. Abley, B. Black, and V. Gill, “Goals for IPv6 Site-Multihoming Architectures.” RFC 3582 (Informational), Aug. 2003.

[38] M. Handley, V. Paxson, and C. Kreibich, “Why the internet only just works,” *BT Technology Journal*, vol. 24, pp. 119–129, July 2006.

[39] R. Stewart, “Stream Control Transmission Protocol.” RFC 4960 (Proposed Standard), Sept. 2007. Updated by RFCs 6096, 6335.

[40] A. Ford, C. Raiciu, M. Handley, and O. Bonaventure, “TCP Extensions for Multipath Operation with Multiple Addresses.” RFC 6824 (Experimental), Jan. 2013.

[41] A. Ford, C. Raiciu, M. Handley, S. Barre, and J. Iyengar, “Architectural Guidelines for Multipath TCP Development.” RFC 6182 (Informational), Mar. 2011.

[42] C. Huitema, “Multi-homed TCP.” Internet Draft, May 1995.

[43] M. Honda, Y. Nishida, C. Raiciu, A. Greenhalgh, and M. Handley, “Is it still possible to extend tcp?,” in *11th Internet Measurement Conference*, pp. 1–14, Nov. 2011.

[44] A. Ford, C. Raiciu, M. Handley, and O. Bonaventure, "TCP Extensions for Multipath Operation with Multiple Addresses." Internet Draft, Oct. 2012.

[45] C. Raiciu, D. Niculescu, M. Bagnulo, and M. Handley, "Opportunistic mobility with multipath tcp," in *The 6th ACM International Workshop on Mobility in the Evolving Internet Architecture*, pp. 1–6, June 2011.

[46] S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury, and B. Patil, "Proxy Mobile IPv6." RFC 5213 (Proposed Standard), Aug. 2008. Updated by RFC 6543.

[47] C. Bernardos, "Proxy Mobile IPv6 Extensions to Support Flow Mobility." Internet Draft, Oct. 2012.

[48] B. Sarikaya, "PMIPv6 Multihoming Support Extensions for Flow Mobility." Internet Draft, Sept. 2012.

[49] Y. Cui, X. Xu, W. Wang, X. Li, Y. Huo, and W. Luo, "Seamless Handover for Multiple-Access Mobile Node in PMIPv6." Internet Draft, Oct. 2012.

[50] H. Jiang, "Fault Tolerant Support for The Multihomed MN in Proxy Mobile IPv6." Internet Draft, June 2012.

[51] D. Migault and C. Williams, "IPsec Multiple Interfaces Problem Statement." Internet Draft, Nov. 2012.

[52] V. Devarapalli and P. Eronen, "Secure Connectivity and Mobility Using Mobile IPv4 and IKEv2 Mobility and Multihoming (MOBIKE)." RFC 5266 (Best Current Practice), June 2008.

[53] C. Raiciu, C. Paasch, S. Barre, A. Ford, M. Honda, F. Duchene, and M. Handley, "How hard can it be? designing and implementing a deployable multipath tcp," in *9th USENIX Symposium on Networked Systems Design and Implementation*, pp. 1–13, Apr. 2012.

[54] J. Kellokoski, "Challenges of the Always-Best-Connected Enablers for User Equipment in Evolved Packet System," *Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2012*, Oct. 2012.

ORIGINAL PAPERS

PI

USER-CENTRIC APPROACH TO ALWAYS-BEST-CONNECTED NETWORKS

by

Jari Kellokoski and Timo Hämäläinen 2011

ICUMT 2011, 3rd International Congress on Ultra Modern Telecommunications
and Control Systems and Workshops

Reproduced with kind permission of IEEE.

User-Centric Approach to Always-Best-Connected Networks

Jari Kellokoski and Timo Hämäläinen
Department of Mathematical Information Technology
University of Jyväskylä
FI-40014 Jyväskylä, Finland
Email: jari.k.kellokoski and timo.t.hamalainen @jyu.fi

***Abstract*—Mobile Internet has rapidly evolved in the past years with an ever increasing number of novel technologies and services with a variety of access technologies being deployed along side. Today's mobile devices often support multiple communication technologies for accessing Internet services. However, they all do not tap the full potential of these capabilities as users often have to manually select the networks and only one network is used at a time. The concept of Always Best Connected (ABC) allows a person to connect applications using the devices and access technologies that best suit to his or her needs, thereby combining the features of access technologies to provide an enhanced user experience for future Internet. However, an Always Best Connected scenario generates great complexity and a number of requirements, not only for the technical solutions, but also in terms of business relationships between operators and service providers, and in subscription handling. The Third Generation Partnership Project (3GPP) standardized the Evolved Packet System (EPS) where one of the key features is a support access system selection based on a combination of operator policies, user preference and access network conditions. Still the standard focuses mainly on the operator point of view, the user is considered to follow this approach. Yet, the standard offers a number of possibilities where the user centric approach can improve the ABC scenario over the predefined by the operator. This research investigates how to build an Always Best Connected application that works with EPS standard and what kind of user preferences should be taken into account when making the network selection more user centric. Additionally the proof-of-concept implementation of this user centric approach to Always Best Connected model is illustrated.**

Keywords*—*Always Best Connected; IP Multimedia Subsystem; Mobility Management.

I. INTRODUCTION

The integration of heterogeneous access networks and the efficient use of the available communication performance is one of the key challenges for the next generation of mobile communication. Today's mobile devices come with various network interfaces. Even the cheaper smartphones support at least four wireless technologies, i. e. Universal Mobile Telecommunications System (UMTS), Global System for Mobile Communications (GSM), IEEE 802.11 (WLAN in this papers context) and Bluetooth. Over the past years the number of heterogeneous access networks that are available at a specific location grew dramatically as well. Further technologies such as Term Evolution (LTE) or Worldwide Interoperability for Microwave Access(WiMAX) are being deployed currently. A bit too exotic networks such as DVB-H, Vehicular Ad-hoc Networks or Delay Tolerant Networks may provide additional communication abilities. All of these networks show different communication characteristics, e.g. in terms of throughput, delay, availability and costs. However, in combination they offer a high communication performance. In an environment of multiple access technologies, the concept of being always connected becomes Always Best Connected. This refers to being not only always connected, but also being connected in the best possible way [5]. The aim of present research is twofold. First, to develop a user's device-based service that will work with existing EPS standard as there are no available commercial solutions yet. Second, to add additional user centric preferences to be taken into account when doing decisions about the network selection. By combining these, the common software architecture can be created which then can be easily expanded by making modifications to network selection algorithm. Section II gives an overview of the used telecommunication standards, while Section III presents the user centric approach for Always Best Connected mobility. A following proof-of-concept section evaluates the developed prototype implementation. Section V finalizes the paper with Conclusion and Future Work.

978-963-8111-76-0

II. THE BIG PICTURE - TELECOMMUNICATIONS STANDARDS

This section outlines two of the major network technologies, namely IP Multimedia Subsystem and Evolved Packed Core, that have the potential to become the next common baseline for all IP based services.

A. IP Multimedia Subsystem

The IP Multimedia Subsystem is meant to be global and access-independent and to have a standard based IP connectivity and service control architecture, as defined originally by 3GPP in their Release 5. Since that time, it has evolved to also cover Fixed Mobile Convergence (FMC) and provide reliable charging, security and quality of service. The main signaling of IMS is based on the Session Initiation Protocol (SIP) [16]. In order to support universal IP connectivity the IMS should be able to use multiple transport technologies to guaranteed connectivity. So, regardless of the underlying access network or the user's terminal features, services related to IMS should be usable. The IMS can be seen as glue between different services [8]. The OpenIMS core [12] has offered an open-source-based possibility to try out the IMS deployment. Although the OpenIMS is not a commercial solution its performance can be considered to be suitable for smaller players in the telecommunications business [7], [6]. Other additional reasons for the IMS deployment are:

- IMS offers, for 3GPP/ETSI-TISPAN, a standardized and developed IP system environment containing standard interfaces to external systems and networks
- IMS contains, as a default the Authentication, Authorization and Accounting (AAA) system for user identification and service authorization.
- IMS enables SIP/Voice over IP (VoIP) capability by default when using public or private WLAN networks anywhere in the world, and usually comes with a single flat rate fee.

The core elements of the IMS architecture are called Call Session Control Functions (CSCF). There are three main CSCFs: Proxy CSCF (P-CSCF), Serving CSCF (S-CSCF), Interrogating CSCF (I-CSCF). Each of these has its own special tasks [15]. Proxy-CSCF is the first contact point for users within IMS. This means that all SIP signaling traffic from the users terminal will be sent to the P-CSCF. S-CSCF is responsible for handling registration processes, making routing decisions, maintaining session states, and storing service profiles. I-CSCF is a contact point within the service operator's network for all connections destined to a subscriber of that network operator. The Home Subscriber Server (HSS) can be considered as the main data storage for all subscriber and service-related data of the IMS. The most important data that the HSS holds are user identities, registration information, access parameters and service triggering information [1].

B. *Evolved Packed Core*

The 3GPP standardized the Evolved Packet System (EPS), formerly known as System Architecture Evolution (SAE), which consists of a radio part: Evolved URTAN (E-UTRAN) and a network part: Evolved Packet Core (EPC) [4]. The main objectives of the Evolved Packed System are:

- EPS provides higher data rates, low latency, high level of security, support of variable bandwidth and Quality of Service (QoS)
- EPS supports a variety of different access systems (existing and those in the future), ensuring mobility and service continuity between these access systems
- EPS supports access system selection based on a combination of operator policies, user preference and access network conditions – as the operator based ABC
- EPS provides capabilities for co-existence with legacy systems and migration to the Evolved Packet System

In this section focus is on the core network part (EPC) as it plays the key role in providing the IP connectivity. Section also describes the components of the EPC, highlights their major functionalities and outlines the main interfaces between these components. Fig. 1 depicts the non-roaming architecture within the EPS using S5 and S2c interfaces. The EPC architecture that interconnects 3GPP and non-3GPP access networks consists of several main subcomponents, namely eNodeB, Mobility Management Entity (MME), Serving Gateway (SGw) and Packet Data Network Gateway (PDN-Gw). In addition to these, several other components are present for inter-operating with non-3GPP access like WiFi/WiMAX (ePDG, ANGw) for access gateways and the Access Network Discovery and Selection Function (ANDSF). The key control node for an LTE access is the MME, which is responsible for the user tracking, SGw selection, Idle State control, Bearer Control and enforcing user roaming restrictions. The SGw is acting as a mobility anchor for the user plane during the LTE and other 3GPP technologies (intra 3GPP handover), manages the User Equipment (UE) contexts and controls the UE data path. The PDN Gateway provides connectivity from the UE to one or multiple external PDNs simultaneously. The PDN-Gw acts also as a mobility anchor, but between 3GPP and non-3GPP technologies and in addition performs packet filtering and charging. The Home Subscriber Server (HSS) is the central database in the EPC storing user related information as in the IMS. Static user profiles as well as dynamic information like session contexts and locations are stored in the HSS. The Policy and Charging Rule Function (PCRF) encompasses the two main functions of flow Based Charging: charging and QoS controls (e.g. QoS control and signaling, etc.). The ANDSF is a new EPC element in Release 8. and it performs data management and controls functionality to assist the UE on the selection of the optimal access network in a heterogeneous scenario via the S14 interface. The S14 is the Logical interface between the ANDSF and the UE [2]. Authentication, Authorization and Accounting (AAA) in the EPC is performed by the HSS, MME and 3GPP AAA Server. The AAA secures the user subscription, session key management and security tunnel control. The evolved Packet Data Gateway (ePDG) attaches un-trusted non-3GPP access networks like WLANs to the EPC and performs important security functions like tunnel authentication and authorization, IPSec encapsulation/decapsulation of packets The Access Gateway (Access GW) interconnects trusted non-3GPP access networks like WiMAX with the EPC. The Application Function (AF) is an abstraction of the service provider, which communicates with the PCRF to enable AAA at the application layer. The AF may be a single third-party-service or a complex operator controlled service delivery platform. The S2c interface provides the user plane with related control and mobility support between the UE and the PDN GW. This reference point is implemented over a trusted and/or untrusted non-3GPP Access and/or 3GPP access. The S5 interface is providing user plane tunneling and tunnel management between SGW and PDN GW. It is used for SGW relocation due to UE mobility and if the SGW needs to connect to a non-collocated PDN GW for the required PDN connectivity. Two variants of this interface are being standardized depending on the protocol used, namely the GTP and the IETF based Proxy Mobile IP solution [10], [17].

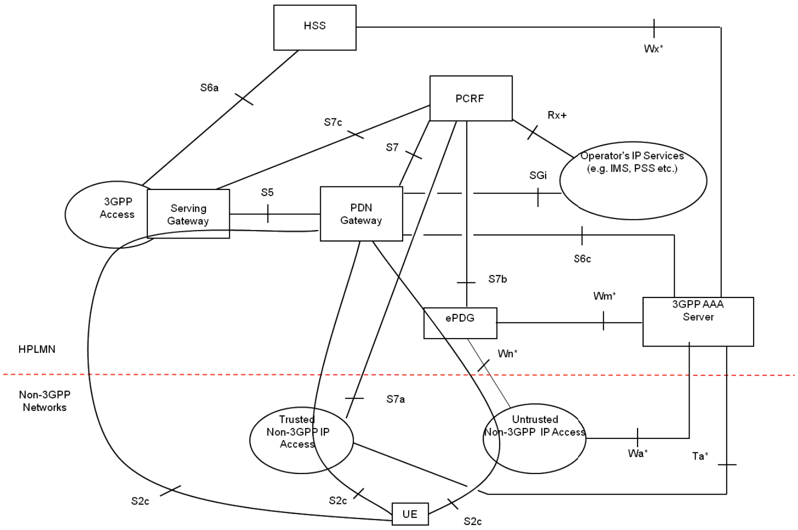


Fig. 1. Non-Roaming Architecture within EPS using S5, S2c [3]

Otherwise, at the EPC architecture in comparison to the IMS, the service itself is not required to use a specific signaling protocol as the SIP.

III. USER CENTRIC APPROACH

This research focuses on stressing the importance of user's choices over the operator's predefined preferences. This means that 3GPP access through Serving Gateway works as the operator has defined. Handovers and other mobility related functionality is not affected. However with non-3GPP networks such as trusted and untrusted IP access networks are in the scope of user's preferences. Next, existing mobility support based on standard is discussed, followed by the properties for more user centric approach.

A. *An Existing UE Mobility Support in Evolved Packed Core*

The components for the UE mobility support have the role of interacting with the core network mobility management components and providing a seamless experience for the applications running on the UE devices, such that operations such as network attachment or handover would be transparently handled. To perform these operations the UE would require an application component, as the background application running on the mobile device that will orchestrate the normal network management procedures. Such devices with needed software are not yet commercially available. The interfaces from the core network side are defined but actual implementations on the UE side are largely missing. To provide value-added functionality the Access Network Discovery and Selection Function (ANDSF) situated in the core network assists the UE with information and operator pushed policies. The ANDSF component has the purpose of communicating with a UE mobility application running on the mobile endpoint device and exchanging information which would enhance both of the Always Best Connected cases, but also allows the network operator to manage and enhance connectivity on a multi-access environment. The ANDSF behavior is described in 3GPP TS23.402 chapter 4,8 [3] and it uses the S14 interface with the ANDSF Management Objects [2]. Fig. 2 gives a good overview of existing core network elements and their relation to access management. A Working Policies Policy Engine can co-operate with the ANDSF, which allows for the delivery of a dynamic and subscriber specific Inter-System UE mobility policies. The operator can configure dynamic behavior, by checking various conditions (e.g. subscriber category, access point names, access restrictions, etc.) and accordingly providing parameterized action (e.g. time-based) to reorder and to indicate its prioritized access network hand-over policies to the UE. Further, the parameters of the Inter-System Mobility Policy can be for example validity areas, time intervals, etc. Once the UE receives a set of such policies, it will apply its current parameters to find a matching policy with the highest priority. From this, the UE can extract an operator-ordered list of access networks directly, that indicate the operators suggested solution for the given client's profile, location and the time of day.

B. *New properties for the User Centric Approach*

User preferences related to connectivity have at least four main factors:

- Quality factors such as connection bandwidth, latency, and reliability

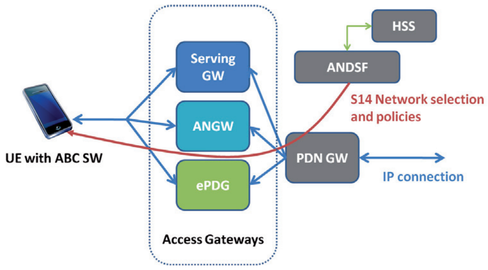


Fig. 2. UE Mobility in the EPS

- Cost, if the usage cost is fixed, time or consumption based or free
- Services, if they are operator specific or common Internet services
- Ease of use, daily routines should not require any extra effort

Of these the ease of use is the one that fits operator based model. In there all the preferences are defined by the operator and no extra effort is required before or during the usage. The same applies to services in case the services are something that the operator is offering. However, quality, common Internet services and specially the cost may not be the best for the user. In terms of quality the WLAN can, in most cases, provide better bandwidth and latency compared to widely deployed 3GPP networks (UMTS, GSM) and WLAN networks are available in homes, offices and various hotspots. This means that they should be utilized whenever possible. Costs of mobile broadband have been dropping due to service provider competition or regulations. Still the mindset is that avoid costs if possible. Flat rate contracts on mobile broadband are easing the importance of cost. These user preferences can be taken into account in UE based application and the same application could also care of network selection defined by the operator through EPC. This application could be called ABC application. This application has the role of orchestrating the mobile client attachment/detachment procedures during the hand-over operations from one Access Network to another. As such, it allows for a seamless experience for the EPC UE clients, by managing the IP connectivity layer operations. It provides wrapper functions to connect and disconnect from each individual access network available, by reusing the client device's standard Layer 2 and 3 attachments. For orchestrating smooth hand-over's, the actual connection and final selection of a connection are provided with a fine-grain control mechanism to be used from the application layers, or managed transparently by the ABC application based on the Inter-System Mobility Policies, received from the ANDSF. The ABC application implements the ANDSF S14 interface, which allows for exchange of information between the core network and the clients. With this mechanism in place, the ABC application can provide the ANDSF its updated network location and connectivity information and it can also receive from the ANDSF coverage maps in the form of Access Network Discovery Information and hand-over indications in the form of Inter-System Client Mobility Policies. Based on the operator pushed Inter-System Mobility Policies, the ABC application can handle transparently (if configured by the subscriber) the operator's indications and requests. Besides this network-triggered hand-over mechanism, of course, manually triggered hand-over's on subscriber's request are supported and have the highest priority over the network-triggered ones. For performing all these operations and for retrieving IP connectivity information, the ABC application should have an API towards the client application layer, which allows for easy integration with existing and future applications.

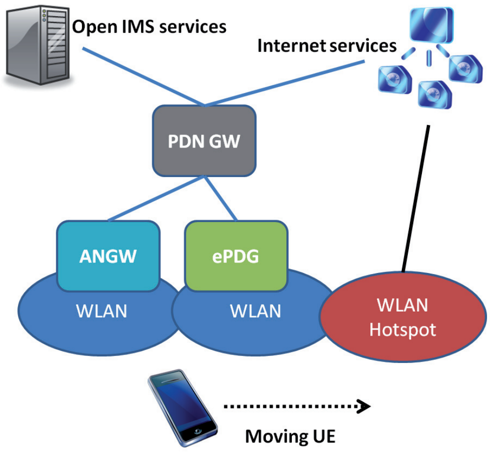
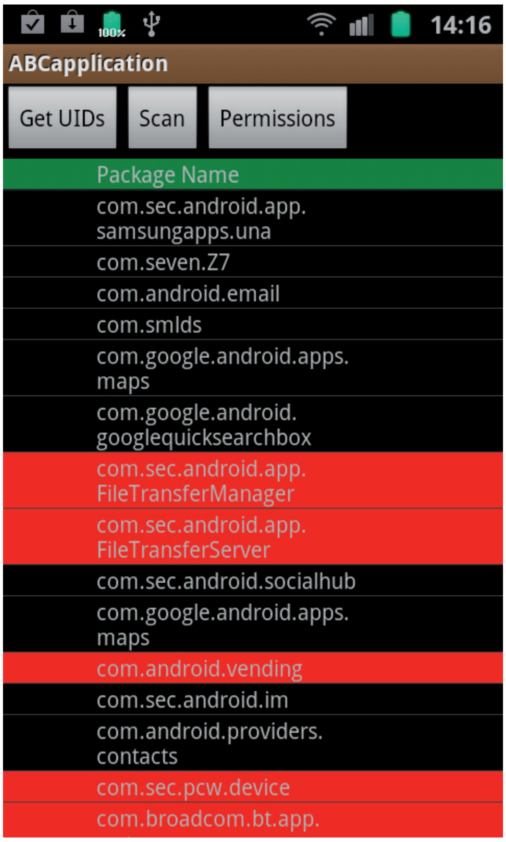


Fig. 3. Proof-of-Concept Test Setup

Both of the platforms (Maemo and Android) were showing similar performance although the detailed performance analysis is left for the future research.

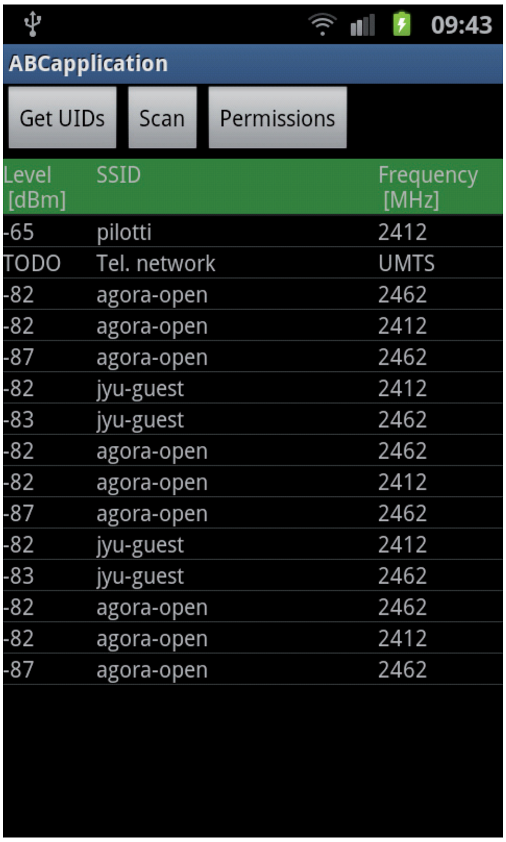
IV. Proof-of-Concept

In this section the user centric Always Best Connected proof-of-concept implementation is presented. The scenario shows how the ABC application, in the UE side, was able to handle the user mobility between the access networks. And it was controlled in co-operation with the operator and user-defined preferences. Figure 3 presents the involved test bed setup. The test bed consists of an Open IMS Core that is responsible for controlling the multimedia sessions. Other main services were operator provided Internet access and a 3rd party Internet access such as a hotspot. Additionally, simulated EPC components were involved in the test environment. In the test bed the UE was connected to several WLAN networks, while the simulated EPC components and a 3rd party hotspot (local break out in the 3GPP standards) were controlling the access. The UE was equipped with an additional software



Package Name
com.sec.android.app.samsungapps.una
com.seven.Z7
com.android.email
com.smlds
com.google.android.apps.maps
com.google.android.googlequicksearchbox
com.sec.android.app.FileTransferManager
com.sec.android.app.FileTransferServer
com.sec.android.socialhub
com.google.android.apps.maps
com.android.vending
com.sec.android.im
com.android.providers.contacts
com.sec.pcw.device
com.broadcom.bt.app.

Fig. 4. The ABC application - applications with Internet connection



Level [dBm]	SSID	Frequency [MHz]
-65	pilotti	2412
TODO	Tel. network	UMTS
-82	agora-open	2462
-82	agora-open	2412
-87	agora-open	2462
-82	jyu-guest	2412
-83	jyu-guest	2462
-82	agora-open	2462
-82	agora-open	2412
-87	agora-open	2462
-82	jyu-guest	2412
-83	jyu-guest	2462
-82	agora-open	2462
-82	agora-open	2412
-87	agora-open	2462

Fig. 5. Available network in priority order in the ABC application

component called the ABC application. This application was able to make use of the access network discovery information from the simulated ANDSF and from the user's manually defined preferences. The ABC application also had simulated the Inter-System Mobility Policies from the ANDSF, which are the practical means for the operator to suggest access network policies to the UE. In the demonstration the UE travels from a trusted non-3GPP (ANGW) to an untrusted non-3GPP (ePDG) and finally connects to a 3rd party WLAN hotspot. The ANDSF and the Inter-System Mobility policy was XML [9] based definitions stored in to the UE ABC application. The Non-3GPP access configuration was host-based and implemented on a Proxy Mobile IPv6. Final access was 3rd party WLAN hotspot. When the UE finally connected there was a break on the communication since seamless mobility could not be achieved when connecting outside of an operator-defined network. The OpenIMS connection was re-established after the short connection break. However this was in agreement with the user's preferences in the ABC application. Mobility between non-3GPP IP access was seamless through the Proxy Mobile IP. Network selection algorithm was simplified: it examined the signal strengths and chose the best network available if the network was defined in the profile. In Figure 4 applications that had Internet permissions were highlighted with red color. This information will be used in the future to profile the applications. This way different application can have different properties. The test environment illustrated by the ABC application is shown in Figure 5. The application shows available networks. The WLAN network "pilotti" is currently used, as shown in the top of the list. The cellular network is also shown, however it was not used at this point. Hand-over's happened only between WLAN networks. In the test the connection was changed from "pilotti" network to "agora-open" and then to "jyu-guest". This was done signal strength. Two mobile environments were used one: one implemented with Qt [14] and run on top of the

Maemo 5 [13] platform in Nokia N900 device, the second was Android [11] based. The performance measurements did show around 2 to 10 second time for the handover. The Android implementation was closer to 2 second and Qt based solution was up to 10 second. These were very initial performance measurement without any optimization.

V. CONCLUSION AND FUTURE WORK

This paper illustrates a user centered approach to the Always Best Connected model by coupling the state-of-the-art technologies of the telecommunication next generation network domain (namely the IP Multimedia Subsystem and the Evolved Packet Core) and user preferences. A generalized connection-aware service architecture enabling the mediation between network and services access was presented. The components of the architecture were discussed, whereas a special focus lies on the user centric mobility management enhanced with the operator predefined preferences. The ABC application is a key component in the architecture and manages both the standard way as defined in EPC and also takes into account the user preferences. This generalized architecture was implemented prototypically using the OpenIMS software toolkit and simulated simple EPC components supporting basic proxy mobile IP configuration. A WLAN-based Internet access over heterogeneously configured networks validated the ABC application in a demonstration. Future research continues with further performance measurements, fine tuning of the network selection algorithm and adding more heterogeneous networks to the test bed.

REFERENCES

[1] 3GPP. IP Multimedia Subsystem (IMS); Stage 2. TS 23.228, 3rd Generation Partnership Project (3GPP), September 2008.

[2] 3GPP. Access Network Discovery and Selection Function (ANDSF) Management Object (MO); V10.3.0 Release 10. TS 24.312, 3rd Generation Partnership Project (3GPP), July 2011.

[3] 3GPP. Architecture enhancements for non-3GPP accesses; V10.4.0. TS 23.402, 3rd Generation Partnership Project (3GPP), July 2011.

[4] 3GPP. Policy and charging control architecture; V10.4.0 Release 10. TS 23.203, 3rd Generation Partnership Project (3GPP), July 2011.

[5] E. Gustafsson and D. Jonsson. Always best connected. *Wireless Communications, IEEE*, page 49, February 2003.

[6] J. Kellokoski, E. Tukia, E. Wallenius, T. Hämäläinen, and J. Naarmala. Call and Messaging Performance Comparison Between IMS and SIP Networks. *Internet Multimedia Services Architecture And Applications (IMSAA), 2010*, pages 1–5, December 2010.

[7] J. Kellokoski, E. Tukia, E. Wallenius, T. Hämäläinen, and J. Naarmala. Registration performance comparison between IP Multimedia Subsystem and Session Initiation Protocol networks. *Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2010*, pages 20–25, October 2010.

[8] V. Leung, T. Wong, and P. TalebiFard. Breaking the silos - access and service convergence over the mobile internet. *MSWiM'08: Proceedings of the 11th international symposium on Modeling, analysis and simulation of wireless and mobile systems*, pages 286–293, October 2008.

[9] World Wide Web Consortium. Extensible markup language (xml) 1.0 (fifth edition). http://www.w3.org/TR/xml/, November 2008.

[10] S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury, and B. Patil. Proxy Mobile IPv6. RFC 5213 (Proposed Standard), August 2008.

[11] Google Inc. Android developers. http://developer.android.com/, June 2011.

[12] Fraunhofer FOKUS NGNI. Openimscore.org. http://www.openimscore.org/, May 2011.

[13] Nokia. Meamo software platform. http://maemo.nokia.com/, June 2011.

[14] Nokia. Qt - cross platform application and ui framework. http://qt.nokia.com/, June 2011.

[15] M. Poikoselkä and G. Mayer. *The IMS IP Multimedia Concepts and Services*. Wiley, Chichester, UK, 2009.

[16] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler. SIP: Session Initiation Protocol. RFC 3261 (Proposed Standard), June 2002. Updated by RFCs 3265, 3853, 4320, 4916, 5393, 5621, 5626, 5630, 5922, 5954, 6026, 6141.

[17] R. Wakikawa and S. Gundavelli. IPv4 Support for Proxy Mobile IPv6. RFC 5844 (Proposed Standard), May 2010.

PII

REAL-LIFE PERFORMANCE ANALYSIS OF ALWAYS-BEST-CONNECTED NETWORK

by

Jari Kellokoski, Joonas Koskinen and Timo Hämäläinen 2012

NTMS 2012, New Technologies, Mobility and Security

Real-life Performance Analysis of Always-Best-Connected Network

Jari Kellokoski, Joonas Koskinen and Timo Hämäläinen
Department of Mathematical Information Technology
University of Jyväskylä
FI-40014 Jyväskylä, Finland
Email: {jari.k.kellokoski, joonas.a.koskinen and timo.t.hamalainen} @jyu.fi

***Abstract*—Mobile Internet has rapidly evolved in the past years with an ever increasing number of novel technologies and services with a variety of access technologies. Indeed, today's mobile devices often support multiple communication technologies for accessing Internet services. However, they all do not tap the full potential of these capabilities, as users often have to manually select each network, and only one network is used at a time. The concept of Always Best Connected (ABC) allows a person to connect applications using the devices and access technologies that best suit to his or her needs, thereby combining the features of access technologies to provide an enhanced user experience for future Internet. This Always Best Connected scenario has been considered to be complex and to generate a number of requirements, not only for the technical solutions, but also in terms of business relationships between operators and service providers. The Third Generation Partnership Project (3GPP) standardized the Evolved Packet System (EPS), where one of the key features is a support access system selection based on a combination of operator policies, user preference and access network conditions. The standard focuses mainly on the operator point of view, and the user is expected to follow this approach. Nevertheless, the standard offers a number of possibilities where the user-centric approach can improve the ABC network selection over the selection predefined by the operator.**

This research shows how to design a simple but efficient algorithm for the network selection when implementing an Always Best Connected application for mobile devices. This application works with the EPS standard. A real-life implementation and proof-of-concept performance measurements are presented. This will show that in real-life the simple and straightforward methods can provide efficient solutions for problems known to be complex.

***Keywords*—Always Best Connected; Performance; Mobility Management.**

I. INTRODUCTION

Integration of heterogeneous access networks and efficient use of the available communication systems is one of the key challenges for the next generation of mobile communication. Today's mobile devices come with various network interfaces. Even the cheaper smartphones support at least two wireless technologies, i. e. the Universal Mobile Telecommunications System (UMTS) and IEEE 802.11 (WLAN in this papers context). Over the past years, the number of heterogeneous access networks that are available at a specific location grew dramatically. Other technologies such as Term Evolution (LTE) or Worldwide Interoperability for Microwave Access (WiMAX) are being deployed currently. All of these networks show different communication characteristics, e.g. in terms of throughput, delay, availability and costs, and in combination they offer a high communication performance. In an environment of multiple access technologies, the concept of being always connected becomes Always Best Connected. This refers to being not only always connected, but also being connected in the best possible way [4].

The aim of the present research is twofold. First, to develop a user's device-based simple algorithm and service that will work with the existing EPS standard and with other known networks such as WLAN hotspots and cellular networks. Second, to make performance measurements of this developed algorithm implementation and to show that the idea works in a real-life mobile environment. The paper is organized as follows. Section II introduces the background and related work. Section III gives an overview of the Evolved Packed System standard, and Section IV presents a novel algorithm design for Always Best Connected mobility. This is followed by a proof-of-concept section that evaluates the prototype implementation developed. Section VI finalizes the paper with Conclusion and Future Work.

II. BACKGROUND AND RELATED WORK

Since the introduction of the Always-Best-Connected term [4] there have been multiple strategies to decide which network is the best at the moment. In their early work Gustafsson et al. made the first proper definitions for Always-Best-Connected network. Their definition of the best connected network came with an estimate of complexity. It was stated that the choises available for a person selecting the best available access network and device at any point in time, will generate great complexity and a number of requirements. Indeed, this complexity has been present in most of the solutions offered. Class or policy based [11], [7] strategies provide differentiation for Quality of Service (QoS) requirements. There may be problems with these methods if the input data is vague. For vague data, intelligent control techniques such as fuzzy [13] or neural networks [12] are usually better. The problem with intelligent control techniques is the complexity when increasing the inputs and options. And there is a challenge on design of the systems as well as training data. Besides these, there have been analytical models [9], [5]. But these often do not grasp the whole complexity of the decision problem. There is also the combined solution [10], which uses network bundles, allowing delays in data transmission while waiting for upcoming opportunities. Its aim is to manage individual application requirements and the effect of concurrent network usage. This approach increases the number of possible configurations, making the decision problem more complex. The solution allocates votes to the application that is then used in choosing the network. This can be considered as a scheduling problem on a parallel machine with job-splitting [6]. It is known to be NP-hard and cannot be optimally solved within polynomial time. In a summary, the approach presented suffers from two major challenges: It is computationally complex, and a real-life implementation is missing or not done in real mobile environment. On the other hand, one can have a straight-forward solution to network selection and a real-life implementation to back this up. This paper examines the actual networks currently in use and the forthcoming 3GPP Evolved Packed Core network. The paper also presents an implementation of an application that enables the always best connectivity. The aim is to show that in real-life as well as with the Evolved Packed Core network, network selection can be simple: it keeps the user in control and performs these operations with a low computational overhead. Additionally, the overall software architecture of always best connected network is discussed. However, such approach comes at the cost that the network selection is not always optimal. The solution could be considered as the most suitable, however.

III. STANDARD - THE EVOLVED PACKED SYSTEM

This section outlines one of the major network technologies, namely the Evolved Packed System, which has the potential to become the next common baseline for all IP based services. The Evolved Packet System, formerly known as the System Architecture Evolution (SAE), was standardized by 3GPP and consists of a radio part: (Evolved URTAN (E-UTRAN)) and a network part: (Evolved Packet Core (EPC)) [3]. The main objectives of the Evolved Packed System (EPS) are to:

- provide higher data rates, low latency, high level of security, support of variable bandwidth and Quality of Service (QoS)
- support a variety of different access systems (existing and those in the future) and ensure mobility and service continuity between these access systems
- support access system selection based on a combination of operator policies, user preference and access network conditions – as an operator-based ABC
- provide capabilities for co-existence with legacy systems and migration to the Evolved Packet System

This section focuses on the core network part (EPC), as it plays the key role in providing the IP connectivity. The section also describes the components of EPC, highlights their major functionalities and outlines their mobility support. The EPC architecture that interconnects 3GPP and non-3GPP access networks consists of several main subcomponents, namely eNodeB, Mobility Management Entity (MME), Serving Gateway (SGw) and Packet Data Network Gateway (PDN-Gw). In addition to these, several other components are present for inter-operating with non-3GPP access. These include WLAN/WiMAX (ePDG, ANGw) for access gateways and the Access Network Discovery and Selection Function (ANDSF).

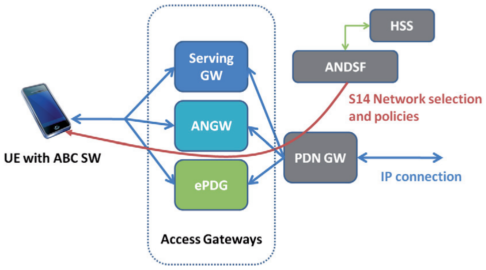


Fig. 1. UE Mobility in the EPS

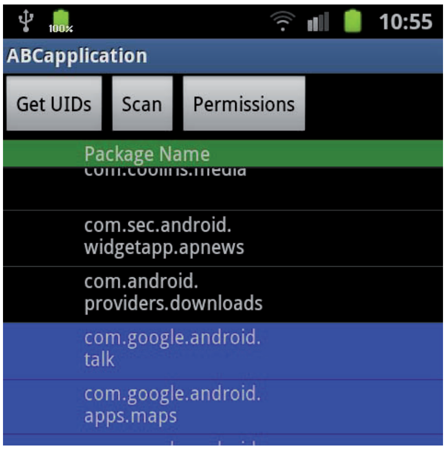
The PDN Gateway provides connectivity from User Equipment (UE) to one or multiple external PDNs simultaneously. The PDN-Gw acts also as a mobility anchor, but between 3GPP and non-3GPP technologies and in addition performs packet filtering and charging. The Home Subscriber Server (HSS) is the central database in the EPC storing user-related information. The Policy and Charging Rule Function (PCRF) encompasses the two main functions of flow based charging: charging and QoS controls (e.g. QoS control and signaling, etc.). The ANDSF is a new EPC element in Release 8 and performs data management and controls functionality to assist the UE on the selection of the optimal access network in a heterogeneous scenario via the S14 interface. The S14 is the Logical interface between the ANDSF and the UE [1]. The Evolved Packet Data Gateway (ePDG) attaches un-trusted non-3GPP access networks like WLANs to the EPC and performs important security functions such as tunnel authentication and authorization and IPSec encapsulation/decapsulation of packets The Access Gateway (Access GW) interconnects trusted non-3GPP access networks like WiMAX with the EPC. The components for the UE mobility support have the role of interacting with the core network mobility management components and providing a seamless experience for applications running on the UE devices, to allow operations such as network attachment or handover be transparently handled. To perform these operations, the UE would require an application component, as the background application running on the mobile device that will orchestrate the normal network management procedures. Such devices with the required software are not yet commercially available. The interfaces from the core network side are defined, but actual implementations on the UE side are largely missing. To provide value-added functionality, the ANDSF situated in the core network assists the UE with information and operator-pushed policies. The ANDSF component has the purpose of communicating with a UE mobility application running on the mobile endpoint device and exchanging information, which would enhance both of the Always Best Connected cases, but it also allows the network operator to manage and enhance connectivity on a multi-access environment. The ANDSF behavior is described in 3GPP TS23.402 chapter 4.8 [2], and it uses the S14 interface with the ANDSF Management Objects [1]. Fig. 1 gives a good overview of the existing core network elements and their relation to access management. A Working Policies Policy Engine can co-operate with the ANDSF, which allows for the delivery of a dynamic and subscriber specific Inter-System UE mobility policies. The operator can configure dynamic behavior by checking various conditions (e.g. subscriber category, access point names, access restrictions, etc.) and, accordingly, providing parameterized action (e.g. time-based) to reorder and to indicate its prioritized access network hand-over policies to the UE.

IV. A NOVEL APPROACH TO ALWAYS BEST CONNECTED IP NETWORK

In this research the network selections are designed to be simple and straightforward. There should not be need for complex calculations. The justification for this comes from real-life. When we look at today's devices, we discern mainly two possibilities for connectivity to Internet services: one through the operator's cellular access and another one through WLAN (IEEE 802.11b/g/n). The standard's chapter III referred to above gives information about how cellular and WLAN access could be combined by the operator. This must be taken into account when designing a network selection algorithm for an Always Best Connected application. Before going into algorithm design, handover types will be clarified.

A. Handover Types

There are many types of mobility cases where the point of attachment can change in an IP network. This is why also handovers have been categorized based on the type of the handover. The "Mobility Related Terminology" (RFC 3753) gives the following definitions for handover. There is a *horizontal handover*: when a mobile node moves between access points which use the same technology. *A vertical handover* take place when a mobile node changes the point-of-attachment technology used, for example in research applications, from WLAN to UMTS. In addition to these definitions, there is one more mobility type. From point of view of IP network it is not a handover, it is just a normal connectivity-related action. This might be called *between-session-mobility*; first the equipment with the required connectivity is used, in some location; then all connections are closed or at least not used while moving to another location; there, the user starts using the connectivity again. A good example of this is a laptop/netbook/tablet user, with scheduled meetings and with all the necessary connections for the device: he/she closes the lid of the device and stops all connections before moving back to a desk or to another meeting room where the needed connections are started again. During the switch, the user is not actively expecting connectivity; it might or might not work. Nevertheless, the actual communication will take place later, once the user is ready to start communicating. This is not directly comparable to smartphone usage although there are similarities when excluding the real-time communication. The usage of smartphone will mostly take place when stationary, as in web browsing, video consuming and messaging.



com.sec.android.widgetapp.apnews

com.android.providers.downloads

com.google.android.talk

com.google.android.apps.maps

Fig. 2. The ABC application permission page

In the algorithm design section below, the algorithm design aims to utilize an EPC solution when available and a low complex algorithm otherwise.

B. Algorithm Design for Always-Best-Connected Application

The main goal of the algorithm design is to achieve support for the EPC system and, if it is not available, find out the most suitable connection for each application. In the approach used the following basic assumptions are made: 1. The user is in control: if some connectivity is setup, specifically by the user, for some application, then it must be respected. 2. Operator provided information (ANDSF) will be used if the information provided has heterogeneous networks defined. If it contains something else, then just the cellular networks are used. 3. Otherwise the ABC algorithm is applied. The algorithm itself is, as far as possible, simple and straightforward. Complexity is avoided by making direct choices based on predefined preferences. The idea is to have either/or choices, that is, some condition is either true or false. This choice has to be made always when an Internet access is requested for a particular application. The main steps (T/F choices) for access point selection in the algorithm are:

1) Valid ANDSF information is available?
2) Application is part of profile, is the profile active/valid?
3) Application is real-time? Always ask for used access-point
4) Known protected WLAN connection is available?
5) Open WLAN connection is available?
6) Use cellular IP connection

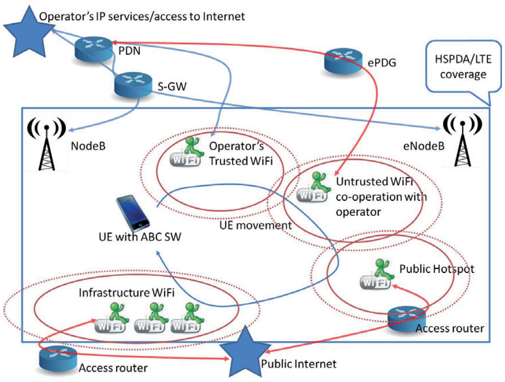


Fig. 3. Test setup

Profiles are user-defined groups of applications and access points made to ease configuration. For example, the user can create home and work profiles where the access points are known. Thus, in the user's home profile the connections are through a home WLAN and in the work profile through a company WLAN. For real-time applications (as in Fig. 2 the Google Talk), it is better to have them in the always ask mode, where the user equipment asks the access point when application is launched or signed in. The always ask mode enables the user to rationalize access point usage. During working hours or at home it is reasonable to a have connection through WLAN. For any other application one should just check if there is a protected or an open WLAN available and, if not, then fall back to a cellular IP connection. The algorithm needs to be revisited if the user equipment is moving and the network environment changes. In case of EPC (valid ANDSF information is available) it should not be any problem, as EPC supports seamless vertical handovers. There might be delays in packet routing and possibly packet loss, but connections should still remain. However, outside EPC the case is problematic from the mobility point of view. There is no other choice then but to drop the existing connections and form a new one, based on steps 2 to 6. Thus, there is no real mobility as connections need to be rebuilt. It is up to the specific application to deal with connection loss.

V. PROOF-OF-CONCEPT PERFORMANCE MEASUREMENTS

In this section the user and device centric Always Best Connected proof-of-concept implementation and performance measurements are presented. The scenario shows how the ABC application, in the UE side, is able to handle user mobility between access networks. The application is functioning, in agreement with the operator information from EPC, based on the ABC algorithm. Initial performance measurements without the novel ABC algorithm were done earlier [14]. The network change times in the open network were around one to ten seconds depending on network conditions and on whether the measurement environment was Android or Qt. The link quality and load has its effect on when it would be effective to change network, especially in case of real-time traffic [8]. In this research, two main scenarios were implemented: one with EPC mobility and another one without it. Implementation was done in the Android software environment. Fig. 3 shows the test setup. The test bed consisted of simulated Evolved Packet Core WLAN accesspoints: one of these was operator's trusted WLAN and the other one was untrusted. Besides the EPC, there were two other WLAN networks: one of hotspot style, with only one WLAN base station, and another one with the WLAN infrastructure network with multiple base stations. Cellular access was through UMTS bases tations to live network. However, since there was no control over the live network, results against the live network are to be considered as informative only. The following scenarios were defined: 1. network change between a public hotspot and an infrastructure WLAN network. 2. authentication overhead in anetwork change within EPC from a trusted WLAN to an untrusted one. In this scenario, the UE needed to authenticate itself before a connection could be made.

A. Challenges

There were some challenges in the test setup. These were caused by the lack of a real EPC system and the current constrains in the Android software environment. The EPC was simulated by adding a delay of 100 ms in the path of signaling. For EPC authentication, the aim was to use IPsec (RFC4301) tunneling as defined in the standard. The idea was that the UE related actions would be done as real as possible. Nevertheless, this was not possible within the Android software environment. Instead, the Secure Sockets Layer (SSL) (RFC 5246) tunnel, which is widely used in web browsers was employed. This was considered to be the next best choice. IPsec tunnel creation times were tested in the Linux environment to get an idea of the performance of a real-life implementation. Additional challenges in the Android environment were the lack of Mobile IP and multibearer connections. This prevented truly seamless handovers between simulated EPC access points since only one connection was possible at a time. All the applications in the UE had to use same connection.

B. Results

Network change times between a public hotspot and an infrastructure WLAN are presented in Table I. The table results show that network change can happen around one second with a small standard deviation. During the measurements, the WLAN network was not used by other users. Clearly, the performance was not sufficient for real-time traffic, as gaps such as this are not acceptable (over 200 ms that is generally kept as a limit for real-time communication). Informative measurements against a live network are also shown in the same table. There is notably delay in live network when compared to WLAN. In contrast, Table II depicts the measurement results with the second scenario where authentication was required by the EPC. Three different approaches were examined: SSL

	WLAN (msec)	σ	UMTS (msec)	σ
Android	941	203	2546	1001
Qt	4125	394	5424	175

TABLE I
Network change delay in open access

	WLAN (msec)	σ
SSL with VPN (Android)	2690	172
SSL tunnel only (Android)	109	47
IPsec in Linux	2083	189

TABLE II
SSL and IPsec handshake times over TCP

tunnel in a Virtual Private Network style, SSL tunnel only as in Browser and IPsec tunnel. As the table shows, the real SSL tunnel creation was time-consuming. The advantage of this approach is that the VPN hides the IP change. That again makes mobility from the application point of view possible if the connection properties otherwise allow it. For example, keep-alive messages will not go through during the network change. The SSL tunnel only solution was clearly faster than complete tunneling but not suitable for real-time traffic when one adds the delay expected from EPC network (over 200 ms only for authentication and EPC processing). IPsec provided slightly faster reponse than real SSL tunneling. Still, even that solution was causing problems for real-time communication.

To summarize off-the-shelf solutions can't provide suitable real-time network change performance. For EPC authentication requirements, there were no standard-based solutions available at all, and the modified solutions did not work fast enough. The IPsec-based solution based on Linux gave hints that performance will improve with increasing computing power in mobile devices.

VI. Conclusion and Future Work

This paper dealt with real-life long-delay problems when performing network changes in heterogeneous networks. These delays can be perceived by end users as service blockers in real-time communication. The paper presented a simple and straightforward network selection algorithm was presented. Evolved Packed Core support was added, so that the algorithm can utilize ANDSF information when it is available. Through two user scenarios network change performance and a selection algorithm were evaluated in an Android based implementation. Due to challenges in the Android environment, some of the measurements were done in Qt and Linux based systems. The measurements did show the difficulty of real-time communication when a network change occurs in a heterogeneous network. All the measurement times were too high, to maintain continuous real-time communications. These facts defend the use a of simple and straightforward network change algorithm. The proposed algorithm makes straightforward either/or choices based on predefined preferences. The algorithm proposes the use of a multibearer solution to handle real-time and non-real-time traffic through different connections. At this point, it was not possible in the Android environment as there could be only one connection at a time. Also, the lack of IPsec tunnels leads to workarounds with SSL tunneling. The results from these measurements further illustrate that the existing devices are not ready for real-time communication within EPC. Tunneling itself was able to make application level tunneling possible where the communication path could handle lengthy delays during a network change. In future, when computing power further increases in mobile devices and when multibearer connections are possible, a finer grade network selection algorithm can be applied: for example, triggers such as signal-to-noise ratio to indicate the start of a network change. Multibearer connections can help in creation of real mobility, where connections are created-before-break, allowing seamless handovers. More computing power is needed to ensure a required level of security in authentication and real-time requirements in communication.

Acknowledgment

The authors would like to thank Janne Villikka for providing the implementation and performance measurements with the ABC application under Qt and Linux.

References

[1] 3GPP. Access Network Discovery and Selection Function (ANDSF) Management Object (MO); V10.3.0 Release 10. TS 24.312, 3rd Generation Partnership Project (3GPP), July 2011.

[2] 3GPP. Architecture enhancements for non-3GPP accesses; V10.4.0. TS 23.402, 3rd Generation Partnership Project (3GPP), July 2011.

[3] 3GPP. Policy and charging control architecture; V10.4.0 Release 10. TS 23.203, 3rd Generation Partnership Project (3GPP), July 2011.

[4] E. Gustafsson and D. Jonsson. Always best connected. *Wireless Communications, IEEE*, page 49, February 2003.

[5] O. Ormond, J. Murphy and G.-M. Muntean. Utility-based intelligent network selection in beyond 3g systems. *IEEE International Conference on Communications, 2006*, pages 1831–1836, December 2006.

[6] C.Y. Lee, and G. Yu. Parallel-machine scheduling under potential disruption. *Optimization Letters, vol. 2 no 1.*, pages 27–37, January 2008.

[7] P.A.A. Gutierrez and I. Miloucheva. Automated qos policy adaptation for heterogeneous access network environments. *Systems and Networks Communications, ICSNC 2007.*, page 65, September 2007.

[8] E.S Boysen and J. Flathagen. Using SIP for Seamless Handover in Heterogeneous Networks. *Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2011*, October 2011.

[9] V. Gazis, N. Alonistioti and L. Merakos. Toward a generic always best connected capability in integrated wlan/umts cellular mobile networks (and beyond). *Wireless Communications, IEEE*, pages 20–29, June 2005.

[10] S. Lahde, M. Wegner and L. Wolf. Efficient network selection in heterogeneous communication scenarios using arbitration. *IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks, 2010*, pages 1–6, August 2010.

[11] T. Bejaoui and N. Nasser. Handover and class-based call admission control policy for 4g-heterogeneous mobile networks. *Computer Systems and Applications, AICCSA 2008.*, pages 373–380, April 2008.

[12] L. Giupponi, R. Agusti, J. Perez-Romero, and O. Sallent. A fuzzy neural jrrm in a heterogeneous scenario supported by prediction strategies for horizontal and vertical handovers. *IEEE International Conference on Fuzzy Systems, 2006*, pages 655–662, September 2006.

[13] A. Wilson, A. Lenaghan and R. Malyan. Optimising wireless access network selection to maintain qos in heterogeneous wireless environments. *8th International Symposium on Wireless Personal Multimedia Communications, WPMC 2005*, pages 1236–1240, September 2005.

[14] J. Kellokoski and T. Hämäläinen. User-Centric Approach to Always-Best-Connected Networks. *Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2011*, October 2011.

PIII

POWER CONSUMPTION ANALYSIS OF THE ALWAYS-BEST-CONNECTED USER EQUIPMENT

by

Jari Kellokoski, Joonas Koskinen and Timo Hämäläinen 2012

NTMS 2012, New Technologies, Mobility and Security

Power Consumption Analysis of the Always-Best-Connected User Equipment

Jari Kellokoski, Joonas Koskinen and Timo Hämäläinen
Department of Mathematical Information Technology
University of Jyväskylä
FI-40014 Jyväskylä, Finland
Email: {jari.k.kellokoski, joonas.a.koskinen and timo.t.hamalainen} @jyu.fi

***Abstract*—Mobile Internet has rapidly evolved in the past years with an ever increasing number of novel technologies and services with a variety of access technologies. Indeed, today's mobile devices often support multiple communication technologies for accessing Internet services. For users the accessing of these data hungry services means that the mobile device has to be charged more often. Energy efficiency in mobile device communication has been considered to be out of users hands. The concept of Always Best Connected (ABC) allows a person to connect applications using the devices and access technologies that best suit to his or her needs, thereby combining the features of access technologies to provide an enhanced user experience for future Internet. This Always Best Connected scenario can make mobile device more energy efficient by using always the most energy efficient connection.**

Mobile communication networks and connected devices consume a small fraction of the global energy supply. However, meeting the rapidly increasing demand for more capacity in wireless broadband access will further increase the energy consumption. For example Cisco Visual Networking Index: Global Mobile Data Traffic Forecast 2010-2015 expects compound annual growth rate of 92 percent during 2010 to 2015 Operators are now facing both investing in denser and denser networks as well as increased energy cost. Current cellular systems based on Universal Mobile Telecommunications System (UMTS) and Long Term Evolution (LTE) is characterized by high spectrum efficiency, but low energy efficiency. In urban areas as well as in homes and offices alongside cellular networks IEEE 802.11 (WLAN in this papers context) networks are available. In this heterogeneous network environment the communication energy efficiency can make significant difference when considering how often the user has to recharge the mobile device.

In this article we analyze energy efficiency of Always-Best-Connected solution. The application is used in measurements in a various real-life use-cases. The results are showing that algorithm can improve overall energy efficiency without compromising the user experience.

Keywords*—*Always Best Connected; Energy Efficient; Mobility Management.

I. INTRODUCTION

Integration of heterogeneous access networks and efficient use of the available communication systems is one of the key challenges for the next generation of mobile communication. Today's mobile devices come with various network interfaces. Even the cheaper smartphones support at least two wireless technologies, i. e. the UMTS and WLAN. Over the past years, the number of heterogeneous access networks that are available, at a specific location, have grown dramatically. All communication networks show different communication characteristics, e.g. in terms of throughput, delay, availability and costs, and in combination they offer a high communication performance. In an environment of multiple access technologies, the concept of being always connected becomes Always Best Connected. This refers to being not only always connected, but also being connected in the best possible way [4]. One of the key characters in cellular communications is power consumption. Today's devices are packed with features which are consuming battery as they offer best possible user experience. Large displays and camera features are the ones which are easily understood by the user when considering current consumption. On the other hand, characteristics in data communication are not well understood. It is known that communication consumes the battery but witch communication path should the user choose in order to save the battery. Furthermore, various today's services such as email fetch, chat, and widgets tend to keep connection always on even when the actual need for this is not necessary. People are mostly using the services in stationary and only then the services need to be updated. The aim of this research is to minimize power consumption used by IP communication without compromising the user experience. The research makes use of previously developed Always Best Connected algorithm [8] which is modified to take the energy efficiency into account. The paper is organized as follows: Section II introduces background and related work. Section III presents a novel energy efficiency algorithm for Always Best Connected IP networks and Section IV is about real-life implementation and measurements to validate the developed algorithm. Section V finalizes the paper with Conclusion and Future Work.

II. BACKGROUND AND RELATED WORK

Since the introduction of the Always-Best-Connected term [4] there have been multiple strategies to decide which network is the best at the moment. In their early work Gustafsson et al. made the first proper definitions for Always-Best-Connected network. This notion of Always Best Connected enables user to remain seamlessly connected to the network in a way that best suits their application needs. The notion of the "best" is based on a number of user and application dependent factors such as personal preferences, device capabilities, security, available network resources and network coverage. There have been previous researches on combining energy efficiency and most suitable connectivity. Their definition of the best connected network came with an estimate of complexity [4]. It was stated that the choices available for a person selecting the best available access network and device at any point in time, will generate great complexity and a number of requirements. There is also a solution [6], which uses network bundles, allowing delays in data transmission while waiting for upcoming opportunities. Its aim is to manage individual application requirements and the effect of concurrent network usage. This approach increases the number of possible configurations, making the decision problem more complex. The solution allocates votes to the application that is then used in choosing the network. This can be considered as a scheduling problem on a parallel machine with job-splitting [5]. It is known to be NP-hard and cannot be optimally solved within polynomial time. Energy efficiency in combination with most suitable connectivity has been part in a previous research. Multi-Constraint dynamic system models have been applied to solve this [7] there access selection is seen as a assigning multiple traffic flows to multiple interfaces. It was modeled as a variant of bin packing problem. Different approximations algorithms were used to find a near-optimal solution to the problem which was intended to minimize power consumption and maximize user experience. However the research did not consider vertical handover caused by substitution or handling overhead incurred by traffic flow partitioning. Another research [3] proposes a framework for a total cost analysis. One of the key aspects is energy consumption which is one of the key conclusions of that research:

- both the energy cost and access network cost are dependent on the transmission range
- for high-density deployments, the idle power of the base stations and backhaul will become a significant factor
- the energy cost is also strongly dependent on the amount of available spectrum. More spectrums more savings to energy and infrastructure cost

In a summary, the approaches presented are suffering from two major challenges: They are computationally complex, and a real-life implementation is missing or not done in real mobile environment. This paper examines energy efficient IP communication in today's networks and presents algorithm that can help reducing energy consumed by data communications. The real-life implementation and power consumption measurements are conducted to show the energy savings. Before going to the algorithm design Evolved Packed System and handover types are introduced.

A. Standard - The Evolved Packed System

This section outlines one of the major network technologies, namely the Evolved Packed System, which has the potential to become the next common baseline for all IP based services. The Evolved Packet System, formerly known as the System Architecture Evolution (SAE), was standardized by 3GPP and consists of a radio part: (Evolved URTAN (E-UTRAN)) and a network part: (Evolved Packet Core (EPC)) [2]. The main objectives of the Evolved Packed System (EPS) are to:

- provide higher data rates, low latency, high level of security, support of variable bandwidth and Quality of Service (QoS)
- support a variety of different access systems (existing and those in the future) and ensure mobility and service continuity between these access systems
- support access system selection based on a combination of operator policies, user preference and access network conditions – as an operator-based ABC
- provide capabilities for co-existence with legacy systems and migration to the Evolved Packet System

The EPC architecture that interconnects 3GPP and non-3GPP access networks consists of several main subcomponents, namely eNodeB, Mobility Management Entity (MME), Serving Gateway (SGw) and Packet Data Network Gateway (PDN-Gw). In addition to these, several other components are present for inter-operating with non-3GPP access. These include WLAN/WiMAX (ePDG, ANGw) for access gateways and the Access Network Discovery and Selection Function (ANDSF). The ANDSF component has the purpose of communicating with a User Equipment (UE) mobility application running on the mobile endpoint device and exchanging information, which would enhance both of the Always Best Connected cases, but it also allows the network operator to manage and enhance connectivity on a multi-access environment. The interface between ANDSF and the UE is specified as a XML form of information [1]. This way the operator can configure dynamic behavior by checking various conditions (e.g. subscriber category, access point names, access restrictions, etc.) and, accordingly, providing parameterized action (e.g. time-based) to reorder and to indicate its prioritized access network hand-over policies to the UE.

B. Handover Types

There are many types of mobility cases where the point of attachment can change in an IP network. This is why also handovers have been categorized based on the type of the handover. The "Mobility Related Terminology" (RFC 3753) gives the following definitions for handover [9]. There is a *horizontal handover*: when a mobile node moves between access points which use the same technology. *A vertical handover* take place when a mobile node changes the point-of-attachment technology used, for example in research applications, from WLAN to UMTS. In addition to these definitions, there is one more mobility type. From point of view of IP network it is not a handover, it is just a normal connectivity-related action. This might be called *between-session-mobility*; first the equipment with the required connectivity is used, in some location; then all connections are closed or at least not used while moving to another location; there, the user starts using the connectivity again. A good example of this is a laptop/netbook/tablet user, with scheduled meetings and with all the necessary connections for the device: he/she closes the lid of the device and stops all connections before moving back to a desk or to another meeting room where the needed connections are started again. During the switch, the user is not actively expecting connectivity; it might or might not work. Nevertheless, the actual communication will take place later, once the user is ready to start communicating. This is not directly comparable to smartphone usage although there are similarities when excluding the real-time communication. The usage of smartphone will mostly take place when stationary, as in web browsing, video consuming and messaging.

III. ENERGY EFFICIENT ALWAYS-BEST-CONNECTED USER EQUIPMENT

In this research the network selections are designed to be energy efficient but still providing the most suitable connection so that the user experience is not compromised. The network environment in this research is a combination of existing networks such as WLAN, GSM and UMTS and prediction of the future in the shape of Evolved Packed Core. The EPC is there because it changes the way how network mobility is managed and what kind of networks can be managed under EPC operator. The main goal of the algorithm design is to achieve most suitable and energy efficient connection for each application with the help of EPC ANDSF information and, if it is not available, find out the most suitable connection otherwise. In the approach used the following basic assumptions are made: 1. The user is in control: if some connectivity is setup, specifically by the user, for some application, then it must be respected. 2. Operator provided information (ANDSF) will be used if the information provided has heterogeneous networks defined. 3. Otherwise the ABC algorithm is applied. The algorithm has either/or choices, that is, some condition is either true or false. This choice has to be made always when an Internet access is requested for a particular application. The main steps (T/F choices) for access point selection in the algorithm are:

1) valid ANDSF information is available?
2) application is part of profile, is the profile active/valid?
3) known protected WLAN connection is available?
4) open WLAN connection is available?
5) use cellular IP connection

Profiles are user-defined groups of applications and access points made to ease configuration. For example, the user can create home and work profiles where the access points are known. Thus, in the user's home profile the connections are through a home WLAN and in the work profile through a company WLAN. During working hours or at home it is reasonable to a have connection through WLAN. For any other application one should just check if there is a protected or an open WLAN available and, if not, then fall back to a cellular IP connection. The algorithm needs to be revisited if the user equipment is moving and the network environment changes or new connection is created. In case of EPC (valid ANDSF information is available) it should not be any problem, as EPC supports seamless vertical handovers. There might be delays in packet routing and possibly packet loss, but connections should still remain. However, at the current Android environment, which is used in implementation and measurements, Proxy Mobile IP is not supported which is the key enabler in seamless handovers. So the case is equal as outside EPC, and in this case, we have to drop the existing connections and generate a new one, based on steps 2 to 5. Thus, there is no real mobility as connections need to be rebuilt. It is up to the specific application to deal with connection loss.

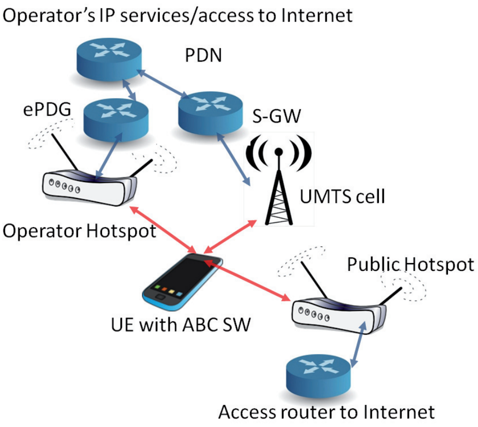


Fig. 1. Test Setup

IV. IMPLEMENTATION AND MEASUREMENTS

In this section the energy efficiency of Always Best Connected application is presented. The ABC application makes the choices of connection network in a heterogeneous network environment. The environment is depicted in Fig. 1 where we have UMTS cells against live network as well as WLAN and simulated EPC+WLAN network coverage. Test cases were selected from real-life examples but simplified so that measurements could be done reliably. Test cases were: 1. Power consumption when attached to UMTS or WLAN network. 2. Handover from UMTS to WLAN and from WLAN to UMTS. 3a. connection creation in UMTS or WLAN and downloading email with attachment. 3b. Connection creation in UMTS or WLAN and HTTP download. The ABC application did choose either WLAN connection or EPC+WLAN connection depending if ANDSF information was available or not. The first test case shows the base power consumption when UE camps in that particular network. Second test case indicates the penalty which is paid if ABC application decides to change existing connection in order to save energy in future communication. Test case 3 is there to show the difference in energy efficiency when actually transferring data.

A. Measurement Setup

The measurement setup is shown in Fig. 2. The user equipment was Android smartphone Samsung Galaxy S II with

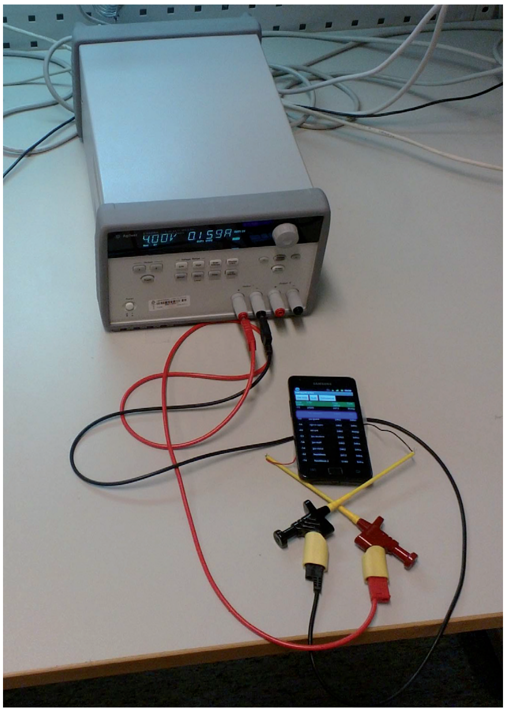


Fig. 2. Measurement Setup

Measurement	Consumption (mA)	Error of the mean
WLAN idle, min. bright.	0.1273	0.0004
WLAN idle, max. bright.	0.2175	0.0007
3G idle, min. bright	0.1265	0.0003
3G idle max. bright	0.2122	0.0004
No mob. Data, Min. bright	0.1261	0.0006

TABLE I
STANDBY CURRENT CONSUMPTION

CyanogenMod firmare (version 7.1). During the measurements the UE had maximun screen brightness. The power supply was Agilent E3648A. During the measurements voltage level was set to 4.0 V (max error 0.05 percent). The power supply was connected to laptop via serial cable. A simple application under Windows XP was created to track power consuption over time. The current consumption measurement frequency was once in every 100 ms.

B. Results

The test case 1. results are shown in Table I, it shows that there is no significant difference over different connections. It is hugely important in which network the UE camps. Second test case results are in Fig. 3. It shows that handover was a consuming operation from energy consumption point of view.

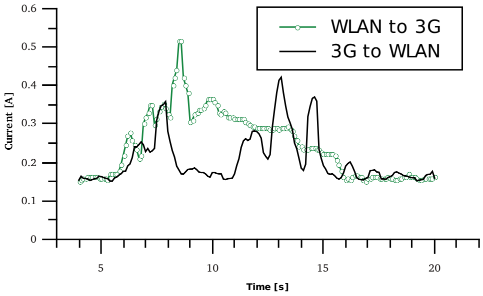


Fig. 3. Handover power consumption

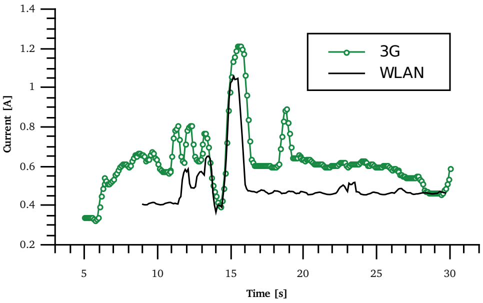


Fig. 4. Email attachment download

However it was not lenghty operation so the overall energy consumption is low. This means that handover is feasible if there are better more energy efficient connections available. On the other hand since the seamless handover was not available which has effect on user experience. For example in case the application in use can't handle connection loss and recreation properly. The third test case was most significant from energy efficiency point of view. Fig. 5 and Fig. 4 are showsing the results from downloads with small and large data amounts. The maximum current consumption is about the same over all communication methods. But the amount of time used in data transfers makes the difference. The WLAN performance was superior compared to UMTS.

V. CONCLUSION AND FUTURE WORK

This paper dealt with analysis of the energy efficiency communication in IP data communication in a heterogeneous network. The energy efficient communication is important for users since all mobile devices have to be charged eventually. It is about how often this is needed. It is also predicted by information technology advisory and telecommunication operators that the amount of mobile data will grow significantly. The paper presented straightforward network selection

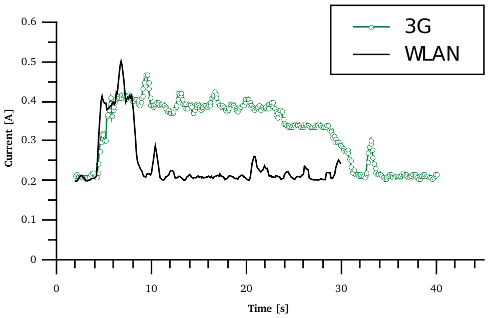


Fig. 5. HTTP download consumption

algorithm. Evolved Packed Core support was added, so that the algorithm can utilize ANDSF information when it is available. Otherwise it used WLAN connections over cellular access that is considered to be last resort if no other connections are available. The network selection was done each time when some application wanted to access network. Existing connections were handovered to this as well due to limitations of existing Android implementation. The implementation of the algorithm was made as the ABC application that was used in near real-life measurements in heterogeneous network environment. The results did show that energy efficiency favor the fastest connection which in this research was WLAN over anything else. Reason is clear, data transfer action is over faster and then the device can reduce the current consumption while slower connections use more time with near equally high current consumption. Handovers did cause high 1 to 2 second current consumption peaks but overall energy consumption is low. Based on energy efficiency, handovers were justified as they enable more efficient communication in the best case. In future, when seamless handovers are possible, it would be interesting to make more detailed calculations, implementations and measurements how to optimize further network change for better energy efficiency. For example, triggers such as signal-to-noise ratio to indicate the start of a network change.

REFERENCES

[1] 3GPP. Access Network Discovery and Selection Function (ANDSF) Management Object (MO); V10.3.0 Release 10. TS 24.312, 3rd Generation Partnership Project (3GPP), July 2011.

[2] 3GPP. Policy and charging control architecture; V10.4.0 Release 10. TS 23.203, 3rd Generation Partnership Project (3GPP), July 2011.

[3] S. Tombaz, A. Vastbergand J. Zander. Energy- and cost-efficient ultra-high-capacity wireless access. *Wireless Communications, IEEE*, pages 18–24, October 2011.

[4] E. Gustafsson and D. Jonsson. Always best connected. *Wireless Communications, IEEE*, page 49, February 2003.

[5] C.Y. Lee, and G. Yu. Parallel-machine scheduling under potential disruption. *Optimization Letters, vol. 2 no 1.*, pages 27–37, January 2008.

[6] S. Lahde, M. Wegner and L. Wolf. Efficient network selection in heterogeneous communication scenarios using arbitration. *IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks, 2010*, pages 1–6, August 2010.

[7] B. Xing, and N. Venkatasubramanian. Multi-constraint dynamic access selection in always best connected networks. *The Second Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services*, pages 56–64, July 2005.

[8] J. Kellokoski and T. Hämäläinen. User-Centric Approach to Always-Best-Connected Networks. *Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2011*, October 2011.

[9] J. Manner and M. Kojo. Mobility Related Terminology. RFC 3753 (Informational), June 2004.

PIV

CHALLENGES OF THE ALWAYS-BEST-CONNECTED ENABLERS FOR USER EQUIPMENT IN EVOLVED PACKET SYSTEM

by

Jari Kellokoski 2012

ICUMT 2012, 4th International Congress on Ultra Modern Telecommunications
and Control Systems and Workshops

Challenges of the Always-Best-Connected Enablers for User Equipment in Evolved Packet System

Jari Kellokoski
Department of Mathematical Information Technology
University of Jyväskylä
FI-40014 Jyväskylä, Finland
Email: jari.k.kellokoski@jyu.fi

***Abstract*—Mobile Internet has rapidly evolved in the past years with an ever increasing number of novel technologies and services with a variety of access technologies. Indeed, today's mobile devices often support multiple communication technologies for accessing Internet services. However, they all do not tap the full potential of these capabilities, as users often have to manually select each network, and only one network is used at a time. The concept of Always Best Connected (ABC) allows a person to connect applications using the devices and access technologies that best suit to his or her needs, thereby combining the features of access technologies to provide an enhanced user experience for future Internet. One of the key features for ABC in a heterogeneous network environment is the ability to make vertical handovers. These handovers are ones where the existing connection is changed from one technology to another. This handover has been considered to be complex and to generate a number of requirements.Over the resent years there have been techniques and standards to overcome the difficulties with vertical handovers. In this research the user equipment requirements of the most significant standards are examined and specification popularity in academic world and commercially is discussed. In addition, the performance of vertical handover with Android-based implementation is examined in real-life heterogeneous network environment. The presented standards are: Voice Call Continuity based on IP Multimedia Subsystem, Unlicensed Mobile Access, Media Independent Handover and The Third Generation Partnership Project Evolved Packet System. The research will show that existing mobile platforms such as Android environment is lacking some of the key requirements for vertical handover and current implementations cannot achieve seamless mobility by means that are currently defined by specifications.**

***Keywords*—Always Best Connected; Evolved Packed Core; Media Independent Handover; Performance; Mobility Management.**

I. INTRODUCTION

Integration of heterogeneous access networks and efficient use of the available communication systems is one of the key challenges for the next generation of mobile communication. Today's mobile devices come with various network interfaces. Over the past years, the numbers of heterogeneous access networks that are available at a specific location have grow dramatically. All of these networks show different communication characteristics, e.g. in terms of throughput, delay, availability and costs, and in combination they offer a high communication performance. In an environment of multiple access technologies, the concept of being always connected becomes Always Best Connected. This refers to being not only always connected, but also being connected in the best possible way [12]. This single point of connection to the IP network is not enough. Connectivity must be maintained while user equipment (UE) is moving. The key enabler to this is mobility management. There are many types of mobility cases where the point of attachment can change in an IP network. This is why also handovers have been categorized based on the type of the handover. The [30] "Mobility Related Terminology" (RFC 3753) gives the following definitions for handover. There is a *horizontal handover*: when a mobile node moves between access points which use the same technology. *A vertical handover* take place when a mobile node changes the point-of-attachment technology used from WLAN (IEEE 802.11)) to UMTS (Universal Mobile Telecommunications System). Over the years many standards have been created to deal with the mobility management. The major techniques that have reached as a standard level are: Generic Access Network (GAN)/Unlicensed Mobile Access (UMA), Voice Call Continuity (VCC) and Evolved Packed System (EPS) by the Third Generation Partnership Project (3GPP) and Media Independent Handover (MIH) by Institute of the Electrical and Electronics Engineers (IEEE) 802.21. The Evolved Packed System is the latest of the standards. It, as the all the previously presented standards, has the potential to become the next common baseline for all IP based services. The aim of this research is twofold. First, to introduce mobility management requirements for the user equipment in existing standards. In particular the focus is on the latest standard the EPS. Second, to make performance measurements in current environment to show if existing user equipment can meet the requirements and what is the performance of vertical handover in Android-based device. The paper is organized as follows. Section II analyses vertical handover enabler specifications. Section III gives an overview of the Evolved Packed System standard and its requirements for UE. Section IV evaluates the performance of Android-based device in the area of vertical handover. Section V finalizes the paper with conclusions and future work.

978-1-4673-2017-7/12/$31.00 © 2012 IEEE

II. ANALYSIS OF VERTICAL HANDOVER ENABLER SPECIFICATIONS

This section takes a look on GAN/UMA, VCC and MIH standards and related work around mobility management. The aim is to highlight the basic functionality and architecture and

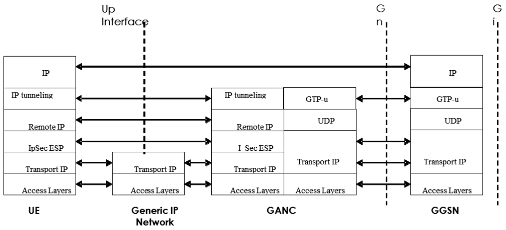


Fig. 1. GAN User Plane Protocols

to discuss how widely and how the specification is being used.

A. Generic Access Network

The Generic Access Network [7] developed by the 3GPP is an evolution from the Unlicensed Mobile Access (UMA). It extends Global System for Mobile Communications (GSM)/General Packet Radio Service (GPRS)/UMTS services to unlicensed spectrum. From the 3GPP core network point of view GAN is just another Radio Access Network (RAN). A UE with multiple air interfaces can access cellular services through GAN and roam between GAN, 2G and 3G. GAN is usually applied through IEEE 802.11 Wireless Local Area Networks (WLAN). The gateway type of approach is applied in 3GPP core network and GAN integration. The gateway is called CAN Controller (GANC), which also performs the functions of GSM Base Station. Fig.1 depicts user plane protocols between GAN entities.

When the UE is powered on, it initially starts in GSM/UMTS mode by executing the normal power-on procedure. When using WLAN, an UE communicates with the GANC through an IEEE 802.11 Access Point (AP). If the UE discovers appropriate APs it switches to GAN mode. The AP itself does not have any extra GAN functionality. It is transparent between UE and GANC. The UE switches to GAN mode by using following steps:

1) Connects to an AP
2) Configures its transport IP address or local IP address. This can be obtained by Dynamic Host Configuration Protocol (DCHP) [23] or by other ways.
3) When IP address is available, the UE performs the discovery procedure to find a suitable GANC
4) Establishes an IPSec [28] tunnel with the Security Gateway (SEGW) which is usually co-located with the GANC
5) Registers with the GANC through the IPSec tunnel
6) If the GANC accepts the registration request, it becomes the serving GANC of the UE. The UE can then switch to GAN mode

The security association of the IPSec tunnel is constructed by using EAP/SIM [25] or EAP/AKA [21] over Internet Key Exchange (IKEv2) [27]. The IPSec tunnel recognizes the UE by its remote IP address. Therefore, the IPSec tunnel does not need to be re-established when the UE moves to another subnet. Only the transport IP address will change. Hence, the IPSec tunnel and any of the upper-layer sessions will not break due to the movement of UE. Signaling messages such as registration, sign-off registration, and keep-alive messages are transmitted over TCP in Generic IP Access Network. The standardized architecture is criticized in the previous research. Several weaknesses are presented; one the most severe of those is [19]: limitations of populating the neighbor list with WLAN so that handover could actually happen to WLAN and the tight coupling to Serving GPRS Support Node that can increase delay for low speed GPRS traffic. This is because high speed WLAN is routed also through it. Another potential source of delay is location independency of GANC [11]. Mobile Switching Center (MSC) recognizes base stations based on unique cell identification. In normal GMS/UMTS network the base station identification is related to its location. However, in GANC case it is just identification without any other relation. This way, UE can connect with GANC using internet broadband connection wherever user is located. This will bring additional traffic to MSC in the form of extra location updates and inter-MSCs handovers. Fine tunings of the GAN are related to improving handover success rate and GAN utilization [16]. In that research there is a proposal for a mathematical model for the pre-registration and preemption behavior in the interworking between 2/3G and GAN. Simulations show that handoff failure probability is reduced and GAN is better utilized. Hard evidence on real GAN/UMA usage is difficult to get. However it is known that the major mobile device manufactures (Blackberry, HTC, Nokia) are providing GAN/UMA capable UEs, and there are operators (Orange - Signal Boost, T-Mobile) providing the service. Based on available information on discussion forums and operator pages it seems that GAN/UMA is used in single locations (homes, small offices, hotspots) without wide area coverage. The user experience is heavily dependent on UE's functionality, some UE's are working fine while others UE's are complained about call drops.

B. Voice Call Continuity

Voice Call Continuity [1] was developed by 3GPP to overcome some of the problems present in GAN architecture and to provide more integral solution to the IP based services. GAN terminals are, after all, considered as an any other Circuit Switched devices. This was not seen as a solid solution for the future services under the umbrella of Fixed Mobile Convergence (FMC). A key characteristic of the VCC architecture is that it is IP Multimedia Subsystem (IMS) [2] centric. The UE measures the signal strengths of its two radio interfaces;it can decide on which domain Circuit Switched or IMS to start a call and when to transfer a call to the other domain. User preferences and operator policies are examined in case both radio signals (cellular and WLAN) if both domains are suitable for a call. The two domains are here only seen as networks connecting the UE to the VCC application (in core network). The Media Gateway (MGW) and the Media Gateway Control Function (MGCF) are IMS elements connecting both of these domains. The VCC application has two main functions [33]: in case of terminating calls it decides the domain towards UE and in case domain switch is needed, VCC application takes care of it. In previous research, there are two reference implementations with performance measurements [29], [22]. In addition a comparison between GAN and VCC is done [20]. Generally these studies show, that VCC is an evolution of GAN due to more tight relation to telephony services (such as supplementary services) and the IMS. In the other hand, technical solutions in the UE side are similar and both can do vertical handovers between cellular and WLAN networks. As with GAN the hard evidence on real VCC usage is difficult to get. Despite this fact, it is known that some major mobile device manufactures (at least Nokia) are providing VCC capable UEs. Known VCC capable operators are rare. Only some Mobile Virtual Network Operator (MVNO) is supporting VCC as a part of their services (OptiMobile). This might be due to needed IMS support. Operators might be still unsure if the IMS will be the standard which is used as baseline for the new services.

C. Media Independent Handover

Media Independent Handover (MIH) is standardized by IEEE in their 802.21 specification [26]. The standard specifies media access-independent mechanisms that optimize handovers between heterogeneous IEEE 802 systems (for example Ethernet or WLAN) and between IEEE 802 and cellular systems. Instead of creating extensions to different access technologies to allow inter-technology handovers, the MIH specifies a common platform to address handovers. In there, each access technology requires only a single extension to ensure interoperability with all other access technologies. The overall network can include a mixture of cells of drastically different sizes, such as those from IEEE 802.15 (Wireless Personal Area Network (WPAN for example Bluetooth), IEEE 802.11 (WLAN), IEEE 802.16 (WiMAX), and 3GPP with overlapping coverage. The handover process can be initiated by measurement reports and triggers supplied by the link layers on the mobile node. The measurement reports can include metrics such as signal quality, synchronization time differences, and transmission error rates. The framework presents MIH reference models for different link-layer technologies. A set of handover-enabling functions within the protocol stacks of the network elements and a new entity created therein called the MIH Function (MIHF).A media independent handover service access point (called the MIH_SAP) and associated primitives are defined to provide MIH users with access to the services of the MIHF. The definition of new link-layer service access points (SAPs) and associated primitives for each link-layer technology. The new primitives help the MIHF collect link information and control link behavior during handovers. The main services that MIHF provides:

- The media independent event service that detects changes in link-layer properties and initiates appropriate events (triggers) from both local and remote interfaces. This is called Media-Independent Event Service (MIES)

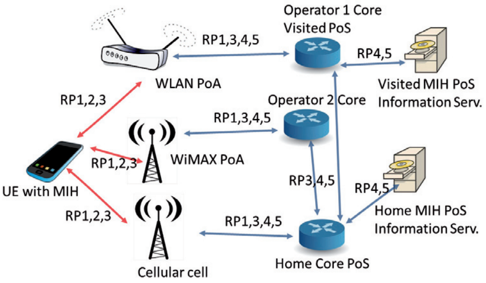


Fig. 2. MIH Communication and Network Model

- The media independent command service provides a set of commands for the MIH users to control link properties that are relevant to handover and switch between links if required. This is called Media-Independent Command Service (MICS)
- The media independent information service provides the information about different networks and their services thus enabling more effective handover decision to be made across heterogeneous networks. This is called Media-Independent Information Services (MIIS)

Fig. 2 shows the MIHF communication and network model. The reference points (RF) 1 and 2 in Fig. 2 can operate on Layer 2 or 3 while RF 3,4 and 5 are operating on Layer 3 or above. The UE is expected to support multiple wireless access technologies. Each Core Operator network (1, 2, or Home) might represent a service provider, corporate intranet provider, or just another part of the visited or home access. In this depicted model, the provisioning provider is operating Cellular, which couples the terminal to the core (labeled Home Core PoS) via RP1. At any given point in time, the subscriber's serving network can be the home subscriber network or a visited network. The network providers offer MIH services in their access networks in order to facilitate heterogeneous handovers into their networks. Each access technology either advertises its MIH capability or responds to MIH service discovery. Each service provider for these access networks allows access to one or more MIH Points of Service (PoS) node(s). The interaction of visited and home subscriber networks could be either for control and management purposes or for data transport purposes. With regard to the MIH Information Service, visited providers can offer access to their information server located in an MIH PoS node. The operator provides the MIIS to mobile nodes so they can obtain pertinent information including, but not limited to, new roaming lists, costs, provider identification information, provider services, priorities, and any other information that would enable the selection and utilization of these services. As a relative new (beginning of 2009) and alternative to 3GPP the MIH specification has collected interest in form of academic research of mobility management. As predicted right after the MIH specification release [13] the challenge has been the lack of conformance statement which would define needed primitives for a particular use case. As a opposite to full scale MIH implementation, the elements of MIH architecture has been presented as a part of other specifications, usually with small modifications. The integration of WiMAX and legacy 3GPP is addressed [18]. The authors introduce a novel handover mechanism enabling seamless mobility without supporting simultaneous transmission on both accesses. Solution is built around the Forward Attachment Function [3], working as target base station optimizing the handover. This was however, identified accountable for packet loss and disconnections. It was improved with the help of Data Forwarding Function, which works as source BS, buffering the incoming packet and forwarding them to the target network. In [14], the authors address the vertical handover support among Next Generation Network (NGN) and features an optimized handover framework based on 802.21. However the mapping of 802.21 MIH features in EPS nodes was briefly discussed, requiring more investigation. The work in [15] presents the placement of 802.21 MIH features in EPS nodes and uses the Access Network Discovery and Selection Function (ANDSF) [6]. Once again, important details and potentials of this integration are superficially addressed. The actual implementations of MIH are almost impossible to find when excluding academic research. Support is not advertised by the device manufactures or any of the operators. It seems, at this point, that the IEEE 802.21 MIH specification is still lacking the major commercial breakthrough, even the research is showing that the potential is there.

III. 3GPP EVOLVED PACKET SYSTEM AND ITS CHALLENGES IN USER EQUIPMENT

This section outlines the Evolved Packed System specified by 3GPP for Release 8, which has the potential to become the next common baseline for all IP based services. Additionally the specification requirements towards UE are discussed. The UE in this research is considered to be Android device, one of the most popular software platforms among the mobile device manufactures.

A. Evolved Packet System

The Evolved Packet System, formerly known as the System Architecture Evolution (SAE), was standardized by 3GPP and consists of a radio part: (Evolved URTAN (E-UTRAN)) and a network part: (Evolved Packet Core (EPC)) [9]. The main objectives of the Evolved Packed System (EPS) are to:

- Provide higher data rates, low latency, high level of security, support of variable bandwidth and Quality of Service (QoS)
- Support a variety of different access systems (existing and those in the future) and ensure mobility and service continuity between these access systems
- Support access system selection based on a combination of operator policies, user preference and access network conditions – as an operator-based ABC
- Provide capabilities for co-existence with legacy systems and migration to the Evolved Packet System

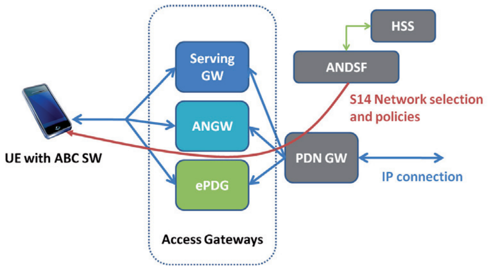


Fig. 3. UE Mobility in the EPS

This section focuses on the core network part (EPC), as it plays the key role in providing the IP connectivity. The section also describes the components of EPC, highlights their major functionalities and outlines their mobility support. The EPC architecture that interconnects 3GPP and non-3GPP access networks consists of several main subcomponents, namely eNodeB, Mobility Management Entity (MME), Serving Gateway (SGw) and Packet Data Network Gateway (PDN-Gw). In addition to these, several other components are present for inter-operating with non-3GPP access. These include WLAN/WiMAX (ePDG, ANGw) for access gateways and the Access Network Discovery and Selection Function (ANDSF). The key control node for an LTE access is the MME, which is responsible for the user tracking, SGw selection, Idle State control, Bearer Control and enforcing user roaming restrictions. The SGw is acting as a mobility anchor for the user plane during the LTE and other 3GPP technologies (intra 3GPP handover), manages the User Equipment (UE) contexts and controls the UE data path. The PDN Gateway provides connectivity from User Equipment (UE) to one or multiple external PDNs simultaneously. The PDN-Gw acts also as a mobility anchor, but between 3GPP and non-3GPP technologies and in addition performs packet filtering and charging. The Home Subscriber Server (HSS) is the central database in the EPC storing user-related information. Static user profiles as well as dynamic information such as session contexts and locations are stored in the HSS. The Policy and Charging Rule Function (PCRF) encompasses the two main functions of flow based charging: charging and QoS controls. The ANDSF is a new EPC element in Release 8 and performs data management and controls functionality to assist the UE on the selection of the optimal access network in a heterogeneous scenario via the S14 interface. The S14 is the Logical interface between the ANDSF and the UE [4]. Authentication, Authorization and Accounting (AAA) in the EPC is performed by the HSS, MME and 3GPP AAA Server. The AAA secures the user subscription, session key management and security tunnel control. The Evolved Packet Data Gateway (ePDG) attaches un-trusted non-3GPP access networks like WLANs to the EPC and performs important security functions such as tunnel authentication and authorization and IPSec encapsulation/decapsulation of packets The Access Gateway (Access GW) interconnects trusted non-3GPP access networks like WiMAX with the EPC. The Application Function (AF) is an abstraction of the service provider, which communicates with the PCRF to enable AAA at the application layer. The AF may be a single third-party-service or a complex operator controlled service delivery platform. The S2c interface provides the user plane with related control and mobility support between the UE and the PDN GW. This reference point is implemented over a trusted and/or untrusted non-3GPP Access and/or 3GPP access. The S5 interface is providing user plane tunneling and tunnel management between SGW and PDN GW. It is used for SGW relocation due to UE mobility and if the SGW needs to connect to a non-collocated PDN GW for the required PDN connectivity. Two variants of this interface are being standardized depending on the protocol used, namely the GTP and the IETF based Proxy Mobile IP solution [24], [35]. Otherwise, at the EPC architecture in comparison to the IMS, the service itself is not required to use a specific signaling protocol as the Session Initiation Protocol (SIP, RFC3261).

B. An Existing UE Mobility Support in Evolved Packed Core

The components for the UE mobility support have the role of interacting with the core network mobility management components and providing a seamless experience for applications running on the UE devices, to allow operations such as network attachment or handover be transparently handled. To perform these operations, the UE would require an application component, as the background application running on the mobile device that will orchestrate the normal network management procedures. Such devices with the required software are not yet commercially available. The interfaces from the core network side are defined, but actual implementations on the UE side are largely missing. To provide value-added functionality, the ANDSF situated in the core network assists the UE with information and operator-pushed policies. The ANDSF component has the purpose of communicating with a UE mobility application running on the mobile endpoint device and exchanging information, which would enhance both of the Always Best Connected cases, but it also, allows the network operator to manage and enhance connectivity on a multi-access environment. The ANDSF behavior is described in 3GPP TS23.402 chapter 4.8 [6], and it uses the S14 interface with the ANDSF Management Objects [4]. Fig. 3 gives an overview of the existing core network elements and their relation to the access management. The Policies defined by the operator are delivered to ANDSF, which allows for the delivery of a dynamic and subscriber specific Inter-System UE mobility policies. The operator can configure dynamic behavior by checking various conditions (e.g. subscriber category, access point names, access restrictions, etc.) and, accordingly, providing parameterized action (e.g. time-based) to reorder and to indicate its prioritized access network hand-over policies to the UE. Further, the parameters of the Inter-System Mobility Policy can be for example validity areas, time intervals, etc. Once the UE receives a set of such policies, it will apply its current parameters to find a matching policy with the highest priority. From this, the UE can extract an operator-ordered list of access networks directly, that indicate the operators suggested solution for the given client's profile, location and the time of day.

C. User Equipment Requirements

The 3GPP TS23.402 Architecture enhancements for non-3GPP accesses [6] and 3GPP TS access to the 3GPP Evolved Packet Core (EPC) via non-3GPP access networks [5] are specifying requirements toward UE. One of the basic definitions is IP Flow Mobility (IFOM) and Multi Access PDN Connectivity (MAPCON) in where the packed data connections are going through different access networks. This is not currently supported by the Android environment. When changing the connection, the existing connection is disconnected before the new one is created. The IP Mobility Management Selection (IPMS) principles state, naturally, that UE and network must support the same mobility management mechanism. The two main choices are network based mobility (NBM) or host based mobility (HBM). In case of HBM the defined protocols are Dual Stack Mobile IPv6 (DSMIPv6) [34] and Mobile IPv4 (MIPv4) [32]. Another critical fact is whether the IP address preservation can be utilized to gain session mobility during vertical handover. Upon initial attachment to 3GPP access, no IMPS is necessary since connectivity to PDN GW see Fig. 3 is always established with network based mobility. Upon initial attachment to a trusted non-3GPP access or handover to it, IMPS is performed before IP address is allocated and provided to UE. When applying NBM the session continuity can take place according to Proxy Mobile IPv6 [24] or by legacy GPRS tunneling protocol [8]. In contrast with HBM the session continuity which can take place in case the network is aware of UE capabilities to support DSMIPv6 or MIPv4. Unfortunately, Android does not support Proxy Mobile IPv6 so at this point the only solution would be rely on GTP on non-3GPP access. However, GTP is proprietary legacy protocol that is not currently supported by WLAN setup boxes. Another challenge is the UE authentication. Trusted/untrusted non-3GPP access network detection has following options: non-3GPP must support 3GPP based authentication then UE can discover the trust relationship during the 3GPP authentication. Or, the UE operates on the basis of pre-configured policy in UE. The user authentication is based on Network Access Identifier [10] where the International Mobile Subscriber Identity (IMSI) is used as identifier. This information can be constructed in Android environment. Authentication procedure itself takes place trough Extensible Authentication Protocol Authentication and Key Agreement EAP-AKA [21] which can be handled in Android environment, as it is the basis for UMTS Authentication. However, the connection from untrusted non-3GPP access to ePDG must be secured and this is done via IPSec tunnel. This is something that is not supported by default in Android platform. As stated in

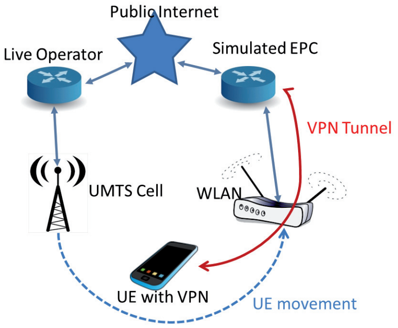


Fig. 4. Test setup

previous section, the ANDSF situated in the core network assists the UE with information and operator-pushed policies. The ANDSF management objects are XML based and the challenge is providing this information to UE. A Specification defines push and pulls types of ways to receive or get ANDSF data. In the pull type the discover can happen over DNS query to predefined address or with help of DHCP query as specified in RFC 6153. The push type message exchange can take place over OMA Device Management [31] via WAP push, this can take place only in 3GPP access networks. In Android environment, DHCP query as specified in RFC 6153 is not supported, and also OMA Device Management is not so clear. Support is not promoted but since the basic idea is the same in multimedia messaging it's likely that the support is there. On the other hand the EPC specification is somewhat loosely written and it might be possible to deliver the ANDSF information other ways too. As a summary, the Android software environment as such (versions 3.2 and 4.0) can't support all the requirements specified by EPC. The biggest challenges are:

- Lack of simultaneous connections
- Lack of IPSec
- Lack of PMIPv6
- Lack DHCP query as specified in RFC 6153

It is clear that these limitations are software related and can change any given time when they get implemented. However, at the present time existing terminals are not off-the-self Evolved Packed Core compatible. Simultaneous connections and IPSec support are the ones that are handy with existing networks, so (my personal expectation is that) they will be implemented first.

IV. PERFORMANCE EVALUATION

In this section, a performance evaluation in the Android 3.0 environment is presented. Fig. 4 depicts the test setup. Performance of vertical handover from legacy 3GPP (UMTS live network in Finland) to simulated EPC network is measured and its suitability to the real-time and non-real-time communication is discussed. The EPC network access is considered as an untrusted and non-3GPP type, in this case WLAN hotspot. Unfortunately, there is no real EPC core environment available, so the network elements are modeled as delays in the communication path. Estimated delay for EPC in this research is 100 ms. There is research using lower values such as 10 ms for legacy 3GPP network [17], this however feels very optimistic. Secure connection is created between UE and EPC via WLAN hotspot. Since there are known limitations of available Android environment, these needs to be handled in a different manner. The lack of PMIPv6, simultaneous connections and IPSec are covered by using a Virtual Private Network (VPN) in Android UE. This way, the applications using the VPN connection get an internal IP address that they use all the time. The IP address changes in the network access are not affecting this internal IP address. There is delay and packed loss caused by network access change. However in this research author considers only the time delay caused by the vertical handover. Its effect on individual application is out of the scope. Same applies with the packed loss it depends on the bitrate of used application. Overall, the usage of VPN can cover the PMIPv6 for the single application. Similar way, VPN hides the network access changes from individual application using VPN even the VPN has to re-create the tunnel after the previous network disconnected and the new network connection is made. The lack of IPSec is also covered by VPN, as IPSec is not supported, the VPN can be created by a Secure Sockets Layer (SSL) RFC 5246 which is widely used in web browsers. This was considered to be the next best thing. Finally, the last missing functionality, the DHCP query as specified in RFC 6153 for ANDSF information availability, is covered by the assumption that either the used Android UE supports OMA DM or XML file made available by other means. In this performance evaluation it is available (in the UE) and it only shows that WLAN hotspot is available for connections. The real-life measurement are shown in Table I, (standard deviation for UE Authentication was 1943 ms). As the table shows, the real VPN tunnel creation and network change was time-consuming. Clearly, the performance was not sufficient for real-time traffic, as gaps such as this are not acceptable (over 200 ms that is generally kept as a limit for real-time communication). The complete analysis of the details what is generating this delay is still ongoing. Nevertheless it would appear to distribute nearly equally between the disconnection and connection of network access and re-recreation of the VPN tunnel. To summarize this solution can't provide suitable performance for the real-time applications during vertical handover.

All values in msec	
Action	3G to WLAN
UE Authentication (VPN)	6893
Estimated EPC delay	100
Total time	6993

TABLE I
VERTICAL HANDOVER AND ESTIMATED EPC DELAY

V. CONCLUSIONS AND FUTURE WORK

This paper dealt with challenges and requirements for User Equipment for enabling the Always Best Connected IP connectivity. The approach was to examine existing specifications namely: 3GPP Generic Access Network, 3GPPVoice Call Continuity, IEEE 802.21 Media Independent Handover and 3GPP Evolved Packed System. Based on specification details, related academic research and information available from user equipment manufactures and user comments, each specification was evaluated. This survey did show that the oldest specification of these the GAN was the most widely used technique for providing a one way of achieving Always Best Connected UE. The VCC was considered to be rarely used in real-life implementations, although some evidence of this was detected. The IEEE 802.21 MIH specification shared much interest in academic side however it was mostly present as a part of other, usually 3GPP, specification. Several partial implementations and simulations have shown that the MIH specification has potential, but the wide adaption of the MIH architecture is non-existent. The Evolved Packed System and Evolved Packed Core specification was considered as the latest attempt to enable always best connectivity to IP network. The specification was detailed examined and UE requirements of it were analyzed against Android 3.0 and 4.0 software platform. It was detected that the examined versions of Android did lack essential features of EPC. Most significant of these lacking features were: simultaneous connections, PMIPv6, IPSec and support for DHCP queries as specified in RFC 6153. Despite these facts, vertical handover performance evaluation was conducted in the Android environment against simulated EPC network. The Android limitations were overcome with the help of VPN tunneling. The results did show successful implementation of mobility management for single application level in EPC network environment. However, the delays were too large (almost 7 seconds from UMTS to WLAN) for any real-time communication. In Future, more detailed analysis of the root causes of vertical handover delays will be conducted. Additionally, the author will follow Android and EPC development closely and continue implementing vertical handover system to Android environment when new features enable this.

REFERENCES

[1] 3GPP. Generic Access Network (GAN); Stage 2. TS 23.206, 3rd Generation Partnership Project (3GPP), December 2007.

[2] 3GPP. IP Multimedia Subsystem (IMS); Stage 2. TS 23.228, 3rd Generation Partnership Project (3GPP), September 2008.

[3] 3GPP. E-UTRAN Improved network controlled mobility between E-UTRAN and 3GPP2/mobile WiMAX radio technologies. TS 36.938, 3rd Generation Partnership Project (3GPP), January 2010.

[4] 3GPP. Access Network Discovery and Selection Function (ANDSF) Management Object (MO); V10.3.0 Release 10. TS 24.312, 3rd Generation Partnership Project (3GPP), July 2011.

[5] 3GPP. Access to the 3GPP Evolved Packet Core (EPC) via non-3GPP access networks, Stage 3. TS 24.302, 3rd Generation Partnership Project (3GPP), December 2011.

[6] 3GPP. Architecture enhancements for non-3GPP accesses; V10.4.0. TS 23.402, 3rd Generation Partnership Project (3GPP), July 2011.

[7] 3GPP. Generic Access Network (GAN); Stage 2. TS 43.318, 3rd Generation Partnership Project (3GPP), April 2011.

[8] 3GPP. GPRS Tunnelling Protocol (GTP) across the Gn and Gp interface. TS 29.060, 3rd Generation Partnership Project (3GPP), December 2011.

[9] 3GPP. Policy and charging control architecture; V10.4.0 Release 10. TS 23.203, 3rd Generation Partnership Project (3GPP), July 2011.

[10] B. Aboba, M. Beadles, J. Arkko, and P. Eronen. The Network Access Identifier. RFC 4282 (Proposed Standard), December 2005.

[11] L. Yang, L. Wensheng and D. Chunjian. Architecture supporting multiple mscs in uma/gan networks. *Third International Symposium on Intelligent Information Technology Application*, pages 102–105, November 2009.

[12] E. Gustafsson and D. Jonsson. Always best connected. *Wireless Communications, IEEE*, page 49, February 2003.

[13] K. Taniuchi, and et.al. Ieee 802.21: Media independent handover: Features, applicability, and realization. *Communications Magazine, IEEE*, pages 112–120, January 2009.

[14] L. Sarakis, G. Kormentzas, and F.M. Guirao. Seamless service provision for multi heterogeneous access. *Wireless Communications, IEEE*, pages 32–40, 2009.

[15] L. Sarakis, G. Kormentzas, and F.M. Guirao. Improvements to inter system handover in the epc environment. *New Technologies, Mobility and Security (NTMS)*, pages 1–5, February 2011.

[16] K-H. Chen, and J-C. Chen. Handoff failure analysis of adaptive keep-alive interval (aki) in 3gpp generic access network (gan). *Wireless Communications, IEEE*, pages 4226–4237, October 2011.

[17] E.S. Boysen, and J. Flathagen. Using sip for seamless handover in heterogeneous networks. *Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)*, pages 1–8, October 2011.

[18] P. Taaghol, A. Salkintzis, and J. Iyer. Seamless integration of mobile wimax in 3gpp networks. *Communications Magazine, IEEE*, pages 74–85, 2008.

[19] R. Yaqub, I. Ul Haq and K.M. Yahya. Architecture supporting network discovery in future heterogeneous networks. *Multitopic Conference INMIC 2008, IEEE*, pages 313–317, December 2008.

[20] S.V. Kale, and T. Schwengler. Comparing unlicensed mobile access (uma) and voice call continuity (vcc) architectures. *Consumer Communications and Networking Conference, IEEE*, pages 1–2, January 2009.

[21] J. Arkko and H. Haverinen. Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA). RFC 4187 (Informational), January 2006. Updated by RFC 5448.

[22] M. Schmidt, B. Lamparterand S. Schmid. Voice call continuity - a critical step towards all-ip based next generation networks. *Global Telecommunications Conference, GLOBECOM 2008*, pages 1–5, November 2008.

[23] R. Droms. Dynamic Host Configuration Protocol. RFC 2131 (Draft Standard), March 1997. Updated by RFCs 3396, 4361, 5494.

[24] S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury, and B. Patil. Proxy Mobile IPv6. RFC 5213 (Proposed Standard), August 2008.

[25] H. Haverinen and J. Salowey. Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM). RFC 4186 (Informational), January 2006.

[26] IEEE. Media Independent Handover Services. Standard 802.21, The Institute of Electrical and Electronics Engineers (IEEE), November 2008.

[27] C. Kaufman. Internet Key Exchange (IKEv2) Protocol. RFC 4306 (Proposed Standard), December 2005. Obsoleted by RFC 5996, updated by RFC 5282.

[28] S. Kent and K. Seo. Security Architecture for the Internet Protocol. RFC 4301 (Proposed Standard), December 2005. Updated by RFC 6040.

[29] R. Keller, M. Vorwerkand C. Barschel. Voice call continuity - a novel mobility scheme for voice on call control level. *Vehicular Technology Conference, VTC-2006*, pages 1–5, September 2006.

[30] J. Manner and M. Kojo. Mobility Related Terminology. RFC 3753 (Informational), June 2004.

[31] OMA. Enabler Release Definition for OMA Device Management. ERELD 1.2, Open Mobile Alliance, July 2008.

[32] C. Perkins. IP Mobility Support for IPv4, Revised. RFC 5944 (Proposed Standard), November 2010.

[33] M. Poikoselkä and G. Mayer. *The IMS IP Multimedia Concepts and Services*. Wiley, Chichester, UK, 2009.

[34] H. Soliman. Mobile IPv6 Support for Dual Stack Hosts and Routers. RFC 5555 (Proposed Standard), June 2009.

[35] R. Wakikawa and S. Gundavelli. IPv4 Support for Proxy Mobile IPv6. RFC 5844 (Proposed Standard), May 2010.

PV

CONTEXT AND LOCATION AWARE ALWAYS-BEST-CONNECTED CONCEPT FOR HETEROGENEOUS NETWORK

by

Jari Kellokoski, Joonas Koskinen and Timo Hämäläinen 2012

Wireless Days 2012

Context and Location Aware Always-Best-Connected Concept for Heterogeneous Network

Jari Kellokoski, Joonas Koskinen and Timo Hämäläinen
Department of Mathematical Information Technology
University of Jyväskylä
FI-40014 Jyväskylä, Finland
Email: {jari.k.kellokoski, joonas.a.koskinen and timo.t.hamalainen} @jyu.fi

***Abstract*—Advances in wireless communication technologies are driving the evolution toward ever faster networks in terms of throughput and latency. User Equipments (UEs) have solid processing power, cameras and displays to produce and consume rich media and services. Their multi-standard interfaces allow them to utilize network-dependent services. However, tapping the full potential of these connected services call for the Always Best Connected (ABC) concept, allowing a person to connect to the services with the help of a personal mobile device and access technologies that are best suited to that person's needs. This paper introduces context and location aware elements in the decision making. The context relates to the services used: some of them, streaming and secure connections for example, can be sensitive to connection characteristics such as IP address change. Location awareness is introduced as a policy to assist in network selection. A reference implementation of the context and location aware ABC concept is introduced. Real-life use cases with real-life services in WiMAX, WLAN and UMTS environments are presented to back up the selected approach.**

Keywords—Always Best Connected; Mobility Management; Context and Location Awareness.

I. INTRODUCTION

Integration of heterogeneous access networks and efficient use of the available communication systems is one of the key challenges for the next generation of mobile communication. Today's mobile devices come with various network interfaces. In an environment of multiple access technologies, the concept of being always connected becomes Always Best Connected. This refers to being not only always connected, but also being connected in the best possible way [5]. This ABC scenario has been considered to be complex and to generate a number of requirements, not only for the technical solutions, but also in terms of business relationships between operators and service providers. The complexity is clearly visible in the previous research collected by S. Fernandes and A. Karmouch [4]. Their comprehensive survey points out that although there is a large amount of research on seamless vertical mobility, most proposed solutions only partially meet the requirement for full mobility. One of the most recent enabler for ABC is the Evolved Packet System (EPS) standardized by the Third Generation Partnership Project (3GPP) [2]. This standard offers a number of possibilities where the user-centric approach can improve the ABC network selection over the selection predefined by the operator. The aim of this research is introduce a context and location awareness decision-making ABC algorithm, and to implement and make real life use casebased measurements of the ABC application. The rest of the paper is organized as follows. Section II gives an overview of context-related services and Section III presents an ABC algorithm that supports context and location in the decision making. This is followed by a proof-of-concept section that evaluates the implementation developed. Section V finalizes the paper with Conclusion and Future Work.

978-1-4673-4404-3/12/$31.00

II. CONTEXT AND ITS RELATIONS TO SERVICES

The classical definition of traffic classes has a connection to 3GPP Universal Mobile Telecommunications System (UMTS) QoS classes. The latter have been defined since the 3GPP release 99 in the Quality of Service Concept and Architecture [3]. There are four different classes: conversational, streaming, interactive and background. The main distinguishing factor between these classes is how delay sensitive the traffic is. The conversational class is targeted for traffic which is very delay sensitive while the background class is the most delay-insensitive traffic class. The conversational class is perhaps the most demanding, as it deals with real time communications between human end-users. The obvious use case is Voice over IP (VoIP) and one of the best known service is Skype. Streaming, on the other hand, has remained as specified in the traffic class. Services based on video streaming, for example YouTube, have gained popularity both in the desktop and mobile world. Streamed videos are usually buffered as far as possible. The most obvious use case for the interactive traffic class would be web-browsing. This usage exhibits the request response pattern and although there are no hard latency values, the user expects fluent response and transmission without errors. The background class, on the other hand, uses cases related to activities taking place in the background beyond the user's immediate attention. Good examples of that are weather widgets, an email-fetch and file uploads or downloads.

III. CONTEXT AND LOCATION IN ABC NETWORK

In previous research, the authors have explored the Always Best Connected challenges and performance in connection with 3GPP Evolved Packed Core (EPC) support [8]. The EPS was standardized by 3GPP and consists of a radio part: (Evolved URTAN) and a network part: EPC [2]. The Access Network Discovery and Selection Function (ANDSF) is a new EPC element in Release 8 and performs data management and controls functionality to assist the UE on the selection of the optimal access network in a heterogeneous scenario via the S14 interface [1].

A. ABC Algorithm without Context and Location Awareness

The ABC algorithm itself is, as far as possible, simple and straightforward. The idea is to have either/or choices, that is, a single condition is either true or false. This choice has to be made always when an Internet access is requested for a particular application or connection lost. The main steps of inquiry for access point selection in the algorithm are: 1. Is valid ANDSF information available? 2. The application is a part of the profile: is the profile active/valid? 3. Is the application real-time? Always inquire about the used access point? 4. Is there any known protected WLAN connection available? 5. Is there an open WLAN connection available? 6. Use cellular IP connection. With the Android implementation of the ABC algorithm the network change time between WLAN networks was slightly less than one second (0.94 second) and between 3G networks roughly 2.5 seconds [8].

B. Algorithm with Context and Location Awareness

Bringing along context and location awareness assumes for more intelligence from the ABC algorithm. When the traffic classes and their real-life counterpart' applications were examined, it became obvious that simple detection and classification of applications would be challenging. For example the proprietary protocol of Skype was not trivial to detect nor was the YouTube streaming based on Flash player. Equally, highly context-sensitive bulk data transfer, such as FTP that can't recover from a connection change, could be identified easily but without any mobility management could not be properly managed. Context sensitiveness was related to actual transfer of data, the idea being that when there is enough traffic there is also context that must be respected. An additional step was added to monitor network traffic. By doing this, the algorithm can keep the existing connection whenever there is a homogeneous network available. Location-based data where utilized in ABC application context in the form of cell ID. This way, the preferred access network could use the visited network history as a clue for discovery of preferred connection. The history data was a cell ID list of five most recently visited cells. The idea was that when the current cell ID is found on the preferred connection list, no network change will occur unless the UE runs out of coverage. A clear advantage of this is that when the UE camps on everyday geographical area then the preferred access network will be able to keep the preferred connection. Equally, when cell ID is not found on the list, then the UE is either travelling or orienting back to everyday geographical area. The main steps of inquiry for access point selection are:

1) Has a valid preferred connection been selected and cell ID found from the history list?
2) Network traffic is above threshold: no changes to access point unless connection lost?
3) Is there a known protected WLAN connection available?
4) Is there a open WLAN connection available?
5) Use cellular IP connection.

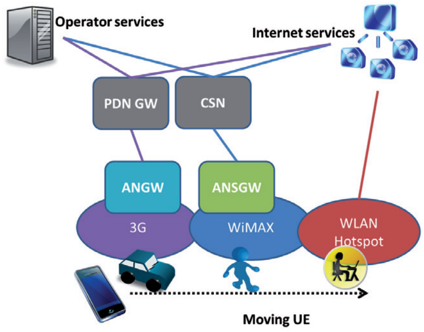


Fig. 1. Proof-of-Concept Test Setup

IV. PROOF-OF-CONCEPT IMPLEMENTATION

The functionality and real-life performance was evaluated through use case scenarios. The classes and their equivalent services were: Conversational - Voice Over IP call by Skype, Streaming - YouTube, Interactive - Facebook and Google Chat as a social media service, Dropbox as a cloud service, Background - File Transfer Protocol (FTP) and Flickr as bulk and background data transfer. Initial performance measurements without any particular ABC algorithm were done earlier [7]. The link quality and load influence the timing of network change, especially in case of real-time traffic [6]. Fig. 1 depicts the test setup where three access networks, each with a different technology, were available: WiMAX, UMTS 3G, and hotspot WLAN. Each of the networks are operated by a different operator. The test run was repeated, with service derived from the traffic class. The ABC application did take care of network change by selecting the best access network. The ABC application was developed on top of Linux.

A. Results without Context and Location Awareness

The route was the same always. Testing started from the 3G coverage area. The UE moved under the WiMAX coverage and finally under the WLAN coverage where the UE camped stationary until the test scenario ended. First the UE was in a vehicle which started to move closer a WiMAX basestation at an approximate of speed of 40 km/h for a distance of roughly 1.2 km until it stopped on a parking area where the UE was removed from the vehicle. At this point, the

WiMAX coverage was excellent and the UE camped there for a one minute. After that, the UE started to move, at a walking speed, inside the cafeteria where the WLAN coverage was available. The walking distance was 300 meters and the starting point was outside the WLAN coverage. Finally, inside the cafeteria the UE was stationary for 2 minutes until scenario ended. The Results: Conversational - Skype; The call was interrupted each time when the underlying network connection changed. However, the call itself was not terminated, instead the connection continued when it was re-established. Streaming - YouTube; streaming was started before the test execution began. During network change, the buffered stream was consumed and the view paused. After an access network change, the streaming was continued by manually selecting a time beyond the previously buffered stream section. Interactive - Google and Facebook chats; were nearly unaffected by the network change. With the Facebook, there had a short period of unavailability during the network change. Still, the messages were buffered during that time and delivered when the user got back online. Background - Flickr and FTP; the data transfer was started before the test execution. In both cases the data transfer was disconnected when access network was changed.

B. *Results with Context and Location Awareness*

The scenarios were run with two different sets, one with empty location information (a) and the other one with known WiMAX location information (b) where WiMAX was set as preferred connection. In the conversational class with the Skype call (case a) there was so much data traffic that the algorithm considered it to be real-time traffic and kept the original connection (3G) until the call was terminated by the user in the cafeteria. After that the connection was changed to WLAN. In case b, the operation was similar otherwise, but in the cafeteria the connection was changed to WiMAX as the cell ID was in the location list and it was considered to be a preferred connection. Functionality was similar in the streaming class with YouTube in both of the sub-cases. In the interactive class, the Facebook and Google chat did not create enough traffic for the algorithm to keep the connection fixed. In sub-case a) the change was first to WiMAX and then to WLAN. However, the chat session was not affected any more than in the original case without context and location awareness. With sub-case b), the UE changed to WiMAX once it became available. It was found from the last visited list, and it camped there until the test ended, as it was the preferred connection. The Dropbox case created so much traffic that the ABC algorithm considered it a real-time application and did not change the access network until synchronization was complete. As with the conversational class in case a), connection in the cafeteria was changed to WLAN and in case b) to WiMAX. The background class had the same functionality as the Skype call and Dropbox synchronization. The ABC application considered continuous traffic as a real time traffic and kept the existing connection. The connection was changed once the data transfer was complete.As the results show, straightforward context and location awareness has clear advantages from the user point-of-view. The services consumed by the user are not interfered by the network changes and the preferred connection works well when the user move around in a geographically restricted area, for example between home and work. Equally, there are challenges with the context and location awareness. At this point the traffic is not classified only the amounts of traffic are monitored. There is no cost optimization, although the preferred connection selection can assist in cost reduction. Location awareness is not effective to highly mobile users. Location adaption is based on visited cells and has no ability to predict future movements.

V. CONCLUSION AND FUTURE WORK

This paper dealt with context and location awareness in heterogeneous network environment. The paper presented a simple and straightforward context-aware network selection method. The algorithm uses network data traffic monitoring to identify ongoing context and avoids tearing down these contexts if network coverage allows it. Location awareness was included in the form of history location data by storing cellIDs of the preferred network. The proposed algorithm was implemented and tested in real-life heterogeneous network environment. The test setup was derived from the four 3GPP traffic classes: conversational, streaming, interactive and background. The tests did show that from the user's point-of-view the experience can be maintained and the most suitable network will get selected once the service allows it. Location data will work as enforcing policy for the preferred connection in a geographically most visited area. Still, it is clear that without mobility management the conversational traffic will remain outside all-IP communication solutions. In future, the aim is to further optimize the location buffer and network data traffic analysis for a fine detail network selection algorithm.Additionally, multibearer connections could be improved to make room for real mobility management that allows make-before-break connectivity.

REFERENCES

[1] 3GPP. Access Network Discovery and Selection Function (ANDSF) Management Object (MO); V10.3.0 Release 10. TS 24.312, 3rd Generation Partnership Project (3GPP), July 2011.

[2] 3GPP. Policy and charging control architecture; V10.4.0 Release 10. TS 23.203, 3rd Generation Partnership Project (3GPP), July 2011.

[3] 3GPP. Quality of Service (QoS) concept and architecture. TS 23.107, 3rd Generation Partnership Project (3GPP), December 2011.

[4] F. Fernandes and A. Karmouch. Vertical mobility management architectures in wireless networks: A comprehensive survey and future directions. *Communications Surveys & Tutorials, IEEE Volume 14, Issue 1*, pages 45–63, February 2012.

[5] E. Gustafsson and D. Jonsson. Always best connected. *Wireless Communications, IEEE*, page 49, February 2003.

[6] E.S. Boysen, and J. Flathagen. Using sip for seamless handover in heterogeneous networks. *Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)*, pages 1–8, October 2011.

[7] J. Kellokoski and T. Hämäläinen. User-Centric Approach to Always-Best-Connected Networks. *Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2011*, October 2011.

[8] J. Kellokoski, J. Koskinen and T. Hämäläinen. Real-life Performance Analysis of Always-Best-Connected Network. *New Technologies, Mobility and Security (NTMS), 2012*, May 2012.

PVI

EFFICIENT HANDOVERS FOR MACHINE-TO-MACHINE COMMUNICATIONS BETWEEN IEEE 802.11 AND 3GPP EVOLVED PACKET CORE NETWORKS

by

Jari Kellokoski, Joonas Koskinen, Riku Nyrhinen and Timo Hämäläinen 2012

iThings 2012, The IEEE International Conference on Internet of Things

Efficient Handovers for Machine-to-Machine Communications Between IEEE 802.11 and 3GPP Evolved Packed Core Networks

Jari Kellokoski, Joonas Koskinen, Riku Nyrhinen and Timo Hämäläinen
Department of Mathematical Information Technology
University of Jyväskylä
FI-40014 Jyväskylä, Finland
Email: {jari.k.kellokoski, joonas.a.koskinen, riku.a.nyrhinen and timo.t.hamalainen} @jyu.fi

***Abstract*—Advances in wireless communication technologies are driving the evolution toward ever faster networks in terms of throughput and latency. At the same time, machine-to-machine (M2M) communications is expected to have considerable potential with millions of devices connected within the following years. M2M communications is one of the key capabilities for implementation of the Internet of Things (IoT). Due to this potential, several standard organizations are now focusing on developing enhancements into their standards to support M2M communications. As there is no consensus for the architecture of a general scenario for M2M communications, the heterogeneous mobile ad hoc network (HetMANET) can generally be considered suitable for the M2M challenges. Hence, this calls for the IP mobility management, allowing a device to connect to services and access technologies that are best suited for that need. To examine how-to improve the HetMANET concept using existing standards such as IEEE 802.11 and 3GPP Evolved Packed Core (EPC) this paper introduces a straightforward and energy efficient algorithm for vertical handovers. A reference implementation of the handover concept in Android based vehicular-to-infrastructure is introduced. This reference implementation examines energy and performance efficiency in heterogeneous network environment. In addition, real-life use cases with real-life services on top of WLAN and cellular network environments are presented to back up the selected approach.**

I. INTRODUCTION

Integration of heterogeneous access networks and efficient use of the available communication systems is one of the key challenges for the next generation of mobile communication. Over the past years, the number of heterogeneous access networks that are available at a specific location grew dramatically. All communication networks show different characteristics, e.g. in terms of throughput, delay, availability and costs, and in combination they offer a high communication performance. In an environment of multiple access technologies, the concept of being always connected becomes Always Best Connected (ABC) [5]. In addition to human-to-human (H2H) communications, an emerging technology is empowering full mechanical automation. Such machine-type-communication devices are known as M2M communications [6]. When considering that the ultimate goal of M2M communications is to construct comprehensive connections among all devices it becomes clear that solutions such as the HetMANET are compelling. The M2M scenario has strong relation, in addition to the network available, to the services being consumed by the devices. In this paper, the M2M service relates to a Vehicle-to-Infrastructure (V2I) communication where vehicle provides informational services to the infrastructure, in this case the mobile device. This device stores the received information and presents it to a human user when needed. This scenario, which is straightforward, has many distinctive M2M features. It provides e.g. surveillance for a vehicle (surveillance, tracking), it has remote maintenance and control capabilities, it provides metering information over various sensors in the vehicle. Finally it interacts with consumer devices in this case a mobile device and by utilizing this it has the retail possibilities in the form of infotainment.

The aim of this research is to introduce efficient handover concept in the Android framework into an M2M vehicular infrastructure, and to implement and carry out real life use case-based measurements of the handover and energy efficiency. The testing is conducted in a heterogeneous network environment. The rest of the paper is organized as follows. Section II introduces the background and related work. Section III gives an overview of the M2M services and Section IV presents the handover concept suitable for V2I communication. This is followed by a proof-of-concept section that evaluates the implementation developed. Section VI finalizes the paper with Conclusion and Future Work.

II. BACKGROUND AND RELATED WORK

In their early work Gustafsson, et al. made the first proper definitions for the Always Best Connected network. Their definition of the best-connected network came with an estimate of complexity [5]. The complexity is clearly visible in the previous research collected by S. Fernandes and A. Karmouch [3]. Their comprehensive survey points out that although there is a large amount of research on seamless vertical mobility, most proposed solutions only partially meet the requirement for full mobility.

Context awareness is discussed by Gvrilescu et al. [14] in IEEE 802.21 Media Independent Handover based solution.

In the approached solution vertical handover prediction algorithms are used to improve resource management decisions.

IP mobility management challenges for Vehicular Communication Networks (VCN) is examined by Cespedes et al [4]. Their work is mostly based on IETF Network Mobility Basic Support NEMO BS (RFC 3963). Although this seems to fit well in the context of terrestrial transport systems, its has not been designed to support the dynamics and special characteristics of VCNs. The network based mobility work continues in IETF Network-Based Mobility Extensions (netext) working group. This resulted specifying Proxy Mobile IPv6 (PMIPv6) (RFC 5213) as the base protocol for network-based localized mobility management (NetLMM). To reduce handover latency and data loss in PMIPv6, Fast Handover for PMIPv6 was standardized (RFC 5949). Kim et al [9] note that PFMIPv6 does not fully utize two of the main characteristics of vehicle networks; geographic restriction (road) has an impact on vehicular mobility; and vehicles have high mobility. They propose enchancement to PFMIPv6 and their simulation results from this enhancement suggest that performance, in terms of handover latency, packet loss and signaling overhead, is better than in PFMIPv6.

Air interface is one of the keys of realization of M2M communications. Lien et al [13] provide an overview of M2M communications in 3GPP, with a particular focus on the air interface. Their elaborations show that the characteristics of M2M communications are different from those of H2H communications. Solutions for H2H communications in the context of Always-Best-Connected and energy efficiency are presented by authors in [10], [11].

III. MACHINE-TO-MACHINE SERVICES

The IEEE 802.16 M2M study report includes several M2M use cases [8]. Below, the relevant use cases considering this research are detailed. Secured Access and Surveillance; M2M applications that help prevent theft of vehicles.Tracking, Tracing, and Recovery; services that rely on location-tracking information. In particular, vehicles are equipped with M2M devices that send status data periodically or on-demand to the M2M server. Remote Maintenance and Control; M2M services inform owners/companies of how their equipment is running.Metering;services meter consumption monitored by sensors and send the remote meter readings to the customer. Consumer Devices; M2M connectivity enables cloud computing where data is stored and processed by a 3rd party and presented by user-friendly interfaces. Retail; infotainment category has considerable market potential where M2M devices present infotainment based on user's preferences.

In this research these use case scenarios are present in a V2I service. The central part is the Android based device that communicates over network via 802.11 and a cellular interface and offers all the interfaces currently available in an Android system. The server and communication counterpart is another Android device but with human interface. Fig. 1 depicts the overall (vehicular) communication scenario. Secured access and surveillance scenario signals the counterpart in real-time with the voice recording and the location data that vehicle tampering has occurred. Communication takes place in real-time regardless of the communication cost. The tracking, tracing and recovery use case has similar characteristics as the previous but the data transfer occurs periodically. Remote maintenance and control as well as metering information is provided periodically. This communication should be error free but transferred in a cheapest possible way. The retail use case has a strong relation to the customer device as it can be the device presenting the infotainment provided by the service provides. The vehicular counterpart of the device information can provide a personalization information to the retailers such as route, petrol and time since last stop information. This kind of communication may have real-time characteristics largely due the nature of infotainment. Thus, the presented scenarios have different kind of requirements for the communication characteristics. The classical definition of the traffic classes has a connection to 3GPP QoS classes. The latter have been defined since the 3GPP release 99 in the Quality of Service Concept and Architecture [2]. There are four different classes:conversational, streaming, interactive, background. The main distinguishing factor between these classes is how delay sensitive the traffic is. The conversational class is targeted for traffic which is very delay sensitive while the background class is the most delay-insensitive traffic class.

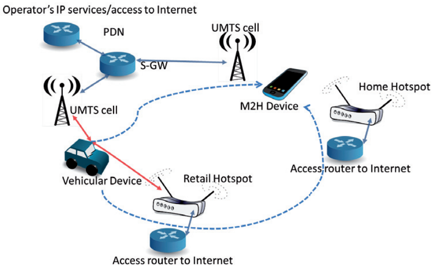


Fig. 1. Vechicular Machine to Human Scenario

IV. EFFICIENT HANDOVERS IN MACHINE-TO-MACHINE IP-NETWORK

The Mobility Related Terminology (RFC 3753) gives the following definitions for the handover. There is a *horizontal handover*: when a mobile node moves between access points which use the same technology. *A vertical handover* takes place when a mobile node changes the point-of-attachment technology used. The Access Network Discovery and Selection Function (ANDSF) is a new EPC element in Release 8 and performs data management and controls functionality to assist the UE on the selection of the optimal access network in a heterogeneous scenario via the S14 interface [1].

A. Handover Concept

The Android framework was modified to allow simultaneous connections over different access technologies. It enabled simultaneous connections for accessing networks in a heterogeneous network environment. The handover complexity is avoided by making direct choices based on a set of predefined preferences. The idea is to have either/or choices, that is, a single condition is either true or false. This choice is made always when an Internet access is requested for a particular application or connection has been lost. The main steps of inquiry for access point selection in the concept are: 1. Is valid ANDSF information available? 2. Is there any known protected WLAN connection available? 3. Is there an open WLAN connection available? 4. Use cellular IP connection.

In case of a valid ANDSF is available the algorithm follows this as it plays the essential role in compatibility with the EPC. The concept considers each connection request as a separate, this way the algorithm is triggered over each time connection is required. If the selection turns out same as the existing connection, the data is multiplexed over the same connection. In the case of a different choice the heterogeneous network support allows the use of simultaneous connections.

V. PROOF-OF-CONCEPT IMPLEMENTATION AND PERFORMANCE

In this section, the Android framework based implementation and performance measurements are presented. The functionality and real-life performance was evaluated through the use case scenarios. These scenarios were derived from the M2M scenarios and four traffic classes defined by 3GPP. The classes and their equivalent services were:

- Conversational - Voice Over IP (VoIP) - Secured Access and Surveillance
- Streaming - YouTube - Consumer Devices, Retail
- Interactive - Facebook and Google as a social media service - Consumer Devices, Retail
- Background - File Transfer Protocol (FTP) as bulk data transfer - Remote Maintenance and Control, Metering

The VoIP call simulates the case where the vehicle is being tampered with and gives an alert to the user by calling to the UE and delivering the real-time location information. The Youtube streaming, Facebook and Google's interactive social media services are considered as a possible infotainment provided by the retailers. FTP can provide background type of data transfer for the Remote maintenance and the Metering service. The testing took place in a heterogeneous network environment were WLAN and cellular networks where available. The link quality and load influence the timing of the network change, especially in case of real-time traffic [7].

A. Android framework modification

Currently the Android framework does not support simultaneous connections. The connectivity service (com.android and server.ConnectivityService) manages connectivity and it was modified for making it possible to have simultaneous connections. The implementation was based on Samsung Galaxy SII but the original software was replaced with Cyanogenmod 9 firmware dated 6.8.2012. The reason for this was that Samsung does offer source code for Galaxy SII. However, there were some hardware related drivers missing. The common network access management process handless the event_state_changed event with message DISCONNECT. When it is triggered happens, the framework tries to connect to some other known network as a failover. If the failover network is found it is reconnected. After the reconnect event, the previous connection if terminated by flushing the Domain Name System (DNS) and the routing information, and then tearing down the existing connections. While connected to the failover network the corresponding interface is powered up and a new entity of with empty DNS and routing information is created. Precondition is that both networks (WLAN and 3G) are known and previously used, thus DNS information is available in both of the cases. Therefore, when the DISCONNECT event is received the flush of DNS data is prevented, the otheraccess network is set immediately as an active network and the state is changed to CONNECTED.

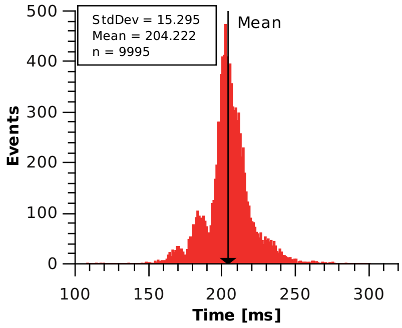


Fig. 2. Handover Performance

B. Performance, Functionality and Energy Efficiency

The network change times between a public cellular network and an infrastructure WLAN are presented in Fig. 2. The results show that the handover times are around 204 ms.During the measurements,the WLAN network was not used by other users. This is significantly better than the around one second without any modifications [12]. The handover measurements started from the DISCONNECT event the handover time itself was unaffected by the previous network. The handover time is within limits of suitability to real-time communication. The times around 200 ms are generally regarded as a limit for the real-time communication. On the other hand, as the handover concept did not offer any solution for mobility management, its up to the service to deal with the connection change. As a result of simultaneous connections the tradeoff is energy efficiency. The idle state, without any communication, the difference in energy consumption is presented in Fig. 3. It shows that although the base consumption can be near the same level as with a single connection, the mandatory keep-alive signalling will resulting higher energy consumption. The

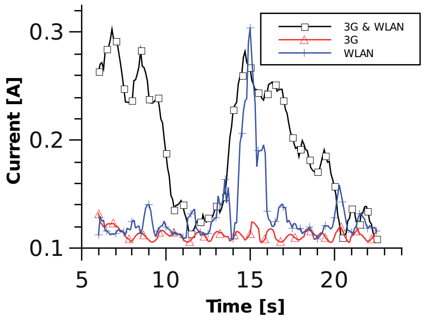


Fig. 3. Energy Efficiency Tradeoff in Idle

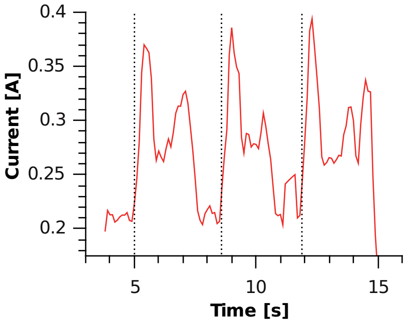


Fig. 4. Handover Power Consumption

handover energy consumption is presented in Fig. 4. In the Figure there are three handovers done from cellular network to WLAN. It shows that the power consumption is momentary high during the network and interface changes but it only takes about 2.5 seconds before the consumption returns to the previous level. In the conversational class the VoIP call was interrupted each time the underlying network connection changed. However, the call itself was not terminated, instead the call continued once the connection was re-established. The user was notified about the connection error. In the streaming class during the network change, the buffered stream was consumed and the video paused. After an access network change, the YouTube streaming was continued by manually selecting a time beyond the previously buffered stream section. As the interactive class scenario was browser-based continuous usage of Facebook and Google chat. In case of the chat the online/offline status of the user and message delivery were monitored. Messages were exchanged every 15 seconds. The Facebook and Google chat were unaffected by the network change from the user's point of view. With the background class the test scenario was bulk data transfer with FTP. The data transfer was disconnected when access to the network was changed.

VI. Conclusion and Future Work

This paper dealt with efficient vertical handovers in heterogeneous network environment at the context of vehicular-to-infrastructure. The paper presented an efficient handover concept in the Android framework. The concept uses simultaneous WLAN and cellular connections to efficiently change the network connection. The proposed handover concept was implemented and tested in real-life heterogeneous network environment. The performance was significantly better than without modifications, around 204 ms. The tradeoff simultaneous connections is the energy efficiency. The impact is seen especially during idle. On the other hand power consumption plays a smaller role in vehicular installation where power is expected to be available. In the future, the aim is to further optimize the handover with further performance improvements. Additionally, to introduce real mobility management protocols such as Proxy Mobile IP for session continuity in a make-before-break communication or multihoming.

References

[1] 3GPP. Access Network Discovery and Selection Function (ANDSF) Management Object (MO); V10.3.0 Release 10. TS 24.312, 3rd Generation Partnership Project (3GPP), July 2011.

[2] 3GPP. Quality of Service (QoS) concept and architecture. TS 23.107, 3rd Generation Partnership Project (3GPP), December 2011.

[3] F. Fernandes and A. Karmouch. Vertical mobility management architectures in wireless networks: A comprehensive survey and future directions. *Communications Surveys & Tutorials, IEEE Volume 14, Issue 1*, pages 45–63, February 2012.

[4] S. Cespedes, X. Shen, and C. Lazo. Ip mobility management for vehicular communication networks: Challenges and solutions. *Communications Magazine, IEEE*, pages 187–194, May 2011.

[5] E. Gustafsson and D. Jonsson. Always best connected. *Wireless Communications, IEEE*, page 49, February 2003.

[6] G. Bi I. Zysman, and H. Menkes. Wireless mobile communications at the start of the 21st century. *Wireless Communications, IEEE*, pages 110–116, January 2001.

[7] E.S. Boysen, and J. Flathagen. Using sip for seamless handover in heterogeneous networks. *Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)*, pages 1–8, October 2011.

[8] H. Cho, and J. Puthenkulam. Machine to Machine (M2M) Communication Study Report. *IEEE 802.16pp-10/0002r6*, May 2010.

[9] M. Kim, S. Lee, and N. Golmie. Enhanced fast handover for proxy mobile ipv6 in vehicular networks. *Wireless Networks*, pages 401–411, May 2012.

[10] J. Kellokoski and T. Hämäläinen. User-Centric Approach to Always-Best-Connected Networks. *Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2011*, October 2011.

[11] J. Kellokoski, J. Koskinen and T. Hämäläinen. Power Consumption Analysis of the Always-Best-Connected User Equipment. *New Technologies, Mobility and Security (NTMS), 2012*, May 2012.

[12] J. Kellokoski, J. Koskinen and T. Hämäläinen. Real-life Performance Analysis of Always-Best-Connected Network. *New Technologies, Mobility and Security (NTMS), 2012*, May 2012.

[13] S-Y. Lien K-C. Chen, and Y. Lin. Toward ubiquitous massive accesses in 3gpp machine-to-machine communications. *Wireless Communications, IEEE*, pages 66–74, April 2011.

[14] M. Gavrilescu, V. Andrei, E.C Popovici, et.al. Context-aware reconfigurable interoperability for vertical handover in wireless communications. *Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology*, pages 1–5, May 2011.

PVII

REAL-LIFE MULTIPATH TCP BASED MAKE-BEFORE-BREAK VERTICAL HANDOVER

by

Jari Kellokoski 2013

ISCC 2013, The Eighteenth IEEE Symposium on Computers and
Communications

Reproduced with kind permission of IEEE.

Real-life Multipath TCP based Make-Before-Break Vertical Handover

Jari Kellokoski
Department of Mathematical Information Technology
University of Jyväskylä
FI-40014 Jyväskylä, Finland
Email: jari.k.kellokoski@jyu.fi

***Abstract*—The emerging of the new technologies results in the situation that the User Equipment (UE) may use multiple interfaces to access the network with multiple technologies, which can be summarized as multihoming in a heterogeneous network. In order to promote the widespread deployment of the UEs, mobile operators should consider the mobility management in the network. The Third Generation Partnership Project (3GPP) standardized the Evolved Packet System (EPS) which among others promotes network based mobility management based on Proxy Mobile IPv6 (PMIPv6) protocol. Multipath TCP provides the ability to simultaneously use multiple paths between peers. This paper examines the use of Multipath TCP as a part of EPS to enable make-before-break vertical handovers. An Android based implementation and performance measurement in a real network environment are presented. The implementation show MPTCP suitability for vertical handovers but certain implementation challenges have to be taken into account. Finally, energy efficiency tradeoff in real-life multipath communication is made visible.**

I. INTRODUCTION

Traffic in mobile networks have continued to grow at an impressive rate worldwide. While voice remains a cornerstone of most operators' service offerings, it is data growth, driven by the uptake of smart devices and apps, which is having the most significant impact on networks globally. Improvements to coverage and speed in urban areas are key to meeting the demand for improved user experience. One way of meeting this demand is the deployment and utilization of heterogeneous networks. In other words, smarter usage of the frequency spectrum is required: that is if more spectrum is available it should be utilized instead of consuming the crowded part of the spectrum. The 3GPP standardized the EPS, where one of the key features is a support access system selection based on a combination of operator policies, user preference and access network conditions [5]. The non-3GPP access networks are also covered by the standard. The EPS is under active development by 3GPP and the Internet Engineering Task Force (IETF) working groups such as Network-Based Mobility Extensions (netext). One of the key working item is multiple interface support for a seamless handover. Multipath TCP (one of the most recent protocol standard of IETF) is a modified version of TCP [22] that implements a multipath transport and achieves these goals by pooling multiple paths within a transport connection, transparently to the application [9]. The aim of the present research is twofold. First, to examine suitability of Multipath TCP (MPTCP) and implementation with it as a enabler for multiple interface support in EPS. Second, to make performance and energy efficiency measurements during vertical handover as a proof-of-concept. The paper is organized as follows. Section II gives overview of background and related work. Section III introduces the MPTCP as a part of EPS. Section IV discusses about the implementation for MPTCP in an Android environment. This is followed by performance and energy efficiency measurements during vertical handover. Section VI finalizes the paper with Conclusion and Future Work.

II. BACKGROUND AND RELATED WORK

The EPS, formerly known as the System Architecture Evolution (SAE), was standardized by 3GPP and consists of a radio part: (Evolved URTAN (E-UTRAN)) and a network part: (Evolved Packet Core (EPC)) [5]. The EPC architecture that interconnects 3GPP and non-3GPP access networks consists of several main subcomponents, namely eNodeB, Mobility Management Entity (MME), Serving Gateway (SGw) and Packet Data Network Gateway (PDN-Gw). The PDN Gateway provides connectivity from User Equipment (UE) to one or multiple external PDNs simultaneously. The PDN-Gw acts also as a mobility anchor, but between 3GPP and non-3GPP technologies and in addition performs packet filtering and charging. The Access Network Discovery and Selection Function (ANDSF) is a new EPC element in Release 8 and performs data management and controls functionality to assist the UE on the selection of the optimal access network in a heterogeneous scenario via the S14 interface [1]. The S14 is the Logical interface between the ANDSF and the UE [1]. Today's mobile devices are not yet at the 3GPP Release level 8 although most if not all of the lacking functionality is software based [15]. This research shows that one of the biggest challenges is lack of simultaneous connections for example in Android environment. Existing Android solutions utilize only one access at the time and when the access is changed the existing connection is teared down. The network performance for off-the-shelf Android devices is around one second [17]. In authors' research on simultaneous connection, the Android environment was modified to allow simultaneous access via IEEE 802.11 and cellular access. The handover performance with these modifications was around 200 ms, that may be considered to be in the limits of real-time communication [18].

Although today's mobile devices are not supporting EPS standard yet, they have multiple radio interfaces such as IEEE 802.11 and cellular access. Meanwhile, TCP is still only single-path. To gain robustness and smooth vertical handovers advantages, transport protocol engineered to utilize multiple paths is needed. MPTCP is extension of TCP protocol to perform this. The first proposal date early as 1995 [13]. However, the existence of middleboxes greatly constrains the design choices. Equally, the challenge is to make MPTCP robust to path failures as well as robust to failures in the presence of middleboxes that attempt to optimize single-path TCP flows [12]. MPTCP operates at the transport layer and aims to be transparent to both higher and lower layers. It is a set of additional features on top of standard TCP. MPTCP is designed to be usable by legacy applications with no changes [10]. Key terms of MPTCP are:

- Path: a sequence of links between a sender and a receiver, defined in this context by a 4-tuple of source and destination address/port pairs
- Subflow: a flow of TCP segments operating over an individual path, which forms part of a larger MPTCP connection. A subflow is started and terminated similarly to a regular TCP connection
- MPTCP Connection: a set of one or more subflows, over which an application can communicate between two hosts. There is a one-to-one mapping between a connection and an application socket
- Token: a locally unique identifier given to a multipath connection by a host. May also be referred to as a ”Connection ID”

The MPTCP suitability for make-before-break handovers is examined, these results show that by nature of multipath has strong potential to act as an enabler for vertical handovers [23]. The impact to energy efficiency in case of simultaneous interface usage plays important role for mobile devices. This has been researched together while developing MPTCP [21], [20]. Their result show the need for further research on the topic. Existing interfaces have been optimized for single-path usage and mix usage between the interfaces is a new scenario. For example interface initiation and long tails consume energy. This is also visible in author work on handover energy efficiency [16], [18].

III. MULTIPATH TCP AS A PART OF EVOLVED PACKED CORE

The 3GPP TS23.402 Architecture enhancements for non-3GPP accesses [3] and 3GPP TS access to the 3GPP Evolved Packet Core (EPC) via non-3GPP access networks [2] are specifying requirements toward UE. One of the basic definitions is IP Flow Mobility (IFOM) and Multi Access PDN Connectivity (MAPCON) in where the packed data connections are going through different access networks. The IP Mobility Management Selection (IPMS) principles state, naturally, that UE and network must support the same mobility management mechanism. The two main choices are network based mobility (NBM) or host based mobility (HBM). In case of HBM the defined protocols are Dual Stack Mobile IPv6 (DSMIPv6) [26] and Mobile IPv4 (MIPv4) (RFC 5944). Upon initial attachment to 3GPP access, no IMPS is necessary since connectivity is always established with network based mobility. Upon initial attachment to a trusted non-3GPP access or handover to it, IMPS is performed before IP address is allocated and provided to UE. When applying NBM the session continuity can take place according to PMIPv6 (RFC 5213) or by legacy GPRS tunneling protocol [4]. However, GTP is proprietary legacy protocol that is not supported in large scale outside 3GPP access. The support for UE having multiple interfaces is described in Internet draft “Proxy Mobile IPv6 Extensions to Support Flow Mobility” [6].

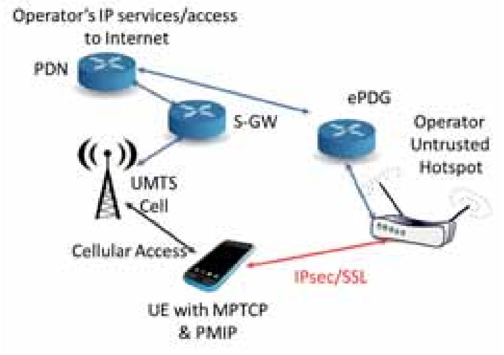


Fig. 1. Test setup, multihomed UE over cellular and WLAN access

The NBM with Proxy Mobile IPv6 is being actively developed by 3GPP and IETF Network-Based Mobility Extension (netext) working group. At the time of writing, there are tree active Internet-Drafts to address multihoming and Proxy Mobile IPv6 challenges. The challenge is clear: network based mobility management by Proxy Mobile IPv6 versus host centric approach by MPTCP. May these protocols work together to complement each other: the PMIPv6 as an network operator way to manage mobility and authentication in core network and MPTCP as an UE to control its interfaces and communication effectively?

“PMIPv6 Multihoming Support Extensions for Flow Mobility” [25] proposes changes to local mobility anchor (LMA) and Mobility Access Gateway (MAG) behavior so that flow mobility can seamlessly be supported in PMIPv6. The flow mobility enables distribution of specific traffic flows on different physical interfaces. Instead of creating an independent mobility session for each interface, the bindings from each simultaneously active interface are kept together so that the flows can be moved among interfaces. The change is done in home network prefix options where new flag is introduced which distinguish firstly or only connected interface from other possible interfaces.

“Seamless Handover for Multiple-Access Mobile Node in PMIPv6” [8] introduces similar idea as above but with the help of two new mobility header messages Streamless Handover Initiate (SHI) and Streamless Handover Acknowledge (SHAck) messages. “Fault Tolerant Support for The Multihomed MN in Proxy Mobile IPv6” [14] has yet another nuance for multihomed UE support. In PMIPv6, Binding Cache Entry (BCE) is created in LMA to binding the MAG with UE. The solution extends the multihoming flag and the Status flag SHOULD be included in the new BCE entry. The multihoming flag is used to identify if the MN is the multihomed. When the multihomed MN joins the network, MAG is used to

Transfers	3GWLAN	WLAN	3G
2	15.7	16.9	0.58
4	15.5	16.9	0.281
8	16.7	16.4	0.269
16	16.4	15.4	0.41

TABLE I. NUMBER OF CONCURRENT TRANSFERS AND SPLIT BETWEEN ACCESSES

communicate with LMA to register the location information for MN and sends the Proxy Binding Update (PBU) message to LMA. LMA creates a BCE entry for each interface of MN. If the received PBU messages from different MAGs with the same UE-ID, the multihoming flag is set as 1; otherwise the value is set as 0. The status flag is used to identify whether the interface that the BCE entry corresponds is available, or whether the state of the interface is in use.

All the reviewed Internet drafts assume operation in a single-domain PMIPv6 network that may not be the case in real-life heterogeneous network environment. However, this consideration is out of scope in this research. Another challenge is authentication. The EPC requires IPsec based security associations between untrusted access nodes which in many cases are WLAN access points. The IPsec has not been designed for nodes with multiple interfaces [19]. The IPsec may configure another IP address trough MOBIKE (RFC 5266) with the ADDITIONAL_IP*_ADDRESS Notify Payloads. These payloads are only provided for the interface used by the IPsec. The main reason is that MOBIKE has been designed for a single interface.

As a summary, multipath communication was not originally engineered to EPC which, at least at the moment, is promoting network base mobility. On the other hand, based on the comprehensive research on multipath communication, it must be host centric mostly due to the vast number of middleboxes around Internet [11], [24]. To overcome this challenge changes to NBM and particularly to PMIPv6 are explored by the IETF working groups. The authors proposal for multipath TCP utilization within EPC environment is to take into use the proposed home network prefix option [25] as well as he ADDITIONAL_IP*_ADDRESS in IPsec. This way, the multihoming may be utilized at least between two interfaces with one flow in each interface. This would bring multihoming to EPC in a straightforward way and would require only minimal changes to existing protocols. The changed protocol would be the PMIPv6 and its home network prefix options.

IV. MULTIPATH TCP AND EVOLVED PACKET CORE IN ANDROID ENVIRONMENT

To examine MPTCP's suitability to vertical handovers in EPC environment the following (Fig. 1) test setup was constructed. It consisted of a simulated Evolved Packet Core WLAN accesspoint and a Cellular access over UTMS in a live network. The WLAN accesspoint was untrusted and the UE required IPsec connection to EPC. During the measurements the WLAN network was not used by other users. For EPC authentication, the aim was to use IPsec (RFC4301) tunneling as defined in the standard. Nevertheless, this was not possible within the Android software environment [15]. Instead, the Secure Sockets Layer (SSL) (RFC 5246) tunnel, which is widely used in web browsers was employed. This was considered to be the next best choice. The authentication resuls was (SSL tunnel only) 109 ms with 47 ms standard deviation the further details of this measurement can be found here [17]. The UE implementation was done in the Android software environment but with modifications to off-the-shelf firmware to support MPTCP. The following changes were made: Cyanogen MOD 9 (Android version 4.0.4) software as a baseline for software development, Kernel - version 3.0.32-CM-ge9cef6c-dirty with MPTCP changes from https://github.com/mptcp-galaxys2. The following scenarios were defined: file download (around 20 MB) through a single and multipath and handovers between WLAN and cellular access with corresponding energy consuption during the tests. The energy consumption was measured during handovers and file downloads. The power supply (Agilent E3648A) was connected to a laptop via serial cable. A simple application under Windows XP was created to track the power consuption over time. The current consumption measurement frequency was once in every 100 ms. During the measurements the voltage level was set to 4.0 V (max error 0.05 percent). The UE was let to settle for 15 s after boot-up, screen off, and measurement was started and no contact with the UE during the measurements.

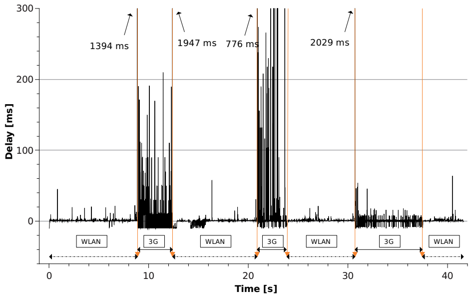


Fig. 2. Multipath TCP vertical handover performance

V. PERFORMANCE AND ENERGY MEASUREMENTS

The download results are presented in Table I. Testing was done using 2,4,8 and 16 parallel threads and every test was run for 20 s. The results show that multihoming may operate on an Android based UE with multiple interfaces. The actual benefit of multihoming is minor when bandwidth difference between interfaces is large: 54 Mbps with WLAN compared to 512 Kbps 3G subscription. As a result of simultaneous connections the tradeoff is energy efficiency. The vertical handover times between a public cellular network and a WLAN are presented in Fig. 2. The results show packet delay between two consecutive packets without transmission interval (10 ms). Handover was done by setting the network device that was currently in use to the backup state. MPTCP started using the other interface automatically. A moving window average filter (using 5 points) was applied to the results during the analysis. The results show that, with the current implementation, the connection change is a time consuming operation although interfaces were up and running during the tests. The link quality and load has its effect on when it would be effective to change the network, especially in the case of the real-time traffic [7].

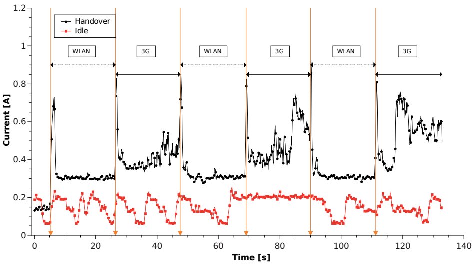


Fig. 3. Energy efficiency during handovers compared to idle

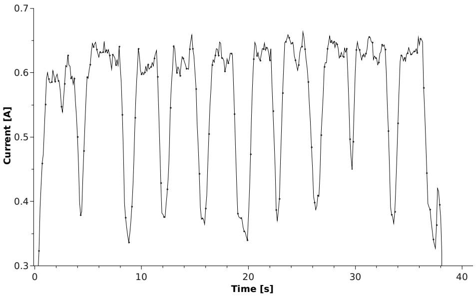


Fig. 4. Multihoming download over WLAN and 3G

This poses challenges for make-before-break handover for real-time traffic. Although packets were not lost and mobility is managed for the application there will be a short break in the communication. It is up to the corresponding application to handle the delay between two consecutive packets. Another result visible from the Fig. 2 is the delays in communication path on the 3G network. There were temporary congestions in the live network which presented as detectable delays between packets. After congestion the delays were as low as seen in third round with 3G. Despite the fact that delays on the 3G path were temporary the handover time remained high in every handover between WLAN and 3G. 4. The energy efficiency was examined during handovers. The results are depicted on Fig. 3. It shows that the interface change is an energy intensive operation. However, the actual data transfer and keeping the other interface as a backup consumes only mildly extra energy when compared to idle consumption. This is clearly seen when comparing energy consumption to a multihomed download over WLAN and 3G as in Fig.

VI. CONCLUSION AND FUTURE WORK

This paper dealt with the handover performance and energy efficiency of MPTCP protocol based communication in IP networks. Additionally the MPTCP suitability as a part of 3GPP Evolved Packed Core network was examined. The ECP promotes on network based mobility management whereas MPTCP is host centric. This creates a challenge for MPTCP utilization in the EPC network. The clear advances in multipath communication have pushed 3GPP and IETF to work to overcome the challenges. The author proposes to take into use the proposed home network prefix option to the PMIPv6 and use the ADDITIONAL_IP*_ADDRESS field in the IPsec. Thus the multihoming may be utilized at least between two interfaces with one flow in each interface. The Android framework was modified and tested against a live and partly simulated EPC network. The results show that the MPTCP may be used for vertical handovers although make-before-break handovers suffer communication break within around 750 to 2200 ms. However, from the application point of view the mobility works and overall energy efficiency is not compromised. Future work will focus on analysis of MPTCP protocol implementation to further improve vertical handover time.

ACKNOWLEDGMENT

I would like to thank Joonas Koskinen and Pasi Kalliolahti for fitting MPTCP to Samsung Galaxy SII and assisting me with the performance and energy efficiency measurements. And to Timo Hämäläinen for his guidance and ideas.

REFERENCES

[1] 3GPP. Access Network Discovery and Selection Function (ANDSF) Management Object (MO); V10.3.0 Release 10. TS 24.312, 3rd Generation Partnership Project (3GPP), July 2011.

[2] 3GPP. Access to the 3GPP Evolved Packet Core (EPC) via non-3GPP access networks, Stage 3. TS 24.302, 3rd Generation Partnership Project (3GPP), December 2011.

[3] 3GPP. Architecture enhancements for non-3GPP accesses; V10.4.0. TS 23.402, 3rd Generation Partnership Project (3GPP), July 2011.

[4] 3GPP. GPRS Tunnelling Protocol (GTP) across the Gn and Gp interface. TS 29.060, 3rd Generation Partnership Project (3GPP), December 2011.

[5] 3GPP. Policy and charging control architecture; V10.8.0 Release 10. TS 23.203, 3rd Generation Partnership Project (3GPP), September 2012.

[6] CJ. Bernardos. Proxy Mobile IPv6 Extensions to Support Flow Mobility. Internet Draft, October 2012.

[7] E.S. Boysen and J. Flathagen. Using sip for seamless handover in heterogeneous networks. *Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)*, pages 1–8, October 2011.

[8] Y. Cui, X. Xu, WD. Wang, XM. Li, YZ. Huo, and W. Luo. Seamless Handover for Multiple-Access Mobile Node in PMIPv6. Internet Draft, October 2012.

[9] A. Ford, C. Raiciu, M. Handley, S. Barre, and J. Iyengar. Architectural Guidelines for Multipath TCP Development. RFC 6182 (Informational), March 2011.

[10] A. Ford, C. Raiciu, M. Handley, and O. Bonaventure. TCP Extensions for Multipath Operation with Multiple Addresses. Internet Draft, October 2012.

[11] M. Handley, V. Paxson, and C Kreibich. Why the internet only just works. *BT Technology Journal, Vol 24*, pages 119–129, July 2006.

[12] M. Honda, Y. Nishida, C. Raiciu, A. Greenhalgh, and M. Handley. Is it still possible to extend tcp? *11th Internet Measurement Conference*, pages 1–14, November 2011.

[13] C. Huitema. Multi-homed TCP. Internet Draft, May 1995.

[14] H. Jiang. Fault Tolerant Support for The Multihomed MN in Proxy Mobile IPv6. Internet Draft, June 2012.

[15] J. Kellokoski. Challenges of the Always-Best-Connected Enablers for User Equipment in Evolved Packet System. *Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2012*, October 2012.

[16] J. Kellokoski, J. Koskinen, and T. Hämäläinen. Power Consumption Analysis of the Always-Best-Connected User Equipment. *New Technologies, Mobility and Security (NTMS), 2012*, May 2012.

[17] J. Kellokoski, J. Koskinen, and T. Hämäläinen. Real-life Performance Analysis of Always-Best-Connected Network. *New Technologies, Mobility and Security (NTMS), 2012*, May 2012.

[18] J. Kellokoski, J. Koskinen, R. Nyrhinen, and T. Hämäläinen. Efficient Handovers for Machine-to-Machine Communications Between IEEE 802.11 and 3GPP Evolved Packed Core Networks. *The IEEE International Conference on Internet of Things*, November 2012.

[19] D. Migault and C. Williams. IPsec Multiple Interfaces Problem Statement. Internet Draft, November 2012.

[20] C. Paasch, G. Detal, F. Duchene, C. Raiciu, and O. Bonaventure. Exploring mobile/wifi handover with multipath tcp. *The 6th ACM International Workshop on Mobility in the Evolving Internet Architecture*, pages 1–6, June 2011.

[21] C. Pluntke, L. Eggert, and N. Kiukkonen. Saving mobile device energy with multipath tcp. *The 6th ACM International Workshop on Mobility in the Evolving Internet Architecture*, pages 1–6, June 2011.

[22] J. Postel. Transmission Control Protocol. RFC 793 (Standard), September 1981. Updated by RFCs 1122, 3168, 6093, 6528.

[23] C. Raiciu, D. Niculescu, M. Bagnulo, and M. Handley. Opportunistic mobility with multipath tcp. *The 6th ACM International Workshop on Mobility in the Evolving Internet Architecture*, pages 1–6, June 2011.

[24] C. Raiciu, C. Paasch, S. Barre, A. Ford, M. Honda, F. Duchene, and M. Handley. How hard can it be? designing and implementing a deployable multipath tcp. *9th USENIX Symposium on Networked Systems Design and Implementation*, pages 1–13, April 2012.

[25] B. Sarikaya. PMIPv6 Multihoming Support Extensions for Flow Mobility. Internet Draft, September 2012.

[26] H. Soliman. Mobile IPv6 Support for Dual Stack Hosts and Routers. RFC 5555 (Proposed Standard), June 2009.