Helsinki University of Technology Laboratory for Theoretical Computer Science
Research Reports 108
Teknillisen korkeakoulun tietojenkäsittelyteorian laboratorion tutkimusraportti 108
Espoo 2007 HUT-TCS-A108

A NETWORK MOBILITY MANAGEMENT ARCHITECTURE FOR A HETEROGENEOUS NETWORK ENVIRONMENT

Henrik Petander

TEKNILLINEN KORKEAKOULU
TEKNISKA HÖGSKOLAN
HELSINKI UNIVERSITY OF TECHNOLOGY
TECHNISCHE UNIVERSITÄT HELSINKI
UNIVERSITE DE TECHNOLOGIE D'HELSINKI

Helsinki University of Technology Laboratory for Theoretical Computer Science
Research Reports 108
Teknillisen korkeakoulun tietojenkäsittelyteorian laboratorion tutkimusraportti 108
Espoo 2007 HUT-TCS-A108

A NETWORK MOBILITY MANAGEMENT ARCHITECTURE FOR A HETEROGENEOUS NETWORK ENVIRONMENT

Henrik Petander

Dissertation for the degree of Doctor of Science in Technology to be presented with due permission of the Department of Computer Science and Engineering, for public examination and debate in Auditorium T3 at Helsinki University of Technology (Espoo, Finland) on the 14th of December, 2007, at 12 o'clock noon.

Helsinki University of Technology
Department of Computer Science and Engineering
Laboratory for Theoretical Computer Science

Teknillinen korkeakoulu
Tietotekniikan osasto
Tietojenkäsittelyteorian laboratorio

Distribution:
Helsinki University of Technology
Laboratory for Theoretical Computer Science
P.O.Box 5400
FI-02015 TKK, FINLAND
Tel. +358 9 451 1
Fax. +358 9 451 3369
E-mail: lab@tcs.tkk.fi
URL: http://www.tcs.tkk.fi/

ISBN 978-951-22-9098-7
ISBN 978-951-22-9099-4 (PDF)
ISSN 1457-7615

Multiprint Oy
Espoo 2007

ABSTRACT: Network mobility management enables mobility of personal area networks and vehicular networks across heterogeneous access networks using a Mobile Router. This dissertation presents a network mobility management architecture for minimizing the impact of handoffs on the communications of nodes in the mobile network. The architecture addresses mobility in legacy networks without infrastructure support, but can also exploit infrastructure support for improved handoff performance. Further, the proposed architecture increases the efficiency of communications of nodes in the mobile network with counter parts in the fixed network through the use of caching and route optimization. The performance and costs of the proposed architecture are evaluated through empirical and numerical analysis. The analysis shows the feasibility of the architecture in the networks of today and in those of the near future.

KEYWORDS: Mobility management, Network mobility, Mobile IP

TIIVISTELMÄ: Verkkojen liikkuuvudenhallinta mahdollistaa henkilökohtaisten ja ajoneuvoihin asennettujen verkkojen liikkuvuuden heterogeenisessä verkkoympäristössä käyttäen liikkuvaa reititintä. Tämä väitöskirja esittää uuden arkkitehtuurin verkkojen liikkuvuudenhallintaan, joka minimoi verkonvaihdon vaikutuksen päätelaitteiden yhteyksiin.

Vanhoissa verkoissa, joiden infrastruktuuri ei tue verkkojen liikkuvuutta, verkonvaihdos täytyy hallita liikkuvassa reitittimessä. Standardoitu verkkojen liikkuvuudenhallintaprotokolla NEMO mahdollistaa tämän käyttäen ankkurisolmua kiinteässä verkossa pakettien toimittamiseen päätelaitteiden kommunikaatiokumppaneilta liikkuvalle reitittimelle. NEMO:ssa verkonvaihdos aiheuttaa käynnissä olevien yhteyksien keskeytymisen yli sekunnin mittaiseksi ajaksi, aiheuttaen merkittävää häiriötä viestintäsovelluksille.

Esitetyssä arkkitehtuurissa verkonvaihdon vaikutus minimoidaan varustamalla liikkuva reititin kahdella radiolla. Käyttäen kahta radiota liikkuva reititin pystyy suorittamaan verkonvaihdon keskeyttämättä päätelaitteiden yhteyksiä, mikäli verkonvaihtoon on riittävästi aikaa. Käytettävissa oleva aika riippuu liikkuvan reitittimen nopeudesta ja radioverkon rakenteesta. Arkkitehtuuri osaa myös hyödyntää infrastruktuurin tukea saumattomaan verkonvaihtoon. Verkkoinfrastruktuurin tuki nopeuttaa verkonvaihdosprosessia, kasvattaen maksimaalista verkonvaihdos tahtia. Tällöin liikkuva reitin voi käyttää lyhyen kantaman radioverkkoja, joiden solun säde on yli 80m, ajonopeuksilla 90m/s asti ilman, että verkonvaihdos keskeyttää päätelaitteiden yhteyksiä.

Lisäksi ehdotettu arkkitehtuuri tehostaa kommunikaatiota käyttäen cache-palvelimia liikkuvassa ja kiinteässä verkossa ja optimoitua reititystä liikkuvien päätelaitteiden ja kiinteässä verkossa olevien kommunikaatiosolmujen välillä. Cache-palvelinarkkitehtuuri hyödyntää vapaita radioresursseja liikkuvan verkon cache-palvelimen välimuistin päivittämiseen. Heterogeenisessä verkkoympäristossä cache-palvelimen päivitys suoritetaan lyhyen kantaman laajakaistaisia radioverkkoja käyttäen. Liikkuvan reitittimen siirtyessä laajakaistaisen radioverkon peitealueen ulkopuolelle päätelaitteille palvellaan sisältöä, kuten www sivuja tai videota cache-palvelimelta, säästäen laajemman kantaman radioverkon rajoitetumpia resursseja.

Arkkitehtuurissa käytetään optimoitua reititystä päätelaitteiden ja niiden kommunikaatiokumppaneiden välillä. Optimoitu reititysmekanismi vähentää liikkuvuudenhallintaan käytettyjen protokollien langattoman verkon resurssien kulutusta. Lisäksi optimoitu reititysmekanismi tehostaa pakettien reititystä käyttäen suorinta reittiä kommunikaatiosolmujen välillä.

Esitetyn arkkitehtuurin suorituskyky arvioidaan empiirisen ja numeerisen analyysin avulla. Analyysi arvioi arkkitehtuurin suorituskykyä ja vertaa sitä aikaisemmin ehdotettuihin ratkaisuihin ja osoittaa arkkitehtuurin soveltuvan nykyisiin ja lähitulevaisuuden langattomiin verkkoihin.

AVAINSANAT: Liikkuvuudenhallinta, Verkkojen liikkuvuus, Mobile IP

Contents

LIST OF FIGURES

LIST OF TABLES

PREFACE

I would like to thank my instructor, professor Hannu H. Kari for his support on writing this thesis through out the writing process, continuing even after he left Helsinki University of Technology. I would also like to thank professor Ilkka Niemelä for taking over the role of the supervisor at the last minute.

Further, I would like to thank my colleagues at National ICT Australia for making it possible for me to concentrate on writing my thesis and for their support on writing the publications used for this thesis. I would especially like to thank professor Aruna Seneviratne and doctor Eranga Perera on their role in helping me write the publications.

Finally, I am grateful for the pre-reviewers, Professor Valeri Naumov and Dr Göran Schultz, whose comments helped me in improving this thesis.

1 INTRODUCTION

With the almost ubiquitous availability of wireless communication networks and the increasing communication capabilities of electronic devices, the prediction that most devices are constantly connected to the Internet is fast becoming a reality. In fact, the penetration of Internet capable mobile phones exceeds in many countries that of personal computers. In spite of these trends, so far the way we communicate and access online data has not changed dramatically and does not meet the demands of users [8]. This is due to a number of factors which limit the ways we can access data and communicate while on the move: the limitations of user interfaces on mobile devices due to small size of the devices, the limitations of processing capabilities, and limitations in communication capabilities [23].

Mobile devices typically have limited battery capacity due to the design objective of minimizing their weight and size. To reduce power consumption, the processing power of mobile devices, such as Personal Digital Assistants (PDAs) and smartphones are often only a fraction of that of even the most modest personal computers. However, with the increased processing power of low power processors, the limits on the types of applications which can be run on low power mobile devices due to processing are fast being eradicated.

The limited size and processing power of the mobile devices reflect on the way users can interact with them. For example, the small screen and lack of a proper keyboard limit the text reading and entering capabilities of PDAs. To address these limitations, new types of user interfaces such as projected keyboards [92] and multimodal interfaces [81] have been proposed.

The limitations of communication capabilities are in part due to the inherent physical characteristics of wireless networks which makes communication over these networks several magnitudes less reliable and slower than communication over wired networks. The restrictions on antenna size, number of antennae, and transmit power limit the range and throughput of wireless communications for a mobile device. Further, the radio communications utilize a shared medium which limits the communication.

In addition to the laws of physics, the protocols and network architectures which are used to enable the communications limit the way mobile users can take advantage of the available wireless networks. Many mobile devices, especially smart phones and PDAs, are already being equipped with multiple radio interfaces enabling them, in theory, to connect to multiple access networks at the same time. This would enable them to use a wireless overlay consisting of multiple access network types of complementing characteristics [100]. However, in spite of these advanced hardware capabilities, the devices cannot currently take full advantage of the heterogeneous access networks effectively due to the lacking support for handoffs, i.e. handing over of communications from one network to another one, on the protocol level. This prevents users, for example, from starting a voice call over a low cost network, such as IEEE 802.11 Wireless Local Area Networks (WLANs) and when leaving the limited coverage of the WLAN network performing a so called vertical handoff, i.e. inter-technology, handoff to a wider coverage, but more expensive Wireless Wide Area Network (WWAN), e.g. an UMTS network.

Handling of mobility inside a single type of network (horizontal handoffs) has been traditionally handled below the network level from the point of view of the TCP/IP protocol stack. This is possible as long as the new and old networks are part of the same IP network. However, handoffs between different IP networks require the mobility management to be handled on the IP layer or above it. This would be the case at least for vertical handoffs and for handoffs between networks operated by different providers.

1.1 Overview of Network Mobility Management

In this subsection, I will first give an overview of the concept of network mobility and Mobile Routers. I will then briefly discuss Network Mobility protocol which is becoming the standard way of handling mobility of networks in IPv6. Alternative mechanisms for handling network mobility and a deeper discussion of Network Mobility protocol are given in Section 3.

Two emerging forms of ubiquitous connectedness are personal area networks (PANs) that interconnect a users devices together and vehicle networks, especially in public transport systems, which will enable passengers to access network services, while on the move. Further, vehicle networks are used to connect vehicle sensors together and to other networked resources, such as central management servers.

In both cases, it is often advantageous to use one device within the *mobile network* as a *Mobile Router* (MR) which connects the devices in the mobile network to the Internet using a wired or more typically wireless connection [85]. Using a Mobile Router enables all the devices in the network to take advantage of the communication capabilities of the Mobile Router. For example a dedicated Mobile Router in a vehicle network could take advantage of external antennas outside the vehicle and be less constrained by power and size than mobile devices, due to being able to draw power from the power system of the vehicle. Additionally, the use of a Mobile Router allows for aggregation of mobility and routing related signaling, thus reducing the protocol overheads of mobility management.

Network Mobility protocol (NEMO) [22] is an Internet Engineering Task Force standardized [49] protocol for managing the mobility of a network using a Mobile Router. In NEMO, handling of the mobility related signalling and management of routing of packets to and from the mobile network are aggregated into the Mobile Router, as shown in Figure 1. The Mobile Router runs the NEMO protocol with a special router, the Home Agent, which acts as a fixed anchor point for maintaining the reachability of the Mobile Router and the devices within the mobile network. NEMO hides the mobility from the *Mobile Network Nodes* (MNNs), i.e. nodes within the mobile network. This enables Mobile Network Nodes without any mobility management capabilities to communicate with nodes outside the mobile network in spite of the Mobile Router moving between different networks.

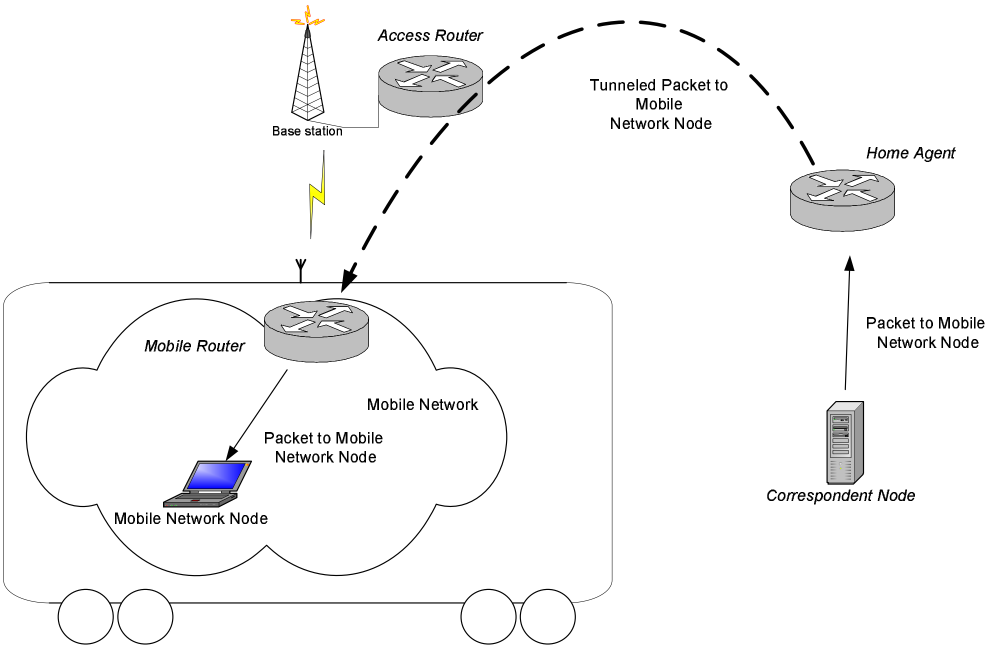

Figure 1: NEMO network mobility architecture.

1.2 Contributions of this Dissertation

I claim the following contributions for this dissertation. The referenced publications (P1-P7) are listed in the next subsection and my personal contribution to them in Subsection 1.4.

- Architecture
  - Mobility management enhancements for network mobility. This dissertation proposes enhancements for mobility management of mobile networks in a heterogeneous network environment. (P1, P2, P3)
  - Mobile Router bootstrapping enhancements. The dissertation additionally proposes how to improve the use and configuration of the mobility management services. (P5)
  - Mobile caching. The architecture proposed in this dissertation introduces the use of proactive caching to increase the efficiency of mobile communications in a heterogeneous wireless environment. (P6)
- Mobility management schemes
  - Network mobility enhancements: This dissertation addresses the overheads of the network mobility management protocol by extending a previously proposed route optimization scheme, OptiNets. (P1)
  - Make-Before-Break handoff scheme: A Make-Before-Break handoff scheme [1] with two network interfaces is proposed for NEMO.

---

[1] In a Make-Before-Break handoff, connectivity is established via the next point of attachment before losing the connecitivity via the current point of attachment.

(P1)
  - Localized mobility management: This dissertation proposes a localized mobility management forwarding scheme which combines Make-Before-Break handoffs with loss recovery using buffering and selective delivery of lost packets from a buffer after completion of the handoff. (P2, P3)
  - Novel handoff timing algorithm for Vertical handoffs: The basic idea of the localized mobility management protocol for Make-Before-Break handoffs is combined with a novel handoff timing algorithm for vertical handoffs based on application or transport protocol context. (P2)

- Protocol design
  - Localized mobility management: This dissertation proposes a new localized mobility management protocol for handling Make-Before-Break handoff capable Mobile Nodes. (P2, P3)
  - Make-Before-Break handoff support: This dissertation proposes a protocol extension to NEMO and Mobile IPv6 for supporting Make-Before-Break handoffs in Mobile IPv6. (P1)
  - Protocol overhead minimization: The dissertation proposes an improved version of the OptiNets protocol for reducing the protocol overheads of mobility capable nodes within a NEMO managed mobile network. (P1)

- Test bed
  - Proof of concept implementation of the architecture: As a part of this dissertation, a proof of concept implementation of the architecture was developed. (P1, P2, P3, P4)
  - Network mobility test bed: Design and building of a configurable test bed used for experiments in the publications P1, P2, P3, P4, P6 and P7. (P4, P3)

- Performance analysis
  - Practical measurements of test bed systems: The effects of asynchronous signalling and interference to its performance are analysed.
  - Analytical approach for performance modeling of the new improvements: The performance and overheads of the proposed architectures and protcols are evaluated using experiments and analysis for the protocols and architectures proposed in P1,P2 and P3. (P1, P2, P3, P7, and Section 5)
  - Identification of the bottlenecks: The bottlenecks in the overall system are identified and addressed in the protocol design. (P1, P2, P3)
  - Comparisons with other solutions: The proposed architectures and protocols are compared with state-of the art (P1, P2, P3, P4, P5, P7, and Section 5)

1.3 List of publications

This subsection first lists the publications and then describes my personal contribution to each of the publications.

Journal papers

P1 Henrik Petander, Eranga Perera, Kun-chan Lan, Aruna Seneviratne, "Measuring and improving performance of network mobility management in IPv6 networks", in *IEEE Journal on Selected Areas in Communications (JSAC)*, vol. 24, number 9, pp. 1671-1681, September 2006.

P2 Henrik Petander, Eranga Perera, Aruna Seneviratne, "Multicasting with selective delivery: A SafetyNet for vertical handoffs", in *Springer Journal on Personal Wireless Communication special issue on seamless handover*, vol. 43, number 3, November 2007.

Conference papers

P3 Henrik Petander, "Optimizing Localized Mobility Management for Make-Before-Break Handoffs", in proceedings of *Newcom-Acorn joint workshop, Vienna, Austria*, 20-22 September 2006

P4 Kun-chan Lan, Eranga Perera, Henrik Petander, Christoph Dwertmann, Lavy Libman, Mahbub Hassan, "MOBNET: The Design and Implementation of a Network Mobility Testbed", in *The 14th IEEE Workshop on Local and Metropolitan Area Networks (LANMAN 2005)* , pp. 1-6, 18-21 September 2005.

P5 Sun Qian, Mu Lei, Henrik Petander, Kun-chan Lan, Mahbub Hassan, "On Securing Dynamic Home Agent Address Discovery of on-board Mobile Router in Mobile IPv6 networks", in proceedings of The 12th International conference on Telecommunications (IEEE ICT 2005), Capetown, South Africa, 03-06 May 2005.

P6 Eranga Perera, Henrik Petander, Aruna Seneviratne, "Bandwidth fuelling for Network Mobility", in proceedings of *The Third International Conference on Wireless and Optical Communication Networks (WOCN 2006)*, Bangalore, India, April 11-13 2006.

P7 Henrik Petander, Eranga Perera, Aruna Seneviratne, Yuri Ismailov, ”An experimental Evaluation of Mobile Node based versus Infrastructure based Handoff Schemes”, in proceedings *of IEEE international symposium on a World of Wireless, Mobile and Multimedia Networks, 2007 (Wowmom 2007)*, pp. 1-4, Helsinki, 18-21 June, 2007

1.4 My own contribution to the publications

For the paper P1, I implemented the protocol optimizations for NEMO handoffs. I came up with the idea and designed the Make-Before-Break handoffs using two network interfaces. I refined the OptiNets route optimization protocol. I designed the experiments and performed the analysis on the results. The contribution of Eranga Perera was to help me in the writing process and provide feedback on the analysis methods. Kun-Chan Lan supervised my initial work on this paper and Aruna Seneviratne co-supervised me for the duration of writing the article. Both provided additional feedback on the writing process. My contribution to the publication was approximately 85%.

For the paper P2, I came up with the idea of the protocol improvements and developed further the initial idea from my supervisor, Aruna Seneviratne, to use the protocol for vertical handoffs. I designed the algorithm for using application or transport context for timing or delaying vertical handoffs. I designed and executed the experiments and analyzed the results. I extended my implementation work from P3 to support the new protocol and the algorithm. The contribution of Eranga Perera for this paper was helping in the writing process. Aruna Seneviratne also supervised the writing of this paper and provided feedback. My contribution to this paper was approximately 70%.

For the paper P3, I came up with the ideas in the paper and developed an implementation of them. I designed the experiments and analyzed the results. My contribution was 100%.

For the paper P4, I finalized the implementation of the NEMO basic support protocol and designed and built the wired and wireless parts of the testbed. I designed and carried out the experiments for which results are shown in the paper. Kun-Chan Lan was the lead author for the paper and integrated my text into the paper. Eranga Perera supervised the implementation of the NEMO protocol and initial design of the testbed. Christoph Dwertmann worked with me to integrate the mobility emulator into the testbed. My contribution to the work described in the paper is approximately 40%.

For the paper P5, I helped Sun Qian and Mu Lei to analyze the vulnerabilities in the DHAAD protocol and to design a mechanism for securing the protocol. Additionally I developed the mechanism into a protocol extension for DHAAD and wrote the paper. Sun Qian and Mu Lei analyzed the correctness of the secure version of the protocol and did most of the design work for securing the protocol. Professor Mahbub Hassan supervised the work of Sun Qian and Mu Lei and together with Kun-Chan Lan provided feedback and generally helped in the writing process. My contribution was approximately 25%.

For the paper P6, I helped Eranga Perera to develop further her idea of using a cache server in a Mobile Router environment. My contribution was to integrate the OptiNets protocol into the caching architecture, help in the experiment design, analysis of the results and writing of the paper. My contribution was approximately 30%.

For the paper P7, I designed the experiments based on the testbed developed for P1 P2 and P4, and analyzed the results. I performed the analytical comparison of the protocols and did most of the writing. Eranga Perera helped me in the writing process and Aruna Seneviratne together with Yuri Ismailov helped in placement of the paper and provided feedback on the paper as it progressed. My contribution was approximately 80%.

1.5 Outline of this dissertation

This dissertation is organized as follows. The research problem this dissertation aims to solve is presented in Section 2.1. In the next section (Section 2.2), the criteria for evaluating solutions for the research problem are presented. Next, the background and related work are discussed in Section 3. This is followed by presentation of solutions to the research problem in Section 4. In Section 5, the solutions are evaluated according to the criteria defined in Section 2.2 and compared with relevant related proposals. The impact and significance of the work are discussed in Section 6. Finally, Section 7 concludes the dissertation.

2 RESEARCH PROBLEM

2.1 Research problem

Mobile Routers moving in a heterogeneous network environment can take advantage of the different, often complementing, characteristics of the various wireless network technologies. Satellite and cellular networks can provide wide coverage outside urban areas. However, the cost of communications for these technologies is often significant. Shorter range, high bandwidth wireless technologies, such as IEEE 802.11 WLAN and WiMax can provide high data rates at a low price but cover only hot spots (WLAN) or urban areas (WiMax). For a Mobile Router to provide cost effective high bandwidth communication services to Mobile Network Nodes, it needs to be able to switch between the different technologies and between different providers networks frequently to provide connectivity via the best available network.

Each time a Mobile Router changes its point of attachment to the network, the handoff results in a period of disconnectivity. The impact of handoff delay with standard IPv6 NEMO stack is shown in Figure 2 for TCP and in Figure 3 for UDP. In the foreign to foreign network handoff in which a Mobile Router moves between two foreign networks, i.e. networks which do not belong to the same IP network as the home network[2], the impact is large for UDP. For TCP, the impact of the handoff is further increased by the conservative resending mechanism which is designed for congestion avoidance instead of dealing with packet loss from wireless errors or a handoff. Furthermore, in a NEMO mobile network setting, the devices in the mobile network would not be aware of the mobility of the Mobile Router and could not determine that the impact on their connections was a result of mobility instead of congestion. This significant disruption of traffic has made it unfeasible to take full advantage of all available networks, since the large impact of a handoff between different IP networks combined with the cost of signaling could mitigate any gains achieved from switching to a faster network for a potentially short time.

Due to the large negative impact of IP layer handoffs, high coverage wire-

---

[2] The nodes in the mobile network have IP addresses which belong topologically to the home network IP range

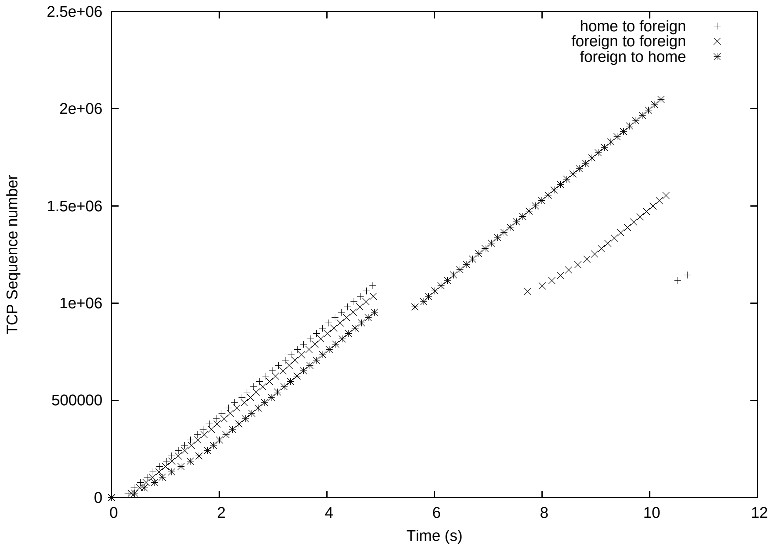

Figure 2: Effect of NEMO handoffs on a 10 second TCP session for a handoff from home to foreign network, foreign to foreign, and foreign to home network.

less technologies which allow minimizing the frequency of handoffs (e.g. satellite) or handle them transparently on the link layer (e.g. cellular systems, such as GPRS or UMTS) have been used for providing on board Internet access [82]. The use of these higher cost wireless technologies has slowed the deployment of on board mobile networks and limited their applications. However, were it feasible to reduce the impact of IP level handoffs between different wireless technologies and providers to a level at which they would not be discernible to application performance, mobile networks could be used for providing services which have so far provided not enough value to the providers, e.g. passenger Internet access in public transportation. In other words, the ability of a Mobile Router to perform *seamless handoffs*, i.e. handoffs which do not have a noticable negative impact on application performance, in a heterogeneous network environment is crucial for enabling more wide-spread use of mobile networks.

In addition to seamless switching between the networks, the Mobile Router needs to minimize the utilization of high cost networks, i.e. networks with less resources available. This can be achieved by correct timing of the vertical handoffs between the different technologies and use of caching. However, it also requires that the protocols used for achieving the seamless mobility do not create unnecessary signaling and data traffic overheads.

In this dissertation, an architecture for enabling seamless handoffs in heterogeneous wireless networks is developed. The architecture consists of a mobility management protocol for supporting seamless Make-Before-Break handoffs with and without support from the access network, caching and optimized routing mechanisms for increasing the efficiency of communications of Mobile Network Nodes and a security architecture to secure the operation and configuration of the protocols in the architecture.

The main foci of this dissertation are architectural and protocol improvements for decreasing the impact of the handoffs of Mobile Routers in a heterogeneous wireless network environment on communications be-

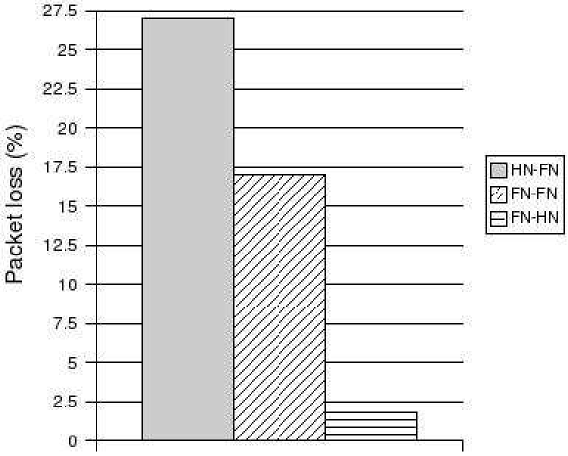

Figure 3: Effect of NEMO handoffs on a 10s UDP session for a handoff from home to foreign network (HN-FN), foreign to foreign (FN-FN), and foreign to home network (FN-HN).

tween mobile network nodes and fixed network counter parties. Additionally, the dissertation aims to minimize the usage of high cost networks to increase the scope of applicability of the proposed solutions.

2.2 Solution Criteria

The architecture designed in Section 4 of this dissertation will be evaluated according to the following criteria in Section 5.

Criterion 1 *Uninterruptibility:* The solutions should minimize interruptions from the mobility of the Mobile Router or the Mobile Nodes to the communications between the Correspondent Nodes and the Mobile Nodes.

Criterion 2 *Sparetime usage:* The solutions should utilize available unused capacity of networks.

Criterion 3 *Performance:* The solutions should have minimal performance impact on communications and should optimize usage of wireless resources.

Criterion 4 *Security:* The architecture should not introduce new vulnerabilities.

Criterion 5 *Deployability:* The solutions should require changes to a minimal number of entities in the network.

3 MOBILITY IN A HETEROGENEOUS WIRELESS NETWORK ENVIRONMENT

In this section, an overview of mobility in a heterogeneous environment is presented and state-of the art research is discussed.

3.1 Wireless network technologies

Wireless network technologies enable mobile communications, and in the case of network mobility, enable the Mobile Router to provide connectivity to the Mobile Network Nodes while moving. In a heterogeneous network environment, there are typically multiple overlapping network technologies which cover any single place.

In nearly all outdoor areas, there is satellite coverage. Services, such as Globalstar, Spaceway and Iridium [36] enable high bandwidth communication (upto 100 Mbps downlink for Spaceway) using Low Earth Orbit (LEO satellites) even in remote areas. However, the high coverage area comes at a cost, for example the total capacity of a Spaceway satellite is 4.4 GBps and the operators need to balance the significant launching costs and high operating costs of the network with the limited bandwidth. Therefore, it is often desirable to use satellite communications only as a last resort, when no other access technologies are available.

Cellular mobile phone technologies, such as 2nd generation cellular GPRS [9] networks, and third generation UMTS [1], [45] and CDMA2000 [60] networks enable relatively high speed communication with data rates up to 14 Mbps for HSDPA UMTS [45] when the mobile station is stationary. However, the bandwidth is shared between all the mobile users within the cell. Due to fading with distance from the base station and resource sharing, the bandwidth available to a user is often significantly lower than the theoretical maximum [56]. Mobility will further decrease the available bandwidth due to the need for more coding to protect the data from the negative effects of Doppler shift. The coverage of 3rd generation cellular networks is often good for at least urban areas and along main roads. However, the available bandwidth depends on the density of deployment of base stations, so rural areas often do not enjoy data rates close to the maximum. As a downside, the cost of using the cellular technologies for data communications is often high.

First generation WiMax, IEEE 802.16-2004 [31] based networks provide a more flexible alternative to traditional wired broadband access technologies with theoretical speeds of up to 70 Mbps for subscribers at fixed locations. However, the IEEE 802.16-2004 based networks do not support changing of base stations. The next generation of WiMax based on the upcoming IEEE 802.16e [48] standard adds mobility support to the WiMax networks by enabling handoffs between the base stations allowing mobility of the user equipment up to vehicular speeds.

Wireless Local Area Networks (WLANs) enable high speed communications at a limited range using unlicensed spectrum which enables low cost wireless connectivity in so called WLAN hotspots. The WLAN networks are currently based on IEEE802.11b [78] and IEEE802.11g [79] standards with some deployments of IEEE802.11a [77] based networks and in the near future on IEEE802.11n [106] standards. The IEEE 802.11 networks provide high speed communications with theoretical maximum data rates varying from 11 Mbps for 802.11b to over 540 Mbps for 802.11n in a limited area with the coverage radius of an access point being from tens of meters indoors to a few hundred meters outdoors. With directional antennae it is possible to achieve communication ranges of a few kilometres.

The low cost of IEEE 802.11 equipment and deployment of hot spots makes their use appealing. However, the technology has its drawbacks. The 802.11b networks show high error rates for high speed mobility based on both emulated radio channels [99], and mathematical analysis of the radio channel [107]. Empirical results by Ott et al [80] suggest that these problems affect mostly downlink UDP traffic, e.g. streaming of real time media, and may not prevent use of IEEE 802.11b hot spots even at high speeds of up to 180 km/h with TCP. Research by Sibekas et al. also indicates that IEEE 802.11a may provide somewhat better performance at higher speeds [96] than IEEE 802.11b, whereas the impact on 802.11n is still unknown. The latency of WLAN handoffs leads to disruption of hundreds of milliseconds for many IEEE 802.11b cards [69]. The disruptions caused by handoffs are amplified by the congestion control algorithms for TCP, as discussed in P1. At higher speeds, the frequent handoffs may make use of multiple overlapping WLAN hotspots infeasible for TCP bulk data traffic unless the duration of the handoff is reduced or its impact mitigated.

Wireless Personal Area Networking (WPAN) technologies such as Bluetooth and IEEE 802.15.3 based Ultra Wide Band (UWB) [3] can be used to interconnect devices at ranges of a few meters with speeds ranging from hundreds of kilobits per second for Bluetooth to hundreds of megabits per second for UWB. Due to the short range they are more applicable to connecting Mobile Network Nodes to the Mobile Router than connecting a potentially fast moving vehicular Mobile Router to the access network. However, if the Mobile Router is a mobile phone connecting other devices in a Personal Area Network (PAN) to the Internet, it may be feasible to use PAN technologies to connect also the mobile network to the Internet.

The different wireless technologies vary in their strengths and weaknesses and for a Mobile Router it is advantegous to be able to roam between the technologies. To do so without disrupting the connectivity and reachability of the Mobile Network Nodes, the Mobile Router needs to run a mobility management protocol.

3.2 Mobility management protocols

Mobility management is used in this dissertation to refer to the task of handling the mobility to ensure reachability and session continuity of the mobile devices. Mobility management has been traditionally handled at the link layer [89], [2], [70], [30]. These approaches have the advantage of hiding the mobility both from the applications and the TCP/IP protocol stack. The approaches have worked well for mobility within a single network technology, e.g. GSM, and within a single operators network. However, the trend towards an increasingly heterogeneous wireless environment requires mobility also between technologies which the link layer approaches as such do not provide. Although there have been efforts to combine the link layer mobility management schemes [103], with an ever increasing number of link technologies and operators, this approach does not scale well due to the ever increasing number of different link layer technologies.

In some cases, it may be possible to equip a Mobile Router with a single radio interface, e.g. a satellite, which provides wide enough coverage.

However, for data intensive applications of mobile networks, e.g. providing passengers in a train with Internet access, the high costs and relatively low speeds of the high coverage technologies make it preferable to use multiple network technologies. Thus, the link layer approach to mobility management can not provide a general solution to network mobility management.

Network layer approaches or to be more accurate mobility management protocols sitting between the network layer and the transport layer enable the use of a single mobility management protocol with multiple link types and multiple applications and transport protocols. Mobile IP for IP version 4 [86], and Mobile IP for IP version 6 [52] introduce a fixed mobility agent, the *Home Agent*, acting as an anchorpoint for Mobile Nodes which communicate with *Corresponding Nodes* via the Home Agent using an IP address from its home network, known as the *Home Address*. Mobile IP uses an IP overlay network to connect the Mobile Node to the home network. This overlay network is realized using tunneling between the current *Care-of Address* (CoA), i.e. an IP address from the network the Mobile Node is attached to, and its Home Agent. The Mobile IP overlay network hides the mobility from applications and from the Correspondent Node, unless Mobile IP route optimization is used. In Mobile IPv6 route optimization, the Mobile Node signals its current Care-of Address to the Correspondent Node to enable the Correspondent Node to send and receive packets directly with the Mobile Node.

Host Identity protocol (HIP) [73], and SHIM layer for IPv6 (SHIM6) [75] are alternative approaches to Mobile IP. Whereas Mobile IP and IP in general use an IP address as both an identifier and as a locator, HIP defines a new identifier, which is derived cryptographically from the identity of the host. In HIP, the Mobile Node and the Correspondent Node communicate directly and reachability of the Mobile Node is achieved using a redirection agent, the rendezvous server, which informs the Correspondent Node of the current location of the Mobile Node. SHIM6 introduces a shim layer between the IP layer and the transport layer to enable multihomed hosts to move connections between multiple IP addresses. This also enables session continuity for Mobile Nodes. SHIM6 architecture does not provide a reachability service, although it could be used together with Dynamic DNS [25] or other ways of looking up the current location of a user.

3.3 Network mobility management

Most work on mobility management has focused on managing the mobility of a single host. However, many of the proposals have been extended to cover Mobile Routers, thus enabling network mobility. NEMO [22] is an extension to Mobile IP which allows the Mobile Node to act as a Mobile Router. In NEMO, the Mobile Router acts as a router between a virtual link to its home network, i.e. the tunnel between the Mobile Router and its Home Agent, and the link of the mobile network. The use of NEMO hides the mobility from the nodes on the mobile network link, since the Mobile Router advertises a network prefix belonging to the home network topology and all the mobile network nodes configure addresses from this prefix, known as the mobile network prefix. Therefore, their addresses and communications are not impacted by Mobile Router changing its point of attachment, i.e. its Care-of Address. Further, the mobility is hidden from Correspondent Nodes.

The nodes in the mobile network, known as *Mobile Network Nodes* which are static,e.g. sensors in a vehicle network, are known as *Local Fixed Nodes* [33]. Mobile Nodes visiting the mobile network are known as *Visiting Mobile Nodes* [33]. NEMO protocol treats both in the same way by hiding the mobility of the Mobile Router from them. If the Visiting Mobile Nodes are using a mobility management protocol there will be two layers of mobility management which may create additional overheads as discussed in more detail in the following subsection.

Novaczki et al. propose an extension to HIP [76] which lets the Mobile Router act as a HIP proxy for the Mobile Network Nodes. This approach relies on the Correspondent Nodes being HIP enabled, but does not require routing of traffic via a fixed anchorpoint, unlike NEMO which uses the Home Agent.

An extension to Session Initiation Protocol (SIP) has been proposed for network mobility management [63]. It uses a SIP Network Mobility Server to manage the mobility of the SIP nodes in a mobile network. The server acts a SIP proxy for the SIP hosts inside the mobile network enabling a NEMO like operation.

3.4 NEMO route optimization approaches

Use of NEMO protocol incurs overheads due to the use of tunneling between the Mobile Router and its Home Agent. Additionally, if the Mobile Router is topologically far from its home network, the routing of packets via the Home Agent leads to increased roundtrip times. If a Mobile Network Node with mobility management capabilities of its own attaches to a mobile network managed with NEMO, there will be two nested levels of mobility management. In case of a Mobile IPv6 Visiting Mobile Node, this would result in two nested tunnels and routing of packets via two Home Agents, i.e. the Home Agent of the Mobile Router and the Home Agent of the Visiting Mobile Node. The overheads can be further amplified if Mobile Networks are nested, i.e. one Mobile Router attaches to a mobile network served by another Mobile Router. This would be the case of a mobile user carrying a PAN connecting to a mobile network inside a bus.

The HIP based Network Mobility approach does not suffer from the routing overhead, since no Home Agent is used. However, the use of IPsec between the Mobile Router and the Correspondent Node will create protocol overheads and the establishment of the HIP security associations and delegation of authority would results in additional overheads. The use of SIP based network mobility [63] does not have per packet overheads nor does it use tunneling via a fixed anchor point . However, it is not directly comparable with the NEMO and HIP based approaches, since it only works for applications which are SIP based.

There exist several proposals for reducing the protocol and routing overheads of NEMO by using different mechanisms to either bypass the Home Agent or switch to one which is closer to the current location of the MR. These *route optimization* proposals are presented in this section and the most relevant ones are compared with the proposed architecture along with the HIP based network mobility scheme in Section 5.

The route optimization proposals can be divided into two broader groups, proposals for nested Mobile Networks and proposals for single-level Mobile Networks. Kang et al. propose use of bi-directional tunneling between the highest level Mobile Router and the Home Agent [55]. Thubert's proposal [83] uses a reverse routing header to record a route through the hierarchy of Mobile Routers. Reverse routing header enables Dynamic Source Routing [53] like routing within a hierarchy of Mobile Routers, by having the Mobile Network Nodes insert an empty routing header into each packet. The Mobile Routers on the path to the Correspondent Node then insert their addresses to the routing header. When the Correspondent Node receives the packet and sends a reply, it reverses the order of the addresses in the routing header to ensure that the packet reaches the Mobile Network Node. The use of reverse routing header requires additional support from the Correspondent Node, when compared with Mobile IPv6 route optimization [52]. These two proposals target a multi level hierarchy of Mobile Routers and thus provide a general solution.

In the unnested case, the route optimization can be achieved by running a protocol between the Mobile Router and a corresponding router [88]. This scheme requires support from the network infrastructure to enable optimal routing. Further, it does not address the overhead from two layers of mobility management in the case of Visiting Mobile Nodes. Jeong et al. propose a mechanism [51] in which the Mobile Router acts as a proxy for the Mobile Network Nodes to enable the Mobile Network Nodes to use host based route optimization, e.g. Mobile IPv6 route optimization.

Wakikawa et al. propose [87] the use of dynamically assignable Home Agents to enable the Mobile Router to switch Home Agent to reduce the routing overhead. This method improves the routing of packets and thus reduces the end-to-end network latency and reduces the load on the network. However, it does not reduce the protocol overhead from tunneling.

The architecture in this dissertation employs a mechanism which shares many characteristics with Jeong et al.'s method. However, there are some key differences in the mechanisms which reflect onto their performance as discussed in detail in Section 5.

3.5 Approaches to improving handoff performance in Network Mobility

Handoff latency is one of the main causes for packet loss and performance degradation in the mobile network context. As discussed in Section 2.1 and in publication P1, the handoff latency with NEMO and a standard IPv6 stack in 802.11 WLAN is on the average 1.75 s. A latency this large has a significant impact on any on-going communications, if the handoff is performed in a *Break-Before-Make* fashion, i.e. the Mobile Router loses connectivity with the previous Access Router before establishing connectivity with the new one. On the other hand, if the Mobile Router can establish connectivity to a new Access Router before losing the connectivity with the previous one, i.e. perform a *Make-Before-Break* handoff, it can avoid packet loss. Further, if in in addition to no packets being lost, the packet interarrival times are not impacted, the handoff will not degrade the on going communications and can be considered *seamless*.

Previous work [91], [104] has proposed the use of hierarchical structure to reduce the address configuration delay through advanced configuration. Such hierarchical schemes separate mobility management into local mobility and wide area mobility. Based on the observation that the majority of handoffs happen locally, a Mobility Routing Point [11] is placed at each local domain. The Mobility Routing Point intercepts all packets on behalf of the Mobile Router in the same local domain. In this case, a Mobile Router's Home Agent is only informed when the Mobile Router moves into a new domain and the Home Agent is unaware of the movement of the Mobile Router within the domain. In other words, local mobility is handled by the Mobility Routing Point while wide area mobility is managed using Mobile IP. Since most handoffs occur locally, such a scheme can avoid potential delay associated with registrations to the Home Agent. Hierarchical Mobile IPv6 [97], [27] is an IETF standardized localized mobility management protocol based on this idea.

These proposals have attempted to reduce the handoff latency by localizing the handoffs within a network domain. A more complete approach is provided by Fast Handovers for Mobile IPv6 (FMIPv6) [61], [62] which mitigates the impact of handoff by using proactive handoffs, localized forwarding, and context transfer between the Access Routers (ARs). Bicasting or multicasting (n-casting) with simultaneous bindings [32] can be used with FMIPv6 to improve the handoff performance. Fast Handovers for Mobile IPv6 can be combined with Hierarchical Mobile IPv6 as proposed by Jung et al. [35] in the F-HMIPv6 proposal, Gwon et al. in their FF-HMIP proposal [44], and by Hsieh et al. in their Synchronized MIP (S-MIP) proposal [46], [47].

There exists an infrastructure based proposal specifically designed for NEMO which takes the approach proposed in publication P1 further and uses two Mobile Routers at opposite ends of a train to create additional overlap between the old and new access network [54]. However, the same effect could be achieved by using two external antennas for the scheme in publication P1, and therefore this scheme is not included in the analysis.

In addition to network layer mechanisms, there have been several proposals to improve the link layer handoff performance for IEEE 802.11 networks, including the SyncScan [90] and the Neighbor Graphs proposals [95] which rely on infrastructure support from the access points to reduce the handoff latency. The MultiScan proposal by Brik et al. [10] utilizes two interfaces to enable Make-Before-Break handoffs.

In some cases, it is not possible to use localized mobility management protocols due to handoffs in legacy networks or switching between different access network types or different operators networks. In these cases, Mobile Node or Mobile Router based approaches can be used to improve the handoff performance.

The discovery of the Access Router on the new link [74] and configuration of a new IPv6 Care-of Address [101] delay the handoff significantly as discussed in publication P1. Daley et al. [19] propose the use of IPv6 multicast to minimize the latency of Duplicate Address Detection which is a part of the address configuration in IPv6. In this dissertation, Optimistic

Duplicate Address Detection (ODAD) [72] is used for reducing the network attachment delay together with Fast Router Advertisements [18], [17]. In addition, IP layer soft handoffs using two network interfaces are utilized for lossless handoffs.

3.6 Network selection and handoff timing algorithms

Several different approaches to vertical handoff timing have been proposed in the literature. Signal strength, speed, and handoff latency estimations are used in [71] to derive the correct time for handoffs. The available network bandwidth can be used to complement the signal strength information [39], [34]. The asymmetric nature of the networks is considered more in [66] by factoring in costs and user preferences. Guo et al propose the use of fuzzy logic and neural networks to optimize the timing to use multiple rules for the handoff decision, including number of users in the candidate networks [43]. Vidales et al. [38] propose the use of concepts from autonomous systems design, including finite-state transducers for improving handoff decisions based on potentially conflicting rules. The handoff timing algorithm proposed in this dissertation (in publication P2) uses packet loss and application state to delay or in the best case completely avoid an upward vertical handoff without degrading application performance.

3.7 Application adaptation and content delivery

In a heterogeneous network environment, handoffs often result in changes to the availability of network resources for an application. Typically in vertical handoffs, the available bandwidth and delay will change dramatically when moving between WLAN and WWAN technologies. Even in horizontal handoffs the available bandwidth may differ markedly due to differences in network loads or the received signal strength.

Mobility management protocols try to minimize the impact of the handoff on applications. However, any changes in the available resources will affect the applications. There exist different ways to handle this, depending on the type of the application.

Real time applications

Real time applications consume a stream of information which is consumed as soon as it arrives with minimal buffering. Often the data is received at a constant rate. To adjust a real time application to changes, in the network bandwidth, different encoding methods may be used for voice and video with varying levels of lossful or lossless compression. Some of the encoding algorithms such as [4] can be changed on the fly at any point in the stream and others can be only changed at certain points in the stream [50]. A receive buffer can be used to deal with variances in the end-to-end delay with the downside of increased delay. For example in Voice over IP protocol the jitter buffering needs to be balanced against with the end-to-end delay to keep conversations interactive.

Non-real time applications

Non-real time applications are typically considered to consist of file downloads. However, this category also includes non-interactive data streaming which is used for applications such as watching or listening pre-recorded movies or music on devices with sufficient storage. The delivered data rate needs to keep up with the consumed data rate and a buffer is used for this. These streaming applications can take advantage of higher bandwidth when it is available and use buffered data to compensate against temporary connectivity via networks with lower bandwidth or even periods of no connectivity.

The buffering can be done in the application or in other parts of the system. For streamed data this is simple as data access is sequential. Caching can be used for non sequential access to different data to improve the efficiency of the use of network resources. This is important for file downloads in applications such as web browsing and file transfers, since all the data belonging to a single file typically needs to be downloaded (or uploaded) before it can be used and therefore buffering cannot be used as such. However, especially in web browsing there are often collections of data which are downloaded sequentially in a predictable sequence.

Caching has been widely used with web browsing in the HTTP protocol to localize the traffic. This is done by storing a copy of each web page requested by users into a local proxy server and serving the cached copies for successive requests [98]. This type of caching, known as *shared caching*, reduces the traffic between the local network and the Internet. However, in a wireless environment with mobile hosts the main bottleneck for communications has been and still is the wireless link and using a cache server in the wired network does not improve the efficiency of the use of this resource.

Private caching, i.e. caching done in the user device has been used to store a copy of each page or object on the disk of the system which reduces the traffic between the local host and the local network. In a wireless environment this can increase the efficiency of communications of mobile hosts. However, in its simplest form, it does not help when a mobile device tries to access data which it has not accessed before. Simulation studies have shown that caching is more effective when done in a proxy server than on the local system due to overlapping requests from different end systems. In a mobile network environment this suggests that caching would be beneficial to perform in a proxy server located in the mobile network.

Transparent caching enables use of caching without configuration of the end users systems. In a mobile network environment this is a desirable characteristic as mobile devices will enter and leave the network.

Caching can be done reactively, i.e. by storing documents which are retrieved based on a client request and assuming that they will be requested again. Conversely, a cache can use *Predictive caching* to prefetch data before a client requests for it. Predictive caching can be used to improve the efficiency of using heterogeneous wireless networks by retrieving in advance data when low cost fast networks are available. Further it can be used to handle periods of disconnection as proposed by Kuenning and Popek [16], who use a predictive caching for a network filesystem. However, implementation of more general predictive caching in low power mobile devices is challenging due to limitations in the processing power, storage and battery capacity in these devices.

In all caching, the effectiveness increases with increased storage available. In the early studies, it was assumed that all possible documents could be stored and the client requests could always be delivered from the cache. However, with the increased amount of networked content it is not practical for a cache server located in a mobile network to store such large amounts of data. Even with a dedicated cache server inside a mobile network, it would not be practical to cache all possible content. Thus, it is necessary to only store a subset of the available information. Thus, prediction and *cache replacement policies* [12], [7], [105] become critical for ensuring a high *hit rate* for the cache.

A proxy architecture for mobile networks have been proposed by Rodriguez et al. [82] and Chakravorty et al. [14]. In their proposals, web pages are compressed in a proxy server to which the proxy clients connect and caching is used to improve the performance. In [14] the proxy clients are located in the mobile devices, while in [82] the client is located in the Mobile Router. Both the proxy server and clients employ caching. The architecture is similar to the idea proposed in this dissertation (P6). However, the architecture in this dissertation uses multiple cache servers on the wired network side to take advantage of locality.

3.8 Security of Network Mobility Management

The use of mobility management protocols changes delivery of traffic between the end hosts. In the case of NEMO, the Mobile Router and Home Agent reroute traffic flowing between Mobile Network Nodes and Correspondent Nodes using tunneling, so that the mobility and location of the Mobile Router is hidden from the Mobile Network Nodes and the Correspondent Nodes. This redirection would open vulnerabilities in the Correspondent Nodes, the Home Agent of the Mobile Router and the Mobile Network Nodes, unless the signaling used in NEMO was secured. In the design of NEMO it is assumed that the Mobile Router and the Home Agent share a trust relationship which can be used to secure the signaling with IPsec message authentication [57], [58]. The keys are derived using the IKEv2 key establishment protocol [21] based on pre shared secrets or certificates.

Use of route optimization between the Mobile Network Nodes or the Mobile Router and the Correspondent Nodes can not in general rely on pre existing trust relationships, since the Mobile Network Nodes may communicate with any nodes on the Internet [37]. However, solutions based on the Mobile IPv6 route optimization can leverage the security mechanism defined in [52] for route optimization, since the support for Correspondent Node functionality already exists in many IPv6 stacks. HIP and SIP based mechanisms have different security characteristics and may be able to use the security mechanisms designed into the protocols.

Localized mobility management protocols, such as FMIPv6 [62] and HMIPv6 [27] assume a trust relationship between the Mobile Router and the access network which can be used for authorizing access to the link and mobility signaling. However, authorization of access to the service is not sufficient, the Mobile Router needs to show that it has ownership of the addresses it uses in the signaling to prevent traffic hijacking and denial-of service (DoS) attacks. This is challenging for localized mobility management. Whereas in Mobile IPv6 and NEMO the Mobile Node has a fixed home address which can be used in a certificate or a database, in the case of HMIPv6 and FMIPv6, the Mobile Node communicates with the nodes in the access network with a location specific Care-of Address which can not be bound to a public key or shared secret in advance. Therefore, mechanisms such as cryptographically generated addresses [5] have been proposed for providing proof of address ownership for Care-of Addresses for signaling in FMIPv6 and HMIPv6.

4 PROPOSED ARCHITECTURE

This section presents an architecture for network mobility. The architecture depicted in Figure 4 consists of four key components: 1) a route optimization scheme enabling efficient routing for visiting mobile nodes, 2) a mobile caching architecture based on the route optimization scheme, 3) an access technology independent handoff scheme, 4) a localized mobility management scheme for vertical and horizontal handoffs, and 5) a secure configuration protocol for the architecture.

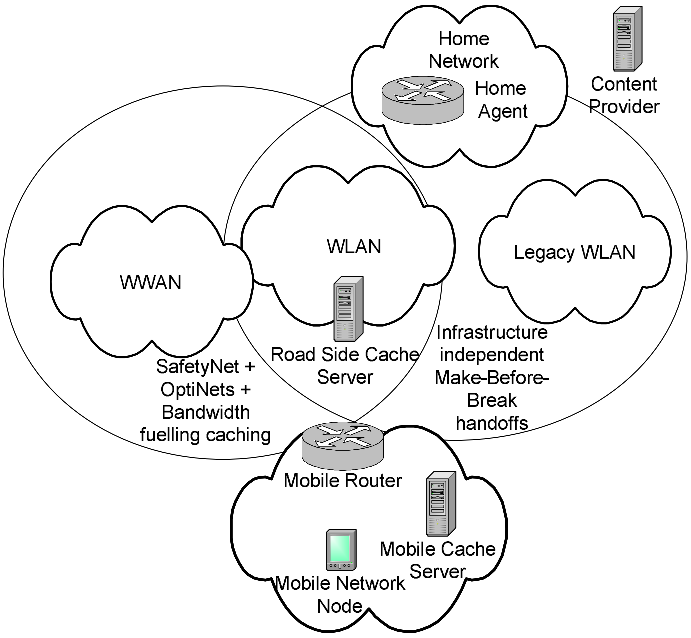

Figure 4: An overview of the proposed architecture.

The architecture provides a basic mobility management solution using infrastructure independent Make-Before-Break handoffs as presented in publications P1 and P7 to minimize the disruptions from the mobility. The scheme enables a Mobile Router to provide seamless connectivity to the Mobile Network Nodes without any support from the network, which would be the case in handoffs in legacy networks, such as the WLAN networks of today and also in handoffs between different operators networks. An overview of the scheme is presented in Section 4.3 and a detailed description is given in publication P1.

However, if the network operator supports mobility, the mobility management architecture can exploit the support to minimize the impact of handoffs on the connections of Mobile Network Nodes and to increase the efficiency of the communications. The proposed SafetyNet localized mobility management solution proposed in publications P2 and P3 for lossless horizontal and vertical handoffs improves the handoff performance from the basic solution by enabling recovery of packets lost during handoffs which cannot be completed before losing connectivity with the old network. An overview of the SafetyNet mechanism is given in Section 4.4 and a detailed design is given in publications P2 and P3, with P3 presenting a motivation and a basic design and P2 improving the design and applying it to vertical handoffs.

The efficiency of the communications is increased using a caching architecture, *Bandwidth Fuelling* together with a route optimization mechanism for NEMO, *OptiNets*. OptiNets Route optimization mechanism, proposed in P1, uses the capabilities of Visiting Mobile Nodes to enable Mobile IPv6 based route optimization between the Visiting Mobile Nodes and Correspondent Nodes. The Mobile Network Nodes use topologically correct Care-of Addresses from the visited network address hierarchy for the route optimization. The Mobile Router acquires and manages the Care-of Addresses from servers in the visisted network. An overview of the OptiNets mechanism is given in Section 4.1 and the mechanism is presented in more detail in Publication P1.

Bandwidth Fuelling, as proposed in publication P6, uses a client side cache server in the mobile network to serve the clients data during periods of low speed or limited connectivity. The cache of the client side server is updated opportunistically from server side cache servers deployed topologically close to the Access Routers to which the Mobile Router can connect via WLAN hot spots with high speed connectivity. This mechanism builds on the OptiNets route optimization mechanism to increase the efficiency of the cache update. An overview of the Bandiwdth Fuelling mechanism is given in 4.2 and a detailed description is presented in Publication P6.

The architecture can be configured dynamically using a secure configuration protocol proposed in P5. The configuration and security of the architecture are discussed in detail in Section 4.5.

4.1 Optinets route optimization for visiting mobile nodes

As discussed in Section 3.4, use of the NEMO protocol gives rise to non-optimal routing and protocol overheads. In this section, an optimization technique proposed by Perera et al [84] is incorporated into the architecture to overcome non optimal routing for mobility capable nodes within the mobile network. This dissertation improves the optimization technique further and implements, measures and analyzes the effects of using this technique.

In order to cater for the nodes present in the network that have no mobility management capabilities, the NEMO Basic Support protocol hides the mobility from all the nodes in the mobile network. This design restricts the MIPv6 enabled nodes from achieving better performance. If the Visiting Mobile Nodes (VMNs) within the mobile network were aware of the current location, they would be able to perform standard MIPv6 Route Optimization and avoid indirect routing via both Home Agents i.e. the Home Agent of the Mobile Router and the Home Agent of the Visiting Mobile Node. In OptiNets Route Optimization, this is achieved by requiring the Mobile Router to advertise a network prefix acquired from the foreign network on its mobile network interface. Using the prefix, the MIPv6 capable nodes within the mobile network can then auto configure a location specific Care-of Address.

In this work, the OptiNets technique is improved from [84] by restricting the use of the location specific CoA auto configured by the Visiting Mobile Nodes using the foreign network prefix only for the purpose of route optimization with Correspondent Nodes. This enables the Visiting Mobile Nodes to use the location specific CoA for communication with the Correspondent Nodes avoiding indirect routing via the Home Agents while avoiding the overhead of idle Visiting Mobile Nodes (i.e. Visiting Mobile Nodes which are not actively communicating) performing a network layer handoff each time the Mobile Router changes its point of attachment to the Internet. Idle Visiting Mobile Nodes do not use this newly acquired CoA to register with the Home Agent, i.e. these nodes will not use the location specific CoA until they start to communicate with a CN. Further, a special ICMPv6 option in the Router Advertisement (RA) is used for the foreign network prefix advertised by the MR in order to ensure that only Visiting Mobile Nodes (and not Local Fixed Nodes) would use the prefix to configure a CoA for route optimization.

To acquire the prefix from the foreign network, the Mobile Router runs the DHCPv6 prefix delegation protocol with the current Access Router. The Mobile Router then advertises this delegated prefix on its mobile network interface using a special ICMPv6 prefix option in the Router Advertisement message. Using this prefix the Visiting Mobile Nodes can auto configure a CoA for route optimization. The active VMNs will then initiate Mobile IPv6 route optimization with the Correspondent Nodes they are communicating with as specified in the Mobile IPv6 RFC [52]. Figure 5 depicts the operation of the mechanism. The mechanism is described in more detail in publication P1.

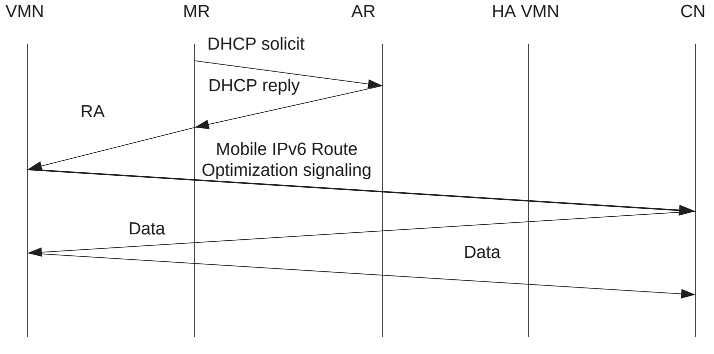

Figure 5: Signaling chart for OptiNets Route Optimization.

4.2 Caching

The architecture introduces a Mobile Cache Server which serves data to Mobile Network Nodes and Roadside Cache Servers which enable localized cache updates for the Mobile Cache Server. Roadside Routers provide high bandwidth, low-latency WLAN access to the Roadside Cache Servers. An overview of the proposed bandwidth fuelling architecture with roadside networks is given in Figure 6.

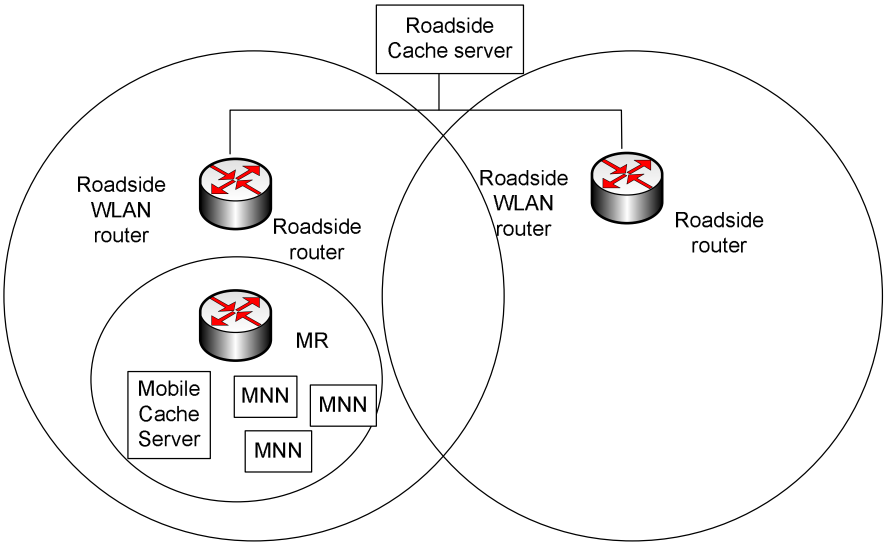

Figure 6: Bandwidth fuelling architecture.

Normally Mobile Routers would be equipped only with a WWAN Egress interface for connecting to the WWAN access network and a LAN or WLAN ingress interface connecting to the mobile network. In order for a Mobile Router to connect directly to the Roadside network, it would need to be equipped also with a WLAN Egress interface.

The fast WLAN connection together with the localized server allows the Mobile Cache Server to be updated during the time span that the Mobile Router is in the coverage area of the Roadside network. A Roadside Network could consist of one or more Roadside Routers connected to a Roadside Cache Server. The technical aspects of the architecture are given by first considering access to a Roadside Cache Server via a single Roadside Router while the mobile network is static, i.e. the vehicle has stopped. This will be followed by the case of using a cluster of Roadside Routers for access while the vehicle with the mobile network is moving.

It is assumed that the Mobile Routers are preconfigured with the identities of Roadside networks controlled by their Roadside access providers. Therefore the Mobile Router can detect the availability of Roadside Routers belonging to these networks and connect. It can then acquire a block of addresses from the Roadside Network and delegate an address to the Mobile Cache Server as proposed in the OptiNets Route optimization mechanism. The Mobile Cache Server then uses the location specific address from the roadside network to communicate directly with the Roadside Cache Server. This is in contrast to the indirect routing normally used with NEMO where packets to and from the mobile network are routed via the home network of the Mobile Router.

In the case, where the mobile network is within the coverage area of a Roadside Network consisting of multiple Roadside Routers the Mobile Cache Server needs to maintain the connectivity to the Roadside Cache Server for the duration of the cache update. Although this could be achieved with the NEMO tunneling via the Mobile Router and its Home Agent as shown before, this would potentially mitigate the benefits of using a Roadside Cache Server. Therefore as in the static case the OptiNets RO mechanism is used to enable the Mobile Cache Server to obtain a location specific address via the Mobile Router. In order for the Mobile Cache Server to benefit from the location specific address and perform direct routing when the network is moving the Mobile Cache Server needs to be MIPv6 capable. Having the MIPv6 capability would enable the Mobile Cache Server to use the location specific address and communicate directly with the Roadside Cache Server.

Upon receiving a request for data, the Mobile Router would first attempt to retrieve the information from the Mobile Cache Server. If the information is not available on the Mobile Cache Server, the Mobile Router would use its WWAN connection and serve the device. If the Mobile Router is unable to handle the request at the given time, it will inform the mobile device of the delay in serving the request. The architecture can be optimized to handle such situations. For example, the Mobile Router could request the Mobile Cache Server to start pre-fetching the information as soon as possible. The idea of pre-fetching via the Mobile Cache Server could be extended to enable customized services such as online audio or video clips.

This dissertation proposes the idea of using context information in order to enable pre-fetching of data to a Roadside Cache Server before the Mobile Network enters the road side network coverage area. This context information can be based on a combination of geographical context and vehicle route information. Mobile Router uses the context information and identifies the network it is about to enter and looks up the address of the corresponding Roadside Cache Server. It then informs the Mobile Cache Server of the address of the Roadside Cache server. Using this address, Mobile Cache Server sends a request for pre-fetching to the Roadside Cache Server using NEMO tunneling. Successful pre fetching of data to the Roadside Cache Servers would ensure that the customized data are ready to be downloaded efficiently using the low cost WLAN connection while the mobile network is in a coverage area of the Roadside network.

Timely fetching of customized data to the Roadside Cache Server depends on the ability to predict mobility correctly. However, even without mobility prediction the Roadside Cache Server would be able to provide the Mobile Cache Server with fresh non-customized data, such as local news, tourist information and traffic information.

4.3 Infrastructure independent Make-Before-Break handoffs

CDMA networks introduced make-before break handoffs using link layer soft handoffs, in which a mobile station is connected to multiple base stations simultaneously [59]. The CDMA soft handoffs are based on the capability of the CDMA network interface in the mobile station to listen to multiple base stations simultaneously. The soft handoffs extends Make-Before-Break handoffs by delivering data via multiple paths simultaneously in a synchronized manner, so that the Mobile Station can combine the streams. Note that this capability is not present in many of today's networks, such as IEEE 802.11 networks.

However, it is possible to perform Make-Before-Break handoffs on the IP layer by using multiple interfaces simultaneously. The concept of IP layer Make-Before-Break handoffs using multiple network interfaces was first introduced by Matsuoka et. al in their work which proposed soft handoffs with packet level bicasting with forward error correction [65]. This emulates closely CDMA behaviour. In publication P1 and P7, the multihoming part of their solution is adopted and and integrated into the NEMO handoff procedure to perform seamless handoffs using two interfaces. Unlike in Matsuoka et al.'s work bicasting is not used due to the reasons discussed below.

Bitlevel bicasting with forward error correction provides better performance in overlap areas with low signal to noise ratios than unicasting, since the receiver can combine the two bit streams using the forward error correction algorithm. It is possible that packet level bicasting would provide similar benefits. However, to the best of my knowledge the benefits of packet level bicasting is still an open research issue with no strong evidence on its feasibility. Further, the technique may not be generically applicable to common networks[3]. Since the use of packet level bicasting with forward error correction creates significant data transmission overheads during the handoff period and the benefits of the approach are uncertain, the approach is not used in the proposed architecture. However, use of bicasting with a different error recovery mechanism is introduced in the SafetyNet proposal in the next subsection and in publications P2 and P3.

A lossless Make-Before-Break handoff can be performed between two access networks using two network interfaces using the algorithm illustrated in Figure 7. The algorithm differentiates between an active interface and a scanning interface. The MR uses the active interface for delivering traffic between the mobile network and the Internet. The scanning interface is used to scan for new access points (APs) and perform a handoff, when a better AP than the current one is found. The algorithm for making the handoff decision is abstracted in Figure 7, and can be implemented using existing technologies such as signal to noise ratio comparisons [6] combined with movement prediction algorithms [64]. The handoff is started when the predicted signal strength of the current access point at the time when the handoff is finished would be below an acceptable level and a candidate access point would according to the prediction have acceptable signal strength at that point. When the handoff is completed the data traffic is switched to the new interface and the original active interface becomes the scanning interface.

Using the above described algorithm it is possible to perform completely lossless handoffs, provided that the coverage of the old access network and the new access network overlap sufficiently and the handoff decision is done

---

[3] Due to the CRC mechanism employed in IEEE 802.11 networks, a bit error in a packet leads to discarding of the packet before the IP layer receives the packet and can correct the error.

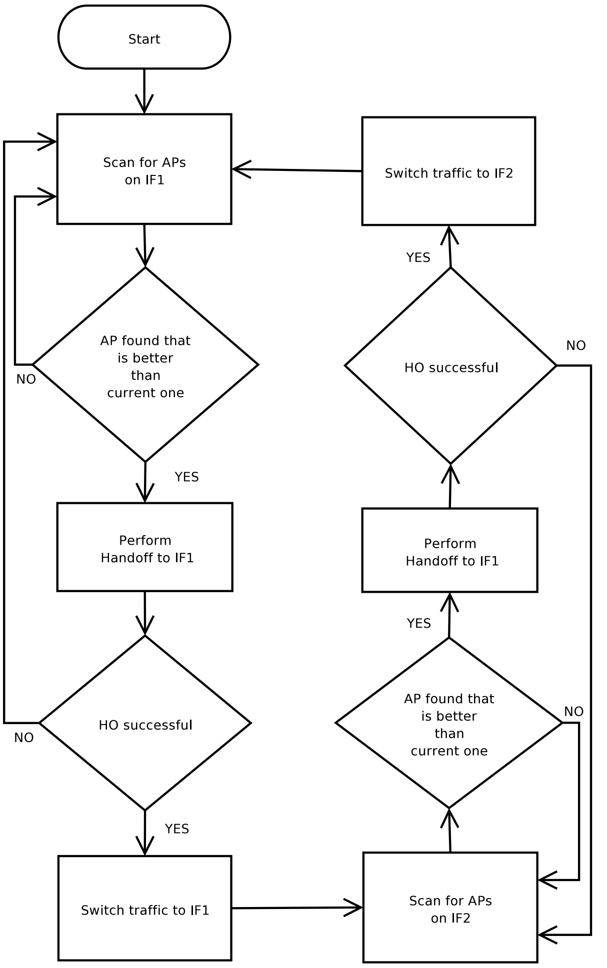

Figure 7: Seamless handoff algorithm for two interfaces.

at the correct moment. This aspect is analyzed in more detail in Section 5.1.

4.4 Localized handoff management

Use of Make-Before-Break handoffs enables lossless handoffs, if the Mobile Node can finish the handoff before losing connection with the previous Access Router. If the connection is lost early, which may easily happen with the long handoff latencies present in NEMO, the Mobile Router will lose packets. Use of a localized mobility management, such as Fast Handovers for Mobile IPv6 reduces the handoff latency significantly. However, the Fast Handovers for Mobile IPv6 protocol is designed for Break-Before-Make handoffs and does not perform well in Make-Before-Break handoffs, as shown in P2 and P3.

In SafetyNet, the Fast Handovers for Mobile IPv6 protocol is adapted to fit the architecture presented in this dissertation by extending it to support Make-Before-Break handoffs. The design of SafetyNet allows recovery of packets lost during the handoff when attaching to the new Access Router, as described in the following paragraphs. The protocol is based on FMIPv6 Bicasting with Selective Delivery (FMIPv6-BSD) proposed in publication P3, a protocol for seamless horizontal handoffs.

At the initialization of the handoff, the previous Access Router (pAR) starts n-casting packets to candidate new Access Router(s) (nARs) as well as to the Mobile Router to ensure that any packets lost during the handoff can be recovered. Packets lost during the handoff, i.e. packets that the MR did not receive directly from the pAR, are delivered to the Mobile Router at the finalization of the handoff from the buffer of the new Access Router. The pAR marks the packets it n-casts during the handoff using a sequence number which allows the Mobile Router to notice which packets it missed and request those when it arrives at the link of the nAR. This selective delivery mechanism, ensures that only the lost packets are delivered from the buffer, as opposed to the entire contents of the buffer which would be the case with Fast Handovers for Mobile IPv6 [61].

Using a vertical handoff timing algorithm based only on the signal strength, the Mobile Router would finalize the handoff immediately after the initialization of the handoff. As opposed to this, in the SafetyNet handoff timing algorithm, the Mobile Router keeps using the pAR until it 1) arrives at a nAR of the preferred lower cost network type, allowing it to avoid a vertical handoff and instead perform a horizontal handoff, or until it 2) loses an amount of packets deemed intolerable to the application thus requiring a vertical handoff. When either of these conditions is met, the Mobile Router attaches to the selected nAR and finalizes the handoff. Figure 8 gives an overview of the operation of the SafetyNet protocol and the timing algorithm. The algorithm is described in more detail in publication P2.

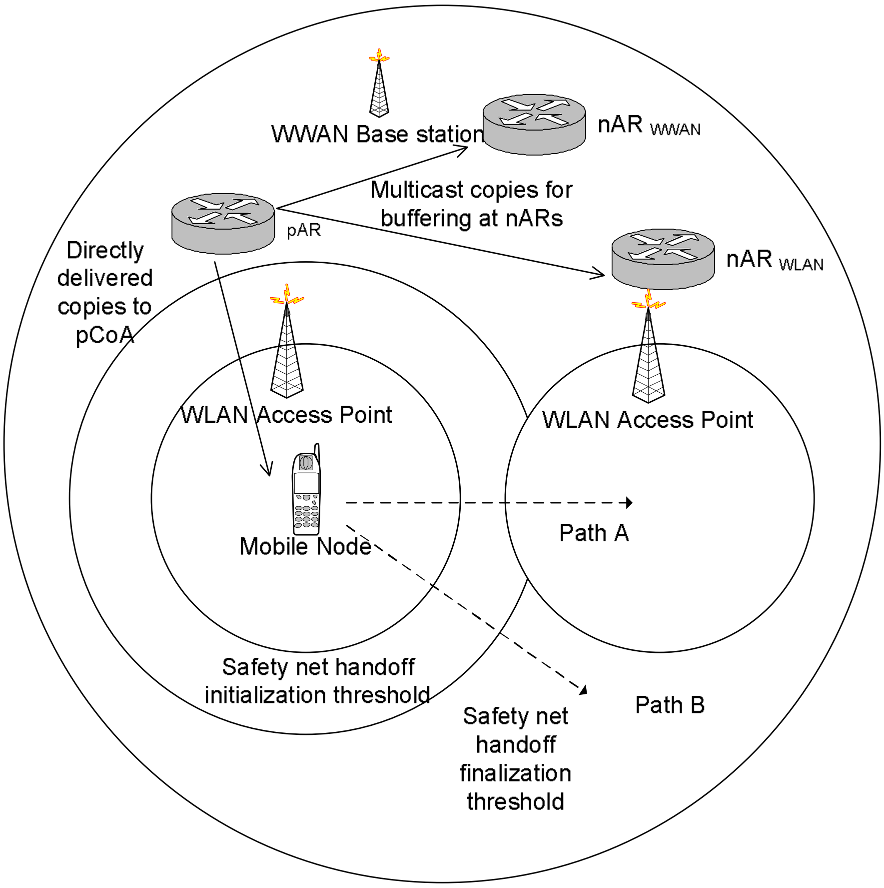

Figure 8: Safetynet Architecture.

In Figure 8, the Mobile Router initializes the handoff towards both the

WLAN 2 and WWAN Access Routers. It then delays the finalization of the handoff until either of the two conditions described above is met. In the case of the Mobile Router moving on Path A, the delaying of the finalization of the handoff allows it to perform a horizontal handoff to the nAR of WLAN2. In the case of Path B, the Mobile Router eventually performs a handoff to the nAR of the WWAN. In this case, the delaying of the handoff finalization may incur some packet loss. However, the use of the SafetyNet protocol allows the Mobile Router to recover any packets lost during the handoff. The algorithm for the delaying of the handoff uses application or transport state for the decision. For example, streaming applications have a buffer which allows for delaying of the handoff until the data in a missed packet would be used. By finishing the handoff so that the missed packet can be delivered before the data needs to be accessed by the application, it is possible to hide the packet loss from the application while at the same time increasing the dwelling time in the WLAN. The algorithm is described in more detail in P2.

OptiNets and caching use the SafetyNet architecture to enable transfer of OptiNets prefix delegation context and bandwidth fuelling cache contents between the previous and new access routers. This reduces the over the air signaling required to re-establish the prefix delegation and cache state and reduces the latency of the handoff. Further, the transfer of the cache contents enables colocation of the road side cache server in the Access Routers, and thus increases the benefits gained from the locality of the road side cache servers.

4.5 Security of the architecture

This section describes the security of the proposed architecture and the secure configuration of the Mobile Router. The localized mobility management and caching use AAA to establish keys between the Mobile Router and the visited network as specified in [40]. These keys are then used for securing the different protocols the Mobile Router runs with the access network. Further, the Mobile Router establishes security associations and a shared secret key with the Home Agents in its home network with the help of the home network AAA server. Figure 9 shows an overview of the proposed security architecture.

The Mobile Router and the Handover Key Server in the visited network share a Handover Master Key. The Mobile Router and the Handover Key Server use the Handover Master Key to derive session keys for each protocol using the Handover Key Protocol [40]. In the proposed architecture, SafetyNet uses the Handover Key Protocol to establish a shared secret key between the Mobile Router and the previous and new Access Routers. The SafetyNet signaling is then secured using message extensions for end point authentication and integrity protection as specified in the revised proposal of Fast Handovers for Mobile IPv6 in [62]. Since the Handover Key is established with the current Access Router before the handover, the Handover Key Protocol does not reduce the handoff performance as long as the interval between handoffs is sufficient for the protocol to finish.

The OptiNets optimized routing mechanism requires the Mobile Router

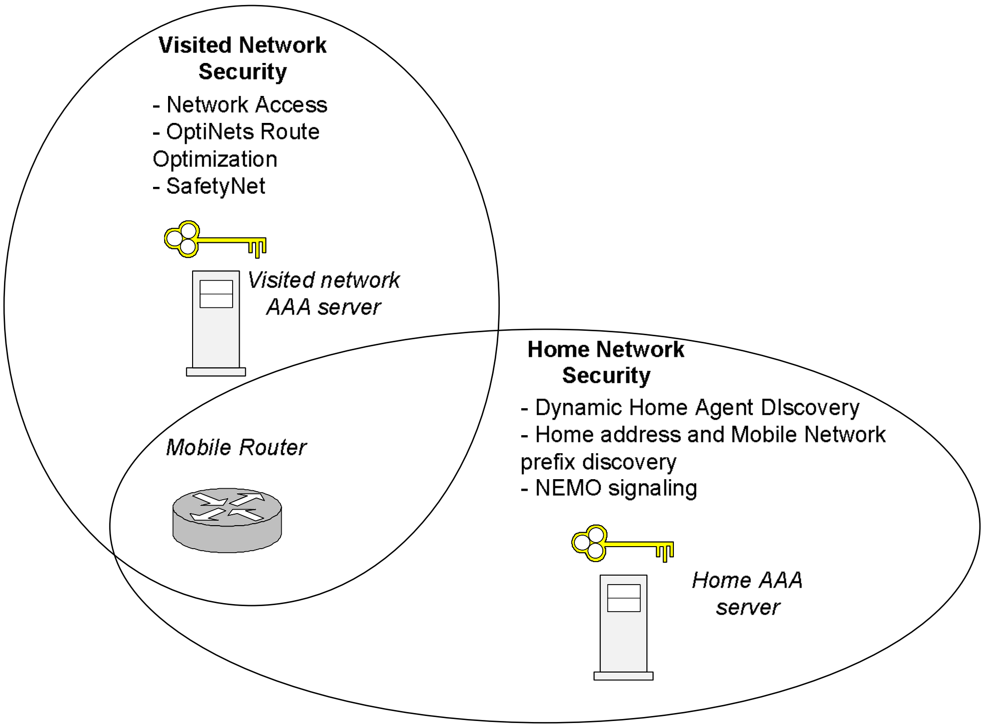

Figure 9: Overview of the Security Architecture.

to delegate a prefix from the visited network using DHCPv6 prefix delegation. To ensure that the prefix is from a valid Access Router and that an authorized Mobile Router gets the prefix, the DHCPv6 messages need to be authenticated. The authorization and authentication is achieved using the DHCPv6 message authentication mechanism defined in [29], [28] with a second Handover Key established using the Handover Key Protocol.

As opposed to the Handover Key used with SafetyNet, the Handover Key Protocol is run after the handoff with the new Access Router. This increases the handoff latency. However, the use of SafetyNet or infrastructure independent Make-Before-Break handoffs ensures that the Mobile Router can deliver packets to and from Mobile Network Nodes with addresses from the old delegated prefix until the new Handover Key is established and the new OptiNets prefix becomes available to the Mobile Network Nodes.

A third Handover Key is established between the mobile cache server and the roadside cache server for authentication and integrity protection of the cache update requests and retrieval of cached content. The cache update request and retrieval messages are protected using a message authentication code created with the Handover Key over the contents of each message.

In addition to securing the Mobile Router - Access Router communications, AAA is used for establishing an IPsec security association for NEMO and a shared secret key for secure home agent discovery between MR and the home network. The Mobile Router establishes the shared secret with the home network Handover Key Server to enable the use of the secure home agent address discovery protocol defined in publication P5. With the address of the Home Agent known, the Mobile Router can run IKEv2 as defined in [21] to establish security associations with the selected Home Agent and to discover a home address [26]. Further, using an extension to NEMO signaling as proposed in [102], the Mobile Router can get a Mobile Network Prefix from its Home Agent.

Figure 10 presents an overview of the signaling used to establish the security associations and shared secret keys when a Mobile Router starts up. The Mobile Router and the Access Router re-establish the Handover Keys after every handoff, whereas the Handover key for Dynamic Home Agent Address Discovery between the Mobile Router and the home network Home Agents can be used as long as the Mobile Router is running. If the Mobile Router needs to switch its Home Agent using Dynamic Home Agent Discovery protocol, it needs to re-run IKEv2 with the new Home Agent to re-establish the IPsec security associations.

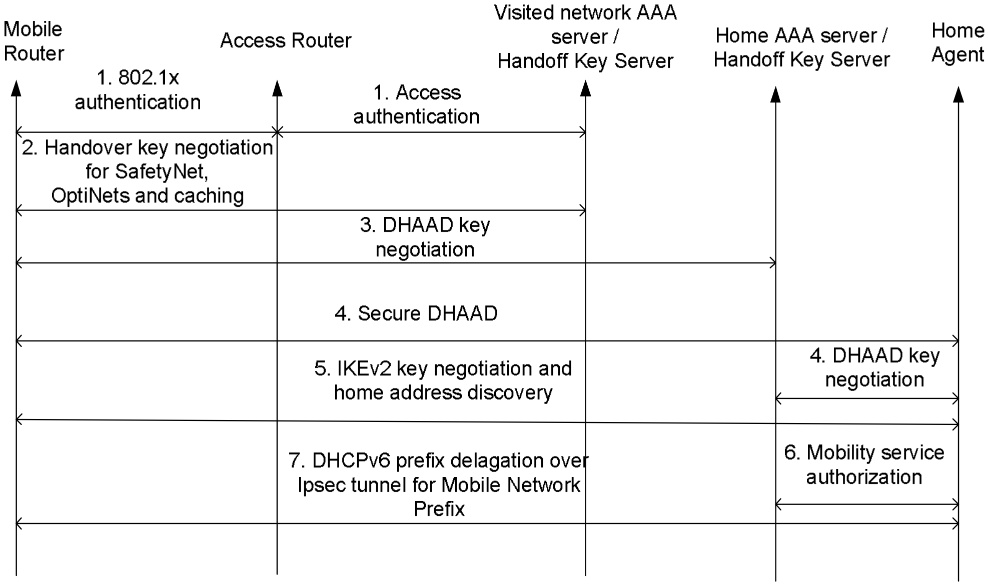

Figure 10: Signaling for establishing the security associations and Handover Keys.

5 ANALYSIS

In this section, the architecture is evaluated according to the criteria defined in Section 2.2 and compared with related solutions. Since the related work consists mostly of solutions to the individual problems of overhead, caching, handoffs and configuration, the proposed architecture is compared against the relevant partial state of the art solutions in each criteria.

5.1 Uninterruptibility

The most important criteria is uninterrupibility, i.e. that the communications of users of the mobile network are not affected negatively by handoffs of the Mobile Router. This section presents the central results from publication P1 and P7 for infrastructure independent handoffs and from P2 for the SafetyNet localized mobility management proposal. Additionally, new analysis is presented on handoff success rates for fast movement and the impact of incorrect handoff decisions on the connections of Mobile Network

Nodes. Further, the comparison of the two handoff schemes with other solutions in P1 and P7 for the infrastructure independent Make-Before-Break handoffs, and in P2 and P3 for the SafetyNet mechanism is extended to cover the relevant state-of the art proposals discussed in Section 3.

Analytical and numerical evaluation of the viability of the Infrastructure independent Make-Before-Break and SafetyNet handoff schemes

A Mobile Router can perform seamless horizontal handoffs by using two radio interfaces. In other words, the infrastructure independent Make-Before-Break handoffs do not affect the applications running between the Mobile Network Nodes and Correspondent Nodes at all. The empirical performance is evaluated for UDP and TCP traffic in detail in publications P1 and P7. The empirical results in P1 show that the handoffs do not affect UDP or TCP traffic between the Mobile Network Nodes negatively, as long as the handoff can be performed as a Make-Before-Break handoff and the interference between the radio interfaces is minimized. Further, the empirical comparison in publication P7 shows that the handoff performance of the Make-Before-Break handoffs is better than that of infrastructure based Fast Handovers for Mobile IPv6 for TCP.

In order to perform a Make-Before-Break handoff, the coverage areas of the previous and the new networks need to overlap sufficiently, so that the handoff to the new access network can be finished before the Mobile Router leaves the effective coverage of the previous access network. The effects of this requirement are analyzed below for the infrastructure independent Make-Before-Break handoffs proposed in publication P1.

The required overlap $l_{overlap}$ depends on the speed of movement v_{mr} and latency of the handoff t_{ho}. This can be described more formally using the following equation: $l_{overlap} \geq v_{mr} * t_{ho}$. Thus even with two interfaces it is worthwhile to minimize the handoff time, since this allows to increase the speed of the Mobile Router with a given overlap, or optimize the overlap of cells for Mobile Routers moving with a certain maximum speed.

In real radio networks, the cell geometry is rarely regular due to the radio characteristics of the antennae used and the natural and man made structures which, attenuate or completely block, and also reflect the signals. For example, in a road side environment with access points or base stations on regular intervals along the road with directional antennae, the cell geometry may be simple and the overlap may be significant. In this dissertation the cell model is used for validating the applicability of Make-Before-Break handoffs to short range radio networks in as generically as possible. Therefore, an ideal cell structure for open air propagation shown in Figure 11 is used to keep the results as general as possible. However, this choice may impact the applicability of the results to specific scenarions.

The minimum overlapping coverage area between the cells in an ideal open air cellular model was defined by Hsieh et al. [47] as follows, with r depicting the cell range and d the difference between the effective cell coverage radius and the good cell coverage radius:

$$a'b' = 2r \cdot \sin\left\{\frac{\pi}{3} - \arcsin\left[\frac{\sqrt{3}}{2}\left(1 - \frac{d}{r}\right)\right]\right\} \tag{1}$$

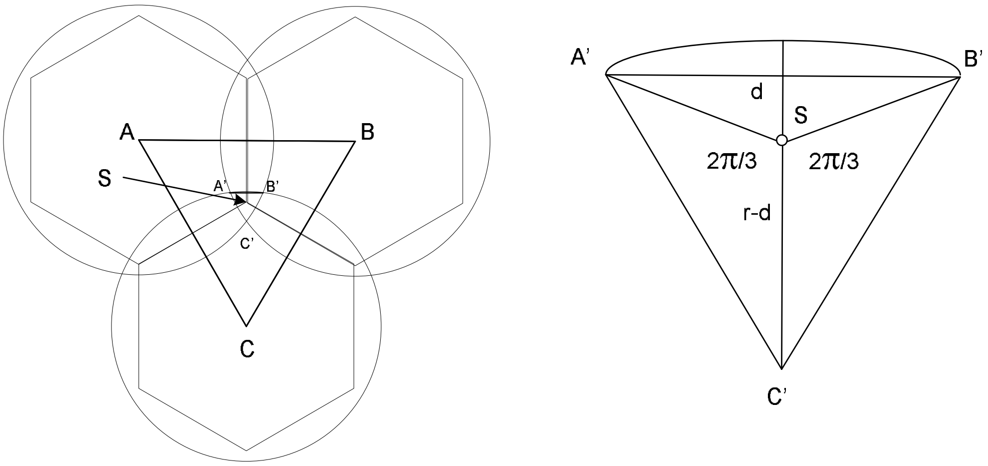

Figure 11: Overlapping area in an ideal cellular access network.

Using the above equations the minimum available time for completing the handoff as a Make-Before-Break handoff is analyzed as a function of the speed of movement in a cellular WLAN network with cell radius $r = 80m$ and $d = 8m$ in Figure 12. A small cell size was selected to show that the handoff can be completed as a Make-Before-Break handoff at speeds up to 22 m/s as long as the handoff latency can be kept under 1 s.

If the Mobile Router is moving at speeds which result in a handoff every few seconds, it needs to constantly scan for better access points at a rate of several times a second using active WLAN scanning. In other words, the inactive WLAN card needs to switch to a new channel and send a probe and wait for a reply for a short period of time before moving on to the next channel. This limits the rate of handoffs, since with 11 channels in WLAN, a waiting period for the probe replies on each channel and a channel switching latency of 5-19 ms, as measured in [90] the scanning latency of all channels becomes several hundreds of milliseconds. The results acquired by Ramani et. al in [90] show a total WLAN scanning latency of 350-400 ms for Prism2 based cards and 500 ms for an Atheros based card under Windows. In publication P1, a total handoff latency of 200 ms was observed for a Prism 2.5 based card. As a part of the handoff, all channels were scanned. Assuming that the association with the new access point takes less than 10 ms as suggested in [90], the time required for one scan would be 190 ms. If a minimum of 3 samples are required as suggested in [47], then the scanning of all channels for 3 times will take 570 ms. After this the Mobile Router can select the best next Access Point and the Access Router behind it according to the AP selection algorithm discussed in Section 4.3.

If there is not enough time for a well informed handoff decision, the Mobile Router may either end up losing connectivity with the current Access Router before finishing the handoff which would lead to a complete or partial Break-Before-Make handoff or having to perform a handoff based on incomplete information about the best candidate for the next Access Router. However, it may be possible to optimize the scanning process by skipping the channels on the second and third scan which did not have any access points on the first scan.

In case the handoff decision is made only after losing contact with the current Access Router, the resulting Break-Before-Make handoff would impact any on-going communications. In experiments done for publication P1, this impact was approximately 230 ms, due mostly to the WLAN scanning [4]. The detailed breakdown of the handoff latency is presented in publication P1 and depends on the network topology, and whether the network supports network level optimizations, such as Fast Router Advertisements [18], [17].

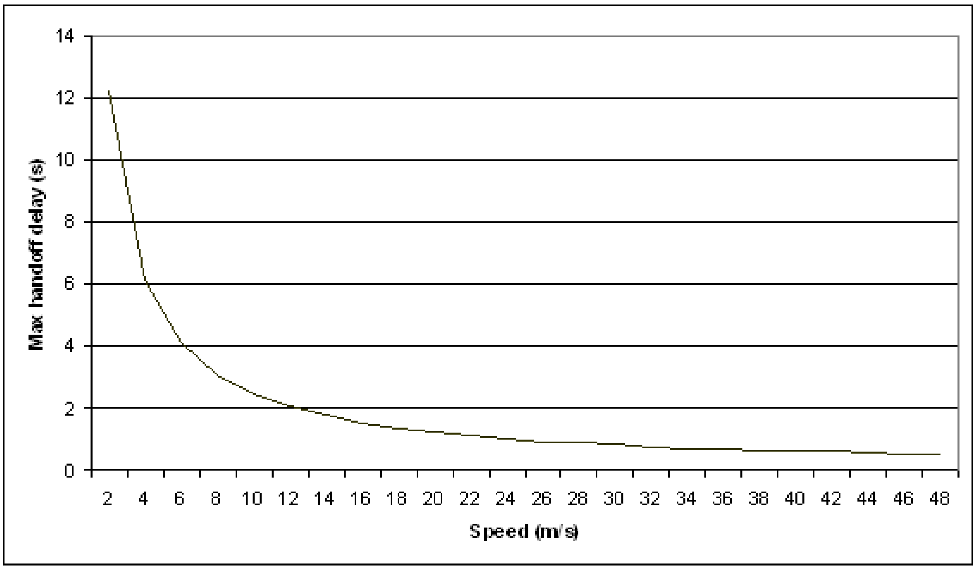

Figure 12: Maximum handoff time for achieving Make-Before-Break handoff as a function of the speed of the Mobile Router with a fixed cell size $r = 80m$ and difference between good and effective covearge areas $d = 8m$.

A handoff decision based on a limited number of scans may lead to an erroneus selection of a new Access Router. An erroneus handoff decision results in a second handoff immediately after the first one preceded by three additional scans to ensure selection of the right Access Point and Access Router. In a scenario of very fast mobility, the second handoff would need to be performed as a Break-Before-Make handoff. It is assumed that the Mobile Router moving from A' to B' in Figure 11 performs three scans and based on them performs a handoff first to access point at C with a probability of $P_{failure}$ and to access point at B with probability $1 - P_{failure}$. If the Mobile Router connects to C, it will notice the low signal to noise ratio of C and start looking for a better access point. To do this, it first performs 3 scans and then initiates a handoff towards B. If the time it takes to do these operations exceeds the dwelling time in the overlapping area, the Mobile Router will lose connectivity for a time of $T_{disrupt}$ with the maximum handoff delay $T_{MaxHandoffDelay}$ from Figure 12.

$T_{disrupt} = P_{failure} * max(0, 2*(3*T_{scan} + T_{handoff}) - T_{MaxHandoffDelay}) + (1 - P_{failure}) * max(0, 3 * T_{scan} + T_{handoff} - T_{MaxHandoffDelay})$

The impact of an erroneus handoff decision for the infrastructure independent Make-Before-Break handoffs as a function of the speed of the Mobile Router is analyzed in Figure 14. It can be seen that the impact of an

---

[4] in the WLAN driver used for P1, the scanning is always performed as a part of the handoff in the driver used, even if the channel and hardware address of the next Access Point are known.

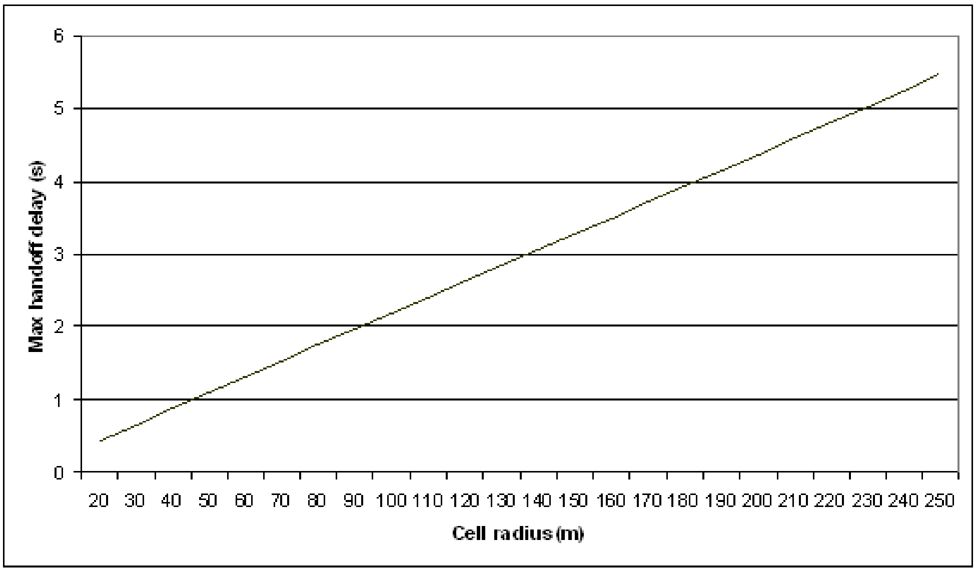

Figure 13: Maximum handoff time for achieving a Make-Before-Break handoff as a function of the cell size with a given speed $v = 14m/s$ for the Mobile Router. The difference between good and effective covearge areas is set as $d = 8m$.

erroneus handoff decision does not affect the on-going traffic until the speed of the Mobile Router reaches 10 m/s. At higher speeds the importance of a correct handoff decision increases and even the small probability of 10% of an incorrect handoff decision starts to disrupt the traffic to and from the Mobile Network Nodes.

The SafetyNet protocol enhances Make-Before-Break handoffs as discussed in publications P2 and P3. It enables the Mobile Router to receive all the packets lost during time $T_{disruption}$ from the buffer of Access Router B' after attaching to it. This is possible due to the use of multiple candidate access routers in the SafetyNet architecture which allows initiation of handoff towards multiple new Access Routers and finalization of the handoff according to the SafetyNet timing algorithm. In the case of SafetyNet, the Mobile Router moving from A to B on the line between A' B' would initiate the handoff toward B and C at A' and finalize it towards B after crossing the line C'S. Even with SafetyNet it would be possible that the Mobile Router would still lose packets, but the probability would be significantly smaller than with the infrastructure independent handoff mechanisms or with Fast Handovers for Mobile IPv6 which enables a handoff only towards one Access Router. The tradeoff of increased buffer space and over-the wire data transmission and signaling costs to increase the success rate of a handoff is analyzed in publication P2 and shows that it is feasible to use the capacity in the wired network to increase the success rate of the handoff.

To analyze the sensitivity of the SafetyNet protocol to incorrect handoff decisions, assume that the Mobile Router initiates the handoff towards B and C and tries to finalize the handoff with C. If the Mobile Router manages to finalize the handoff, before noticing the handoff was initiated towards the wrong access router, it needs to initiate a new handoff towards A and B. It does not have to perform a full scan due to it already having a list of candidate

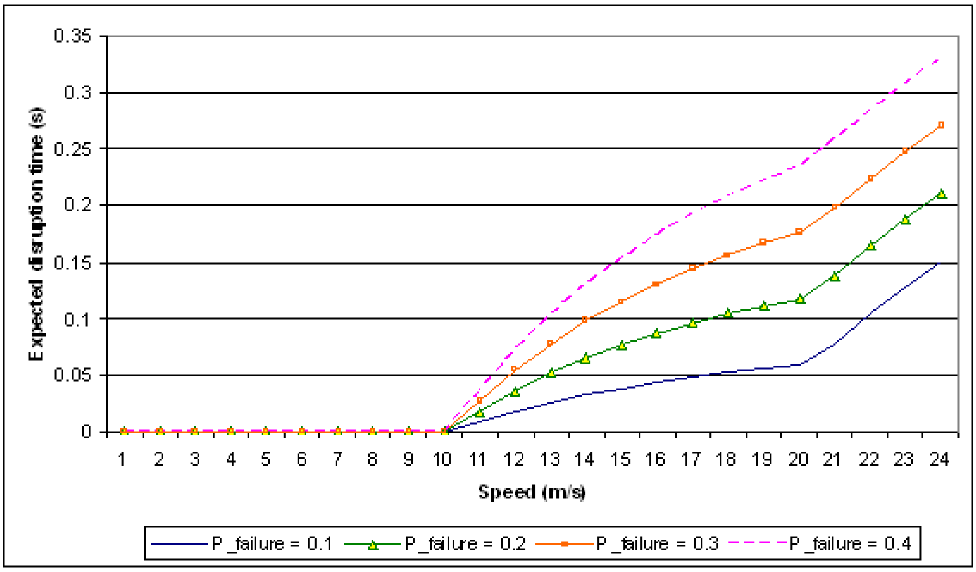

Figure 14: Disruption caused by a handoff as a function of the speed for the Mobile Router for different probabilities of erroneus selection of next access router with a fixed cell size $r = 80m$ and difference between good and effective covearge areas $d = 8m$.

access points and the access routers behind them from the previous handoff towards the Access Routers at B and C as described in P2. It only needs to compare the signal strength of A, B and C which would lead to a delay of 3 * (10+2) ms. Further, this scan can be done after initiating the handoff, so it does not affect the critical delay of establishing the forwarding[5].

The delay for establishing the bicast forward tunnel to the new Access Router at B is the sum of the Round Trip Time (RTT) between the Mobile Router and the Access Router at C and the RTT between the Access Routers at B and C. In the case of a WLAN network with a 80m cell radius, this latency could be estimated to account for 50 ms. After the forward tunneling is established, the Mobile Router will be able to recover any packets it misses due to moving out of the coverage area of C before connecting to B. The connection to the Access Router B would take approximately 10-20 ms, due to the RTT between the Mobile Router and B. After connecting, the Mobile Router would be able to receive any packets it did not receive directly during the connection time from C. Thus, the maximum disruption time would be approximately 50 ms from the start of the second handoff, i.e. the duration of the initialization of the second corrective handoff $T_{handoffInit}$. However, if the Mobile Router does not manage to connect to the Access Router at C, it will instead finalize the handoff with B and therefore not lose any packets. The expected disruption $T_{disrupt}$ for the SafetyNet protocol is given with $P_{failure}$ denoting the probability of finalizing the handoff with the incorrect Access Router at C [6].

---

[5] After the n-cast forwarding is established, all packets lost during the handoff can be recovered from the buffer of the nAR.

[6] The second case of trying to finalize the handoff with the incorrect Access Router, but failing is counted as a success, since it does not lead to disruption of traffic in the ideal cell topology model.

$$T_{disrupt} = P_{failure} * max(0, T_{scan} + T_{handoffInit} + T_{handoffFinalize} + T_{handoffInit} - T_{MaxHandoffDelay}) + (1 - P_{failure}) * max(0, T_{scan} + T_{handoffInit} - T_{MaxHandoffDelay})$$

The negative impact of erroneus selection of the Access Router with which the handoff is finalized is analyzed numerically in Figure 15. It is assumed that the handoff can always be finalized with Access Router at C, so as to require a second handoff to simplify the analysis. However, even with this pessimistic assumption the use of SafetyNet improves the handoff performance significantly and allows disruption free handoffs up to speeds of 46 m/s. Since the Doppler shift has a strong impact on the performance of IEEE802.11b at least for downlink UDP traffic at speeds much lower than 90 m/s and thus limits the maximum speed [80], it can be said that the SafetyNet protocol provides sufficient handoff performance for IEEE 802.11 networks. More generally, it can be concluded that the use of the SafetyNet provides disruption free connectivity to any combination of short or long range radio networks with handoff processes with similar or lower latencies than IEEE 802.11 and with a cell radius larger than 80 m at speeds up to 90 m/s.

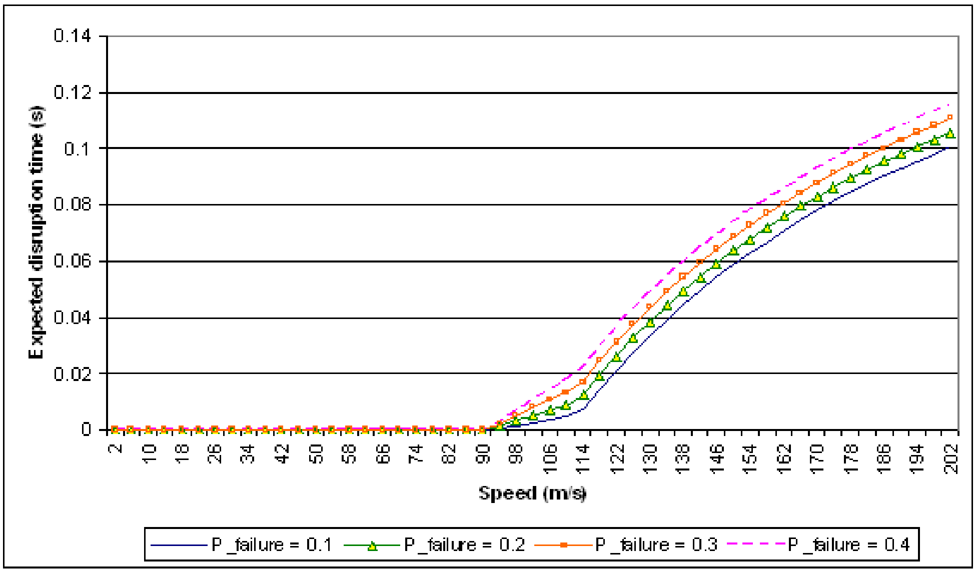

Figure 15: Expected disruption time caused by a handoff as a function of the speed for the Mobile Router using the SafetyNet protocol for different probabilities of erroneus selection of next access router with a fixed cell size $r = 80m$ and difference between good and effective covearge areas $d = 8m$.

In the above analysis it was assumed that all the packets missed at the link of the previous Access Router could be delivered from the buffer without delaying new packets. The ability to recover packets from the buffer of the new Access Router requires sufficient bandwidth on the link to deliver all the packets from the buffer that were missed due to connecting to the incorrect new Access Router at C at an accelerated rate so as to not delay the delivery of fresh packets arriving in the buffer. On saturated links this may lead to delaying of packets. An overview of the impact of saturated links on the performace of SafetyNet is given in Section 5.1 and discussed in more detail in publication P2.

Comparison of infrastructure independent handoff performance
The architecture presented in this dissertation uses system and protocol level improvements to minimize the negative impact of the handoffs for horizontal and vertical handoffs. The handoff performance is compared with the state of the art infrastructure independent proposals, which address the network and link layer handoff latencies.

Table 1 presents the theoretical handoff latency minima for network level handoffs for NEMO, NEMO with Fast router advertisements [17], [18] and NEMO with Optimistic DAD and Fast Router Advertisements (Fast RAs) without link layer handoff components from publication P1. In reality, the handoff latencies are always larger than this due to the RTT between the Access Router and the Home Agent, the RTT between the Mobile Router and the Access Router and due to the additional latency caused by the link layer handoff. In the research leading to P1, the link layer handoff latencies were found to be between 100 ms and 1400 ms, depending on the used WLAN hardware. Thus, the use of network layer protocol optimizations alone is not sufficient for achieving lossless handoffs.

Table 1: Theoretical Minima for Network Layer Handoff Latencies with NEMO.

Handoff type	NEMO without optimizations	With Fast RAs	With ODAD	With Fast RAs and ODAD
Home to Foreign	2.75 s	2.5 s	1.25 s	1 s
Foreign to Foreign	1.75 s	1.5 s	0.25 s	0 s
Foreign to Home	0.25 s	N/A	0.25 s	0 s

The protocol level optimizations can be complemented with system level optimizations, as proposed in publication P1. This enables the mitigation of packet loss resulting from the remaining handoff latency. In Table 2, the effectiveness and applicability of previously proposed system level improvements is compared with that of the proposed NEMO Make-Before-Break handoffs. The performance values for the other proposals are taken from Brik et al's study [10].

SyncScan and the Neighbor Graphs proposal rely on infrastructure support from the access points to enable the fast handoff, whereas the MultiScan proposal [10] utilizes two interfaces in a somewhat similar way as the proposed mechanism. However, Multiscan requires that the same MAC and IP address are used on both interfaces. Since the first 64 bits of IPv6 addresses depend on the network topology, it is possible to use the same IP address on the primary and secondary interface only, if the old and new Access Points are part of the same IP network. This requirement prevents one from using their scheme for handoffs between different access providers networks or between different parts of a larger network divided into different IP networks, e.g. a campus network with outdoor Access Points connected to a different Access Router than the Access Points inside a building. Thus, the MultiScan

Table 2: Comparison of system level handoff improvements for WLAN handoffs.

	Number of required radio interfaces	**Effective handoff latency**	**Access Point support required**	**Inter-network handoff support**
MultiScan	2	0 ms	no	no
SyncScan	1	2-3 ms	yes	no
Neighbor Graphs	1	40 ms	yes	no
Make-Before-Break	2	0 ms	no	yes

proposal is not applicable as such to improving the performance of IP level handoffs.

The proposed Make-Before-Break scheme for NEMO provides comparable performance to the leading competing proposal MultiScan and provides this performance regardless of the network topology, unlike MultiScan which depends on the old and new Access Point belonging to the same IP (sub)network. Further, the system level mechanism in NEMO Make-Before-Break handoffs is combined with changes to the NEMO logic to take advantage of the Make-Before-Break handoffs which mitigates the negative effects from the handoff latency from the round trip time between the Mobile Router and the Home Agent, as described in more detail in publication P1.

Comparison of infrastructure assisted handoff performance

The architecture improves upon infrastructure based horizontal and vertical handoff mechanisms. The proposed approach in P2 and P3 is compared with related work: with Hierarchical Mobile IPv6 (HMIP), Fast Handovers for Mobile IPv6 [61] (FMIPv6), with a combination of Fast Handovers for Mobile IPv6 and Hierarchical Mobile IPv6 (F-HMIP and FF-HMIP) and with Synchronized MIP [46], [47].

Hierarchical Mobile IPv6 (HMIPv6) [97], [27] uses a hierarchy of Mobility Anchor Points to eliminate the component of handoff latency resulting from the signaling latency between the Access Router and the Home Agent. Fast Handovers for Mobile IPv6 (FMIPv6) [61], [62] uses buffering in access routers to reduce or eliminate packet loss from link layer handoff latency. Both F-HMIP and FF-HMIP combine Hierarchical Mobile IPv6 with Fast Handovers for Mobile IPv6 to reduce the signaling load on the wired part of the network and FF-HMIP additionally reduce the impact of inter-domain handoff using chaining of Mobility Anchor Points. In addition to the functionality of F-HMIP, S-MIP synchronizes the delivery of packets to improve the handoff performance.

The functionality of the handoff schemes is summarized in Table 3. All the FMIPv6 based schemes can prevent packet loss through the use of buffering, provided that there is enough bandwidth to deliver all the packets from the buffer after the handoff. This aspect and its problems are discussed in detail in publications P2 and P3. However, only Fast handovers for Mobile IPv6 with bicasting and Safetynet enable the Mobile Router to receive packets continuously during the handoff by utilizing bi-casting or in the case of SafetyNet, n-casting. For longer link layer handoff latencies, this functionality has a large impact on handoff performance, as shown in the next paragraph. Both SafetyNet and S-MIP use buffer management techniques to improve handoff performance, although for different purposes. SafetyNet uses buffer management to ensure that no duplicate packets are delivered to the Mobile Router in spite of bi-casting or n-casting of the traffic, whereas S-MIP uses synchronized delivery of packets from buffer to minimize packet loss.

Table 3: Functionality comparison of the infrastructure based handoff schemes.

Name of Scheme	**Lossless handoffs**	**Gap-free connectivity**	**Buffer management**	**Inter-domain handoffs**
FMIPv6	yes	no	no	no
FMIPv6 with bi-casting	yes	yes	no	no
S-MIP	yes	no	yes	no
HMIP	no	no	no	no
F-HMIP	yes	no	no	no
FF-HMIP	yes	no	no	yes
SafetyNet	yes	yes	yes	yes*

*Architecture supports inter-domain handoffs with the NEMO Make-Before-Break handoffs.

A summary of an experimental comparison for Fast Handovers for Mobile IPv6 and the proposed architecture is presented in Figure 16. The figure shows the impact of the handoff on the progress of TCP and the amount of data which is resent because of packet loss or delays in delivery. The graph is created from TCP sequence number data for the handoffs in publication P2. The TCP progress is measured during the handoff period, starting from the start of the handoff and ending after the TCP data rate has stabilized after the handoff. The TCP resent data is measured from the amount of segments that are resent. The methodology of the experiments used is given in Section 4.1 and more extensive results are given in Section 4.2 of publication P2.

The resending occurs due to congestion on the link of the new Access Router when the new Access Router starts delivering the packets which have accumulated into the buffer during the link layer handoff. If the available bandwidth of the new link is equal to the sending rate of the Correspondent Node or smaller than the rate, the wireless link of the new Access Router will become saturated, thus delaying the delivery of the buffered packets and also fresh packets arriving. The resending of packets in Figure 16 for FMIPv6 and FMIPv6 with bicasting is due to this. This behaviour is analyzed in more detail in publications P2 and P3 for Fast Handovers for Mobile IPv6.

Table 4 extends the performance comparison to Mobile IPv6, HMIP, F-HMIP, FF-HMIP and S-MIP using the results from publications P1 and P2. The results for HMIP can be extrapolated from the results for Mobile IPv6,

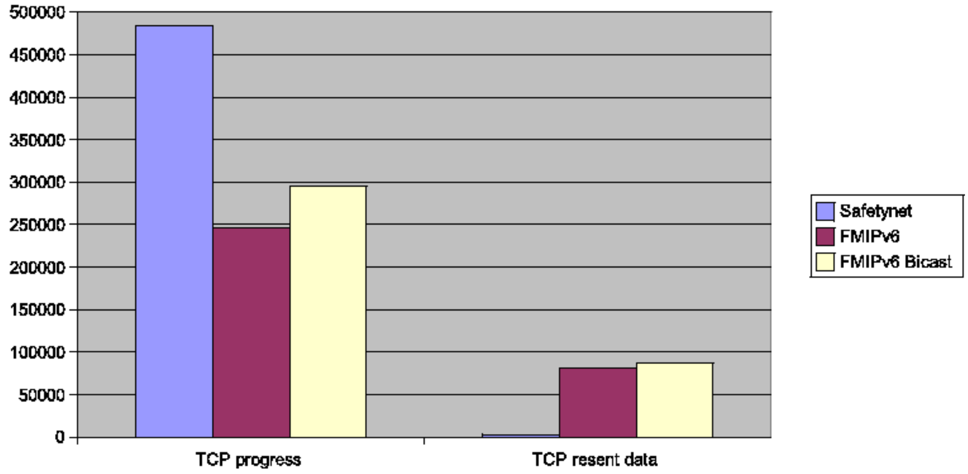

Figure 16: Experimental performance comparison for localized mobility management.

since the hierarchical registration scheme mitigates the impact of the network latency between the Home Agent and the Mobile Router. In the case of Mobile IPv6 (NEMO) handoff in P1, this part of the handoff contributed to 20 ms of the total latency of 1780 ms. The results for S-MIP, F-HMIP and FF-HMIP are extrapolated from the results for FMIPv6. F-HMIP and FF-HMIP do not change the buffering mechanism in FMIPv6, and therefore they would suffer from the same performance limitations as FMIPv6. The model used in design of S-MIP aims to eliminate the impact of network latencies between the different network elements, but does not address the more critical element of link layer handoff latency. The link layer handoff latency would have the same effect on an implementation of S-MIP in the testbed used in P2 and P3 as for FMIPv6, since the receiving of packets in S-MIP is interrupted for the duration of the link layer handoff as in FMIPv6. Therefore, S-MIP would perform similarly as FMIPv6 in Figure 16. For the synchronized packet delivery mechanism to improve the performance of S-MIP over FMIPv6, the latencies in the processing of packets and the network latencies in the wired part of the testbed would have needed to be significantly higher than in the experimental testbed. Therefore, the performance of S-MIP was approximated to be the same as for FMIPv6.

The performance differences can be explained by the differences in the functionality of the protocols. FMIPv6 and all the protocols derived from it avoid packet loss for UDP traffic by utilizing buffering at the new Access Router. However, this is not sufficient for a seamless handoff when the bandwidth of the flow to the Mobile Router is close to the bandwidth available at the new link and the handoff latency is significant, and thus the Fast Handovers for Mobile IPv6 handoff shows a large performance impact on TCP. The use of bicasting allows the Mobile Router to receive packets during the handoff with the Fast Handovers for Mobile IPv6 and the SafetyNet protocols. However, redelivery of already received packets from the buffer after the link layer handoff has a large negative impact on TCP, as discussed in publication P2. The use of selective delivery of packets from the buffer after the link layer handoff in SafetyNet ensures that the limited wireless link bandwidth is used efficiently and that TCP does not see any duplicates, thus minimizing the impact of the handoff.

Table 4: Extended comparison of intra-domain handoff performance.

Name of Scheme	**Impact of handoff on TCP**	**Impact of handoff on UDP**
FMIPv6	49%	0%
FMIPv6 with bi-casting	39%	0%
S-MIP*	49%	0%
HMIP**	20%	17,5%
F-HMIP***	49%	0%
FF-HMIP***	49%	0%
SafetyNet	0%	0%

*Results for S-MIP are extrapolated from FMIPv6 performance in P2. **Results for HMIP are extrapolated from performance of NEMO in P1. ***Results for F-HMIP and FF-HMIP are extrapolated from FMIPv6 performance in P2.

5.2 Performance

In this section, the performance overhead of using the proposed mobility management archictecture is compared with other proposals. The overheads are compared for network mobility management and for localized mobility management.

The use of NEMO incurs protocol header and routing overheads. The proposed architecture employs OptiNets Route Optimization protocol to reduce these overheads for mobility capable mobile network nodes. In publication P1, the effectiveness of OptiNets Route Optimization protocol is compared with NEMO and Mobile IPv6 routing and it is shown that the use of OptiNets Route Optimization reduces the communications overheads when multiple Mobile Network Nodes are communicating, even for frequent handoffs. Further, the use of OptiNets reduces the end-to-end network latency which may improve TCP performance as dicussed in P1. An overview of the experimental results from P1 is given below and extended to to other route optimization schemes.

The TCP performance of a NEMO Local Fixed Node, a Visiting Mobile Node with out route optimization, a Visiting Mobile Node with Mobile IPv6 route optimization (i.e. avoiding the Home Agent of the Visiting Mobile Node), and a Visiting Mobile Node with OptiNets (i.e. avoiding both the Home Agent of the Visiting Mobile Node and the Home Agent of the Mobile Router) is compared experimentally using the methodology described in Section III.D of publication P1.

The performance is measured in a static case, in which the Mobile Router is located in a foreign network and in a dynamic case, in which the Mobile Router moves between two foreign networks. The results for the static case, as shown in Figure 17, indicate that the performance of the other schemes decreases as the latency between the MR and the Home Agent of the Mobile Router increases, whereas the performance of the OptiNets scheme is not affected. The results for the dynamic case in Figure 18 show that the performance of the OptiNets scheme is comparable with the static case. The TCP performance of the other schemes is the same as in the static case, and therefore only the NEMO Local Fixed Node performance is shown for comparison.

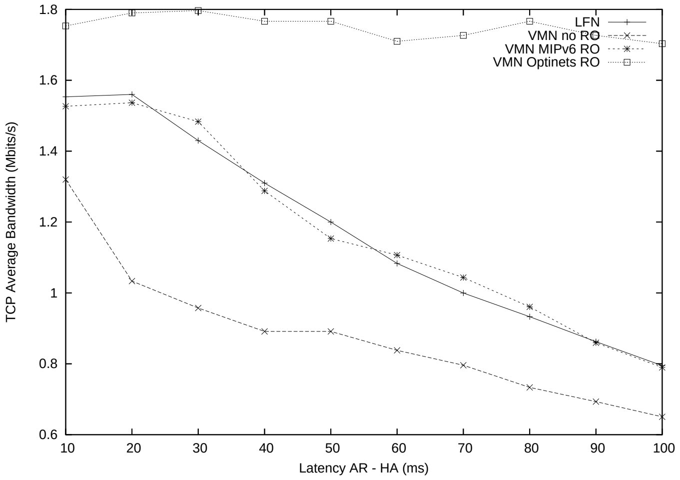

Figure 17: TCP Performance Comparison in Static Case.

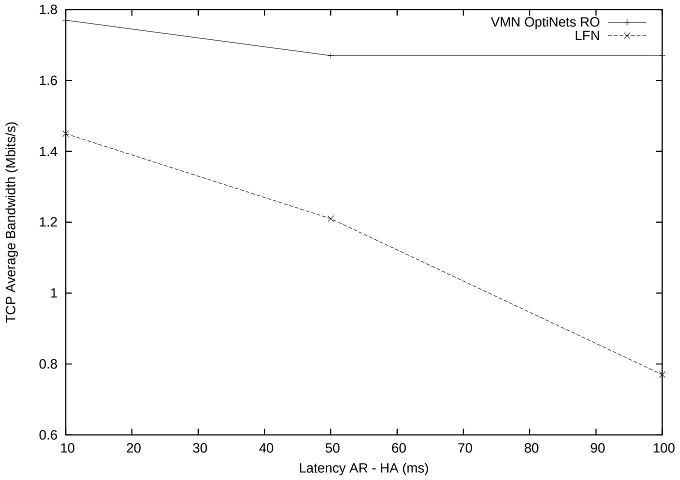

Figure 18: TCP Handoff Performance Comparison for LFN, MIPv6 MN OptiNets RO.

In addition to the analysis done in P1, the OptiNets scheme is compared here with state of the art route optimization schemes. The TCP performance gained from using ORC scheme [88] depends on the vicinity of Correspondent Routers to Correspondent Nodes. If the Correspondent Router is on the shortest (or fastest) routing path between the Mobile Router and the Correspondent Node, the ORC scheme would perform comparably to OptiNets. However, this would be the best case for ORC. Jeong et al's [51] proposal would provide similar TCP performance as OptiNets. The TCP performance with the HIP based mobile network protocol would depend on the processing power of the Mobile Router and the Correspondent Node and the used encryption and authentication algorithms. With sufficient computing resources the HIP based approach would perform similarly to the OptiNets based scheme.

The per packet header overhead did not have an effect in the previous two measurements, since the TCP performance was limited by the end-to-end latency and not by the available bandwidth (2 Mbps), due to the use of the default TCP window size. In Figure 19 the relative overhead of the different schemes is analyzed. A 64 kbps Constant Bit Rate stream with 220 byte packets as traffic is used and the amount of signaling and per packet protocol overhead is calculated relative to the total amount of data sent over the air interface between the Mobile Router and the Access Router. It can be seen that the use of OptiNets incurs the smallest total overhead of the NEMO variants regardless of the handoff frequency, when one Mobile Network Node is communicating up to one handoff per second, which is the maximum frequency specified in [52]. The results show that the use of OptiNets reduces the per packet overhead to a level comparable to that of a route optimized Mobile IPv6 Mobile Node connecting directly to the Access Router, bypassing the Mobile Router.

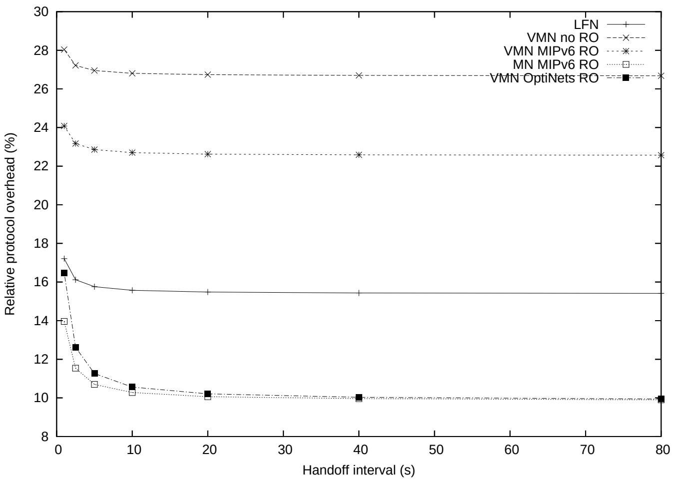

Figure 19: Overhead Comparison for 1 Mobile Network Node running Constant Bit Rate Traffic with varying Handoff Interval.

The effect of multiple Mobile Network Nodes with the same traffic type as in Figure 19 is analyzed and the results given in Figure 20 indicate that the relative overheads of NEMO and OptiNets decrease as the number of MNNs increases. This is due to the aggregation of the mobility signaling.

In this introduction, the comparison presented above from publication P1 is extended to Jeong et al's Proxy Mobile Router proposal and HIP Mobile Router scheme using experimentally measured message sizes for Jeong et al's proposal shown in Table 6 and for HIP shown in Table 5. Message sizes and calculations from publication P1 are used for OptiNets. For one Mobile Network Node, the over the air overhead between the Mobile Router and the Access Router of OptiNets is slightly higher (72 bytes) than that of Jeong et al's proxy based scheme, due to the larger signaling overhead of running DHCPv6 with Prefix Delegation (280bytes) when compared with proxy neighbor discovery used in Jeong et al's proposal which accounts to 208 bytes.

Table 5: HIP Network Mobility Message Sizes in Bytes.

Name of Message	Size	Use
I1	80	Start
R1	800	Start
I2	864	Start
R2	168	Start
Readdress M1	288	Handoff
Readdress M2	256	Handoff
Readdress M3	232	Handoff

Table 6: Mobile Router Proxy Route Optimization Message Sizes in Bytes.

Name of Message	Size	Use
Neighbor Solicitation for DAD	64	Handoff
Neighbor Solicitation for Care-of Address	72	Handoff
Neighbor Advertisement for Care-of Address	72	Handoff

However, in OptiNets the DHCPv6 signaling is run once regardless of the number of Mobile Network Nodes whereas in the Proxy MR scheme each Mobile Network Nodes results in 208 bytes of signaling. Therefore, as the number of Mobile Network Nodes increases to 2 or more, the overhead of OptiNets becomes lower than that of the Proxy Neighbor Discovery Scheme.

For HIP based network mobility, the overhead is at least 1912 bytes for the initiation of the HIP security associations at the start of the session between the Mobile Network Node and the Correspondent Node[7]. Then every time the Mobile Router moves, that is changes its Care-of Address, the updating of the security associations incurs an overhead of 776 bytes per Mobile Network Node. These figures assume that the RSA signature algorithm [24] is used with HIP. However, HIP is not directly comparable to NEMO and Mobile IPv6 based network mobility due to the increased security provided by HIP, unless it is used solely for the purpose of providing connectivity to the Mobile Network Nodes.

The use of a localized mobility management protocol incurs overheads from both the signaling and packet delivery mechanisms. These overheads occur both on the radio link between the Mobile Router and the Access Router and also in the wired part of the network. Table 7 compares the over the air overheads for the localized mobility management protocols and Table 8 the over the wire overheads. The signaling overheads of the protocols do not vary much except for FF-HMIP which combines the signaling of FMIPv6 and HMIPv6. However, as analyzed in publication P2, if TCP is used and the retransmissions of TCP are counted towards the cost of running a protocol, the differences in the total costs between the protocols become significant. Figure 21 illustrates these differences for FMIPv6, FMIPv6 with

---

[7] The delegation of authority from the Mobile Network Nodes to the Mobile Router requires sending of larger certificates and the overhead would be several hundreds of bytes larger.

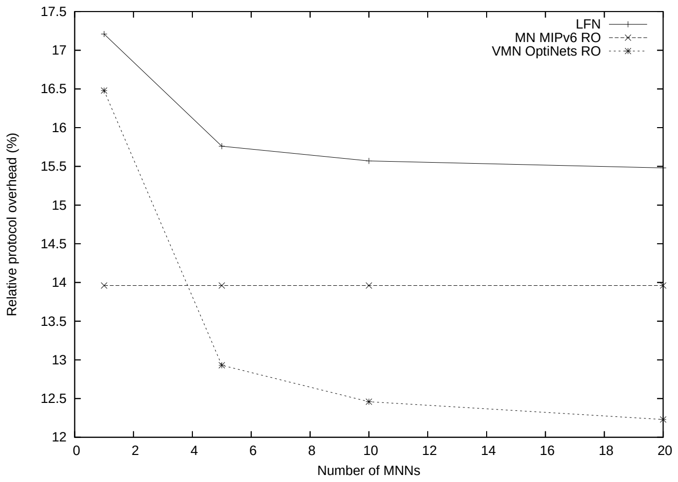

Figure 20: Overhead Comparison for a NEMO Local Fixed Node, OptiNets Route Optimization and Mobile IPv6 Mobile Node, with varying Number of MNNs.

bicasting and SafetyNet. Based on the analysis in Table 4, the costs for S-MIP, F-HMIP and FF-HMIP can be extrapolated to be close to those of FMIPv6.

5.3 Sparetime usage

The caching architecture proposed in publication P6 enables more efficient utilization of available low cost wireless bandwidth by use of prefetching of data to the roadside cache servers and transfer of the cache contents to the mobile cache server using unutlized bandwidth. The effectivenesss of the scheme depends on the caching algorithms used and content requested by users. With full prediction, i.e. the caching algorithm can predict all the content requested by users, and a sufficient number of WLAN hotspots, all non-real time content could be delivered via the roadside cache servers. The use of the localized road side cache servers together with the mobile cache server as proposed architecture increases the efficiency of cache updates by

Table 7: Comparison of over the air overheads of the protocols.

Name of Scheme	Signaling overhead	Data transmission overhead
FMIPv6	328 bytes	40 bytes per packet
FMIPv6 with bicasting	328 bytes	40 bytes per packet + bicasted packets
S-MIP*	328 bytes	40 bytes per packet
HMIP	160 bytes	40 bytes per packet
F-HMIP	328 Bytes	40 bytes per packet
FF-HMIP	488 bytes	80 bytes per packet
SafetyNet	378 bytes	Lost packets + 40 bytes for each lost packet

*Overheads for S-MIP are extrapolated from FMIPv6 overheads.

Table 8: Comparison of over the wire overheads of the protocols.

Name of Scheme	**Signaling overhead**	**Data transmission overhead**
FMIPv6	184 bytes	40 bytes per packet
FMIPv6 with bi-casting	232 bytes	40 bytes per packet
S-MIP*	184 bytes	40 bytes per packet
HMIP	160 bytes	40 bytes per packet
F-HMIP	184 bytes	40 bytes per packet
FF-HMIP	344 bytes	80 bytes per packet
SafetyNet	232 bytes	40 bytes per packet

*Overheads for S-MIP are extrapolated from FMIPv6 overheads.

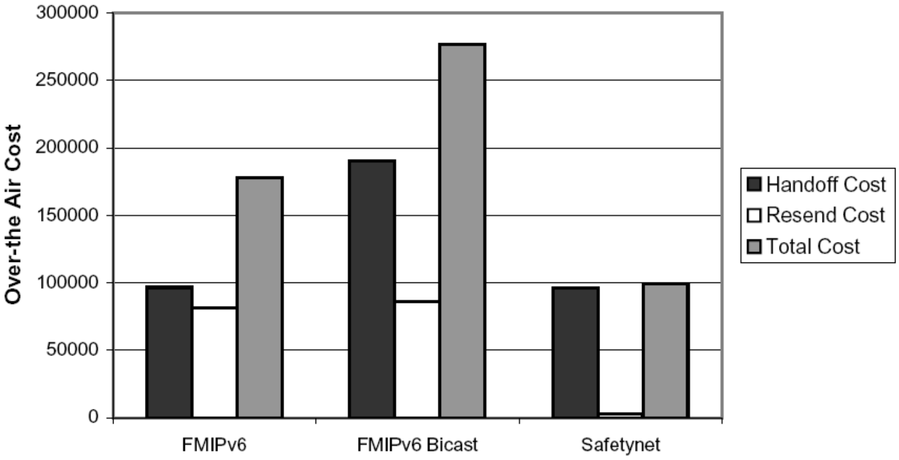

Figure 21: Total over the air cost comparison for localized mobility management.

up to 100% over the use of only a mobile cache server which retrieves data from remote servers, as shown in publication P6.

The Mobile Access Router (MAR) proxy architecture suggests a somewhat similar architecture, involving a proxy server in the fixed network and proxy client in the mobile network [82]. However the focus is more on efficient use of WWAN networks. The methods used in MAR and [13] include compression of data, caching of tcp connections to minimize the delay from start-up of new connections and transforming of web pages to suit the capabilities of a mobile device. These approaches could be used to further increase the performance of the architecture proposed in this dissertation.

5.4 Security

The proposed architecture has the goal or criteria of providing a mobility management framework for mobile networks without introducing new vulnerabilities. Section 4.5 presented the security of the architecture. In this section, the architecture is evaluated according to the following common security criteria used in networking:

1. **Integrity**, it should not be possible for an attacker to tamper with messages in transit.
2. **Source authentication**, it should not be possible for an attacker to pose as one of the participants in the protocol.
3. **DoS resiliency**, it should not be possible for an attacker to halt the operation of the participants of the protocol or use the participants of the protocol to flood third parties with unwanted traffic.
4. **Confidentiality**, confidential contents should be protected from attackers able to hear the messages.

The infrastructure independent Make-Before-Break handoffs do not change NEMO signaling and as such are as secure as NEMO. NEMO is based on Mobile IPv6 which can be considered to be secure against attackers, as long as the Mobile Router or Home Agent, or the home AAA server are not compromised. This is due to the security of Mobile IPv6 being researched for a decade and no vulnerabilities have been discovered in the basic functionality of sending Binding Updates and receiving Binding Acknowledgements when IPsec is used with integrity protection [57], [58] to secure the signaling. Securitywise, the significant change in NEMO, is that the protocol extends Mobile IPv6 to allow the Home Agent to reroute traffic flowing to the mobile network prefix instead of a single Home Address. The mechanism used in Mobile IPv6 for authorizing Binding Updates to the Home Agent is based on IPsec security association for the Home Address of a Mobile Node. In NEMO, there is an access control list in the Home Agent which is used for binding the prefix scoped Binding Updates to the Home Address. If this mechanism is implemented and used properly, NEMO signaling can be considered secure.

As with standard NEMO, a rogue Mobile Network Node could cause a denial-of service (DoS) attack on the wireless link between the Mobile Router and the Access Router. The scope of this threat can be reduced by using access control mechanisms in the Mobile Network to prevent unauthorized access and by enabling auditing. Further, Quality of Service mechanisms can be deployed in the Mobile Router to prevent hogging of resources by a single Mobile Network Node and to ensure fair sharing of the resources.

SafetyNet changes Fast Handovers for Mobile IPv6 protocol by introducing bicasting of packets and selective delivery of packets from the buffer of the new Access Router. These changes should not open up new vulnerabilities, and therefore security mechanism detailed in [40] should be sufficient to protect the participants of the protocol as well as third parties against attackers targeting the protocol.

The OptiNets route optimization scheme uses a key established with the Handover Key Protocol with DHCP message authentication [29] to ensure that only Mobile Routers authorized to receive prefixes can get them and that an attacker can not pose as the Access Router. Further the DHCPv6 message authentication ensures that the packets can not be tampered in transit. To ensure that a rogue Mobile Router can not starve the Access Router of available OptiNet network prefixes, the amount of prefixes available to each

Mobile Router needs to be limited. Since the prefixes are not confidential, the messages do not need to be encrypted.

The bandwidth fuelling cache architecture is protected against attacks from attackers outside the Mobile Network. However, if the attacker is a rogue Mobile Network Node, it may be able to request large amounts of data from the Mobile Cache server, resulting in flooding of the wireless link between the Roadside cache server and the Mobile Router, thus preventing valid cache requests from being fulfilled. To prevent this attack from succeeding to starve the other cache users, the Mobile Cache Server and the Road Side Cache Server need to connect the cache update requests with user or Mobile Network Node identities requesting the content and balance the load from the different users. Further, cache content retrieval packets will be marked with user specific IPv6 flowlabels. This enables the Access Router to use different traffic queues to enforce fair sharing of the wireless link resources.

5.5 Deployability

The solutions should require as few changes to entities in the network as possible. The architecture is designed to use standard IPv6 mobility protocols as building blocks to minimize the changes to Mobile Nodes, Mobile Routers, access and home network infrastructure and Correspondent Nodes.

The use of infrastructure independent Make-Before-Break handovers is transparent to Correspondent Nodes, Home Agents and does not require any support from the Access Network infrastructure. However, it does require the capability in the Mobile Router to connect to the previous and new access network simultaneously for the duration of the handoff. In the case of a horizontal handoff between two access networks of the same type, this often translates to the requirement of having an additional radio interface. However, the work done by Ramani et al. in [90] suggests that the combination of fast switching between two access points in 802.11 and the use of buffering together with virtualized connectivity as suggested in [15] may enable the use of infrastructure independent Make-Before-Break handoffs with a single radio interface. Further, equipping a Mobile Router with an additional interface may be feasible for Mobile Routers serving multiple Mobile Network Nodes, due to increased network performance during handoffs for all the nodes. This would be the case for example for a Mobile Router located in a bus or a train serving the passengers and on-board embedded systems.

The use of SafetyNet localized mobility management protocol requires support from the Mobile Node and the access network. It is transparent to the Home Agent and the Correspondent Nodes. In the Access Network, the Access Routers need to have sufficient memory to enable buffering of packets during the handoff. The buffering requirements in the Access Routers are the same as for Fast Handovers for Mobile IPv6, with L_{buff} depicting the length of the buffer, $T_{handoff}$ handoff latency and Bw data rate:

$L_{buff} = T_{handoff} * Bw$

In a 802.11g WLAN network with a theoretical maximum data rate of 54 Mbps, the maximum required buffer for a Mobile Router using all the bandwidth of an Access Point would be approximately 1.08 Mb for a handoff taking 200 ms. Therefore, the buffering requirements should not limit the deployment.

OptiNets route optimization requires changes to the Mobile Router and the Mobile Network Nodes which take advantage of the protocol. However, it is backward compatible with Mobile Network Nodes not supporting the protocol. The Access Routers need to support DHCPv6 prefix delegation to enable the use of the OptiNets protocol. Correspondent Nodes taking part in the OptiNets route optimization only need to support Mobile IPv6 route optimization to take advantage of the scheme.

Bandwidth fuelling cache architecture requires protocol support from the Access Network infrastructure, the Mobile Router and the Mobile Cache Server. The Road Side Cache Servers can be integrated into the Access Routers serving the road side networks or be stand alone servers located in close proximity of the road side networks. If the road side networks are connected to the core access network using fast links, they can use a single roadside cache server. However, if the roadside networks are connected to the core networks using slow links, which is often the case for WLAN deployment, the architecture would benefit from denser deployment of Roadside Cache Servers, possibly even of colocating them with WLAN access points.

The security architecture proposed in the dissertation utilizes standards based protocols from the Internet Engineering Task Force, as discussed in Sections 4.5 and 5.4, and modifies only the Dynamic Home Agent Address Discovery protocol to enable secure discovery of Home Agents. When compared with the Internet Engineering Task Force proposal of replacing the Dynamic Home Agent Address Discovery protocol with a DHCPv6 based solution, the secure DHAAD mechanism proposed in this dissertation enables configuration of the Home Agent from any network, even from ones which do not have a trust relationship with the Home Network. This enables the deployment of the Home Agent for example in the de-militarized zone of a corporate network while using any Internet Service Provider's access network for connectivity.

The architecture proposed in this dissertation does not require support from Access Networks or Correspondent Nodes, or Mobile Network Nodes for seamless handoffs. However, it can take advantage of support from the access network to increase the handoff performance in non-optimal cases. Further, it can utilize additional mobility management capabilities in Mobile Network Nodes to increase the efficiency of communications with the help of limited support from the Access Network. In a heterogeneous environment, the architecture adds capabilities to the Mobile Router and the access network to increase the utilization of spare bandwidth in low cost networks through the SafetyNet handoff timing algorithm and the Bandwidth fuelling caching architecture.

6 DISCUSSION

In this section, the impact of the proposed solutions is discussed. The proposed architecture focuses on Mobile Routers able to connect to multiple access networks simultaneously. Currently, most mobile devices do not have this capability. An exception to this is mobile phones or data cards employing CDMA radio technology which enables them to connect to two base stations simultaneously. However, this is only possible when the base stations are connected to the same operators network. The emphasis on the design of radio, link, and network technologies has been on solutions that can cope with a wide range of conditions, for example UMTS networks support varying user movement rates from walking speed to users travelling in fast trains at over a hundred kilomteres per hour. This has lead to complex systems which are expensive to manufacture, deploy and use.

The ability to have multiple radio interfaces in a Mobile Router enables the use of less complex radio technologies when they are available and the rate of movement is slow enough. However, as discussed in Section 2.1, it is crucial that the Mobile Router can switch between the wireless technologies without disrupting the communications of the Mobile Nodes in the Mobile Network. The mobility management protocols being standardized at the moment in the MIPSHOP [68] and MIP6 [67] working groups of the Internet Engineering Task Force [49], such as Hierarchical Mobile IPv6 and Fast handovers for Mobile IPv6, have been designed for mobility management in a Break-Before-Make environment in which a Mobile Node or Router will lose connectivity with its current network before establishing connectivity with a new one. This design impacts the performance in Make-Before-Break handoffs as discussed in publication P2 for Fast Handovers for Mobile IPv6 and in publication P1 for Mobile IPv6.

The architecture proposed in this dissertation enables seamless handoffs in a multi radio environment, when the Mobile Router is capable of Make-Before-Break handoffs within network technologies and between different network technologies. With seamless handoffs between the radio technologies, a Mobile Router can opportunistically take advantage of the cheaper and higher bandwidth WLAN networks to provide better service to the Mobile Network Nodes. When the low cost WLAN networks become unavailable or the rate of movement increases the tolerance of the coding mechanisms, the Mobile Router can resort to the higher cost, lower bandwidth WWAN radio technologies. By using the proposed SafetyNet protocol and handoff timing algorithm, this can be done in a way which maximizes the usage of the low cost networks without sacrificing application performance.

The deployment of the SafetyNet protocol in the access routers could be done without changing the hardware, since the buffer space required to support handoffs are low. The increase in network traffic from bi or n-casting is another potentially limiting factor to its deployment. However, the way the n-casting is used limits the impact to the wired section of the access network, since only a single copy of each packet is delivered over the wireless link to the Mobile Router.

The wired connection between the Access Routers of a single network is typically controlled by a single operator, and therefore the cost of running the protocol should not be prohibitive, as long as it does not require upgrading of the networking equipment connecting the Access Routers. Many wireless access networks have overprovisioned wired parts with the wireless last hop acting as the bottleneck. For example, WLAN access points often connect to a switched 100 Mbps or 1000 Mbps wired ethernet in corporate networks.

Thus, I believe that the use of SafetyNet would be feasible even in the networks of today. Further, the use of the OptiNets route optimization together with SafetyNet would reduce both the over-the air and the over-the wire overheads of the traffic and optimize the routing path, thus offsetting the handoff overheads of the SafetyNet protocol.

In this dissertation, the SafetyNet localized mobility management protocol was shown to improve the performance of downlink TCP traffic from the Access Routers to the Mobile Router due to the selective delivery of packets lost during the handoff. However, the SafetyNet protocol could be improved further to include recovery of packets sent uplink from the Mobile Router to the Access Network which are lost during the handoff period due to bit errors. A similar mechanism is already in use in the GPRS link layer control protocol as described in [94] in Section 6.9.1.2.2 in steps 11 and 12 for Break-Before-Make handoffs, allowing the Mobile Station and the new Serving GPRS Support Node, i.e. the new Access Router to resume sending of packets in both directions from the correct packet. Due to the use of Make-Before-Break handoffs in SafetyNet, the recovery of upstream packets would require additional signaling between the new and the previous Access Routers to retrieve the information (sequence numbers) of the packets the previous Access Router received from the Mobile Router during the handoff and a message from the new Access Router to the Mobile Router to request for the messages.

The seamless horizontal handoffs enable moving between different access points or base stations of the less complex network technologies without sacrificing the connection quality for Mobile Network Nodes. This allows Mobile Routers to use overlapping low cost networks from the same or different operators as long as they remain within the coverage area of the networks. For example in urban areas, there are often several WLAN networks available. With companies such as FON [41] providing ubiquitous WLAN coverage through consumer's home access points, the ability to perform seamless horizontal handoffs would enable continuous roaming within WLANs as long as the speed of movement would be relatively low. In a city environment, this would enable a Mobile Router to provide connectivity to travellers in buses and trains via overlapping WLAN networks.

As discussed in Section 3.1, there have been simulation studies discussing the limitations of the WLAN coding which could affect the throughput of IEEE 802.11 noticeably for high vehicular speeds. However, according to Gaertner [42] et al. speeds up to 50 km/h should not impact the performance. A simulation and experimental study done in a railroad environment [93] showed that speeds up to 90 miles per hour did not have a negative impact on the performance of 802.11b. Ott et al. showed that 802.11b could be used for providing Internet access with TCP to cars moving at speeds up to 180 km/h. Further, an experiment done by Amico and Lauss [20] using rockets suggests that 802.11b can be used even at speeds of up to 600 m/s, at least for uplink packets. Therefore, use of WLANs can be considered realistic even for vehicular Mobile Routers, especially in an urban environment. Further, the use of the proposed architecture would not limit the rate of movement for speeds up to 90 m/s due to the limitations of the coding in IEEE 802.11b and the transport protocols in a high mobility WLAN scenario discussed above.

An important characteristic of any technology is the cost of its deployment and use. The proposed architecture enables the seamless handoffs within and between access technologies with a cost that is comparable or lower to the currently standardized approaches. The use of route optimization and caching further increases the efficiency of the communications in a heterogeneous environment, by reducing the signaling and protocol overheads and enabling delay tolerant applications to focus their communications over low cost networks. This enables the use of the lower bandwidth networks for interactive or real time communications.

The results presented for the SafetyNet protocol and handoff timing and the infrastructure independent Make-Before-Break handoffs in the analysis section are applicable not only to Mobile Routers, but to Mobile Nodes in general. The infrastructure independent Make-Before-Break handoffs require the ability to connect to a new network before losing connectivity with the previous one. In many network types, such as WLAN and GPRS, this would require two network interfaces which would increase the size, cost and power consumption of a mobile device. Therefore, the technology may be more suitable to vehicular Mobile Routers which are less constrained by the power and size limitations and the extra cost may be justifiable by the seamless connectivity in legacy networks. However, it may be possible to use the scheme with a single network interface by utilizing virtualization as proposed in [15]. Although virtualization as such would not provide much benefit for link layer handoffs due to the switching delay, it would allow a Mobile Router or Mobile Node to avoid packet loss during the network attachment and network layer (Mobile IP or NEMO) handoff.

The security architecture enables roaming between multiple operators networks securely by making the configuration and security of the global mobility management services independent of the localized services. This allows the mobility service provider to act as an aggregator of the different access network providers networks, i.e. combinining the different access network provider's services to a single service which is provided to the users of the mobile network. The additional services of prefix delegation, localized mobility management and caching provided by the access providers allow improved service for the mobile users when available and reduce the use of wireless resources in the access networks. However, due to the access technology independent nature of the proposed global mobility management scheme, the Mobile Router can provide seamless roaming regardless of the capabilities of the access networks.

7 CONCLUSION

Deployment of a Mobile Router allows aggregation of mobility management and routing. In scenarios such as vehicle networks, it allows use of external antennas and external power sources, and can thus provide better connectivity to Mobile Network Nodes. Further, the aggregation of mobility management reduces mobility related signaling and allows use of simple Mobile Network Nodes which do not support mobility management.

Mobile Routers can be equipped with single or multiple wireless network interfaces. Use of a single radio technology enables a Mobile Router to provide service to the users of the mobile network according to the characteristics of the selected network technology. In a heterogeneous network environment there are often several wireless network technologies available simultaneously. These technologies have different characteristics, making some of them suitable for use at vehicular speeds at a higher cost while some provide high data rates at low cost but can not deal as well with the higher speeds. By dynamically selecting the technology which best matches the cost, speed and quality of service requirements of the users of the network, a Mobile Router can provide better service at a lower cost.

High speed mobility within the heterogeneous network environment would result in frequent handoffs. These frequent handoffs could disrupt the communications of the Mobile Network Nodes, if not handled carefully. Seamless handoffs, i.e. the ability to switch between the technologies without disrupting user traffic, are therefore a prerequisite for effective use of heterogeneous wireless networks for potentially high speed network mobility. Further, high speed mobility in areas covered by multiple short range WLAN networks results in frequent handoffs between the Access Points of the WLAN networks. Seamless horizontal handoffs are required for the use of overlapping WLAN networks to provide continuous connectivity to Mobile Network Nodes without disruptions.

This dissertation presented an architecture for network mobility management in heterogeneous IPv6 networks. The architecture enables a Mobile Router to provide seamless connectivity to users within the mobile network in spite of changes in the network point of attachment of the Mobile Router. The seamless connectivity is achieved using a localized mobility management scheme for infrastructure assisted vertical and horizontal handoffs. The architecture enables efficient use of network resources through optimized routing, caching, and handoff timing algorithms with support from the network infrastructure. However, roaming in legacy networks or between competing operators networks may result in the infrastructure support not being present. Seamless handoffs in these cases are supported through infrastructure independent Make-Before-Break handoffs.

The architecture was analyzed through experimental and numerical studies. The empirical analysis of the performance of the architecture validated the design in an indoor testbed. The numerical analysis extended the validation to a mobile environment with ideal cell and radio models. The analysis showed that the use of the architecture reduced the impact of handovers when compared with state of the art mobility management protocols, such as Fast Handovers for Mobile IPv6. Further, the performance overheads of the proposed architecture were shown to be in most cases smaller than those of the existing proposals. However, further work needs to be done using outdoor testbeds to analyze the impact of vehicular speeds and less than ideal radio environments on performance of the architecture.

Deployment of the proposed architecture would allow for leveraging of the complementing characteristics of the different network technologies to provide a seamless wireless overlay in which the most suitable network could be used according to the situation. The seamless handoffs made possible by the architecture are a key enabling factor in the use of heterogeneous networks for potentially high speed Mobile Routers. The caching and route optimization would make the use of potentially scarce Wireless Wide Area Network resources more efficient by exploiting unused network capacity of Wireless Local Area Networks and by reducing the overhead of the mobility management.

REFERENCES

[1] Technical Specification Group Services 3rd Generation Partnership Project and System Aspects. 3g ts 23.060 version 3.2.1 (2000-01), general packet radio services (gprs) stage 2.

[2] A. Acharya, Li Jun, B. Rajagopalan, and D. Raychaudhuri. "mobility management in wireless ATM networks". *Communications Magazine, IEEE*, 35(11):100–109, Nov 1997.

[3] G.R. Aiello and G.D. Rogerson. "ultra-wideband wireless systems". *Microwave Magazine, IEEE*, 4(2), Jun 2003.

[4] Apple. Motion jpeg format. http://developer.apple.com/documentation/QuickTime/QTFF/qtff.pdf.

[5] T. Aura. Cryptographically generated addresses, March 2005. internet-rfc : RFC3972.

[6] S. Aust, D. Proetela, N.A. Fikouras, C. Paupu, and C. Gorg. "Policy based Mobile IP handoff decision (POLIMAND) using generic link layer information.". In *Proceedings 5th IEEE International Conferenco on Mobile and Wireless Communication Networks*, oct 2003.

[7] Omri Bahat and Armand M. Makowski. Optimal replacement policies for non-uniform cache objects with optional eviction. In *IEEE INFOCOM 2003*, March 2003.

[8] Guruduth Banavar, James Beck, Eugene Gluzberg, Jonathan Munson, Jeremy Sussman, and Deborra Zukowski. Challenges: an application model for pervasive computing. In *MobiCom '00: Proceedings of the 6th annual international conference on Mobile computing and networking*, pages 266–274, New York, NY, USA, 2000. ACM Press.

[9] Christian Bettstetter, Hans-Jörg Vögel, and Jörg Eberspächer. GSM phase 2+ general packet radio service GPRS: Architecture, protocols, and air interface. *IEEE Communication Surveys*, 2(3), 1999.

[10] V. Brik, A. Mishra, and S. Banerjee. "Eliminating handoff latencies in 802.11 WLANs using multiple radios: applications, experience, and evaluation". In *Internet Measurement Conference 2005*, 2005.

[11] A. Campbell, J. Gomez, S. Kim, and C. Wan. "Comparison of IP Micro-mobility Protocols". *IEEE Wireless Communications*, pages 72–82, February 2002.

[12] Pei Cao and Sandy Irani. "cost-aware www proxy caching algorithms". In *USENIX Symposium on Internet Technologies and Systems*, 1997.

[13] R. Chakravorty, J. Cartwright, and I. Pratt. GPRSWeb: Optimizing the Web for GPRS links. In *Proceedings of ACM Conference on Mobile Systems, Applications and Services (MobiSys)*, San Francisco, CA, May 2003.

[14] R. Chakravorty, A. Clark, and I. Pratt. "Optimizing Web Delivery over Wireless Links: Design, Implementation and Experiences.". *IEEE Journal of Selected Areas in Communications (JSAC)*, 23(2):402–416, feb 2005.

[15] R. Chandra and P. Bahl. Multinet: Connecting to multiple ieee 802.11 networks using a single wireless card. In *Proceedings of ieee-infocom 2004*, Hong Kong, March 2004. IEEE.

[16] Ratner D., Reiher P., Popek G. J., and Kuenning G. H. Replication requirements in mobile environments. In *Dial M M for Mobility: 1st International Workshop on Discrete Algorithms and Methods for Mobile Computing and Communications*, Budapest, Hungary, October 1997. held in conjunction with ACM/IEEE MobiCom'97.

[17] G. Daley, S. Narayanan, and G. Perkins. "A probabilistic scheme for fast Router Advertisement responses in IPv6". internet-draft, feb 2005. work in progress.

[18] G. Daley and E. Nordmark. "Deterministic Fast Router Advertisement Configuration". internet-draft, oct 2004. work in progress.

[19] Greg Daley and Richard Nelson. Duplicate address detection optimization using ipv6 multicast listener discovery, February 2003. draft-daley-ipv6-mcast-dad-02.txt.

[20] W. D'Amico and M. Lauss. Wireless local area network flight demonstration for high doppler conditions. *John Hopkins APL Technical Digest*, 25(4), 2004.

[21] V. Devarapalli and F. Dupont. Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture, April 2007. internet-rfc : RFC4877.

[22] V. Devarapalli, R. Wakikawa, A. Petrescu, and P. Thubert. Network mobility (NEMO) basic support protocol, January 2005. internet-rfc : RFC3963.

[23] Mark Dunlop and Stephen Brewster. The challenge of mobile devices for human computer interaction. *Personal Ubiquitous Comput.*, 6(4):235–236, 2002.

[24] D. Eastlake. RSA/SHA-1 SIGs and RSA KEYs in the Domain Name System (DNS), May 2001. internet-rfc : RFC3110.

[25] D.E. Eastlake. Secure domain name system dynamic update, April 1997. internet-rfc : RFC2137.

[26] G. Giaretta (ed.). Mobile IPv6 bootstrapping in split scenario. internet-draft, December 2006. work in progress.

[27] Hesham Soliman (ed.). Hierarchical mipv6 mobility management (revised), March 2007. work in progress.

[28] R. Droms (ed.). Dynamic Host Configuration Protocol for IPv6 (DHCPv6), July 2003. internet-rfc : RFC3315.

[29] R. Droms (ed.) and W. Arbaugh (ed.). Authentication for DHCP Messages, June 2001. internet-rfc : RFC3118.

[30] EIA/TIA. Cellular radio-telecommunications intersystem operations, tech. report. is-41 revision c. Technical report, EIA/TIA, 1995.

[31] C. Eklund, R.B. Marks, K.L. Stanwood, and S Wang. "ieee standard 802.16: a technical overview of the wirelessman air interface for broadband wirelessaccess". *IEEE Communications Magazine*, 40(6):98–107, Jun 2002.

[32] K. Elmalki and H. Soliman. "Simultaneous Bindings for Mobile IPv6 Fast Handovers". internet-draft, jul 2005. work in progress.

[33] Thierry Ernst. Network mobility support terminology, November 2006. work in progress.

[34] Cheng Wei Lee et al. "a framework of handoffs in wireless overlay networks based on mobile ipv6". *IEEE Journal on Selected Areas in Communications*, 23(11):2118–2128, nov 2005.

[35] H. Jung et al. "Fast Handover for Hierarchical Mobile IPv6 (F-HMIPv6)". internet-draft, apr 2005. work in progress.

[36] M. Ibnkahla et al. High speed satellite mobile communications: Technologies and challenges. *Proceedings of the IEEE*, 92(2):312–339, 2004.

[37] P. Nikander et al. Mobile IP Version 6 Route Optimization Security Design Background, December 2005. internet-rfc : RFC4225.

[38] P. Vidales et al. "autonomic system for mobility support in 4g networks". *IEEE Journal on Selected Areas in Communications*, 23(12):2288–2304, dec 2005.

[39] Q. Zhang et al. "efficient mobility management for vertical handoff between wwan and wlan",. *IEEE Communications Magazine*, 41(11):102–108, Nov 2003.

[40] V. Narayanan et al. Establishing Handover Keys using Shared Keys, March 2007. draft-vidya-mipshop-handover-keys-aaa-04.txt.

[41] http://www.fon.com.

[42] G. Gaertner and V. Cahill. "understanding link quality in 802.11 mobile ad hoc networks". *IEEE Internet Computing*, 8(1):55–60, Jan 2004.

[43] Q. Guo, J. Zhu, and X. Xu. "an adaptive multi-criteria vertical handoff decision algorithm for radio heterogeneous network". In *proceedings of of ICC 2005*, volume 4, pages 2769–2773, may 2005.

[44] Y. Gwon, J. Kempf, and A. Yegin. "Scalability and robustness analysis of mobile IPv6, fast mobile IPv6, hierarchical mobile IPv6, and hybrid IPv6 mobility protocols using a large-scale simulation". In *IEEE International Conference on Communications*, volume 7, pages 4087–4091, jun 2004.

[45] Harri Holma and Antti Toskala. *"WCDMA for UMTS: Radio Access for Third Generation Mobile Communications"*. Wiley, John and Sons, Incorporated, 3 edition, 2004.

[46] Robert Hsieh and Aruna Seneviratne. A Comparison of Mechanisms for Improving Mobile IP Handoff Latency for End-to-End TCP. In *ACM MobiCom'03*, San Diego, USA, sep 2003.

[47] Robert Hsieh, Zhe Guang Zhou, and Aruna Seneviratne. S-MIP: A Seamless Handoff Architecture for Mobile IP. In *IEEE INFOCOM 2003*, 2003.

[48] Ieee80216e committee, http://ieee802.org/16/tge.

[49] Internet Engineering Task Force, http://www.ietf.org.

[50] ISO. ISO/IEC 13818-1:2000, Generic coding of moving pictures and associated audio information: Systems, edition 2.

[51] Jaehoon Paul Jeong, Kyeongjin Lee, Jungsoo Park, and Hyoungjun Kim. Nd-proxy based route and dns optimizations for mobile nodes in mobile network, February 2004. draft-jeong-nemo-ro-ndproxy-02.txt.

[52] D. Johnson, C. Perkins, and J. Arkko. Mobility Support in IPv6, June 2004. internet-rfc : RFC3775.

[53] David B Johnson and David A Maltz. Dynamic source routing in ad hoc wireless networks. In Imielinski and Korth, editors, *Mobile Computing*, volume 353. Kluwer Academic Publishers, 1996.

[54] Ved P. Kaflei, Eiji Kamioka, and Shigeki Yamada. Comoroho: Cooperative mobile router-based handover scheme for long-vehicular multihomed networks. *IEICE Transactions on Communications*, E89-B(10), oct 2006.

[55] Hyunsik Kang, Keecheon Kim, Sunyoung Han, Kyeong-Jin Lee, and Jung-Soo Park. Route optimization for mobile network by using bi-directional between home agent and top level mobile router, June 2003. draft-hkang-nemo-ro-tlmr-00.txt.

[56] Nadjia Kara, Omneya Issa, and Alain Byette. Real 3g wcdma networks performance analysis. In *LCN '05: Proceedings of the The IEEE Conference on Local Computer Networks 30th Anniversary*, pages 586–592, Washington, DC, USA, 2005. IEEE Computer Society.

[57] S. Kent and R. Atkinson. IP Authentication Header, November 1998. internet-rfc : RFC2402.

[58] S. Kent and R. Atkinson. IP Encapsulating Security Payload (ESP), November 1998. internet-rfc : RFC2406.

[59] D. Kim and D. Sung. Characterization of soft handoff in cdma systems. *IEEE Transactions on Vehicular Technology*, 48(4), jul 1999.

[60] D.N. Knisely, S. Kumar, S. Laha, and S. Nanda. "evolution of wireless data services: Is-95 to cdma2000". *IEEE Communications Magazine*, 36(10):140–149, Oct 1998.

[61] R. Koodli. Fast Handovers for Mobile IPv6, July 2005. internet-rfc : RFC4068.

[62] R. Koodli. Fast Handovers for Mobile IPv6 (revised). internet-draft, October 2007. work in progress.

[63] C.H. Lee, J.R. Zheng, and C.M. Huang. SIP-based network mobility (SIP-NEMO) route optimization, October 2005. draft-ming-nemo-sipnemo-00.txt.

[64] George Y. Liu and Gerald Q. Maguire Jr. A class of mobile motion prediction algorithms for wireless mobile computing and communications. *MONET*, 1(2):113–121, 1996.

[65] Hosei Matsuoka, Takeshi Yoshimura, and Tomoyuki Ohya. A robust method for soft ip handover. *IEEE Internet Computing*, 7(2):18–24, 2003.

[66] J. McNair and F. Zhu. "vertical handoffs in fourth-generation multinetwork environments". *IEEE Wireless Communications*, 11(3):8–15, jun 2004.

[67] Internet Engineering Task Force, Mobility for IPv6 working group. http://www.ietf.org/html.charters/mip6-charter.html.

[68] Internet Engineering Task Force, Mobility for IP: Performance, Signaling and Handoff Optimization. http://www.ietf.org/html.charters/mipshop-charter.html.

[69] Arunesh Mishra, Minho Shin, and William Arbaugh. An empirical analysis of the ieee 802.11 mac layer handoff process. *SIGCOMM Comput. Commun. Rev.*, 33(2):93–102, 2003.

[70] S. Mohan and R. Jain. "two user location strategies for personal communication services". *IEEE Personal communications*, 1(1):42–50, 1994.

[71] S. Mohanty and I. F. Akyildiz. "a cross-layer (layer 2 + 3) handoff management protocol for next-generation wireless systems". *IEEE Transactions on Mobile Computing*, 5(10):1347–1360, oct 2006.

[72] Nick Moore. Optimistic duplicate address detection for ipv6, February 2005. draft-ietf-ipv6-optimistic-dad-05.txt.

[73] R. Moskowitz and P. Nikander. "Host Identity Protocol (HIP) Architecture", May 2006. internet-rfc : RFC4423.

[74] T. Narten, E. Nordmark, and W. Simpson. Neighbor Discovery for IP Version 6 (IPv6), December 1998. internet-rfc : RFC2461.

[75] E. Nordmark and M. Bagnulo. "shim6: Level 3 multihoming shim protocol for ipv6". internet-draft, May 2007. work in progress.

[76] Szabolcs Novaczki, Laszlo Bokor, and Sandor Imre. "a hip based network mobility protocol". *2007 International Symposium on Applications and the Internet Workshops (SAINTW'07)*, 0:48, 2007.

[77] IEEE LAN/MAN Standards Committee of the IEEE Computer Society. Ieee standard for information technology- telecommunications and information exchange between systems-local and metropolitan area networks-specific requirements-part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications-amendment 1: High-speed physical layer in the 5 ghz band, 1999.

[78] IEEE LAN/MAN Standards Committee of the IEEE Computer Society. "ieee standard for information technology- telecommunications and information exchange between systm - local and metropolitan area networks - specific requirements - part 11: Wireless lan medium access control (mac) and physical layer (phy) specification - amendment 2: Higher-speed physical layer (phy) extension in the 2.4 ghz band - corrigendum1", 1999.

[79] IEEE LAN/MAN Standards Committee of the IEEE Computer Society. Ieee standard for information technology-telecommunications and information exchange between systems-local and metropolitan area networks-specific requirements-part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications-amendment 4: Further higher-speed physical layer extension in the 2.4 ghz band, 2003.

[80] J. Ott and D. Kutscher. Drive-thru Internet: IEEE 802.11b for "automobile" users. In *INFOCOM 2004. Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies*, volume 1, page 373, Mar 2004.

[81] Sharon Oviatt. Multimodal system processing in mobile environments. In *UIST '00: Proceedings of the 13th annual ACM symposium on User interface software and technology*, pages 21–30, New York, NY, USA, 2000. ACM Press.

[82] Rodriguez P., Chakravorty R., Chesterfile J., Pratt I., and Banjee S. "MAR: a commuter router infrastructure for the mobile internet". In *Mobisys*, pages 217–230, 2004.

[83] Thubert P. and Molteni R. IPv6 Reverse Routing Header and its application to Mobile Networks, June 2004. draft-thubert-nemo-reverse-routing-header-05.txt.

[84] E. Perera, A. Seneviratne, and V. Sivaraman. Optinets: An architecture to enable optimal routing for network mobility. In *International Workshop on Wireless Ad-hoc Networks (IWWAN âĂŹ04)*, May 2004.

[85] Eranga Perera, Vijay Sivaraman, and Aruna Seneviratne. Survey on network mobility support. *SIGMOBILE Mob. Comput. Commun. Rev.*, 8(2):7–19, 2004.

[86] Charles Perkins. "ip mobility support for ipv4", Aug 2002. internet-rfc : RFC3344.

[87] Wakikawa R., Valadon G., and Murai J. "Migrating Home Agents Towards Internet-Scale Mobility Deployability". In *ACM 2nd CoNEXT Conference on Future Networking Technologies*, Lisboa, Portugal, December 2006.

[88] Wakikawa R., Koshiba S., and Uehara K. Orc: Optimized route cache management protocol for network mobility. In *Protocol for Network Mobility , Proceedings of the 10th International Conference on Telecommunication (ICT)*, Tahiti , Papeete, French Polynesia, February 2003.

[89] M. Rahnema. "overview of the gsm system and protocol architecture". *Communications Magazine, IEEE*, 31(4):92–100, Apr 1993.

[90] Ishwar Ramani and Stefan Savage. Syncscan: Practical fast handoff for 802.11 infrastructure networks, mar 2005.

[91] Ramachandran Ramjee, Thomas F. La Porta, S. Thuel, Kannan Varadhan, and S. Y. Wang. HAWAII: A domain-based approach for supporting mobility in wide-area wireless networks. In *ICNP*, pages 283–292, 1999.

[92] Helena Roeber, John Bacus, and Carlo Tomasi. Typing in thin air: the canesta projection keyboard - a new method of interaction with electronic devices. In *CHI '03: CHI '03 extended abstracts on Human factors in computing systems*, pages 712–713, New York, NY, USA, 2003. ACM Press.

[93] "study of high-speed wireless data transmission for railroad operation". Technical report, US Department of Transportation, Federal Railroad Administration, apr 2007. RR07-10.

[94] Technical Specification Group Services and System Aspects. General packet radio service (gprs);service description;stage 2;release 6. Technical report, 3rd Generation Partnership Project, 2006. 3GPP TS 23.060 V6.15.0.

[95] M. Shin, A. Mishra, and W. Arbaugh. "Improving the latency of 802.11 Hand-offs using Neighbor Graphs". In *Mobisys 2004*, Boston, USA, jun 2004.

[96] S. Sibecas, C.A. Corral, S. Emami, and G. Stratis. "on the suitability of 802.11a/ra for high-mobility dsrc". In *Vehicular Technology Conference, 2002. VTC Spring 2002. IEEE 55th*, volume 1, pages 229–234.

[97] Hesham Soliman, Claude Castelluccia, Karim El-Malki, , and Ludovic Bellier. Hierarchical mipv6 mobility management (hmipv6), July 2005. internet-rfc : RFC4140.

[98] Squid web caching proxy, http://www.squid-cache.org.

[99] C. Steger, P. Radosavljevic, and J.P. Frantz. "performance of ieee 802.11b wireless lan in an emulated mobile channel". In *Vehicular Technology Conference, 2003. VTC 2003-Spring. The 57th IEEE Semiannual*, volume 2, pages 1479–1483, 2003.

[100] Mark Stemm and Randy H. Katz. Vertical handoffs in wireless overlay networks. *Mob. Netw. Appl.*, 3(4):335–350, 1999.

[101] S. Thomson and T. Narten. Ipv6 stateless address autoconfiguration, December 1998. internet-rfc : RFC2462.

[102] P. Thubert and T.J. Kniveton. "Mobile Network Prefix Delegation". internet-draft, nov 2006. work in progress.

[103] Unlicensed mobile access. http://www.umatechnology.org.

[104] A. Valko. Design and performance of cellular access networks. In *IEEE Personal Communication, Special issue on IP-based Mobile Telecommunications Networks*, 2000.

[105] Stephen Williams, Maec Abrams, and Charles R. Standridge. Removal policies in network caches for world-wide web documents. In *ACM SigComm '96*, 1996. http://www.sigcomm.org/sigcomm96/papers/williams.html.

[106] Yang Xiao. "ieee 802.11n: enhancements for higher throughput in wireless lans". *IEEE Wireless Communications*, 12(6):82–91, Dec 2005.

[107] Ting Zhou, H. Sharif, M. Hempel, P. Mahasukhon, and Song Ci. Performance of ieee 802.11b in mobile railroad environments. In *Vehicular Technology Conference, 2005. VTC-2005-Fall. 2005 IEEE 62nd*, volume 4, pages 2527–2531, Sept 2005.

HELSINKI UNIVERSITY OF TECHNOLOGY LABORATORY FOR THEORETICAL COMPUTER SCIENCE RESEARCH REPORTS

HUT-TCS-A95	Timo Latvala Automata-Theoretic and Bounded Model Checking for Linear Temporal Logic. August 2005.
HUT-TCS-A96	Heikki Tauriainen A Note on the Worst-Case Memory Requirements of Generalized Nested Depth-First Search. September 2005.
HUT-TCS-A97	Toni Jussila On Bounded Model Checking of Asynchronous Systems. October 2005.
HUT-TCS-A98	Antti Autere Extensions and Applications of the A^* Algorithm. November 2005.
HUT-TCS-A99	Misa Keinänen Solving Boolean Equation Systems. November 2005.
HUT-TCS-A100	Antti E. J. Hyvärinen SATU: A System for Distributed Propositional Satisfiability Checking in Computational Grids. February 2006.
HUT-TCS-A101	Jori Dubrovin Jumbala — An Action Language for UML State Machines. March 2006.
HUT-TCS-A102	Satu Elisa Schaeffer Algorithms for Nonuniform Networks. April 2006.
HUT-TCS-A103	Janne Lundberg A Wireless Multicast Delivery Architecture for Mobile Terminals. May 2006.
HUT-TCS-A104	Heikki Tauriainen Automata and Linear Temporal Logic: Translations with Transition-Based Acceptance. September 2006.
HUT-TCS-A105	Misa Keinänen Techniques for Solving Boolean Equation Systems. November 2006.
HUT-TCS-A106	Emilia Oikarinen Modular Answer Set Programming. December 2006.
HUT-TCS-A107	Matti Järvisalo Impact of Restricted Branching on Clause Learning SAT Solving. August 2007.
HUT-TCS-A108	Henrik Petander A Network Mobility Management Architecture for a Heterogeneous Network Environment. December 2007.

ISBN 978-951-22-9098-7
ISBN 978-951-22-9099-4 (PDF)
ISSN 1457-7615