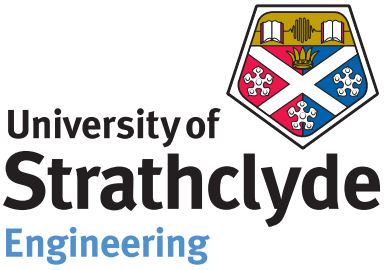


Intelligent Seamless Handoffs

Jorge Espí Alemañ

Centre for Intelligent Dynamic Communications (CIDCOM)
Department of Electronic & Electrical Engineering

University of Strathclyde

A thesis submitted for the degree of

Doctor of Philosophy

March 2013

This thesis is the result of the author's original research. It has been composed by the author and has not been previously submitted for examination which has led to the award of a degree.

Signed: Date:

To the memory of my loving father

Acknowledgements

This thesis would not have been possible unless the supervisor on Prof. John Dunlop and Dr. Robert Atkinson. I am grateful for their advice, support and encouragement and the time we have spent discussing the details of the work contained in this thesis. My thanks also to Dr. David Harle.

I would like to thank Dr. Qi Wang and Dr. Chong Shen as they introduced me on the everyday-life of the research work. I am also indebted to my many of my colleagues at the Communications Division, and very especially Neil Sinclair, Dr. Joan Cortes and Jakub Konka, for their friendship.

I would like to thank the University of Strathclyde, for giving me the opportunity of becoming part of it.

Finally, I would like to express my deepest gratitude to my family.

Abstract

The prevalence of multiple heterogeneous radio access technologies promises better quality of service to users. Users, provided with multihomed devices, may now access their desired services via just one or multiple interfaces simultaneously, and to change access network or interface according to their current preferences and ongoing service requirements so that they are *always best connected*. In this ideal scenario, network mobility becomes a broader technological challenge, as it incorporates user-centric satisfaction evaluation methods for the cost and perceptual quality of the current applications, heterogeneous access network monitoring techniques for network information discovery, mobility management schemes for session continuity and application adaptivity strategies for optimum application performance.

This thesis provides an overview of the challenges presented by intelligent seamless handoff requirements, and then provides a pragmatic solution to intelligent seamless mobility. The thesis problem space is divided into distinct domains. The first part of this thesis focuses on mobility management schemes since such schemes define the architectural framework from which heterogeneous networking rises. Secondly, this thesis explores TCP throughput during handoff within heterogeneous environments. Finally, this thesis proposes a novel network selection algorithm for multihomed users running a variety of applications. These contributions have been thoroughly tested and validated by simulation.

Contents

List of Figures

List of Tables

Nomenclature

$\varphi(s_k^p)$ MLP activation function for neuron k when pattern p

E HNN Lupanov (energy) function

V_k HNN activation value for neuron k

x_i^p input i when pattern p

$\Leftrightarrow$ if and only if

y_k^p output from neuron k when pattern p

θ_k threshold value for neuron k

w_{jk} neurons j-$k$interconnection value

Acronyms

ABC Always Best Connected

ACK Acknowledgement

BA Binding Acknowledgement

BU Binding Update

CGA Cryptographically Generated Address

CN Correspondent Node

CoT Care-of Address Test message

$CoTI$ Care-of Address Test Initiation message

$CRRM$ Centre for Radio Resource Management

DAD Duplicate Address Detection

DoS Denial of Service

$DUPACK$ Duplicated Acknowledgements

ELN Explicit Loss Notification

$FBack$ Fast Binding Acknowledgement

FBU Fast Binding Update

$FMIPv6$ Fast Handoffs for MIPv6

FNA Fast Neighbour Advertisement

HNN Hopfield Neural Network

HoT Home Address Test message

$HoTI$ Home Address Test Initiation message

$ICMPv6$ Internet Control Message Protocol-v6

ISP Internet Service Provider

MAC Medium Access Control

MIH Media Independent Handoff

$MIPv6$ Mobile IPv6

MLP Multilayer Perceptron

MN Mobile Node

NAR New Access Router

$NCoA$ New Care-of Address

PAR Previous Access Router

PAR Previous Access Router

$PCoA$ Previous Care-of Address

$PCoTI$ Proactive Care-of Address Test Initiation message

PDU Protocol Data Unit

$PHoTI$ Proactive Home Address Test Initiation message

PKI Public Key Infrastructure

$PRO - FMIPv6$ Proactive Route Optimisation for Fast Mobile IPv6

$PrRtAdv$ Proxy Router Advertisement

QoE Quality of Experience

QoS Quality of Service

RAT Radio Access Technology

RAT Radio Access Technology

RTO Retransmission Time-Out

$RtSolPr$ Router Solicitation for Proxy

RTT Round-Trip Time

$RTTVAR$ Round-Trip Time Variance

$SMSS$ Sender Maximum Segment Size

$SRTT$ Smooth Round-Trip Time

UNA Unsolicited Neighbor Advertisement

Chapter 1

Introduction

Over the last few years, the relative importance of network mobility technology has, as a result of the twin drivers of technology advances and society's demand for communication, information and multimedia contents, increased significantly. Some of the most important causes behind this phenomenon are the rapid spread of 3G wireless networks and the rapid adoption of smartphone technologies. Also, of major importance, is the adoption by the mobile user communities, of services and applications that have been so successfully accepted by residential users. Among such services there are instant messaging and music on-the-go applications, and other network sites as myspace, YouTube or facebook. Along with the classically entertainment-oriented residential users, enterprise customers can also benefit from new delivery technologies such as VoIP or applications for video-conferencing at reduced costs. Unsurprisingly, the last decade has witnessed a remarkable increase in the popularity of wireless networks.

However, firstly, mobile users are not yet provided with the network throughput of the wired broadband systems; and secondly, residential users do not enjoy either the simple mobility management features provided by radio access technologies different from cellular networks (3GPPx), like WiFi or WiMax. In this context, the addition in the number of deployed wireless networks and Radio Access Technologies (RATs) expands the possibilities for the fulfilment of the mobile user's *Quality of Experience*.

1.1 Heterogeneous Networks and Multihoming

The increase in the variety of RATs and the number of wireless networks has given rise to the concept of *heterogeneous* networks or environments (Figure 1.1). In heterogeneous environments, the coverage from different RATs potentially overlaps, augmenting the network resources available to users. To put it another way, heterogeneous networks are expected to fulfil the demand for higher bit rates, which are anticipated to increase in the near future. Thus, for instance, 3G/WLAN interworking would become a extremely attractive synergy: provided that the WLAN hot spot is within the 3G network coverage and that the user is equipped with a dual mode terminal, integrating the two technologies (i.e. *multihoming*) would provide users with high speed and low cost data services within limited coverage areas, as well as any-time, any-where connection. Thus, increasing the 'pool' of available resources, would considerably increase both user satisfaction and network utilisation efficiency.

There are additional benefits to multihomed devices. For instance, by multihoming, a device should be able to insulate itself from certain failure modes within one or more transit providers. Also, as mentioned previously, multihoming enables load sharing, i.e. distributing traffic between multiple interfaces. Multihoming permits bandwidth aggregation, improved signal coverage and the ability to choose the most desirable network considering the ongoing application requirements.

User's applications present very different demands for network resources. These demands can be adapted to the network resources to some degree, or by adopting a completely different allocation of resources. For instance, some applications (such as VoIP clients) dynamically adapt their generated traffic load to the link's capacity by varying the frame rate and size. Alternatively, applications can exploit trade-offs between different resources: e.g. a video stream application can vary the extent of compression used in order to match the hardware processing capabilities.

Internet Service Providers (ISPs) can also benefit from multihoming and resource allocation. From a networking perspective, distributed applications can be executed in environments that may include different network architectures as

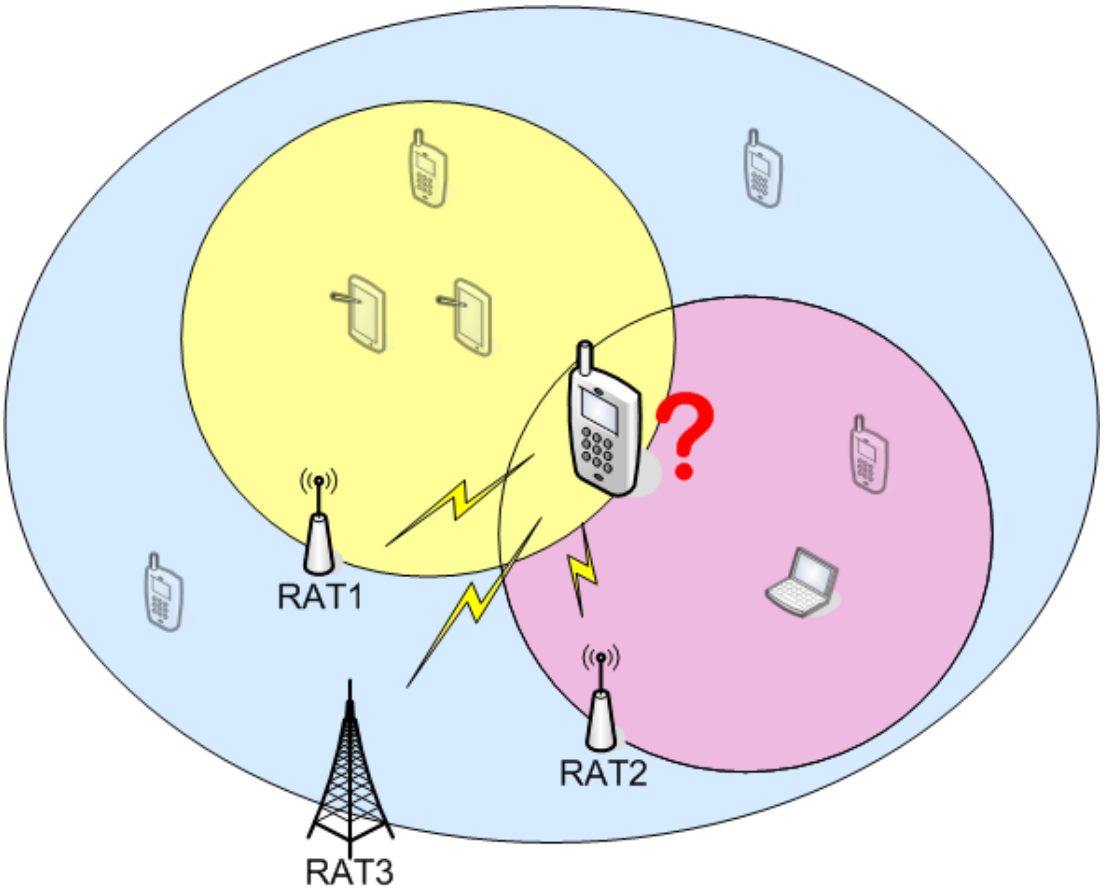


Figure 1.1: Example Scenario: the multihomed user's device has a choice of RATs [2]

well as a range of computer platforms. Many distributed applications have critical response time requirements. However, the timeliness of a response however depends on the availability of resources: network bandwidth to transfer information, end-to-end latency and node's local link congestion. Increasing the number of networks and therefore the radio resources exponentially increases the potential for management of the users' traffic load generation and, ultimately, of the frequency spectrum.

Yet current trends in the deployment of access networks is resulting in the development of ever-increasingly complex heterogeneous network environments. The appearance of new access technologies promises better QoE, but also hinders the efforts of the research community and also from industry to minimise the implementation complexity of new services and applications. New and existing network deployments often overlap, requiring new solutions to exploit the radio resources synergistically. Heterogeneous networks call for multi-platform co-operative schemes to fulfil user promises of improved QoE.

Before heterogeneous networks can effectively provide a qualitative improvement on the user's QoE, there are a number of issues related to co-operation and adaptability that, at the time of writing of this thesis, have as yet to be addressed. Some examples are as follows. For instance, the performance of a fast processor (in an application server) or network link with additional computation or traffic load can deteriorate significantly, but if the application is moved to another system, then the user may not experience a slowdown. When running a distributed application, the impact of link congestion can be mitigated by migrating to a different part of the network. A data warehouse may appear to stop operating when additional users commence extensive queries, but if the data is replicated on another server, the application may forward the requests to this server thereby preserving the perception of a timely response. The quality perceived by a user running a video stream or having a Voice Over IP (VoIP) conversation is directly related to network parameters such as jitter, latency and bit error rate (BER). In heterogeneous environments, applications seldom have exclusive access to resources; instead, network links and processors are shared by many applications and users. Finally, inter-RAT or *vertical* handoffs require to be optimised since they incur macromobility: handoff produces significant changes not only at L2 but also at L3 (explained in detail in Section 1.2). These examples illustrate the

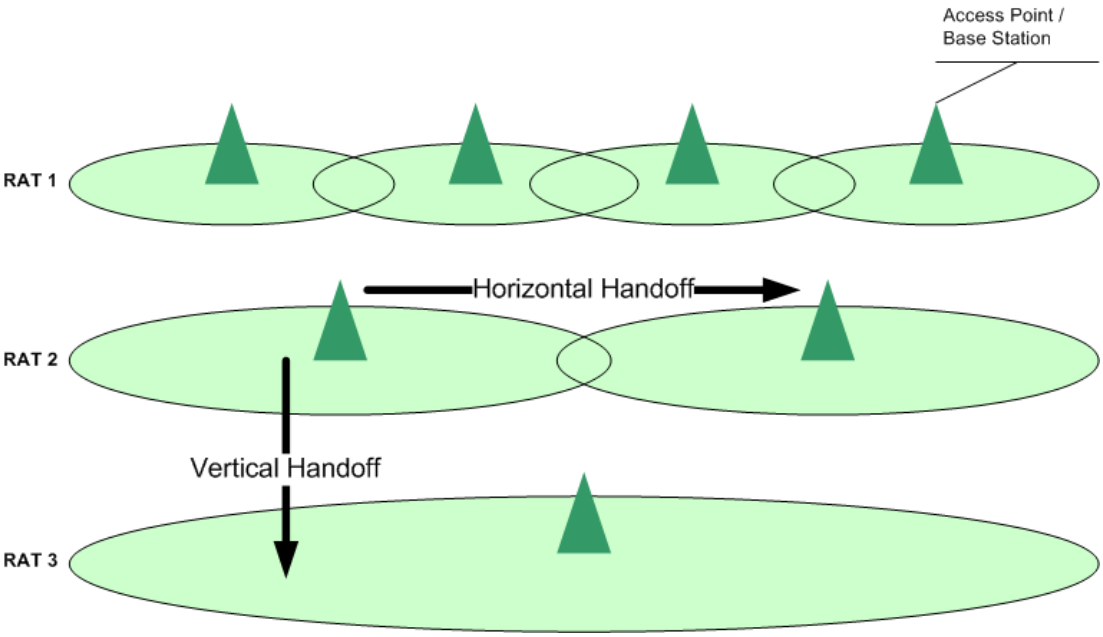


Figure 1.2: Horizontal and Vertical Handoffs

diversity of issues ISPs must face before achieving the full potential of heterogeneous networks. This thesis focusses on a sub-domain of the problem space of multihoming in heterogeneous environments; the intelligent seamless handoffs.

1.2 Handoff in Heterogeneous Environments

The process of detaching from one access point (AP) and connecting to the next is referred to as handoff. There are two different types of handoffs, those in which both APs are part of the same access network and those in which the mobile node's change of point of attachment interfaces to a different RAT. The first group is known as *horizontal* handoff, whereas the second is referred to as *vertical* handoff. For instance, an IEEE802.11b-enabled mobile node may, on the basis of the received signal strength indicator (RSSI), trigger the detachment from the current AP to connect to another one. Alternatively, more comprehensive knowledge of the available networks resources may trigger inter-RAT handoffs. As Figure 1.2 shows, in heterogeneous environments both horizontal and vertical handoffs can take place.

Horizontal handoffs are carried out using RAT-specific schemes. The proce-

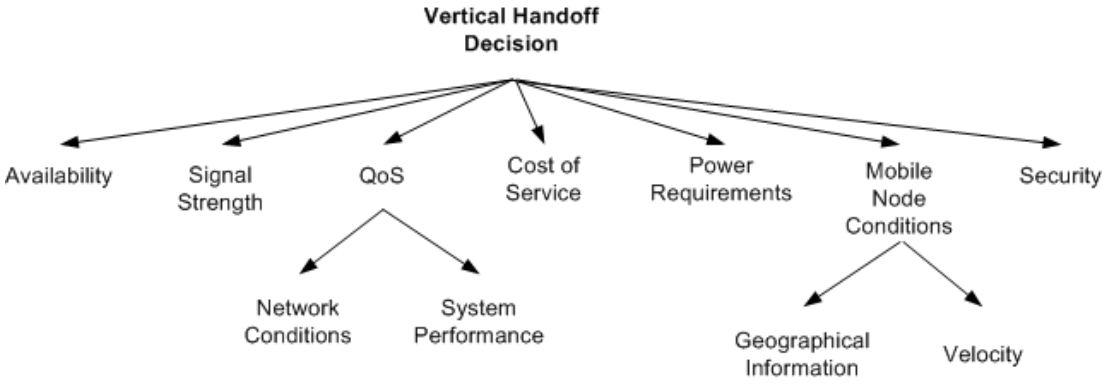


Figure 1.3: An enumeration of Vertical Handoff Decision Attributes

dures executed at handoff are limited to RAT-specific mechanisms and their scope is limited to L2 parameters such as, going back to the example above, the RSSI. However, vertical handoffs require higher-level descriptors and actions at handoff. Firstly, higher-level descriptors are needed due to the fact that applications not only rely on the RSSI to perform, but also on many other network parameters, such as link capacity, RAT-inherent jitter, user profile, application types or service accessibility, etc (Figure 1.3). Secondly, as a consequence of transferring the user's session from one network to another, the IP address must change in order to be topologically correct, i.e. it must be formed from the new network's IP prefix. Thus, there is an implicit requirement for mobility management (L3 or above) and for solving the related authentication and authorisation issues.

The above-enumerated vertical handoff's issues call for the implementation of an architecture that presents, in a unified manner, both the range of available radio interfaces and the applications' request for resources; a handoff decision system; and handoff schemes for seamless mobility. Several functionalities are required for the feasibility of this architecture: the development of adaptive applications, a unified mechanism for network information retrieval and a RAT-agnostic handoff scheme to roam freely around the different available networks. These are explained below.

Application adaptivity is the ability at handoff to perform predictably and efficiently under a broad range of conditions. Adaptivity schemes can be applied as middleware, coded directly on the application or by means of

altering the communication protocols they rely on, e.g. TCP, in the case of FTP applications.

Network Information Discovery provides mechanisms for users and operators to produce accurate information about the available access networks. These mechanisms include RAT-specific monitoring techniques and accessible information service points, such as the *Common Radio Resource Management* (CRRM); a network functionality that provides a unified interface to enable the retrieval of link parameters (such as capacity) and other network-context information [5, 6, 7].

Mobility management scheme at L3 or above enables both horizontal and vertical handoffs, since this approach is L2-agnostic. This scheme, however, can be used to trigger L2 procedures towards handoff (as explained later in Section 1.3).

Supporting seamless mobility between heterogeneous networks presents further challenges since each network is characterised by different mobility dynamics, QoS and security and Authentication, Authorisation and Accounting (AAA) requirements. Moreover, applications are characterised to some extent by time dependency. For instance, TCP periodically computes the network performance to dynamically adapt to available channel capacity. Also, interactive applications such as VoIP and video streaming have stringent performance requirements with regard to end-to-end delay and packet loss. Handoff may breach these performance bounds by introducing delays caused by network discovery and L2 handoff procedures, IP set-up and mobility management. Figure 1.4 illustrates the main functional blocks of an intelligent seamless handoff architecture. As the diagram depicts, the architecture requires an informed and coordinated decision system; is vital for any improvement in the user's QoE.

Thus, there is a number of issues that mobile nodes will face in order to achieve intelligent seamless handoffs in heterogeneous environments. The next section presents a potential user terminal architecture, and highlights those issues that have been considered in this thesis.

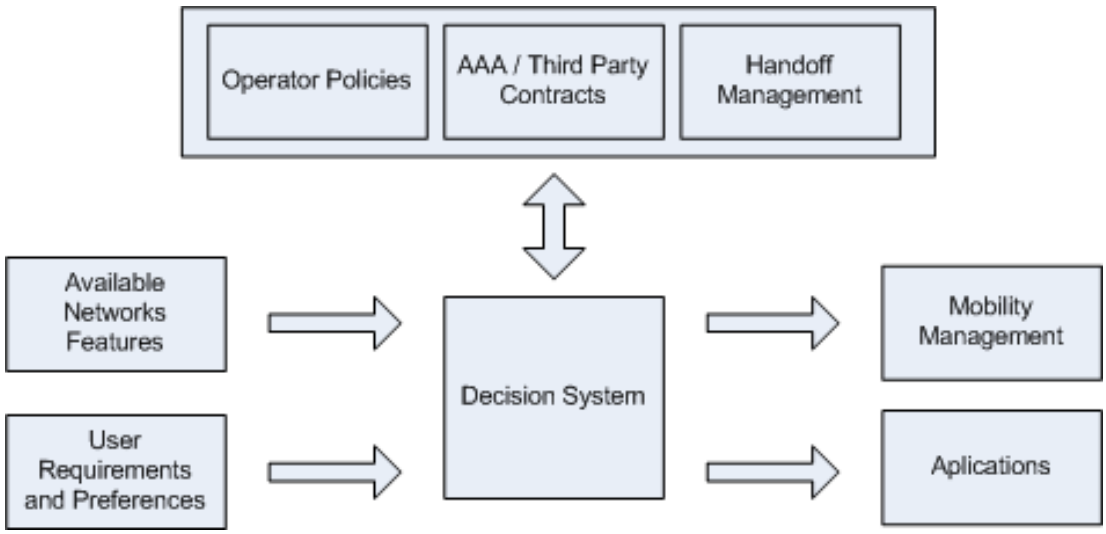


Figure 1.4: Main Functional Blocks of an Intelligent Seamless Handoff Architecture

1.3 A Solution for the Terminal Architecture

In order to accommodate any extended functionalities of intelligent network selection, network handoff signalling and transport-level enhancement a parallel control layer should be superimposed to the standard TCP/IP stack. This architecture permits the information retrieval from the different constituent protocols of any given network entity, as well as their management towards cooperative and synchronised tasks. The nature of the system information includes, but is not limited, to:

- L2 operational state (Link Going Down, Imminent Handoff, At Handoff, Handoff Done).
- L2 Expected Handoff Delay and RAT-specific reports.
- L3 location management and handoff information, e.g. network context information such as the AP-ID duple.
- L4 average goodput or other arbitrary KPIs.
- L5 (application) requirements or KPI features.
- User's requirements and preferences, and permissible costs.

Due to the diverse nature of the information that this control layer handles, there is a demand for flexible information exchange capable of handling arbitrary data structures. The information should be retrieved in a cooperative manner, either on demand or via an event-driven information service. These requirements require a cross-layer media-independent notification system. For standardisation and extensibility purposes, the IEEE 802.21 Media Independent Handover (MIH) standard has been considered as the support framework of the system [8, 9].

1.3.1 IEEE 802.21

The IEEE 802.21 standard defines an extensible set of media access independent mechanisms that enable the optimization of handoff between heterogeneous IEEE 802 networks and facilitates handoff between IEEE 802 networks and cellular networks. Its main purpose is to improve mobile user experience by facilitating handoff in heterogeneous environments, including different radio technologies—both wired and wireless—where handoff is not otherwise defined; and to enable mobile devices to perform seamless handoffs.

Other key functionalities of the IEEE 802.21 MIH information service are:

- Reducing battery usage by avoiding unnecessary scanning and making an intelligent use of the network context information. For instance, turning on an IEEE 802.16 radio module only if a 802.16 network is available.
- Reducing power consumption used by the backend (core) network.
- Reducing the handover time by passing security and QoS information to the next point of service.
- Allowing service providers to enforce their policies and roaming agreements.

Handoff decision making involves cooperative use of both MN and network infrastructure. Handoff control, handoff policies, and other algorithms involved in handoff decision making are generally handled by communication system elements that do not fall within the scope of this standard. However, it is beneficial to describe certain aspects of the overall handover procedure so that the role and purpose of the MIH services in the handover process are clear. The following subclauses give an overview of how IEEE 802.21 enables network selection and service continuity.

- Network Selection
  - Allows users to select between 802.3, .11, .16, 3GPP and 3GPP2 networks: current research efforts address co-operative networking in heterogeneous environments [10, 11].
  - Various applications have different tolerance characteristics for delay and data loss. By making a provision for such characteristics, users can connect to the desired network taking informed application-aware decisions further considering the user's preferences and the user or network's policies [12]. This standard specifies the means by which such information can be made available to the MIH users to enable effective network selection.
  - Base stations can notify users at changes on networks' availability [9]. The users are informed about link type, link identifier, link availability, link quality, etc.
- Service Continuity: Service or session continuity is defined as the continuation of the service during and after the handover while minimizing aspects such as data loss and duration of loss of connectivity during the handover without requiring any user intervention. In this respect, IEEE 802.21 provides the necessary facilities for *make-before-break* handoffs [13].

Most importantly, IEEE 802.21 provides an open interface, an easily extensible and operative framework for link state reporting, inter-system information service and handoff control (command) system. It aims to provide an architecture to enable low-latency handoff across heterogeneous environments, by helping in the handoff decision-making, network information gathering and standarising the protocol interfaces so that it can be implemented in distributed environments. Moreover, IEEE 802.21 helps to execute handoffs by providing status information and event information at handoff. However, it does not define handoff policies, nor specifies network selection procedures, i.e. it does not define L2 handoff procedures nor network detection procedures since these mechanisms are L2 technology-specific. It does not address either security mechanisms. This loose-coupling approach permits its application to heterogeneous environments;

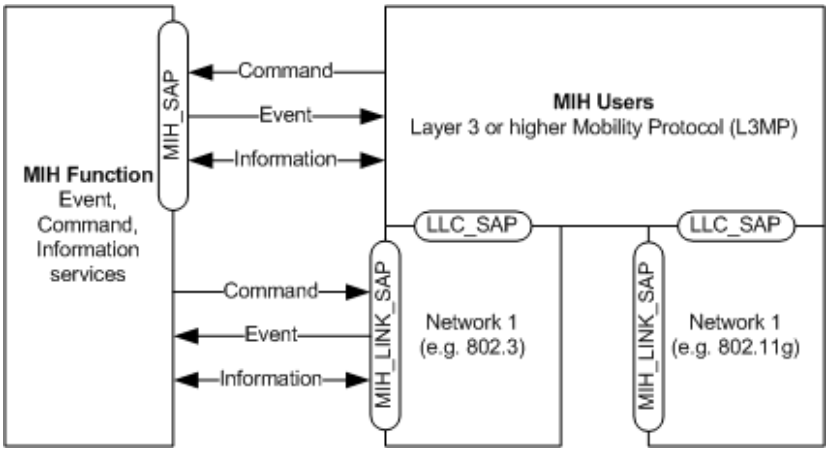


Figure 1.5: MIH services and their initiation

leaving L2 to specify the handoff procedures allows for future changes with the L2 protocols.

IEEE 802.21 comprises three types of services:

- Event Service: it delivers *triggers* on events, e.g. 'Link Up', 'Link Down' or 'New Link Available'.
- Information Service: it is a request/reply-oriented information service for faster handoffs, providing lists of available networks, network operator, network-context information, etc.
- Command Service: while the former two services are mainly used for informational purposes, the command service provides a set of commands for the MIH users to control link layer properties and actions relevant to handoff, e.g. 'Switch Link', 'Configure Link'

MIH users access these services through well-defined service access points (SAPs). MIH users employ a set of primitives, also defined in the standard, to access the services of the MIH Function. Figure 1.5 shows how these three types of services cooperate within the IEEE 802.21 architecture.

As a final consideration, IEEE 802.21 embodies the afore-mentioned (seamless handoff extensions to heterogeneous environments) system framework requirements, i.e. inter-operability, extensibility and the possibility of different types of communication services: command (action request) and information retrieval on

request and on event. Chapter 3 explains how an IEEE 802.21-based system architecture has been implemented for the purposes of numerical evaluation.

1.4 About this Thesis: Solution Overview

In the pursuit of a feasible and effective design for a seamless heterogeneous handoff strategy, the challenges surrounding heterogeneous handoff are investigated and a focused literature review on existing schemes is presented. Ideally seamless handoff is achieved by the coordinated action of a number of protocols and network entities which make informed and accurate decisions on when, why and to which network the handoff is to be performed. However, such a scenario is not realistic. The intelligent seamless heterogeneous handoff problem is complex; it is a multi-stage decision problem with uncertain, imperfect or incomplete information, multiple static and dynamic inputs with a strong temporal dependency and involves synchronisation with a number of network entities and protocols [2].

This thesis explores the benefits of an architectural framework that enables seamless handoffs in heterogeneous environments in order to accommodate the mobile users' demands of session continuity and ubiquitous connectivity. This architectural framework takes a cross-layer approach: facilitating the information sharing, interaction and thus co-operation between different protocols via direct inter-layer communication. Moreover, for the fulfilment of the mobile node's demands there is a requirement for, firstly, *establishing network selection*, secondly, *reducing the latency of the handoff signalling* and finally, *decreasing any repercussion on upper level protocols and applications*. The work carried out in this thesis proposes a set of enhancements to the standard handoff procedures. Among these enhancements there is a consideration for proactive schemes to handoff signalling, specifically Fast Handoffs for Mobile IPv6 (FMIPv6); an intelligent network selection algorithm (NSA); and modifications of the TCP protocol. These three schemes taken together, along with other minor contributions, provide the facilities required for the cross-layer architecture to operate at handoff while offering lower latency and better QoS.

1.4.1 Justification of Research

A first-rate user experience is the key to the success of the future communications industry. The co-existence of different RATs promises better QoE. Users expect to benefit from the diverse range of wireless technologies to support their applications' demands of network resources. However, major challenges, derived from the technological limitations of the different radio technologies, the novelty of the appearance of this heterogeneous environments and the current lack of both technological and economical incentives for the radio interfaces co-design, need to be overcome. These three factors limit the extent of the current possibilities of inter-connection and inter-operation across the different access network domains.

1.4.2 Objectives

This thesis enables mobile users with the capability to choose the network that best matches their application needs and provides them the subsequent handoff procedures. These aims, in turn, can be subdivided into the following secondary goals:

1. Provide a complete review of existing schemes for intelligent seamless handoffs.

2. Provide of simulation platform for the algorithm design and numerical evaluation of novel communication protocols for mobile users.

3. Establish an architectural framework that permits a L2-agnostic approach to seamless handoffs.

4. Optimise network selection on the basis of the traffic requirements generated by user applications.

5. Alleviate the QoS degradation at handoff: reducing packet loss and communication latency, decreasing the L3 and above signalling latency and minimising the impact of handoff on the applications.

6. Support adaptability for the mobile users to confront dynamic network conditions, radio technologies and hardware capabilities.

1.4.3 Thesis Structure

The reminder of the thesis is organised as follows. Chapter 2 presents an overview of the State of the Art addressing the contributions to NSAs in heterogeneous environments, the FMIPv6 protocol and other proactive handoff schemes and the different solutions that can be found in the literature to the TCP's counterproductive behaviour at handoff. Chapter 3 introduces the evaluation environment: this section gathers the assumptions made during the implementation process; also, this chapter presents the software simulation platform and enumerates the different verification methodologies that underpin the validity of the numerical results. The following chapters, 4, 5 and 6, enumerate the proposed solutions for faster, seamless handoffs. Chapter 4 introduces the so-called Proactive Route Optimisation for FMIPv6 (PRO-FMIPv6). This scheme provides lower handoff latency compared to other current approaches. Chapter 5 describes a TCP enhancement that allows for minimising the handoff-induced disruption on TCP flows. Chapter 6 explains a novel NSA based on neural networks that optimises the network selection choice by virtue of matching the required QoS with that offered by the different available networks. This approach permits fine adjustment of the user demands to the networks facilities, optimising the networks resources. Finally, Chapter 7 concludes this thesis and presents the future work.

Chapter 2

State of the Art of Seamless Handoff Techniques

Intelligent seamless handoffs are an integral part of any envisioned future heterogeneous networking. This chapter reports on the evolution of the wireless environment and outlines the motivation for the work on the design of a user-centric handoff management scheme. The motivation behind handoff management and network selection derives from addressing network-centric to service- and user-centric goals. This paradigm shift is happening as users' choice of networks is expanding to include a diversity of RATs from different operators and service providers and the range of complexity of applications is increasing with new functionality and characteristics.

This chapter presents different stances of the future heterogeneous service-oriented architecture. Firstly, handoff management is introduced as a problem subspace of the heterogeneous networking. Secondly, this chapter presents the evolving characteristics, challenges and the state of the art of network selection, mobility management and, ultimately, applications' adaptivity at handoff.

2.1 Evolution of the Wireless Environment

During the past decade, the telecommunications industry has grown as more business players are getting involved, rapidly evolving both technically and economically. It's long past that the traditional two-player technology-driven market, where traditional network providers dictated usage conditions, gave way to a

multi-player service-oriented market, where offering a satisfactory QoE is the key to maximising revenue potential. As the industry has unbundled, the coupling of network access and service provision has been reduced, to the extent that service providers are being established as a third party into the wireless arena. The resulting three-player market structure—users, network operators and service providers—has further increased the business dynamism and the technological challenges as well as the users expectations of QoE. Each of these three players or levels in the evolution of the wireless environment are described below.

Service providers seek to increase their revenue by offering attractive services to the user community. The key relationships between service providers, the users community and the network providers is shown in Figure 2.1. This figure also illustrates a parallelism with the envisioned service-oriented heterogeneous environments. In such environments, users are expected to access an array of services to supply their communication, entertainment and information needs, operating from a variety of terminals.

Research in the area of service provision in heterogeneous environments focusses on dynamic adaptation of contents to variations in individual preferences, mobile terminal conditions and the current radio access network and access technology. While network operators explore network connectivity policy definition, service providers consider best service delivery; therefore user QoE depends on the inter-reliance between the two (this has been subject of discussion between network- and user-centric views [14, 15]).

Network access providers have increased in the telecommunications market over the past decade and, with them, the number of Mobile Virtual Network Operators (MVNOs), hotspot providers, satellite and wireless broadband providers and home and company networks. Furthermore, different operators use different mixes of RATs, with different coverage, management and capacity capabilities to cater for diverse service requirements. Figure 2.2 shows some different types of wireless networks available and their typical coverage areas. Each of these networks was developed to cater for a specific need. For instance, WLANs are designed for high-rate data transmission, whereas WWAN address mobile entities and satellite networks allow for remote connectivity.

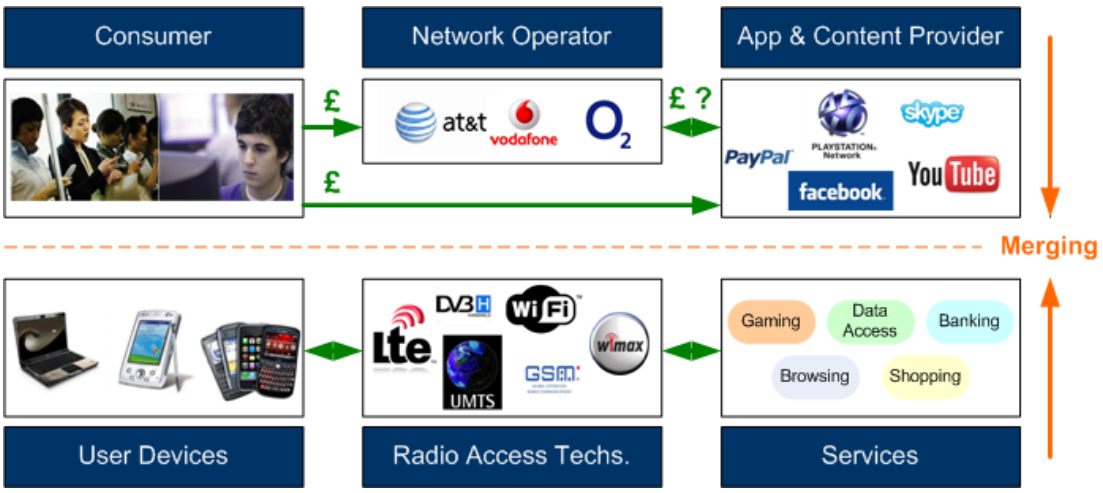


Figure 2.1: Key Market Relationships and their Technological Counterparts [2]

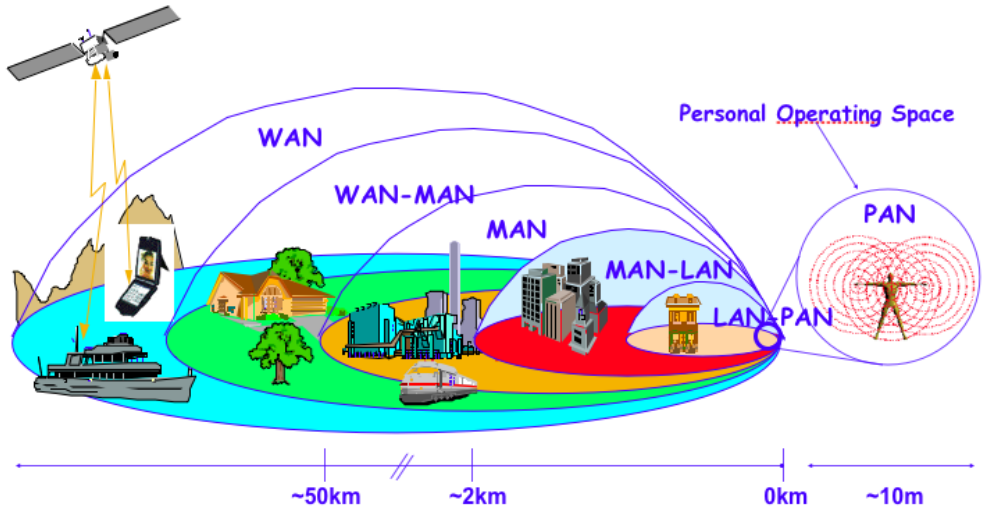


Figure 2.2: Radio Communications Technologies [3]

Networks have also evolved technologically, influencing factors include the adoption of more complex modulation schemes, taking advantage of more advanced radio chips with lower power consumption, more intelligent medium access mechanisms or lower-latency networking enabled by the evolving core-network technologies. Wireless networking has evolved from the early stages of wireless communication where voice was the sole supported service (the First Generation or 1G) underpinned by switched circuit technology, to the latest developments in multimedia broadband, cellular IP networking and ultra-high data rate transmission. Figure 2.3 illustrates the evolution of the major wireless access technologies.

Users have over the past five years become more technologically proficient and service-hungry, spoilt by the user's en masse embrace of smartphones, laptops, PDAs and such hand-held devices. As the user service demands increase, so does the need of continuous ubiquitous access. Currently, users expect connecting capability with geographical independence. Moreover, mobile users accustomed to flat-rate and flat-bandwidth connectivity also frequently pay for a second access if they are, e.g. at airports or cafés, where users tend to run more intensively network applications such as web-browsing or file-downloading and therefore can benefit from hotspot connectivity.

It is therefore remarkable that users expect a high QoE, but they also have different expectations depending on previous experiences, current context (such as location, activity, mobility, remaining battery, and near future plans) and the capabilities of their terminal. In order to fulfil such expectations, firstly, the terminal needs inbuilt intelligence to aid the decision as to which access network to choose for each session, and it must be capable of taking informed decisions on the basis of users' preferences (such as preferred services or cost), network metrics (like coverage, security and capacity) and mobile characteristics (whether the terminal is multi-homed or is capable of multiple simultaneous connections, embedded RATs, speed, battery). Secondly, RAT-agnostic user-centric mobility management schemes must be adopted by both access providers and terminals, to allow

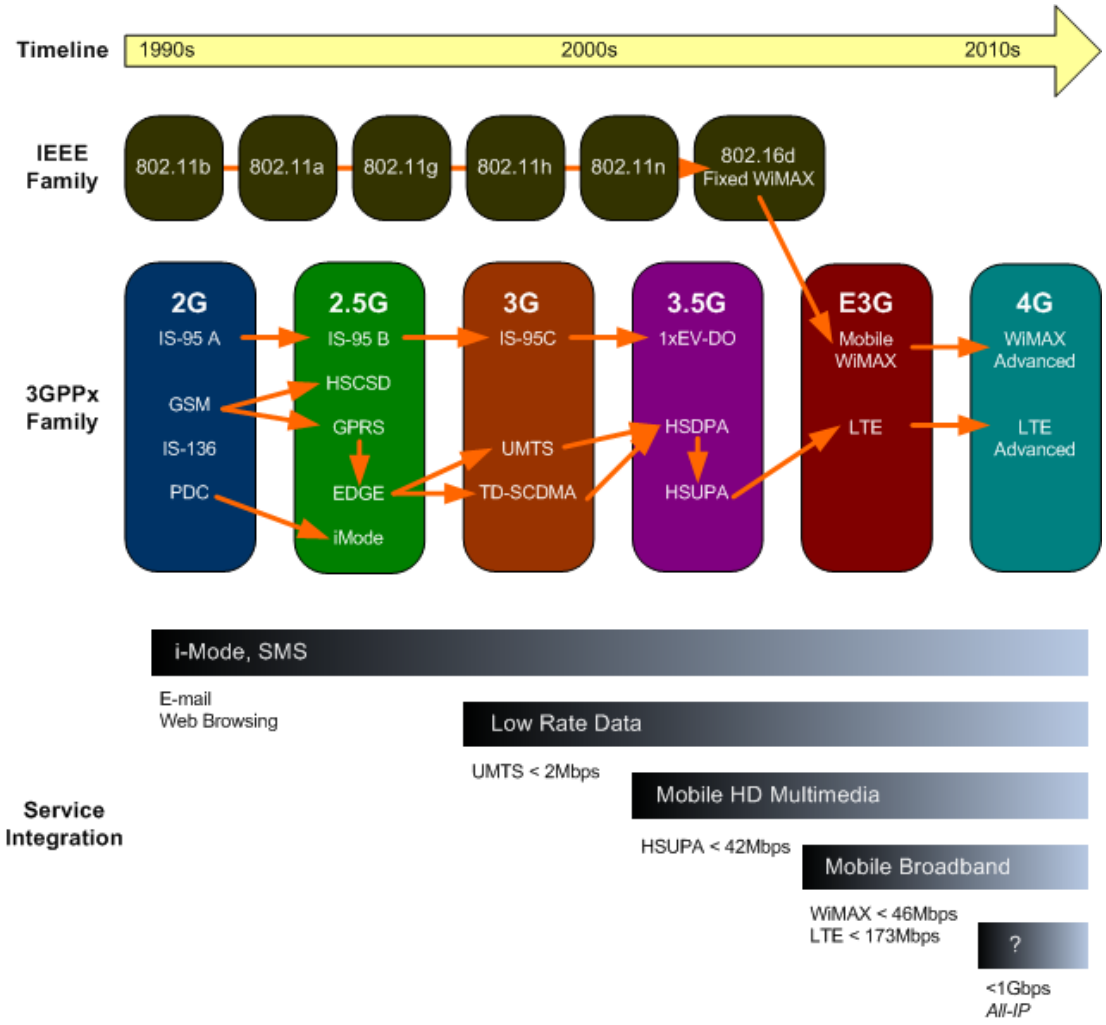


Figure 2.3: Evolution of the most widely adopted Wireless Access Communication Technologies [4]

for seamless connectivity and ubiquitous IP reachability. Thirdly, applications should proactively adapt to current network conditions in keeping in with the principles of seamless mobility.

2.1.1 Towards *Always Best Connected*

As the merging of Internet and telecommunication networks into an *all-IP* environment takes place, different views emerge as to how they should integrate and on how these next generation wireless networks should be shaped. In materialising the network architecture there are a number of *actors* involved: users, network operators, service providers, application service providers and third-party providers and operators. Each one of these actors often has conflicting interests and thereby its own perspective on the Always Best Connected (ABC) paradigm [16].

ABC encompasses a vision, which may be defined differently by the actors involved. This is because the definition criteria for the *best* connectivity is subject to different interests. Network operators would envision ABC as a model based on maximising benefit while dedicating to users the minimum possible network resources required to support the user's services. Thus, it is beneficial or advisable for the operator to either control or have direct business agreements with the service providers, as well as with the individual users. Alternatively, the user's viewpoint on ABC would consider an inexpensive Internet access and a seamless ubiquitous connectivity to all types of services. In this context, a regulated consumer-friendly market where multiple overlapping access networks, service providers and operators would be viewed positively. Finally, service providers focus on the open nature of the access interfaces, both to users' requests and to network providers access and billing, and on the flexibility and dynamism on offering its services on third-party networks.

Hence, although a number of business models may co-exist, there are two main opposed stances of the resulting all-IP network: the network-centric and the user- or service-centric views. The network-centric vision embodies a continuation of current approaches to access billing, i.e. users being tied to a single network operator subscription. At the other end, *pure* user-centric views support user freedom of choice for the most suitable access network for the terminals and

ongoing services, or the combined choice of multiple access networks in cases where the terminal is multihomed. This thesis focusses on the user-centric vision.

Regardless the degree of market regulation and technological concentration, and for both network- and user-centric approaches, independent researchers [14, 16] identify a number of required ABC enabling technologies; some need to be implemented in the terminal, while others need to be implemented in the network side. The ABC functionalities considered in this thesis were previously defined in Chapter 1. A more comprehensive definition of the ABC functional blocks is as follows:

Access Discovery permits an ABC terminal to find the available access networks/devices. Once connected, the terminal periodically performs access discovery to find better connection alternatives. Access network routers/access devices must present information in a uniform manner via a generic set of parameters, describing QoS, cost and type of RAT. Access network devices should accurately produce this information investigating how to collect the network statistics, since networks are highly dynamic environments.

Access Selection provides *better* choices of access network for users *or* for network operators. Access selection usually comes down to either allocating resources for minimising cost, maximising the perceived QoS or minimising cost provided that certain QoS constraints are satisfied. Access selection can be carried out either by the network or by the user. Section 2.4 explores the use of network selection strategies on heterogeneous environments.

AAA Support provides users of with information about what they can do–Authentication–, credentials–Authorisation–and Accounting (AAA). In an heterogeneous environment, where several operators co-exist and where single-radio or multihomed users can make use of the different networks, AAA presents both technical and business challenges.

Convergence Interface is a uniform interface for transmitting IP packets over wireless links. This interface (defined in [2, 14]) is present only at access routers or cellular network Base Stations, and provides a mechanism for the IP layer to interface with a variety of wireless technologies.

Mobility Management enables both vertical and horizontal handoffs, and provides mobile nodes of session continuity and continued reachability. Section 2.2 presents an extensive overview of the state of the art of mobility management schemes.

Profile Handling is a two-sided problem. First, as part of the QoS provisioning, operators should guarantee a differentiated treatment for each user or aggregated flows on the basis of their tariff, the user's personal preferences for choice of access and application adaptation. Research work on this issues points to the use of Integrated or Differentiated Services Architecture, Resource Reservation Protocol and Multiprotocol Label Switching. Secondly, users' profiles should be securely stored in the servers of the ABC service providers and updated in accordance with the business agreements made with network operators. Such profiles are also needed for AAA purposes.

Applications adaptation. It is essential for applications to dynamically adapt to the current network conditions and to support the reconfiguration of each communication session (e.g. a VoIP flow) in response to a variety of external factors such as media formats, mobility, application QoS requirements and access network characteristics. With regard to the adaptation response, it may well be performed by the application itself, or by the transport protocol it may rely on (e.g TCP, in the case of FTP applications). The adaptation scheme initiation may be triggered by the application itself (reacting to network changes and in response requesting the application server to adapt), or by the access network and/or the terminal (proactively) providing information about the network characteristics (for instance, notifications on QoS changes). Section 2.3 offers an analysis of TCP-based application adaptation.

The work presented in this thesis focuses on (i) the mobility management; (ii) the proactive adaptation of the TCP transport protocol; and (iii) the access selection algorithms on multihomed environments, from a user-centric perspective. Figure 2.4 illustrates the terminal architecture and highlights the elements (i-iii) explored or contributed to in this thesis. This terminal architecture is based on the traditional TCP/IP stack layers, coupled with the extensions proposed by

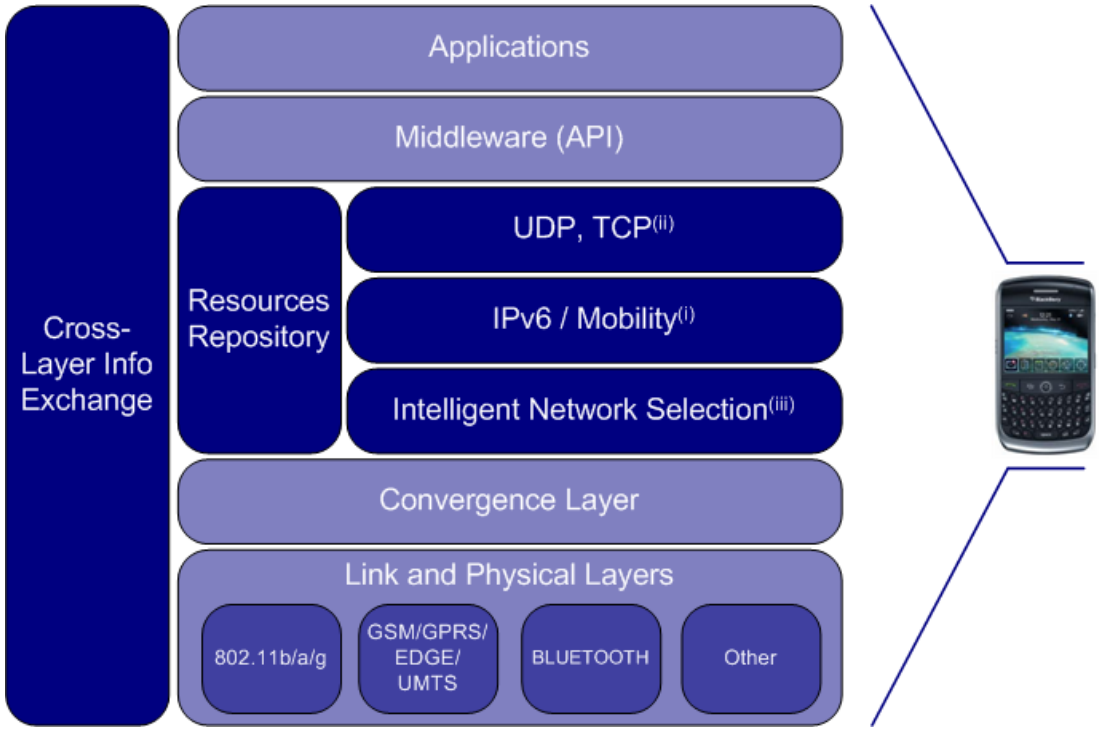


Figure 2.4: A Solution for the ABC Terminal Architecture

Ganchev et al. [14]: a *convergence layer*, which provides a uniform access to the network interfaces; a *network selection layer*, which offers the best choice of networks or combination of multiple networks for any particular situation; a *middleware (API) layer*, which enables applications to advertise their QoS requirements and to be notified or the current network(s) characteristics; and finally, a *vertical resource repository*, interfacing the API and convergence layers, and storing the ABC user and/or network profiles, policies and preferences. These layers are integrated according to the IEEE802.21 model, i.e. a co-designed cross-layer information exchange terminal architecture which, in co-operation with other access network entities, enables an intelligent seamless handoff management.

2.2 Mobile IPv6

Mobile IPv6 (MIPv6) [17] is the *de facto* standard for IPv6 mobility management. This section introduces MIPv6 and alternative L3 mobility protocols (L3MPs), viz. Fast Handoffs for MIPv6 (FMIPV6) [18], Proactive Bindings for MIPv6 [19]

and Enhanced Route Optimisation [20]. The forthcoming discussion will enumerate the requirements for these L3MPs to operate in heterogeneous environments.

2.2.1 On the Need for Layer 3 Mobility Management

Mobile users require their ongoing connections to be maintained and remain reachable while in transit, e.g. from the office to the street. Geographical movement between different locations may cause degradation in the received signal power or quality derived from path loss and interference and could trigger a request to join another access network. Hence, in general geographical movement may trigger a movement to a new location in the Internet topology. Alternatively, the user applications may change their QoS requirements (higher bandwidth or lower tariff) and join a more appropriate access network to cope with those demands.

From the mobile device's perspective, the networking environment changes; some network prefixes vanish, some new ones may appear. In this sense, a physical movement could be regarded as a process of network renumbering. However, the standard IPv6 protocol offers no support for network renumbering. Currently, if a user provided with a laptop wants to leave one network and join another, he or she must restart the IPv6 network attachment procedures. Every ongoing connection would be torn down. Therefore, any suitable solution for inter-access network handoff must accommodate session continuity and reachability. This prerequisite will be referred as 'Requirement 1' in the forthcoming discussion.

Also, although the number of mobile devices is predicted to increase, the L3MP is required to connect mobile nodes to nodes such as servers, routers or other hosts in the Internet that themselves may not be L3MP-enabled. Moreover, at this moment of design and development of the L3MPs, the IPv6 is poised to supercede IPv4. For these reasons, L3MPs have to support IPv6 non-L3MP enabled networking—Requirement 2.

As IPv6, L3MPs are requested to provide networking capability to a wide spectrum of devices enabled with different radio technologies. In the future this situation may become more complex: devices may connect to several networks simultaneously, making use of different interfaces at once. In this case, the device is said to be multihomed. Work is being undertaken in multihoming-enabling

technologies due to the multihoming intrinsic advantages, such as aggregated bandwidth. The multiplicity of dissimilar access networks is such that multihoming techniques must support different link layer protocols, and must offer support for possible multihoming extensions—Requirement 3.

Additionally, the services and network applications mobile users are anticipated to use are the same as by fixed users. One reason for the emergence of the 3G technologies is bringing pre-existing 'common' applications like web-browsing, video-streaming or VoIP within the mobile user reach, i.e. introducing typically residential user applications into the cellular network. Also, WiFi users are another group of mobile users which has long benefited from the same applications and services of those fixed users. Hence, the general trend is towards homogenisation and standardisation of services across the different types of networks.

The convergence of the communication and Internet worlds towards a service-oriented architecture highlights the requirement for applications to be running on different radio technologies. However, in order to make applications fully operative in different devices and over different types of connection, they must be lower-layer agnostic. Thus, the use of different networks should not motivate any changes to change the behaviour of the transport protocols; as TCP and UDP must be still operative in order to support the applications within acceptable levels of performance. Therefore, MIPv6 mobility management tasks must offer upper layer transparency—Requirement 4.

Hence, some of the main requirements for further development in IP mobility management have been set forth. The following sections will introduce the MIPv6 and FMIPv6, Proactive Bindings for MIPv6 and Enhanced Route Optimisation protocols, and how they deal with the requirements mentioned above.

A note on transport- and application-level approaches

Both transport and application-level solutions for seamless mobility can be found in the literature. Transport-level advantages include: (i) authentication can be implicitly established at session establishment, thus securing the end-to-end communication and location management; (ii) also, there is no packet redirection at handoff, thus the path between the communicating hosts is symmetric, and therefore RTT does not artificially increase because of handoff, avoiding retransmission inefficiencies issues [21].

However, tearing down a connection and bringing it back up at the new location presents the following drawbacks: (i) in-flight packets at handoff are lost—although after handoff is completed, they can be recovered via purpose-specific schemes; (ii) transport-level approaches need to be enabled on both end-points, thus if transport-level support nodes are required, then security is compromised; (iii) finally, transport-level approaches handoff management, opening venues of attack and precluding the MN's continued reachability.

Application-level are mostly based on the Session Initiation Protocol (SIP) due to its IETF compliance and its widespread acceptance to support multimedia-sessions [22, 23]. In general, application-level solutions eliminate the need for mobility stack in mobile nodes and, due to their end-to-end nature, do not require support from any other mobility elements in the network.

Application-level mobility—based on SIP—approaches have several drawbacks: (i) SIP addresses multimedia session management, which usually runs on Real-Time Transport Protocol (RTP) over UDP, and it does not support TCP connections thus is not transparent to the broad range of TCP applications; (ii) also, likewise transport-level mobility, application-level enhancements need to be enabled on both communication end-points; (iii) finally, in-flight packets at handoff are lost and, considering that enhacements are limited to the application level, then no handoff-specific packet retransmission schemes would apply, thus other L4 mobility schemes, such as TCP Migrate, could be a better solution for TCP flows.

From the security standpoint, both transport- and application-level solutions can effectively secure the end-to-end communication. However, these solutions may preclude the use of IPsec Transport mode [24]. On the other hand, IPsec Tunnel mode may still be feasible, considering the network-layer mobility awareness since the IPsec security associations are established on a per-address basis. Either case, given the need for secured communications, particularly true in wireless environments, and the subsequent need for network-layer re-implementation at the MN, then either a L3 solution would be preferable, or a L4+ security should be used, such as SSL/TLS [25].

Secondly, avoiding L3 management also precludes routing security mechanisms. For instance, the MIPv6 standard relies on a mixed routing-cryptographic scheme for securing location management. The CN, prior to forward packets to

the NCoA, checks the reachability of the MN at the NAR link. Only after the CN confirms the MN reachability at the NCoA, the binding is established. Contrariwise, transport and application-level solutions open venues for DoS by flooding attacks.

For these reasons, the work in this thesis focusses on network-layer enhancements. The following sections describe the most relevant current L3MPs.

2.2.2 MIPv6 Outline

There are a number of motivations why a node may decide to switch from one wireless network to another: a higher received signal power (perhaps as a consequence of mobility) or for bandwidth reasons (as a consequence of changing QoS requirements). In such a eventuality, MIPv6 provides mechanisms through which the mobile node maintains its ongoing connections. MIPv6 is largely based on IPv6, but it comprises of a number of modifications. In effect, MIPv6 packets are routed transparently over IPv6 networks.

MIPv6 operation is as follows. A mobile node, initially connected to its *home link*, moves to a *foreign link*, managed by another router. Using the IPv6 protocol without mobility support, every connection would be broken; therefore the mobile user would have to re-start the ongoing sessions. Alternatively, MIPv6 would operate in a rather different manner. Firstly, the mobile node should join the foreign link. Once it has obtained an IPv6 address, the node sends back to its mobility support manager or *home agent* a packet known as *binding update*. The home agent is to track record of these bindings by means of the *binding update list*.

The home agent is an entity defined in the MIPv6 protocol. It works as a standard IPv6 router, but embraces the functionality of tunneling packets to the address included in the binding update message: when it receives the binding update, it forwards every packet addressed to the mobile host in the home link to its new address. The only MIPv6-aware entities in this example are the mobile node and the home agent. Hence, implementing such functionality for users on an IPv6 network is limited to setting a home agent in the user's home link, and enabling MIPv6 support on the mobile device. Since MIPv6 control and signalling messages are based on either Internet Control Message Protocol-v6

(ICMPv6) or IPv6 protocols, they are natively routed through IPv6 networks. In addition to the binding update sent to the home agent, if the correspondent node is also MIPv6-enabled, the mobile node could send another binding update to it directly. In this way, direct communication between correspondent and mobile nodes is established: routes are optimised and there is no need of triangular routing through home agent.

2.2.3 Data structures and mobility headers

The MIPv6 protocol defines several data structures; among them, there is a new IPv6 protocol, the *mobility header*. Also, MIPv6 extends IPv6 to include a new Destination Option and further types of messages in the ICMPv6 protocol; two for use in the dynamic home agent address discovery mechanism, and two for renumbering and mobile configuration mechanisms. All these are explained in the following sections.

Mobility header

The mobility header is an IPv6 extension header used by each entity when performing any task related to bindings. This header defines a number of mobility functionalities or options for use within this message:

1. Binding creation or update: facilitated by means of the Binding Update and Acknowledgement messages.

2. Binding out-of-date management: via the Binding Update Request message. It is sent by the correspondent node. Mobile nodes may reply Binding Update Reply Messages.

3. Return Routability Procedure: used for secure communication between correspondent and mobile node while updating binding. For this purpose four messages are exchanged: Care-of Test / Care-of Test Init Messages and Home Test / Home Test Init Messages. Return Routability is explained later in this section.

4. Signalling errors related to mobility management: Correspondent node uses Binding Error Message to signal errors, such as any inappropriate attempt to use the Home Address destination option without an existing binding.

Home Address IPv6 Destination Option

Home Address Destination Option is carried by the Destination Option extension header. It is used in a packet sent by a mobile node while away from the home network, to inform the recipient (correspondent node or home agent) of the mobile node's home address. Scenarios of application of this option are:

1. While sending a binding update message, the mobile node must include its home address in the packet. The source address will be fixed to its care-of address to avoid ingress filtering of the visited link access router. Therefore, the home agent will retrieve the home address of the mobile node from this field.

2. While sending packets to the correspondent node once a binding has been established. Using this option, the correspondent node is able to associate the source (care-of) address of the packet to the correct home address, consequently enabling transparent connectivity to upper layer protocols. The mobile node will still be able to deal with its own authentication procedures, like IPsec (Authentication or ESP), including in the checksum or at the input of any algorithm the home address. Then, the home agent will swap care-of address and home address fields. To receive the packet properly, the correspondent node will swap again both fields.

Type 2 routing header

This header is used to route packets directly from the correspondent to the mobile node's care-of address. Unlike the "classical" routing header, for security reasons the type 2 only allows for one address field [26]. For instance, an attacker could place an IP address different from the home address in the address segment while communicating with a mobile node as correspondent node. In that case, the mobile node would forward the packet to a node different to itself. The correspondent node may use this mechanism if it is trying to connect a network to which is not authorised. When receiving the packet, the mobile node forwards the packet to the address included in the address segment of the type 2 routing header. Since this address is its home address, the mobile node is forwarding to itself. Therefore, the mobile node receives the packet as if it was addressed to its home address.

New IPv6 ICMP Messages

As has been explained, four additional ICMPv6 message types are defined in MIPv6. Two of them are the Dynamic Home Agent Address Discovery (DHAAD) Request/Reply types. These messages are used for home agent discovery purposes. The other two message types have been designed in order to enable the mobile node to obtain information about the home link when resident in a foreign network. These message types are known as the Mobile Prefix Solicitation and Advertisement. Both messages work in the same fashion as their analogous Neighbor Discovery Routing Sol/Adv messages. However, in contrast to the Neighbor Discovery messages, Mobile Prefix messages are globally routable. Moreover, these new messages not only include information about new prefixes in addition to the existing ones, but also they report those deprecated as a result of network renumbering or failing.

Conceptual data structures

In order for MIPv6 to function correctly, a number of data structures are defined to apply to various participating nodes of the MIPv6-enabled network.

- Binding cache: A cache maintained by each home agent and correspondent node. It contains a number of bindings for one or more mobile nodes ("home address" and"associated care-of address" bindings).
- Binding update list: A cache maintained by the mobile node. Contains all the bindings sent to the home agents and correspondent nodes.
- Home agents list: Used to inform mobile nodes of the available home agents in its home-link. This list is managed by the Home Agent Discovery procedures, discussed later in this section.

Binding cache and binding update list are not exchanged by any node. For that reason, they do not have to support any binary framework nor conform to any specific format; their implementation can be proprietary.

2.2.4 MIPv6 Operation

MIPv6 nodes use two different globally routable addresses: A stable IP address (home address) and a volatile or temporary one (care-of address). The home address is used for two purposes: first, mobile nodes are expected to be globally addressable, i.e. reachable within any point on the Internet topology; second, as long as the transport layer connections are linked with IP source addresses, the MIPv6 protocol must offer upper layers a transparent service while changing IP addresses (care-of addresses).

Home and care-of addresses must meet the topological requirements of the Internet and, consequently, are composed of a subnet prefix and an host identifier. When a mobile node changes its position inside the Internet topology, it forms a care-of address from the visited subnet prefix. Afterwards, the node adds the association between its care-of address and its home address to its binding update list, and sends a Binding Update (BU) message to its home agent to inform it about such a movement. The home agent will update its binding cache and, from that moment on, it will forward every packet addressed to the mobile node's home address to the associated care-of address. However, the BU message may fail to reach the home agent, or it may be rejected; therefore, the home agent must send a Binding Acknowledgment (BA) to the mobile node to indicate that the BU has been received and processed successfully.

On successful BU-BA exchange, a bidirectional tunnel (IPv6 encapsulation) between the mobile node's care-of address and its home agent is created, enabling the home agent to perform two functions:

1. Prevent the home address of the mobile node from being allocated to another node, i.e. sending Neighbour Advertisement messages when required.

2. Intercept and forward packets addressed to mobile node on the home link.

Any packets addressed to the mobile node using its home address will be intercepted by the home agent in the home link and forwarded to the mobile node via tunnelling. Figure 2.5 depicts the basic MIPv6 handoff operation. In Step 1, a bidirectional packet flow between mobile node and correspondent node is assumed. In Step 2, the node moves from one position to another, joining the foreign network. Steps 3 and 4 are concerned with signalling processes: first, a

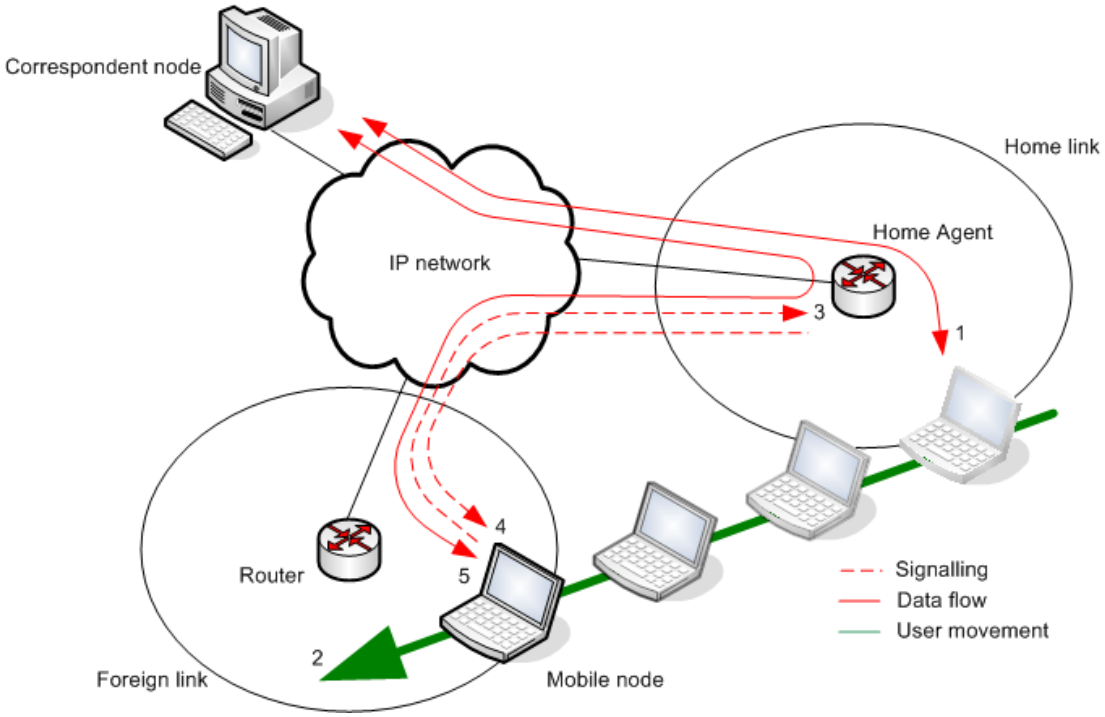


Figure 2.5: MIPv6 basic handoff operation

BU is sent from mobile node to home agent in order to make it aware of mobile node's care-of address, and to set up the associated binding with its home address. In 4, the binding is acknowledged. Finally (Step 5), a bidirectional flow through the home agent is able to transparently maintain the mobile node's ongoing connections to the correspondent node: in cases when the correspondent node is not MIPv6-enabled, reachability of the mobile node though its home address is still maintained.

The BU-BA exchange enables the creation of a bidirectional tunnel between the home agent's IP address and mobile node's home address, a procedure referred to as Reverse Tunnelling. As will be explained in the forthcoming discussion, this tunnelling is performed using IPv6 encapsulation. Thus, after decapsulating the mobile node will be able to present the original packet preserving its integrity to its upper layers; original destination and source addresses are preserved and there is no modification of possible cryptographic protection or authentication. This process of tunnelling is necessary to carry out the communication since

1. if the home agent changes the home address by the care-of address in the

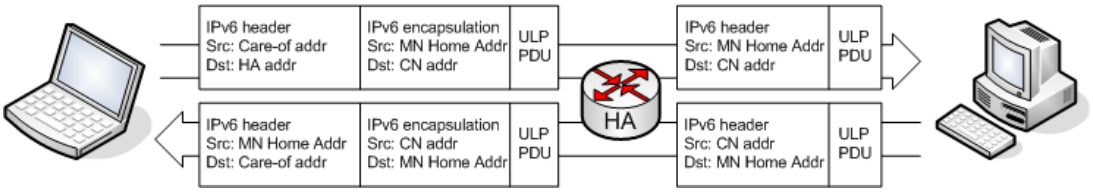


Figure 2.6: Communication through home agent

IP destination field, Authentication or ESP (if applicable) will fail; and

2. if the correspondent node receives a packet from the care-of address instead of from the home address, the tuple (IP address, socket) won't be recognised by the correspondent node and will drop the packet [27].

As explained above, setting up the tunnel is critical for future communication to take place. The mobile node must receive a BA in response to a BU; otherwise it cannot rely on any packets being addressed to its home address being forwarded to its true location. Therefore, a correct exchange of BU-BA must be carried out when not resident in the home link. Figure 2.6 depicts the communication scenario through the home agent [28].

2.2.5 Binding Updates and Acknowledgements

MIPv6 defines a new IPv6 extension header, the mobility header. The mobility header is used to carry every MIPv6 message. It has four permanent fields, one of which is used as a switch to indicate the functionality of the message. Binding Updates and Acknowledgements, among others, are derived from the mobility header and this field provides the differentiation.BUs and BAs are used for managing bindings. Bindings are valid for a specific space lifetime, set to 420 seconds in the MIPv6 standard [17]. This time period was defined in accordance with the expected average connection time to a network while the user is mobile. The bindings are stored in

1. the *binding cache*, in the home agent and optionally in correspondent node, as explained later in the subsection on route optimisation, and in

2. the *binding update list*, in the mobile node.

It is noted that, if bindings were not able to expire or be invalidated and removed, the memory on the home agent or mobile node could become overloaded, rendering such devices incapable to set any other bindings. Hence, a finite lifetime for bindings is needed. In order to refresh their bindings, mobile nodes may send binding update messages in two different manners. First is when the lifetime of the binding is about to expire. The second reason for refreshment is when the mobile node changes its care-of address.

The following section introduces the process by which a mobile node changes the registered care-of address and binds it to the home agent.

2.2.6 Moving to a foreign network

When a mobile device moves to a new location in the Internet topology, it triggers a chain of events designed to make communication possible. Specifically, the mobile device needs to: firstly detect movement, i.e. a change in the topology; secondly form a new care-of address; and finally send a binding update to its home agent. The mobile node will require the home agent's IP address while sending the binding update. This necessitates a mechanism that allows the mobile node to obtain the available home agent's IP address(s) in its home link. MIPv6 integrates a solution to this problem. These processes are now discussed.

Home Agent Discovery

For the mobile node to be reachable by its home agent, it must update its position by sending a binding update when changing from one subnet to another, i.e. one IP prefix domain to another. This way, the home agent will be able to forward the packets to the mobile node's care-of address derived from the new prefix. A prerequisite to sending a binding update to the home agent is knowing the IP address of the home agent beforehand. Such a requirement may be facilitated by manual configuration of the home agent's IP address in the mobile node. However, this method has some drawbacks. The home agent's address could change due to address re-assignment in the home network, or the home agent may fail for any number of reasons, such as mechanical or electrical failure; therefore the mobile node would have to select another home agent. An alternative to manual configuration is proposed for MIPv6; the Dynamic Home Agent Address Discovery (DHAAD) mechanism [17].

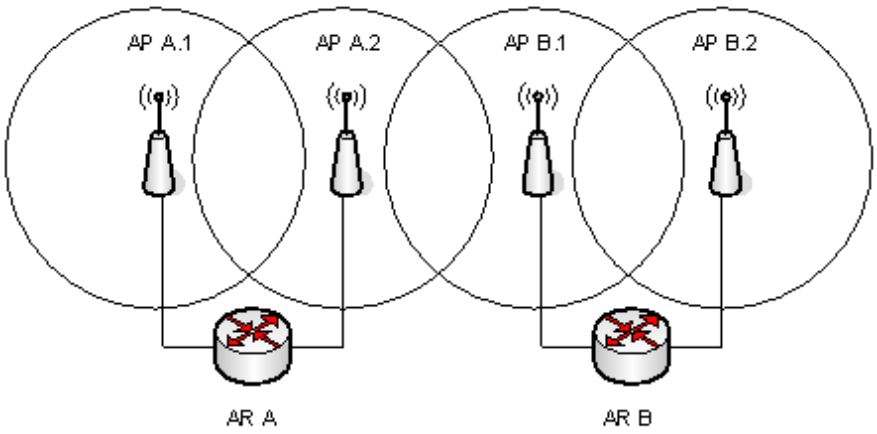


Figure 2.7: Handoff in wireless networks

Movement detection

The mobile node may detect movement by a change in the on-link IP prefixes. In each link, several different prefixes may be found. Some new prefixes may be added, some of them may be deprecated or the routers initially announcing them may now no longer be bi-directionally reachable. Hence, movement detection should not be triggered by receiving Router Advertisements based on a new prefix.

In contrast, generic movement detection uses Neighbor Unreachability Detection [29] procedures to detect that the default router is now not available. Two scenarios of interest are depicted below.

1. A mobile node could move between two links, where each is served by a different AP, but both are connected to the same AR. In this case, the network prefix remains the same. In this situation, mobility detection mechanisms can only be conducted in layer 2 since layer 3 cannot detect any change in the position in the Internet topology as the network prefix does not change. In Figure 2.7, moving from AP A.1 to AP A.2 does not result in a topological movement. However, movement from AP A.2 to AP B.1 does invoke layer 3 handover procedures, and subsequently the mobile node must not carry out MIPv6 procedures.

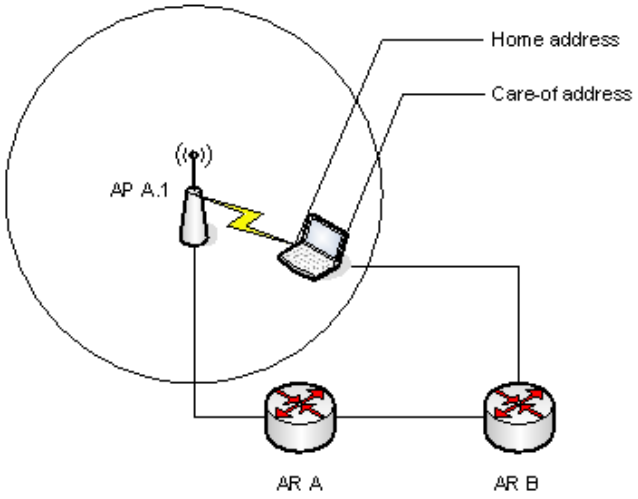


Figure 2.8: Multi-interfaced mobile node

2. A multi-interfaced or *multihomed* mobile node could switch its ongoing connections between interfaces, each connected to different networks. Figure 2.8 demonstrates the case where a mobile node uses an Ethernet connection in preference to a wireless connection. The mobile node could decide to register its care-of address on the Ethernet link, and update its home agent and correspondent nodes. The mobile node will receive all incoming traffic through the Ethernet interface rather than the wireless one. This is effectively a change in position within the network topology.

From the foregoing discussion, it becomes evident that IP mobility may be triggered by layer 2 link migrations, but this cannot be considered as a general case. Hence, the IP layer must be able to identify when to invoke layer 3 handover procedures. Moreover, as a matter of interest, Figure 2.8 depicts a situation where there is no real physical movement of the mobile user: derived from the abovementioned Requirement 3, the user is able to employ the facilities of MIPv6 to roam and support their connections between interfaces transparently for upper layer protocols and applications.

The IPv6 specifications allow more than one prefix to be announced on a single link. In this eventuality, a mobile node will be certain about movement when new prefixes are detected or when the prefix from which the currently used

IP address is derived has vanished: the emergence of new prefixes could trigger a mobile node to try to join a new (better in terms of costs or QoS) network. Alternatively, if the current network becomes unavailable, the mobile node will be forced to look for an alternative network.

In summary, MIPv6 uses the facilities of the Neighbour Discovery protocol, including Router Discovery and Neighbor Unreachability, to perform its L3 movement detection. Upon any movement detection, the node performs DAD on its link-local address, selects a new default router as a consequence of Router Discovery, and then performs Prefix Discovery with that new router to form new care-of address. The mobile node then registers its new primary care-of address with its home agent.

Forming a new Care-of Address

After detecting that it has moved, a mobile node should generate a new care-of address in the foreign link. This can be performed via stateless [30] and stateful [31] address autoconfiguration. The mobile node may use either one or other. In any case, IPv6 addresses will be obtained from the subnet prefixes of each link. The two main motivations are:

1. makes route aggregation achievable.

2. avoids ingress filtering and IP spoofing [32].

Once these processes—home agent discovery, movement detection, new care-of address generation and BU-BA exchange—have been carried out, the mobile node will be fully operative in the foreign domain as it was in the home link.

2.2.7 Route Optimisation

In addition to the exchange of BU-BA between mobile node and home agent, MIPv6 provides for a second mode of communication between the mobile node and a correspondent node. This second mode is based on the so-called 'route optimisation', where the mobile node sends a BU message to the correspondent node. This message is the mechanism by which the mobile node informs the correspondent of its care-of address. On receipt, the correspondent node updates an internal binding cache. Therefore, packets from the correspondent node will

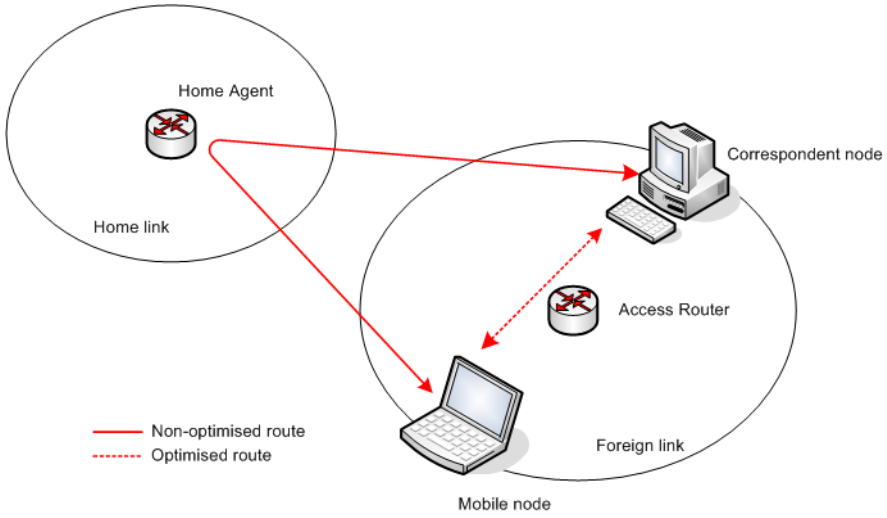


Figure 2.9: Worst case scenario for routing through the home agent

be routed directly to the mobile node's care-of address. This direct path will generally be the shortest path between the nodes and may result in an improvement in QoS—such as reduced jitter, delay and packet loss [33]. This scheme has the additional benefit in that it allows for more efficient use of the network bandwidth (Figure 2.9).

The BU-BA message exchange between mobile and correspondent node is also cryptographically secured, as in the case of the communication between mobile nodes and home agent. The difference lies in, while the security association between mobile nodes and home agent is out of the MIPv6's scope, the security association between mobile and correspondent node is embodied in the Return Routability (RR) procedure. This procedure is an integral part of the MIPv6 protocol.

Mobile and correspondent nodes perform home and care-of address test simultaneously, so the correspondent node checks the reachability of the mobile node at both addresses. This process is carried out by means of the Home/Care-of Test Init messages, and the Home/Care-of Test messages.

On completion of the RR procedures, while sending packets directly to the mobile node, the correspondent node must include the mobile node's care-of address in the IP destination field of the IPv6 header. To enable seamless mobility, a mechanism is required for the mobile node to offer any received packet to its transport layer like it is received at its home address. To allow this, the mobile

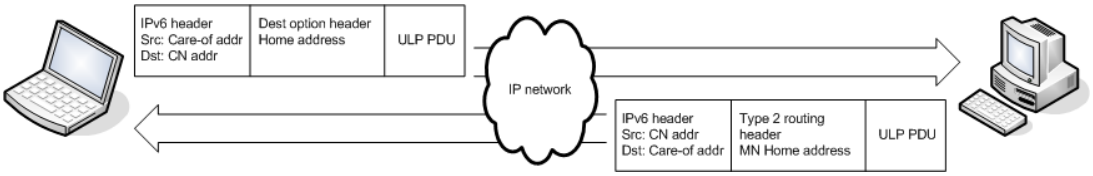


Figure 2.10: Communication over optimised routes

node's home address must be included in any received packets. The reason for this approach to the problem, rather than, i.e. using the binding update list of the mobile node to get the related IP home address to the incoming IP care-of address, is that a mobile node can potentially have several care-of addresses associated to one or more home addresses. Hence, a very same care-of address may be related to different home addresses. If the mobile node is not able to effectively obtain the related home address from the care-of address the packet is sent to, incoming packets will be dropped and connections will be automatically closed.

The mobile node makes use of the Home Address Destination option while sending packets to the correspondent node as explained in Section 2.2.4. In this way, the correspondent node is able to associate the source (care-of) address of the packet to the correct home address. Meanwhile, communications back to the mobile node from the correspondent node include the routing header type 2. These mechanisms provide the mobile and correspondent nodes' upper layer protocols of a transparent, seamless connectivity (Figure 2.10).

Regarding the correspondent node's binding cache, population follows the same mechanism as in the home agent's. Each node stores the bindings for a time period equal to the lifetime field value on the BUs. However, a Binding Refresh Request is used by a correspondent node to request that a mobile node re-establish its binding with the correspondent node. This message is typically used when the cached binding is in active use but the binding's lifetime is close to expiration. The correspondent node may use, for instance, recent traffic and open transport layer connections as an indication of active use [17].

2.2.8 Mobile IPv6 Fast Handoffs

MIPv6 is the *de facto* standard for handover management of roaming users on the IPv6 Internet. After handover, the ability of a MIPv6-enabled node to immediately send packets from a new subnet link depends on the 'IP connectivity'

latency. This latency in turn depends on movement detection, new CoA configuration and home agent's registration latencies.

The afore-mentioned MIPv6 processes are carried out sequentially, and hence latencies are cumulative and represents a performance limitation that may lead to a less satisfactory user experience, particularly for delay sensitive applications.

The Fast Handoffs for MIPv6 (FMIPv6) protocol attempts to perform MIPv6 handovers more intelligently. In order to avoid the handover sub-processes' latency addition, FMIPv6 defines new signalling control functionalities. By rearranging the scheduling of sub-processes, these functionalities adopt a slightly different approach to the classical MIPv6 handover procedure.

The MIPv6 handover process is comprised of the following sequence:

1. Movement detection.

2. Form a CoA in the visited link.

3. Register the new CoA in the Home Agent's Binding Cache.

This scheme corresponds to a *reactive* approach to handover: only after movement has been detected, does the MN start signalling actions to obtain IP connectivity. Alternatively, FMIPv6, illustrated in Figure 2.11, permits a *proactive* approach to handoff: it enables a MN to detect promptly that it has moved or is about to do so through the use of L2 triggers.

These triggers depend on the link layer technology in use and their use is at the implementers discretion. The pre-defined IEEE 802.21 triggers include the following examples: Link Up, Link Down, Link Detected, and Link Parameters, Link Going Down. For instance, via the Link Going Down signal from the L2, the MN could anticipate an imminent handoff with time in advance. In general, acting accordingly with the information received from L2, MNs are expected to improve network performance [8].

So far, the MN is able to discover available APs using link-layer specific mechanisms. Now, to facilitate obtaining other subnets' information, FMIPv6 provides the 'Router Solicitation for Proxy (RtSolPr)' and 'Proxy Router Advertisement (PrRtAdv)' messages. Through the exchange of RtSolPr and PrRtAdv messages, the MN obtains the information known as the '[AP-ID, AR-Info]' tuple. From this information, the MN formulates a prospective new CoA (NCoA) prior handover,

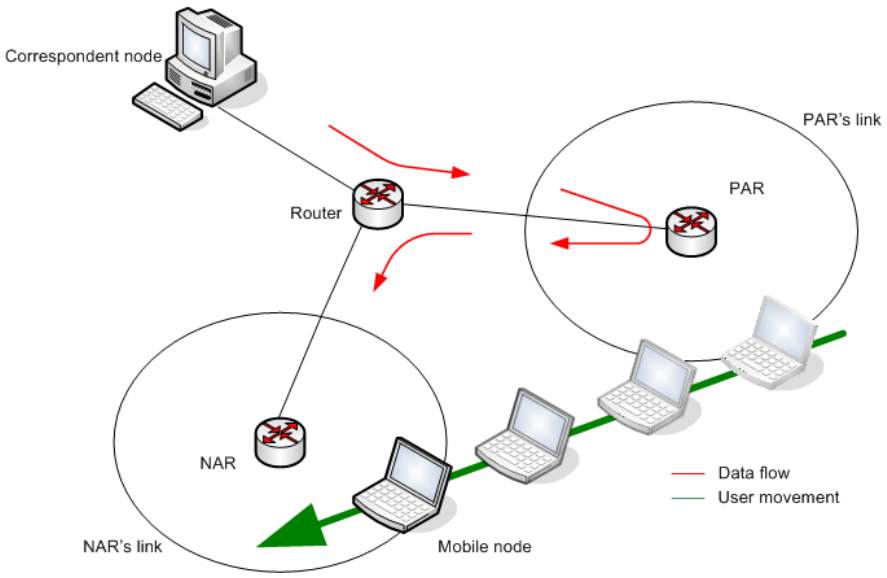


Figure 2.11: FMIPv6 network example

while is still attached to the Previous Access Router (PAR)'s link. This process is executed by means of the 'Fast Binding Update (FBU)' and 'Fast Binding Acknowledge (FBAck)' messages. These messages are exchanged between the MN and the PAR. Thus, immediately after handover the MN can use the NCoA.

Nonetheless, the PAR is not able to check the validity and availability of the NCoA in the new link; as a result of the inability of the PAR to perform 'Duplicate Address Detection (DAD)' in the new link if Stateless Address Autoconfiguration is used. Alternatively, if addresses are being allocated by the NAR, it becomes evident that the acknowledgement must come from the NAR. For this purpose, the access routers exchange messages to confirm that the NCoA is acceptable. FMIPv6 handles this functionality with the 'Handover Initiate (HI)' and 'Handover Acknowledge (HAck)' messages. These two messages offer other important functionalities to FMIPv6-enabled MNs. Firstly, the FMIPv6 protocol specifies an IPv6 encapsulation tunnel between the PAR and the NAR (through HI and HAck, the tunnel is set). Thus, after FBU is sent from the MN to the PAR, still in the PAR's link, the messages addressed to the MN are forwarded to the NAR address, that buffers them. When the MN attaches to the NAR's link, it sends a 'Fast Neighbor Advertisement (FNA)' message to retrieve all buffered messages. Secondly, another important functionality of HI and HAck messages is

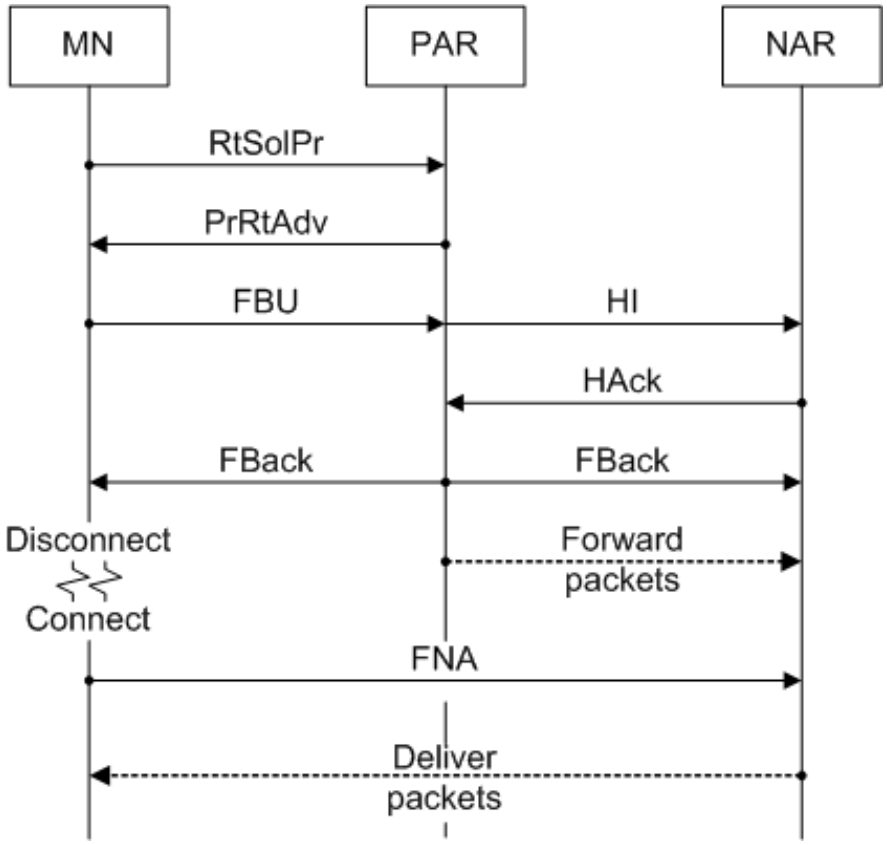


Figure 2.12: Predictive FMIPv6

the network-resident context transference. The routers may exchange information concerning access control, QoS and header compression.

On receipt of the FNA by the NAR, sent by the MN to the NAR once it is attached to NAR's link, the FMIPv6 procedures are complete. Next, the MN behaves as stated previously [18], sending the BU to HA. On receipt of the BA from HA, the MN starts RR procedures for route optimization [17].

Operation

The mechanism by which the MN sends a FBU and receives an FBack on the PAR's link is illustrated in Figure 2.12. This scenario is known as proactive mode. In case the MN does not send the FBU from PAR's link, or does not receive the FBack prior to handover, the reactive mode of operation applies. Reactive mode is illustrated in Figure 2.13.

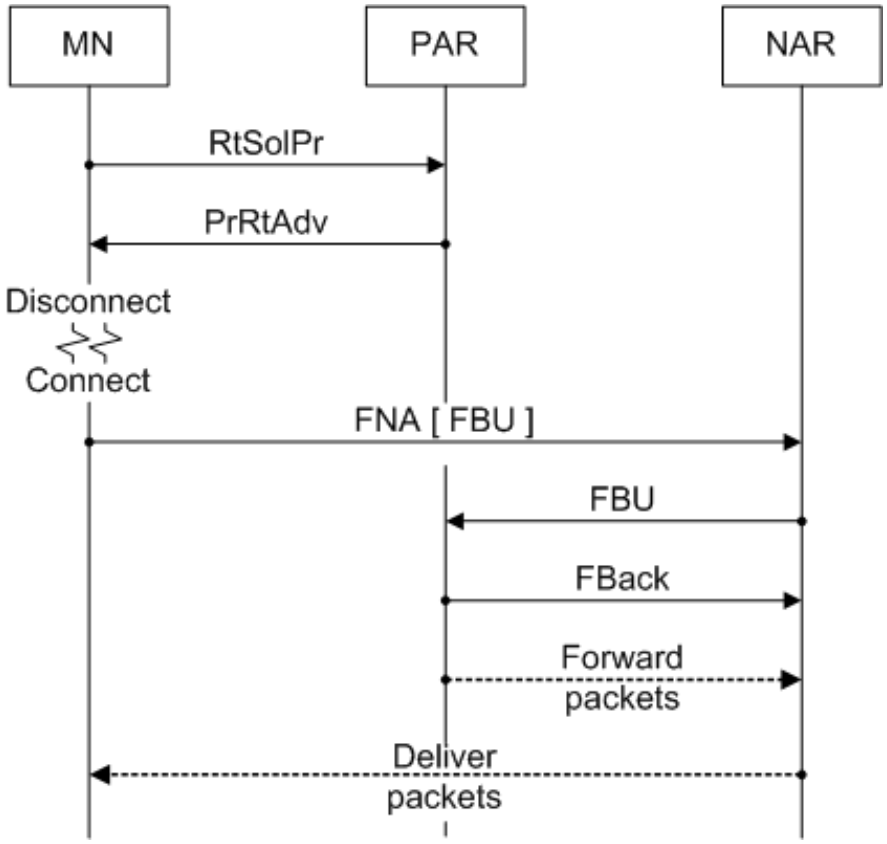


Figure 2.13: Reactive FMIPv6

The MN is provided with network detection and information collection capabilities while still connected to its current subnet. For instance, a MN may discover available access points by means of link-layer specific mechanisms (e.g. a 'scan' in WLAN) and then request subnet information concerning those discovered access points via router discovery.

In the FMIPv6 context, the MN sends RtSolPr to resolve access point identifiers to subnet router information. RtSolPr messages may be sent at any time. However, they are expected to be sent by the MN according to link-layer notifications, referred as 'L2 triggers', e.g. the MN's link-layer may detect another subnet (identified by an AP-ID) with a better quality of signal, prompting the handover mechanisms. RtSolPr contains one or more AP-IDs. Alternatively, RtSolPr may contain a wildcard request, demanding all the available tuples on PAR's memory. According with the requested AP-ID, the PAR will then send a PrRtAdv, as illustrated in Figure 2.14.

The figure shows the different available APs for the mobile node to connect to. In case when the MN wants to join AP A.2, as it is connected to one of the interfaces of AR A, FMIPv6 procedures are not applicable. The handover process is limited to L2. If the next AP does not support FMIPv6, as AP C.1, the PAR will indicate so in the RtSolAdv message. Alternatively, if the next AP is unknown to the PAR, like AP D.1, the MN will have no information upon which make forward progress on the FMIPv6 handover process, and it will have to instigate standard IPv6 procedures for reconnection from AR D's link. It may happen that link layer mechanisms provide the parameters necessary for the MN to send packets. In these cases, the use of RtSolPr and PrRtAdv is optional.

Once the MN is aware of the (AP-ID, AR-Info) tuple, it sends an FBU message. If the MN sends it from the PAR's link, it must use its PCoA. Otherwise, if handover anticipation is not possible, once the MN attaches to the new subnet it must send an FBU encapsulated in an FNA, using its NCoA, although still tentative. The NAR processes then the FBA (FBU) message. If the NAR validates the NCoA, it will forward the encapsulated FBU to the PAR. In response to the FBU from the NCoA, the PAR will send an HI to NAR with code 1 and will start forwarding packets to MN's NCoA.

When the PAR receives an FBU from the PCoA, it sends an HI message to the NAR with code 0. The NAR's address is determined by performing the

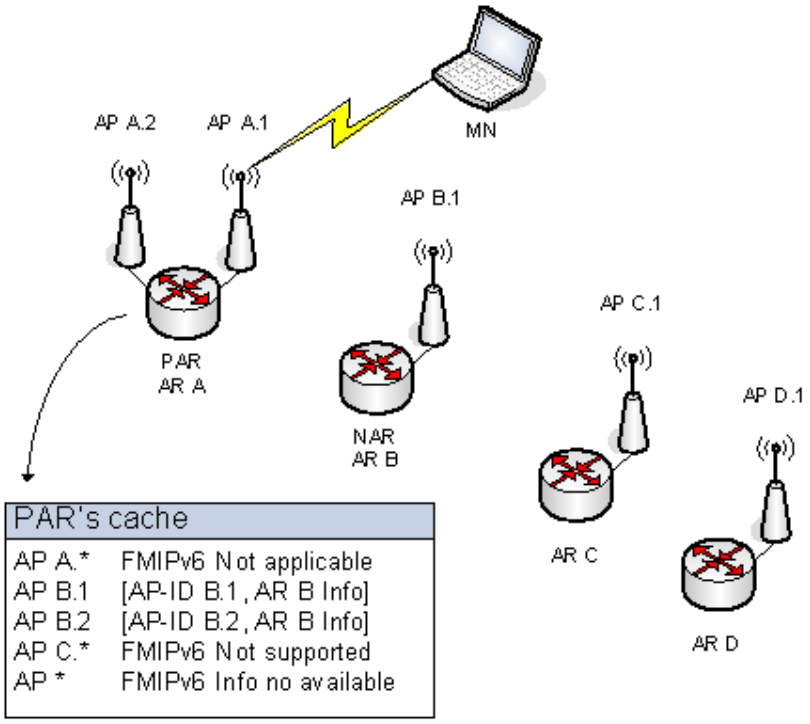


Figure 2.14: PAR cache example

longest prefix match of the NCoA (included in the FBU) with the prefix list of neighbouring routers. The HI message includes the MN's PCoA, NCoA and Link-layer Address. In response to the HI message with code 0, the NAR performs DAD of the NCoA in its link. The NAR answers the handover request with a HAck message. If HI includes code 1, the NAR will skip this process as it was carried out while processing the FNA.

On receipt of a HAck, the PAR must create a binding between the PCoA and the NCoA and send an FBack message to both previous and new links. The FBack will be either received by MN if it is still connected to the PAR's link, or buffered by the NAR. When the MN establishes connectivity with the NAR, it should send a Fast Neighbour Advertisement (FNA). The NAR will forward the buffered packets addressed to the MN. Exception handling is very limited in the FMIPv6 protocol. In any case, if the NCoA is not accepted by either PAR or NAR, MN will start reactive mode of operation.

2.2.9 Alternative Layer 3 Approaches

There are a number of alternatives to the MIPv6/FMIPv6 handoff scheme. This section considers two other relevant solutions, viz. the Proactive Bindings for FMIPv6 and Enhanced Route Optimisation protocols [19, 20].

Proactive Bindings for FMIPv6

In standard FMIPv6, after L2 handoff has taken place, the MN must update the HA and, optionally, the CN(s) with its NCoA. In order to do so, the MN exchanges a BU and a BA with its HA, and subsequently initiates the RR procedure with its CN. These exchanges incur latencies. Proactive Bindings for FMIPv6 (PB-FMIPv6) [19] aims to reduce the route optimisation signalling latency in FMIPv6 by delegating to the NAR the tasks related to NCoA registration with the HA and CN(s), i.e. the RR procedures (Fig. 2). These tasks are conducted while the MN is in the process of performing link layer handover.

The process is as follows. The Proxy NAR (PrNAR), on receipt on the HI message, composes a prospective NCoA and sends create a binding with the HA on behalf of the MN via the BU and BA message exchange. Likewise, the PrNAR conducts RR towards route optimisation on behalf of the MN: home

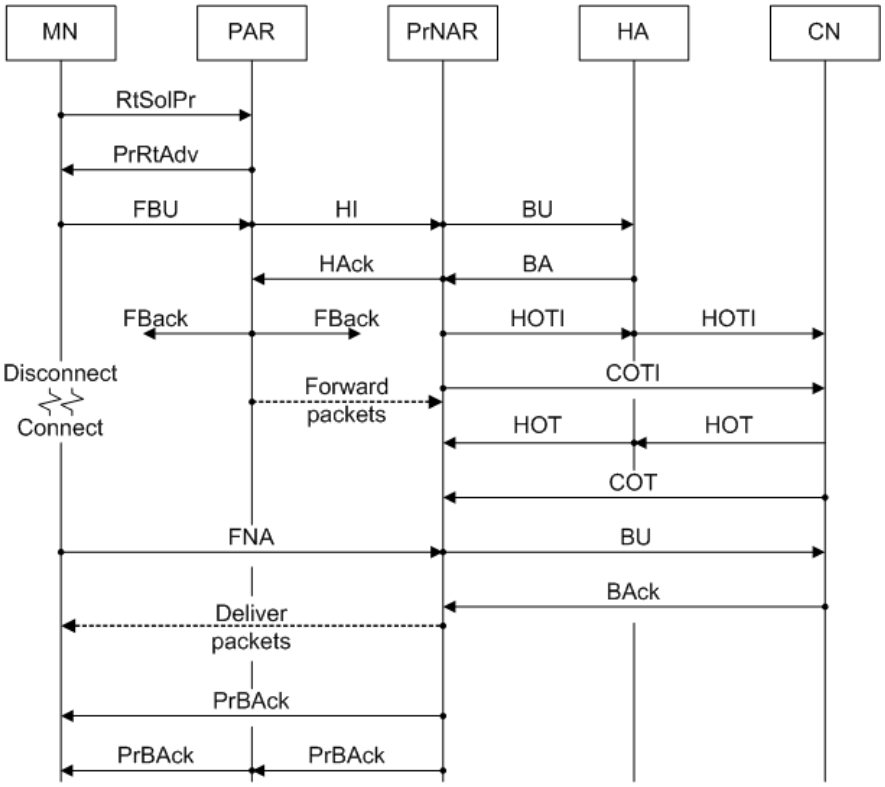


Figure 2.15: PB-FMIPv6 signalling

and care-of reachability tests are facilitated by the HoTI-HoT and CoTI-CoT message exchanges and finally, the CN binding is done via a BU and BA exchange. Consequently, this approach takes advantage of the simultaneous execution of RR and MN's link layer handover, and therefore, the overall latency of standard FMIPv6 handover may be reduced.

Enhanced Route Optimization

Enhanced Route Optimization (ERO) specifies an enhanced version of the Mobile IPv6 RR procedure. With ERO, the home address test, i.e. the HoTI-HoT exchange is preformed proactively prior to handover hence avoiding the associated cumulative latency. The home address test provides strong authentication because the home address is a Cryptographically Generated Address (CGA). This type of address has the property of being verifiably bound to a public/private key pair. In this manner, the MN proves ownership of the home address by evidencing knowledge of the corresponding private key. These stronger security facilities

preclude attacks from nodes on the home address test path (between MN and HA), permitting longer binding lifetimes and consequently reducing the signalling overhead.

Secondly, a RR-like care-of test is also performed after handoff, to check the reachability of the MN at the NAR link. However, unlike the standard RR procedures, an early BU-BA piggybacked within the CoTI and CoT messages permits immediate re-establishment of direct communication via the MN's NCoA. While this early binding of PCoA and NCoA takes place, ERO evaluates the reliability of the communication in order to avoid DoS attacks by flooding the NAR's link. This process makes use of 'credits' to temporarily limit the traffic volume between the CN and NCoA until the NCoA has been fully authenticated. The MN earns 'credits while receiving traffic at the NCoA, and the amount of traffic that the MN can send to the MN is related with its credit count: the trust relationship between the CN and the MN is based on a balanced upload/download traffic figure.

After the care-of test is concluded, the MN updates its binding at the CN via a RR BU-BA exchange. This last step completes the signalling process after handoff. At this point, credit-based DoS control does no longer apply as the MN has securely updated the binding at the CN.

Figure 2.16 illustrates ERO in a FMIPv6-enabled environment. Interestingly enough, the figure depicts the most favourable case concerning handover latency: in this scenario, the MN has previously performed the home test, so the CN trusts the MN's reachability though its home address. The MN also benefits from the enhancements provided by the early binding update process.

Strengths and Weaknesses of Existing Solutions

The PB-FMIPv6's NAR acts as a proxy on behalf of the MN to conduct the RR signalling tasks. In comparison with standard FMIPv6, this approach may be advantageous in those cases where the NAR receives the HI message before the MN joins the new link. Two factors determine whether this occurs: the end-to-end delay between the PAR and the NAR, and link layer handover delay. In the special case where the HI message arrives earlier than the MN at the new link, this approach represents an advantage in terms of overall signalling latency: while the mobile node is still carrying out link layer handover, the NAR performs

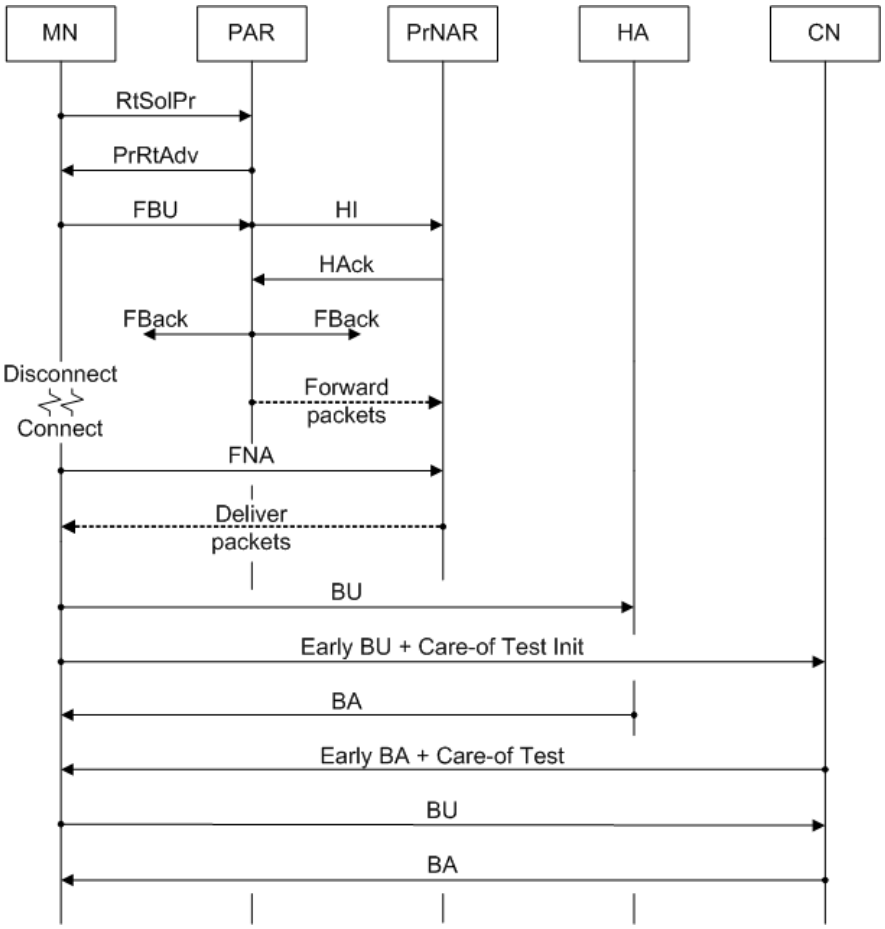


Figure 2.16: ERO signalling

route optimisation. Otherwise, in those cases where the link layer handover delay is lower than the message trip time from the PAR to the NAR, the MN will join the new link before the NAR has been triggered to start the signalling procedures, thus incurring avoidable delays.

Also, Nikander et al. [34] suggest that the RR procedure may be vulnerable to attacks from nodes on the path along the CN and the MN. Under this premise, MIPv6 specifies that the packet payload should use end-to-end protection such as IP security (IPsec). However, MIPv6 MNs may still suffer denial of service or flooding.

One of the aims of ERO is to securely authenticate MNs without preconfigured credentials or public-key infrastructure. In order to do so, ERO relies heavily on a secured exchange of a home address keygen token. This token is used for cryptographic authentication of the MN in successive CN registrations. However, this does not stop attackers from redirecting traffic to another care-of address. Reachability of the MN at NCoA must be checked. For this reason, ERO performs the care-of test that, for performance reasons, can be concurrently carried out with an early BU-BA exchange. On completion of the Care-of Test, the MN must send a BU to the CN, which replies with a BA.

However, ERO's credit-based system introduces a significant limitation on the data transmission performance, as the CN has an upper bound for the packet transmission rate which is equal to the data reception rate from the MN. In cases where the communication is asymmetric, e.g. video- or audio-streaming, or file transfer, the MN will only communicate with the CN to acknowledge the data received. The CN will then have a restricted transfer capability as long as the amount of data able to be sent to the MN is equal or lower than the addition of the acknowledgment packet payload sizes received from it. Alternatively, in those cases where MN and CN have established a bi-directional communication, e.g. VoIP, the MN will have to wait a RTT from its care-of to the correspondent address to start receiving packets and will impair perceived QoS. For these reasons, the ERO credit-based system constrains the data throughput of the system.

On the positive side, both systems do offer relevant handoff performance improvements in some given circumstances. Nonetheless, truly seamless handoffs call for schemes that further reduce the handoff signalling latency, offering high interoperability in heterogeneous networks. In keeping with this principle, many

research contributions address alternative schemes to the RR-based protocols. For example, Hierarchical MIPv6 [35] relies on the deployment of *local* home agents and, by providing the mobile users of a local and a regional IPv6 address, managing in an optimised manner local and global (inter-site) mobility; Location Independent Networking for IPv6 [36], Host Identity Protocol [37, 38] rely on administrative agreements and tunnelling schemes.

Other approaches have not gained that much attention from industry and research communities. Rossi et al. [39] further improves the MIPv6 route optimisation security. This work relaxes the security assumptions made at the design of RR, thus considering potentially devastating the interception of HoT messages. This work presents a combined solution based on first, a strong CGA association between the PCoA and the NCoA—making it more resilient to replay and time-memory tradeoff attacks while increasing the brute-force computational complexity, as it would be as secure as the number of bytes of the PCoA and the tokens length combined. Secondly, the security certification management is managed via DNSSEC, under the assumption that mobile network operators put in place trusted domain authority servers for scalability purposes.

In the literature, other works can be found based on less realistic assumptions. For instance, Shi et al. [40] proposes a one-message exchange route optimisation scheme, based on a global-scale PKI infrastructure. In turn, Susanto et al. [41] explores the use of a pool of pre-generated pool of keys for securing the communication with the CN. This pool of keys is generated when first end-to-end session between MN and CN is established. At the following handoffs, route optimisation message exchange is secured using exclusively these keys. Since there is no reachability check at the NCoA, this scheme opens venue to flooding attacks. Moreover, since the keys are exchanged in plaintext, an eavesdropper could hijack the session.

2.3 TCP Behaviour at Handoff

TCP is probably the most widely used transport protocol within networking's most popular applications, including the World Wide Web (WWW), E-mail, File Transfer Protocol, Secure Shell, peer-to-peer file sharing, and some streaming media applications. TCP provides these applications a reliable stream delivery

system, guaranteeing in-order packet delivery and avoiding packet loss and duplication. In order to achieve this, TCP relies upon monitoring of the packet reception characteristics, and on a set of transmission control mechanisms.

When the transfer flow fluctuates, e.g. due to packet reordering or loss, these mechanisms react taking conservative measures to stabilise the flow. Since, mobile environments in general, and handoff in particular, impact the TCP flows. This section explains standard TCP operation, addressing precisely the problems that affect the standard TCP protocol in this context and presents some of the existing solutions. Chapter 5 will introduce this thesis' proposal for improving TCP performance at handoff.

2.3.1 The TCP Machinery

Reliable transport protocols such as TCP are primarily designed for traditional (wired) networks where packet losses mostly occur because of congestion. However, networks with wireless and other lossy links also suffer from significant losses due to channel bit errors and handoff disruption. TCP responds to all losses by invoking congestion control and avoidance algorithms, resulting in degraded end-to-end performance in wireless and lossy systems [42]. Each TCP packet is associated with a sequence number, and only successfully received in-order packets are acknowledged to the sender by the receiver, by sending corresponding packets (acknowledgements, ACKs) with sequence numbers of the next expected packets. On the other hand, packet loss or reception of out of-order packets indicates failures. To eradicate such failures, TCP implements flow control and congestion control algorithms based on the sliding window and additive increase multiplicative decrease (AIMD) [43] algorithms, and the use of four different timers:

- Retransmission Time-Out (RTO) timer: this timer is used to detect when a segment should be retransmitted because it has not been acknowledged by the receiver.
- Persist timer: this timer keeps the end-to-end flow information.
- Keepalive timer: this timer detects when the other end is unreachable.
- 2 Maximum Segment Lifetime (2MSL) timer: this timer measures how long a connection has been idle.

In the TCP flow control both the TCP sender and the TCP receiver participate. The receiver must advertise, at connection establishment, its maximum capacity to process the segments received; this value is known as the *receiver's window*, or *rwnd*. However, this information does not permit either the sender or the receiver to control the congestion derived from the TCP flow at intermediate nodes or along the path along which the TCP flow is running. For that reason, TCP implements further flow control functionalities. TCP flow control functionalities are embodied in four intertwined mechanisms: slow start, congestion avoidance, fast recovery and fast retransmit. These mechanisms are introduced next.

1. Slow Start

   The slow start algorithm is used by a TCP sender to control the amount of outstanding data that injects into the network. This mechanism makes use of two per-connection status variables, namely, the *congestion window*, or *cwnd*, and the *slow start threshold*, or *ssthresh*. The cwnd is a sender-side limit on the amount of data that can be transmitted before receiving an ACK for the outstanding data. The connection's maximum outstanding data is determined by the minimum of cwnd and rwnd.

   At the beginning of a transmission passing through a network with unknown conditions, TCP makes increasing use of the available capacity to avoid congesting the network with an inappropriately large transmission rate. The slow start algorithm is used for this purpose at the beginning of the transmission, or to reduce the congestion as indicated by the expiration of an RTO timer. When slow start is triggered, the cwnd is initialised to one segment. Each time an ACK is received, the cwnd is increased by at most one segment[1]. After the first RTT seconds, the sender would expect to double the cwnd as a consequence of receiving an ACK. In the next round (i.e. 2·RTT seconds) two ACKs would be received by the sender, what would double the cwnd size. Therefore, during slow start there is an expectation that the cwnd size will increase exponentially according to Equation (2.1), where n is the current round (or times RTT seconds) since

[1]For the purpose of this discussion, both cwnd and rwnd are maintained in bytes [44]. However, slow start manages the cwnd in Sender Maximum Segment Size(SMSS) units [45]

slow start was triggered. This iterative process ends when cwnd exceeds the ssthresh or when congestion is observed.

$$cwnd = SMSS \cdot 2^n \tag{2.1}$$

When the cwnd exceeds the ssthresh, TCP enters into congestion avoidance.

2. Congestion Avoidance

   Congestion avoidance is used when the cwnd value is higher than the ssthresh. During congestion avoidance, the sender increases the cwnd by one full-sized segment per RTT. In most implementations, TCP updates the cwnd according to Equation (2.2) each time a non-duplicate ACK (non-DUPACK) is successfully received. Equation (2.2) provides a fair approximation to increase one segment each RTT, thereby giving rise

$$cwnd = cwnd + \frac{SMSS \cdot SMSS}{cwnd} \tag{2.2}$$

   When the TCP sender detects segment loss by means of the RTO timer, it sets the value of ssthresh according to Equation (2.3)

$$ssthresh = \max\left\{\frac{Flightsize}{2}, 2 \cdot SMSS\right\} \tag{2.3}$$

   where $Flightsize$ is the amount of data outstanding in the network. Furthermore, on expiration of an RTO timer the TCP sender resets the cwnd to one segment, regardless of the value of the initial window, and retransmits the lost segment. The TCP sender uses then the slow start algorithm to increase the cwnd from one full-sized segment until it exceeds the value of ssthresh; at this point the congestion avoidance algorithm takes over.

   Duplicated Acknowledgements (DUPACKs) also provide information of packet loss. However, receipt of DUPACKs indicates loss of segments due to sporadic effects of the network, rather than due to congestion. For this reason, DUPACKs are treated differently than RTO expiration. The mechanisms that handle DUPACKs, namely, fast retransmit and fast recovery, are explained next.

3. Fast Retransmit

   TCP uses the fast retransmit mechanism [45] to detect and repair packet loss. Fast retransmit is based on the assumption that DUPACKs are sufficient indication of packet loss. Fast retransmit is triggered on receipt of three DUPACKs (four identical ACKs received sequentially without any other intervening packets). After receiving three DUPACKs, the TCP sender retransmits what is the allegedly lost packet, without waiting for the RTO timer to expire.

4. Fast Recovery

   After receipt of a DUPACK, fast retransmit governs the transmission of segments until a non-DUPACK arrives. As highlighted before, a DUPACK not only indicates that a segment has been lost, but also indicates that other segments are being correctly transferred, and therefore are not making use of the network resources. The TCP sender can inject new segments to the network, but using a reduced cwnd [44, 45]. The process is as follows: on receipt of the third DUPACK, the TCP sender sets ssthresh according to Equation (2.3). Next, it retransmits the supposedly lost segment and sets cwnd to ssthresh+3. This artificially inflates the cwnd to cope with the number segments that have already left the network (three). For each additional DUPACK received, the sender is to increase the cwnd by SMSS. This would increase the cwnd to reflect the segments already received by the their addressee. Subsequently, if cwnd>0, the sender transmits as many segments as allowed. On receipt of an ACK that acknowledges new data (points to a segment number higher that the one included in the DUPACKs), the sender sets the cwnd to ssthresh to "deflate" the cwnd.

TCP Reno [45, 46] is one of the most widely adopted TCP schemes. It implements the four intertwined congestion control mechanisms previously described: slow start, congestion avoidance, fast recovery, and fast retransmit. TCP maintains two variables, the cwnd, which is initially set to be one SMSS, and the ssthresh. An example case follows. At the beginning of a TCP connection, the sender enters the slow start phase, in which cwnd is increased by one MSS for every ACK received; thus, the TCP senders cwnd grows exponentially in RTTs. When

cwnd reaches ssthresh, the TCP sender enters the congestion avoidance phase. Reno employs a sliding window-based flow control mechanism allowing the sender to advance the transmission window linearly by one segment upon reception of an ACK, which indicates the last in-order packet received successfully by the receiver. When packet loss occurs at a congested link due to buffer overflow at the intermediate router, either the sender receives DUPACKs, or the senders RTO expires. These events activate TCPs fast retransmit and recovery, by which the sender reduces the size of its cwnd by half and then linearly increases cwnd as in congestion avoidance, resulting in a lower transmission rate to help relieve the link congestion.

2.3.2 TCP Assumptions in Wireless Environments

TCP's assumptions on wired links are not always applicable to wireless links. Whereas packet reordering and duplication, as indicated by the receipt of DUPACKs, can be addressed by the fast retransmit and recovery mechanisms, network congestion, as indicated by the expiration of the RTO timer, is addressed by slow start and congestion avoidance. However, these mechanisms build on the behaviour of wired links, which typically show lower BER and higher capacity than the wireless links. Therefore, TCP deals with the wireless link-level capacities, avoiding congestion by means of maintaining lower values of the cwnd (than in a purely wired network), although BER is the main reason for the decrease in the performance of TCP.

To cope with the relatively poor BER associated with the wireless medium, wireless links usually implement their own error correction and avoidance mechanisms similar to those of TCP. For instance, IEEE802.11b/g [47, 48] makes use of the 'Request To Send' and 'Clear To Send' airframe exchange to avoid the *hidden terminal* problem, which could produce airframe collision. Likewise, cellular systems, such as WCDMA, allow for retransmissions of the lost airframes. However, these processes incur higher end-to-end delays in the communication system, which could lead to further congestion especially if the RTO timer expires before an ACK is received. This would cause the TCP sender to retransmit the original (unacknowledged) data segment. Both the original and the retransmitted segment would arrive at the receiver. The receiver would therefore generate

two ACKs for the same segment. In the eventuality that the TCP sender receives three DUPACKs, it will trigger the fast retransmission algorithm explained above, bringing down the cwnd size and retransmitting the allegedly lost segments. Unnecessarily triggering the fast retransmit algorithm reduces the throughput of the TCP flow and results in a poor link utilisation.

It becomes evident that wireless links have a derogatory impact on TCP flows. However, there is an expectation that current trends will lead to a full use of the concept of wireless mobility, i.e. the capability of users to freely move geographically and 'move' flows between APs and potentially multiple interfaces. Additionally, not only user behaviour but also communication networks have evolved greatly in the past decade. Packet switching technologies have merged the traditional voice and data networks together into converged and integrated multimedia networks. The horizon of the converged and integrated network is extending further to incorporate wired, wireless, and satellite technologies. The all-IP wired and wireless heterogeneous network is becoming a reality. TCP/IP has become the dominant communication protocol suite in today's multimedia applications. Hence, TCP/IP needs to depart from its original wired network oriented design and evolve to meet the challenges introduced by heterogeneous networking.

2.3.3 TCP Challenges in Mobile Environments

With the advances of wireless technologies and ever-increasing user demands, the IP protocol suite has to extend its capability to encompass the wireless aspect. Every likelihood, future all-IP networks will most be heterogeneous, implying that the communication path from one end to another will consist of both wired and wireless links. However, the TCP mechanisms used and relied upon in wired networks exhibit weaknesses in hybrid environments. The problems stem from the unique characteristics of wireless links as compared to wired links; the current TCP's design assumption of the packet loss model (inherently higher bit error rates of wireless links compared to wired links), and the effect of temporary disconnections due to handoff or signal fading. The problems manifest in applications in the form of degradation of throughput, inefficiencies in network resource utilisation, and excessive interruption of data transmission.

More specifically, during a MIPv6 or FMIPv6 handoff, the MN is not able to receive or acknowledge any TCP segments. Depending on the handoff delay, the packet loss and reordering patterns, and the congestion control mechanisms used by the CN, retransmission time-outs (RTOs) may expire or fast retransmission procedures may be triggered. For instance, at handoff, even if a single packet is lost, the current standard implementation of TCP assumes that the loss was due to congestion and throttles the transmission by bringing the congestion window down to the minimum size. Coupled with the TCP slow-start mechanism, such an action means that the sender unnecessarily holds back, increasing the transmission rate, even though the receiver often recovers quickly from the temporary, short disconnection. This is mathematically explained in Appendix B where it can be seen that the network capacity can remain partially underutilised for a while even after a reconnection. Related issues are explored in detail in Chapter 5.

2.3.4 Existing Solutions

There are a number of research contributions to the shortcomings of standard TCP. The forthcoming discussion presents some of the most relevant approaches.

SNOOP

The SNOOP protocol [49] is a TCP-aware link layer protocol designed to improve the performance of TCP over networks consisting of wired and single-hop wireless links. The main problem with TCP performance in networks that have both wired and wireless links is that packet losses that occur because bit-errors are mistaken by the TCP sender as being due to network congestion, causing the sender to drop its transmission window and often time out, resulting in degraded throughput. The Snoop protocol works by deploying a *SNOOP agent* at the base station capable of performing retransmissions of lost segments based on duplicate TCP acknowledgments (which are a strong indicator of lost packets) and locally estimated last-hop round-trip times. The agent also suppresses duplicate acknowledgments pertaining to wireless losses from the TCP sender, thereby preventing unnecessary congestion control invocations at the sender. This combination of local retransmissions based primarily on TCP acknowledgments, and suppression of duplicate TCP acknowledgments, is the reason for classifying SNOOP as a

transport-aware reliable link protocol. The state maintained at the base station is soft, and thus does not complicate handoffs or overly increase their latency. The scheme has been shown to yield significant throughput improvements for TCP environments limited by single-hop wireless in-building links.

For data transfers from the mobile host, SNOOP supports a mechanism called Explicit Loss Notification (ELN), which is use to implement a link-aware transport protocol. With ELN, TCP uses hints from base stations in the network and/or the receiver (an inter-node cross-layer signalling scheme) to decouple retransmissions from congestion control. This helps TCP perform congestion control only for congestion-related losses and not for losses that result from data corruption.

The SNOOP protocol could be regarded as the key contribution to wireless link error-related throughput degradation. Other approaches also address this problem, such as ITCP [50], MTCP [51] and M-TCP [52]. Among other striking differences, these protocols split the connection between the receiver and the sender at an intermediary mobility support node (equivalent to the MIPv6 home agent). Splitting a connection, however, presents some adverse consequences as explained later in this section.

Freeze-TCP

The Freeze-TCP scheme [53] is based on a proactive (prior to handoff) signalling exchange between the MN and the CN. A MN can possibly predict and detect an impending handoff if, for instance, the signal strength is fading. Alternatively, a MN may be asked by its network operator to carry out handoff. In both scenarios, the MN is aware beforehand of the imminent handoff. Freeze TCP makes use of this lead time by notifying the CN of the handoff event. On receipt of the notification, the CN pauses the congestion control mechanisms and therefore the lack of acknowledgements does not result in a reduction of the congestion window.

Freeze-TCP takes on an end-to-end approach to flow control at handoff for MNs. Experience of deployments of ITCP, MTCP, M-TCP and ESBN highlights the importance of a self-consistent end-to-end approach that does not require the involvement of any intermediary nodes, such as base stations, to cooperate in the L4 signalling. Freeze-TCP approach does not require any changes on the sender side or intermediate routes either; modifications to TCP are restricted to

the receiver side, making possible to interoperate with the existing infrastructure. Therefore, relying in an end-to-end unilateral TCP re-design is beneficial for the sake of scalability and interoperability.

Freeze-TCP works as follows. When the MN detects an impending handoff, it should try to send at least one ACK, advertising a zero window (ZWA) size. On receipt of a ZWA, the CN enters zero window probe (ZWP) mode, therefore avoiding any reduction of its congestion window. During the ZWP mode, the CN repeatedly sends zero window probes. Even if these messages are lost, the CN does not reduce the congestion window size. However, those data segments injected to the network before the ZWA is received remain timed by the RTO. In order to avoid triggering the RTO for the outstanding data sent before the ZWA is received, Freeze TCP proposes sending the ZWA in advance, before handoff. This time period, referred to as the 'warning period', ideally should be long enough to ensure at least one ZWA and all outstanding data reach the CN. If the warning period too long, the CN will be forced into ZWP prematurely, thereby leading to idle time prior to handoff taking place. Otherwise, if the warning period is too short, the MN may not be able to send the ACKs for the incoming data. Also, if this warning period is not sufficiently large, the MN may not be able to send out the ZWA, so the CN would not enter the ZWP mode which will the triggering of the congestion control mechanisms; as a consequence of the ensuing the packet loss during disconnection. Therefore, the warning period must be chosen according to the connection-specific variables. Freeze-TCP sets this value to the RTT. During periods of bulk data transfer, such a value allows a receiver to send out a ZWA and to acknowledge all the in-flight data segments. Numerical evaluation highlights the adequacy of setting the warning period to the RTT value. Warning periods distant from the RTT value result in poorer average performance.

The TCP sender exponentially backs off sending ZWPs. Therefore, a MN can undertake fairly long handoff delays. However, if the MN loses a ZWP from the CN, there is the possibility of a substantial idle time after re-connection, since the CN backoffs some time after the ZWP is sent. This is an inconvenient because, after handoff, the flow would be resumed after this idle time. To avoid this idle time, Freeze TCP makes use of the fast retransmit algorithm as follows. After handoff is completed, the MN sends three DUPACKs for the last data segment

Table 2.1: Priorisation of the Access Classes

Priority	Access Class	Application Type
1,2	AC_BK	Background
0,3	AC_BE	Best Effort
4,5	AC_VI	Video
6,7	AC_VO	Voice

received prior to sending the ZWA. In response, the CN will trigger the fast retransmit algorithm. The CN will not bring down the congestion window size in those cases where packet loss did not occur.

Yoshimoto('07)

As mentioned previously, when a MN which has an ongoing communication carries out handoff, the QoS may deteriorate as a consequence of the sender reducing the congestion window size when RTO timeouts. The solution provided by Yoshimoto et al. [54] permits immediate recovery of the congestion window without modification to TCP, but rather building upon the facilities provided by the IEEE 802.11e Enhanced Distributed Channel Access (EDCA) protocol. EDCA is defined as a MAC method for IEEE 802.21e based on Carrier Sense Multiple Access with Congestion Avoidance (CSMA/CA). Among other functionalities, it facilitates setting different priority levels to data packets. EDCA supports eight priority levels classified into four main priority classes called Access Categories; shown in Table 2.1. By varying the priority of the packets sent to the MN, this approach rapidly recovers the congestion window.

Before handoff, the sender (CN) transmits packets to the receiver (MN) with low priority: the flow is classified as AC_BE and the APs forward packets accordingly with this Access Category. On receipt of an trigger indicating impending handoff, the MN sends a 'Handoff Execution' notification to the CN and starts handoff. When the CN receives the notification, it stops sending data until further notification. As a consequence of the disruption interval derived from handoff, the MN does not inject any further ACKs into the network causing the RTO timer to expire and thereby reducing the congestion window. After handoff, the MN sends a 'Handoff Completion' notification to the CN. On receipt of this notification, the CN raises the packet flow priority to AC_VO. The flow, once prioritised

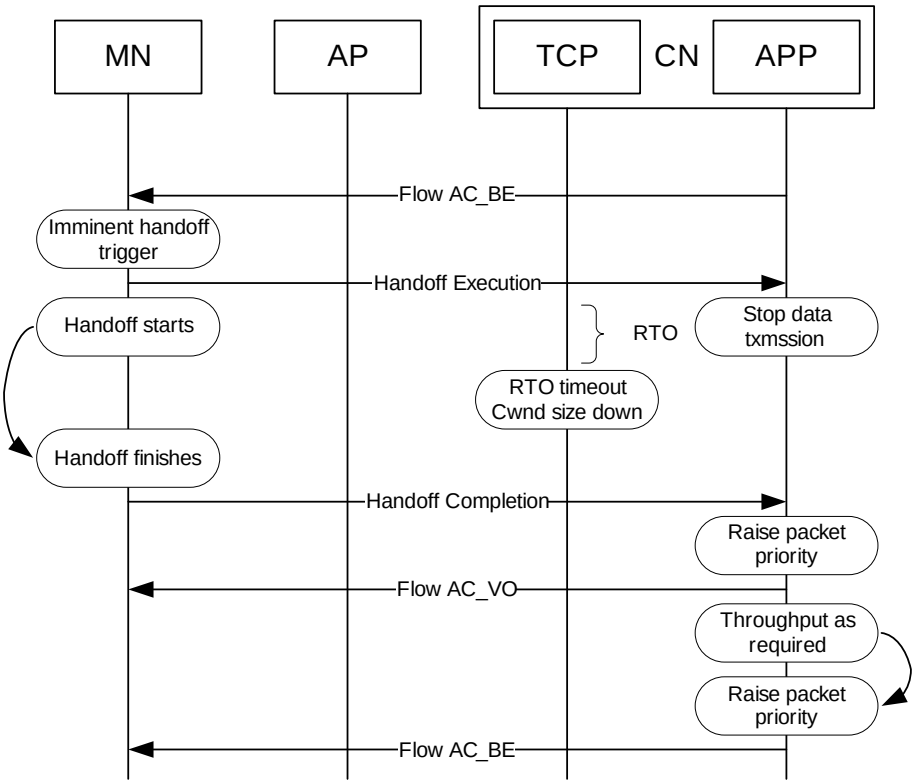


Figure 2.17: Flow in Yoshimoto('07)

over other intervening transmissions on a contended medium, will prompt a more rapid increase on the congestion window. As a result, the congestion window will quickly converge to the value required by the application requirements or bound by the network capacity. However, raising packet priority may compromise the throughput of other existing transmissions. To mitigate any unfairness, the CN subsequently lowers the packet priority to AC_BE. Figure 2.17 illustrates the aforementioned process.

This scheme presents several inconveniences. First and most importantly, notifications are sent to and from the CN and MN's application layers. That implies that modifications should be made to every user's application's code to ensure interoperability. Secondly, it is assumed that the TCP flow is initially classified as AC_BE, so that at handoff the CN raises its priority level to AC_VO to cope with the reduced congestion window size [54] . The consequences of this approach for other flows competing on the link are not clear. Presumably, if these

other flows are AC_BE, the scheme will effectively drive the congestion window into the congestion avoidance stage quicker than under non-prioritised conditions. However, there is a need to explore the effects of this scheme when other flows have different prioritisation. Thirdly, this scheme's scope is limited to IEEE 802.11e-enabled networks. All these points constrict the large-scale applicability of the scheme.

Le('06)

Le et al. [55] also propose a mobility-aware approach for enhancing TCP performance at handoff based on MIPv6. In common with Freeze TCP and Yoshimoto('07), and in keeping with the end-to-end semantics of TCP, this work implements explicit 'Handoff Initiation' and 'Handoff Termination' notifications, sent by the MN prior to and after handoff respectively. On receipt of a Handoff Initiation notification, the CN pauses the TCP congestion control mechanisms. During handoff, the CN does not bring down the congestion window size. After the MN has completed handoff, it sends the Handoff Termination notification to the CN. On receipt of this notification, the CN ignores the outstanding segments in the send window, which are in flight by the time the MN starts handoff. MIPv6 does not permit these packets to be diverted to the MN's NCoA, and therefore are lost. The CN reacts by retransmitting these segments. Secondly, the CN quickly estimates the available capacity along the new path [56] and sets the congestion window size and ssthresh accordingly. Finally, the CN resets the bogus timing parameters. The reason for this is that, in addition to the handoff latency, and since the RTT may vary significantly in heterogeneous environments, traditional TCP artificially inflates the RTT and RTO values. This work reinstates the RTT/RTO from the RTT value acquired from the new network.

Strengths and Weaknesses of Existing Solutions

These existing solutions have been preliminarily evaluated in the foregoing discussion. However, if these schemes are to cooperate in highly dynamic heterogeneous networks they should assessed more deeply with regard to the following:

1. Capability of inter-operation with the existing infrastructure. Ideally, there should be no requirement for modification of the intermediate routers or the

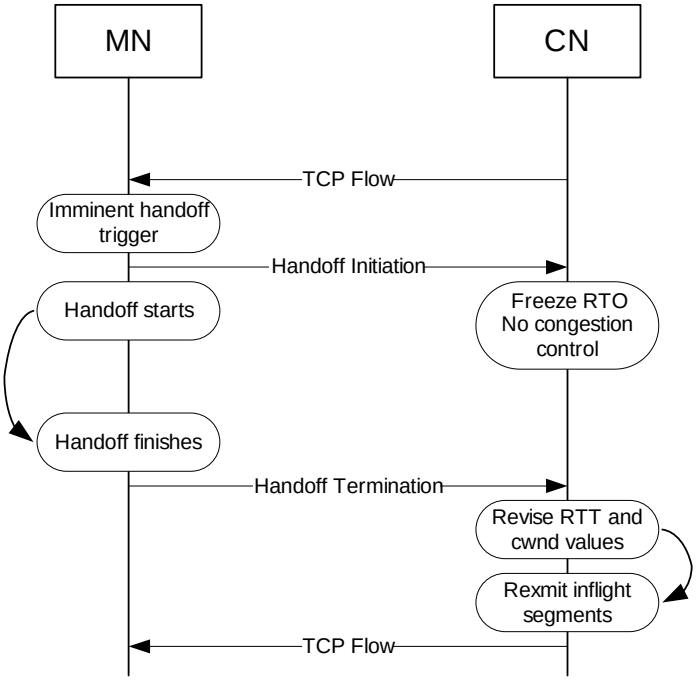


Figure 2.18: Flow in Le('07)

participating nodes because, particularly in the case of heterogeneous networking, these may belong to different communication companies, network carriers or MVNOs. This consideration affects ITCP, MTCP and M-TCP, which split the connection in two or more segments. Moreover, it would be desirable to obtain the maximum benefit out of new network and protocol deployments. For instance, the FMIPv6 provides of packet buffering capacity the router in the visited link (of the considered schemes only ITCP and MTCP provide buffers).

2. Capability of handling encrypted traffic. As network security is becoming increasingly critical due to the deployment of networks, wireless access technologies and operators, encryption is likely to be widely adopted. Any scheme that requires intervening intermediate nodes will fail to handle encrypted traffic. Some solutions which, in turn, yield lower performance, are presented in Goff et al. [53].

3. Capability of pervasive management of the communication. Data segments and their corresponding ACKs may take different paths. "Man-in-the mid-

dle" approaches (SNOOP, I-TCP, MTCP) may have difficulties in intercepting the packets. Such a case becomes specially challenging when the nodes are multihomed.

4. Capability of roaming freely in an arbitrary network topology and across different RATs. Some of the existing solutions rely on link level notifications (like SNOOP) or they present some extent of link coupling—I-TCP, MTCP, Yoshimoto('07). Vertical handoffs, however, may involve different RATs and access networks where signalling protocols and link dynamics may be different. Thus, the need for link-decoupled approaches.

5. Capability of rapid adaptation to the new link's characteristics. None of the considered solutions other than Le('06) provide mechanisms for fast adaptation to the new link after handoff.

In keeping with the IETF end-to-end arguments in system design [57], end-to-end is achieved when only the knowledge and help of the application or protocol standing at the end points of the communication system is required—although the communication system support may be helpful as performance enhancement. It would be therefore advantageous or desirable to implement end-to-end solutions for the migration of TCP connections.

On the positive side, most solutions considered achieve significant improvements on the network throughput in particular circumstances. SNOOP and the other mentioned highly link-coupled approaches handle efficiently high BER. Freeze-TCP and Le('06) maintain the end-to-end semantics and can handle encrypted traffic. Yoshimoto('07) offers a highly dynamic environments by means of link adaptation. Table 2.2 summarises the characteristics of the these TCP mobility solutions and the proposed scheme presented in Chapter 5.

A note on UDP

UDP is an unreliable transport protocol: it does not support end-to-end congestion control and ordered data delivery mechanisms. Hence, applications using UDP either need to exercise their own flow control mechanisms or settle for a support protocol such as Datagram Congestion Control Protocol [58], or have no congestion control at all. Some applications, though, do not need a reliable

Table 2.2: Characteristics of various TCP mobility enhancements

	Mobility Enhancement				
Characteristic	SNOOP	Freeze-TCP	Le('06)	Yoshimoto('07)	Enh-TCP
Requires intermediate node TCP mods	yes	no	no	no	no
Handles encrypted traffic	no	yes	yes	yes	yes
Keeps end-to-end TCP semantics	no	yes	yes	no[a]	yes
Handles long disconnections	no	yes	yes	yes	yes
Frequent disconnections[b]	no	no	yes	no	yes
Handles high BER	yes	no	no	no	no
Proactive sizing of handoff delay	no	no	no	no	yes
Addresses variable new links' characteristics	no	no	yes	yes	yes[c]
Permits use of FMIPv6 buffer	no	no	no	no	yes
Avoids DUPACKs	no	no	no	no	yes

[a]Congestion control at handoff is delegated to application.

[b]New network characteristics may not match those of the previous network. The cumulative effect after frequent handoffs may eventually disrupt the communication.

[c]Although there is an expectation Enh-TCP can be combined with adaptation mechanisms such as TCP Prairie [56], at this point, adaptation is only partially resolved

end-to-end data flow. For instance, real-time video or voice over IP applications do not benefit from retransmissions or transport-level buffering. Real-time application users are more tolerant to sporadic interruptions than to delays. Such applications usually number their payload sequentially. When a packet is received, the application codecs [59, 60] or other in-built algorithms assess whether the received data is above a delay threshold. If the data is excessively delayed, the application drops the data.

During a MIPv6/FMIPv6 handoff, the MN is unable to send or receive any packets. FMIPv6 facilities include a buffer at the NAR so that the packets sent to the PCoA during the handoff are stored until solicited by the MN. Hence, these packets are delayed at the NAR and, therefore, UDP applications will experience packet loss since these packets are dropped (arrived out of the applications-specific

time window). To minimise the UDP packet loss, special attention has to be drawn to radio technology-dependent handoff delay, but previous work [61, 62] also highlights the importance of reducing the L3 signalling delays and the L3 synchronisation with the L2 at handoff.

2.4 Network Selection for Multihomed Hosts

Mutihomed devices are those provided with more than one interface. There are a number of reasons why it is beneficial to multihome devices:

- Permanent and ubiquitous access: extending coverage area via distinct access technologies, thus enabling permanent connectivity;
- Redundancy and fault recovery: permanent connectivity is ensured as long as at least one interface is connected;
- Load balancing: distributing traffic load through multiple points of attachment, avoiding network congestion;
- n-casting: duplicating a particular flow through n interfaces simultaneously helps reducing packet loss (typically applied to real-time traffic and to mobile environments);
- Bandwidth aggregation: multiple interfaces simultaneously connected to different links increase the total available bandwidth;
- Preference Settings: providing either the user or the ISP with the capability of choosing the preferred RAT or access network regarding cost, efficiency, link parameters'—bandwidth, delay, jitter or packet loss—adequacy to the running applications, battery consumption, security or any other aspect that may have an effect on the QoE, and finally
- Transparency: truly seamless management of multihoming facilities avoids the disruption of the ongoing sessions and the QoS.

As it seems, achieving these goals is a challenging venture. Multihoming success derives primely from a synergetic operation of a number of intervening protocols, access technologies and policy bases. This requires the enhancement

of different components of the network with different degrees of awareness of the constituent elements of the communication process and their interactions. For instance, a load balancing entity must be provided with a set of routing or policy tables in order to effectively divert traffic flows accordingly. Additionally, it should be aware of the different available interfaces and should be capable of using these (carrying L2 and L3 procedures) in parallel. Depending on the granularity of the flow diversion, the multihomed entity should consider multiple IPv6 address registration [63].

2.4.1 Challenges and Open Research Issues

There is a number of functionalities addressed by the research community which yet pose challenges. The most significant issues that need to be solved in accommodating an user-centric network selection system include:

Network Selection Decision System Architecture Design is the key to low-latency information and signalling exchange between the intervening entities—e.g. mobile terminal and access points, AAA, policy repositories or access network information servers (such as the CRRM)—and from it depends the future openness of heterogeneous networks for users to roam free of network tides—network-centric or user-centric intelligence.

Network Monitoring and Access Discovery as identified in Section 2.1.1, is needed for assessment of the different available access networks and discovery of new ones. The information discovered in this phase depends on the RAT, the type or amount of information advertised by the network operators, the RAT-specific mechanisms that the terminal may use as well as the monitoring methodology. Multihomed devices add further complexity since they either may be provided with several interfaces or with a Software Defined Radio [64], thereby requiring additional attention. The goal is for the decision information and repository entity to quickly gain information on available network's characteristics, without disrupting ongoing communications and minimising the terminal's battery consumption.

Decision Inputs for handoff and network selection systems have evolved as new services—and thereby the variety of application demands—have been

accepted by the mobile user's community. Since the 1G, when cellular networks only provided voice communication, to the most recent developments on multi-service, multihomed heterogeneous ambient networks, the scope of decision inputs has broaden from RSS and hysteresis values to a number descriptors [65]. These new metrics include both networking-sided parameters—such as BER, latency, jitter, capacity and power output limitations—and user- or service-sided parameters—such as user preferences on billing, applications requirements for end-to-end delay and PER, terminal's remaining battery and terminal speed.

QoS Definition and Representation must enable an uniform characterisation of the available access networks: if these are to be compared by a decision system, then they must be expressed in the same terms. This is sometimes puzzling due to the intrinsic differences between RATs. For instance, different RSS levels may yield different BERs, channel capacity may be either a fixed or elastic value (TDMA or CSMA), pricing may be given either per bit or in a monthly basis, and some parameters are difficult to characterise numerically (such as security).

Secondly, application requirements must be represented by means of the same metrics that characterise access networks. Applications requiring connectivity should provide the decision algorithm with the relevant decision metrics and, if one application comprises multiple traffic flows, the requirements for each individual flow should be stated separately to allow for finer-granularity on the network selection.

User Preferences and Application Requirement Discovery is often a complex issue. Both users and applications do not react binarily with regard to network quality; their satisfaction or performance level depends on complex multi-variant functions. For instance, distinct VoIP codecs' expected Mean Opinion Scores (MOSs) have been modelled on the basis of several QoS metrics, such as channel BER, end-to-end delay and jitter [66, 67]. Furthermore, users also introduce sometimes conflicting metrics in the decision-resolution process; users seek for the highest possible performance level, minimising both the monetary cost and the preference-configuration burden (and the subsequent annoyance factor). Current research on such issues focusses

on attractive GUIs [68, 69], heuristics and utility functions, and machine-learning approaches [70].

Network Selection Algorithms compare the available networks characteristics with the user and application requirements and then decide which network or combination of networks is the most suited for the ongoing applications or application flows. Network selection algorithms should provide quick, efficient and stable responses. Section 2.4.2 below explains in further detail the issues addressed by network selection algorithms. Section 2.4.3 provides an overview of network selection algorithms and their integration with network and applications QoS modelling.

The aim of this thesis is to develop an access network selection algorithm able to cope with the goals expected for multihomed devices. The following section will provide a formal statement of the problem that network selection algorithms are to tackle.

2.4.2 Problem Definition

Network selection algorithms must dynamically manage the allocation and de-allocation of traffic to the available networks. Their aim is to optimise the allocation of the available networks resources according to the running applications demands so that every ongoing communication's QoS is maximised.

The algorithm should be triggered whenever: (a) a new session set-up request is made; (b) the user changes his/her preferences or requirements[1]; (c) the user's terminal detects a new network; (d) an ongoing service can no longer be supported by a particular radio link, e.g. due to signal degradation; (e) the current network initiates handoff to perform load balancing or due to operator-specific reasons.

Additionally, the network selection algorithm should be provided with communication interfaces with inputs discovery, mobility management and further network and application policy and information entities. Most user-centric approaches, as explained in next section, incorporate cross-layer information schemes. In turn, network-centric schemes often rely on signalling schemes.

[1]In the forthcoming discussion, the authors will differentiate between user preferences and user requirements. Preferential attributes are those to be maximised. Requirements are mandatory values for attributes.

2.4.3 Network Selection Algorithms

Network selection procedures rely on a set of enabling technologies, as outlined before. These include network discovery, architectural design and the capability of interpreting user expectations and mapping them in terms of network metrics. The final decision—on which a possible impending handoff depends—is taken by an informed independent decision-making entity. This decision should optimise the user's satisfaction, being stable (avoiding the ping-pong effect) and energy- and computationally light-weight. However, firstly, the decision inputs are often untrustworthy due to the network's dynamism and its intrinsic unreliability; and secondly, it is difficult to evaluate the degree of *fitness* of a network to the user's requirements.

Network selection algorithms aim to solve these questions. As the number of unknowns increases, the strategies will vary. Among the network selection algorithms than can be found in the literature, there are differences with regard to the considered input parameters, the parameter acquisition methodology, the decision architecture and the decision algorithm. All these factors influence the quality of the final decision accordingly:

- *Used Metrics.* Radio access networks are characterised by sets of metrics. Obviously, the more metrics considered the more informed the decision will be and therefore better the network quality expectation. On the downside, the more metrics considered, the more heavily loaded (time- or energy-consuming) the decision processor will be.

- *Decision Input Discovery* can be performed either in a *purely* user-centric manner or assisted by the network operators. In general, the user-centric approach presents disadvantages in comparison to the network-centric solutions. These include higher battery usage, the need of novel RAT-specific monitoring schemes and new evaluation techniques of the wireless medium. Moreover, any time radios dedicate to the input discovery may disrupt the ongoing communication flows. In contrast, network operators have better suited tools for the inputs discovery and have access to restricted information, such as antenna transmission power or details on frequency allocation and interference.

- *Network Selection Architectures* vary from (a) virtually non-existing architectures, where users produce the input values as discovered via access medium observation and they are provided with cross-layer information schemes or evolved mobility protocols, to (b) the inclusion of a number of network entities for policy storage, policy enforcement, access network monitoring and information schemes.

- *Decision Algorithms.* Network selection can be viewed from different perspectives, aiming at different goals—such as reducing unnecessary handoffs, avoid *ping-pong* effect, minimise network operator costs or maximising user experience—and thus require different approaches. Policy-based network selection is the simplest approach; empirically-tested scenarios can be generalised so that general policies define model the terminal's handoff demeanour. Other more complex approaches view network selection as a multivariate constrained optimisation problem. Constrained optimisation problems are solved by means of Multiple Attribute Decision Making (MADM) schemes such as *Cost Functions* (either arbitrary or constructed from empirical data), *Technique for Order Preference by Similarity to Ideal Solution* (TOPSIS) or *Analytic Hierarchy Process* (AHP). Also, machine learning approaches—like Bayesian Networks, Genetic Programming, Fuzzy Logic and Artificial Neural Networks—have been used for network selection.

Table 2.3 presents several network selection schemes and describes them in terms of used metrics, architecture design, input discovery and decision methodology. Surprisingly, giving the plethora of multihomed devices available on the market, little attention has been drowned to multihomed network selection. Xue et al. [82] proposes a network-centric solution for efficient RRM in multihomed (WLAN-LTE) environments. It encompasses a proportional-bandwidth algorithm, aimed at maximising the user's allocated bandwidth with respect to the user requirements. Users are attached to WLAN or LTE links (not allowing for bandwidth aggregation) depending on their reachability, and the available bandwidth on the links. Algorithmically, it reduces the network allocation problem to a LP suboptimal optimisation problem, reducing the $O(2^{K\cdot(N+L)})$ complexity of NP-hard problems to the $O(K^3 \cdot (N+L)^3)$ complexity of constrained LP—where K is the

number of users, and N and L the number of WLAN links and LTE channels (subcarriers time OFDM symbol intervals) respectively.

In turn, WISE [83, 84] introduces a reactive solution for network selection for multihomed nodes, permitting only one simultaneous interface usage. It involves a sender-side modification on the standard SCTP protocol. It encompasses, firstly, bandwidth estimation techniques to discriminate losses due to congestion from those due to wireless losses ; secondly, a revision on SCTP congestion control procedures that enables more efficient response in the event of wireless loss-induced cwnd reduction; finally, a reactive path management mechanism that switches the 'primary-secondary' SCTP path definition when any of the alternate paths offers more available bandwidth.

Horde [85] also proposes a user-centric packet scheduler (striping) solutions for multihomed environments. Horde comprises two different mechanisms. Firstly, exports a set of flexible QoS abstractions to the application, thus involving explicitly the application in the dynamic determination of the striping policy. These application-reported QoS objectives include latency, packet loss rates, expected loss correlation and bandwidth, and are translated into an application utility function. Secondly, Horde defines a scheduling mechanism that decides how to transmit the packets from the data streams on the multiple network channels, in an attempt to satisfy the QoS utility function. This multi-channel data stream striping is supported via per-channel independent congestion control.

Horde's packet scheduler can cope with highly dynamic environments (usually due to vehicular motion and channel use competition), heterogeneous networks and data streams. Firstly, it evaluates the streamed packets RTT. Secondly, it estimates the channel's capacity. With these two indicators, Horde is capable of predicting the link quality in the short term, and therefore take decisions proactively.

Horde presents, however, an inadequate QoS-requirements abstraction model. Previous work has discussed the non-binary relationship between the link quality and the goodness of the link, both in VoIP and other media-streaming scenarios and TCP scenarios. Thus, reducing the application QoS response to different link attributes to a 'one-value-per-attribute' or target link attributes does not represent a fair account of the application's perceived QoS. For instance, G711 VoIP codec sets stringent requirements on bandwidth, while latency would also

significantly affect performance. In turn, TCP-flows required bandwidth could vary while affecting linearly the service latency; however, packet error bursts would severely affect the goodput. The result is, while applications may report ideal network channel attribute requirements, the packet scheduler should take leveraged decisions and commit to tradeoffs to optimise the performance of all the ongoing applications. Horde's application-level policy definition does not permit the packet scheduler to take such as informed decision.

Calabuig et al. [86], in turn, proposes a network-centric algorithm that minimises the packet transmission latency. It encompasses a highly computationally efficient Hopfield neural network [87] decision engine, which enables real-time routing and scheduling decisions.

2.5 Summary

This chapter has explored the most relevant challenges surrounding user-centric intelligent seamless mobility. Network selection plays a pivotal role on when and why perform handoff; next, it is of major importance solving the heterogeneous mobility issues and enabling applications adaptivity. These processes are not triggered sequentially, but they act co-operatively, and therefore the individual problems co-design is key for truly seamless handoffs.

Additionally, this Chapter has presented and analysed state-of-the-art solutions. Building from the experience gained, this thesis will present (in Chapters 4-6) a combined solution for intelligent seamless handoffs in heterogeneous environments. The next chapter now describes the Evaluation Methodology.

Table 2.3: Characteristics of various Network Selection Algorithms

	NSA Attributes				
Protocol	Metrics	Input Discovery	Architecture	Decision Algorithm	Miscellaneous
Fibria et al. [71]	Throughput, Delay, BER	TBA	User centric	AHP, GRC	Incorporates a Karnaugh Maps-based Location-aware Decision Scheme
Agoulmine et al. [72]	SNR; RSS, Remaining Battery and User Preferences (mobile node speed, running applications), Cost Handoff Frequency	Terminal-enabled	User centric, network-asisted	Policy-based	No modifications on network architecture required. Consideres terminal-cross layer information scheme.
Cai and Cheng [73]	Bandwidth, Security, Cost	AAA Server	User centric	Arbitrary Benefit Functions	Allows for simultaneous use of multiple IFs
Nasser et al. [74]	Cost, Security, Power Consumption, RAT	Vertical Handoff Decision Entity	Network centric	Multi-layer Perceptron ANN	New network middleware required.
Chung et al. [75]	Access Network profile and utilisation, PER, Power Consumption, security, QoS provisioning and network utilization.	SIP and MIH-enabled network connectivy	Network centric	AHP	Consideration for user preferences
Ibañez and Martí [76]	Bandwidth, Latency, PER, Jitter	TBA	Network centric	Cost Function	Consideration of benefit as function of minimum service requirements
Gyekye and Agbinya [77]	Latency, Bandwidth, RSS, Speed, Coverage Area	TBA	User centric	FMADM and Genetic Algorithms	Consideres service or appllication-triggered handoffs. Also, it does not set arbitrary wieghts to the inputs but uses GAs to fine-tune them. Only addresses WiMax-UMTS handoffs.
Ai et al. [78]	RSS, Throughput, Delay, BER, Security, Cost,	TBA	User centric	Fuzzy Logic	Decision Input weights are firstly configured via AHP.
He [79]	RSS, Bandwidth, Cost and User Preferences	TBA	Network centric	Fuzzy Logic	Fuzzy Piolicy Base based on arbitrary allocation of weights.
Liu and Chang [80]	Bandwidth, Cost, Fairness and Availability	TBA	User centric	TOPSIS	
Ong and Khan [81]	Latency, Jitter	Network Monitoring	User centric	SAW	Incorporates a novel access network monitoring scheme based on Bootstrap Approximation, Cumulative Sum Monitoring and Bayesian Estimation

Chapter 3

The Evaluation Environment

This thesis proposes, first, handling the network selection and triggering the handoff procedures from a specialised NSA module; as opposed to a RAT-dependent approach. Secondly, a novel signalling protocol for L3 handoff that supports heterogeneous environments is proposed. Finally, since handoff causes temporary QoS degradation and delays which affect upper layer time-sensitive protocols, an extension to TCP has been added to the handoff enhancement compound. These techniques are presented in Chapters 4, 5 and 6. For these techniques to be operational in standard network entities there is a requirement for a cross-layer information support mechanism.

This chapter presents the architecture of the cross-layer information system model and its software implementation. This chapter also discusses an underlying modelling platform that allows the verification and numerical evaluation of the techniques presented in this thesis.

3.1 OMNeT++

OMNeT++ is a C++ discrete event simulation framework, originally developed by A. Varga in 1999 at the Centre for Telecommunications and Information Engineering (CTIE) in Monash University [88, 89]. It has an extensible architecture, that has paved the way for the open source and research communities to add additional functionalities and simulation models. Figure 3.1 gathers some of the most important contributions to the OMNeT++ framework. Specifically, OMNeT++ has been used to model different problem domains:

1. modeling of wired and wireless communication networks;
2. protocol modeling;
3. modeling of queueing networks;
4. modeling of multiprocessors and other distributed hardware systems;
5. validating of hardware architectures;
6. evaluating performance aspects of complex software systems;
7. in general, modeling and simulation of any system where the discrete event approach is suitable, and can be conveniently mapped into entities communicating by exchanging messages.

The extensibility and versatility of OMNeT++ derives from its component architecture. The smallest non-divisible unit is called *module*. Modules are combined in a variety of ways to build up simulation models. For instance, the ICMP protocol can be implemented as a detached module, and at compile time it can be connected to other modules, such as an IPv4 implementation, to form a network layer *compound module*, which in turn could be interconnected to other modules to form a network entity such as a router. In doing so, the depth of module nesting is not limited. The network topologies are described using a high-level network description language (*NED*). Different modules communicate via *gates* or predefined links between them, passing messages that contain arbitrary data structures.

OMNeT++ is composed of:

- a simulation kernel library,
- a compiler for the NED topology description language,
- the OMNeT++ IDE based on the Eclipse platform [90],
- a GUI for simulation execution and links into simulation executable (Tkenv),
- a command-line user interface for simulation execution (Cmdenv),
- system utilities (makefile creation tool, etc.), and
- documentation, sample simulations, tutorials, etc.

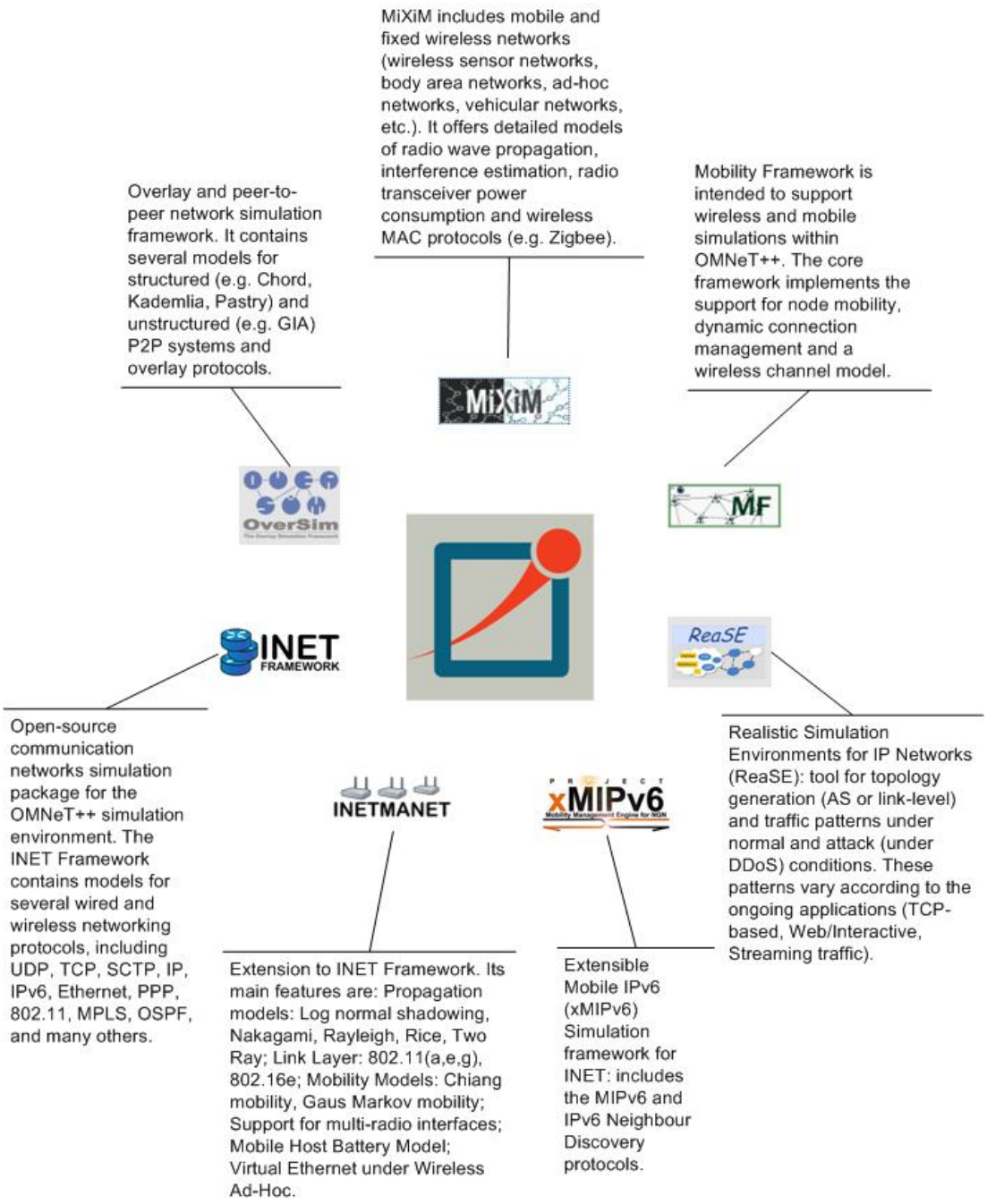


Figure 3.1: OMNeT++ Main Contributed Environment Models

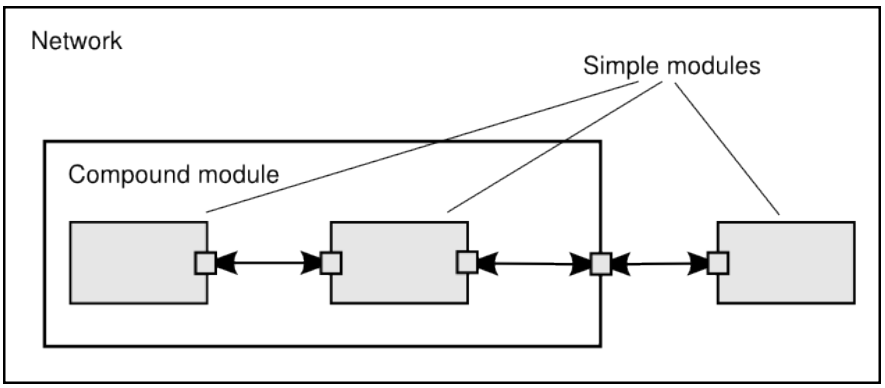


Figure 3.2: Simple modules add up to form compound modules

3.1.1 Modeling Concepts

An OMNeT++ model consists of separate modules that communicate by exchanging messages. The simplest functional modules are termed simple modules; they are written as sets of C++ classes, using the simulation class library, and describe the simulated algorithms. Simple modules can be grouped into compound modules and so forth; the number of hierarchy levels is unlimited. The whole model, usually referred as network in OMNeT++, is itself a compound module. Messages can be sent either via connections that span modules or directly to other modules. The concept of simple and compound modules is similar to Discrete Event System Specification atomic and coupled models [88]. Figure 3.2 represents a network entity composed by several modules. The figure shows how simple modules are interconnected through gates to form the compound module.

Modules communicate with messages that may contain arbitrary data types, in addition to usual attributes such as a timestamp. Simple modules typically send messages via gates, but it is also possible to send them directly to their destination modules. Gates are the input and output interfaces of modules: messages are sent through output gates and arrive through input gates. An input gate and output gate can be linked by a connection. Connections are created within a single level of module hierarchy; within a compound module, corresponding gates of two submodules, or a gate of one submodule and a gate of the compound module can be connected. Connections spanning hierarchy levels are not permitted, as they would hinder model reuse. Because of the hierarchical structure of the model, messages typically travel through a chain of connections, starting and

arriving in simple modules. Compound modules act like "black boxes" in the model, transparently relaying messages between their inner realm and the outside world. Parameters such as propagation delay, data rate and bit error rate, can be assigned to connections. OMNeT++ also defines connection types with specific properties (termed channels) and reuses them in several places. Modules can have parameters; parameters are used mainly to pass configuration data to simple modules, and to help define model topology. Compound modules may pass parameters or expressions of parameters to their submodules.

OMNeT++ provides efficient tools for the user to describe the structure of the actual system. Some of the main features are the following:

- hierarchically nested modules,
- modules are instances of module types,
- modules communicate with messages through gates and along channels,
- flexible module parameters instantiation, and
- topology description language.

These features are explained as follows.

Hierarchical Modules: An OMNeT++ model consists of hierarchically nested modules that communicate by passing messages to each other. The top level module is referred to as the system module. The system module contains submodules that can also contain submodules themselves. The depth of module nesting is unlimited, allowing the user to reflect the logical structure of the actual system in the model structure. The lowest level of the module hierarchy is formed by simple modules, which contain the algorithmic behaviour or simplest data structure: for instance, the IPv6 Neighbour Discovery Destination Cache or the TCP Reno congestion control mechanisms. Simple modules are coded as C++ functions using the OMNeT++ simulation class library and optionally any other C++ library-compliant library, so that programmers are free to use object-oriented concepts (inheritance, polymorphism etc) and design patterns to extend the functionality of the simulator.

Module Types: Both simple and compound modules are instances of module types. Simple modules serve as building blocks for the constitution of more complex compound modules. In doing so, the every module in the hierarchy preserves its integrity. Compound modules can be grouped indiscriminately to form new types of compound module. For instance, consider the compound module *BasicTCP*, composed by the modules *Fast Retransmission and Recovery* and *Slow Start and Congestion Avoidance*, two compound modules themselves. A (compound) module *RenoTCP* could be created by super-seeding the BasicTCP module and re-defining the inherited C++ TCP congestion control functions. However, this would not compromise the behaviour of those algorithms coded in the Fast Retransmission and Recovery and the Slow Start and Congestion Avoidance modules in the original BasicTCP model.

Messages, Gates, Links: Modules communicate by exchanging messages. At simulation, messages can represent frames or packets in a computer network, jobs or customers in a queuing network or other types of mobile entities. Self-messages can also be used as timers to trigger events. Messages can contain arbitrarily complex or large data structures. Simple modules are both the origin and destination of messages. Simple modules produce messages and they address them either directly to other modules directly along a predefined path, through gates and along links. Gates are the input and output interfaces of modules; messages are sent out through output gates and arrive through input gates. OMNeT++ supports only unidirectional gates. Therefore, messages are sent through output gates and are received through the input gates.

Modeling of Packet Transmissions: OMNeT++ permits the characterisation of physical connections. Connections support the following parameters: data rate, propagation delay, jitter, bit error rate and packet error or bit error rate, or may be disabled. These parameters can be either fixed (NED and omnetpp.ini files) or variable (following different probability distributions). These parameters and the underlying algorithms are encapsulated into channel modules. The user can parameterise the channel types provided by OMNeT++ and also create new ones.

Parameters: Modules can have input parameters. Parameters are used to customise simple modules' algorithmic behavior and simulation tractability. Parameters can take string, numeric or boolean values, or can contain XML data trees. Numeric values include expressions using other parameters and calling C++ functions, random variables from different distributions also included within OMNeT++, and values input interactively by the user either at the omnetpp.ini file or in separate parameter files. Alternatively, numeric-valued parameters can also be used to parameterise the model topology in order to construct topologies in a flexible way. Within a compound module, parameters define the number of submodules, number of gates, and the way the internal connections are made, leaving the burden of topology description to the pre-programmed algorithms (contained in the simple modules). For instance, due to radio range and sensitivity, a priori a wireless link can't be assured to be up; the corresponding module (e.g. the IEEE 802.11b radio) is to either connect or disconnect two entities.

Topology Description Method: The user defines the structure of the model in NED language descriptions. The NED language is a very high-level description language that permits the topology characterisation, compound module composition and enumeration of simple module input and output parameters and gates interconnections. NED files have *.ned extension.

3.1.2 Using OMNeT++

Previous section introduced the concepts and the architecture of simulated environments modeled with OMNeT++. This section provides insights into working with OMNeT++ in practice. Issues such as model files and compiling and running simulations are discussed. Additionally, Figure 3.3 provides an overview of the OMNeTT++ work-flow.

Building Simulations

An OMNeT++ model consists of the following parts:

- NED language topology description(s) (.ned files) that describe the module structure with parameters, gates, etc. NED files can be written using any

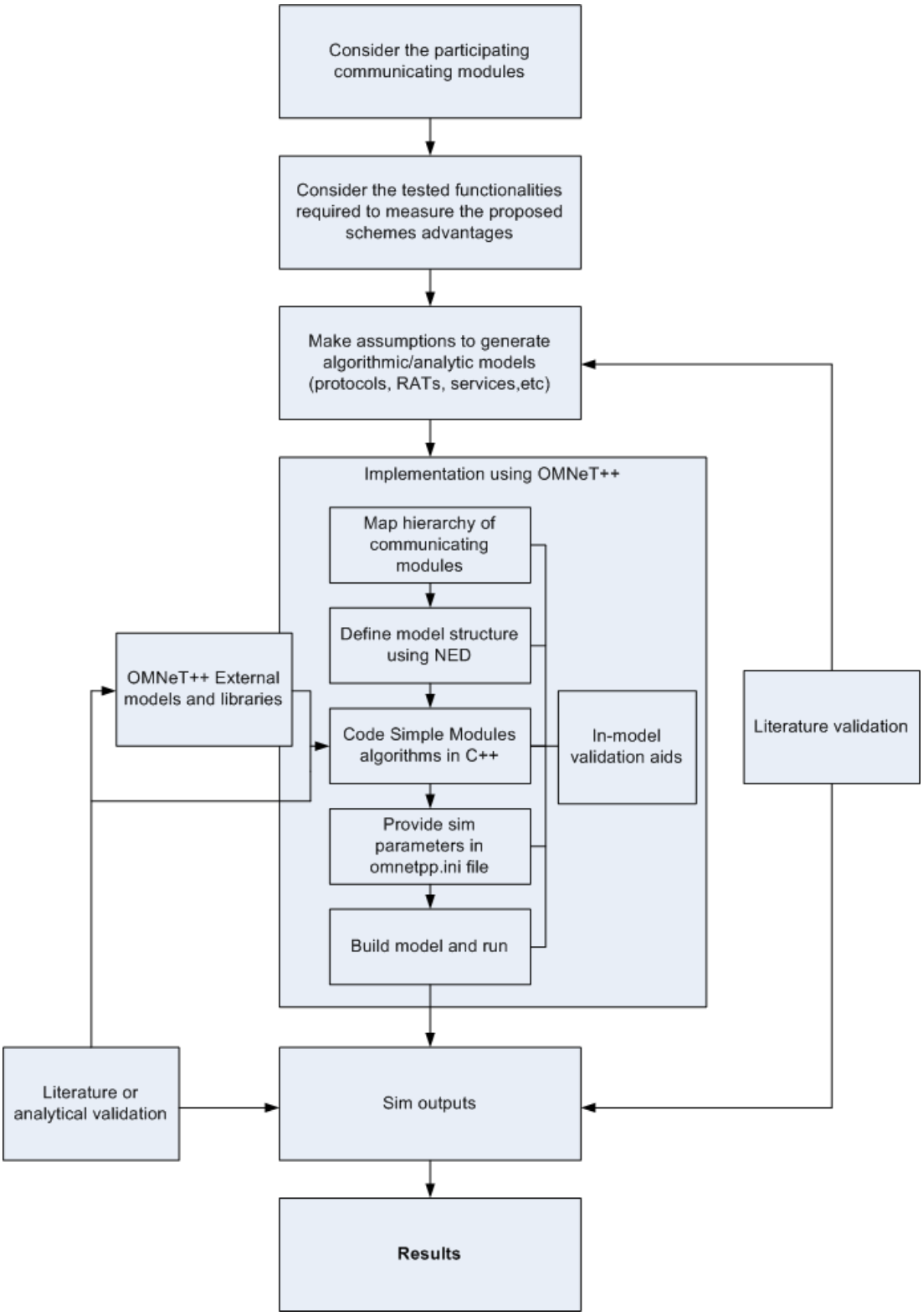


Figure 3.3: Flowchart of the OMNeT++ working process

text editor, however the OMNeT++ IDE provides support for two-way graphical and text editing.

- Message definitions (.msg files) define various message types and instantiate data fields on them. OMNeT++ will translate message definitions into full-fledged C++ classes.

- Simple module sources. These are files that contain the algorithms and module behaviour represented as C++ functions.

Simulation programs are built from the above components. Firstly, .msg files are translated into C++ code. Secondly, all C++ sources are compiled and linked with the simulation kernel and a user interface library to form a simulation executable or shared library. Finally, the NED files are loaded dynamically when the simulation program starts.

Running the Simulation

The simulation system provides the following components:

- Simulation kernel. This contains the code that manages the simulation and the simulation class library. It is written in C++ and compiled into a shared or static library.

- User interfaces. OMNeT++ user interfaces are used in simulation execution, to facilitate debugging, demonstration, or batch execution of simulations. They are written in C++ and compiled into libraries.

The simulation may be compiled as a standalone executable program; thus it can be run on other machines without OMNeT++ being present, or it can be created as a shared library. In the latter case the OMNeT++ shared libraries must be present on that system. When the program is started, all NED files containing the model topology are read, then the configuration file (omnetpp.ini) is read. This file contains settings that control how the simulation is executed, values for model parameters, etc. The configuration file can also prescribe several simulation runs; in the simplest case, each will be executed by the simulation program one after another.

To support user interaction, OMNeT++ includes a GUI that provides the user with functionalities such as real-time monitoring of environment values, allowing the user to intervene by changing variables inside the model, modifying the simulation speed and the configuration of the output trace files. This is very important in the development/debugging phase of the simulation project. Equally important, hands-on experience allows the user to get a feel of the model's behaviour. The graphical user interface can also be used to demonstrate a model's operation.

The same simulation model can be executed with various user interfaces, with no change in the model files themselves. The user would typically test and debug the simulation with a graphical user interface. Once the model behaviour has been checked for flaws, the user would finally run the simulation with a simpler, faster user interface that supports batch execution (no graphical support). Batch execution is extremely useful at running the same simulation model while modifying environment values, e.g. mobile node speed (m/s) or the mobility pattern (e.g. linear, random or Bonn mobility) in a WLAN simulation.

Component Libraries

Module types can be stored in files separate from the place of their actual use, enabling the user to group existing module types and create component libraries. This has enabled the emergence of a community of contributors to the original OMNeT++ source code to accommodate a number of different problem domains, systems, protocols and services.

Obtaining the Results

The output of the simulation is written into result trace files: output vector files, output scalar files, and possibly the user's own output files. OMNeT++ contains an Integrated Development Environment (IDE) that provides rich environment for analysing these files. Moreover, output files are line-oriented (human readable) text files which makes possible to export them to a variety of applications, including Matlab, GNU R, Perl, Python, and spreadsheet programs.

3.1.3 INET Framework

The INET Framework is an open-source communication networks simulation package for the OMNeT++ simulation environment. INET Framework contains IPv4, IPv6, TCP, Stream Control Transmission Protocol (SCTP) [91], UDP protocol implementations among others, and several application models. The framework also includes an Multiprotocol Label Switching (MPLS) [92] architecture model with Resource Reservation Protocol for Traffic Engineering (RSVP-TE) [93] and Label Distribution Protocol (LPD) [94] signalling. Link-layer models are PPP [95], Ethernet and 802.11. Static routing can be set up using network autoconfigurators, or one can use routing protocol implementations. The INET Framework supports wireless and mobile simulations as well. Support for mobility and wireless communication has been derived from the Mobility Framework (Figure 3.1). Section 3.2 describes the constituting parts of the INET Framework in detail.

3.1.4 Testbed Verification and Validation

Each individual module considered in the implementation of the simulation testbed must be verified prior to simulation. OMNeT++ considers different methods to assess the *health* of the simulation environment, as the status of the running programs is referred as in the OMNeT++ documentation. These methods are as follows:

- Related performance metrics are measured at multiple layers for verification. For example, the total number of packets transmitted, received, dropped, retransmitted, etc are computed for each session. Throughput in the application, transport, network, MAC and physical layers are compared.
- OMNeT++ provides a GUI environment for debugging a simulation. It can run the simulation step-by-step, in batch mode, or advance to a specific simulation time. It also supports real-time visualisiation of the simulation variables and internals traces as sequence charts at execution, and generating documentation. Therefore the GUI environment is very helpful in

verifying the simulation models. After individual verification of each module, the system module is tested with different network topology and traffic patterns using the above techniques.

- OMNeT++ (version 4.0 above) includes an Eclipse-based comprehensive simulation IDE. The IDE supports all stages of a simulation project: developing, building, configuring and running simulation models, and analysing results. By manually comparing the trace with the correct expected procedures (based on analytical characterisations), the correct implementation of each module can be verified.

- Messages atomicity and uniqueness. This property on the message module definition precludes messages to be shared (avoiding duplications) among different network entities.

Due to the modular and hierarchical implementation of the OMNeT++ simulation framework, once the simple modules' algorithms (e.g. the ICMPv6 protocol) and their interfaces have been established and verified, alteration of functionality of one of the elements needs only to be checked in that specific element. For example, once it has been checked with above-numbered methods that the TCP module has been correctly implemented, changes on the simulated radio interface do not affect TCP code, and therefore TCP does not have to be re-checked. Furthermore, the TCP module could be exported and applied as an external library to other simulation environments, such as a wireless sensor network testbed.

3.2 TCP/IP Model

In order to construct a realistic network, the INET framework along with the INETMANET propagation models have been imported to the simulation environment. Next, the basic features of the MIPv6 and FMIPv6 protocols, along with a set of modifications on the TCP scheme, have been coded and integrated within the initial INET model. Finally, as a variation of the *off-the-self* standard approach, the IEEE 802.21 protocol and a comprehensive NSA module have been added to the simulated network entities in order to fulfil the required functionalities of intelligent seamless handoffs. This section describes the assumptions and considerations taken at the simulation testbed set-up.

3.2.1 Radio Propagation Model [1]

Radio propagation associated phenomena are well known, despite the complex and non-deterministic behaviour of factors such as the signal fading, multipath effects and random hardware-induced errors on the transmission and reception of signals. Empirical models are frequently used with this uncertainty. Alternatively, analytical models are most often addressed to outdoor modeling, due to the difficulty of modeling indoor propagation accurately. The work carried out in this thesis, although it focusses on urban outdoor environments, is also potentially susceptible to modelling inaccuracies. Assumptions are made and, in some cases, do not reflect real-world conditions. However, these axioms or assumptions are made so that they simplify the implementation and evaluation procedures, without loss of the generality. For instance, assuming the world is flat could be interpreted as a mistake since world's curvature restricts the transmission range and it has been shown that, for instance, there is a noteworthy change on the link quality between ground level and waist level nodes. However, the flat world assumption would hold true when considering short-range (less than 100 m.) transmissions on idealistic outdoor environments, such as perfectly flat vegetation-free fields. Whether an specific assumption is appropriate depends, therefore, on the problem domain.

There are also axioms whose accuracy to model real-world conditions is so limited that their application is often misleading. Kotz et al. [1] describes some of these untrue axioms of common use:

1. A radio's transmission area is circular.

   This axiom obviously contradicts the antenna gain patterns presented by, e.g. manufacturers. Not only is it neither circular nor convex, it often is non-contiguous.

2. All radios have equal range.

   Although successful communication becomes less likely with increasing distance, it is also affected by many other factors, e.g. the angle between sender and receiver antennas.

3. If A's transmissions reach B, B's transmissions reach A (symmetry).

This axiom is not true since, for instance, a node may be affected by interference from another source (*hidden terminal* problem).

4. If A can reach B, communication's BER is 0%.

   For instance, additive noise can produce incorrect symbol detection at the receiver.

5. Signal strength is a simple function of distance.

   Although the RSSI decreases according to a power law model (explained below), other variations of real environments cause an impact as well; e.g. obstruction, reflection, refraction and scattering.

For problem tractability and simplicity and because it sufficiently matches empirical results, Axioms 1 and 2 have been accepted; i.e. in simulation, the radio tranmission area is circular and presents equal range. In turn, Axioms 3, 4 and 5 have been ruled out so that the radio model copes with interference and the aforementioned quality factors. The radio channel has been thereby modeled as follows:

Path Loss Reception Model according to the received power, P_r, is computed as:

$$P_r = \frac{P_t G_t G_r}{d^\alpha} \left(\frac{\lambda}{4\pi} \right)^2 , \tag{3.1}$$

being λ the signal wavelength, G_t and G_r the transmitting and receiving gains respectively and P_t the transmitted power (watts). The path loss exponent α varies from 2 to 5 depending on the environment. Here it is assumed to be 3, consistent with empirical measurements in urban areas [96].

Fast Fading is produced by the node's movement and multipath propagation. The implemented radio model does not take this effect into consideration.

Slow Fading is a consequence of events such as *shadowing*, the obstruction of the line of sight by large obstacles. To account for the effect of slow fading on the received power, the term χ^σ is added to Equation (3.1). χ is a log-normal random variable modeled as a zero-mean Gaussian function with standard deviation σ. A value of σ equal to 1dB is assumed here for the outdoor environment although fine-tuning using empirical measurements

will be required in order to reflect the actual scenario being modeled. For instance, pedestrian-walking mobility models often assume the range 5 to 12dB [97, 98].

Noise and Interference may come in the form of interfering EM radiation from other sources, e.g. other network entities, microwave ovens, cordless telephones and Bluetooth devices, or thermal noise. An accurate interference model is particularly important in densely populated or very active networks where several simultaneous transmissions are likely to happen. This thesis adopts an additive interference model as designed by INET [88]. In essence, during a packet reception time, every neighbouring transmission is considered as interference and its signal strength Equation (3.1) is additively evaluated, along with thermal noise, for the SINR (Signal to Interference-plus-Noise Ratio) calculation. If the SINR does not exceed the 4dB threshold, a collision is assumed and the packet is discarded. The threshold value is adopted from the model provided in the INETMANET Framework for OMNeT++ [99].

Finally, even if the packet passes the threshold test and can be considered interference free, it may present a non-zero bit error rate (BER) caused by the demodulation/decoding effects. The BER is calculated depending on the modulation scheme and the SINR obtained. This value provides, in turn, a figure for the packet error rate (PER) and ultimately the total number of corrupted bits on the whole packet. This value is then compared to a channel coding system-dependent threshold that indicates whether the packet was correctly received.

Radio Channel and Radio Chip Simulation Parameters are presented in Table 3.1.

This model is currently found in the INET framework. Similar radio models can be found in the literature. They offer both simplicity at the modelling stage, computational speed at simulation and fitness to experimental results [1].

[1]Section 3.2.2 explains this choice of frequency

Table 3.1: Radio Channel and Radio Chip Parameters

Radio Channel	
Carrier Frequency	2.4 E+9 Hz[1]
Path Loss α	3
Shadowing Distr.	Log-normal
Shadowing σ	1 dB
Fast Fading	-
Radio Chip	
Bitrate	11 E+6 bps
P_t	20.0 mW
Thermal Noise	-110 dBm
Sensitivity	-85 dBm
SNIR Threshold	4 dB
G_t	1
G_r	1

3.2.2 IEEE 802.11

IEEE 802.11 standard is composed of a family of protocols for wireless local area network (WLAN) communication. The IEEE 802.11 standard comprises several over-the-air modulation techniques, data link schemes and frame formats. The most widely used are those defined by the 802.11b [47] and 802.11g [48] protocols, which are amendments to the original standard. IEEE 802.11b was released on 1999. It has a maximum physical layer bit rate of 11 Mbps and uses the same media access method (CSMA/CA) defined in the original standard. In turn, IEEE 802.11g was ratified on 2003. It offers up to 54 Mbps and uses a different modulation scheme than IEEE 802.11b, but is fully backwards compatible. Both operate in the 2.4 GHz band.

The IEEE 802.11b INET implementation has been used for the testbed set-up and its subsequent numerical evaluation. The following protocol features are not supported: fragmentation, power management and polling (PCF). Physical layer algorithms such as frequency hopping and direct sequence spread spectrum are not modeled directly. Fields related to these unsupported features are omitted from management frame formats as well. For instance, the FH/DS/CF parameter sets, the beacon/probe timestamp which is related to physical layer

synchronization, the listen interval which is related to power management, capability information which is related to PCF. Likewise, the IEEE 802.11g protocol implementation has been provided by the INETMANET framework. Due to OMNeT++ and INET's modularity and ease of configuration, the software modifications have mainly consisted on the inclusion on the original testbed of the designated modules. Again, this 802.11g implementation does not consider any of the features related to fragmentation, power management or PCF.

The IEEE 802.11b/g INET models accuracy has been previously experimentally verified [100].

3.2.3 Ethernet

INET contains a set of modules for simulating Ethernet networks and supports classic Ethernet (10Mbps), Fast Ethernet (100Mbps), Gigabit Ethernet (1000Mbps). There are two MAC implementations available within the INET suite: a fully functional version with the complete CSMA/CD protocol, and a simplified one without CSMA/CD that can be used for full-duplex links. They both support raw Ethernet, Ethernet-II and Ethernet SNAP frames. There is a hub and a switch model; the switch relay unit has several flavours which differ in their networking performance.

3.2.4 IPv6, Neighbour Discovery and ICMPv6

The INET framework offers basic implementations of the IPv6, Neighbour Discovery and ICMPv6 protocols, respectively [29, 101, 102]. The IPv6 code permits IPv6 datagram handling (sending, forwarding, receiving and dropping). The IPv6 NeighbourDiscovery module implements all tasks associated with neighbour discovery and stateless address autoconfiguration [30]. It manages the data structures associated to the IPv6 Neighbour Discovery protocol, namely, destination cache, neighbour cache and prefix list - the latter merged into the routing table/destination cache. The ICMPv6 model handles ICMPv6 errors and echo request and replay. Finally, there is a consideration of the processing delays of these protocols. These are set to 1 μs.

3.2.5 MIPv6 and FMIPv6 Handoffs

As integral part of the work carried out in this thesis, there is a consideration for a functional implementation of the MIPv6 and FMIPv6 protocols. The developed code includes the signalling messages defined in these standards [17, 18], allowing for FMIPv6 predictive and reactive handoffs, packet forwarding, binding update and acknowledgment, home address and correspondent node's registration and return routability. Binding refreshing is not supported. These implementations have been verified both analytically and by means of the OMNeT++ GUI.

3.2.6 UDP

The INET implementation of UDP is consistent with RFC 758 [103].

3.2.7 TCP

The INET implementation of TCP is consistent with that on:

- RFC 793 - Transmission Control Protocol [104],
- RFC 896 - Congestion Control in IP/TCP Internetworks [105],
- RFC 1122 - Requirements for Internet Hosts – Communication Layers [106],
- RFC 1323 - TCP Extensions for High Performance [107],
- RFC 2018 - TCP Selective Acknowledgment Options [108] and
- RFC 2581 - TCP Congestion Control [45].

3.2.8 VoIP G.726

The VoIP Tool software [109] provides an extensive implementation of the VoIP G.726 codec [110]. These libraries are an add-on to the INET framework. They consist of two separate modules: *VoIPSourceApp* and *VoIPSinkApp*. Both are application layer modules that operate over UDP, and therefore they can be integrated on standard INET nodes such as hosts, servers or mobile nodes in a manner similar to other standard UDP traffic generators and sinks.

VoIPSourceApp accepts an audio file and a destination IPvX address and port as input, and transmits the audio file's contents as voice traffic over UDP. For transmission, the VoIPSourceApp application re-samples the audio at the indicated frequency (by default 8KHz) and depth (by default 16 bits), and encodes it with the given codec (by default G.726) at the given bit rate (by default 40Kbps). While transmitting, VoIPSourceApp chops the coded audio file into segments, each carrying *dt* milliseconds of voice (by default 20ms). Segments that are solely silence (all samples are below a given threshold in absolute value) are transmitted as special 'silence' segments. The module does not simulate any particular VoIP protocol (e.g. RTP), but instead accepts a 'header size' parameter that can be set accordingly.

VoIPSinkApp listens on an UDP port, where it expects to receive VoIP segments. Incoming audio segments are saved into a result audio file that can be compared with the original for further evaluation. VoIP segments are numbered, and out-of-order segments are discarded (the corresponding voice interval will be recorded as silence into the file). VoIP segments that miss their deadlines will similarly be discarded. It is assumed that the audio is played back with *delay* (equivalent to the *buffer time depth* G.726 parameter, by default 20ms), which allows some jitter for the incoming segments. The resulting audio file is closed when the input audio file has been fully transmitted.

3.2.9 FTP

An FTP-based [111] TCP bulk data transfer application, based on the INET model, has been implemented in order to model basic TCP data transmission. This model is consistent with the FTP request/reply solicitation scheme for file transmission. The model supports data representation only in binary mode and data transfer only in stream mode. None of the security features is supported. None of the directory commands are supported, except those related to file requesting (RETRIEVE, TERMINATE).

3.3 Summary

This chapter has introduced the evaluation environment. This consist of software implementations of a number of RATs, networking protocols and applications in the OMNeT++ simulation environment. Code debugging has been performed. Additionally, when possible, visual inspection through the OMNeT's GUI and analytical models have helped validating the results. However, performance metrics and more technical aspects of the implementation details are address in the following chapters.

The following chapters (4-6) describe the specific enhancements than this thesis explores for intelligent seamless handoffs. Each chapter will briefly remind the reader the state of the art, following with a sound explanation of the proposed enhancement(s) and, finally, performance measurements.

Chapter 4

Proactive Route Optimisation for FMIPv6

Section 2.2 presented the State of the Art in signalling mobility solutions for heterogeneous networks. These solutions achieve session continuity for the MN's applications and continued reachability. It has been noted, however, that the involved signalling schemes leave room for reducing the signalling load and packet loss, and for optimising the establishment of the optimum path between the MN and the CN(s).

This Chapter introduces a new solution for L3 mobility in heterogeneous networks, which reduces signalling delays (up to 50% in comparison with other approaches), thus in turn minimising the QoS impact at handoff—reducing end-to-end latency and tunneled traffic load.

4.1 Introduction

The MIPv6-enabled MN performs handoff for a wide variety of possible reasons, such as signal degradation on the current link, or the promise of a better QoS. Such a decision is based solely on L2-level indicators as, for instance, RSSI or packet loss, excluding L3 from the decision making or even awareness of an impending handoff. Therefore, MIPv6 takes a reactive approach to handoff. By contrast, FMIPv6 enables a proactive approach. A FMIPv6-enabled MN would trigger L3 handoff procedures prior to handoff biased by L2 triggers, balancing

the signalling burden between before and after handoff, alleviating signalling-originated QoS disruption; thereby smothering handoff.

A FMIPv6-enabled MN, on receipt of a L2 trigger indicating an imminent handoff (and the potentially available APs as identified by their L2-IDs), sends a RtSolPr message to its present access router to resolve one or more AP-IDs to subnet-specific information. In response, the PAR replies with a PrRtAdv message containing one or more [AP-ID, AR-Info] tuples. On receipt of the PrRtAdv message, the MN is effectively capable of formulating a prospective NCoA and sends an FBU message to the PAR. By use of the FBU message, the MN binds the PCoA to the NCoA at the PAR and solicits the PAR to start forwarding packets (IP-IP tunneling) to the NCoA at the NAR's link. As a consequence, the communication disruption is limited to the L2 handoff procedures, e.g. synchronizing to the new AP.

During the L2 handoff, the packets addressed to the MN's NCoA are buffered by the NAR. Once the MN has completed the L2 handoff, it notifies its attachment to the NAR's link by sending an UNA to the NAR. The MN sends this message on receipt of a 'Router Advertisement', although recent work suggests that this message is to be triggered by a L2 event notifying the L2 handoff completion [18, 112, 113]. Next, the MN receives the packets addressed to its PCoA through the PAR-NAR tunnel at its NCoA. This tunnel allows bidirectional communication, so that the MN is capable of sending data packets using its NCoA. Likewise, these packets would be tunneled back to the PAR. When the PAR receives a reverse-tunneled packet, it must verify if a secure binding exists for the MN identified by the PCoA in the tunneled packet, before forwarding that packet.

Subsequently, the FMIPv6-enabled MN updates the binding cache of its HA with its NCoA and next, optionally, the CN's binding cache for optimal routing via the RR procedure [17], as explained in Section 2.2.7. The additive nature of the RR protocol signalling delay should be noted: only after L2 and L3 handoffs are completed, route optimisation takes place. Since the MN completes FMIPv6 and MIPv6 procedures until it completes the RR signalling, the MN's segments are routed through the HA. Only when the RR is successfully finished, the MN communicates with the CN along the optimised route. This approach appears inefficient. FMIPv6 improved the initial MIPv6 approach by proactively carrying out part of the L3 handoff signalling. In this thesis, a further enhancement

to MIPv6 is proposed: the Proactive Route Optimisation for FMIPv6 (PRO-FMIPv6). This proposed protocol would reduce further the route optimisation signalling delays by proactively carrying out the route optimisation signalling.

The foregoing discussion highlighted the fact that FMIPv6 relies on L2 triggers to send RtSolPr, FBU and UNA messages and, therefore, such triggers do impact upon the FMIPv6 performance. These triggers are not defined in the FMIPv6 standard. FMIPv6, though, paves the way for the establishment of an information exchange framework from which mutual interactions between L2 and L3 could enhance the MN's perceived QoS, i.e. reducing packet loss and incurring in avoidable delays that may result from any lack of synchronisation between L2 and L3. Much effort has been carried out from across the research community to find an integrated approach to define a set of standard L2 triggers [113].

One of the most promising approaches is the one taken by the IEEE802.21 Working Group [8]. The IEEE802.21 standard defines an extensible set of media-independent access mechanisms, that enhance the inter-operability of heterogeneous network environments to facilitate handoffs. There is an expectation that future work will address MIH-FMIPv6 interoperation. Primarily, because FMIPv6 clearly depends on L2 triggers to improve its performance: FMIPv6 signalling should be synchronised with L2 procedures so that, e.g. the PAR-NAR tunnel is not set too far in advance with respect to the L2 handoff. Also, as explained in Section 4.5, FMIPv6 could benefit from the L2 triggers since they would enable L3 management of the L2 buffering and retransmission procedures, reducing packet loss. Secondly, MIH-FMIPv6 interoperation is expected since the IEEE802.21 standard specifically considers L2 trigger definition and their interoperation within a multiple layer-interoperated framework.

Chapter 4 is structured as follows. Section 4.2 introduces the PRO-FMIPv6 protocol. Next, Section 4.3 illustrates the IETF-compliant signalling formal format. Section 4.4 offers a more detailed explanation of the operation of each on of the involved network entities. Section 4.5 explains the interaction of PRO-FMIPv6 with the link interfaces, which is based on the IEEE802.21 cross-layer notification protocol. Using simulation models, Section 4.6 compares the performance of the proposed protocol with other relevant approaches. To assert the effectiveness of the protocol, parameters such as latency, tunneled load, throughput and security are evaluated. Finally, conclusions are drawn.

4.2 Protocol Overview

The proposed protocol integrates a novel signalling scheme for route optimisation within the FMIPv6-provided facilities. In common with FMIPv6, the MN also formulates a prospective NCoA when it is still present on the PAR's link through the RtSolPr and PrRtAdv messages. This address can be used immediately in the new subnet link when the MN has received a FBack message prior to its movement [18, Section 6.2.3]. In the event of moving without receiving an FBack, the MN can still use the NCoA after announcing its attachment through an UNA message (with the 'O' bit set to zero) [29]. The NAR may respond to this UNA message if it wishes to provide a different IP address. In this way, NCoA configuration latency is reduced.

The information provided in the PrRtAdv message can be used even when DHCP [31] is used to configure a NCoA on the NAR's link. Here, the protocol supports forwarding using PCoA, and the MN performs DHCP once attached to the NAR's link. The MN still formulates a NCoA for FBU processing; however, it must not send data packets using the NCoA in the FBU.

Like FMIPv6, the MN generates the NCoA from the NAR's prefix, retrieved from the PrRtAdv message. However, additionally, the MN generates two random numbers, referred to as *tokens*. The length of these tokens is implementation-dependent. The NCoA is composed according to Equation (4.1), where new_net_pref is the NAR's prefix, $t1$ refers to the token1 and $t2$ to token2. The hash algorithm could be negotiated by the MN with the CN. In this work, it is proposed to make use of the SHA1 algorithm [114] universally, therefore facilitating agreement between the MN and the CN.

$$NCoA = new\_net\_pref \| hash\left(HoA \| t1 \| t2\right) \tag{4.1}$$

Each token (token1 and token2) is included in a Mobility Header-based message: the 'Proactive Home Address Test Initiation' (PHoTI) message and the 'Proactive Care-of Address Test Initiation' (PCoTI) message, respectively. These messages traverse different paths through the Internet to the CN. The PHoTI message is sent to the CN via the HA just like the HoTI message in standard MIPv6, and the PCoTI message is sent via the NAR. The CN receives both packets (PHoTI and PCoTI) from the HoA and NCoA respectively; requiring both

HA and NAR to proxy those packets. The HA must set the IPv6 source address field in the PHoTI packet to the HoA, and the NAR must set the PCoTI source address to the NCoA. Moreover, the PAR and the HA update their MN's NCoA entries with the NCoA included in the PHoTI message.

On receipt of the two tokens, the CN is able to check whether the HoA and NCoA fit with that in Equation (4.1). If the NCoA is valid, the CN updates its binding cache and replies with a BA. However, if the check is not valid, the packets are silently discarded.

Immediately after sending FBU(PHoTI) and PCoTI, the MN starts L2 handoff. After joining the new link, the MN announces its attachment with an UNA message that instructs NAR to forward packets to the MN. The MN should receive a FBack message from the PAR indicating that the tunnel is correctly set. The MN should receive at least one FBack since this message is bicasted by the PAR to both the PCoA and NCoA. Likewise, the MN should also receive a BA from the HA acknowledging the MN's NCoA. Finally, the MN should also receive a BA from the CN if the address check is valid.

Figure 4.1 illustrates the PRO-FMIPv6 signalling scheme.

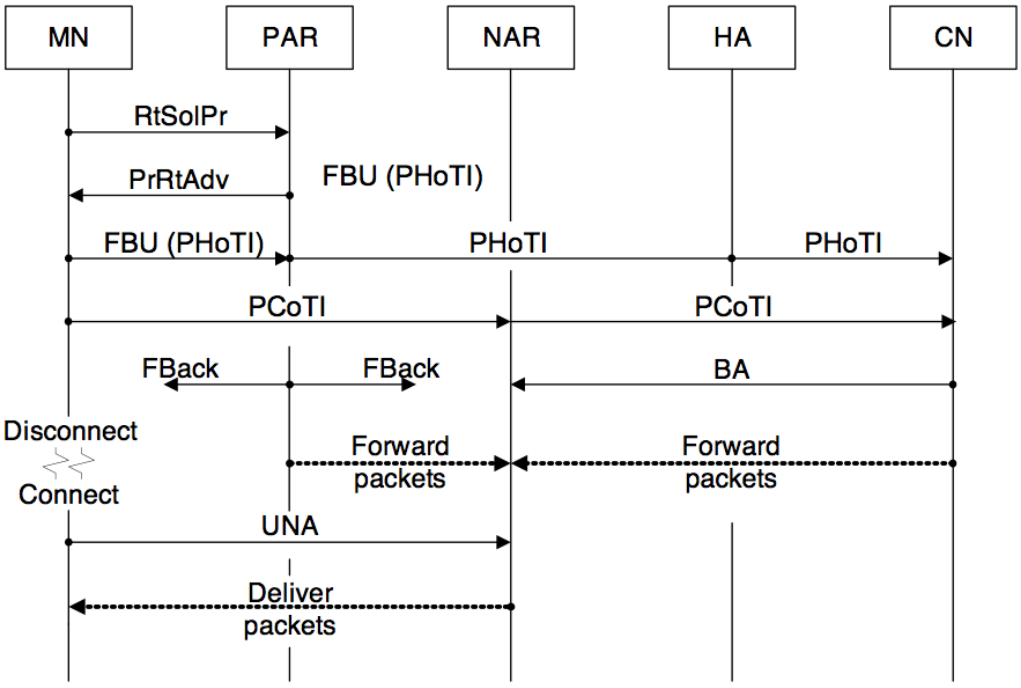


Figure 4.1: PRO-FMIPv6 signalling

4.3 Message Formats

The PRO-FMIPv6 protocol has been implemented in an IETF-compliant manner. In order to do so, modifications to both MIPv6 and FMIPv6 Mobility Header-based messages (Sections 2.2 and 2.2.8) are proposed. Furthermore, a new type of Mobility option has been defined, aka, the BU Info Mobility option. In the following sections, the formal format of the proposed messages is discussed in detail.

4.3.1 Modifications to MIPv6 and FMIPv6 Mobility Header-based Messages

Three messages have been proposed for modification, namely, the FBU, the HoTI and the CoTI messages.

Modified FBU Mobility Message Format

The 'O' flag has been added as follows.

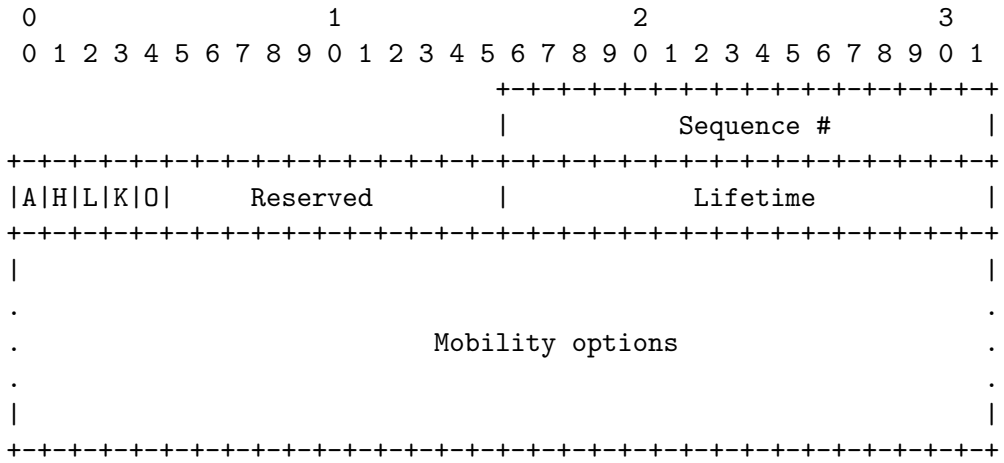


Figure 4.2: Modified FBU Mobility Message

IP Fields:

Source Address: The PCoA

Destination Address: The IP address of the Previous Access Router.

'A' flag: See [18].

'H' flag: Must be set to unity. See [17, 18].

'L' flag: See [17].

'K' flag: See [17].

'O' flag: The Proactive Route Optimisation ('O') is set by the MN to request the PAR to forward the enclosed mobility options to the HA.

Reserved: This field is unused. It must be set to zero.

For descriptions of other fields present in this option header, refer to [18, Section 6.2.2].

The FBU message is sent by the MN using its PCoA to the PAR's IP address.

PHoTI Message

In RFC3775 [17], the HoTI message is designed to initiate the Return Routability procedure and request a home keygen token from a CN. The HoTI message has been modified including the 'O' flag to indicate proactive optimisation. As with the HoTI message, the PHoTI message is forwarded by the HA to the CN using the Mobility Header Type value 1. When this value is indicated in the Mobility Header Type field, the format of the Message Data field in the Mobility Header is as follows:

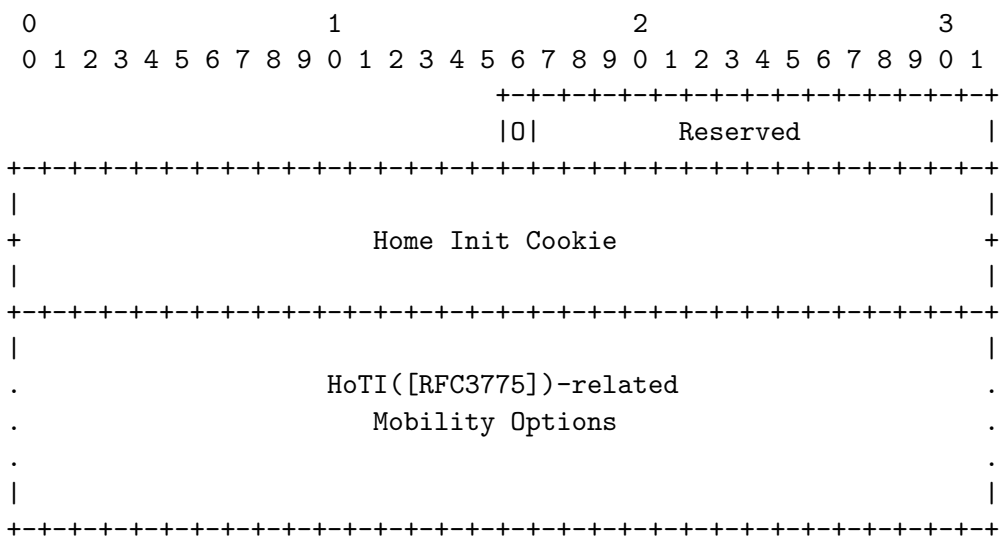


Figure 4.3: Proactive HoTI

Proactive CoTI Message

In RFC [17], the CoTI message is used to initiate the Return Routability procedure and request a care-of keygen token from the CN. The CoTI message has been modified to include the 'O' flag to indicate proactive optimisation. As with the CoTI message, the PCoTI message is forwarded by the NAR to the CN using the Mobility Header Type value 1. When this value is indicated in the header Type field, the format of the Message Data field in the header is as follows:

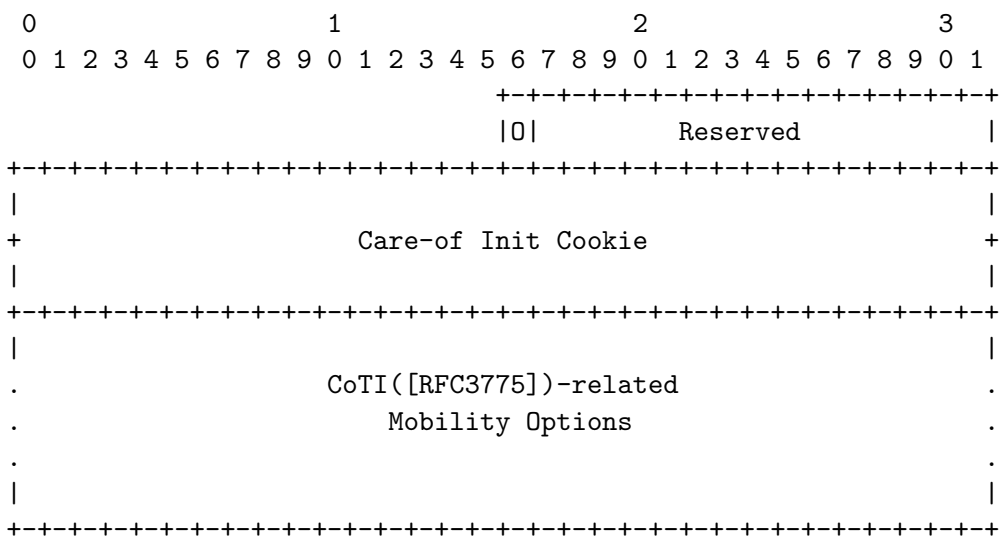


Figure 4.4: Proactive CoTI

4.3.2 New Mobility Options

A new mobility option has been proposed, namely, the BU Info option. This option has been conveniently inspired by the MIPv6 BU message, as it exhibits similar functionality.

BU Info Option

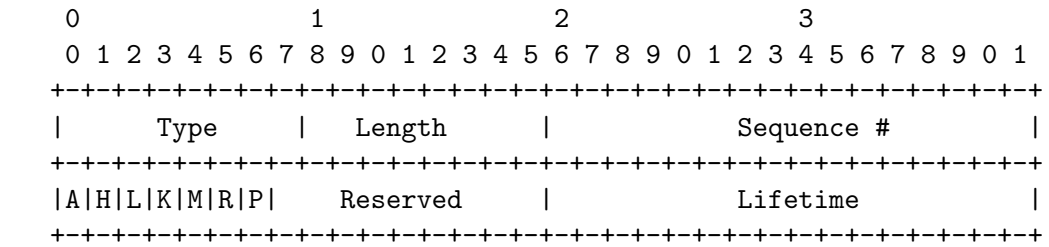


Figure 4.5: BU Info

The BU Info option header is equivalent to the BU message. The flags remain the same as in the MIPv6 standard, including those defined in [115, 116, 117] ('R', 'M' and 'P' respectively). The prospective allocated Mobility Header Type is 28.

For descriptions of other fields present in this option header, refer to [17, Section 6.1.7].

4.4 Protocol Details

4.4.1 Correspondent Node Operation

Data Structures

In addition to a Binding Cache, the CN must maintain a Token Table, where the CN keeps track of the tokens received and mobility related information from the MN. Each MN currently in contact with the CN for route optimisation has one entry. Each entry has five fields:

- HoA: obtained at session set up
- NCoA: retrieved from PHoTI (IP in IP encapsulation) and PCoTI messages
- Token1: token included in PHoTI message
- Token2: token included in PCoTI message
- NAR's prefix: retrieved from PCoTI message

Route Optimisation Signalling

The CN, on receipt of either the PHoTI or the PCoTI message, must create an (incomplete) entry in the Token Table. This entry will be kept until the second message is received or MAX_TOKEN_LIFETIME seconds are elapsed. The MAX_TOKEN_LIFETIME timeout period is devised to prevent any memory exhaustion that may result from the size of the CN Token Table.

If both messages are correctly received within a MAX_TOKEN_LIFETIME seconds time frame, the CN must then validate the following:

1. NCoA must be a unicast routable address.
2. PHoTI and PCoTI must have same nonce index.

3. Fields in the Token Table MN's entry (NAR's prefix, tokens 1 and 2, Home Address) must meet Equation (4.1).

If the tests are met, then the CN processes the BUInfo option (included in the PHoTI message) [17, Section 9.5.1]. Next, the CN sends a BA to the MN's NCoA [17, Section 9.5.4]. If the tests are not met, the MN's entry is removed from the Token Table.

The PRO-FMIPv6 protocol does not address refreshing the bindings. Preliminary but exploratory work suggests adopting the facilities of MIPv6, i.e. the Binding Refresh Request message and its associated procedures.

4.4.2 Home Agent Operation

The Home Agent operation is largely based on RFC 3775 [17]. On receipt of a PHoTI message, the Home Agent checks the validity of the enclosed BUInfo option. If the validity check is successful, the Home Agent must send a BA to the MN's NCoA. Next, the Home Agent forwards the PHoTI message to the CN's address. Otherwise, if the validity check fails, the Home Agent silently ignores the PHoTI message.

The Binding Cache entry must last MAX_RR_BINDING_LIFETIME seconds. On expiration of the Binding Cache entry, the Home Agent operates as in [17].

4.4.3 New Access Router Operation

The NAR must behave accordingly with RFC 5568 [18]. Prior to handoff, the MN sends the PHoTI and the PCoTI messages, that traverse different paths towards the CN. The PCoTI message is routed along the PCoA-NCoA-CN path. The NAR, on receipt of the PCoTI message, must forward it to the CN, including the PCoA as a home address option (defined in RFC 3375 [17]).

4.4.4 Previous Access Router Operation

The PAR operation is largely based on RFC 5568 [18]. Additionally, of receipt of the PHoTI message, it must forward it to the HA, including the PCoA as a home address option [17].

4.4.5 Mobile Node Operation

The protocol is instigated when the MN sends the RtSolPr to its PAR to resolve one or more Access Points Identifiers to subnet-specific information. In response, the PAR sends the PrRtAdv containing one or more [AP-ID, AR-Info] tuples [18]. From the information received in the PrRtAdv message, the MN generates a prospective NCoA using Equation (4.1). In order to do so, the MN generates two random tokens which concatenates to the HoA and applies a SHA1 hash function to the result.

The MN will then send two messages, the FBU and the PCoTI. The FBU message comprises a PHoTI message and a BUInfo option enclosed in a MIPv6 FBU message. The MN sends this message to the PAR. In the BUInfo option, bit 'A' must be set. The PCoTI message is sent to the NAR, who will forward it to the CN (IPv6 encapsulation).

Next, the MN performs handoff to the NAR. After the attachment, the MN should receive two acknowledgements, specifically, from the PAR and the HA. The MN may receive a third acknowledgement from the CN, in the special case where the CN is PRO-FMIPv6 enabled.

4.4.6 Configurable Parameters

MNs rely on the configuration parameters defined in RFC3775 [17, Section 12] and RFC 5568 [18, Section 9]. MNs must have configuration mechanisms to adjust these parameters.

In addition, the value of MAX_TOKEN_LIFETIME ([17]) is reduced to 5 seconds. The rationale behind this is that the MN sends both the PHoTI and the PCoTI messages simultaneously and therefore the CN expects to receive them at approximately the same time.

4.5 IEEE 802.21-Enabled L3 Buffer Management

In communication networks, if a certain level of congestion occurs, routers typically process the incoming packets and store them in their link interfaces buffers until the packets can be sent. Link interfaces may also have to buffer packets in those cases where, even if the wireless link does not represent a bottleneck for the

communication, packets are temporary queued before transmitted. For instance, the MN may performing L2 operations such as the IEEE802.11 'CARD', or it may be making an episodic but intense use of the channel capacity, like the derived from the FMIPv6 signalling. Consequently, FMIPv6-enabled handoff may produce packets to be queued at the PAR.

FMIPv6 signalling sets up a tunnel between the PAR and the NAR so that each incoming packet addressed to the MN's PCoA is forwarded from the PAR to the NAR. This tunnel is effective on receipt of a HAck message by the PAR. The NAR buffers the tunneled packets until the MN, once attached to the NAR's link, requests them [18]. Therefore, those packets stored in the PAR's link-layer buffer by the time it receives the HAck are not forwarded to the MN's NCoA, and hence are lost as the link-layer protocol will eventually drop them. Consequently, link layer buffering can be regarded as a potential source of packet loss.

This thesis presents an IEEE802.21-based signalling scheme that allows the PAR to re-process the packets queuing in the PAR's link layer buffers so that the buffered packets are forwarded to the MN's NCoA.

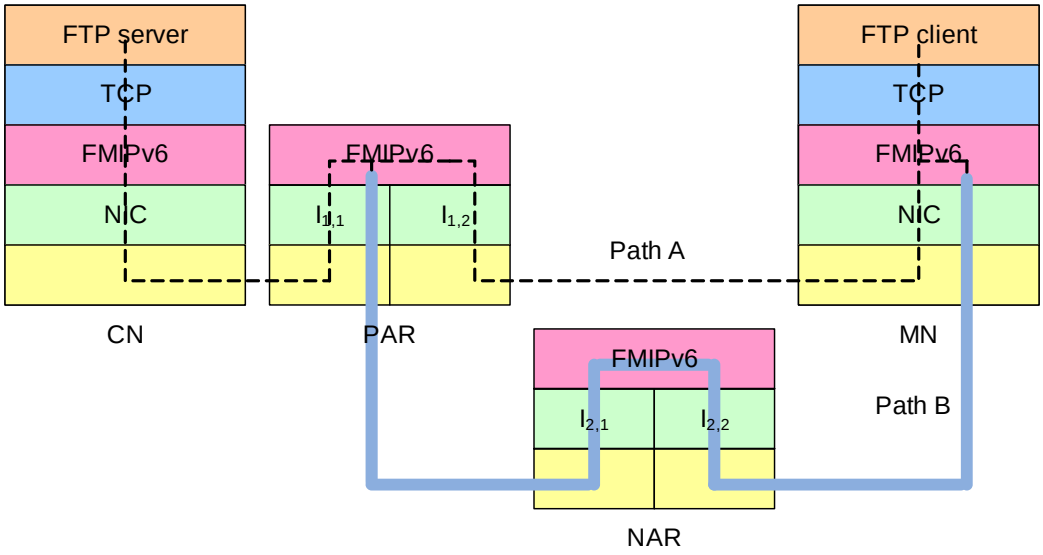


Figure 4.6: Layered FMIPv6 network example

Figure 4.6 shows a layered model example of FMIPv6 handoff. Prior to handoff, the communication between the MN and the CN is follows path 'A'. As the figure depicts, PAR's incoming packets addressed to the MN from the CN enter

though the interface $I_{1,1}$, and after they are processed at L3, they are queued at the interface $I_{1,2}$ buffer until they are sent to the MN's PCoA. After the PAR-NAR tunnel is set up, following FMIPv6 procedures, the communication between the MN and the CN is along the path 'B'.

The proposed mechanism is essentially the use of a notification from PAR's L3 to L2 asking for the buffered packets. These packets are then re-processed at L3 which, in case these are addressed to the MN's PCoA, are tunneled to the NAR. The notification processes are based on IEEE802.21, as explained next.

4.5.1 Protocol Details

The IEEE802.21 standard defines an extensible set of media access independent mechanisms. It aims to enhance the inter-operability of IEEE802 (.15, .11, .16) and cellular networks (3GPP, 3GPP2) to facilitate handoffs. To optimise handoffs, the standard provides communication between different network entities, and between different layers. This communication is carried out through the MIH 'Service Access Point' (SAP). MIH users employ a set of primitives to access the services of the MIH Function. The MIH Function comprises three types of services: Event, Information and Command. While the first two are mainly used for informational purposes, the latter service provides a set of commands for the MIH users to control link layer properties and actions relevant to handoff (Figure 1.5).

The proposed Buffer Management protocol defines a new IEEE802.21 mandatory command. This command is invoked from the PAR's FMIPv6 module and is addressed to the PAR interface that the MN is connected to. The command is called upon establishment of the tunnel between the PAR and the NAR when instigated by FMIPv6-enabled handoff. The command solicits retrieval of all the data packets addressed to the MN contained in the L2 buffer.

To facilitate the implementation of the command, appropriate new media dependent SAP primitives and media independent SAP primitives have been defined. These are shown in Figure 4.7. The MN's L3 issues MIH commands, which are translated by the MIH Function into link-specific commands. The Link_Buffer_Retrieve command supports the media dependent SAP. It is used to

request L3 protocol data units (PDUs) from the L2 buffer. Two primitives support this command: Link_Buffer_Retrieve.request and Link_Buffer_Retrieve.confirm.

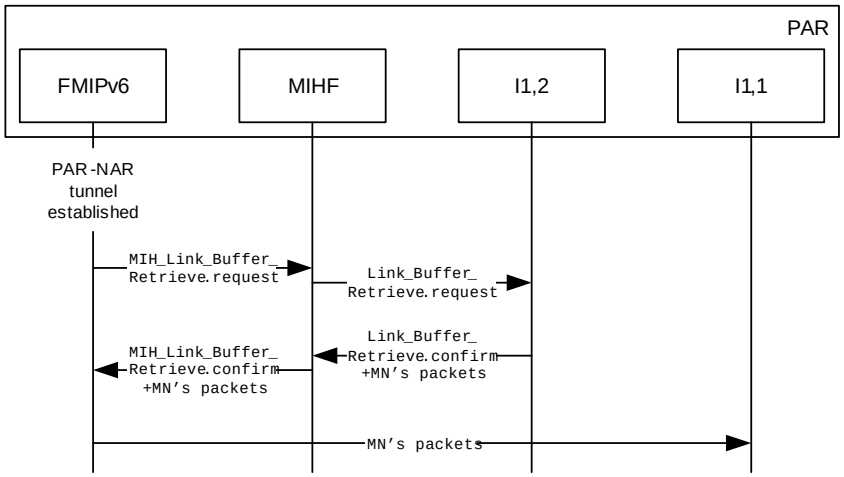


Figure 4.7: Proposed intra-PAR MIH signalling

The primitives are defined as follows:

```
Link_Buffer_Retrieve.request {
    MobileNodeLinkAddress,
    ReasonCode
}
MobileNodeIPvXAddress: Type LINK_ADDR. MN's link address.
ReasonCode: Type LINK_BR_REASON. Reason why the buffer is retrieved.

Link_Buffer_Retrieve.confirm{
    Status,
    ListBufferedPackets
}
Status: Type STATUS. Status of operation.
ListBufferedPackets: Type LIST(L3_PDU). List of (decapsulated) packets.
```

The MIH_Link_Buffer_Retrieve command supports the media independent SAP. It is issued by upper layer entities to request packets from the L2 buffer therefore avoiding packet loss that the FMIPv6 handoff may cause. Two primitives support this command: MIH_Link_Buffer_Retrieve.request and MIH_Link_Buffer_Retrieve.co
The primitives are defined as follows:

```
MIH_Link_Buffer_Retrieve.request {
    DestinationIdentifier,
    MobileNodeIPvXAddress,
    LinkIdentifierList,
    ReasonCode
}
DestinationIdentifier: Type MIHF_ID. This identifies the local MIHF that
    will be the destination of this request.
MobileNodeIPvXAddress: Type IP_ADDR. MN's IPv6 address.
LinkIdentifierList: LIST(LINK_TUPLE_ID). List of link identifies for
    which status is requested. If the list is empty, request the
    buffered packets from all the interfaces.
ReasonCode: Type LINK_BR_REASON. Reason why the buffer is retrieved.

MIH_Link_Buffer_Retrieve.confirm{
    SourceIdentifier,
    Status,
    ListBufferedPackets
}
SourceIdentifier: Type MIHF_ID. Identifies the invoker of this
    primitive.
Status: Type STATUS. Status of operation.
ListBufferedPackets: Type LIST(L3_PDU). List of (decapsulated) packets.
```

Additionally, a new type of *reason code* [9] (LINK_BR_REASON) has been defined. It is included in the Link_Buffer_Retrieve and MIH_Link_Buffer_Retrieve primitives. Reason code numbers are as follows.

0 Reason is FMIPv6 handoff. The packets are requested from L3 to reprocess the IPv6 destination address they have to be sent to. MAC protocol should not be affected in any manner. Packets are dequeued silently from the L2 buffer. L2 management-related packets must not be retrieved from the buffer.

1-127 Reserved for IEEE 802.21 future use.

128-255 Vendors specify their own specific reason codes in this range.

As a result of carrying out this notification scheme, packets are sent from L2 to L3: those packets addressed to the MN's PCoA will be, next, tunneled to the NAR according to RFC 5568 [18].

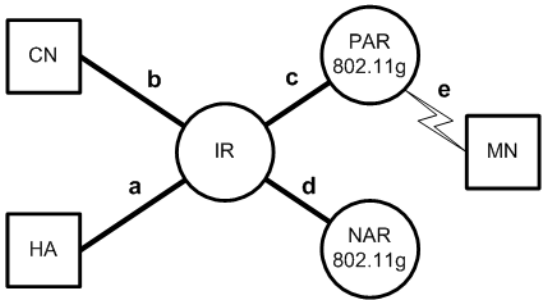
The proposed IEEE 802.21 mechanism retrieves, from the L2 buffer, only those packets unrelated to L2 management because their scope is limited to the PAR link. Likewise, some types of L3 messages must not be forwarded to the MN's NCoA, e.g. Routing Advertisement Neighbour Discovery messages. Hence, PAR must not forward those packets from the buffer generated by its L3 (other than FMIPv6 messages).

4.6 Performance Evaluation

Simulation experiments have been conducted to estimate a range of parameters related to the overall handoff signalling performance. Since the aim of the protocols discussed is to quickly update the CN's binding cache, the time delay before communication through the optimised route can be re-established is the metric of interest. Secondly, the impact of the L3 Buffer Management at handoff and other network-related performance metrics are discussed.

The simulations have been carried out using the INET Framework for OMNeT++ [88]. Figure 4.8 shows the system model from which network performance is evaluated. The network is composed of 6 participating nodes, with their interconnecting links described in terms of packet delivery latency [118] and throughput. Each of the links can be configured with a packet latency value to emulate the anticipated latencies in a real system between the CN, HA, MN, PAR, and NAR. The wired links are Gigabit Ethernet, while the wireless link is 54 Mbps IEEE802.11g.

PAR and NAR's access links are in different subnets, and thus a number of processes are triggered at the handoff. First, IEEE 802.11 networks do not facilitate efficient handoffs: therefore, the MN would disconnect from PAR's AP, then reconnect to NAR's AP, then obtain a valid IP address at NAR's link (NCoA), finally re-establishing communication with the CN(s) using the NCoA. This process is equivalent to handoff in heterogeneous environments and, although two IEEE 802.11 APs have been considered at simulation for (i) the RAT software implementation reliability (imported from OMNeT++); (ii) ease of code analysis



Link	Latency (ms)
a	5
b	45
c	5
d	5
e	N.A

Figure 4.8: System Model

and troubleshooting; and (iii) predictability of the results while comparing to previous studies, this network configuration does not hinder the general applicability of the results.

Four scenarios (A-D) are considered for each of the four schemes (FMIPv6, PB-FMIPv6, ERO, PRO-FMIPv6); the scenarios are differentiated in terms of total L2 handoff delay: 0s, 0.25s, 0.5s, and 1s respectively. Scenario A, corresponding to a handoff delay of 0s, is of particular interest for two reasons: (1) from a theoretical perspective it provides an upper bound on the performance of each protocol, (2) from a practical perspective it provides a realistic assessment of the performance that may be expected when MNs are multihomed ([119], [120])—this is particularly pertinent given the plethora of terminals with multiple interfaces on the market at present. The other scenarios permit comparative analysis for a range of handoff delays since previous studies have demonstrated that relative performance is dependent on L2 handoff latency. All scenarios assume an identical service: a stream of UDP packets sent from the CN to the MN at an interval of 20ms (consistent with standard VoIP codecs). At a predefined time, a L2 hint [8] is simulated which initiates the handoff process. In all cases proactive handoff is assumed. In the ERO protocol simulation, the MN is considered to have performed the home test prior to handoff, so the CN trusts the MN's reachability through its home address. In PRO-FMIPv6 protocol experiments, Optimistic Duplicate Address Detection-*DAD*-is used; FBAck message functionalities are reduced to acknowledging the packet forwarding from PAR to NAR. This has no effect on the performance evaluation because the signalling delay is computed from the trigger of the L2 handoff, and as for the other approaches, if DAD is enabled, it is carried out prior to the L2 handoff and the

route optimisation signalling through the HI and HAck messages. An extension of the PRO-FMIPv6 scheme to include DAD is explored in Appendix A.

As a consequence of path changes during handoff, some packets sent along the new route may arrive earlier to the MN than the other packet(s) sent along the previous, non-optimised route, causing reordering. Moreover, as a consequence of different delays assumed for each segment of the network, and the design of the signalling schemes, the binding updates will reach either the HA or the CN at different times, depending of the paths they traverse.

4.6.1 Latency

Figure 4.9 illustrates the aforementioned effects on the system model depicted in Figure 4.8, and shows the performance of the four considered protocols in the scenarios A-D. Performance, in terms of latency, is measured as the delay from the start of the L2 handoff until the establishment of direct communication between MN and CN (optimised route). Immediately after handoff, and prior to establishing the optimised route, the mobile node receives packets along the path CN-PAR-NAR. This path is associated with higher packet latency than the optimised (CN-NAR) one.

In scenario A, the link layer handoff delay is set to 0s. The results derived from this scenario set an upper bound to the performance of the ERO and FMIPv6 protocols. Given that they perform signalling tasks on the new link, having a 0s L2 handoff delay, they don't suffer from additional delays from the link layer procedures. Meanwhile, PB-FMIPv6 and PRO-FMIPv6 take no advantage of the concurrent scheduling of tasks (route optimisation signalling and link layer handoff). There are notable differences on the performance, however, as result of the trip times of the signalling messages involved: ERO, FMIPv6, PB-FMIPv6 and PRO-FMIPv6 take 0.22s, 0.26s, 0.26s and 0.15s, respectively, to set the optimised route.

In scenarios B, C and D the link layer handoff delay is set to 0.25s, 0.5s and 1s respectively. As ERO and FMIPv6 carry out signalling procedures in the new link after joining it, these delays are added towards the establishment of the optimised route. Alternatively, in both PB-FMIPv6 and PRO-FMIPv6, as the

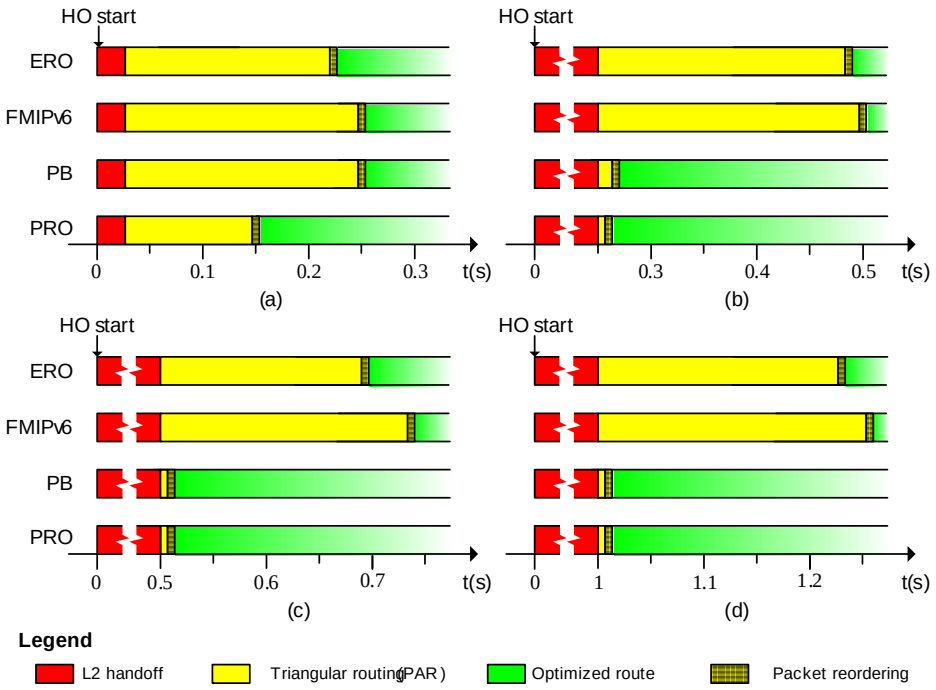


Figure 4.9: Route Optimisation Delays

signalling mechanisms are performed in parallel while the MN is in the process of joining the new link, these latencies are therefore not cumulative.

In general, link layer procedures' delay is cumulative to the overall signalling latency of ERO and FMIPv6. However, making use of PB and PRO, this delay just sets an upper bound on the performance: Table 4.1, obtained from the results on Figure 4.9, corroborates this statement. Thus, the key for faster updates of the CN's binding cache yields on performing the home and care-of address checks concurrently. For these reasons, the solution proposed in this paper performs better than the other protocols under consideration in the scenarios A and B. In the scenarios C and D, it performs as fast as the PB-FMIPV6 protocol. Consequently, a PRO-FMIPv6 enabled MN is expected to switch communications with a CN to the optimised route after handoff faster than using the other approaches considered in this work.

Table 4.1: Delay to set optimised route after L2 handoff

HO delay(s)	0	0.25	0.5	1
ERO	0.215	0.221	0.228	0.202
FMIPv6	0.262	0.261	0.269	0.253
PB	0.262	0.025	0	0
PRO	0.15	0	0	0

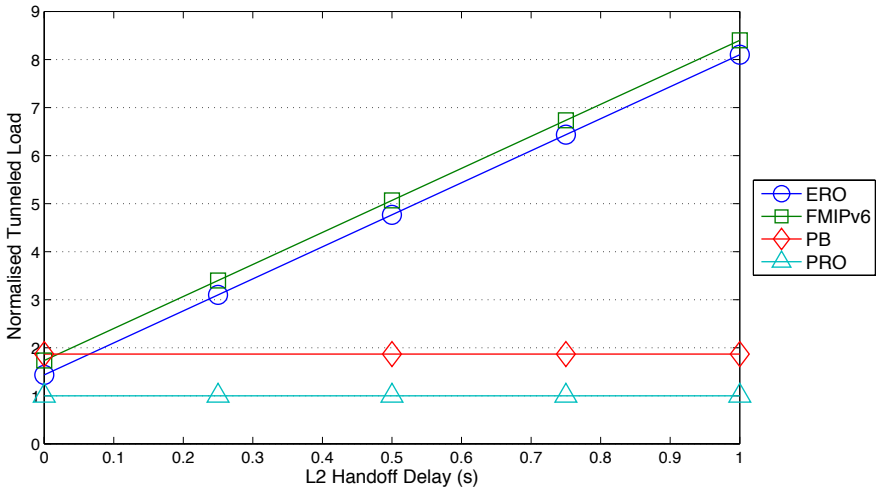


Figure 4.10: Effect of L2 Handoff Delay on the Tunneled Load

4.6.2 Tunneled Load

The The PRO-FMIPv6 signalling scheme performance has also been evaluated in terms of tunneled traffic load. Figure 4.10 shows the tunneled load of PRO-FMIPv6 in comparison with FMIPv6, ERO and PB-FMIPv6 while varying the L2 handoff delay. It can be observed that, for FMIPv6 and ERO, the tunneled load raises as the handoff delay increases. In contrast, PB-FMIPv6 and PRO-FMIPv6 depict constant values: the average tunneled loads in which they incur is independent from the effects L2 handoff delay.

This different behaviour is a consequence of the scheduling of the signalling tasks. An either FMIPv6 or ERO-enabled MN solicits packet forwarding from PAR to NAR before L2 handoff, and only after the MN's L3 connectivity is established and the HA's Binding Cache has been updated, the MN updates

the CN's Binding Cache. During this time window, the packets addressed to the MN are tunneled from PAR to NAR. This implies that the tunneled load is directly related to how quick the MN establishes IP connectivity with the NAR and then completes the binding process. Quite the opposite, a PB-FMIPv6 (or a PRO-FMIPv6)-enabled MN would generate a lower tunneled load.

PB-FMIPv6 brings forth this reduction on the tunneled load by enabling the NAR to act as a proxy for the MN thus proactively performing the binding process on behalf of the MN as soon as it receives the HI message (and verifies NCoA as being valid) while the MN is still attached to PAR (see Figure 2.15). During this period, the MN could perform the L2 handoff. This early initiation and hence completion of the binding process will enable the CN(s) to have an early notification of the MN's NCoA resulting in the packets bypassing the PAR and arriving directly at the NAR over optimised paths as determined by the generic Internet routing protocols. Thus the duration of the PAR-NAR tunnel, and hence the tunneling load, is not dependent on the L2 handoff latency.

Likewise, PRO-FMIPv6 permits the route optimisation signalling tasks to be undertaken concurrently while the MN's L2 handoff takes place, leading to a similar behaviour to that of PB-FMIPv6, i.e. constant values of tunneled load. However, the PRO-FMIPv6's route optimisation signalling to update the CN's Binding Cache is radically different from the PB-FMIPv6's: there are fewer messages involved in the process, which yields a quicker binding updating an therefore a lesser significant tunneled load.

PRO-FMIPv6 entails a considerable reduction in the tunneled load, as illustrated in Figure 4.11. Figure 4.11 shows the percentage of this reduction with reference to the other three main approaches considered in this thesis: FMIPv6, ERO and PB-FMIPv6. It is observed that, for the considered scenario and while varying the L2 handoff delay, the reduction percentage ranges between 46% and 90%. This reduction in the tunneled load involves a reduction of the processing load at the PAR and an increase of the bandwidth demand of the PAR-NAR link.

These values for the tunneled load are expected to vary with the binding latency as a consequence of the signalling messages involved in each protocol and their round-trip times. However, as a result of the reduced signalling message exchange, the tunneled load associated to PB-FMIPv6 is expected to remain considerably higher than the tunneled load derived from the PRO-FMIPv6 scheme.

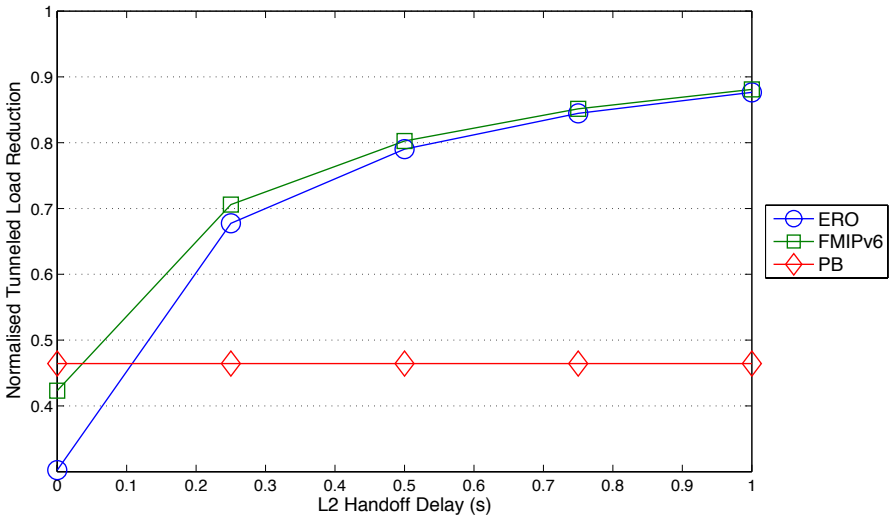


Figure 4.11: Tunneled Load reduction comparison

4.6.3 Throughput

On the forthcoming discussion, the effects on the throughput derived from the reduction on the signalling and the proposed IEEE802.21-enabled L2 buffer management scheme will be explored.

The effectiveness of the proposed solution is assessed while varying both the different PAR's links congestion levels and the handoff disruption time. The congestion level has been progressively increased by augmenting the size of receiver's advertised window (*rwnd*). The handoff disruption time ranges from 0 to 500ms. A delay of 0s is of interest because it provides an assessment of the performance of a multihomed MN, which is of interest given the availability of multihomed devices currently available on the market. Higher handoff delays give insight into comparative analysis as previous studies have demonstrated that TCP performance at handoff is dependent on layer 2 handoff latency.

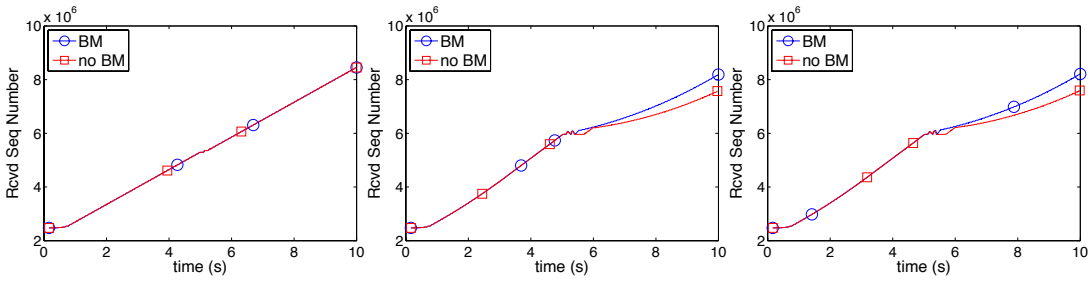
The experiment design is as follows. The TCP model implemented is consistent with TCP base [104, 106, 107] and Reno congestion control [45]. The minimum value of the RTO is bound to 200ms, as in most Linux-based TCP implementations[1]. The proposed scheme performance is evaluated from the *received*

[1]Linux 2.4 and previous versions set the minimum RTO to 20ms (default) and Linux 2.6 set the minimum RTO to 200ms (default). Current versions of FreeBSD set it to 30ms. Sun

packet sequence number of the ongoing TCP Reno flow between the CN and the MN at FMIPv6-enabled handoff.

Figure 4.12 shows the received packet sequence number at FMIPv6 handoff. The L2 handoff disruption time has been arbitrarily set to 100ms. Three different scenarios have been considered based on an increasingly congested link, for which the MN's rwnd has been set to 64kB, 128kB and 256kB, specifically.

For a 64kB rwnd (Figure 4.12a), no packets are stored in PAR's L2 buffer by the time the MN starts handoff. Therefore, the proposed buffer management scheme cannot lead to any performance improvement. Contrariwise, Figures 4.12b and 4.12c show scenarios where there are some packets queued in the PAR's L2 buffer as a result of wireless link congestion. In these scenarios, buffer-retrieving and packet-forwarding lead to an enhancement on the TCP performance as packet loss is avoided. Additional sources of packet loss—such as signal degradation and channel congestion—cause the TCP congestion control mechanisms to be triggered (entering into the slow start stage), but buffer management allows for faster recovery of the TCP congestion avoidance stage.



(a) 64kB (b) 128kB (c) 256kB

Figure 4.12: Received Packet Sequence Number Evolution for different rwnd sizes

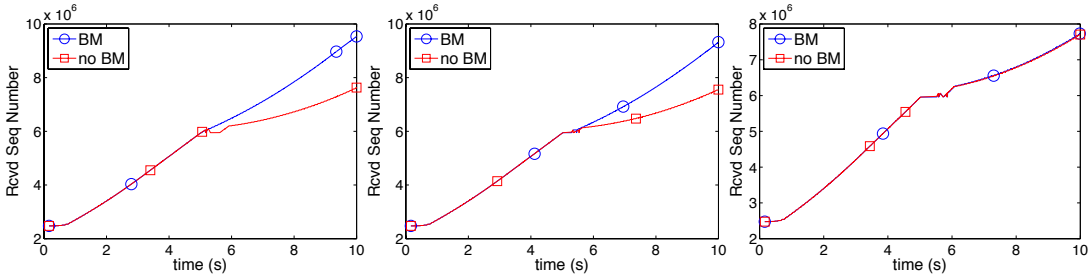
Figure 4.13 illustrates the received packet sequence number considering wireless link congestion at FMIPv6 handoff. The rwnd size has been set to 256kB. Three different scenarios have been considered according to the L2 handoff delay: 0, 250ms and 500ms.

Figures 4.13a and 4.13b demonstrate two important facts about the TCP performance on congested links. Firstly, slow start is triggered as a consequence of

Solaris 9 and above set it to 400ms

additional packet loss sources. This packet loss is consequence of lack of synchronization between L2 and L3 handoffs [121], and the implemented radio module temporarily dequeuing packets from the L2 buffer. This is a MAC-radio interface implementation issue that future work should address. Secondly, Figures 4.13a and 4.13b also show that, in spite of the sources of packet loss pointed out below that make the TCP trigger slow start, the proposed buffer management scheme (on Section 4.5) reduces the delay until the re-establishment of the TCP congestion avoidance stage.

Figure 4.13c depicts the 500ms L2 handoff delay scenario. In this scenario, RTO timers time out at the CN as a consequence of the L2 handoff delay, which is larger than the CN's computed RTO value. Using the proposed buffer management scheme, the MN can effectively avoid packet loss; but at CN, TCP congestion control mechanisms are triggered so that the non-acknowledged packets are re-sent. Therefore, in cases where TCP congestion control mechanisms are triggered due to large L2 handoff delays, the proposed buffer management scheme does not incur in any TCP performance enhancement.



(a) 0s (b) 250ms (c) 500ms

Figure 4.13: Received Packet Sequence Number Evolution for different L2 handoff delays

From direct observation of the Figures 4.12 and 4.13, the proposed scheme can make TCP flows advance to the congestion avoidance stage up to 200% faster.

4.6.4 Security

Route optimisation involves binding the PCoA to the NCoA at both the HA and the CN. The update of the HA's Binding Cache is assumed to be secure since there is a pre-existing administrative agreement between MN and HA. This agreement

would enable an encrypted BU and BA exchange between both entities by means of, for instance, IPsec [122]. Conversely, there is no administrative agreement between the CN and the MN. Therefore, the MN must secure the PCoA-NCoA binding at CN by other means.

Return Routability Security Considerations

The *de facto* standard, namely, Return Routability, relies on a combined routing-cryptographic approach: the CN is able to check MN's reachability at both PCoA and NCoA, and these checks enable the creation of a shared key to encrypt the BU and BA exchange (Section 2.2.7). This approach makes the following assumptions:

1. The routing prefixes available to a node are determined by its current location within the Internet topology, and therefore the node must change its IP address as it moves. That is, nodes must rely on the routing prefixes served by, e.g. the local routers via Router Advertisements or DHCP servers.

2. The routing infrastructure is secure and able to deliver packets to their intended destinations as identified by the destination address included in the IP Destination Address field. To implement such a routing infrastructure, routers must collectively maintain a distributed database of the network topology and forward each packet accordingly.

3. Ingress filtering is applied with a reasonable level of granularity between an ISP and its customers, between upstream and downstream ISPs and between neighbouring ISPs, thereby limiting the addresses within a network prefix a malicious entity can spoof.

Grosso modo, Return Routability hinges on a non-compromised Internet infrastructure. If the Internet infrastructure is compromised, then the packets may not be forwarded to their destination addresses, making, e.g. the CoTI and CoT exchange have no validity. Likewise, if the Internet infrastructure is compromised, the HA address may be spoofed by a malicious node, forging the HoTI message, which would permit a DDoS attack. Therefore, the security achieved by Return Routability depends on the integrity of the Internet.

However, even in those cases where the integrity of the Internet remains, there can be further venues of attack. For instance, a malicious node situated where the HA-CN and the NCoA-CN paths converge may drop the Return Routability packets or forge them. This scenario leaves room for an attacker to carry DoS or flooding attacks. Nikander et al [34] identifies additional scenarios where the security of the route optimisation can be violated.

ERO Security Considerations

ERO aims to securely authenticate MNs through a secure exchange of a HoA keygen token. The home address test also provides strong authentication since the HoA is a Cryptographically Generated Address (CGA) [123]. This type of address has the property of being cryptographically and verifiably bound to a public-private key pair, without the need of preconfigured credentials or public-key infrastructure. In this manner, the MN proves ownership of the HoA by evidencing knowledge of the corresponding private key not incurring in significant changes within the Internet infrastructure, e.g. setting up a PKI, certification authorities or trusted servers [124]. Section 2.2.9 introduces in detail the ERO security design principles.

The following issues have been identified:

1. The use of cryptographically generated HoA to secure the route optimisation: the MN shows ownership of the HoA by knowledge of the corresponding private key. The NCoA is a non-CGA. At connection start-up for the CN, the MN must register its HoA with the CN in order to perform route optimisation in the future if needed, i.e. when a handoff takes place. After that, since the MN may not be in a link managed by its HA, the MN would have to perform ERO route optimisation. This process of HoA registration and then route optimisation at connection start-up severely increases the initial delays on the communication, and its effects are specially disruptive for short term communications such as DNS requests [17, Section 8.2].

2. Processing of CGAs: CGAs involve computationally expensive algorithms. This could represent an issue for mobile devices with limited processing capabilities, and for CNs that simultaneously communicate with a large number of MNs, such as publicly accessible servers. To avoid excessive

usage of their memory and processor resources, ERO-enabled devices must implement mechanisms to protect themselves from DoS attacks. Some of these mechanisms, suggested in [125], include CNs rejecting very large keys, specifically, above 1575 bits, without processing.

3. Credit Based Authentication: During the concurrent Early Binding Update-CoA Test, the CN makes use of 'credits' to temporarily limit the traffic volume sent to the NCoA until the NCoA has been fully authenticated. However, this approach introduces a significant limitation on the data transmission performance, as the CN has an upper bound for the packet transmission rate equal to the data reception rate from the MN. In cases where the communication is asymmetric, e.g. video- or audio-streaming, or file transfer, the MN will only communicate with the CN to acknowledge the data received. The CN will then have a restricted transfer capability as long as the amount of data able to be sent to the MN is equal or lower than the addition of the acknowledgment packet payload sizes received from it. Alternatively, in those cases where MN and CN have established a bi-directional communication, e.g. VoIP, the MN will have to wait a RTT from its care-of to the correspondent address to start receiving packets and will impair perceived QoS.

4. Permanent Home Keygen Token before handoff: To obtain any performance improvement with respect to RR, the HoTI/HoT exchange must take place before handoff. Two possibilities arise at this point. Firstly, the MN may decide to wait for a L2 notification or similar trigger to send a HoTI message to each CN that it has a session established with. This would slow down the handoff process and reduce the reaction time for successful completion of a FMIPv6 handoff, especially in those cases where the MN is connected with a number of CNs. Secondly, the MN may decide to carry out the HoTI/HoT exchange whenever a communication with a CN is established. This second approach would effectively reduce the latency of the future handoffs. However, ERO is benefited on the following handoffs, where HoTI/HoT exchange with the CN is no longer necessary. If the communication does not last long enough, there will be no perceived benefit from advancing the HoTI/HoT exchange. Furthermore, the MNs have no

way to discern whether their communications are to be running for lengthy periods. Therefore, the permanent Home Keygen Token exchange before handoff implies several performance limitations.

The PRO-FMIPv6 approach

PRO-FMIPv6 does not address the security pitfalls derived from the Internet infrastructure, as neither do RR or ERO. FMIPv6 secures the PCoA-NCoA binding at the CN while reducing the signalling load in which Return Routability and ERO incur. To do so, it cryptographycally generates the NCoA to bind it with the PCoA, and two tokens. Each of these two tokens are sent from the PCoA, but the HA and the NAR forward them to the CN, so that the CN perceives them as sent from the PCoA and NCoA respectively. Each of the tokens traverses a different path through the Internet towards the CN, which increases the difficulty for a malicious node to eavesdrop them. The message that includes the first token, travels along the PCoA-HA-CN route. This message content is encrypted since it also includes the BUInfo option. The HA decrypts it and forwards the token (in the PHoTI message) to the CN. The message that includes the second token goes unencrypted along the PCoA-NAR-CN route. On receipt of these two messages, the CN is effectively able to check the origin of each token and assert whether the tokens, the PCoA and the NCoA meet the Equation 4.1. Thus, PRO-FMIPv6 also relies on a non-compromised Internet infrastructure.

PRO-FMIPv6 further improves some minor security aspects in comparison with the standard Return Routability protocol, as outlined in the foregoing discussion. Firstly, a malicious MN may try to redirect traffic from his HoA or PCoA to a NCoA. For example, if a MN is connected with a server through a high-speed connection, the MN could redirect the stream towards a low-speed NAR (in terms of processing or link capacity). PRO-FMIPv6 prohibits the MN carrying out this kind of attack: the NAR can voluntarily discard the PCoTI message if the QoS required for the MN is too high, if the proposed NCoA is not acceptable, if the source PCoA or HoA is from a domain not accepted, if the NAR does not have any established trust relationship with the PAR, if the required buffer size is too large or if the access control parameters do not meet the security requirements. The NAR retrieves information on all the previously mentioned aspects from the HI message.

Even if this kind of DoS attack could be effectively carried out, the malevolent MN would not be capable of specifying any concrete IPv6 address. The rationale behind this is that it would be virtually impossible for a MN to find two random numbers such that the result of Equation (4.1) is equivalent to the target IPv6 address. However, it must be noted that this approach may solve flooding attacks only marginally . The attacker could still generate a different NCoA with the same subnet prefix as of the victim's IP address. Flooding packets redirected to towards this CoA would then not have to be processed by any specific node, but they would impact an entire link or subnet and therefore cause comparable damage.

Secondly, a malicious third party may try to steal a node's (either mobile or fixed) IPv6 address by creating a binding cache entry at the CN. PRO-FMIPv6 prevents attackers from doing this. When a HA receives a PHoTI message for whose HoA has no administrative agreement, it silently ignores it. Therefore, the CN won't receive the PHoTI message. On receipt of the PCoTI, the CN will create an (incomplete) entry in the Token Table keeping it for a maximum of MAX_TOKEN_LIFETIME seconds. Once MAX_TOKEN_LIFETIME are elapsed, the entry will be removed from the Token Table.

Thirdly, one or more attackers may want to consume all the memory available in the CN's tokens table by sending a number of PHoTI or PCoTI messages. In any case, every time a CN receives a PHoTI(t1) or PCoTI(t2) message, the CN overrides the correspondent HoA or NCoA respectively, so therefore there is only one entry at the tokens table for each MN, independently of how frequently performs the signalling towards route optimisation. Moreover, registers in the token table are only kept for MAX_TOKEN_LIFETIME seconds.

Finally, the protocol inherits the vulnerabilities firstly identified in [126, Section 8] for the RtSolPr, PrRtAdv and FBU messages. [18] suggests solutions on those issues, which can be trivially applied to PRO-FMIPv6.

4.7 Limitations and Future Work

The RR scheme leaves room for improving the handoff user experience in terms of security. RR ensures that the MN is reachable at both the HoA and CoA, and provides a mixed routing-cryptographic method for securing the binding between

HoA and CoA at the CN. RR, however, relies heavily on the assumption of a non-compromised network infrastructure which precludes IP-spoofing and ingress filtering. Having established this assumptions, then the RR is a secure protocol, under the IETF scrutiny.

However, if MN and CN exchange messages through a non-trusted network, RR plain-text messages may be intercepted. Two of the outmost attacks on RR are session hijacking and man-in-the-middle attacks, and DoS and flooding attacks [39]. A rogue node, able to intercept a HoT message, can forge a CoTI message with his own IP address as CoA. Therefore, the CN responds with a CoT message that the attacker uses in combination with the intercepted HoT message to form a valid binding update management key. The attacker would then send a legitimate BU to the CN, thus successfully stealing the MN session or acting as an intermediary between CN and MN.

Other attacks would rather focus on implementation-specific caveats, such as the binding cache memory. An attacker could intercept a number of home and care-of tokens from different MN sessions. Next, it could send legitimate BUs to the CN in a short time (before bindings expire at CN), making the CN store many sessions in memory. Also, an attacker may bind a number of HoAs to the same CoA, thus aggregating the bandwidth and flooding the CoA.

Certificate-based route optimisation protocols also present security deficiencies or inadequacies, as certificates must be kept by trusted authorities. However, the presence of fragmented authentication infrastructures is necessary for the CN to validate the CA that issued the HoA subnet prefix certificate, thus strengthening the cryptographic protection of the binding. Yet, this requirement posses scalability and flexibility issues when expanding to a global mobility services demand. Furthermore, the different administrative domains would be forced to co-operate as they currently do for roaming purposes, and therefore business agreements should be predefined, limiting the use of different radio access technologies and network access.

Also, CGAs present security issues. Firstly, they require computationally expensive algorithms. This may be an issue both for MNs—due to their low memory and processing power—and CNs—which they communicate with a large number of MNs [39]. Secondly, the CGHoA (asymmetric) association at session setup enables securing future BUs. However, an attacker may intercept the initial

signalling messages from the MN, exchanging with the attackers own generated CGHoA, then responding back to the MN. Because the security association is unilateral (only the MN address is a CGA), the MN will validate the attackers responses.

In turn, credit-based systems introduce a significant limitation on the data transmission performance, as they set an upper bound for the CN packet transmission rate which is equal to the data reception rate from the MN. In cases where the communication is asymmetric, e.g. video- or audio-streaming, or file transfer, or due to congestion, packet loss or handoff delay, the MN will only communicate with the CN to acknowledge the data received. The CN will then have a restricted transfer capability as long as the amount of data able to be sent to the MN is equal or lower than the addition of the acknowledgment packet payload sizes received from it. This may, however, alleviate flooding attacks in those scenarios where a number of rogue bindings have been placed in the CN by an attacker, but the attacker is not able to perform an out-of-band acknowledgement of the segments.

PRO-MIPv6 assumes a non-compromised network infrastructure, that precludes ingress-filtering and IP spoofing. It includes both CGA mechanisms and a mixed routing-cryptographic scheme. However, as from the previous discussion, these approaches also present security vulnerabilities. Thus the need to investigate on further security enhancements to binding management security.

Additionally, apart from the aforementioned security issues, the protocols introduced in this chapter also present inadequate signalling latencies. These latencies should be further reduced to improve the users QoE.

Future research should address these security and performance concerns. Efforts could focus on stronger cryptographic schemes, network architecture designs, the addition of support protocols for location management security purposes, such as Secure Neighbour Discovery and DNSSEC or other trusted authorities; and for handoff performance management purposes, such as IEEE802.21.

4.8 Summary

In this chapter, the PRO-FMIPv6 protocol has been described. This signalling protocol allows for faster and more efficient FMIPv6 handoffs because the MN

updates the Binding Cache of the CN while the link layer handoff procedures are being carried out. It also makes use of a different approach than Return Routability for securing the home and care-of address checks.

The performance of this protocol has been measured in terms of route optimised handoff latency. Simulation results confirm the PRO-FMIPv6 protocol achieves a reduction of up to 50% in comparison with other relevant protocols: base Return Routability, PB-FMIPv6 and ERO, in cases where the link layer handoff is either negligible or significant. In those cases where link layer handoff delay is significant, PRO-FMIPv6 is as efficient as PB-FMIPv6, while the other protocols under consideration negatively affect the packet reception at the MN.

A security analysis has been also carried out in this paper. Results highlight that PRO-FMIPv6 is as safe as Return Routability or PB-FMIPv6. In turn, ERO is safer than these other protocols, but it is more computationally expensive and presents a higher impact on the network throughput.

A novel IEEE802.21-based FMIPv6-operated mechanism has also been described. This scheme avoids the packet loss at FMIPv6-enabled handoff derived from PAR's L2 buffering at the moment of PAR-NAR tunnel set-up.

To assess the performance enhancement, the received packet sequence number evolution during handoff has been explored. Two factors have been taken into account, the advertised rwnd size, which is directly related to the extent of the wireless link congestion, and therefore with the PAR's buffer queue size, and the L2 handoff delay.

Simulation results show relevant benefits on implementing the proposed buffer management scheme: since fewer packets are lost at handoff, TCP flow advances earlier (up to 200% faster) into congestion avoidance.

Chapter 5

TCP Performance Enhancement at Handoff

In keeping with the ABC paradigm, a MN must be able to handle the L2 and the subsequent L3 handoffs seamlessly. The previous chapter presented a L3 signalling scheme that would enhance the mobile user's QoS. L2 and L3 handoffs, though, impact on higher levels of the TCP/IP stack since their inherently-involved disruption time interrupts upper level protocols' connectivity.

This Chapter presents a TCP enhancement that aims at reducing the handoff's QoE impact on users. Based on a novel congestion control algorithm and the FMIPv6 co-design, the proposed solution improves the goodput figures at handoff, reducing the service latency and thus increasing the effective channel capacity by up to 35% in the considered scenarios.

5.1 Introduction

The handoff process, in a macro-mobility scenario, involves both L2 and L3 handoffs. L2 handoff disruption time is derived, e.g. in IEEE802.11 networks, from scanning channels, synchronizing to new APs and performing link level signalling. L3 handoff disruption time is derived from the new IPv6 address configuration (NCoA) and transmission of a BU to the HA and the CN. Therefore, handoff entails a disruption time during which transport and application level protocols cannot access the network.

There is a growing concern from across the research community about the repercussions of L3MP on higher level protocols and applications. The mobility procedures' disruption time especially affects delay-sensitive communications, such as those RTP or TCP-based, which operate considering timings. For instance, Portoles et al. [127] evaluates the performance of VoIP traffic (by means of the *R factor*, [66]) of the MIPv6 and SIP mobility protocols in IEEE 802.21 protocols. Kim and Moh [128] introduce a similar study focussing on FMIPv6-enabled WiMAX networks. Also, the impact of cellular networks on VoIP networking is especially relevant due to their in-built mobility management schemes [129]. In turn, Fathi and Chakraborty [130] present an extension of this work on VoIP towards heterogenous network environments. Other studies on VoIP performance of a number of mobility-enabling protocols can be found in the literature.

Likewise, TCP and TCP-based applications have also been subject of thorough scrutiny. The research community's work ranges from mere measurements of throughput at handoff [131, 132] to complex analytical modeling of the TCP behaviour [21, 133, 134]. A number of alternative schemes and modifications to TCP have been proposed to overcome the problems that it presents at handoff. In Section 2.3.4, three approaches that effectively increase throughput at handoff [53, 54, 55] were introduced. Many other approaches have also been proposed. For a more general reflection on the issues of TCP in nomadic networks see Tian et al. [135].

The purpose of the present chapter is to introduce a set of modifications to TCP that enhance the its performance at handoff. For the sake of simplicity, only the FMIPv6 *proactive* handoff type has been considered.

Consider a FMIPv6-enabled MN that establishes a TCP-based communication, for instance to start an FTP file download with a CN, and at some point carries out handoff to another link. As explained in Section 2.3, the CN, unaware of the MN's handoff, would continue to send TCP segments expecting data ACKs from the MN. However, TCP was engineered for wired, fixed topologies and therefore it assumes that any losses or RTT deviations are due to congestion. Therefore, during FMIPv6 handoff, even if no packet loss occurs, TCP assumes network congestion due to the disconnection time, and reacts triggering congestion control mechanisms, thereby decreasing the network throughput.

In those cases where the timeout for the outstanding data occurs before the handoff termination, TCP will perform Slow Start. Otherwise, in those cases where the handoff process is finished before the RTO expires, the CN will perceive a larger RTT and it will re-compute TCP connection status variables. This could entail higher RTO values thereby delaying lost packet retransmissions. Moreover, due to handoff, packet loss or to flow deviation may occur, which cause some extent of packet reordering [136]. This packet reordering would make the MN send duplicate ACKs (DUPACKs) thereby triggering Fast Retransmissions and Fast Recovery at the CN.

If the CN continues to send TCP data packets downstream while not receiving any corresponding ACKs, it will gradually reduce the TCP usable window size. This mechanism, known as *sliding window*, is a constituent part of TCP congestion control. When the TCP usable window size decreases to zero, the CN cannot send packets. In this manner, as the CN does not receive any ACKs, it (incorrectly) assumes network congestion and stops sending segments. At the other end-point of the communication, the MN is performing the L2 and the subsequent L3 handoffs. FMIPv6 [18] and related approaches enable a proactive approach to handoff: before handoff, the MN forms a NCoA and solicits the PAR to start forwarding packets to that address at the NAR link. As a consequence, the communication disruption is limited to the link layer procedures, e.g. synchronizing to the new IEEE 802.11 access point. Theoretically, the packets addressed to the MN's PCoA are not lost, as they are forwarded to the NCoA and buffered by the NAR until the MN has joined the NAR's link and requests them.

Previous work extensively explores the RTO expiration of unacknowledged data at the CN [53, 54, 55]. While these approaches are effectively able to avoid RTO expiration during handoff, they leave room for enhancing the performance of TCP at handoff, and for making full use of the FMIPv6 buffering facilities. Moreover, they offer partial solutions since they address a limited number of scenarios. The complexities of the web of interactions within larger operative frameworks, such as the Internet, should be thoroughly discussed and their effects should be bound by well-engineered contingency plans (see Section 5.6.7).

The TCP enhancement proposed in this research aims to make efficient use of the NAR's buffering capability for TCP flows while dealing with the issues targeted by previous work, i.e. RTO expiration and cwnd shrinking. The use of

the proposed enhancement helps to ensure fairness and reduces some security risks for both the MN's and the other users of the subnets that the MN is performing handoff across. Numerical evaluation illustrates the improvements in which the proposed enhancement incurs into. Among others, it reduces the burstiness and increases the throughput of TCP Reno.

This chapter is organised as follows. Section 5.2 introduces the Enhanced TCP scheme. Next, Section 5.3 illustrates the IETF-compliant signalling formal format. Section 5.4 offers a more detailed explanation of the operation of each on of the involved network entities. Section 5.5 explains the interaction of Enhanced TCP with L3MPs, which is based on the IEEE802.21 cross-layer notification protocol. Section 5.6 compares the performance of of suggested algorithm with standarised implementations of TCP and other relevant approaches via simulation. To assert the effectiveness of the algorithm, goodput, congestion window evolution and fairness and security are thoroughly analysed. Finally, conclusions are drawn.

5.2 Protocol Overview

The proposed scheme, illustrated in Figure 5.1 works as follows. Immediately after establishing the communication with the MN, the CN keeps track of the average transmission rate all through the duration of the TCP flow. In order to do so, it uses a similar approach to the SRTT calculation. This avoids miscalculating the average transmission rate due to the transmission bursts, which frequently affect TCP flows.

Prior to handoff, the FMIPv6-enabled MN triggers the signalling tasks according to [137]. In this proposal, the FMIPv6 HAck and PrRtAdv messages are modified to include the so-called FMIPv6 Buffering option. This option includes the available capacity of the NAR's buffer allocated to the MN (Permissible Buffer Size, PBS), and the Expected Handoff Delay (EHD) in case the MN decides to handoff to its link. The specific option format is illustrated in Figure 5.2. Subsequently, the MN sends a Handoff Start notification to the CN. The notification is embodied in a TCP option header field. This option header, shown in Figure 5.3, comprises the same functionalities as its L3 equivalent the FMIPv6 Buffering op-

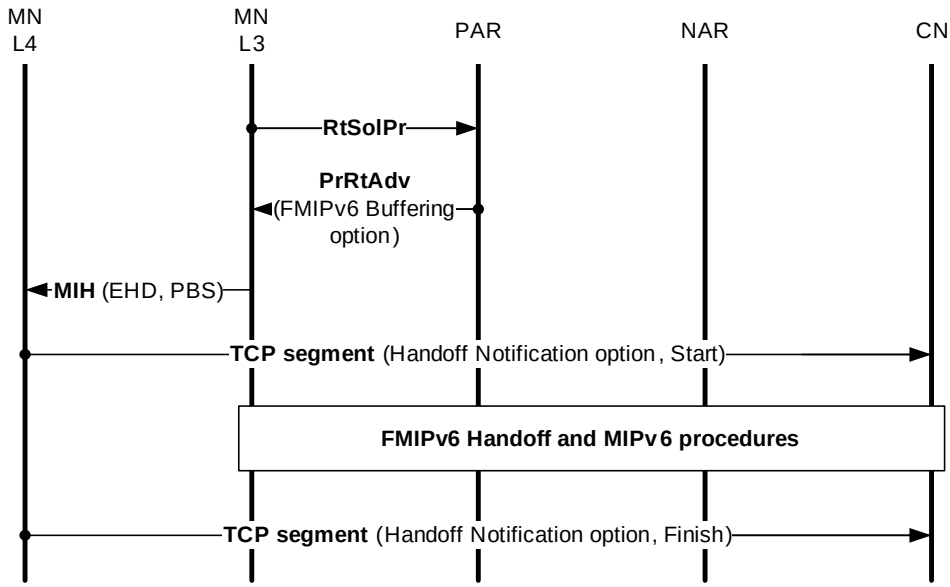


Figure 5.1: Enhanced TCP signalling

tion. Both options, presented in Section 5.3, have a 1-byte kind field and a 1-byte length field, followed by a 4-bit EHD field and a 4-bit PBS field.

On receipt of the Handoff Start notification message from MN, the CN cancels the RTO timer for the MN's outstanding unacknowledged data. Next, CN sets a Handoff Delay timer using the value retrieved from the EHD field and continues sending segments at the same transmission rate until the Handoff Delay timer expires, or the total amount of sent segments' size exceeds the PBS. After the Handoff Delay timer expires, or on receipt of a Handoff Finish option, the CN resumes standard TCP congestion control mechanisms.

Through the facilities provided by FMIPv6, all the packets sent to the PCoA during this period are forwarded from the PAR to the NAR, which buffers them. The NAR may also buffer packets from HA and CN, in those cases where a proactive route optimization scheme applies. After the MN has joined the new link, and has performed the necessary L3 signalling issues (e.g. DAD), it starts receiving and acknowledging the buffered TCP segments. When the CN receives a Handoff Finish Notification message, it assumes the MN has already performed handoff, so it cancels the Handoff Delay Timer and resumes normal TCP operation. Also, it sets the RTO timer for the unacknowledged data, making use of the RTT.

On expiration of a RTO for data sent during the MN's handoff, the CN assumes handoff failure (at transport level). Generally, RTO expiration is a consequence of either failure of the L3 handoff (MIPv6-related procedures); or impossibility of the MN to acknowledge data before the RTO expires, due to either network congestion or low throughput in the new link. As experimental evidence suggests, high levels of congestion in either PAR or NAR may disrupt or prevent the transmission of MIPv6 packets. These effects are specially adverse in FMIPv6, which transmits some packets proactively according to L2 triggers. If these triggers are not produced sufficiently in advance to handoff, it is likely handoff signalling may fail.

Moreover, if the network is congested, it is more likely that the MN is not able to acknowledge all the buffered segments before the RTO expires. To avoid this issue, the RTT timer is not cancelled. The first RTT value computed after handoff will be, therefore, artificially increased by the value of the handoff delay. Thus, the MN will have enough time to acknowledge the buffered segments, even under moderate congestion levels. The RTT value, smoothed by the formulae in [45], will eventually adopt the new (stable) value of the path NCoA-CN.

Also, RTOs may expire as a result of packet loss. This packet loss can be consequence of L2 procedures, L3 signalling mechanisms or buffer overload at the NAR. High levels of congestion, signal fading and synchronization issues may also affect the correct transmission of segments. As it seems, handoff is a complex process which has an effect on different levels of the TCP/IP stack; it is therefore difficult to model the packet loss characteristics for each level and react intelligently. The proposed solution does address this issue. When an RTO expires, it triggers standard TCP congestion control mechanisms.

5.3 Message Formats

The proposed enhancement for TCP flows at handoff relies on two different options. Firstly, the NAR uses the FMIPv6 buffering option to send through the PAR the EHD and PBS values. Secondly, before handoff, the MN retransmits these values within the TCP Handoff notification option. Finally, after handoff, the MN sends a sends a second Handoff notification option setting both the EHD

and PBS fields to zero. Next, the FMIPv6 Buffering and TCP Handoff options are introduced.

5.3.1 New FMIPv6 Options

Buffering Option

This option is defined within the Mobility Header option space, and it should be included in the NAR's HAck message and forwarded to the MN in the PAR's PrRtAdv message. Thus, the MN is aware of the buffering capabilities of the NAR before starting handoff.

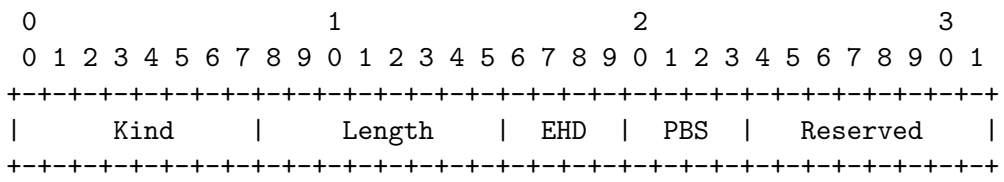


Figure 5.2: FMIPv6 Buffering Option

Kind: TBD.

Length: The size of this option in 8 octets including the Type and Length fields.

EHD: Expected Handoff Delay field. NAR calculates it according to Equation (5.2a).

PBS: Permissible Buffer Size field. NAR calculates it according to Equation (5.2b).

Reserved: This field is unused. It must be set to zero.

5.3.2 New TCP Options

Handoff Notification

This option is to be included within a TCP PDU. The MN would attach, before handoff and only in case the EHD is different from zero, this option to a TCP message and send it to the CN. Thus, the CN is aware of the buffering capabilities of the NAR.

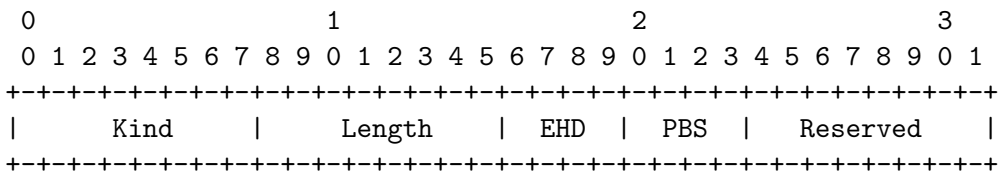


Figure 5.3: TCP Handoff Option

Kind: 29 [138].

Length: The size of this option in 8 octets including the Type and Length fields.

EHD: Expected Handoff Delay field. The MN should forward the value retrieved from the PrRtAdv's Buffering option.

PBS: Permissible Buffer Size field. The MN should forward the value retrieved from the PrRtAdv's Buffering option.

Reserved: This field is unused. It must be set to zero.

A note on format design

The message formats on Figures 5.2 and 5.3 appear to be very similar, potentially inducing the reader to mistakenly consider both messages part of an inefficient solution. However, it must be taken into account that these messages operate at different level within the TCP/IP stack: While the FMIPv6 Buffering option operates at L3, the TCP Handoff option operates at L4. This solution presents two advantages, specifically:

1. The signalling between the NAR, the PAR and the MN is carried out using L3 PDUs. Thus, neither the PAR nor the NAR have to implement TCP message encapsulation.

2. The signalling between the MN and the CN is carried out at using L4 PDUs. If the signalling were limited to L3, not only the MN but also the CN would have to implement a cross-layer notification scheme.

The packet formats proposed, therefore, are the most appropriate to fulfil the required functionalities. Other secondary advantages arise from this approach, such as the possibility of *piggybacking* the notifications into other messages, thereby reducing the overall signalling latency. Also, it permits the MN to modify the PBS and EHD values in case the MN does not consider them appropriate.

5.4 Protocol Details

In the forthcoming discussion, the operational procedures for the participating nodes are introduced in detail.

5.4.1 Correspondent Node Operation

The major part of the computational burden rests on the CN, whose TCP code has to be modified. In fact, this work proposes a new congestion control scheme. The new scheme would be triggered exclusively during the MN's handoff, on receipt of a Handoff Start notification message. There are two possibilities for the CN to resume standard TCP congestion control procedures: either by receiving a Handoff Finish notification or by the MN's failure to perform handoff correctly, as indicated by a handoff delay watch. In the forthcoming discussion, the CN's protocol details, illustrated in Figure 5.4, are explained.

At the beginning of the TCP session, after TCP's three-way *handshake* establishment phase, the CN keeps track of the average amount of bytes sent each RTT ($\bar{V}$) in 500ms intervals. The rationale behind this is to avoid the transitory data transmission rate spurious—consequence of bursty nature of TCP—hence having a more accurate long-term estimate. Together with the RTT value, this methodology permits the CN to calculate an approximation to the transmission rate. The CN tracks this value throughout the duration of the communication.

Eventually, the MN starts handoff procedures. On receipt of the Handoff Start notification from the MN, the CN cancels the RTO timer for the MN's outstanding unacknowledged data. The CN also freezes the RTT value, as it will be explained later, and cancels its Keep Alive timer so that no probes are sent. The CN does not necessarily have to freeze the Persist timer since probes

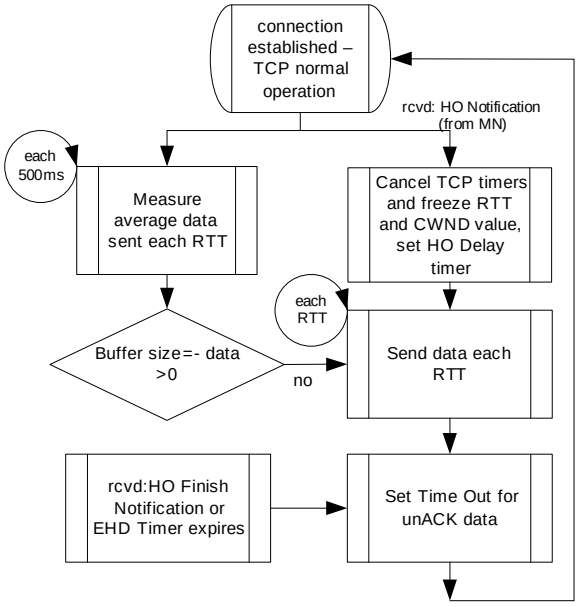


Figure 5.4: Sender's algorithm

are not sent securely are therefore having no reply from the MN has no further consequences, i.e. no triggering of the congestion control procedures.

The CN should freeze the RTT value to avoid including the handoff delay contribution to the packets RTT at handoff. After the MN has completed handoff, if the PBS is higher than zero, there will be some segments stored at the buffer of the NAR which will cause a degree of burstiness. If the MN has performed handoff to a link with higher available bandwidth, this burst will not represent an issue. However, in those cases where the MN performs handoff to a link with lower available bandwidth, this burst may increase network congestion. Now, some CNs may take the risk of increasing the RTO timer somehow proportionally to the buffered segment size, at the cost of triggering *lately* the congestion control mechanisms, such as Slow Start and so forth. In doing so, these CNs must not cancel nor freeze the RTT measurements, thereby increasing the RTO value. Alternatively, some CNs may want sustain a strict control of the congestion control, and therefore they should freeze the RTT value to that prior to receiving the Handoff Start notification from the MN. In doing so, these CNs will preserve a value of RTT not affected by the handoff delay, which in turn derives into more congestion effective RTOs. These nodes, however, should be consistent with the accepted PBS value. If congestion and its implicit security issues are

relevant, it should not forward any segments during handoff, definitely avoiding any possibility of congestion in the MN's new link (Section 5.6.7).

Next, CN sets a Handoff Delay timer using the value retrieved from the EHD field and starts sending $\bar{V}$ bytes each RTT until the Handoff Delay timer expires, or the total amount of bytes sent since the Handoff Start notification was received exceeds the *buffer size*, which is retrieved from the PBS field. In those cases, once the Handoff Delay timer expires, the CN sets the RTO timer for the unacknowledged data, making use of the RTT. Otherwise, if the CN receives a Handoff Finish notification from the MN before the Handoff Delay timer timeouts, it starts the RTO timer and resumes standard TCP congestion control mechanisms.

5.4.2 Mobile Node Operation

Before handoff, the MN obtains the PBS and EHD values from the PAR's PrRtAdv message. If these are not available, the MN should formulate an educated guess on these values based on the RAT. If the MN overestimates the PBS value, it may perceive packet loss if

$$PBS < \int_{HOstart}^{HOfinish} txrate_{noHO}(t)dt \tag{5.1}$$

because any incoming packets to the NAR will be dropped if its buffer is full. Likewise, the MN should not understimate the EHD—where $HOfinish - HOdelay$ is the handoff delay and $txrate_{noHO}$ is the transmission rate prior to handoff. If so, the EHD timer at the NAR will expire before the MN has joined NAR's link, re-starting the RTO timer. Since the CN has not received new ACKs after the Handoff Start notification, the RTO has not been re-calculated yet. The RTO timer will expire if the handoff delay experienced is larger than the EHD (see discussion on Appendix B).

Once the MN has obtained the EHD and PBS values, it encodes them using Equations (5.2a) and (5.2b). Since the EHD and PBS fields on the Handoff Notification message are 4-bits long, these equations allow for a span of 0-320

seconds and 0-32MB respectively.

$$EHDfield = \left\lceil log_2 \frac{realEHD}{10ms} \right\rceil \tag{5.2a}$$

$$PBSfield = \left\lfloor log_2 \frac{realPBS}{1kB} \right\rfloor \tag{5.2b}$$

The logarithmical codification of the real EHD and PBS values is similar to *companding* methods, such as the A-law and μ-law [139], in the sense that it encodes the PBS and EHD parameters reducing the quantization error for small values. For the purpose of this work and the considered scenarios, the reference values have been arbitrarily set to 10ms and 1kB. Thus, the bounds permitted are within the ranges of latency and capacity that may be expected from the currently available access technologies such as WLAN, Bluetooth, Ethernet or cellular networks. These values could be modified, for instance, to provide larger dynamic ranges at the cost of worse proportional distortion for small values.

On the option fields' values computation, a conservative approach has been taken: While the EHD value is rounded up, the PBS is rounded down. Therefore, the CN is prompted to send a lower volume of data while expecting a higher handoff delay as the MN may suffer a contingency at handoff; e.g. higher latencies on the connection establishment with the NAR, the NAR's buffer size reduction or packet loss.

Finally, after the L2 handoff has taken place, the MNs L2 triggers a MIH event. The MN's TCP, subscribed to the MIH services, receives the trigger therefore sending the Handoff Finish message. This message consists of a Handoff notification with the EHD and PBS values set to zero. After the notification is sent, no further TCP operations are required.

5.4.3 New Access Router Operation

The NAR does not incur in any additional signalling message exchange with neither the MN nor the CN. The NAR is simply acting as a recipient for the messages addressed to the MN's NCoA. The NAR stores them until the MN joins the new link and solicits them using the FMIPv6 facilities. At that moment, the NAR forwards the buffered packets to the MN. Therefore, the NAR is not implementing any L4 functionalities.

The NAR's buffering capability is bound in terms of time and space, and these boundaries may be different for different MNs since they may have a different subscription level. Two parameters describe them: PBS and EHD. These parameters must be included in the FMIPv6 PrRtAdv message. Thus, the MN would obtain them from the PAR and it would advertise them to the CN prior to handoff. The CN, aware of the NAR's buffering capability, will bind the non-congestion controlled data segment sending period to EHD seconds and the outcoming traffic volume below PBS kB. The NAR must not store packets for longer than EHD seconds. After EHD seconds are elapsed, the NAR must silently drop every packet addressed to the MN in its buffer. Also, if the buffered packet's volume exceeds the PBS, the NAR must silently drop every new incoming packet addressed to the MN.

5.5 IEEE802.21-Enabled L3 Interaction

Before handoff, the MN sends a Handoff Start notification to the CN, triggering the Enhanced TCP congestion control mechanisms. Next, the MN performs handoff and, once it is completed, the MN sends a Handoff Finish notification so that standard TCP operation resumes. In order to send these two notifications, the MN's TCP entity must gather information on the handoff status. This information is obtained relying solely on L3 event messages. Enhanced TCP defines two new IEEE802.21 MIH event messages. By virtue of these messages, the L3MP (i.e. FMIPv6) notifies TCP when there is an impending handoff and when the handoff is completed. These two messages, the MIH_Handoff_Imminent and the MIH_Handoff_Complete, are embodied in the next two primitives.

```
MIH_Handoff_Imminent.indication {
    SourceIdentifier,
    EHD,
    PBS
}
SourceIdentifier: Type MIHF_ID. This parameter identifies the invoker of this
    primitive, which can be either the local MIHF or a remote MIHF.
EHD: Type UNSIGNED_INT(1). Expected Handoff Delay, as computed by the MN.
PBS: Type UNSIGNED_INT(1). Permissible Buffer Size, as computed by the MN.
```

```
MIH_Handoff_Complete.indication{
    SourceIdentifier,
    Status
}
SourceIdentifier: Type MIHF_ID. This parameter identifies the invoker of this
    primitive, which can be either the local MIHF or a remote MIHF.
Status: Type STATUS. Status of operation.
```

5.5.1 A note on end-to-end

Due to the FMIPv6 involvement on the Enhanced TCP procedures, the proposed solution does not qualify as an orthodox end-to-end approach, but it benefits from two of the reasons why the end-to-end approach is important on the first place. These two reasons are: protection of the innovation and reliability and robustness. Firstly, the implementation of the proposed Enhnaced TCP scheme does not preclude other non-Enhanced TCP enabled users, as this protocol is coded as an optional TLV within the IP packet. Thus, Enhanced TCP does not suppose a hard-wiring of the network protocols in any form. Secondly, reliability may be compromised from deliberate, active attacks on the network infrastructure.

Security issues have been considered at the Enhanced TCP design by: (i) the evaluation of the security relationships between the involved nodes—e.g. the PAR-NAR tunnel for PBS and EHD information retrieval must be verified prior establishment; and (ii) the determination of trust boundaries—when communication occurs across trust boundaries, routing, cryptographic or other security protection has been provided. First, if the NAR is not Enhanced TCP-enabled, flooding attacks are minimised. Second, if the NAR is Enhanced TCP-enabled and if the MN's advertised values of PBS and EHD does not match the NAR's, then the NAR itself can discard the PCoTI message coming from that MN.

Having considered the implications of the support mechanisms on Enhanced TCP, and given the fact that these are not critical for the Enhanced TCP operation, it is safe to assume that the proposed solution satisfies the IETF requirements of end-to-end-system design.

5.6 Performance Evaluation

5.6.1 General Considerations

The performance of the proposed scheme, referred to as Enhanced TCP, is compared with TCP Reno's as the handoff disruption time varies in two scenarios differentiated by the buffer size available at NAR: 100kB or 1MB (the choice of these values will be explained in next section).

The system model is equivalent to that on Figure 4.8, where handoff takes place between two WiFi APs. This scenario is valid for the study of heterogeneous handoffs because heterogeneous handoffs are make-before-break type, where current and next network accesses often belong to different administrative domains or there has been no provision for seamless mobility. Thus, since IEEE 802.11 does not support soft handoff, the particular case of roaming between two WiFi access points could also be extended to the study of heterogeneous handoffs in terms of both the signalling and the QoS disruption evaluation.

The handoff delay ranges between 0s and 1.5s. Again, a handoff delay of 0s, is of particular interest because, from a practical perspective, it provides a realistic assessment of the performance that may be expected where the MN were multihomed [119, 120]. Other handoff delay settings permit comparative analysis for a range of handoff delays since previous studies have demonstrated that relative performance is dependent on L2 handoff latency. All cases assume an identical service: a downlink TCP flow from the CN to the MN. At a predefined time an L2 hint [8] is simulated which initiates the PRO-FMIPv6 protocol-driven handoff [140].

Goodput

Figure 5.5 illustrates the average throughputs of TCP Reno and Enhanced TCP (100kB and 1MB buffer sizes). As expected, the TCP Reno throughput decreases with increasing handoff disruption time. This decrease is more noticeable when the handoff takes longer than 1s, which is exactly the RTO value that is computed by the CN in this particular scenario. When this happens,the CN triggers Slow Start as it assumes network congestion has occurred. In contrast, Enhanced TCP offers higher throughput. In case the NAR's buffer is limited to 100kB, the CN

injects up to 100kB of unacknowledged data. As explained before, if the handoff delay, defined as

$$HOdelay = HOfinish - HOstart \tag{5.3}$$

satisfies the inequality

$$BS < \int_{HOstart}^{HOfinish} txrate_{noHO}(t)dt \tag{5.4}$$

where $txrate_{noHO}$ stands for transmission rate on the no-handoff scenario and BS for buffer size, then the throughput is lower than the throughput in the no-handoff scenario. The larger the inequality, Equation (5.4), the lower the performance. If the NAR's buffer size is augmented from 100kB to 1MB, Figure 5.5 reports an augmentation of the throughput as the handoff delay increases. The rationale behind this is that the send window advertised by a MN to optimize its download throughput, while adhering to a conservative congestion avoidance philosophy, should be computed as:

$$capacity(bits) = bandwidth(bits/s) \cdot RTT(s) \tag{5.5}$$

However, in the simulation environment, the send window size is arbitrarily set to $64 \cdot SMSS$, i.e. 65536 bytes, and therefore the 1MB-buffer at the NAR acts as a 1MB extension of the send window size, which results in a higher performance. Also, users advertising higher window sizes will perceive an improved network goodput.

As a matter of interest, using Equation (5.5) is not always valid because the maximum allowable window size advertisement is 65536 bytes. The Window Scale Option circumvents this issue, extending the size up to 2^{30} bytes (1GB), but it can only appear in a SYN segment. Therefore, it must be set at the connection establishment. See Section 7.4 for a future work details on this issue.

Figure 5.6 illustrates the effect on an FTP-flow of the L2 handoff disruption. This figure shows the TCP Reno's and Enhanced TCP's (1MB buffer size) congestion window evolution during the 1MB file download for different L2 handoff delays (0, 0.25, 0.5 and 1 s). At t=0s the MN sets a TCP connection with the CN. At t=5s the MN, already in congestion avoidance stage, starts handoff. For

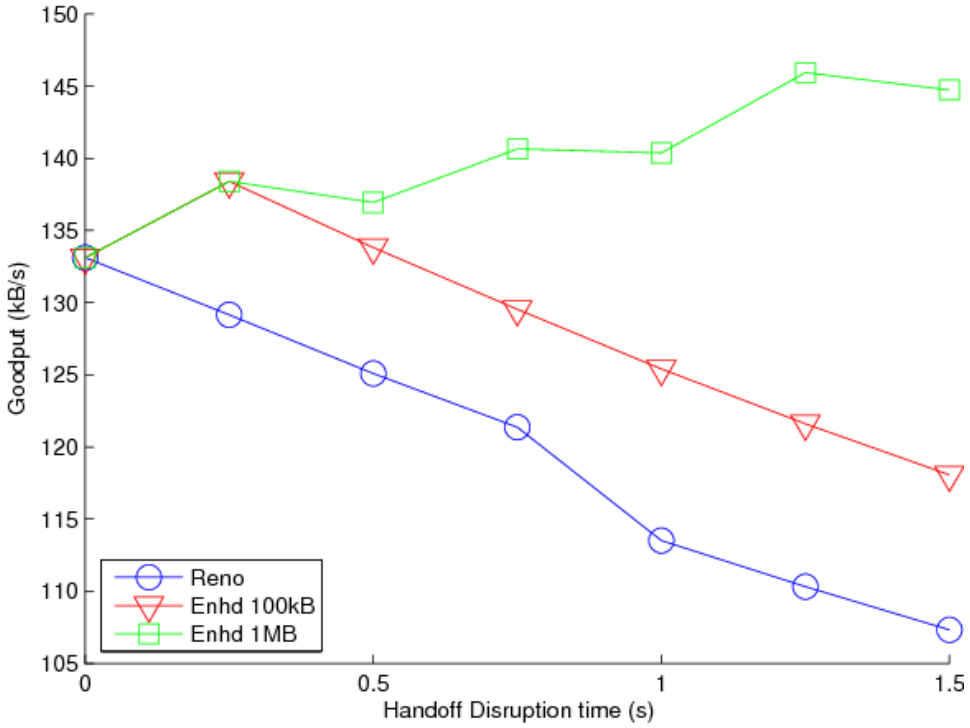


Figure 5.5: Average throughput for a 1MB file download

a 0.5s handoff delay, a TCP Reno-enabled sender waits until an acknowledgment is received. TCP would treat this as episodic network congestion, but it triggers no course of action except updating the RTTVAR and SRTT connection variables. Conversely, if the handoff delay is larger than the RTO (1s in this particular scenario), TCP Reno's congestion window is reduced to one SMSS and Fast Retransmissions are triggered.

Alternatively, the Enhanced TCP-enabled CN maintains the same data transmission rate. On receipt of Handoff Finish Notification from MN, the CN resumes normal TCP operation: the segments' ACKs receipt results on an augment of the congestion window and CN keeps track of all the connection-related parameters, such as RTT, SRTT, RTTVAR and RTO.

Congestion Window Evolution

Figure 5.7 depicts the sequence number of the received TCP segments versus time for different L2 handoff delays (0, 0.25, 0.5 and 1 s), from which a comparison between TCP Reno and Enhanced TCP can be observed. TCP connection starts

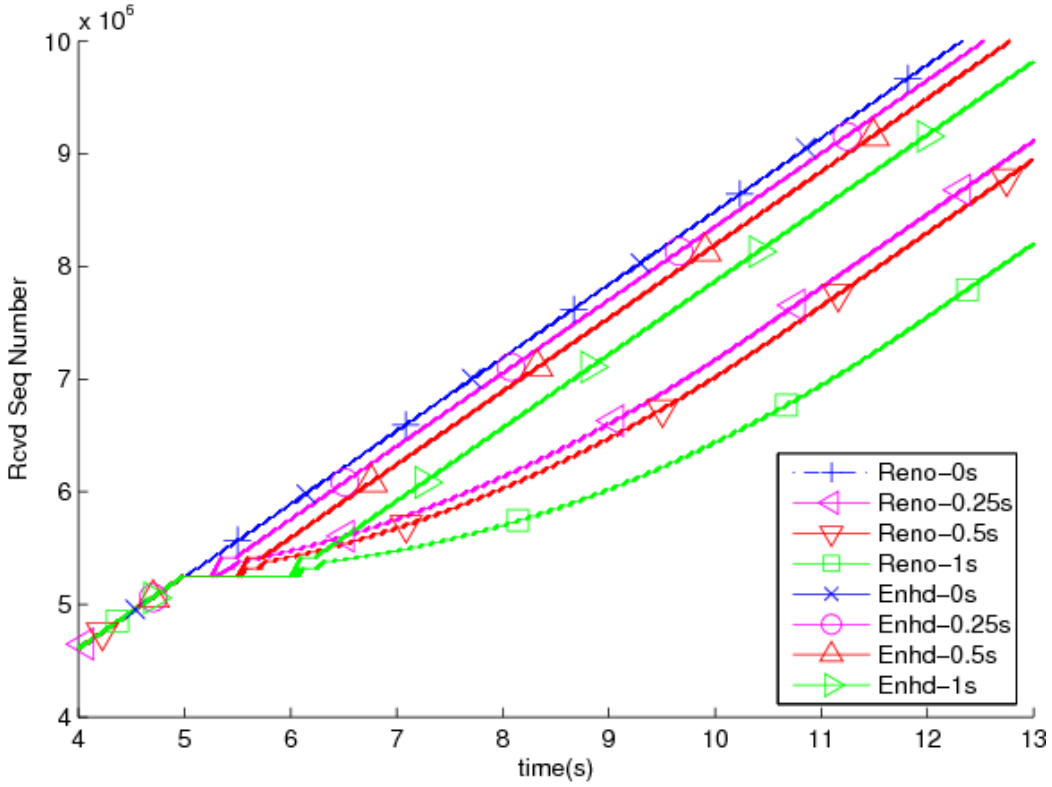


Figure 5.6: Mobile Node's Received Sequence Number evolution

at t=0, sequence number set to 25000. The Enhanced TCP curves show how, after handoff, the MN receives the buffered data segments (at NAR) so that it resumes normal TCP operation without decreasing the average data rate. TCP Reno curves, however, are severely affected by handoff, especially for handoff delays higher that the RTO value (they trigger Slow Start).

Also, the TCP Reno curves show sharp peaks on the cwnd evolution. These are caused by the number of DUPACKs received at the CN, which in turn are the result of the segments lost at handoff. These DUPACKs have an interesting effect on TCP. On receipt of three incoming DUPACKs, TCP triggers Fast Retransmit and Fast Recovery mechanisms, retransmitting the lost segment and setting cwnd to ssthresh plus 3·SMSS. This artificially inflates the cwnd by the number of segments (three) that have left the network because the receiver (i.e. the MN) has buffered them. However, due to the number of lost segments, an approximately equal number of DUPACKs is produced by the MN. For each one of these additional DUPACKs, the CN inflates the cwnd by one SMSS to reflect

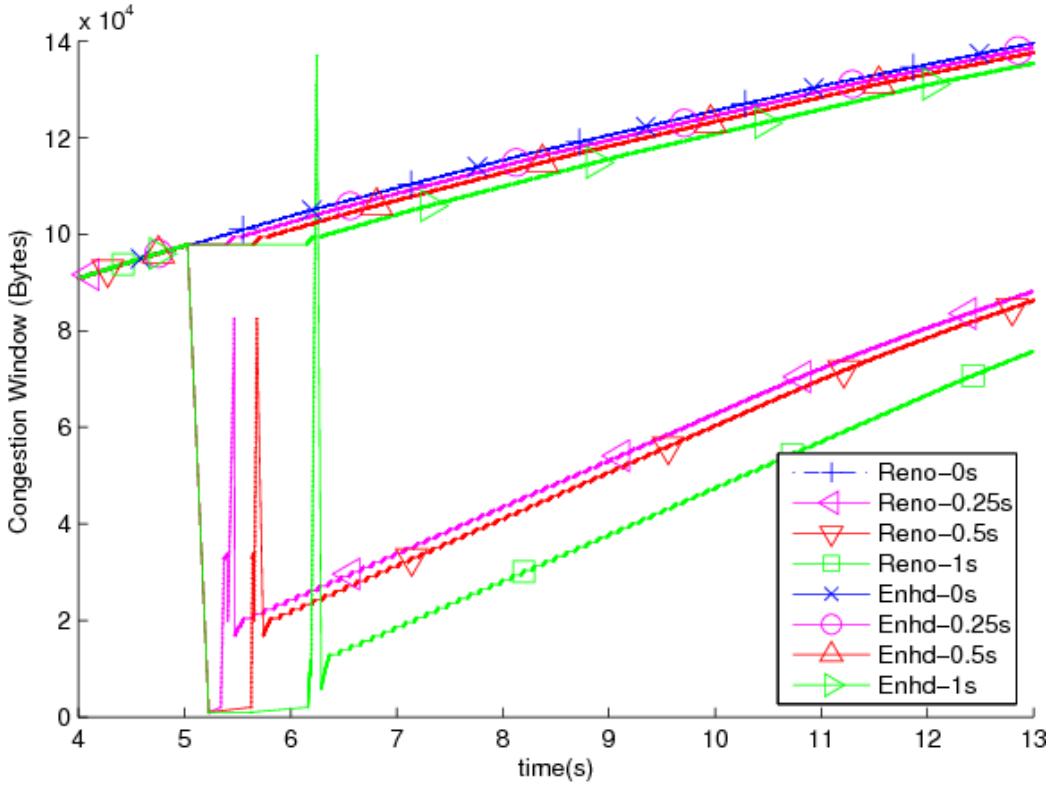


Figure 5.7: Correspondent Node's Congestion Window evolution

the additional segment that has left the network (which corresponds to the peaks on the cwnd evolution). This makes the transmission enter a loop of retransmissions from which the MN is not able to recover. Finally, at RTO expiration, TCP prunes the retransmitted segments and enters Slow Start. Obviously, this process yields in the poor performance that Figure 5.7 illustrates.

5.6.2 Impact of End-to-End RTT

Figure 5.8 illustrates the effect of handoff on the congestion window size for a fixed 0.25s L2 handoff delay. In Figure 5.8a the delay of link c (MN-PAR) is set to 20 ms, and the delay of link d (MN-NAR) is set to 5ms. In Figure 5.8b, the delays of links c and d are set to 5 and 20 ms respectively. The Enhanced TCP curves show that the CN's congestion window dropping was avoided, whereas the Reno TCP curves show congestion mechanisms were triggered, therefore reducing the network goodput. The figures also show a different segment reception rate for the links. The rationale behind this is that the cwnd is lower that the $bandwidth \cdot RTT$

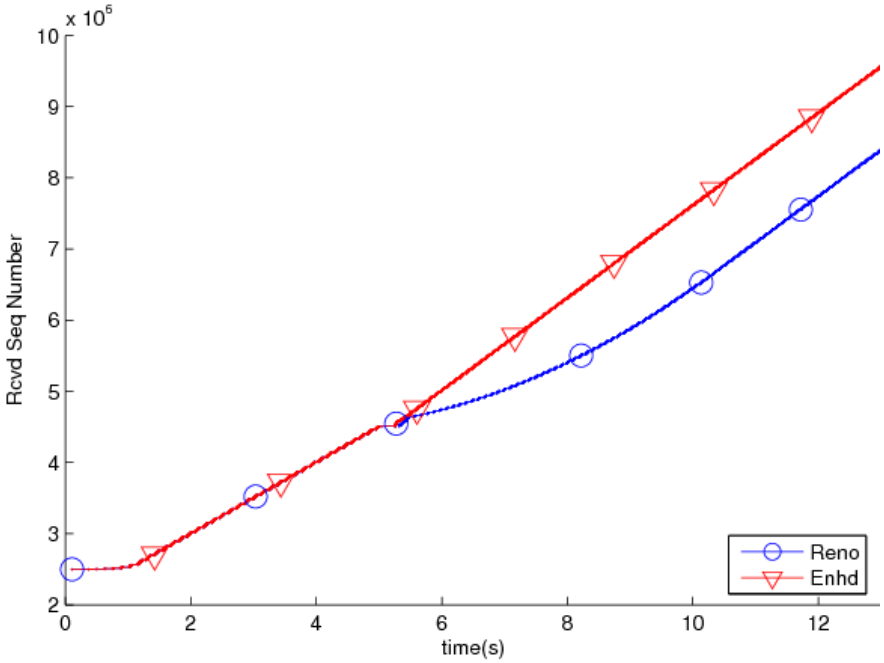
on both links. Since the available bandwidth in both links is the same, varying the parameter RTT entails a different performance. As the figures depict, the reception rate is higher for the 5ms-delay link than for the 20ms-delay link. No other effects derived from the use of the Enhanced TCP scheme are acknowledged.

5.6.3 Impact of Expected Handoff Delay

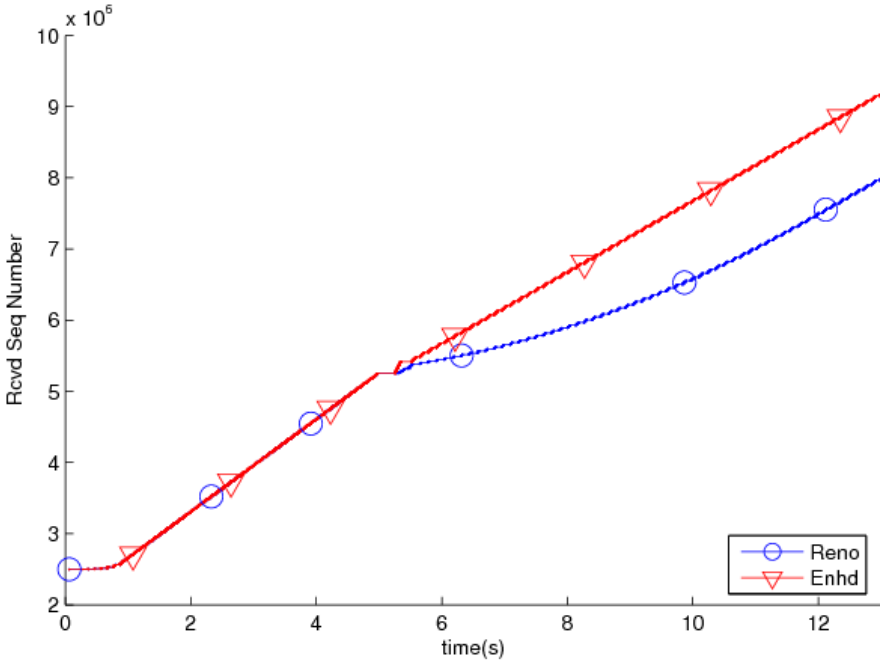
The EHD value plays a determining role on the performance of the Enhance TCP scheme at handoff. The MN, before handoff, must be aware of this value or offer a fair approximation. By virtue of the FMIPv6 facilities, the MN may retrieve the EHD value from the NAR, the PAR or some other network entity, such as a local CRRM. However, in those cases where the MN cannot obtain the EHD before handoff, it must produce an educated guess based on the RAT being used. Next, the MN notifies this value to the CN. On receipt of this notification, the CN sets the EHD timer and triggers the Enhanced TCP congestion control mechanisms. The CN makes use of this mechanisms during the MN's handoff until either it receives a Handoff Finish notification or the EHD timer timeouts. In any of these two eventualities, the CN resumes standard TCP mechanisms and re-starts the RTO.

The implications of EHD approximation errors are of major importance. If the EHD value is higher than the actual handoff delay, then the CN will go back to standard TCP operation, triggered by the reception of the Handoff Finish notification. This is the most desirable situation since the MN would enjoy a higher throughput and the CN a smoother cwnd evolution during handoff. However, if this value is too high, the CN may discard it due to its security implications (see Section 5.6.7). Alteratively, if this value is lower than the actual value taken by the MN to perform handoff, the CN will go to standard TCP operation before the MN has successfully completed the handoff procedures. This is likely to make the RTO expire, therefore making the CN bringing down the cwnd size which in turn leads to a performance comparable to that of standard TCP. Thus, the EHD value is a critically important element of the scheme's performance.

The effects of different EHD values are evaluated on two different scenarios, where the PBSs have been set to either 0kB or 100kB and the handoff delay is set to 1s. These two scenarios have been presented since they provide a fair



(a) c=20ms, d=5ms.



(b) c=5ms, d=20ms.

Figure 5.8: Effect of different link delays

perspective of the effects of the segment buffering at the NAR in those cases where

the cwnd size shrinks due to incorrectly estimated EHD values. As intuitively can be anticipated, buffering contributes to network congestion. In those cases where the RTO expires shrinking the cwnd size, in presence of buffering the TCP flow takes longer to re-establish itself. Reformulating the previous sentence, in the eventuality of RTO expiration, buffering is harmful. The EHD should be chosen so that it is not likely to trigger an RTO timeout before the handoff is completed, nor to be rejected by a distrustful CN.

Figure 5.9 illustrates the 0kB-buffer scenario. The advertised EHD values are set to 100ms, 300ms, 500ms, 700ms and 900+ms. As the figure shows, for every EHD higher than 900 ms the cwnd maintains its value after handoff as there is no RTO timeout, and the received sequence number evolution preserves an ascending linear trend. EHD values lower than 900 show a rather different behaviour. RTO expiration, and the consequent cwnd size reduction, impoverishes the throughput. The exponential growth of the received segment rate is better understood by remembering the principles of TCP's congestion control mechanisms: at RTO expiration, the cwnd is reduced to one segment and enters into Slow Start stage, where the cwnd doubles its size every RTT seconds (approximately), leading to an exponential increase of the transmission rate. After several RTT seconds are elapsed, the transmission rate tends to a more stable value.

Figure 5.10 illustrates the 100kB-buffer scenario. As previously done, the advertised EHD values are set to 100ms, 300ms, 500ms, 700ms and 900+ms. As the figure shows, for EHD values higher than 900 ms the CN does not contract the cwnd. The MN is effectively capable of receiving the buffered segments and transmitting their corresponding ACKs to the CN before the RTO timeouts. In comparison, EHD values lower than 900ms lead to RTO expiration. At this point, the effects of buffering become appreciable. The CN, at EHD timer expiration, re-establishes the cwnd value (removing the artificially increment during handoff) and goes into the Slow Start stage. The MN, once it has completed the handoff, it transmits ACKs for the buffered segments, but since the CN considers these are lost, it retransmits the segments as well. This effect is cumulative and leads to an increase in the transmission of duplicated segments, thereby affecting the throughput. This effect is the more substantial the larger the amount of buffered data, as Figure 5.10 shows. The characteristics for 500ms and 700ms are clearly

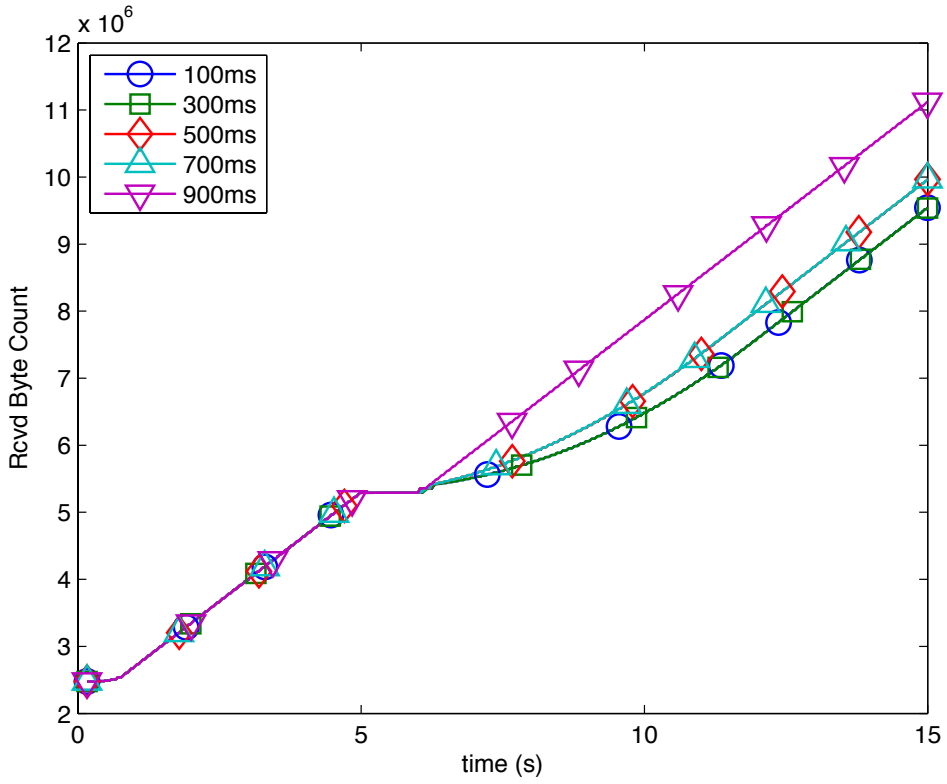


Figure 5.9: Impact of EHD on Rcvd Segment Number evolution. 0kB buffer. 1s handoff delay.

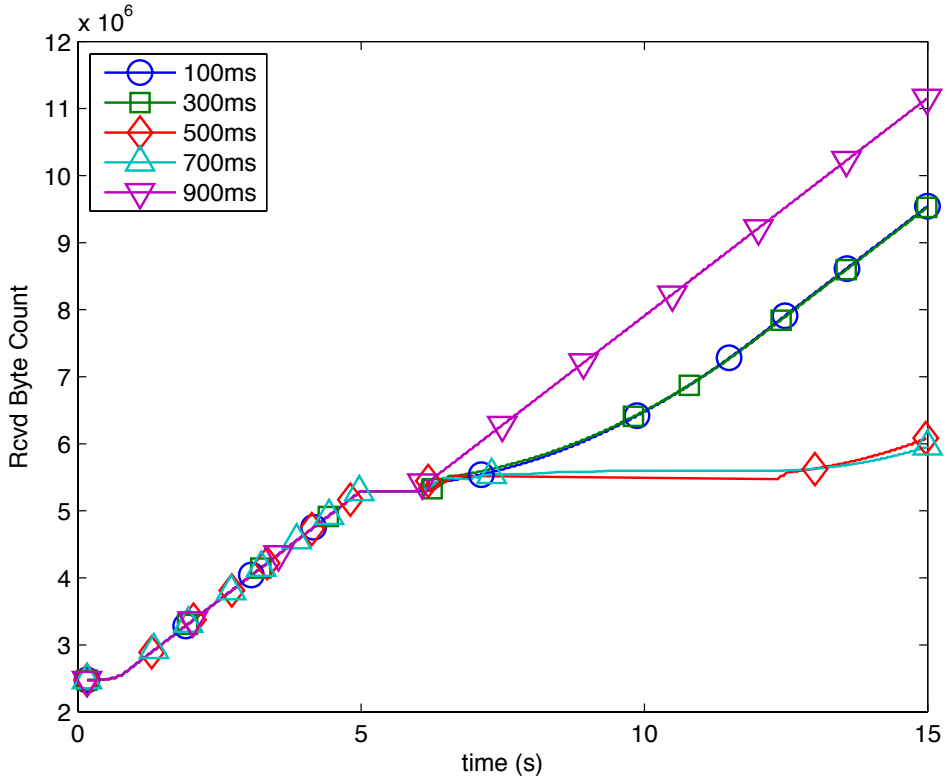


Figure 5.10: Impact of EHD on Rcvd Segment Number evolution. 100kB buffer. 1s handoff delay.

the most affected by segment duplication. For 100ms and 300ms, the transmission rates tend to recover as quick as standard TCP, in spite of the reception, immediately after handoff, of duplicated segments.

5.6.4 Impact of Permissible Buffer Size

The NAR's FMIPv6 buffering facilities have paved the way towards smoother, more efficient handoffs since they reduce packet loss. This buffer, originally designed to cope with packet loss derived from the mobility procedures, also permits storing segments during the MN's handoff from other sources rather than the PAR, such as the *Mobility Anchor Point* (in HMIPv6-enabled networks) or the CN (if proactive route optimisation applies). Like the EHD value, the MN must be aware of the PBS value or produce a reasonable approximation. It must be noted that, irrespectively of the RAT being used, handoff delays are usually short

and therefore the NAR's buffer is not intensively used. Moreover, some of the FMIPv6-based schemes do not consider bidirectional communication or any prior knowledge of the NAR's dynamic conditions, such as available bandwidth or link error rate, and therefore obtaining an updated PBS value may be an issue for a handoff-impending MN. In consequence, it is recommended the MN to produce a PBS approximation based on the RAT.

Advertising an accurate PBS value is critical for the performance of the Enhanced TCP protocol. The MN may perform handoff to a higher capacity link (e.g. UMTS to WiMAX handoff, or WiFi to a less congested WiFi), to a link with similar capacity or to a link with lower capacity. In the MN handoffs to a link with higher capacity, there is no inconvenience on advertising a high PBS value, which should be in the order of $EHD \cdot R_{PAR} < PBS < EHD \cdot R_{NAR}$, R being the transmission rate. If the MN handoffs to a link with same or lower capacity, it should advertise a 0B PBS. If the MN performs handoff to a link with lower capacity, advertising a high PBS value would impact negatively on the protocol performance. This effect will increase as the EHD increases because so will do the number of segments injected in the network, increasing risk of congestion (Section 5.6.6 explores thoroughly this scenario). For this reason, advertising a PBS higher than 0B is discouraged if the links' capacities are similar.

The effects of the advertised PBS values are evaluated on two different scenarios, where the L2 handoff delay is set to either 250ms or 500ms (keeping a constant 1s. EHD value). These two scenarios are fairly generic since handoff across different RATs is expected to take in the order of tens to hundreds of ms. The performance of the Enhanced TCP has been tested under a number of different PBS values. Higher values of the PBS are expected to incur higher bandwidth demands in the new link immediately after handoff, since the NAR will try to forward the stored segments to the MN. As explained in the previous paragraph, the MN should advertise a PBS value so that it is effectively able to receive and acknowledge a segments load size equivalent to PBS bytes.

Figure 5.11 illustrates Received Sequence Number on the 250ms L2 handoff delay scenario, for different PBS values, specifically: 0B, 100kB, 200kB, 300kB, 400kB and 500kB. Under standard TCP-enabled communication, the flow's throughput would be severely affected due to RTO expiration at the CN

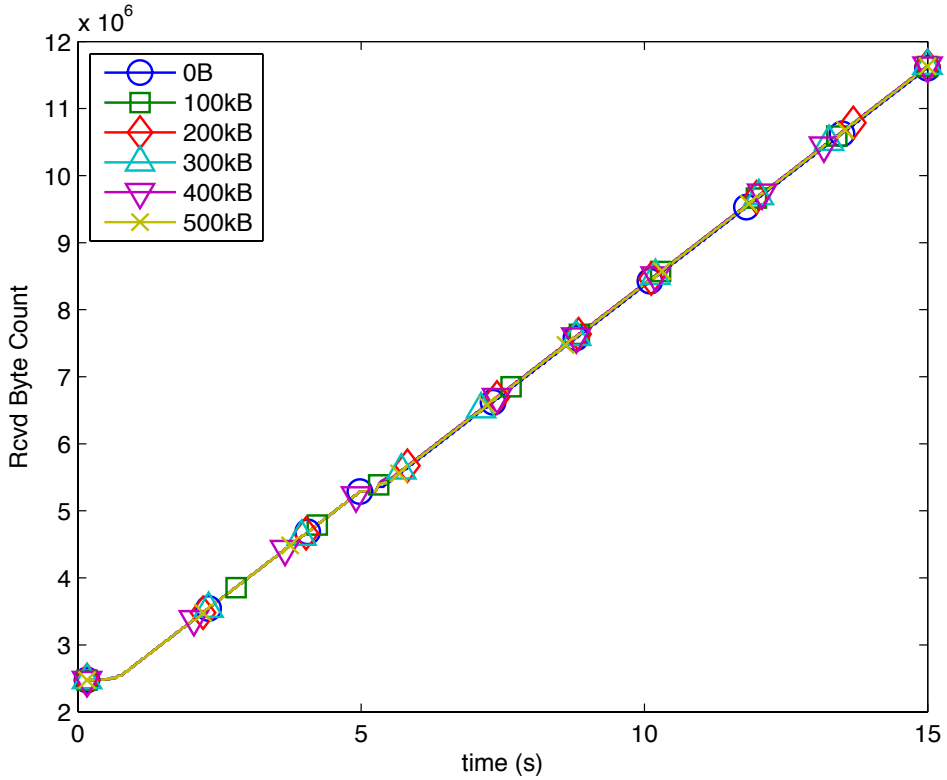


Figure 5.11: Impact of PBS on Rcvd Segment Number evolution. 1s EHD. 0.25s L2handoff delay.

(see Section 5.6.1). However, Enhanced TCP permits a smoother handoff because it avoids the CN from contracting the cwnd. Enhanced TCP offers the same performance for the different PBS values. The rationale behind this is that the CN transmits $\bar{V}$ bytes every RTT, which in the simulation environment is set to 100ms, and therefore, since $\frac{\bar{V}}{RTT} \cdot HOdelay < PBS$ for any of the considered PBSs, the amount of data buffered at the NAR is exactly the same.

At this point, it is important to have a closer look to Figure 5.5. This figure depicts a monotonically increasing linear trend on the averaged data rate during a 1MB file download (FTP service), and where the PBS is set to 1MB. Why higher buffer sizes derive onto higher average performance? Firstly, the transmission rates have been considered only during the time the MN was connected to the link (excluding the handoff delay) and during which the MN was transmitting and receiving segments. Secondly, it must be taken into account that the MN's

awnd size is 64kB, lower than $bandwidth(bits/s) \cdot RTT(s)$. This awnd precludes the MN from making full use of the implemented IEEE802.11g link's bandwidth, and therefore the NAR can forward the buffered segments within RTO seconds. This bandwidth usage is 'stretched' to cope with the segment forwarding, even for the most aggressive of the considered eventualities (the linear trend does not decay as the handoff delay reaches 1.5s). The combined effect of bandwidth usage elasticity with high PBS values is therefore the responsible of the perceived increase of throughput.

Figure 5.12 illustrates the Received Sequence Number on the 500ms L2 handoff delay scenario, for different PBS values. As before, these have been set to 0kB, 100kB, 200kB, 300kB, 400kB and 500kB. The figure depicts a behaviour similar to that in the previous scenario. There is a clear disruption on the flow's throughput during 500ms due to L2 and L3 handoffs procedures and, immediately after handoff, communication is re-established smoothly. Special attention must be drawn to the moment where the MN finishes the handoff procedures. By comparison with Figure 5.11, there is a significant difference on the number of packets forwarded to the MN. This is a consequence of the handoff taking longer, which results in a higher number of segments being buffered at the NAR. The bandwidth demand is, once again, stretched so that it accommodates the rush of segments being released from the NAR's buffer.

5.6.5 Impact of concurrent UDP flows

On completion of the handoff procedures, a FMIPv6-enabled MN requests the buffered packets from the NAR. This increases the burstiness of the TCP flow immediately after handoff. Other concurrent flows are affected by this burstiness in a greater or lesser extent, depending of the amount of buffered data, but FMIPv6 handoff and buffering may have secondary long-term effects. Firstly, TCP-friendly flows will be affected by the TCP congestion control mechanisms, which will stop the CN from sending data segments until reception of ACKs for the in-flight data. Secondly, non-TCP friendly flows (not constricted by congestion control mechanisms, such as many based on UDP) may entail a relevant number of packets to be buffered at the NAR. In this section, the dynamics of competing Enhanced TCP and UDP flows will be explored.

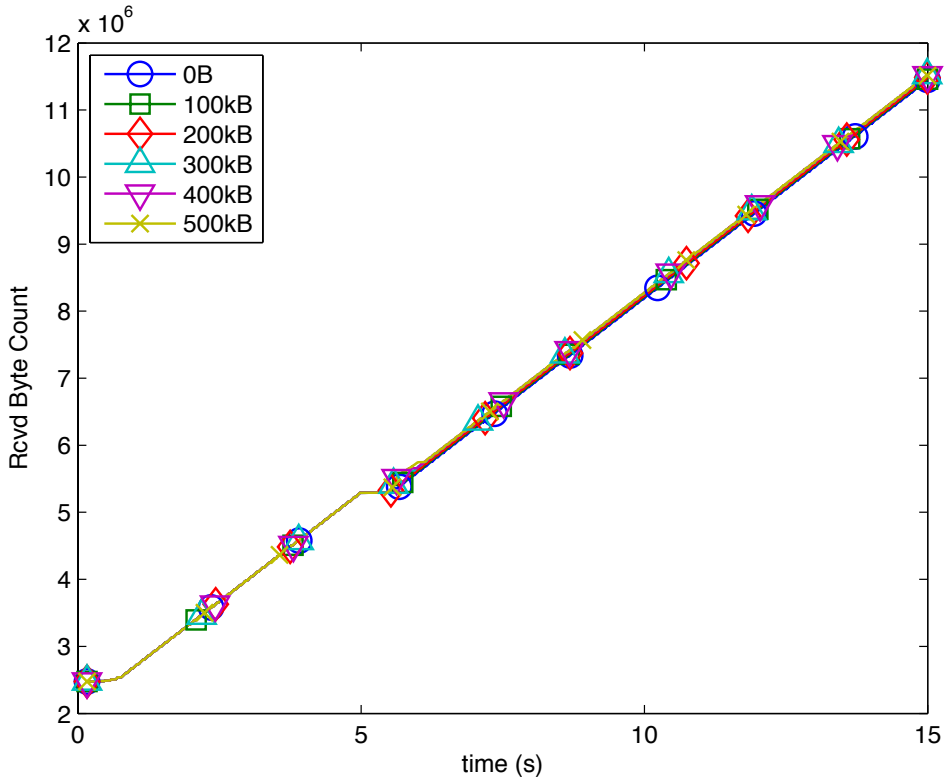


Figure 5.12: Impact of PBS on Rcvd Segment Number evolution. 1s EHD. 0.5s L2handoff delay.

The segments of a downstreamming UDP flow have been numerated. Figure 5.13 shows the Received Sequence Number evolution of this UDP stream. This UDP-based application transmits a 100kB/s constant bit rate stream, with the application level PDU set to 1024B long. The MN concurrently runs an FTP application, being 64kB the TCP awnd size. In Figures 5.13a-d, the handoff delay has been set to 100ms, 300ms, 500ms and 700ms respectively, and they show the characteristics for the TCP Reno and Enhanced TCP (0B and 1MB PBS) protocols. These PBS values represent, for the link's capacity, two extreme values: 0B implies no additional disruption to the UDP in terms of performance, since the NAR would not buffer any FTP segments. On the opposite end, a 1MB PBS would adversely affect in the UDP's performance, especially for the larger handoff delays, since it entails a larger number of buffered segments at NAR.

Figure 5.13a shows the 100ms handoff delay scenario. The UDP characteristic is disrupted during the 100ms handoff delay, but quickly after handoff it is re-established to a fairly constant reception rate—as the linear trend of the graph points out. Figure 5.13b illustrates the 300ms scenario. It can be observed a similar behaviour to that exposed by 5.13a, with the exception of the 1MB PBS line. This line shows an important disruption due to temporary network congestion. This congestion in turn is produced by the combined effect of the NAR flooding the network with FTP segments, and the CN, since it is receiving DUPACKs, enters into the Fast Retransmit loop (see Section 5.6.6). This is produced due to either packet loss (even one lost segment may produce similar results) or packet duplication, which is likely in FMIPv6 scenarios [18, Section 4]. Finally, Figures 5.13c and 5.13d depict the 500ms and 700ms handoff delay scenarios respectively.

5.6.6 Impact of Links' Capacity

A proper monitoring of the network conditions is vital for the completion of a smooth handoff, since the NAR produces the EHD and PBS values based on these conditions. Previous sections have explored the effects of malapropos EHD (Section 5.6.3) and PBS (Section 5.6.4) values independently. One of the consequences of an overestimated PBS is the temporary congestion or saturation of the NAR's link due to traffic bursts originating from the NAR's buffer. This

traffic load would be subsumed to that present in the NAR's link at the moment of handoff, what could enlarge the congestion period therefore having long term effects on the TCP flow (such as bringing down the cwnd size). This section explores this effect precisely, considering both a 0kB PBS and an (inappropriate) 1MB PBS, while varying network congestion levels. The performance of Enhanced TCP is further compared to that of TCP Reno.

Network congestion levels play a pivotal role in the performance of TCP Reno and Enhanced TCP at handoff. For instance, a severely constricted TCP flow at PAR's link may rapidly increase after handoff if a fair share of bandwidth is available at NAR. Conversely, a TCP flow enjoying a low congestion level at PAR's link may result in re-transmissions (Slow Start or Fast Retransmissions triggered at CN) if NAR's is highly congested. As explained before, these effects are cumulative with the PBS contribution to burstiness. Next, five different scenarios are considered according to different congestion levels. The naming criteria is as follows: X% congestion level refers to a 0% congestion level at PAR's link, and a X% congestion level at NAR's. Likewise, -X% congestion level refers to a X% congestion level at PAR's link, and a 0% congestion level at NAR's. The congestion levels considered are -50%, -25%, 0%, 25% and 50%. Additionally, the L2 handoff delays have been set to 100ms, 300ms, 500ms and 700ms. Figures 5.14-5.21 illustrate the results, drawing special attention to the Received Sequence Number evolution, Flightsize and MN's Number of Dropped Segments during handoff.

The focus of the analysis presented is on both cwnd and flightsize. Together, these two metrics explain the TCP Reno an the proposed Enhanced TCP activity at handoff. First, from visual inspection of the flightsize illustrations, the strong correlation between the use of the NAR's buffer and the number of unacknowledged bytes becomes obvious. Also, it is relevant to the performance of Enhanced TCP how quick the cwnd adapts to the reception of segments by the mobile node and the subsequent coming back to standard TCP operation. The results are especially significant because they mostly hold *even* with a 1MB PBS (which according to Eq. (5.2b) is a far too high value).

Some other scenarios, however, require a separate explanation. If the advertised PBS is higher than 0, then the correspondent will continue to send TCP segments until the amount of bytes injected while handoff is higher than the

PBS[1]. In those scenarios where the TCP flow was using the full link's capacity prior to handoff, and in the NAR's link there is a degree of congestion, then the NAR's link becomes saturated. This effect leads to decreased TCP goodput.

Experimental results, however, highlight the goodput increase resulting from the use of a 0 PBS for Enhanced TCP-enabled mobile nodes. It is therefore recommendable, as mentioned several times in the previous sections, for the mobile node to advertise accurate values for both EHD and PBS.

5.6.7 Fairness and Security

This work proposes that the CN should temporarily ignore the need of ACKs from the MN for the communication to flow, while keeping the same data segment transmission rate. These segments are to be stored by the NAR until the MN, after joining the NAR's link, requests them. This bursty forwarding of segments compromises the fairness of the network. In the previous section, the effect of concurrent UDP flows, which are not TCP-friendly, was thoroughly explored. However, the implications of the proposed scheme where other TCP flows compete for the link must be analysed as well. These TCP flows, which obviously are TCP-friendly, react to the appearance of a new flow in the link.

Presently, the proposed scheme does not proactively shape the traffic rate according to the new link characteristics. Therefore, it is important to carefully consider all the implications of the proposed scheme in terms of fairness, and to explore its effects on the congestion control mechanisms of the other competing (TCP) flows. In the forthcoming discussion, these will be introduced, highlighting the advantages and disadvantages for the individual connection, and the consequences for the network.

Advantages of the Proposed Approach

1. Makes effective use of the FMIPv6 buffering facilities, thereby reducing communication latency after handoff.

2. Precludes RTO expiration, avoiding cwnd size reduction and therefore optimising the data transfer time.

[1]For the analysis of the link's capacity effect on the system goodput, the EHD values have been set above the actual handoff delays.

3. Signalling does not incur in additional handoff latency and overhead is diminishable.

4. Limits the duration and volume of the data sent during MN's handoff, avoiding congestion on the new link.

Disadvantages for the Individual Connection

The proposed approach may induce NAR to drop segments as a consequence of overloading the allocated buffer size. To avoid this situation, the MN notifies the CN of the maximum PBS and EHD prior to L2 handoff so that it sets both time and volume limitations to the amount of traffic is sending to the NCoA without making use of congestion control mechanisms. Also, the NAR provides a separate buffer for the MN's segments, different from the L2 queue. Therefore, segment drop is minimised in uncongested or moderately-congested networks.

It must be noted, however, the consequences that the use of this scheme may have for other (concurrent) application flows. Much research has been carried out on the dynamics of competing flows in a link, paying special attention to the so-called TCP friendliness of the flow control mechanisms. Thus, a radical differentiation lies between flow dynamics that comprehend some feedback or congestion control, and the flows that don't comprehend such mechanisms. The use of the Enhanced TCP approach depicts a whole new scenario of study, which deserves a thorough analysis. Section 5.6.5 sheds some light on this respect. The study should be extended to the impact on different application flows or transmission codecs, as they have different bandwidth usage characteristics.

Disadvantages for the Network

1. Burstiness and unfairness in the NAR's link. TCP traffic is fairly bursty in the Internet today. For instance, a delayed ACK (covering two or more previously unacknowledged segments) received during congestion avoidance causes the CN's congestion window to slide and therefore two segments to be sent. A delayed ACK received during Slow Start would slide the CN's congestion window by two segments and then be incremented by one segment, resulting in a three segment burst. Alternatively, considering the

opportunistic behaviour of some contention-based MACs, where two delayed ACKs may be received by the sender side quasi-simultaneously, ten segments bursts occurring are not rare. Also, assuming delayed ACKs, a single dropped ACK causes the subsequent ACK to acknowledge four segments. If in Slow Start phase, this leads to a five segment burst. If in Congestion Avoidance, this leads to a four segment burst.

The proposed enhancement for TCP would cause the NAR to buffer the segments addressed to the MN, until the MN requests them. At that moment, the NAR would forward them to the MN. The burst generated would be larger than the typical bursts of the established TCP flow by a factor $\frac{HO_{delay}}{RTT}$. This entails fairness concerns for the other users of the network. The proposed enhancement includes the facilities to limit both the bandwidth and the persistency of the TCP flow during handoff, which helps to bound the network resources used by the TCP flow.

Similar problématique has been found on traffic competition for bandwidth in links with scarce resources. From the experience of deployments of non-congestion-controlled *unresponsive* or *disproportionate*-bandwidth flows (as classified by Floyd and Fall, [141]), some solutions have been proposed. These solutions include the identification of non-congestion controlled flows [142, 143], and the design of queueing protocols for the routers to restrict the bandwidth consumed by these so that congestion collapse does not take place [144, 145, 146]. The proposed TCP scheme, since removes the flow congestion control temporarily during handoff, may be benefited from the experience gained from developing these solutions.

2. Reception of duplicate segments. Since the FBU is received by the PAR, until the PAR confirms the PAR-NAR tunnel set-up (on receipt if the HAck message), the PAR may forward the incoming packets to the PCoA to the discretion of the network implementors. Therefore, FMIPv6 may represent an additional source of data segment duplication.

   For the receiver this has no further consequences but a perception of QoS degradation. The receiver acknowledges the incoming segments. From the sender's perspective, duplicate ACKs can be consequence of a number of network problems. Normally, they can be caused by segment dropping,

re-ordering of segments by the network or by replication by the network of ACKs or data segments. The TCP Reno [45] recommends the receiver, in the eventuality of taking delivery of duplicate ACKs, triggering the fast retransmit algorithm.

Fast retransmit is based on the incoming duplicate ACKs. This algorithm uses the arrival of three duplicate ACKs (four identical ACKs without the arrival of any other intervening packets) to assess that a packet has been lost. After receiving three duplicate ACKs, the receiver performs retransmission of, from its perspective seems to be, lost segments. The receiver does not wait for the RTO to expire to retransmit the segments, what may increase the segment burst size.

3. Increased packet drop rate. In networks with high drop rates, the proposed scheme could increase the drop rate even further. The proposed scheme requires the NAR to buffer the segments addressed to the MN's NCoA while the MN performs handoff. At the protocol design, special attention has been paid to smooth the segment sending rate and to keep the extent and the frequency of the bursts. NAR, however, is entitled to buffer all these segments and therefore the bursts are cumulative.

   The effects of this approach are specially adverse in those cases where NAR uses Drop Tail queue management. NARs implementing RED queue management mechanisms should be more tolerant to transient traffic bursts [147].

5.6.8 Other Approaches

SNOOP protocols segments the end-to-end communication between the MN and the CN by deploying a so-called Snoop agent at the base station (2G BSC) or at radio network controller (3G RNC). This Snoop agent is capable of performing retransmissions of lost segments based on duplicate TCP ACKs and locally estimated last-hop round-trip times. The agent also suppresses duplicate acknowledgements pertaining to wireless losses from the TCP sender, thereby preventing unnecessary congestion control invocations at the sender. The scheme has been

shown to yield significant throughput improvements for TCP environments limited by single-hop wireless in-building links, where the MN does not change its BSC or RNC of attachment.

Before handoff, segments flow approximately seamlessly through the Snoop agent as transmission and reception rates are approximately similar—not considering the wireless medium-induced frame errors which would involve frame recovery via ELN. At handoff, however, the MN stops to acknowledge segments, thus causing some buffering at the Snoop agent, which continues to send ACKs. After handoff, via ELN, the MN would quickly trigger recovery of the lost segments. If now RTOs are triggered on the Snoop agent to CN session, the transmission rate in the wireless segment would converge to that of the wired segment. However, if the MN is not able to recover the lost segments from the Snoop agent quickly enough, then the buffer at the Snoop agent may be overloaded, thus triggering standard TCP congestion control mechanisms.

This process is similar to that proposed by the Enhanced TCP scheme, and therefore similar performance results are expected. Enhanced TCP presents, however, several enhancements. Firstly and most importantly, Enhanced TCP facilitates end-to-end explicit handoff notification, which requires the implementation of TCP at the CN, but also improves the handoff experience on macro-mobility and heterogeneous scenarios. Secondly, handoff latency can be advertised by the MN prior to handoff. Thus, RTOs can be avoided by setting appropriate values for the EHD. Finally, also the buffer size at the NAR can be advertised (via the PBS value), precluding buffer overloading issues which would entail severe throughput degradation.

In turn, a Freeze TCP-enabled MN would explicitly send a ZWA message, driving the CN to ZWP mode. After handoff, the MN would send three DUPACKs (four ACKs) for the last segment received prior to handoff, thus triggering the fast retransmit algorithm. Although this mechanism involves a higher signaling load in the radio link than Enhanced TCP, similar results to the Enhanced TCP zero-PBS scenario are expected. In both cases, TCP sessions would be stopped then migrated onto the new link, maintaining the session status variables.

Le et al. [55] approach encompasses explicit handoff initiation and handoff termination messages. On receipt of a handoff initiation message, the CN freezes

the RTO timer and stops TCP congestion control. Next, on receipt of a handoff termination message, the CN retransmits the segments sent after the handoff initiation message was received. This two-message scheme is similar to that proposed in this thesis. However, it is affected by the following inadequacies. First, Le et al. assume that the inflight packets at handoff are lost. This contradicts the FMIPv6 approach and related work, which can drastically reduce the packet loss at handoff by means of cross-layer schemes and packet forwarding. The CN re-injects the supposedly lost packets, thus hindering the network goodput. Snoop, Freeze TCP and very specially Enhanced TCP are therefore expected to outperform this scheme.

Finally, Yoshimoto [54] combines both explicit handoff initiation and termination notifications with EDCA. This approach enables a handoff-specific TCP- and application-level congestion control enhancement, based on the (i) TCP segment injection halt during handoff; and (ii) the packet priority raise to AC_VO category temporarily after handoff. This combined solution precludes packet retransmissions at handoff, and enables a quick convergence to a stable cwnd value.

This solution, however, presents the following issues. First, the RTO may expire, thus hindering the network throughput as session is re-established at the ssthresh cwnd value after handoff. Secondly, it would require modifications at both the transport- and application-levels of the stack. Finally, it is only applicable to EDCA-enabled (IEEE 802.11) networks. For these reasons, even in EDCA-enabled networks, the goodput figures of the Snoop, Freeze TCP and Enhanced TCP schemes would probably be better than Yoshimotos [54].

5.7 Limitations and Future Work

TCP has been subject of thorough revision ever since was proposed in 1974. With the emergence of wireless technologies, new venues for the enhancement of TCP behaviour in error-prone, nomadic environments have been open to the research community. However, educating TCP is proven to be challenging: (i) highly dynamic access networks with often competing flows for the network resources; (ii)the difficulties to distinguish packet loss due to wireless medium errors from network congestion; and (iii) the call for scheme co-design or cognitive approaches, make TCP improvements often partial or over-engineered.

In this sense, Enhanced TCP only addresses the cwnd drop at handoff, as a consequence of packet loss, and facilitates packet buffering for fast retrieve and thus adaptation to the new link's conditions, improving network downlink figures for MNs. It comprises four explicit message exchanges. Firstly, optionally, the MN retrieves the EHD and PBS values from the PAR. Secondly, it notifies these values to the CN via a handoff initiation message. Thirdly, after handoff, the MN sends a handoff termination message to the CN. After joining the new link, the NAR would also forward to the MN the buffered segments during the MN's handoff in those cases where proactive route optimization applies.

However, Enhanced TCP also poses new risks to end users. Namely, DoS attacks may succeed if a rogue device manages to forward a high volume of segments to the NAR's buffer because congestion control is stopped at handoff. Secondly, in a lesser scale, the NARs buffer release may lead to unfairness and network congestion if the MN advertises false network information. Finally, an attacker may impersonate the PAR, thus sending legitimate messages with false PBS and EHD values. A secure network information discovery is needed to avoid this kind of impersonating attack from attackers in the PARs link. Additionally, the PAR should establish a trust relationship with the NAR via an administrative agreement.

In the short term, future work on TCP should address the afore-mentioned problems, finding consisting approaches that yield increased network throughput for mobile users, while maintaining scability, fairness and security. In the long term, future work may address the TCP challenges and the desirable design features of TCP solutions for wireless environments, presented in Section 2.3.4 and repeated here for completeness:

1. Avoiding the need of support from network infrastructure, or limiting the network infrastructure interaction to performance enhancements. Network operators are not expected to share resources or critical information, and therefore future fully-scalable enhancements should be de-coupled from the network infrastructure.

2. Handling encrypted traffic. Network security is becoming increasingly important due to the appearance of critical services on wireless platforms, such as e-banking, and the deployment of wireless access networks.

3. Multihoming support. Multihomed devices require enhancements at the transport level, e.g. to aggregate traffic within the same TCP session.

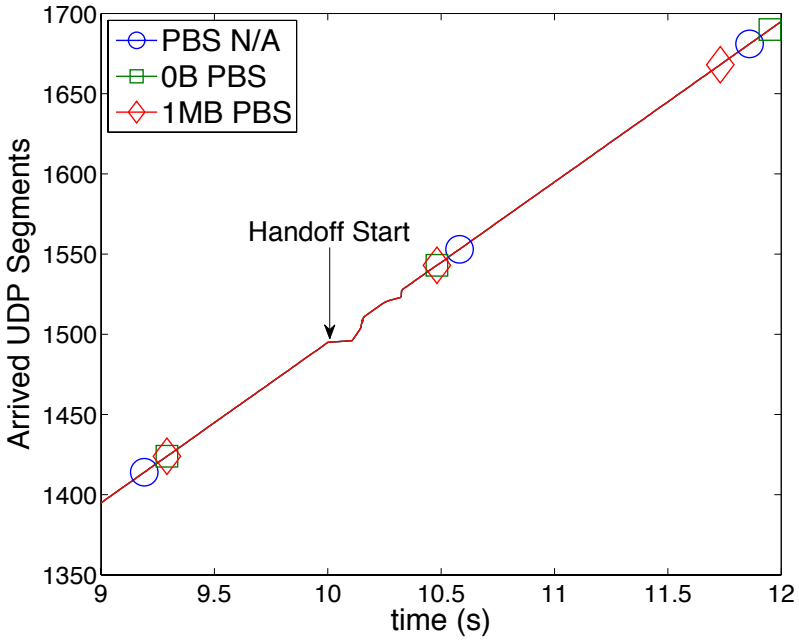
4. L2 and L3 mobility awareness for session migration. Transport-level solutions may be benefited from L2 and L3 information, e.g. to differentiate episodic network congestion from handoff.

5. Quickly adapting to new link characteristics. This is especially desirable in vertical handoffs, where users may roam among different RATs.

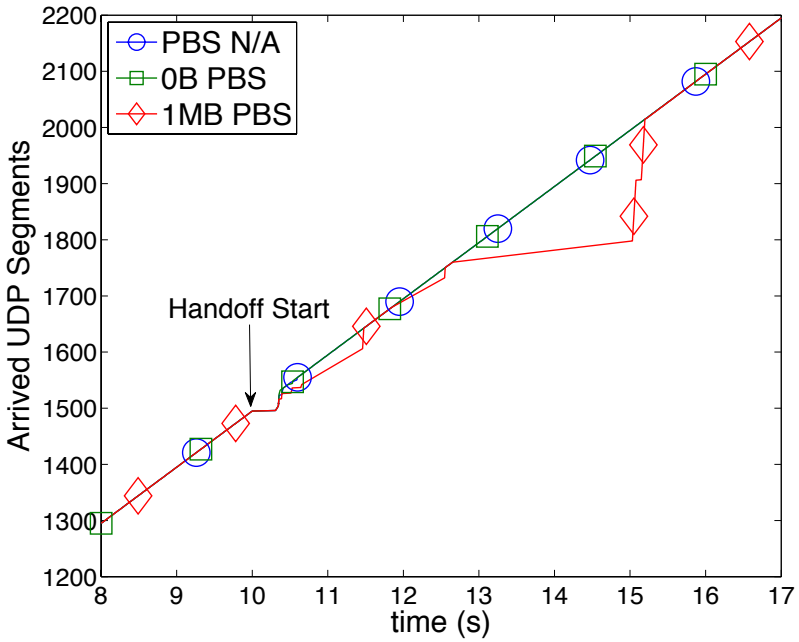
5.8 Summary

This chapter proposed a set of modifications to the TCP Reno's congestion control mechanisms, referred to as Enhanced TCP. Enhanced TCP, by virtue of the proactive L3MP such as those based on FMIPv6, notifies the CN of the MN's impending handoff and triggers a set of procedures that preclude bringing down the cwnd size. Furthermore, Enhanced TCP also comprehends the calculation, formulation and notification of the EHD and PBS values. These values describe the expected handoff delay and the permissible buffer size at NAR. In combination with the FMIPv6 facilities, they provide a lightweight but powerful more efficient handoff.

Enhanced TCP's performance has been thoroughly explored in a wide variety of scenarios, considering the impact of different L2 handoff delays, EHD, PBS, RTT, concurrent applications and link congestion. Simulation results not only highlight the benefits of the Enhanced TCP protocol, but also discuss its impact in the worst-case scenarios. The potential benefits of the Enhanced TCP protocol are better described in terms of network throughput, which increases up to 35% for the considered scenarios. Network congestion at handoff is also reduced due to the savings on packet loss, which in turn reduces the number of retransmissions.

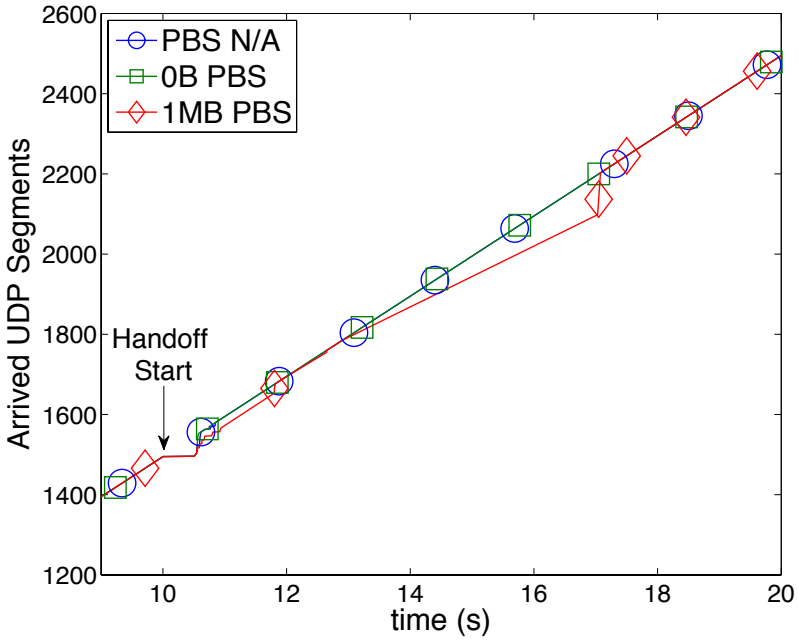


(a) 100ms handoff delay

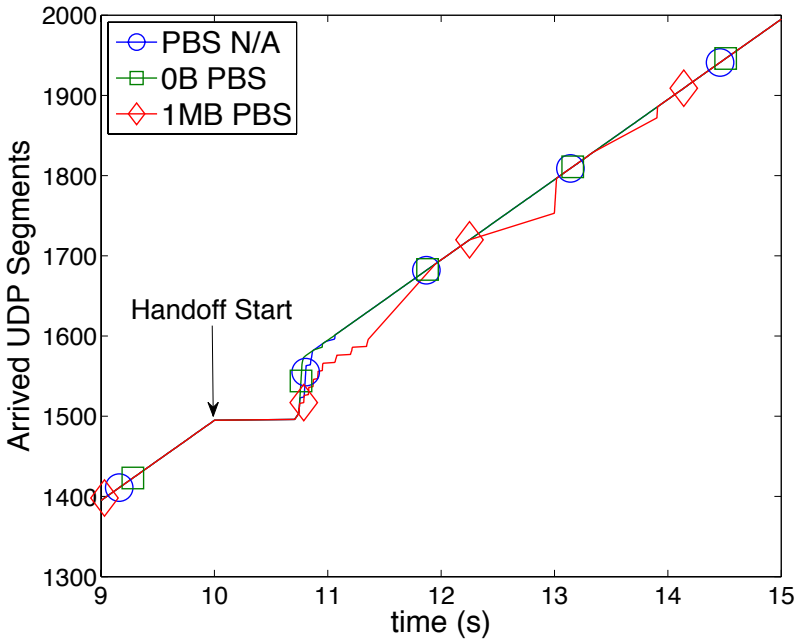


(b) 300ms handoff delay

Figure 5.13: Received Sequence Number evolution for a concurrent UDP application at handoff.

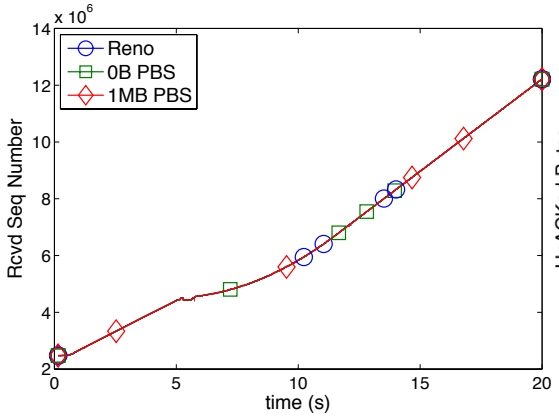


(c) 500ms handoff delay

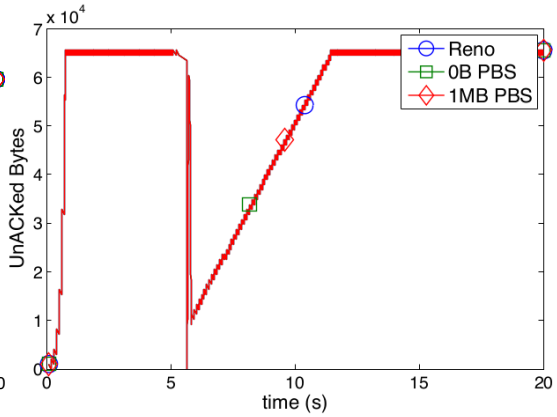


(d) 700ms handoff delay

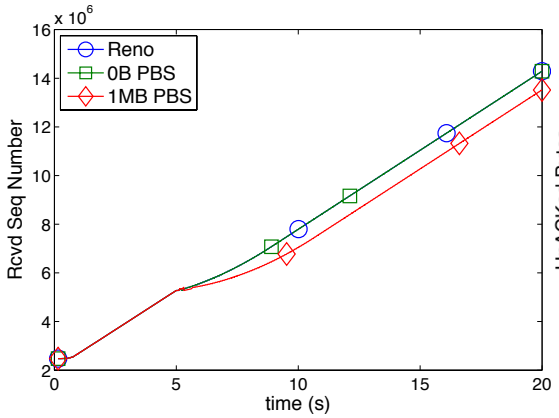
Figure 5.13: Received Sequence Number evolution for a concurrent UDP application at handoff.



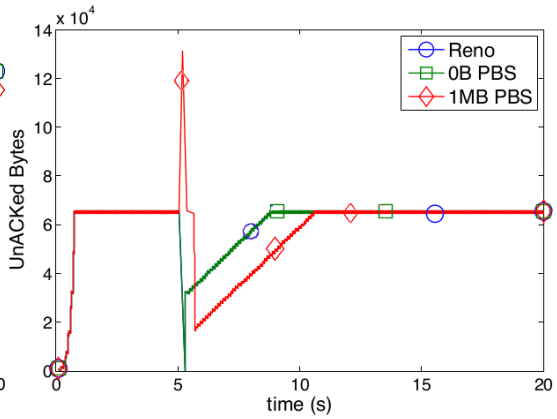
(a) Rcvd Seq Evolution at -50% Congestion



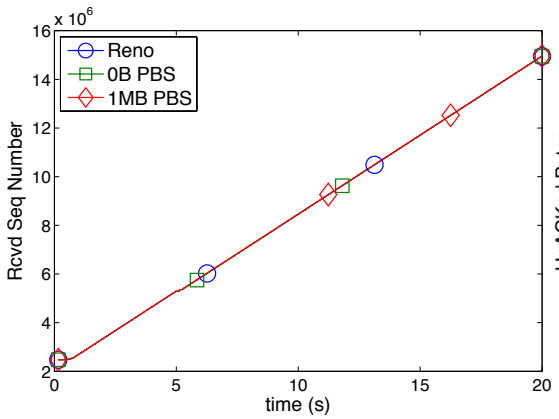
(b) Flightsize



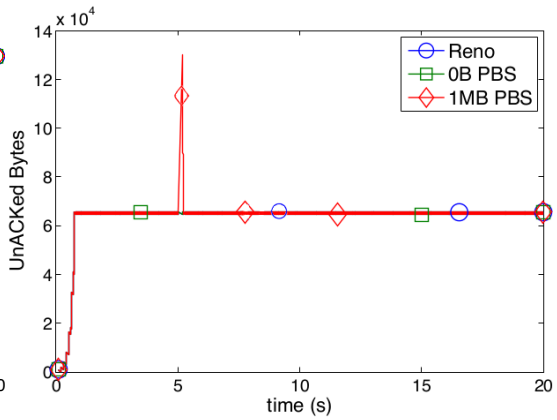
(c) Rcvd Seq Evolution at -25% Congestion



(d) Flightsize

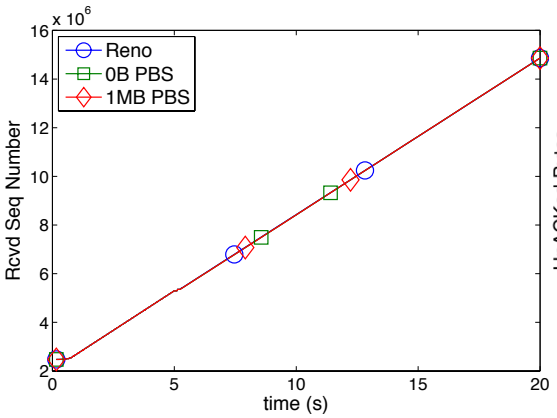


(e) Rcvd Seq Evolution at 0% Congestion

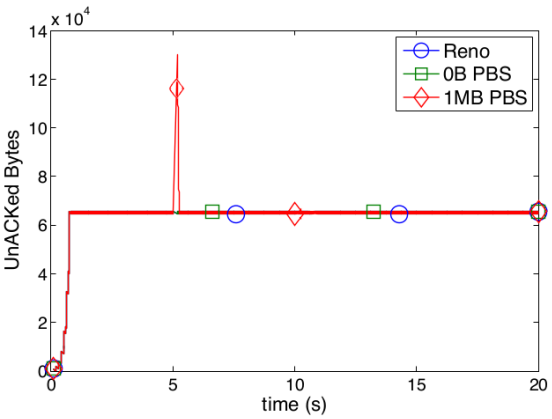


(f) Flightsize

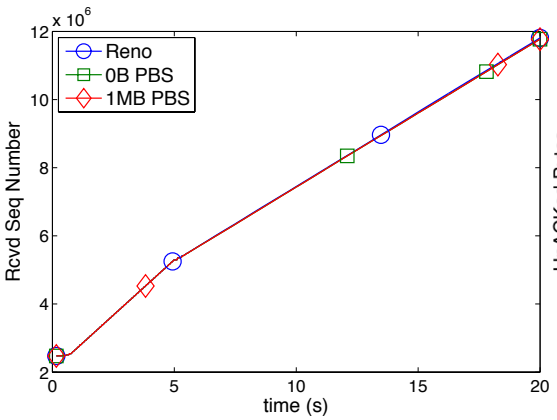
Figure 5.14: Received Sequence Number and In-flight Traffic Load Size for 100ms L2 handoff delay



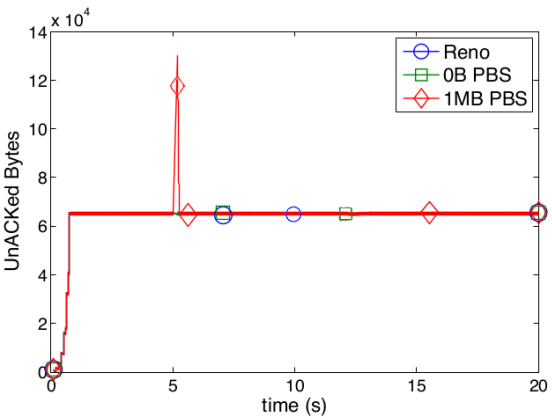
(g) Rcvd Seq Evolution at +25% Congestion



(h) Flightsize



(i) Rcvd Seq Evolution at +50% Congestion



(j) Flightsize

Figure 5.14: Received Sequence Number and In-flight Traffic Load Size for 100ms L2 handoff delay

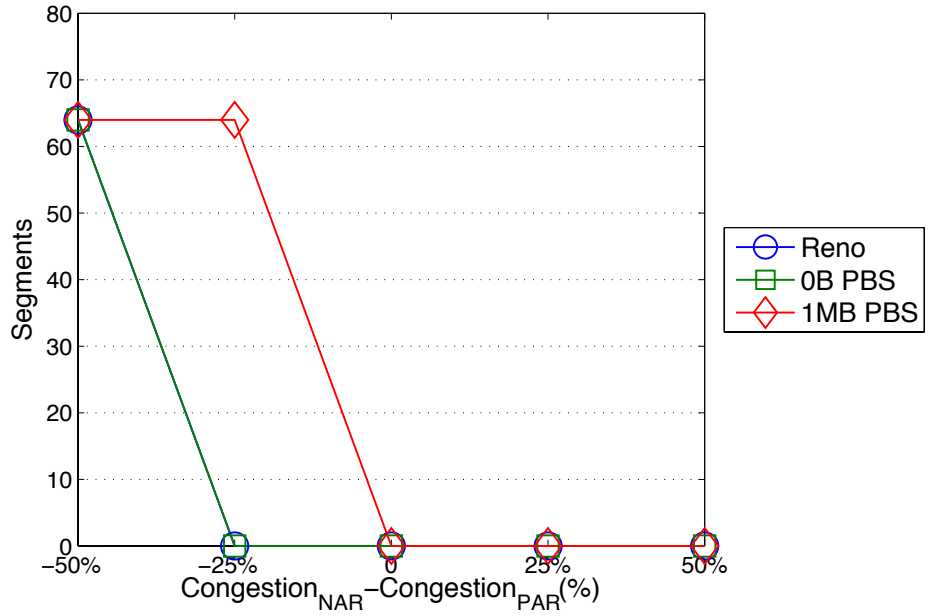
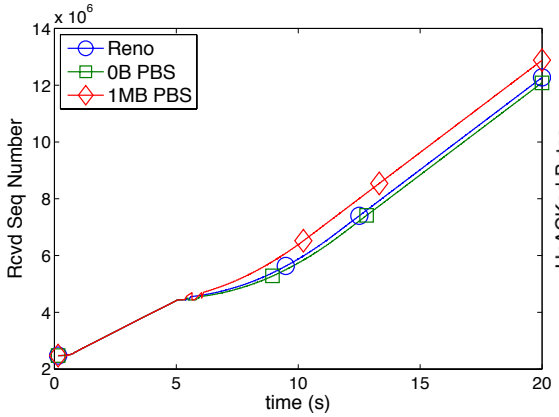
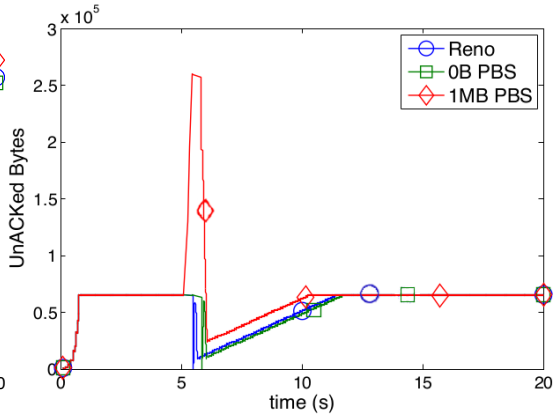


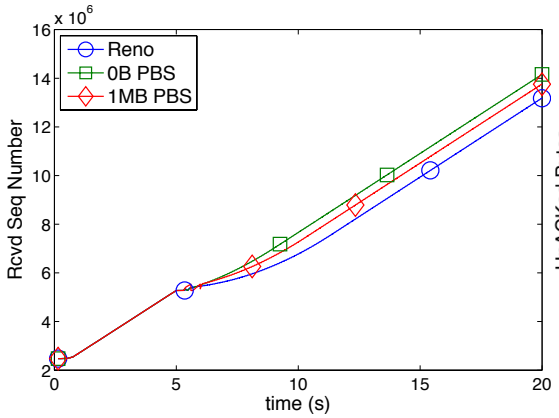
Figure 5.15: Number of Segments Dropped by the MN. 100ms handoff delay.



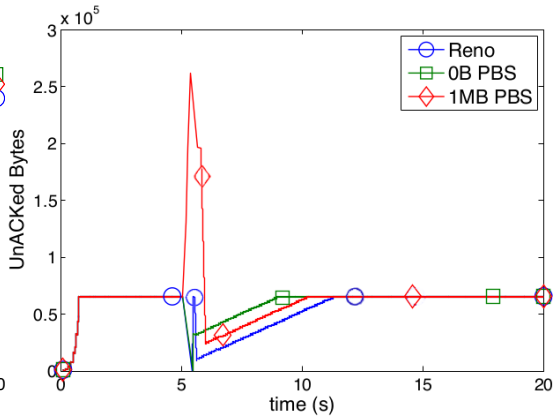
(a) Rcvd Seq Evolution at -50% Congestion



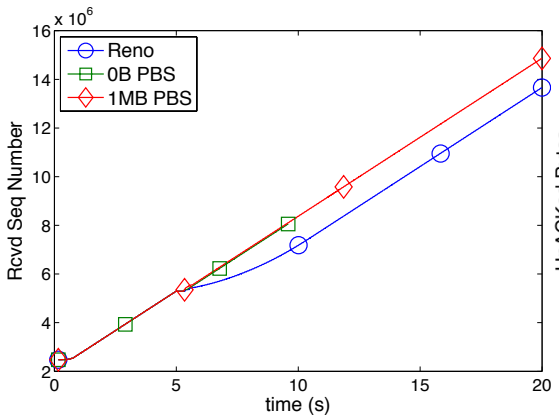
(b) Flightsize



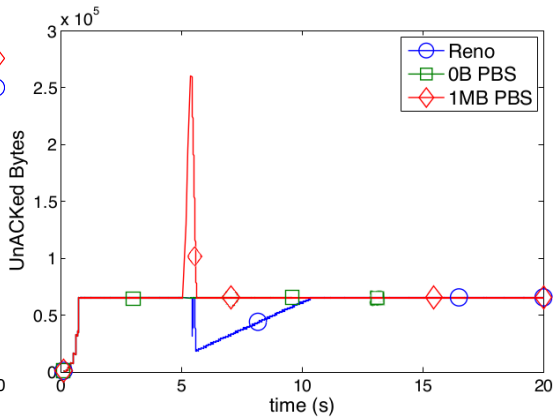
(c) Rcvd Seq Evolution at -25% Congestion



(d) Flightsize

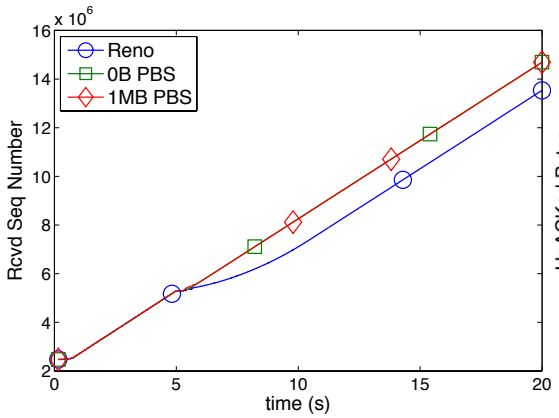


(e) Rcvd Seq Evolution at 0% Congestion

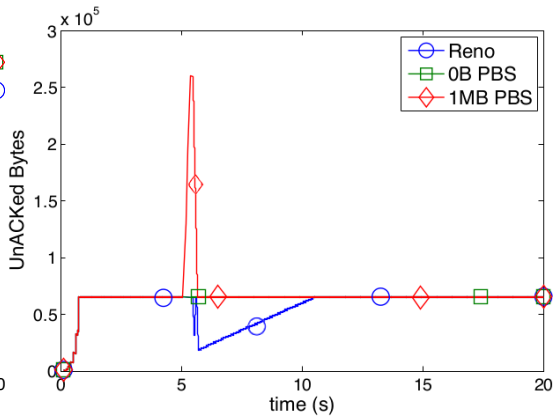


(f) Flightsize

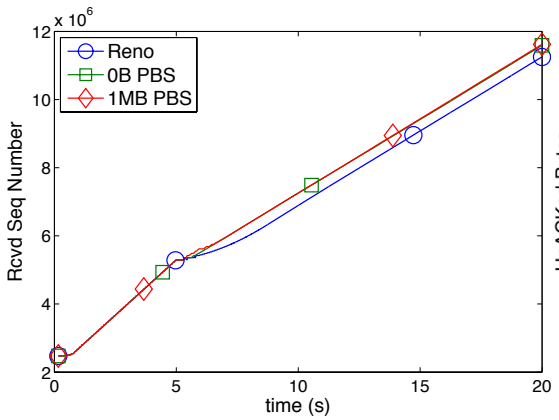
Figure 5.16: Received Sequence Number and In-flight Traffic Load Size for 300ms L2 handoff delay



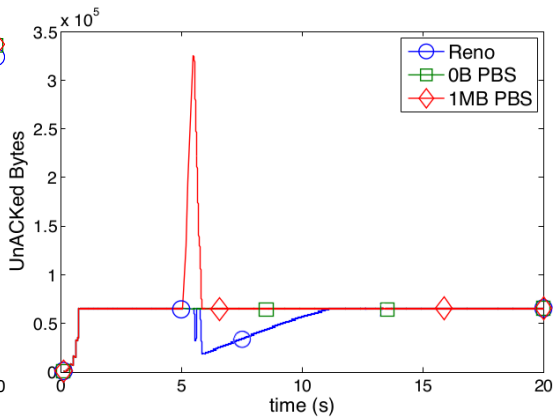
(g) Rcvd Seq Evolution at +25% Congestion



(h) Flightsize



(i) Rcvd Seq Evolution at +50% Congestion



(j) Flightsize

Figure 5.16: Received Sequence Number and In-flight Traffic Load Size for 300ms L2 handoff delay

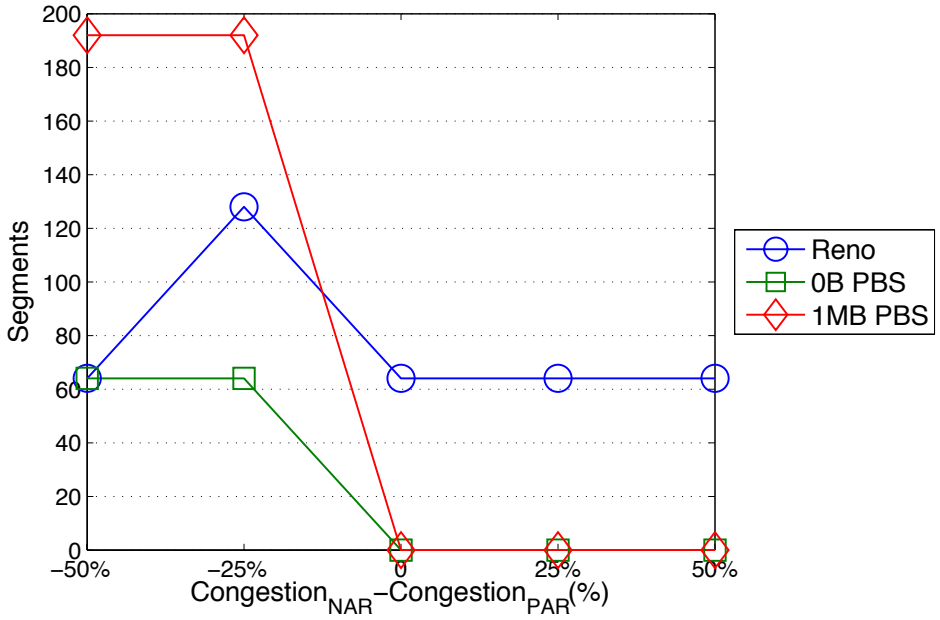
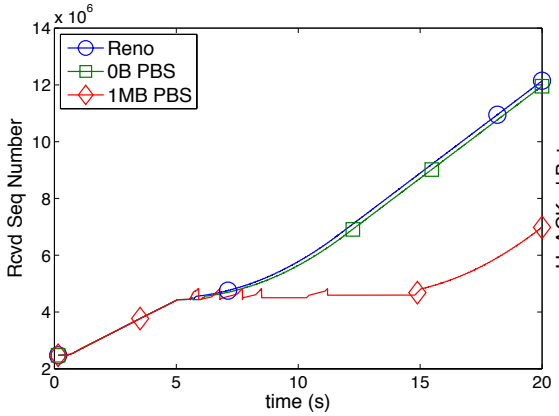
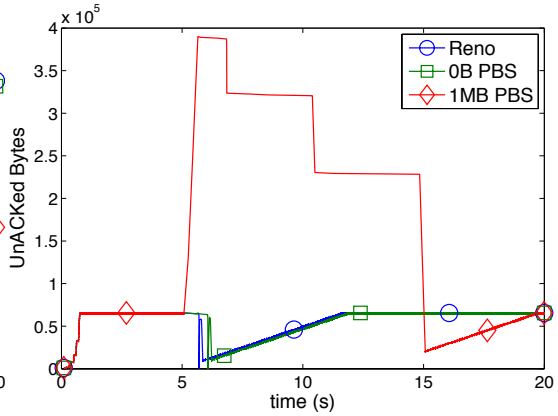


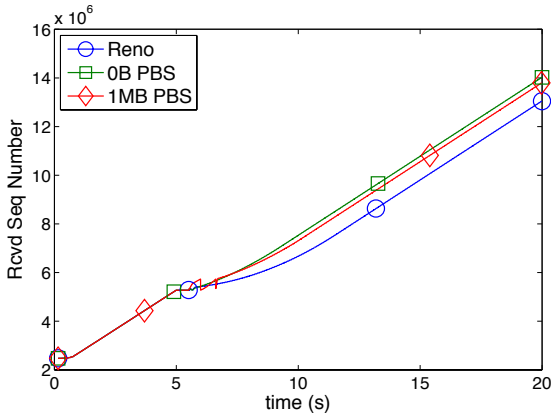
Figure 5.17: Number of Segments Dropped by the MN. 300ms handoff delay.



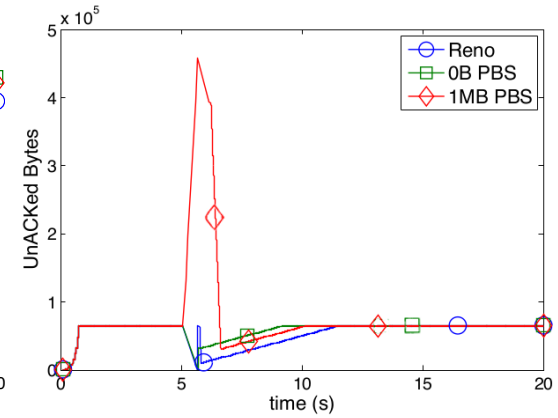
(a) Rcvd Seq Evolution at -50% Congestion



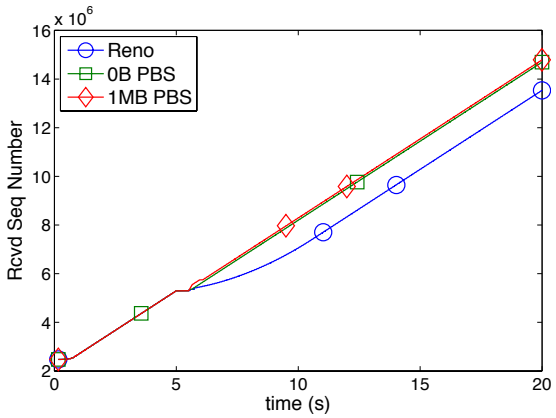
(b) Flightsize



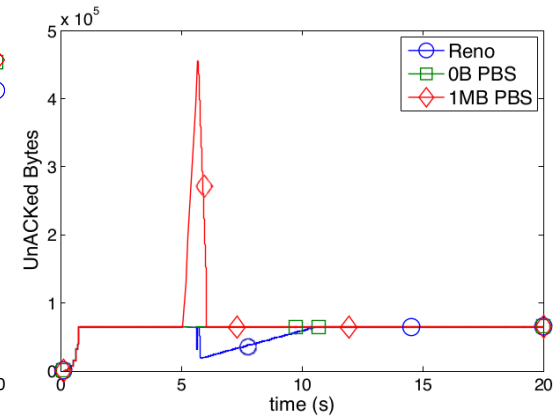
(c) Rcvd Seq Evolution at -25% Congestion



(d) Flightsize

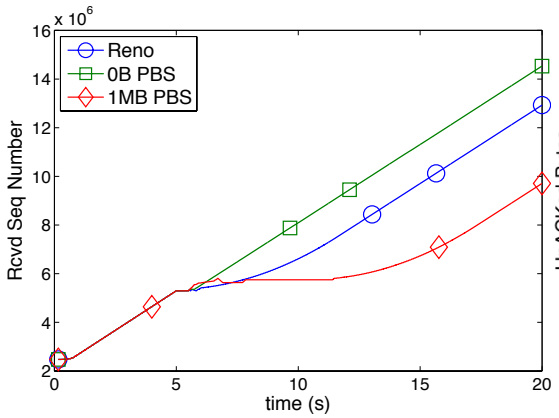


(e) Rcvd Seq Evolution at 0% Congestion

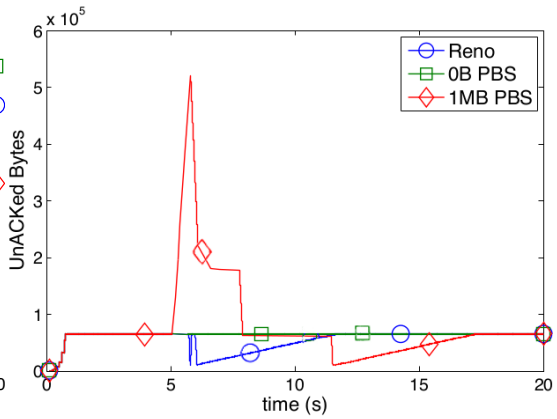


(f) Flightsize

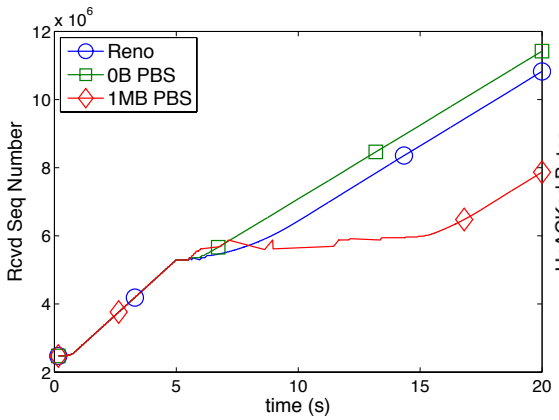
Figure 5.18: Received Sequence Number and In-flight Traffic Load Size for 500ms L2 handoff delay



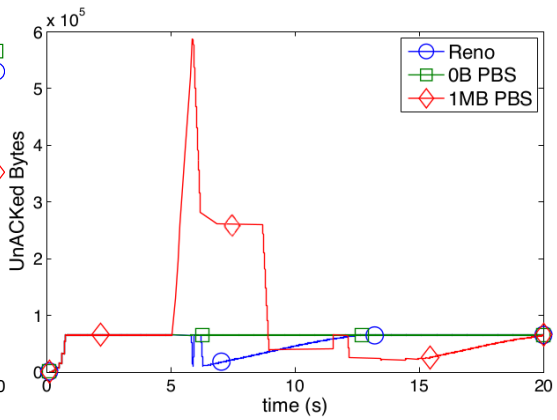
(g) Rcvd Seq Evolution at +25% Congestion



(h) Flightsize



(i) Rcvd Seq Evolution at +50% Congestion



(j) Flightsize

Figure 5.18: Received Sequence Number and In-flight Traffic Load Size for 500ms L2 handoff delay

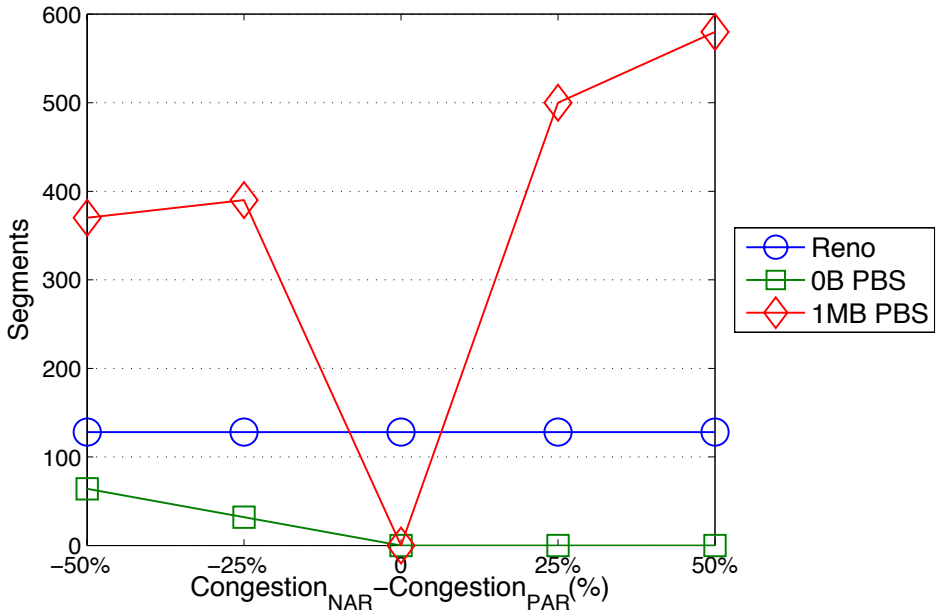
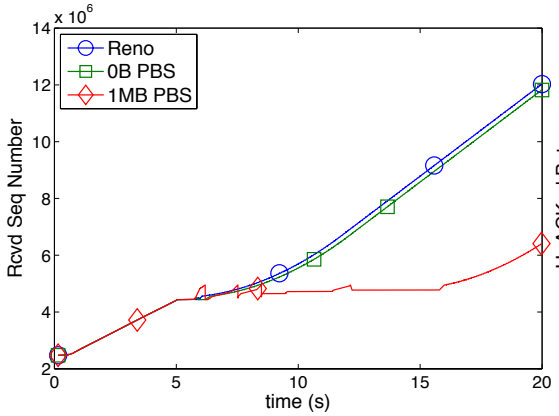
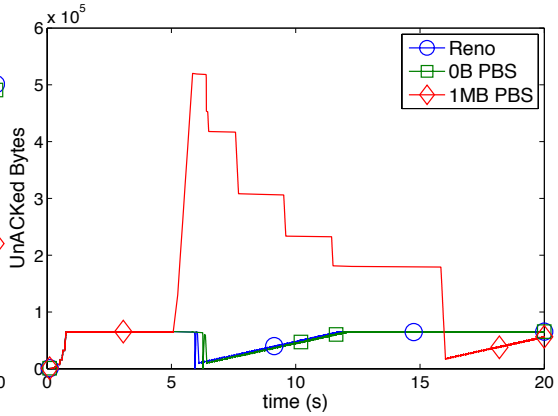


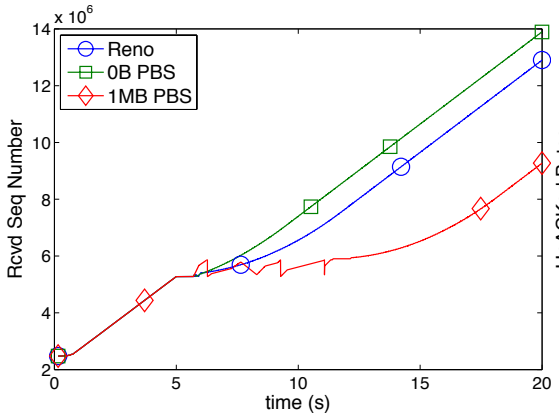
Figure 5.19: Number of Segments Dropped by the MN. 500ms handoff delay.



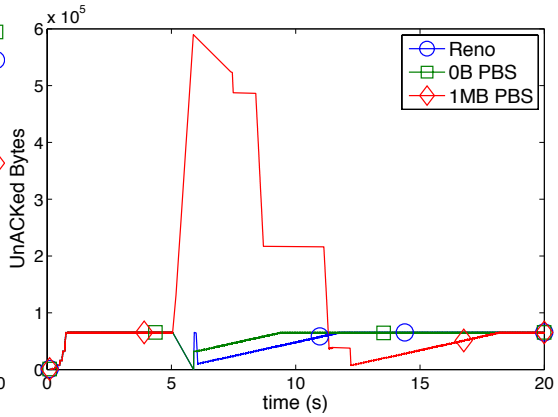
(a) Rcvd Seq Evolution at -50% Congestion



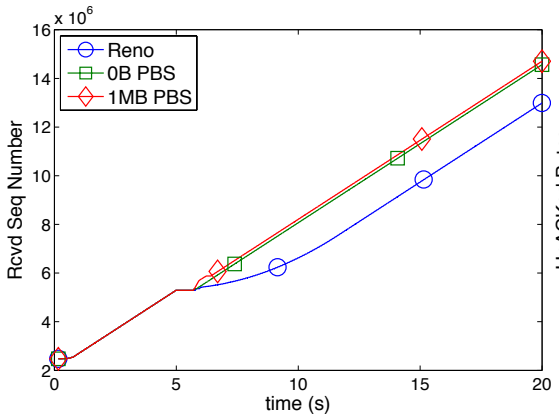
(b) Flightsize



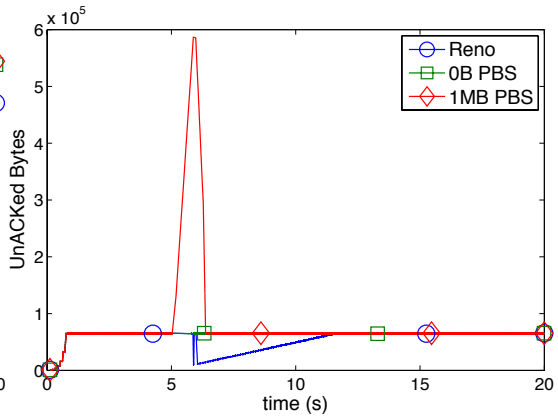
(c) Rcvd Seq Evolution at -25% Congestion



(d) Flightsize

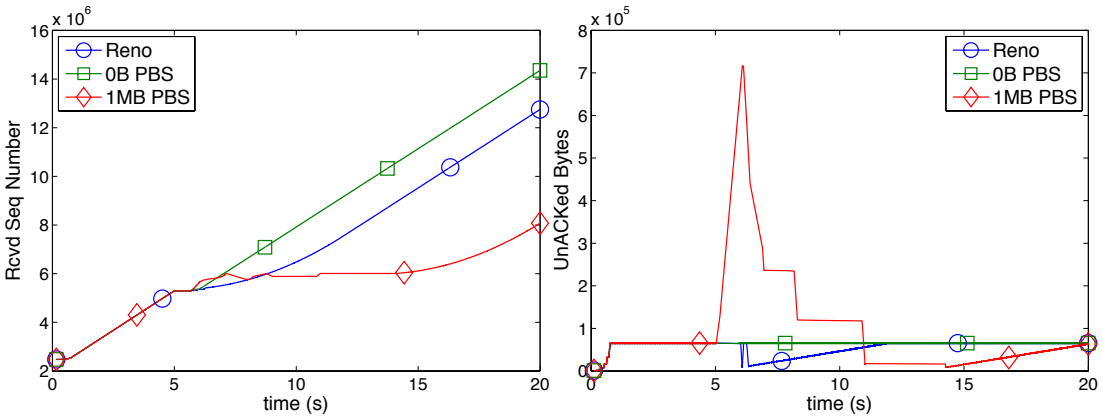


(e) Rcvd Seq Evolution at 0% Congestion

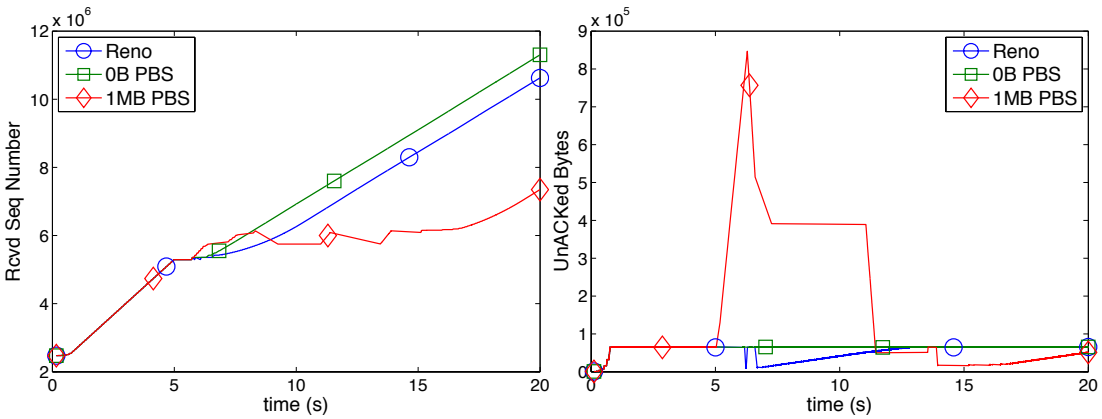


(f) Flightsize

Figure 5.20: Received Sequence Number and In-flight Traffic Load Size for 700ms L2 handoff delay



(g) Rcvd Seq Evolution at +25% Congestion (h) Flightsize



(i) Rcvd Seq Evolution at +50% Congestion (j) Flightsize

Figure 5.20: Received Sequence Number and In-flight Traffic Load Size for 700ms L2 handoff delay

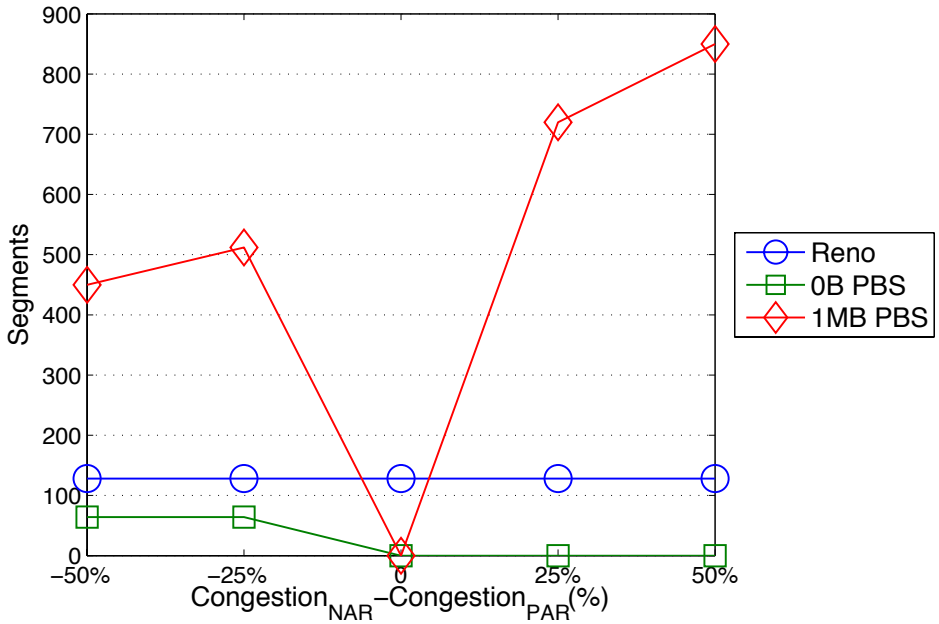


Figure 5.21: Number of Segments Dropped by the MN. 700ms handoff delay.

Chapter 6

An Intelligent Network Selection Algorithm

Chapter 4 introduced a scheme to reduce handoff signalling latencies. In turn, Chapter 5 presented a set of mechanisms to overcome the effect of these latencies on the higher-layer TCP-based protocols and applications. However, one of the most relevant questions in handoff remains: which network is the most desirable target for handoff? This is a nontrivial question involving a number of factors. For instance, a WiFi-UMTS enabled dual-cell phone user would benefit from diverting a web-browsing session from the UMTS interface to the more cost-efficient WiFi interface if there is an 802.11 AP nearby. Continuing with this example, the user may subsequently launch a VoIP application such as Skype [148]. At this point, the user may experience poor QoS in both the web-browsing and VoIP sessions due to the scarcity of 802.11 link resources. Since two networks are available to the user, he or she could use both interfaces simultaneously thereby aggregating available bandwidth. The open question for the user would now be: which is the optimum mapping of ongoing application flows to available channels? For instance, the UMTS link's lower jitter would probably be suited to the VoIP flow whereas the web-browsing bandwidth requirements could possibly be met by the 802.21 link.

These two questions present some technical issues. First, communication networks, and particularly wireless networks, are dynamic systems subject to sudden changes in SINR and latency. Therefore, network characterisation does not present an immediate solution. Second, evaluating the payoff of particular in-

stances of network resources allocation to the users' demands, where a variety of applications with different traffic dynamics compete for the medium, has met with limited success due to the complexity of mobility and traffic models. Third, additionally, solution models must take into account which are the autonomous decision-making entities in the network. Not only users but also network operators and service providers may act as autonomous agents, and they may have conflicting interests as on how the network resources are to be allocated.

This chapter focusses on the problem of network quality assessment and selection, and presents two neural network-based algorithms that can help in solving these two open issues with regards to optimum heterogeneous networks selection.

6.1 Introduction

The interworking of heterogeneous networking technologies to provide improved coverage and QoS differentiation has attracted some interest within the research community [149]. Within 3GPP, some work has focussed on the interworking between 3G and 2G and also Wireless LAN (WLAN) systems [150]. Within the IEEE, a L2 triggering mechanism for intersystem handoff, 802.21, is being developed, while within the IETF, extensions to the Internet Protocols have been proposed to support mobile devices [17, 18]; the L3 nature of these protocols makes them equally applicable to intersystem handoff. Furthermore, at L4, there are a number of contributions to improve the performance of TCP and the QoS perceived by either real or non-real time services for mobile devices [151].

In an ideal world, each service should be supported by the most appropriate RAT, taking into account the QoS requirements of the service and the characteristics of the underlying bearers; thus adhering to Ericsson's ABC paradigm [152]. Decisions are taken on the basis of expected benefit and Network Selection Algorithms' decisions are no exception. Classically, NSAs rely on the Received Signal Strength Indicator (RSSI) to identify the best network for service provision. Higher RSSI levels often yield on a lower Bit Error Rate (BER) and hence better Quality os Service (QoS). Moreover, the higher the RSSI, the closer the MN is to the AP in general (statistically), and therefore the lower the possibility of performing handoff in the short term. Thus, RSSI is an intuitively appropriate indicator of the benefit of connecting to any given link.

Common Radio Resource Management (CRRM) plays a major role on assessing each network's state and managing the resources in a unified manner across each of the heterogeneous technologies. This enables efficient service delivery to the end user for a range of disparate service types across a range of disparate technologies. Mapping services to technologies in a dynamic manner is the core of this chapter.

Much research in this domain has focussed on devices with multiple interfaces that select a RAT on a service per service basis. The underlying assumption in much of that research is that the terminal will be connected to any one of the many RATs at any particular time. Advances in L3 technologies within the IETF provide the potential to be simultaneously connected to more than one network. This approach, known as multihoming, has been the subject of research in a number of IETF working groups [153]. Multihoming can be regarded as a significant enabler for the ABC paradigm because it supports always-on connectivity to multiple networks and hence negating interruption of service due to L2 handoff. This thesis focusses on multihomed mobile hosts that are supporting multiple (dissimilar) services concurrently; the challenge is therefore mapping each of the individual services to one of the available RATs.

Network selection (performed at session set-up time) and network reselection (handoff) can be conducted in a network-centric or user-centric fashion. With the former, centralised or hierarchical distributed control can be exercised to optimise resource utilization across the interworked networks to the network operators' satisfaction. Network-centric approaches are limited to scenarios where a single operator owns and controls multiple RATs (3G, WLAN, etc.), or where business agreements exists between partner network operators. User-centric approaches are not bound by this constraint: indeed the competition between network operators could be exploited by users to increase competition in the marketplace and hence enable cost efficient connectivity.

In summary, this chapter focusses on a multihomed host performing user-centric network selection. Specifically, this thesis presents a novel multihomed user-centric approach to network selection based on Hopfield Neural Networks (MUC-HNN). HNNs are well suited to solving complex optimization problems within tight time frames in comparison with constrained optimization algorithms [154].

The rest of this chapter is structured as follows. Section 6.2 defines the problem. Section 6.4 formulates the problem from the definition of HNN. Section 6.5 illustrates a user case scenario for numerical evaluation of the MUC-HNN algorithm. The algorithm's performance is compared with other three allocation algorithms. Finally, conclusions are summarised in Section 6.7.

6.2 Problem Formulation

Network selection algorithms must dynamically manage the allocation and deallocation of traffic to the available networks. Their target is to optimise the allocation of the available networks resources according to the running applications demands so that every ongoing communication's QoS is maximised.

The algorithm should be triggered whenever: (a) a new session set-up request is made; (b) the user changes his/her preferences or requirements[1]; (c) the user's terminal detects a new network; (d) an ongoing service can no longer be supported by a particular radio link, e.g. due to signal degradation; (e) the current network initiates handoff to perform load balancing or due to operator-specific reasons.

Moreover, the mathematical models should overcome the problems of real-life scenarios. For instance, individual micro-flows generated by the same application must not be distributed across RATs because many applications utilise TCP which favours paths that are symmetrical, i.e. data and acknowledgements will traverse the same RAT. Likewise, the different latencies that are incurred across the different links would disrupt the communication timings in real time applications, largely based on UDP. Therefore, each application flow should only be allocated to a single interface. Also, the network selection algorithms should deal with an arbitrary number of interfaces and available networks since hosts may be provided with several air interfaces. This is also the case where the network selection and resource allocation is managed be the network operators.

Given that user traffic can be dimensioned then network selection can be reformulated as an optimisation problem. There are a plethora of constraint satisfaction algorithms which are candidates for use in network selection: this

[1]In the forthcoming discussion, the authors will differentiate between user preferences and user requirements. Preferential attributes are those to be maximised. Requirements are mandatory values for attributes.

thesis explores a user-centric Hopfield Neural Network (HNN)-based approach. HNNs can efficiently provide solutions for complex problems: they are more scalable than classical constraint satisfaction approaches, reducing both computation time (processing capability) and spatial complexity (memory required).

6.3 FFNN for Network Quality Assesment

An artificial neural network (or simply a neural network) is a biologically-inspired computational model which consists of a weighted interconnection of processing elements called *neurons* [154]. Additionally, a neural network is bound to a training algorithm and a recall mechanism. These two permit the network training, i.e. the interconnections' weights adaptation to desired behavioural specifics of the network. The following sections introduce the concept of neuron, and two network topologies relevant for this thesis work, namely, Multilayer Perceptron and Hopfield networks, and their corresponding training algorithms.

At this point in the discussion, before going deeper into the technical detail, it is convenient to say that neural networks have proved efficient at optimisation and decision making problems.

6.3.1 Artificial Neuron Model

Figure 6.1 illustrates the artificial neuron or Perceptron mathematical model. In general, the neuron model includes the following parameters:

- *Input connections*: $x_1, x_2, x_3, ..., x_n$. There are *weights* bound to the input connections: $w_1, w_2, w_3, ..., w_n$.
- *Transfer function*, calculates the aggregated *net input signal* to the neuron. The transfer function is usually the summation function $\Sigma_{i=1,n} x_i \cdot w_i$.
- An *activation function*. The most used functions are hard-limit threshold, linear threshold, sigmoid or Gaussian (bell-shaped) functions [154]. A single neuron output can be represented by a single value.

The output of neuron k for an input pattern p, can be represented mathematically as

$$y_k^p = \varphi(s_k^p), \tag{6.1}$$

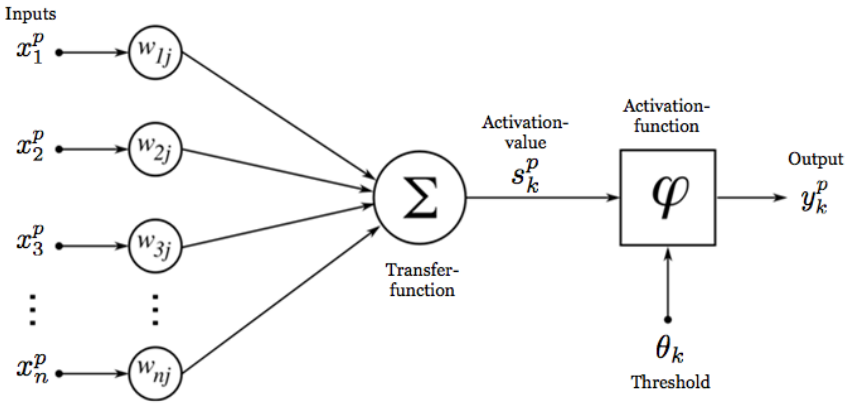


Figure 6.1: Neuron Activation Model

where the *activation value* is the weighted sum of the pattern values x and a bias value θ

$$s_k^p = \sum_j w_{jk} x_j^p + \theta_k, \tag{6.2}$$

and the *activation function* is often given by a sigmoid function like

$$\varphi(s_k^p) = \frac{1}{1 + e^{-s_k}} \tag{6.3}$$

6.3.2 Multilayer Perceptrons

A Multilayer Perceptron (MLP) is a neural network with two or more layers of neurons connected in cascade, with no connections within a layer (feed-forward architecture). Figure 6.2 illustrates a 4-input, 1-output MLP. They are generally composed of an input or hidden layer and an output layer, provided that the hidden layer neurons have nonlinear and differentiable activation functions. The nonlinear activation function in a hidden layer enable the MLP to behave as a universal approximator [155]. Thus, MLPs are suitable for nonlinear function characterisation and representation.

The MLPs were put into practice only when learning algorithms were developed for them. The first relevant contributions to learning algorithms for feed-forward architectures is the so-called *error backpropagation* algorithm [156, 157]. The central idea behind this algorithm is that the errors for the units of the hiden layer are determined by back propagating the errors of the units of the output

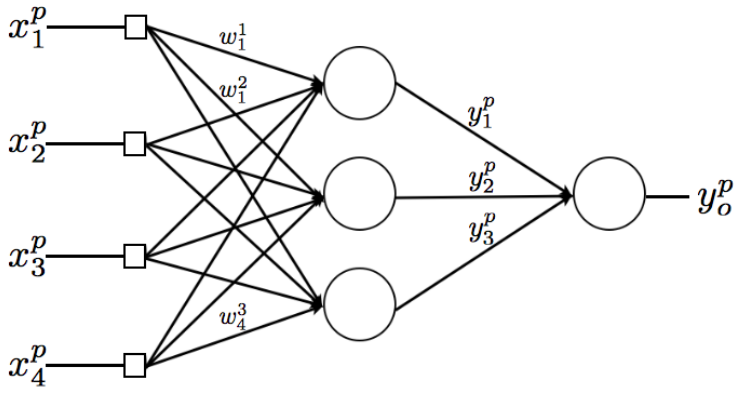


Figure 6.2: 4-input 1-out MLP network

layer. Backpropagation can also be considered as a generalisation of the delta rule for non-linear activation functions and multi-layer networks.

The output value of a perceptron k is given by

$$y_k^p = \varphi(s_k^p) \tag{6.4}$$

where the activation value is

$$s_k^p = \sum_j w_{jk} y_j^p + \theta_k \tag{6.5}$$

Using the delta rule, according to changes in the weights' values are proportional to the impact they have on the error:

$$\triangle_p w_{jk} = -\gamma \frac{\partial E^p}{\partial w_{jk}} \tag{6.6}$$

E^p is defined as the square error at the output, y_o^p for patter p with respect to the desired output, d_o^p:

$$E^p = \frac{1}{2} \sum_{o=1}^{N_o} (d_o^p - y_o^p)^2 \tag{6.7}$$

The forthcoming discussion illustrated the mathematical development of the aforementioned premises. Since

$$\frac{\partial E^p}{\partial w_{jk}} = \frac{\partial E^p}{\partial s_k^p} \frac{\partial s_k^p}{\partial w_{jk}}, \tag{6.8}$$

and by virtue of (6.2)

$$\frac{\partial s_k^p}{\partial w_{jk}} = y_j^p, \tag{6.9}$$

if

$$\delta_k^p = -\frac{\partial E^p}{\partial s_k^p} \tag{6.10}$$

is defined, then it can be shown that from 4.3 the delta rule can be extended to multi-layer networks. Thus, making changes on the network weights according to

$$\triangle_p w_{jk} = \gamma \delta_k^p y_j^p \tag{6.11}$$

will result in a gradient descent on the error surface. The problem now resides on computing the value for δ_k^p. Proceeding with the the chain rule of partial derivatives:

$$\delta_k^p = -\frac{\partial E^p}{\partial s_k^p} = -\frac{\partial E^p}{\partial y_k^p}\frac{\partial y_k^p}{\partial s_k^p} \tag{6.12}$$

From Equation 6.1

$$\frac{\partial y_k^p}{\partial s_k^p} = \varphi'(s_k^p) \tag{6.13}$$

which is the derivative of the activation function evaluated at the net input value s_k^p. Now, the value of $\frac{\partial E^p}{\partial y_k^p}$ is considered in two differ cases. Firstly, assuming $k = o$:

$$\frac{E^p}{y_o^p} = -(d_o^p - y_o^p) \tag{6.14}$$

Substituting this in 6.9 and 6.10:

$$\delta_o^p = (d_o^p - y_o^p)\varphi'(s_o^p). \tag{6.15}$$

This equation holds for any output unit o. Secondly, if k refers to an input unit $k = h$, E^p can be rewritten as a function of the contribution of the unit h.

$$\frac{\partial E^p}{\partial y_h^p} = \sum_{o=1}^{No} \frac{\partial E^p}{\partial s_o^p}\frac{\partial s_o^p}{\partial y_h^p} \tag{6.16}$$

As a result, the network's output constitutes a polynomial approximation to the desired output. This capability allows for modelling non-linear systems, such as the relation between TCP goodput or VoIP MOS and a variety of access

network parameters.

The TCP goodput and VoIP MOS values have been studied under a range of network conditions, shown in Table 6.1. The retrieved performance results have been used in conjunction with the network conditions to train two different MLP NNs. The first NN, NN_{TCP}, provides the estimated TCP goodput by taking into account network capacity, latency, jitter and BER. The second NN, NN_{VoIP}, provides the estimated MOS using the same four network parameters. The next section describes the production of training sets and the networks' training results.

6.3.3 Training for High-Level Performance Indication

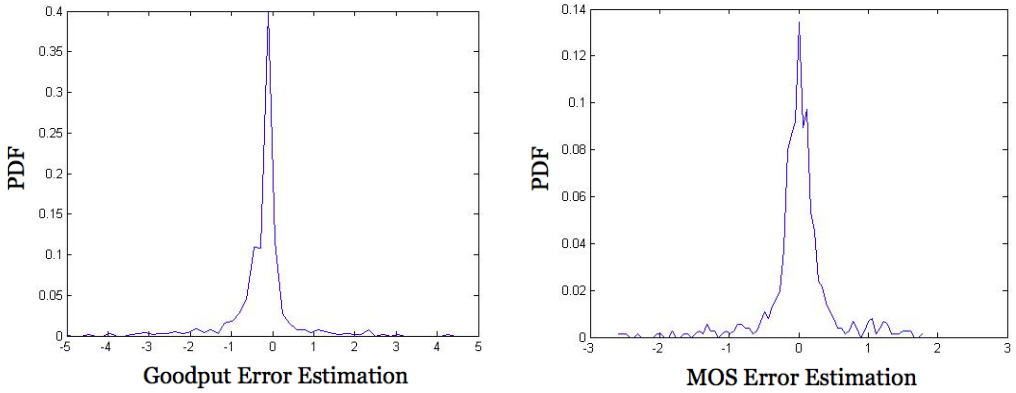
In order to train both $\mathrm{NN_{TCP}}$ and $\mathrm{NN_{VoIP}}$, two different training data sets have been produced using the computer simulation described in Section 6.5.1. The first training data set associates the network conditions to the TCP goodput, whereas the second one associates them to the MOS. This information is vital to the NN training and, the more information is gathered in a variety of circumstances, the better informed the NN is, and hence the better network selection will be [154]. The information is gathered at the NSA from different levels of the TCP/IP stack, since each level is assumed to be the best positioned to provide values for a specific attribute, e.g., the BER should be provided by the L2, while a high-level performance indicator such as the average TCP goodput may be provided by L4.

In general, the network attribute values such as jitter, latency and capacity can be produced by the TCP/IP stack's protocols in a variety of ways, by means of different schemes and mechanisms, or further enhancements. For instance, [81] proposes a method to estimate a WLAN link jitter via Bayesian estimation in conjunction with cumulative sum monitoring. Some of them may also be retrieved from other network entities, as in FMIPv6-enabled networks, where connection information and other link's information is handed to the MN on request [18, 158].

Alternatively, the explored NSAs use a cross-layer information exchange scheme to extract the necessary information from various layers in the stack. In this thesis, the use of the IEEE802.21 approach is proposed [9]. This scheme provides of the capability of sending information requests to, and receiving notifications from, any level of the TCP/IP stack.

Table 6.1: Attribute Ranges for the NN Training Purposes

Attribute	Min	Max
Return Latency (ms)	60	300
Jitter (ms)	12	60
BER (%)	10^{-6}	10^{-1}
Capacity (kB/s)	20	100



(a) PDF for Goodput Error Estimation (b) PDF for MOS Error Estimation

Figure 6.3: Training Error

More importantly, this scheme enables the online characterisation of the network performance, generating mappings with dynamic network conditions. This procedure has been replicated for a number of scenarios, while varying the network attributes capacity, latency, jitter and BER within the ranges established in Table 6.1. Thus, different network conditions have been associated with their respective VoIP MOS and TCP goodput equivalents. Two different FFNNs, NN_{TCP} and NN_{VoIP}, have been trained on the basis of the data sets. In this manner, the MN is capable of predicting at application level the benefits of choosing any specific network of the basis of the network attributes that it retrieves on real-time.

Figures 6.3a and 6.3b show the estimation error PDF for TCP goodput and VoIP MOS, respectively. As Fig. 6.3a illustrates,in most cases error is within ± 5 kB/s interval from the correct value, as retrieved from the simulation. Likewise, Fig. 6.3b shows that the MOS error is bounded within ± 0.4.

In view of the training errors, the FFNN-based network appropriateness evaluation stands as a promising tool for improved QoS in heterogeneous environments.

For each single application flow, a FFNN could be trained so that it copes with the application networking requirements so that the optimum network is selected on this basis. Additionally, either live or—where available depending on RRM entities on the network—proactive network quality evaluation would finally enable intelligent proactive handoffs.

This tool, however, does not apply effectively in more complex scenarios: e.g. the user running more than one application, multihomed scenarios or the effect of allocating more than one application to the user interface. All these scenarios require a more elaborated algorithm with cognitive capabilities beyond non-linear modelling. Section 6.4 describes an algorithm based on HNNs (explained in Section 6.4.1) that would provide networking-efficient solutions to these scenarios.

6.4 MUC-HNN Algorithm

6.4.1 Recurrent Networks: Hopfield

Recurrent networks have feedback connections from neurons in one layer to neurons in a previous later. Different modifications of such networks have been developed and explored. A typical recurrent network has concepts bound to the nodes whose output values feed back as inputs to the network. Thus, the next state of the network depends not only on the connection weights and the currently presented input signals but also on the previous states of the networks. The network leaves a trace of its behaviour; the network keeps a memory of its previous states.

Recurrent networks are more complex as a result of:

1. The synchronization required in order to achieve proper timing when propagating the signals through the network.

2. The inherent difficulty of expressing in a linguistic form (or formulae) the time dependence learned after training.

3. Recurrent networks may manifest chaotic behaviour, and therefore learning may be difficult.

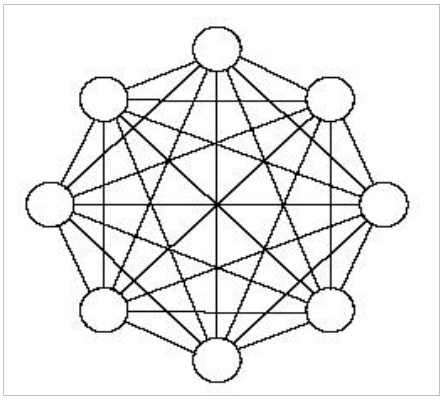


Figure 6.4: One-Dimensional Hopfield Neural Network Example

Recurrent networks suit time-series prediction problems, speech recognition problems, and many others, where in order to recognise the current state, previous states have to be considered. For example, in language and speech processing the semantic meaning of a word is recognised after considering the meaning of adjoining words.

Hopfield networks, named after their inventor John Hopfield (1982), are fully connected recurrent networks (Fig. 6.4). The neurons in Hopfield networks are characterised by the following: binary or unitary input signals, binary or unitary output signals, simple summation functions, and hard-limited threshold activation functions. Additionally, there are a number of contributions from the research community that allow for variants of realizations of the Hopfield network. Every neuron, $i, j = 1, 2, ..., n$ in the network is connected back to every other one, except itself. Input patterns x_j are supplied to the external inputs I_j and cause activation of the external outputs. The response of such a network, when an input vector is supplied during the recall procedure, is dynamic, that is, after supplying the new input patter, the network calculates the outputs and then feeds them back to the neurons; new output values are then calculated, and so on, until an equilibrium state is reached. An equilibrium state is considered to be the state of the system when the output signals do not change for two consecutive cycles, or change within a small constant. The weights in a Hopfield network are symmetrical for reasons of stability in reaching equilibrium, that is w_{ij}=$w_{ji} \forall i, j \in \{1, n\}$.

The Hopfield's equilibrium can also be understood from thermodynamics:

Hopfield networks have an associated energy, which is a dynamical parameter and which can be calculated at any instant t as explained later in Equation 6.17. The energy function represents a surface in a $n-$dimensional space. As the network iterates, it converges towards minimums or hollows of the energy function, which are equilibrium states. The existence of this equilibrium points is a consequence of the attractor principle. During training, the neuron's interconnecting weights are modified so that the network energy function presents some minimums at the corresponding training patterns. When a new a noisy pattern is presented to the network and the network is triggered to oscillate freely, it will eventually rest on the closest basin of attraction to the initial state, therefore associating the input pattern with one of the known patterns.

In the foregoing discussion, it has been shown how Hopfield networks are used for pattern recognition. Nonetheless, Hopfield networks can also be applied to optimization problems: Knowing that Hopfield networks iterate towards minimums of the energy function, the optimisation problem comes down to re-formulate the optimisation goal function as an energy function [154, 159].

Dynamics of the HNN

In an N-neuron HNN, the energy can be described as shown in (6.17).

$$E = -\frac{1}{2}\sum_{i=1}^{N}\sum_{j=1}^{N} V_i V_j \omega_{ij} - \sum_{i=1}^{N} V_i I_i \tag{6.17}$$

where V_i is the ith neuron output, I_i is the bias vector and ω_{ij} is the associated weight to the $i-j$ neurons interconnection.

The neuron activation function is calculated accordingly in (6.18).

$$V = \frac{1}{2}\left(1 + \tanh\frac{U}{U_0}\right) \tag{6.18}$$

where U is the neuron input signal, V is the output signal and U_0 is a constant.

For the network to converge, the activation values are updated using the Euler method:

$$U_i^{t+\Delta t} = U_i^t + \Delta t\left(\sum_{j=1}^{N} V_j \omega_{ij} + I_i - \frac{U_i}{\tau}\right) \tag{6.19}$$

where τ is the time constant of the network, Δt is the time step and U_i^t is the input of neuron i at time instant t.

The energy function of a HNN has various minima (basins of attraction) that represent (sub-optimal) solutions. An unknown input pattern represents a particular point in the energy landscape. As the network iterates in its way to a solution, the point moves through the landscape towards one of the hollows, i.e. to local solutions [160]. By defining a globally monotonic $n-$dimensional energy function on the basis of n network attributes' criteria then optimum network resource allocations can be obtained.

6.4.2 Problem Formulation

Communication network selection is defined as an optimisation problem. The HNN will iteratively converge to a solution where the cost associated with mapping a particular service to a particular RAT is minimised. For this purpose, the following cost function (6.20) has been derived.

The network selection problem has been formulated using a 2-D HNN. The network has $N_{net} \times N_{tt}$ neurons, where N_{net} is the number of available networks and N_{tt} is the number of types of traffic that the application level is generating. A neuron $V_{n,t}$ will be activated when traffic t is allocated to network n.

The proposed energy (cost) function, inspired by Calabuig [86], consists of six terms. The first term forces the neurons to have a '0' or '1' output signal, or to be near these values. The second term guarantees that the same traffic type is not shared among several radios or networks. The third term ensures that only one network is chosen from a particular type: e.g., a mobile device equipped with only one WLAN interface can only connect to one WLAN network simultaneously. The fourth term is intended to enhance the user's network selection. The fifth term precludes the user from demanding more than the maximum available bandwidth in each system. Finally, the sixth term maximises the traffic allocation and hence the total resource utilization. Thus,

$$
\begin{aligned}
E =& \frac{A}{2} \sum_{n=1}^{N_{net}} \sum_{t=1}^{N_{tt}} V_{n,t} \left(1 - V_{n,t}\right) + \frac{B}{2} \sum_{t=1}^{N_{tt}} \left(\sum_{n=1}^{N_{net}} V_{n,t} - 1 \right) \\
&+ \frac{C}{2} \sum_{n=1}^{N_{net}} \sum_{\substack{n'=1 \\ n' \neq n}}^{N_{net}} \eta_{n,n'} \left(\sum_{t=1}^{N_{tt}} V_{n,t} \right) \left(\sum_{t=1}^{N_{tt}} V_{n',t} \right) \\
&+ \frac{D}{2} \sum_{n=1}^{N_{net}} \sum_{t=1}^{N_{tt}} V_{n,t} f^u_{n,t} + \frac{E}{2} \sum_{n=1}^{N_{net}} \sum_{t=1}^{N_{tt}} V_{n,t} \xi_{n,t} \\
&+ \frac{F}{2} \sum_{n=1}^{N_{net}} \sum_{t=1}^{N_{tt}} V_{n,t} \frac{f_{n,t}}{f_{min,t}}
\end{aligned}
\tag{6.20}
$$

, where

$$
\eta_{n,n'} = \begin{cases} 1 & \text{if } n \text{ and } n' \text{ same RAT,} \\ 0 & \text{otherwise.} \end{cases}
$$

, and

$$
\xi_{n,t} = u \left(\frac{B_a}{B_n} - 1 \right) \tag{6.21}
$$

being

$$
B_a = B_t + \sum_{n=1}^{N_{net}} \sum_{\substack{t=1 \\ t \neq t'}}^{N_{tt}} V_{n,t} B_t \tag{6.22}
$$

where B_t refers to the bandwidth required for traffic t, B_n to the available bandwidth at network n, $f_{n,t}$ to the cost associated to selecting network n for traffic t and $f^u_{n,t}$ represents the cost from the user's perspective, as explained in the next section. Thus, by comparison with (6.17) and (6.20) the parameters ω and I are

$$
\omega_{n,t,n',t'} = A \delta_{n,n'} \delta_{t,t'} - B \delta_{t,t'} - C \left(1 - \delta_{n,n'}\right) \eta_{n,n'} \tag{6.23a}
$$

$$
I_{n,t} = -\frac{A}{2} + B - \frac{D}{2} f^u_{n,t} - \frac{E}{2} \xi_{n,t} \tag{6.23b}
$$

The HNN will tend to stabilise at the state that entails a minimum energy, i.e., the best network according to the user's perspective cost function $f^u_{n,t}$. However, the definition of this function is nontrivial: this function merges the network attributes and the user requirements and preferences.

6.4.3 Cost Function Definition

In keeping with a comprehensive characterisation of the available networks appropriateness, the FFNN presented in Section 6.3 may be used. However, in order to compare the MUC-HNN approach with other current solutions fairly and on contestable terms, the original FFNNs benefit models will be reduced to the bandwidth characterisation of the applications QoS demands as follows. The cost associated to selecting network n for traffic t is usually computed as:

$$f_{n,t} = \frac{B_t}{B_n} \tag{6.24}$$

Thus, the network resources are allocated proportionally to the traffic demands. However, this effect is subordinated to the perceived benefit from the ongoing applications.

In this work, a novel user's perspective cost function, $f^u_{n,t}$, is proposed. The cost value decreases as the network exceeds the user's QoS requirements (in terms of available bandwidth), while any network failure to fulfil the user's requirements is highly penalised. Therefore, the term that refers to the user's perspective of costs (fourth term) of (6.20) will have a minimum value when only those networks that have the lowest cost values are activated.

For real-time (RT) services, the associated cost of allocating traffic to networks with available capacity higher than that required is zero since packet dropping as result of congestion does not occur. For non-RT services, the function definition assumes a best effort cost characterization: The cost increases exponentially until it reaches a saturation level. The scale parameter of the cost functions has been arbitrarily set by considering the same perceived cost at 50% of the user requirements ($\frac{B_t}{B_n} = 2$).

$$f^{NRT}_{n,t} = 1 - e^{-0.49\frac{B_t}{B_n}} \tag{6.25a}$$

$$f^{RT}_{n,t} = 1.25\frac{B_t - B_n}{B_t} u\left(\frac{B_t}{B_n} - 1\right) \tag{6.25b}$$

Fig. 6.5 shows the cost characterization for both types of traffic. Thus, the allocation costs at the application level are a direct consequence of the available

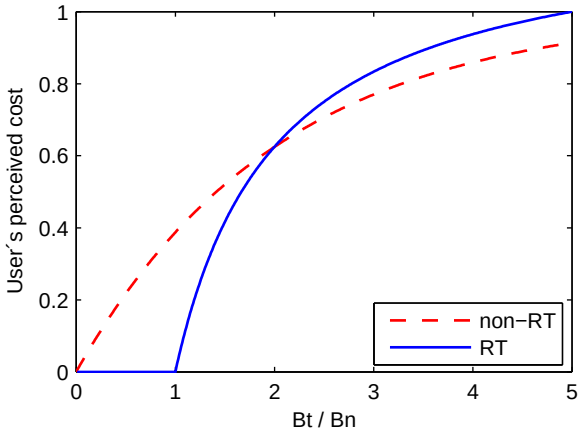


Figure 6.5: Costs associated with RT and non-RT traffic

bandwidth for each traffic taking into account of the application demands, and the consistency of the application performance when resources are scarce.

6.5 Numerical Evaluation

Two differentiated experiments have been carried out to validate the proposed NN-based schemes. Firstly, the performance of the FFNN Network Quality Assessment will be evaluated for for TCP-based flows and for a G.726 VoIP flow. Secondly, the network quality and complex network selection approaches will be combined in the MUC-HNN solution.

6.5.1 Simulation Scenario

Simulations have been conducted to measure the impact of the link's capacity, latency, jitter and BER on the TCP goodput and on the VoIP MOS in IEEE802.11g networks. The system model depicted in Fig. 6.6 was set-up using OMNeT++ and the INET framework. This framework provides a comprehensive model of TCP [45], IPv6 and IEEE802.11x networks. Secondly, the Bohge and Renwaz G.726 VoIP generator and sink [109, 110] have been included in the simulated network entities. Finally, the ITU-T P.862 PESQ MOS Evaluation Tool [70] has been incorporated.

The network is composed by five participating nodes, and the links interconnecting them are configured with a packet latency and throughput values

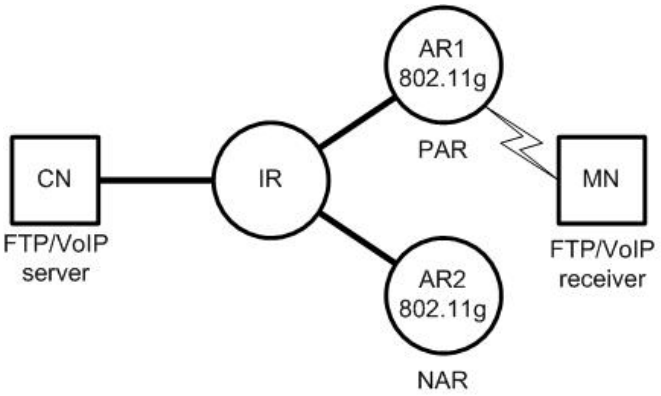


Figure 6.6: Simulated System Model

consistent with the anticipated latencies in a real system between the two VoIP ends, MN and the CN, and two arbitrary Access Points. The wired links are Gigabit Ethernet type. Link delays follow a Gamma distribution; the Gamma distribution is useful to represent a sequence of links with Poissonian delays. The wireless link is 54 Mbps IEEE802.11g.

Two different scenarios have been considered, depending on whether the user is running a TCP-based (FTP service) or VoIP-based application. The NN-based NSA, shown in Section 6.5.2, remains the same in its structure, but the evaluating NN changes accordingly. As previously explained, both developed MLP networks have four inputs (bandwidth, jitter, latency and BER) and one output. However, whereas $\mathrm{NN}_{\mathrm{VoIP}}$ provides the expected MOS, and thus is to be used in the VoIP scenarios, $\mathrm{NN}_{\mathrm{TCP}}$ provides the expected goodput, and therefore is to be used in the FTP scenarios.

6.5.2 FFNN-based Simple NSA

The proposed FF NNs have been implemented to evaluate their utility to network selection. Defining NN as the trained FF NN (either $\mathrm{NN}_{\mathrm{TCP}}$ or $\mathrm{NN}_{\mathrm{VoIP}}$), and $\vec{net}$ as the set of network parameters, a simple NSA could be described as follows.

Moreover, the proposed NN-based NSA proposed in this paper is compared with two other algorithms:

1. RSSI-based: The MN picks up the network with the highest associated RSSI value.

Algorithm 1 NN-based NSA

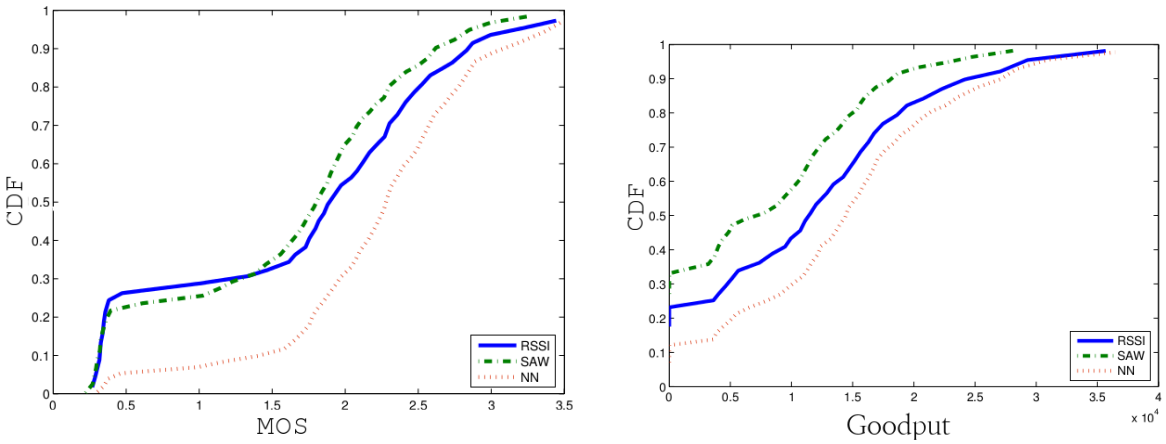
```
if available_networks == 0 then
  return 0;
else
  n = 1;
  for i = 1 to available_networks do
    if NN(net_i) > NN(net_n) then
      n = i;
    end if
  end for
  return n;
end if
```

2. Simple Additive Weighting (SAW): A network's score is produced by adding weighted contributions for each attribute of the network (for simplicity, unitary weights have been considered). The MN picks up the network with the highest score.

Performance Evaluation of the NN-Based NSA

Fig. 6.7a depicts the MOS CDF while varying the following network parameters: capacity, latency, jitter and BER. Both RSSI- and SAW-based approaches to network selection have a similar impact on the user's MOS. In turn, the NN approach, since it offers a better evaluation of the network quality, it incurs in better MOS. Moreover, while RSSI and SAW result, respectively, in 55% and 70% probability of having a MOS lower than two (which is the lower bound for reasonable quality of conversation), NN results in 35% probability.

Fig. 6.7b illustrates the goodput CDF for an FTP bulk transfer. Again, it is evident that the NN improves the user's QoE in comparison to both RSSI and SAW approaches: e.g., users have less than 20kB/s goodput with 42%, 70% and 74% probability, respectively. In general, users enjoy a higher goodput in almost every single case of the considered set of network conditions in comparison to both RSSI- and SAW-based approaches.



(a) MOS (b) Goodput

Figure 6.7: VoIP MOS and TCP Goodput CDF

6.5.3 MUC-HNN NSA

A network simulation has been implemented to conduct numerical evaluation of the MUC-HNN solution. In this model, a multihomed device is provided with three interfaces (UMTS, IEEE 802.11b and Ethernet) that can connect to three access points (and hence RATs) simultaneously. The assumed available bandwidth at the UMTS link is 60 kb/s [161]. For the other two links, a maximum capacity of 2 Mb/s and 10 Mb/s respectively is assumed, while a congestion level is uniformly distributed between 0% and 80%. The device supports three concurrent sessions: VoIP, video streaming and file transfer. All three services have the same preference level. The algorithm is able to allocate zero or more services to an interface.

The traffic models for the VoIP and video streaming have been extracted from [59, 60] respectively: the terminal is assumed to generate a constant bit rate of 64 kb/s for the former, and 5 Mb/s (download) for the latter. FTP file download traffic runs over TCP Reno.

The parameters of the proposed HNN have been calculated and are shown in

the Appendix C:

$$A = 10 \qquad B = 20000 \qquad C = 20000$$
$$D = 1000 \qquad E = 15000 \qquad F = 500$$
$$\tau = 1 \qquad U_0 = 0.1 \qquad \Delta t = 10^{-4}$$

To evaluate MUC-HNN's performance, it is compared with two other algorithms, following the same approach as taken by Calabuig [86]. These other two algorithms are:

1. Round Robin (RR): This technique allocates the resources from the available networks to each traffic cyclically. The maximum available bandwidth is allocated for each type of traffic, permitting no traffic sharing between two or more interfaces.

2. Optimum Bit Rate (OBR): This technique allocates to each type of traffic the network whose available bandwidth is the lowest, above the traffic bandwidth requirements.

Performance Evaluation of the MUC-HNN NSA

From the bandwidth allocated to each type of traffic, the following QoS metrics have been calculated: VoIP packet dropping probability; video stream buffering time (as a percentage over the visualization time); and FTP service latency (for a 1MB file download). Results are based on an average outcome after 1000 simulation runs.

Figure 6.8 illustrates the cumulative distribution function (CDF) of the packet dropping probability for the VoIP traffic. MUC-HNN offers a 0% blocking probability in any scenario, while OBR achieves it in 90% of the cases and RR only in 25%.

Figures 6.9 and 6.10 show the CDF of the percentage of video stream buffering time and the 1MB-file download latency respectively. The proposed algorithm achieves better performance overall. It is noted, however, that in approximately 7% of the user case scenarios its video stream performance is slightly lower than the RR and OBR allocation. This is a consequence of the algorithm enhanced allocation of resources to both the VoIP and the FTP traffic. MUC-HNN reduces

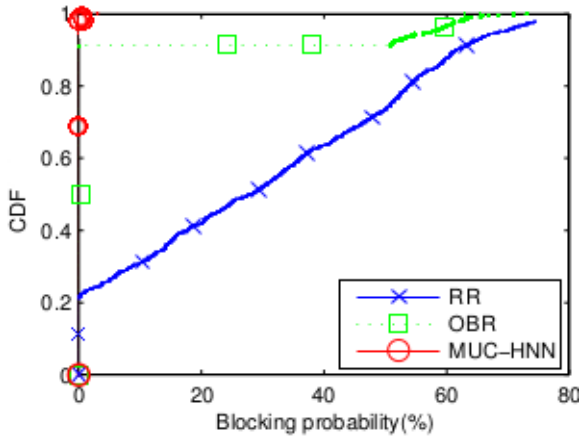


Figure 6.8: CDF for packet dropping probability of the VoIP service

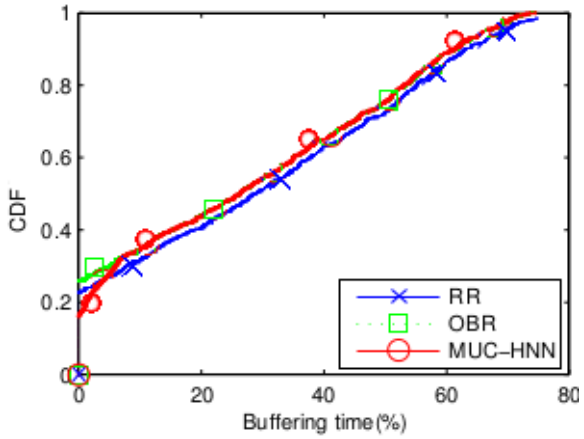


Figure 6.9: CDF for percentage of buffering time over visualization time (video stream service

FTP service latency by 50% in 25% of the cases considered in comparison with RR and OBR algorithms. In the remaining cases, MUC-HNN also attains better performance (approximately 20% latency reduction).

6.5.4 Computational Load

HNNs have been extensively used for pattern recognition and constrained optimization problems [162, 163] and have been successful on problem benchmarks such as the Traveling Salesman Problem, Economic Dispatch, N-Queens and Optimal Edge Selection [164], enabling more extensive variable sets while reducing the computation time. HNNs can also be implemented using analog or optical

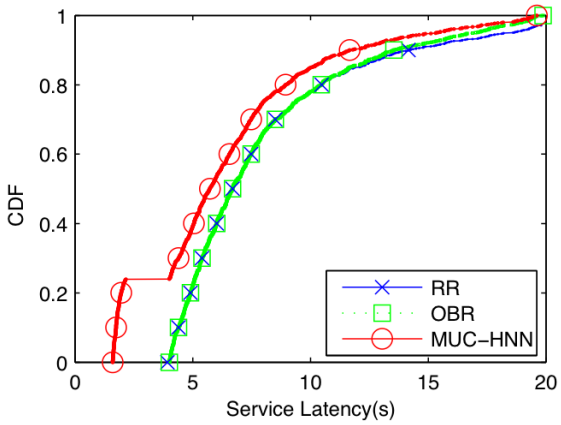


Figure 6.10: CDF for 1 MB file download latency (FTP service)

devices, fostering their computational capabilities.

The activation values of the network neurons and the neuron interconnecting weights define the energy of the network, so-called the Lupanov function. Since all neurons are interconnected, a state flap in one of them can result in other neuron(s) state changes, therefore neurons can update their activation values asynchronously and independently from other neurons. As the network neurons iterate, the Lupanov function converges towards minimums of the energy landscape. This convergence time ultimately defines the performance of the HNN.

Serpen and Parvin [165] and Goya et al. [166] present empirical evaluations of the performance of binary HNNs for graph search problems, such as TSP-like NP-hard constrained optimization problems. Results point to solution stability as the bounding factor for HNNs performance, i.e. rather than number of variables, it's the meta-stability of the HNN that characterises how likely a solution may be. In order to help HNNs converge faster to the basins of attractions—local minima in the energy function—the Lupanov function must be carefully implemented.

The MUC-HNN algorithm proposed in this thesis has been designed with a strong focus on the solution stability and the converge latency. In order to do so, the Lupanov weights have been set according to Appendix C. Next, the Round Robin, OBR and the proposed MUC-HNN algorithms latencies have compared in their MATLAB implementation. The evaluation has considered a trained MUC-HNN. The software run on a Pentium IV 2GHz, 1 GB RAM hardware platform. Ten scenarios have been considered, while varying the network attributes. Figure 6.11 shows that, on average, the MUC-HNN approach is three times slower

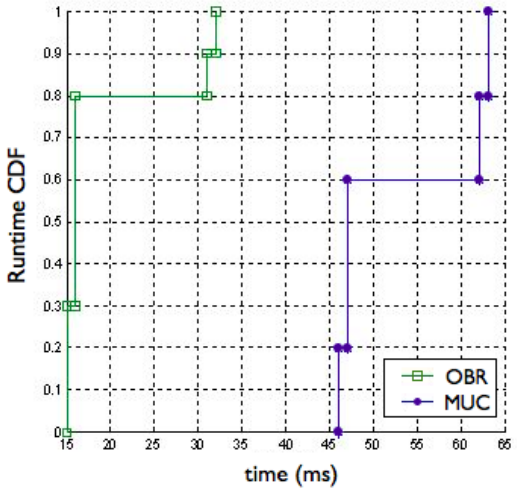


Figure 6.11: CDF for algorithm runtime

(approximately 45ms latency) than OBR (15 ms). Even quicker convergence is expected from Round Robin algorithm due to its $O(1)$ time complexity, in comparison to OBR's $O(n^2)$.

6.5.5 Qualitative Analysis of Other Solutions

In contrast with a per-data stream allocation to the available network channels, Horde and Calabuig approaches permit per-packet interface allocation. This presents the following two advantages: (i) per-packet striping involves dynamic network monitoring systems, therefore providing high adaptivity to varying conditions; and (ii) in-stream QoS evaluation permits differentiated treatment of the packets, e.g. sending the packets which need to be more reliably transmitted (such as the reference I-frames in an encoded video stream) thought the most reliable network channel out the available ones. It is therefore presumable that per-packet routing and scheduling improves the user's QoE, and outperforms the results of the proposed network selection algorithm.

However, network striping presents three issues that have to be more deeply analysed, possibly as part of this thesis future work. First, Horde's software coding makes it computationally impractical. In this sense, Calabuig offers a suitable computationally-efficient solution for network-centric striping, whose exportation to handheld devices is both feasible and advantageous. Secondly, the definition

of the utility functions should be revisited. As part of this thesis work, a number of contributions to network selection for multihomed nodes was discussed. The considered MADM-, AHP-, TOPSIS-based approaches fail both to cope with the NP-hard nature of the multihomed network selection problem, and to accommodate the non-linear nature of the user's QoE.

6.6 Limitations and Future Work

The proposed MUC-HNN NSA algorithm allocates application data streams on a per-channel basis. It does not offer packet-level granularity, e.g. as the works by Horde or Calabuig et al. This design criteria presents strengths and drawbacks. Firstly, since decisions are taken at application flow level, there is no need for separate congestion and transmission control and the subsequent multiplexing, thus implementing the proposed NSA is less burdensome and copes better with the off-the-self protocol stacks. Also, data stream to network allocation is much lighter computationally than applying the striping policies on a per-packet basis—which could be potentially unfeasible in some computing power-bound mobile devices. Horde's and other policy-based approaches involve if-then-else clauses for each packet. This is computationally impractical.

The proposed NSA is, however, inferior to Horde and Calabuig works in some aspects. Firstly, per-packet network allocation allows for very efficient routing decisions and is able to cope with heterogeneous application streams. For instance, an encoded video stream may contain both reference frames (I-frames) and delta frames (P-frames). In order for P-frames to be decoded, the previously sent I-frame must have been received successfully. It is therefore desirable or advantageous to send the I-frames over the most reliable channels. Likewise, to ensure that the audio (if present) is synchronised with the video, frames from both data streams should experience similar reception delay. In-stream QoS modulation may therefore potentiate the user's QoE.

Additionally, Horde's approach to link quality estimation permits dynamic information to input the network selection decision, rather than using default RAT-specific values. This is specially advantageous in highly dynamic environments, where link quality depends on factors such as the extent of fast- and

slow-fading, and competition for channel resources. Other solutions discussed in this thesis offer similar approaches, such as bayesian RTT estimation [81].

In summary, the Horde and Calabuig's approaches to network selection and in-stream QoS modulation is both realistic and advantageous. However, further work should address the scheduler implementation, as Horde's proposal is computationally impractical. In this sense, Calabuig may reduce the computational burden.

Also, in the short term, the proposed FFNN-based QoS estimation mechanism should be integrated with the MUC-HNN, to achieve the full potential of the later. This thesis has only considered a proportional rate constraint cost function; similar criteria is proposed by Xue et al. [82]. The rationale behind this is that, firstly, the scenario is conceptually simpler and easier to validate because it reduces the second order impact of other factors, such as the impact of latency or jitter, on the ongoing applications. Other works in the literature apply exclusively, for instance, link latency criteria [167].

The second reason why the MUC-HNN does not benefit from the FFNN mechanism is logistical. The work on the MUC-HNN took place first, and the in-built limitations of NSAs on accurately defining the user experience triggered the interest of the authors for high-level QoS estimation mechanisms. The backwards integration with the MUC-HNN is, however, seamless. The proposed HNN Lupanov function was designed to converge independently of the value of the cost function by setting appropriate weighing coefficients (see Appendix C). The simulation environment limitation can therefore be overcome by further scripting the algorithm in the OMNET++ environment.

Further work on this area should enhance striping mechanisms. Packet-scheduling calls for per-interface congestion control mechanisms because there are multiple congestion domains. Yet, with multiple destination hosts, multiple control control instances are required on a per interface for every destination. Further work should provide efficient solutions to multihomed congestion control, potentially re-implementing the solutions presented by SCTP multihoming extensions [83, 84, 168] and multipath-capable TCP mechanisms [169, 170].

Moreover, the QoS specification language should be revised. The work presented in this thesis on a FFNN solution for application-level QoS characterisation may help defining accurately the user's perceived QoS, depending on the network

allocation. Further work could improve the impact of per-packet scheduling on the user applications.

6.7 Summary

This chapter addresses, firstly, a high-level network quality descriptor based on neural networks. From link-layer indicators such as latency, BER, jitter and link capacity, the neural model returns the expected MOS (VoIP applications) or throughput (TCP-based applications). This approach permits the evaluation of the appropriateness of the available networks for the ongoing applications. Simulation results show that this approach may help users achieving optimum network selection. While many random factors influence the quality of a wireless network, the FFNN mapping offers arguably accurate results, considering the percentual values of the error estimation and the applications sensitivity.

Secondly, a novel network selection algorithm for multihomed users is proposed. This algorithm is based on HNNs and a newly defined energy-cost function that describes, from a user's perspective, the cost associated to the user's traffic-network allocation when multiple traffic flows and interfaces are involved. It is applicable to heterogeneous networks and can deal with any number of interfaces. While evaluating the performance of this approach, due to the intrinsic limitations of the simulation environment, only the link capacity has been considered to compute the inherent cost of network selection. However, the algorithm may well use the aforementioned high-level quality descriptor. Simulation results show that it may help reducing service delivery latency and increase the MOS.

Chapter 7

Conclusion and Further Work

Heterogeneous networks are expected to provide a very rich spectrum of network resources. In these environments, users would freely roam through different access networks at their convenience. However, handoff incurs a temporary QoS disruption. Thus, there is a need for the development of seamless handoff schemes suitable for heterogeneous environments. In keeping with the Ericsson's paradigm *Always Best Connected*, handoff schemes should meet the following three requirements: predicting and discovering new networks, choosing the best available network(s) intelligently and, finally, handling the connections seamlessly by providing fast proactive mobility management schemes, and alleviating the impact of handoff on applications and higher-level protocols. This thesis has targeted a limited scope of the issues related to the last two previously mentioned requirements for seamless handoff in the context of freely roaming mobile users, supporting some multihoming features, such as multiple network selection and bandwidth aggregation.

The remainder of this chapter presents the conclusions and achievements attained as part of this thesis work, and suggests some future research lines.

7.1 Summary of Contributions

This thesis has attained several achievements. The summary of contributions is as follows:

- the effective software implementation and evaluation of a cross-layer architecture that enables vertical handoffs, partially based on the OMNeT++ and INET Open Source Frameworks,
- the development and assessment of a L3 mobility scheme and the comparison of its performance with other current approaches to mobility management,
- integration of a L3 mobility scheme with added functionalities to the FMIPv6 protocol, such as PAR buffer management, reducing packet loss,
- the modification TCP and its co-operation with the L3 in order to approach the performance bounds at handoff set by the RAT,
- the formulation of a NSA for multihomed devices and the characterisation via MLP neural networks of the performance of TCP and VoIP G.726 codec, and finally,
- the incorporation of the detached contributions into the architecture framework, enabling cross-layer information exchange and co-operation.

These research contributions are also described in the publications listed in Appendix D.

7.2 Summary of Conclusions

In the light of the experimental results and analyses presented in this thesis, it has been deduced that:

- As a consequence of the variety of design principles and dynamics which different access technologies follow, there is a requirement for L2-agnostic mobility management schemes to enable seamless handoffs in the future heterogeneous networks (Chapters 1 and 2).
- Literature investigation points out to the importance of cross-layer schemes for effective protocol co-operation. The emerging IEEE802.21 standard architecture framework provides facilities that can support largely mobility

principles, such as standardised notification and command reporting interfaces. However, the standard should be extended to further facilitate seamless handoffs. The proposed set of IEEE802.21 directives and messages, coupled with the FMIPv6 facilities, helps seamless handoff provision by reducing the additive delays derived from the L3 mobility management (Chapter 3).

- The difficulties found at developing a not only fast, lightweight and computationally efficient but also secure L3 mobility management schemes point out there is a trade-off among these. The proposed PRO-FMIPv6 protocol meets the security standards set by the IETF, being equivalent at this respect to the *de facto* standard, Return Routability. However, PRO-FMIPv6 incurs lower additional delays thereby alleviating the QoS disruption (Chapter 4, Section 2).

- FMIPv6-based approaches can be improved from the experience at developing 4G seamless handoff schemes. 4G protocols co-design principles exportation to FMIPv6 networks calls for stronger links between L2 and L3. This could be provided by IEEE802.21, enabling more organic behaviour and ultimately, by increasing the intra-protocolary intelligence, reducing packet loss and saving the link's capacity usage (Chapter 4, Section 5).

- Depending on the network dynamics and handoff delays, TCP may present significant algorithmic drawbacks at handoff. The integration of a handoff notification scheme to trigger alternative congestion control procedures enhances performance, as evidenced by improved goodput figures (Chapters 3 and 5).

- The FMIPv6 facilities provide the NAR with buffering capacity. This buffering capacity can be exploited by TCP to improve the goodput in those cases where proactive handoff takes place (Chapter 5).

- For user terminals to make effective network selection decisions, they must acquire accurate information from the network. This information should include but may not be limited to link capacity, BER, jitter and security profile. User terminals, moreover, are expected to provide stable and results

even when incomplete, inaccurate, noisy and highly variable data. These technological challenges open new venues of research on network monitoring and assessment-, and on assisted handoff-enabling technologies, such as CRRM or cognitive radio (Chapter 2, Section 4).

- MLP NNs are a powerful instrument to model non-linear multi-variable functions. They show accuracy figures suitable for characterising TCP and VoIP's performance in terms of link capacity, end-to-end delay, jitter and BER. A MLP-based network evaluation methodology can benefit NSAs (Chapter 6, Section 3).

- HNNs can provide better network allocations than other currently used approaches under a range of different heterogeneous environments. However, HNN-based NSAs require proactive approaches to handoff on which the dynamic conditions of networks are monitored. Assuming the existence of a local RRM unit, FMIPv6 and IEEE802.21 provide the necessary facilities for this to happen on open heterogeneous network domains (Chapter 6, Section 4).

In a broader sense, this thesis addresses the feasibility of user-centric approaches to heterogeneous networking. In this sense, the work carried out, decoupled form specific architectural network designs and business agreements, could potentially enable intelligent seamless heterogeneous handoffs.

7.3 Limitations of this Work

Network selection strategies are sensitive to misestimated or wrong access network parameters, such as bandwidth or delay. Flawed network selection may, in turn, augment the extent of network congestion and poses a DoS security risk. Also, if there is a significant difference in the appropriateness between access technologies, where one is significantly better that the others, then most strategies including MUC-HNN will deem the same network allocation.

Likewise, the suppression of the standard TCP congestion control mechanisms at handoff also enables potential DoS attacks. Users advertising an artificially increased visited link capacity, thus virtually augmenting the TCP congestion

window size temporarily, may inject a higher number of packets than the link may support. A network information validation scheme could be integrated into the proposed Enhanced TCP algorithm to avoid this exploit.

7.4 Suggestions for Future Research

Seamless handoff is one of the mobile communication paradigms yet to be achieved. In spite of many efforts from the research and business arenas, seamless handoff is a young area where many questions remain. The incursion of cross-layer designs, autonomic computing and evolved RATs adds new angles to approach the problem.

First, this thesis has led to several co-designed schemes to seamless handoffs. However, these different proposals have been evaluated independently at the simulation environment. Next, these partial enhancements to heterogeneous handoff could be combined then compared to the state of the art.

In the short term, the resource allocation in heterogeneous environments could be reviewed. This thesis has focused on an user-centric network selection algorithm because being provided with an intelligent selection method not tied with any network operator is beneficial for users. However, also network operators can benefit from intelligent resource allocation algorithms for multihomed devices. Considering they fully manage heterogeneous environments, network operators could go further beyond service provisioning; to intelligent frequency planning, network bottleneck avoidance and to other highly beneficial considerations. In order to do so, the MUC-HNN energy-cost function could be extended to include a more organic resource allocation, where, e.g. WiFi hotspots-covered areas may relax the cellular network frequency demands.

The algorithm could also be expanded to consider other decision metrics, such as security or cost. Moreover, this thesis has considered specific VoIP codecs and TCP flavours: future work could involve the definition of other network-application performance functions or the development of a learning procedure as the one used in this thesis, based on FFNNs. Finally, the algorithm processing requirements and output stability should be further explored to support particular mobile terminal hardware capabilities.

With regard to the proposed mobility signalling scheme, the encountered security concerns could be minimised. Further extensions to the PRO-FMIPv6 could address a tighter coupling with the L2, making use of more descriptive L2 triggers and optimising the inter-operation with the mobility network architecture. Also, the case where a single multihomed user can handle multiple connections could be studied. For instance, extending the PRO-FMIPv6 signalling scheme to anticipate multihomed scenarios could further reduce delays: rather than using only one interface for carrying out the signalling, the simultaneous use of several interfaces could minimise the latencies involved in the message exchange.

This thesis has highlighted the impact of handoff on TCP flows. Upward handoff is proven to pose a security risk to mobility subnets, as mobile users may flood the visited link. Accurate network parameters discovery and secure network information exchange mechanisms should be investigated, to avoid network usage unfairness and potential DoS attacks. Also, future research directions should include the integration of rapid or proactive TCP adaptation mechanisms; enabling fast adaptation to the new link's conditions.

The simulation environment could be extended to relax some of the assumptions made in this thesis. These would include specific mobility patterns, realistic mobile terminal processing capabilities, and real-life applications or application traffic models not analysed in this thesis yet very popular among the user community, such as online gaming and video-streaming. Also, implementing user aggregation in the testbed, i.e. recreating multi-agent environments, would add a whole new dimension to the study of network selection schemes, enabling game theory approaches.

Other future work may encompass a wider spectrum of seamless mobility issues, e.g. refining the granularity of application flows, so that they can traverse different interfaces simultaneously; defining *de facto* architectures and protocols for the access discovery and mobility management; user preference discovery (via automated learning or GUI for collecting user information); integrated user mobility patterns and access network geographical information for handoff prediction; and common radio resource management for heterogeneous networks, enabling standardised description of network resources that can be used as input in network selection algorithms.

References

[1] D. Kotz, C. Newport, R. S. Gray, J. Liu, Y. Yuan, and C. Elliott, "Experimental evaluation of wireless simulation assumptions," in *Proceedings of the 7th ACM international symposium on Modeling, analysis and simulation of wireless and mobile systems*, ser. MSWiM '04. New York, NY, USA: ACM, 2004, pp. 78–82. [Online]. Available: http://doi.acm.org/10.1145/1023663.1023679 v, 88, 90

[2] O. Brid, "User-centric network selection strategy in heterogeneous wireless networks," Ph.D. dissertation, University College Dublin, Ireland, 2007. ix, 3, 12, 17, 21

[3] I. WPAN, *Press Kit*, IETF Std. 802.1.15, Jan. 2001. ix, 17

[4] R. Zhang. (2011, Jul.) Agilent Technologies Digest, Maintaining a Healthy Last Mile Connection for 3G/4G Networks. [Online]. Available: http://www.agilent.com ix, 19

[5] M. Lopez-Benitez and J. Gozalvez, "Common radio resource management algorithms for multimedia heterogeneous wireless networks," *Mobile Computing, IEEE Transactions on*, vol. 10, no. 9, pp. 1201 –1213, sept. 2011. 7

[6] J. Gozalvez and J. Gonzalez Delicado, "Crrm strategies for improving user qos in multimedia heterogeneous wireless networks," in *Personal, Indoor and Mobile Radio Communications, 2009 IEEE 20th International Symposium on*, sept. 2009, pp. 2250 –2254. 7

[7] J. Perez-Romero, O. Sallent, R. Agusti, P. Karlsson, A. Barbaresi, L. Wang, F. Casadevall, M. Dohler, H. Gonzalez, and F. Cabral-Pinto, "Common

radio resource management: functional models and implementation requirements," in *Personal, Indoor and Mobile Radio Communications, 2005. PIMRC 2005. IEEE 16th International Symposium on*, vol. 3, sept. 2005, pp. 2067 –2071 Vol. 3. 7

[8] The 802.21 Working Group. (2013, Jan.) IEEE. [Online]. Available: http://www.ieee802.org/21 9, 40, 98, 113, 143

[9] ——, *IEEE P802.21 Media Independent Handover Services*, IEEE Std. D14.0, Sep. 2008. 9, 10, 111, 189

[10] L. Eastwood, S. Migaldi, Q. Xie, and V. Gupta, "Mobility using ieee 802.21 in a heterogeneous ieee 802.16/802.11-based, imt-advanced (4g) network," *Wireless Communications, IEEE*, vol. 15, no. 2, pp. 26 –34, 2008. 10

[11] S. Mansor and T.-C. Wan, "Mobility management in heterogeneous wireless access network with ieee 802.21 services," in *Computer and Network Technology (ICCNT), 2010 Second International Conference on*, 2010, pp. 110 –114. 10

[12] G. Lampropoulos, A. Salkintzis, and N. Passas, "Media-independent handover for seamless service provision in heterogeneous networks," *Communications Magazine, IEEE*, vol. 46, no. 1, pp. 64 –71, 2008. 10

[13] K. Taniuchi, Y. Ohba, V. Fajardo, S. Das, M. Tauil, Y.-H. Cheng, A. Dutta, D. Baker, M. Yajnik, and D. Famolari, "Ieee 802.21: Media independent handover: Features, applicability, and realization," *Communications Magazine, IEEE*, vol. 47, no. 1, pp. 112 –120, 2009. 10

[14] I. Ganchev, G. Morabito, R. Narcisi, N. Passas, S. Paskalis, V. Friderikos, A. S. Jahan, E. Tsontsis, C. Bader, J. Rotrou, and H. Chaouchi, "Always best connected enabled 4g wireless world," in *in IST Mobile and Wireless Communications Summit 2003*, 2003. 16, 21, 23

[15] M. de Leon and A. Adhikari, "A user centric always best connected service business model for mvnos," in *Intelligence in Next Generation Networks (ICIN), 2010 14th International Conference on*, oct. 2010, pp. 1 –8. 16

[16] E. Gustafsson and A. Jonsson, "Always best connected," *Wireless Communications, IEEE*, vol. 10, no. 1, pp. 49 – 55, feb. 2003. 20, 21

[17] D. Johnson, C. Perkins, and J. Arkko, "Mobility Support in IPv6," RFC 3775 (Proposed Standard), Internet Engineering Task Force, Jun. 2004. [Online]. Available: http://www.ietf.org/rfc/rfc3775.txt 23, 33, 34, 39, 42, 93, 97, 102, 103, 105, 106, 107, 122, 182

[18] R. Koodli, "Mobile IPv6 Fast Handovers," RFC 5568 (Proposed Standard), Internet Engineering Task Force, Jul. 2009. [Online]. Available: http://www.ietf.org/rfc/rfc5568.txt 23, 42, 93, 97, 99, 102, 106, 107, 108, 112, 125, 131, 157, 182, 189

[19] F. Yousaf and C. Wietfeld, *Proactive Bindings for FMIPv6*, IETF Draft Std. draft-yousaf-ietf-mipshop-pbfmipv6, May 2008. 23, 46

[20] J. Arkko, C. Vogt, and W. Haddad, "Enhanced Route Optimization for Mobile IPv6," RFC 4866 (Proposed Standard), Internet Engineering Task Force, May 2007. [Online]. Available: http://www.ietf.org/rfc/rfc4866.txt 24, 46

[21] S. Mohanty and I. Akyildiz, "Performance analysis of handoff techniques based on mobile ip, tcp-migrate, and sip," *Mobile Computing, IEEE Transactions on*, vol. 6, no. 7, pp. 731 –747, july 2007. 25, 130

[22] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler, "SIP: Session Initiation Protocol," RFC 3261 (Proposed Standard), Internet Engineering Task Force, Jun. 2002, updated by RFCs 3265, 3853, 4320, 4916, 5393, 5621, 5626, 5630. [Online]. Available: http://www.ietf.org/rfc/rfc3261.txt 26

[23] N. Banerjee, A. Acharya, and S. Das, "Seamless sip-based mobility for multimedia applications," *Network, IEEE*, vol. 20, no. 2, pp. 6–13, 2006. 26

[24] A. C. Snoeren and H. Balakrishnan, "An end-to-end approach to host mobility," in *Proceedings of the 6th annual international conference on Mobile computing and networking*, ser. MobiCom '00.

New York, NY, USA: ACM, 2000, pp. 155–166. [Online]. Available: http://doi.acm.org/10.1145/345910.345938 26

[25] T. Dierks and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2," RFC 5246 (Proposed Standard), Internet Engineering Task Force, Aug. 2008, updated by RFC 5746. [Online]. Available: http://www.ietf.org/rfc/rfc5246.txt 26

[26] T. Aura and J. Arkko, *MIPv6 BU Attacks and Defenses*, IETF Draft Std. draft-aura-mipv6-bu-attacks-01, Mar. 2002. 29

[27] H. Soliman, *Mobile IPv6*. Addison-Wesley, 2004. 33

[28] J. Arkko, V. Devarapalli, and F. Dupont, "Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents," RFC 3776 (Proposed Standard), Internet Engineering Task Force, Jun. 2004, updated by RFC 4877. [Online]. Available: http://www.ietf.org/rfc/rfc3776.txt 33

[29] T. Narten, E. Nordmark, W. Simpson, and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)," RFC 4861 (Draft Standard), Internet Engineering Task Force, Sep. 2007. [Online]. Available: http://www.ietf.org/rfc/rfc4861.txt 35, 92, 99

[30] S. Thomson, T. Narten, and T. Jinmei, "IPv6 Stateless Address Autoconfiguration," RFC 4862 (Draft Standard), Internet Engineering Task Force, Sep. 2007. [Online]. Available: http://www.ietf.org/rfc/rfc4862.txt 37, 92

[31] R. Droms, J. Bound, B. Volz, T. Lemon, C. Perkins, and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)," RFC 3315 (Proposed Standard), Internet Engineering Task Force, Jul. 2003, updated by RFCs 4361, 5494. [Online]. Available: http://www.ietf.org/rfc/rfc3315.txt 37, 99

[32] P. Ferguson and D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing," RFC 2827 (Best Current Practice), Internet Engineering Task Force, May

2000, updated by RFC 3704. [Online]. Available: http://www.ietf.org/rfc/rfc2827.txt 37

[33] C. Ng, F. Zhao, M. Watari, and P. Thubert, "Network Mobility Route Optimization Solution Space Analysis," RFC 4889 (Informational), Internet Engineering Task Force, Jul. 2007. [Online]. Available: http://www.ietf.org/rfc/rfc4889.txt 38

[34] P. Nikander, J. Arkko, T. Aura, G. Montenegro, and E. Nordmark, "Mobile IP Version 6 Route Optimization Security Design Background," RFC 4225 (Informational), Internet Engineering Task Force, Dec. 2005. [Online]. Available: http://www.ietf.org/rfc/rfc4225.txt 50, 122

[35] H. Soliman, C. Castelluccia, K. ElMalki, and L. Bellier, "Hierarchical Mobile IPv6 (HMIPv6) Mobility Management," RFC 5380 (Proposed Standard), Internet Engineering Task Force, Oct. 2008. [Online]. Available: http://www.ietf.org/rfc/rfc5380.txt 51

[36] M. Kunishi, M. Ishiyama, K. Uehara, and H. Teraoka, "Lin6: A new approach to mobility support in ipv6," 2000. 51

[37] R. Moskowitz and P. Nikander, "Host Identity Protocol (HIP) Architecture," RFC 4423 (Informational), Internet Engineering Task Force, May 2006. [Online]. Available: http://www.ietf.org/rfc/rfc4423.txt 51

[38] R. Moskowitz, P. Nikander, P. Jokela, and T. Henderson, "Host Identity Protocol," RFC 5201 (Experimental), Internet Engineering Task Force, Apr. 2008. [Online]. Available: http://www.ietf.org/rfc/rfc5201.txt 51

[39] A. Rossi, S. Pierre, and S. Krishnan, "Secure route optimization for mipv6 using enhanced cga and dnssec," pp. 1–1, 2012. 51, 126

[40] L. Shi, B. Guo, and L. Zhao, "A novel certificate-based mobile ipv6 bingding technology," in *Wireless Mobile and Computing (CCWMC 2009), IET International Communication Conference on*, 2009, pp. 637–639. 51

[41] S. Pack and W. Lee, "Optimal binding-management-key refresh interval in mobile ipv6 networks," *Vehicular Technology, IEEE Transactions on*, vol. 58, no. 7, pp. 3834–3837, 2009. 51

[42] H. Balakrishnan, V. N. Padmanabhan, S. Seshan, and R. H. Katz, "A comparison of mechanisms for improving tcp performance over wireless links," *IEEE/ACM Trans. Netw.*, vol. 5, no. 6, pp. 756–769, 1997. 52

[43] D.-M. Chiu and R. Jain, "Analysis of the increase and decrease algorithms for congestion avoidance in computer networks," *Comput. Netw. ISDN Syst.*, vol. 17, no. 1, pp. 1–14, 1989. 52

[44] W. R. Stevens, *TCP/IP Illustrated*. Addison-Wesley, 1994. 53, 55

[45] M. Allman, V. Paxson, and W. Stevens, "TCP Congestion Control," RFC 2581 (Proposed Standard), Internet Engineering Task Force, Apr. 1999, obsoleted by RFC 5681, updated by RFC 3390. [Online]. Available: http://www.ietf.org/rfc/rfc2581.txt 53, 55, 93, 118, 134, 162, 197

[46] K. Fall and S. Floyd, "Simulation-based comparisons of tahoe, reno and sack tcp," *SIGCOMM Comput. Commun. Rev.*, vol. 26, no. 3, pp. 5–21, 1996. 55

[47] "Iso/iec 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 (includes ieee std 802.11, 1999 edition; ieee std 802.11a.-1999; ieee std 802.11b.-1999; ieee std 802.11b.-1999/cor 1-2001; and ieee std 802.11d.-2001)," *ISO/IEC 8802-11 IEEE Std 802.11 Second edition 2005-08-01 ISO/IEC 8802 11:2005(E) IEEE Std 802.11i-2003 Edition*, 2005. 56, 91

[48] "Ieee standard for information technology- telecommunications and information exchange between systems- local and metropolitan area networks-specific requirements part ii: Wireless lan medium access control (mac) and physical layer (phy) specifications," *IEEE Std 802.11g-2003 (Amendment to IEEE Std 802.11, 1999 Edn. (Reaff 2003) as amended by IEEE*

Stds 802.11a-1999, 802.11b-1999, 802.11b-1999/Cor 1-2001, and 802.11d-2001), 2003. 56, 91

[49] H. Balakrishnan, S. Seshan, and R. H. Katz, "Improving reliable transport and handoff performance in cellular wireless networks," *Wireless Networks*, vol. 1, pp. 469–481, 1995, 10.1007/BF01985757. [Online]. Available: http://dx.doi.org/10.1007/BF01985757 58

[50] A. Bakre and B. Badrinath, "I-tcp: indirect tcp for mobile hosts," in *Distributed Computing Systems, 1995., Proceedings of the 15th International Conference on*, 1995. 59

[51] R. Yavatkar and N. Bhagawat, "Improving end-to-end performance of tcp over mobile internetworks," in *Mobile Computing Systems and Applications, 1994. Proceedings., Workshop on*, Dec. 1994, pp. 146 –152. 59

[52] K. Brown and S. Singh, "M-tcp: Tcp for mobile cellular networks," *SIGCOMM Comput. Commun. Rev.*, vol. 27, pp. 19–43, October 1997. [Online]. Available: http://doi.acm.org/10.1145/269790.269794 59

[53] T.Goff *et al.*, "Freeze-TCP: A true end-to-end TCP enhancement mechanism for mobile environments," in *Proc. IEEE IEEE Computer and Communications Societies (INFOCOMMS)*, Nagoya, Japan, 2000, pp. 1537–1545. 59, 64, 130, 131

[54] M. Yoshimoto, K. Kawano, K. Kinoshita, T. Matsuda, and K. Murakami, "Handoff performance enhancement for tcp-based streaming services in heterogeneous networks," in *Local Computer Networks, 2007. LCN 2007. 32nd IEEE Conference on*, 15-18 2007, pp. 703 –710. 61, 62, 130, 131, 164

[55] D. Le, D. Guo, and B. Wu, "Wlc47-6: Tcp performance improvement through inter-layer enhancement with mobile ipv6," in *Global Telecommunications Conference, 2006. GLOBECOM '06. IEEE*, nov. 2006, pp. 1 –5. 63, 130, 131, 163

[56] N. Parvez and L. Hossain, "Improving tcp performance in wired-wireless networks by using a novel adaptive bandwidth estimation mechanism,"

in *Global Telecommunications Conference, 2004. GLOBECOM '04. IEEE*, 2004. 63, 66

[57] J. Kempf, R. Austein, and IAB, "The Rise of the Middle and the Future of End-to-End: Reflections on the Evolution of the Internet Architecture," RFC 3724 (Informational), Internet Engineering Task Force, Mar. 2004. [Online]. Available: http://www.ietf.org/rfc/rfc3724.txt 65

[58] S. Floyd, M. Handley, and E. Kohler, "Problem Statement for the Datagram Congestion Control Protocol (DCCP)," RFC 4336 (Informational), Internet Engineering Task Force, Mar. 2006. [Online]. Available: http://www.ietf.org/rfc/rfc4336.txt 65

[59] ITU-T. (2009, Nov.) Annex A-Profiles and levels, Recommendation H.264. [Online]. Available: http://www.itu.int 66, 200

[60] ——. (2009, Nov.) Recommendation G.711. [Online]. Available: http://www.itu.int 66, 200

[61] P. McCann, "Mobile IPv6 Fast Handovers for 802.11 Networks," RFC 4260 (Informational), Internet Engineering Task Force, Nov. 2005. [Online]. Available: http://www.ietf.org/rfc/rfc4260.txt 67

[62] Q. Mussabbir, W. Yao, Z. Niu, and X. Fu, "Optimized fmipv6 using ieee 802.21 mih services in vehicular networks," *Vehicular Technology, IEEE Transactions on*, vol. 56, no. 6, pp. 3397 –3407, 2007. 67

[63] R. Wakikawa, V. Devarapalli, G. Tsirtsis, T. Ernst, and K. Nagami, "Multiple Care-of Addresses Registration," RFC 5648 (Proposed Standard), Internet Engineering Task Force, Oct. 2009. [Online]. Available: http://www.ietf.org/rfc/rfc5648.txt 68

[64] M. Dillinger, K. Madami, and N. Alonistioti, *Software Defined Radio: Architectures, Systems and Functions*. John Wiley and Sons Ltd, 2003. 68

[65] D. Tripathi, *Radio Resource Managment in Cellular Systems*. Kluwer Academic Publishers, 2001. 69

[66] Recommendation G.107 - AAP51, "The E-model, a computational model for use in transmission planning," ITU-T. 69, 130

[67] Recommendation G.114, "General Recommendations on the transmission quality for an entire international telephone connection—One-Way Transmission Time," ITU-T, May 2000. 69

[68] J. Puttonen, G. Fekete, T. Vaaramaki, and T. Hamalainen, "Multiple interface management of multihomed mobile hosts in heterogeneous wireless environments," in *Networks, 2009. ICN '09. Eighth International Conference on*, march 2009, pp. 324 –331. 70

[69] M. R. HeidariNezhad and Z. Zukarnain, "A host mobility support with adaptive network selection method in hybrid wireless environment." *JDCTA*, vol. 3, no. 1, pp. 34–39, 2009. [Online]. Available: http://dblp.uni-trier.de/db/journals/jdcta/jdcta3.html#HeidariNezhadZ09 70

[70] Recommendation P-862, "Perceptual Evaluation of Speech Quality (PESQ), An Objective Method for End-to-end Speech Quality Assessment of Narrow-band Telephone Networks and Speech Codecs," ITU-T, Feb. 2001. 70, 197

[71] M. Kibria, A. Jamalipour, and V. Mirchandani, "A location aware three-step vertical handoff scheme for 4g/b3g networks," in *Global Telecommunications Conference, 2005. GLOBECOM '05. IEEE*, vol. 5, dec. 2005, pp. 2752 –2756. 75

[72] Q.-T. Nguyen-Vuong, N. Agoulmine, and Y. Ghamri-Doudane, "Terminal-controlled mobility management in heterogeneous wireless networks," *Communications Magazine, IEEE*, vol. 45, no. 4, pp. 122 –129, april 2007. 75

[73] X. Cai, L. Chen, R. Sofia, and Y. Wu, "Dynamic and user-centric network selection in heterogeneous networks," in *Performance, Computing, and Communications Conference, 2007. IPCCC 2007. IEEE Internationa*, april 2007, pp. 538 –544. 75

[74] N. Nasser, S. Guizani, and E. Al-Masri, "Middleware vertical handoff manager: A neural network-based solution," in *Communications, 2007. ICC '07. IEEE International Conference on*, june 2007, pp. 5671 –5676. 75

[75] T.-Y. Chung, F.-C. Yuan, Y.-M. Chen, B.-J. Liu, and C.-C. Hsu, "Extending always best connected paradigm for voice communications in next generation wireless network," in *Advanced Information Networking and Applications, 2008. AINA 2008. 22nd International Conference on*, march 2008, pp. 803 –810. 75

[76] J. Ibanez and A. Marti, "An access cell selection algorithm for next generation mobile environments," *Latin America Transactions, IEEE (Revista IEEE America Latina)*, vol. 6, no. 2, pp. 194 –200, june 2008. 75

[77] Y. Nkansah-Gyekye and J. Agbinya, "A vertical handoff decision algorithm for next generation wireless networks," in *Broadband Communications, Information Technology Biomedical Applications, 2008 Third International Conference on*, nov. 2008, pp. 358 –364. 75

[78] Y. Chen, J. Ai, and Z. Tan, "An access network selection algorithm based on hierarchy analysis and fuzzy evaluation," in *Wireless Communications Signal Processing, 2009. WCSP 2009. International Conference on*, nov. 2009, pp. 1 –5. 75

[79] Q. He, "A novel vertical handoff decision algorithm in heterogeneous wireless networks," in *Wireless Communications, Networking and Information Security (WCNIS), 2010 IEEE International Conference on*, june 2010, pp. 566 –570. 75

[80] X. Liu and C. Chang, "The topsis algorithm based on a + bi type connection numbers for decision-making in the convergence of heterogeneous networks," in *Advanced Computer Theory and Engineering (ICACTE), 2010 3rd International Conference on*, vol. 2, aug. 2010, pp. V2–323 –V2–327. 75

[81] E. H. Ong and J. Khan, "On optimal network selection in a dynamic multi-rat environment," *Communications Letters, IEEE*, vol. 14, no. 3, pp. 217 –219, march 2010. 75, 189, 206

[82] P. Xue, P. Gong, J. H. Park, D. Park, and D. K. Kim, "Radio resource management with proportional rate constraint in the heterogeneous networks," *Wireless Communications, IEEE Transactions on*, vol. 11, no. 3, pp. 1066–1075, 2012. 72, 206

[83] R. Fracchia, C. Casetti, C. Chiasserini, and M. Meo, "Wise: Best-path selection in wireless multihoming environments," *Mobile Computing, IEEE Transactions on*, vol. 6, no. 10, pp. 1130–1141, 2007. 73, 206

[84] C. Casetti, C. Chiasserini, R. Fracchia, and M. Meo, "Autonomic interface selection for mobile wireless users," *Vehicular Technology, IEEE Transactions on*, vol. 57, no. 6, pp. 3666–3678, 2008. 73, 206

[85] A. Qureshi and J. Guttag, "Horde: separating network striping policy from mechanism," in *Proceedings of the 3rd international conference on Mobile systems, applications, and services*, ser. MobiSys '05. New York, NY, USA: ACM, 2005, pp. 121–134. [Online]. Available: http://doi.acm.org/10.1145/1067170.1067184 73

[86] D. Calabuig *et al.*, "A Delay-Centric Dynamic Resource Allocation Algorithm for Wireless Communication Systems Based on HNN," *IEEE Trans. Veh. Commun.*, vol. 57, no. 6, pp. 3653–3665, Nov. 2008. 74, 194, 201, 238

[87] J. J. Hopfield, "Neurocomputing: foundations of research," J. A. Anderson and E. Rosenfeld, Eds. Cambridge, MA, USA: MIT Press, 1988, ch. Neural networks and physical systems with emergent collective computational abilities, pp. 457–464. [Online]. Available: http://dl.acm.org/citation.cfm?id=65669.104422 74

[88] INET Framework for OMNeT++. (2009, Oct.) OMNeT++ Community Site. [Online]. Available: http://www.omnetpp.org 76, 79, 90, 112

[89] Centre for Telecommunications and Information Engineering(CTIE). (2010, Nov.) Monash University in Melbourne, Australia. [Online]. Available: http://www.ctie.monash.edu.au 76

[90] Eclipse IDE. (2009, Oct.) The Eclipse Foundation. [Online]. Available: http://www.eclipse.org 77

[91] R. Stewart, "Stream Control Transmission Protocol," RFC 4960 (Proposed Standard), Internet Engineering Task Force, Sep. 2007. [Online]. Available: http://www.ietf.org/rfc/rfc4960.txt 86

[92] E. Rosen, A. Viswanathan, and R. Callon, "Multiprotocol Label Switching Architecture," RFC 3031 (Proposed Standard), Internet Engineering Task Force, Jan. 2001. [Online]. Available: http://www.ietf.org/rfc/rfc3031.txt 86

[93] D. Awduche, L. Berger, D. Gan, T. Li, V. Srinivasan, and G. Swallow, "RSVP-TE: Extensions to RSVP for LSP Tunnels," RFC 3209 (Proposed Standard), Internet Engineering Task Force, Dec. 2001, updated by RFCs 3936, 4420, 4874, 5151, 5420, 5711. [Online]. Available: http://www.ietf.org/rfc/rfc3209.txt 86

[94] L. Andersson, I. Minei, and B. Thomas, "LDP Specification," RFC 5036 (Draft Standard), Internet Engineering Task Force, Oct. 2007. [Online]. Available: http://www.ietf.org/rfc/rfc5036.txt 86

[95] W. Simpson, "The Point-to-Point Protocol (PPP)," RFC 1661 (Standard), Internet Engineering Task Force, Jul. 1994, updated by RFC 2153. [Online]. Available: http://www.ietf.org/rfc/rfc1661.txt 86

[96] J. Andersen, T. Rappaport, and S. Yoshida, "Propagation measurements and models for wireless communications channels," *Communications Magazine, IEEE*, vol. 33, no. 1, pp. 42 –49, jan 1995. 89

[97] T. Rappaport. 90

[98] I. . WG, *Status of 802.20 Channel Models*, Channel Modeling Correspondence Group Std., Jan. 2004. 90

[99] INETMANET Framework for OMNeT++. (2009, Oct.) OMNeT++ Community Site. [Online]. Available: https://github.com/inetmanet 90

[100] M. Bredel and M. Bergner, "On the accuracy of ieee 802.11g wireless lan simulations using omnet++," in *Proceedings of the 2nd International Conference on Simulation Tools and Techniques*, ser. Simutools '09.

ICST, Brussels, Belgium, Belgium: ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2009, pp. 81:1–81:5. [Online]. Available: http://dx.doi.org/10.4108/ICST.SIMUTOOLS2009.5585 92

[101] S. Deering and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification," RFC 2460 (Draft Standard), Internet Engineering Task Force, Dec. 1998, updated by RFCs 5095, 5722. [Online]. Available: http://www.ietf.org/rfc/rfc2460.txt 92

[102] A. Conta, S. Deering, and M. Gupta, "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification," RFC 4443 (Draft Standard), Internet Engineering Task Force, Mar. 2006, updated by RFC 4884. [Online]. Available: http://www.ietf.org/rfc/rfc4443.txt 92

[103] J. Postel, "User Datagram Protocol," RFC 768 (Standard), Internet Engineering Task Force, Aug. 1980. [Online]. Available: http://www.ietf.org/rfc/rfc768.txt 93

[104] ——, "Transmission Control Protocol," RFC 793 (Standard), Internet Engineering Task Force, Sep. 1981, updated by RFCs 1122, 3168. [Online]. Available: http://www.ietf.org/rfc/rfc793.txt 93, 118

[105] J. Nagle, "Congestion Control in IP/TCP Internetworks," RFC 896, Internet Engineering Task Force, Jan. 1984. [Online]. Available: http://www.ietf.org/rfc/rfc896.txt 93

[106] R. Braden, "Requirements for Internet Hosts - Communication Layers," RFC 1122 (Standard), Internet Engineering Task Force, Oct. 1989, updated by RFCs 1349, 4379. [Online]. Available: http://www.ietf.org/rfc/rfc1122.txt 93, 118

[107] V. Jacobson, R. Braden, and D. Borman, "TCP Extensions for High Performance," RFC 1323 (Proposed Standard), Internet Engineering Task Force, May 1992. [Online]. Available: http://www.ietf.org/rfc/rfc1323.txt 93, 118

[108] M. Mathis, J. Mahdavi, S. Floyd, and A. Romanow, "TCP Selective Acknowledgment Options," RFC 2018 (Proposed Standard), Internet Engineering Task Force, Oct. 1996. [Online]. Available: http://www.ietf.org/rfc/rfc2018.txt 93

[109] M. Bohge and R. Martin, "A realisitic voip traffic generation and evaluation tool for omnet++," Mar. 2008. 93, 197

[110] ITU-T - Recommendation G.726. (1990) 40, 32, 24, 16 kbits Adaptive Differential Pulse Code Modulation (ADPCM). [Online]. Available: http://www.itu.int/rec/T-REC-G.726/ 93, 197

[111] J. Postel and J. Reynolds, "File Transfer Protocol," RFC 959 (Standard), Internet Engineering Task Force, Oct. 1985, updated by RFCs 2228, 2640, 2773, 3659, 5797. [Online]. Available: http://www.ietf.org/rfc/rfc959.txt 94

[112] H. Lu, P. Hong, X. Zhou, and L. Liu, "Performance evaluation of link layer triggers for fast handovers in mobile ipv6," in *Communications and Networking in China, 2006. ChinaCom '06. First International Conference on*, oct. 2006, pp. 1 –5. 97

[113] Y.-S. Kim, D.-H. Kwon, and Y.-J. Suh, "Seamless handover support over heterogeneous networks using fmipv6 with definitive l2 triggers," *Wireless Personal Communications*, vol. 43, pp. 919–932, 2007, 10.1007/s11277-007-9265-4. [Online]. Available: http://dx.doi.org/10.1007/s11277-007-9265-4 97, 98

[114] D. Eastlake 3rd and P. Jones, "US Secure Hash Algorithm 1 (SHA1)," RFC 3174 (Informational), Internet Engineering Task Force, Sep. 2001, updated by RFC 4634. [Online]. Available: http://www.ietf.org/rfc/rfc3174.txt 99

[115] V. Devarapalli, R. Wakikawa, A. Petrescu, and P. Thubert, "Network Mobility (NEMO) Basic Support Protocol," RFC 3963 (Proposed Standard), Internet Engineering Task Force, Jan. 2005. [Online]. Available: http://www.ietf.org/rfc/rfc3963.txt 104

[116] H. Soliman, C. Castelluccia, K. E. Malki, and L. Bellier, "Hierarchical Mobile IPv6 Mobility Management (HMIPv6)," RFC 4140 (Experimental), Internet Engineering Task Force, Aug. 2005, obsoleted by RFC 5380. [Online]. Available: http://www.ietf.org/rfc/rfc4140.txt 104

[117] S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury, and B. Patil, "Proxy Mobile IPv6," RFC 5213 (Proposed Standard), Internet Engineering Task Force, Aug. 2008. [Online]. Available: http://www.ietf.org/rfc/rfc5213.txt 104

[118] N. V. Hanh and S. Ro, "Simplified Fast Handover in Mobile IPv6 Networks," *Computer Communications*, vol. 31, no. 15, pp. 3594–3603, Apr. 2008. 112

[119] J. Abley *et al.*, *Goals for IPv6 Site-Multihoming Architectures*, IETF Std. RFC 3582, Aug. 2003. 113, 143

[120] G. Huston, *Architectural Approaches to Multihoming for IPv6*, IETF Std. RFC 4177, Sep. 2005. 113, 143

[121] C. Hutzler, D. Crocker, P. Resnick, E. Allman, and T. Finch, "Email Submission Operations: Access and Accountability Requirements," RFC 5068 (Best Current Practice), Internet Engineering Task Force, Nov. 2007. [Online]. Available: http://www.ietf.org/rfc/rfc5068.txt 120

[122] R. Graveman, M. Parthasarathy, P. Savola, and H. Tschofenig, "Using IPsec to Secure IPv6-in-IPv4 Tunnels," RFC 4891 (Informational), Internet Engineering Task Force, May 2007. [Online]. Available: http://www.ietf.org/rfc/rfc4891.txt 121

[123] T. Aura, "Cryptographically Generated Addresses (CGA)," RFC 3972 (Proposed Standard), Internet Engineering Task Force, Mar. 2005, updated by RFCs 4581, 4982. [Online]. Available: http://www.ietf.org/rfc/rfc3972.txt 122

[124] J. Jonsson and B. Kaliski, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1," RFC 3447

(Informational), Internet Engineering Task Force, Feb. 2003. [Online]. Available: http://www.ietf.org/rfc/rfc3447.txt 122

[125] S. Kuang, R. Elz, and S. Kamolphiwong, "Investigating enhanced route optimization for mobile ipv6," aug. 2008, pp. 1 –7. 123

[126] B. Carpenter, "RFC 1888 Is Obsolete," RFC 4048 (Informational), Internet Engineering Task Force, Apr. 2005, updated by RFC 4548. [Online]. Available: http://www.ietf.org/rfc/rfc4048.txt 125

[127] M. Portoles-Comeras, M. Cardenete-Suriol, J. Mangues-Bafalluy, M. Requena-Esteso, and L. Hersant, "Experimental assessment of voip quality in mipv6 and sip mobility scenarios," in *Communications, 2006. ICC '06. IEEE International Conference on*, vol. 5, june 2006, pp. 2048 –2053. 130

[128] H. Kim and M. Moh, "Performance of fmipv6-based cross-layer handover for supporting mobile voip in wimax networks," in *Communications, Computers and Signal Processing, 2009. PacRim 2009. IEEE Pacific Rim Conference on*, 23-26 2009, pp. 221 –226. 130

[129] T. Henttonen, K. Aschan, J. Puttonen, N. Kolehmainen, P. Kela, M. Moisio, and J. Ojala, "Performance of voip with mobility in utra long term evolution," in *Vehicular Technology Conference, 2008. VTC Spring 2008. IEEE*, 11-14 2008, pp. 2492 –2496. 130

[130] H. Fathi, S. S. Chakraborty, and R. Prasad, "Optimization of mobile ipv6-based handovers to support voip services in wireless heterogeneous networks," *Vehicular Technology, IEEE Transactions on*, vol. 56, no. 1, pp. 260 –270, jan. 2007. 130

[131] N. Fikouras, K. El Malki, S. Cvetkovic, and C. Smythe, "Performance of tcp and udp during mobile ip handoffs in single-agent subnetworks," in *Wireless Communications and Networking Conference, 1999. WCNC. 1999 IEEE*, 1999, pp. 1258 –1262 vol.3. 130

[132] X. He, L. Xu, M. Liu, and L. Zhang, "Tcp performance evaluation over wireless networks," in *Electrical and Computer Engineering, 2004. Canadian Conference on*, vol. 2, 2-5 2004, pp. 983 – 986 Vol.2. 130

[133] A. Argyriou and V. Madisetti, "Wlc47-1: Modeling the effect of mobile handoffs on tcp and tfrc throughput," in *Global Telecommunications Conference, 2006. GLOBECOM '06. IEEE*, nov. 2006, pp. 1 –5. 130

[134] J. Ben-Othman, F. Nait-Abdesselam, L. Mokdad, and O. Ramirez, "Performance evaluation of tcp handoffs over mobile ip connections," in *Computer Systems and Applications, 2008. AICCSA 2008. IEEE/ACS International Conference on*, march 2008, pp. 366 –372. 130

[135] Y. Tian, K. Xu, and N. Ansari, "Tcp in wireless environments: problems and solutions," *Communications Magazine, IEEE*, vol. 43, no. 3, pp. S27 – S32, march 2005. 130

[136] M. K. Park, J. Y. Lee, B. C. Kim, and D. Y. Kim, "Design of fast handover mechanism for multiple interfaces mobile ipv6," in *Wireless Pervasive Computing, 2008. ISWPC 2008. 3rd International Symposium on*, 7-9 2008, pp. 697 –701. 131

[137] A. Kato, M. Kanda, and S. Kanno, "Camellia Counter Mode and Camellia Counter with CBC-MAC Mode Algorithms," RFC 5528 (Informational), Internet Engineering Task Force, Apr. 2009. [Online]. Available: http://www.ietf.org/rfc/rfc5528.txt 132

[138] S. Bradner and V. Paxson, *IANA Allocation Guidelines For Values In the Internet Protocol and Related Headers*, IETF Std. RFC 2780, Mar. 2000. 136

[139] J. G. Proakis and M. Salehi, *Communication systems engineering*. Upper Saddle River, NJ, USA: Prentice-Hall, Inc., 1994. 140

[140] J. Espi, R. Atkinson, I. Andonovic, and J. Dunlop, "Proactive route optimization for fast mobile ipv6," in *Vehicular Technology Conference Fall (VTC 2009-Fall), 2009 IEEE 70th*, 20-23 2009, pp. 1 –5. 143

[141] S. Floyd and K. Fall, "Promoting the use of end-to-end congestion control in the internet," *Networking, IEEE/ACM Transactions on*, vol. 7, no. 4, pp. 458 –472, aug 1999. 161

[142] T. Eguchi, H. Ohsaki, and M. Murata, "On control parameters tuning for active queue management mechanisms using multivariate analysis," in *Applications and the Internet, 2003. Proceedings. 2003 Symposium on*, 27-31 2003, pp. 120 – 127. 161

[143] J. Padhye, V. Firoiu, D. Towsley, and J. Kurose, "Modeling tcp reno performance: a simple model and its empirical validation," *Networking, IEEE/ACM Transactions on*, vol. 8, no. 2, pp. 133 –145, apr 2000. 161

[144] S. Floyd and V. Jacobson, "Random early detection gateways for congestion avoidance," *Networking, IEEE/ACM Transactions on*, vol. 1, no. 4, pp. 397 –413, aug 1993. 161

[145] ——, "Link-sharing and resource management models for packet networks," *Networking, IEEE/ACM Transactions on*, vol. 3, no. 4, pp. 365 –386, aug 1995. 161

[146] G. He, F. Lu, A. Guo, and X. Wu, "Dc-sfq: An improved stochastic fairness queuing algorithm," in *Network Infrastructure and Digital Content, 2009. IC-NIDC 2009. IEEE International Conference on*, 6-8 2009, pp. 192 –196. 161

[147] M. Allman, S. Floyd, and C. Partridge, "Increasing TCP's Initial Window," RFC 3390 (Proposed Standard), Internet Engineering Task Force, Oct. 2002. [Online]. Available: http://www.ietf.org/rfc/rfc3390.txt 162

[148] Microsoft Corp. (2010, Sep.) Skype. [Online]. Available: http://www.skype.com 181

[149] S. L. Tompros and S. Denazis, "Interworking of heterogeneous access networks and QoS provisioning via IP multimedia core networks," *Computer Networks: The International Journal of Computer and Telecommunications Networking*, vol. 52, no. 1, pp. 215–227, Jan. 2008. 182

[150] 3GPP. (2009, Nov.) TSG Core Network and Terminals WG4. [Online]. Available: http://www.3gpp.org 182

[151] W. Liao *et al.*, "Improving TCP Performance in Mobile Networks," *IEEE Trans. Commun.*, vol. 53, no. 4, pp. 569–571, Apr. 2005. 182

[152] E. Gustaffson and A. Johnson, "Always best connected," *IEEE Wireless Commun. Mag.*, vol. 10, no. 1, pp. 49–55, Feb. 2003. 182

[153] WGs charts. (2009, Nov.) The Internet Engineering Task Force (IETF). [Online]. Available: http://www.ietf.org 183

[154] N. Kasabov, *Foundations of Neural Networks, Fuzzy Systems, and Knowledge Engineering.* The MIT Press, 1998. 183, 185, 189, 193

[155] M. Minsky and S. Papert, *Perceptrons: An Introduction to Computational Geometry.* The MIT Press, 1969. 186

[156] P. Werbos, "Beyond Regression: New Tools for Prediction and Analysis in the Behavioural Sciences," Ph.D. dissertation, Harvard University, 1972. 186

[157] D. Rumelhart and J. McClelland, *Parallel Distributed Processing: Explorations in the Microstructure of Cogniton.* The MIT Press, 1986. 186

[158] O. Raoof and H. Al-Raweshidy, "Design an interface/network selection mechanism for multi-interface fmipv6 protocol," in *Sensing Technology, 2008. ICST 2008. 3rd International Conference on*, 30 2008-dec. 3 2008, pp. 348 –353. 189

[159] K. V, *Learning and Soft Computing: Support Vector Machines, Neural Networks and Fuzzy Logic Models.* The MIT Press, 2001. 193

[160] B. Krose and P. Smagt, *An introduction to Neural Networks.* The Amsterdam University Press, 1996. 194

[161] J. S. Blogh and L. Hanzo, *Third-Generation Systems and Intelligent Wireless Networking.* Wiley-IEEE Press, 2004. 200

[162] M. Atkins, "Sorting by hopfield net," in *Neural Networks, 1989. IJCNN., International Joint Conference on*, 1989, pp. 65–68 vol.2. 202

[163] J.-S. Lai, S.-Y. Kuo, and I.-Y. Chen, "Neural networks for optimization problems in graph theory," in *Circuits and Systems, 1994. ISCAS '94., 1994 IEEE International Symposium on*, vol. 6, 1994, pp. 269–272 vol.6. 202

[164] S. Sathasivam, N. Hamadneh, and O. H. Choon, "Comparing neural networks: Hopfield network and rbf network." *Applied Mathematical Sciences (Ruse)*, vol. 5, no. 69-72, pp. 3439–3452, 2011. 202

[165] G. Serpen and A. Parvin, "On the performance of hopfield network for graph search problem," *Neurocomputing: An International Journal*, vol. 14, pp. 365–381, 1997. 203

[166] G. Joya, M. Atencia, and F. Sandoval, "Hopfield neural networks for optimization: study of the different dynamics," *Neurocomputing*, vol. 43, no. 14, pp. 219 – 237, 2002, ¡ce:title¿Selected engineering applications of neural networks¡/ce:title¿. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S092523120100337X 203

[167] E. Ribeiro and V. C. M. Leung, "Minimum delay path selection in multihomed systems with path asymmetry," *Communications Letters, IEEE*, vol. 10, no. 3, pp. 135–137, 2006. 206

[168] Y. Yuan, Z. Zhang, J. Li, J. Shi, J. Zhou, G. Fang, and E. Dutkiewicz, "Extension of sctp for concurrent multi-path transfer with parallel subflows," in *Wireless Communications and Networking Conference (WCNC), 2010 IEEE*, 2010, pp. 1–6. 206

[169] D. Wischik, M. Handley, and C. Raiciu, "Control of multipath tcp and optimization of multipath routing in the internet," in *Proceedings of the 3rd Euro-NF Conference on Network Control and Optimization*, ser. NET-COOP '09. Berlin, Heidelberg: Springer-Verlag, 2009, pp. 204–218. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-10406-0_14 206

[170] D. Wischik, M. Handley, and M. B. Braun, "The resource pooling principle," *SIGCOMM Comput. Commun. Rev.*, vol. 38, no. 5, pp. 47–52, Sep. 2008. [Online]. Available: http://doi.acm.org/10.1145/1452335.1452342 206

Appendix A

PRO-FMIPv6 Alternative Signalling Schemes

The original PRO-FMIPv6 design incorporates Optimistic DAD, i.e. it considers a low address collision probability. In those cases where collision is to be fully avoided, then the PRO-FMIPv6 signalling would be modified as Figure A.1 depicts. This scheme does not requires of triggering further in advance the signalling tasks, as the MN must receive the HAck message at the PAR's link. On another note, the results for route optimisation delays hold.

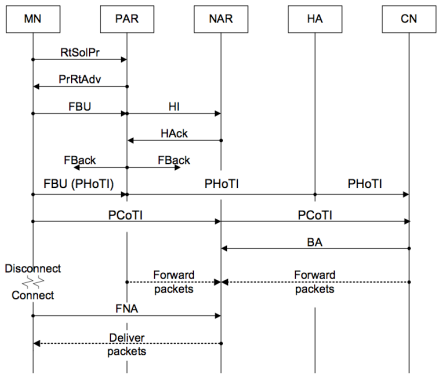


Figure A.1: Non-optimistic-DAD PRO-FMIPv6 Signalling

Appendix B

TCP Formal Analysis

Equations on TCP performance.

Extra segments received

Packets received during SS:

$$\sum_{n=0}^{\lg_2 \frac{W}{2}} 2^n = \frac{2^{\lg_2 \frac{W}{2}+1} - 2^0}{2-1} = W - 1 \tag{B.1}$$

Packets received during CA:

$$\sum_{n=\lg_2 \frac{W}{2}+1}^{W} \frac{W}{2} + 1 + n = \sum_{i=1}^{\frac{W}{2}} \frac{W}{2} + i = \frac{3W^2}{8} + \frac{W}{4} \tag{B.2}$$

Therefore, in standard TCP, from connection re-establishment up to *cwnd*=W:

$$Segmentsreceived = \frac{3W^2}{8} + \frac{5W}{4} - 1 \tag{B.3}$$

In Freeze-TCP, since avoids bringing down the TCP cwnd size, the segments transferred are given by:

$$Segmentsreceived = W\left(\frac{W}{2} + \lg_2 \frac{W}{2}\right) \tag{B.4}$$

Thus,

$$FreezeExtraSegments = \frac{W^2}{8} + W \lg_2 \frac{W}{2} - \frac{5W}{4} + 1 \tag{B.5}$$

The proposed scheme saves RTT seconds derived from signalling after handoff. The previous equations then can be re-written as:

$$Segmentsreceived = W \left(\frac{W}{2} + \lg_2 \frac{W}{2} + 1 \right) \tag{B.6}$$

Ergo,

$$ExtraSegments = \frac{W^2}{8} + W \lg_2 \frac{W}{2} - \frac{W}{4} + 1 \tag{B.7}$$

Appendix C

Energy Function Weighting Coefficients Calculation

The weighting coefficients have been calculated as in [86]. The worst case scenarios are considered so that the choice of weights permits increased convergence rates. Choices that imply a benefit from the user perspective, not necessarily reduce the value of (6.20). Favorable choices are denoted by $+$, while negative choices are denoted by $-$.

First term

The first term of the energy function permits faster convergence of the HNN.

$$\frac{\partial E}{\partial V_{n,t_+}} = \frac{A}{2}\left(1 - 2V_{n,t_+}\right) + \frac{D}{2} f^u_{n,t_+} + \frac{F}{2}\frac{f_{n,t_+}}{f_{min,t}}$$

$$\frac{\partial E}{\partial V_{n,t_-}} = \frac{A}{2}\left(1 - 2V_{n,t_-}\right) + \frac{D}{2} f^u_{n,t_-} + \frac{F}{2}\frac{f_{n,t_-}}{f_{min,t}}$$

The condition for converge towards the minimum is:

$$\frac{\partial E}{\partial V_{n,t_+}} < \frac{\partial E}{\partial V_{n,t_-}}$$

In worst case scenario, $V_{n,t_-} = 1$, $V_{n,t_-} = 0$, $f^u_{n,t_-} = f^u_{n,t_+}$.

$$\frac{A}{2}\left(1 - 2V_{n,t_+}\right) + \frac{F}{2}\frac{f_{n,t_+}}{f_{min,t}} < \frac{A}{2}\left(1 - 2V_{n,t_-}\right) + \frac{F}{2}\frac{f_{n,t_-}}{f_{min,t}}$$

$$A > \frac{\frac{F}{2} min(f_{n,t_-} - f_{n,t_+})}{f_{min,t}}$$

Fifth term

This term avoids network capacity overloading.

$$\frac{\partial E}{\partial V_{n,t_+}} = \frac{A}{2}\left(1 - 2V_{n,t_+}\right) + \frac{D}{2} f^u_{n,t_+} + \frac{F}{2}\frac{f_{n,t_+}}{f_{min,t}}$$

$$\frac{\partial E}{\partial V_{n,t_-}} = \frac{A}{2}\left(1 - 2V_{n,t_-}\right) + \frac{D}{2} f^u_{n,t_-} + \frac{F}{2}\frac{f_{n,t_-}}{f_{min,t}}$$

In worst case scenario, $V_{n,t_-} = 1$, $V_{n,t_-} = 0$, $f^u_{n,t_-} = f^u_{n,t_+}$, $f_{n,t_-} = f_{n,t_+}$

$$E > A$$

Second term

Users must not allocate the same type of traffic to different interfaces simultaneously. The rationale behind this is that users are not enabled to handle connections at transport level seamlessly across several interfaces.

The fourth and sixth terms decrease neuron outputs. Considering δ the maximum desired distance to the desired sum value, equilibrium is achieved when $\mid \sum_{n=1}^{N_{net}} V_{n,t} - 1 \mid < \delta$. Considering the worst case scenario:

$$\left|\frac{D}{2} + \frac{F}{2}\right| < \delta B, B > \frac{D+F}{2\delta}$$

Third term

This term must decrease neuron output if $\eta_{n,n'} = 1$.

$$\begin{aligned}\frac{\partial E}{\partial V_{n,t}} = {} & \frac{A}{2}\left(1 - 2V_{n,t}\right) + B\left(\sum_{n'=1}^{N_{net}} V_{n',t} - 1\right) \\ & + \frac{C}{2}\eta_{n,n'}\left(\sum_{t'=1}^{N_{tt}} V_{n',t'}\right)\left(1 - \delta_{n,n'}\right) \\ & + \frac{D}{2} f^u_{n,t} + \frac{E}{2} + \frac{F}{2}\frac{f_{n,t}}{f_{min,t}}\end{aligned}$$

$$\frac{\partial E}{\partial V_{n,t}} > 0$$

Since $B > A$, worst case scenario is $V_{n,t} = 0$, $V_{n',t} = 0$.

$$\left(\sum_{t'=1}^{N_{tt}} V_{n',t'}\right) C > A + 2B - D f_{n,t}^{u} - E - F\frac{f_{n,t}}{f_{min,t}}$$

Therefore $C >> 0$.

Appendix D

Publications Arising from this Work

An optimum network selection solution for multihomed hosts using Hopfield Networks
J. Espi, R.C. Atkinson, D.A. Harle and I. Andonovic,
IEEE Ninth International Conference on Networks, Apr. 2010.

Downlink TCP performance enhancement at handoff for FMIPv6-enabled nodes
J. Espi, R.C. Atkinson, D.A. Harle, I. Andonovic and C. Arthur,
IEEE 21st International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC), Sep. 2010.

Proactive route optimization for Fast Mobile IPv6
J. Espi, R.C. Atkinson, D.A. Harle and J. Dunlop,
IEEE Vehicular Technology Conference, Sep. 2009.

Policy-based multihoming support in the MULTINET architecture
Q. Wang, R.C. Atkinson, J. Espi and J. Dunlop,
Broadband Europe Progress Meeting, Multinet FP Project, 2007.