A Hybrid Network/Host Mobility Management Scheme for Next Generation Networks

Prepared by:

Francis Mphakiseng Masuabi

Supervised by:

Neco Ventura

Department of Electrical Engineering

University of Cape Town

2011

Submitted to the Department of Electrical Engineering in fulfillment of the requirements for the degree of Master of Science in Electrical Engineering at the University of Cape Town

Declaration

I declare that this Masters thesis, *A Hybrid Network/Host Mobility Management Scheme for Next Generation Networks* is my own work. All sources that I have used or quoted have been indicated and acknowledged in the references. This work has not been submitted to any other university for any other degree or examination. *I know the meaning of plagiarism and declare that all the work in the document, save for that which is properly acknowledged, is my own*

.....
Francis M. Masuabi

.....
Date

Acknowledgements

I would like to thank

- Mr Neco Ventura for his supervision and constructive criticism throughout the duration of my research.
- My late grandparents for their encouragement, support and belief in me. *"Ke lebogela tsotle tse le tiretseng mo bophelong baka botle"*
- My parents for their guidance and support as well as Mohohlo Tšoeu for always being there for me in difficult times
- Lastly, Joyce Mwangama , Richard Good and Dean Christakos and all my colleagues in the CRG lab for the interesting chats and constructive criticism which helped produce this thesis material.

Abstract

The Evolved Packet System (EPS) designed by Third Generation Partnership Project (3GPP) is a successor of the Universal Mobile Telecommunications System (UMTS) network developed to provide high data peak rates, lower latencies and enhanced broadband experience. It is a simple flattened network architecture which distributes the processing load across the network. The EPS consists of a radio access technology known as Long Term Evolution (LTE) which uses Orthogonal Frequency Division Multiplex Access (OFDMA) and Single-Carrier Frequency Division Multiplex Access (SC-FDMA) techniques to enable high spectral efficiency for a wide range of converged IP services to be experienced by the user, as well as a packet core network commonly known as the Evolved Packet Core (EPC). The EPC is a packet switched network that links 3GPP defined access technologies such as the Global System for Mobile communication (GSM) and LTE as well as non-3GPP access technologies such as the Worldwide Interoperability for Microwave Access (WIMAX) and Digital Subscriber Line (DSL).

As a consequence of the EPS heterogeneity, mobility becomes a key issue when the user moves between access technologies, thus it becomes important that the EPC provides seamless service continuity to mobile users. Two different mobility protocols were specified by 3GPP to handle mobility at the network layer between 3GPP and non-3GPP networks, namely the network-based mobility protocol Proxy Mobile IPv6 (PMIPv6) and the host-based protocol Mobile IPv6 (MIPv6). These protocols were standardised by the Internet Engineering Task Force (IETF) to solve IP-based mobility management issues. PMIPv6 is a local mobility management scheme designed to manage mobility within an administrative domain whereas, MIPv6 is a global mobility protocol standardised for mobility across administrative or geographical boundaries. Splitting mobility management into local and global mobility as been shown to be more efficient; as a result, PMIPv6 would manage local mobility while MIPv6 manages global mobility.

Given that the EPS is a multi-access paradigm, some networks may support MIPv6 while others support PMIPv6. Now if the user decides to move between an access network that supports PMIPv6 to another that supports MIPv6 or vice versa, the user's IP session continuity may be compromised. Various issues such as home address management, race conditions and security inhibit the user from experiencing a continued service while roaming between different access technologies supporting different mobility approaches. Thus, to solve these issues, the author proposes a hybrid network/host interworking scheme to allow the MN to transition smoothly between different access networks supporting two distinct mobility approaches.

The results reveal that the handover latency and packet loss of the proposed scheme are acceptable and in some cases perform better than the hierarchical and MIPv6 only scenarios. Furthermore, results also show that PMIPv6 performs better than MIPv6 in a localised domain.

From the study, it was concluded that the proposed scheme can enable the MN to move from a PMIPv6 domain to a MIPv6 domain while continuing its IP session without having a large negative impact on the MNs quality of service. Moreover, to further enhance the proposed scheme, more access networks could be considered so that more complex issues can be investigated. The security of the Mobile Access Gateway could be accounted for when the MN transitions between different accesses. Furthermore, the solution could include a MN moving from an IPv4 access network to an IPv6 network i.e. take DSMIPv6 into account.

Glossary

3GPP	Third Generation Partnership Project
AAA	Authentication Authorisation and Accounting
AH	Authentication Header
BU	Binding Update
BA	Binding Acknowledgement
BBERF	Bearer Binding and Error Reporting Function
CBR	Constant Bit Rate
CDMA2000	Code Division Multiple Access 2000
CoA	Care of Address
CoE	Center of Excellence
CN	Correspondent Node
CP	Control Plane
DAD	Duplicate Address Detection
DHCPv6	Domain Host Configuration Protocol version 6
DNS	Domain Name Server
DSMIPv6	Dual Stack Mobile IPv6
ePDN	evolved Packet Data Network
EPC	Evolved Packet Core
EPS	Evolved Packet System
ESP	Encapsulating Security Payload
E-UTRAN	Evolved Universal Terrestrial Radio Access Network
FMC	Fixed Mobile Convergence
FMIPv6	Fast Mobile IPv6
FTP	File Transfer Protocol
GGSN	Gateway GPRS Support Node
GPRS	General Packet Radio Service
GSM	Global System for Mobile communications
GTP	GPRS Tunnelling Protocol
HA	Home Agent
HMIPv6	Hierarchical Mobile IPv6
HNP	Home Network Prefix
HoA	Home Address
HSS	Home Subscriber Service
HSPDA	High Speed Packet Data Access
ID	Identifier
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange

IMS	Internet Multimedia Subsystem
IP	Internet Protocol
IPSec	IP Security
ISDN	Intergrated Services Digital Network
LMA	Local Mobility Anchor
LTE	Long Term Evolution
MAG	Mobile Access Gateway
MIPv6	Mobile IPv6
NeTLMM WG	Network-based Localised Mobility Management Working Group
MME	Mobility Management Entity
MN	Mobile Node
MOBIWAN	Mobility in Wide Area Networks
NIST	National Institute of Standards Technology
NGN	Next Generation Networks
NS-2	Network Simulator -2
OFDM	Orthogonal Frequency Division Multiplex
oTCL	Object-Orientated Command Language
PBU	Proxy Binding Update
PBA	Proxy Binding Acknowledgement
PCC	Policy and Charging Control
PCRF	Policy and Charging Rules Function
PDN	Packet Data Network
PMIPv6	Proxy Mobile IPv6
PLC	Packet Loss Concealment
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RA	Router Advertisement
RAT	Radio Access Technology
RS	Router Solicitation
RTP	Real Time Protocol
SA	Security Association
SAE	System Architecture Evolution
SGSN	Serving GPRS Support Node
S-GW	Serving Gateway
SPI	Security Parameter Index
TCP	Transmission Control Protocol
UCT	University of Cape Town
UDP	User Datagram Protocol
UE	User Equipment
UP	User Plane
UMTS	Universal Mobile Telecommunications System
UTRAN	Universal Terrestrial Radio Access Network
VOIP	Voice over IP
WLAN	Wireless Local Area Network
WIMAX	Worldwide Interoperability for Microwave Access

Contents

List of Figures

List of Tables

Chapter 1

Introduction

Next Generation Networks (NGN) consist of a combination of different but complementary access technologies. To provide users with ubiquitous connectivity across a wide range of networks, requires some interaction among these access technologies. The integration of existing and emerging heterogeneous wireless networks requires the design of intelligent handoff and location management schemes to enable mobile users to switch across access networks and experience uninterrupted continuity anywhere, anytime from any device [1].

An example of an NGN technology is the Evolved Packet System (EPS) which meets two primary objectives. Firstly, to design the Long Term Evolution (LTE) which is a new radio access technology, based on Orthogonal Frequency Division Multiplexing (OFDM) technology which inherently increases data rates, reduces end-to-end latency for real time applications and lowers set-up times when new connections are made [2]. Secondly, to create the Evolved Packet Core (EPC) which is an access independent all-IP core network which compared to 3G UMTS technology, presents a simplified and optimised architecture which makes use of fewer functional nodes in the user plane, designed not only to support Third Generation Partnership Project (3GPP) radio technologies, but also non-3GPP radio access technologies such as worldwide interoperability for microwave access (WIMAX), wireless local area network (WLAN) and code division multiple access (CDMA2000).

A Mobile Node (MN) should be able to traverse between these access technologies without having to disrupt an on-going session or lose connectivity at any point, hence sustaining a predefined quality-of-service (QoS) ubiquitously regardless of the access technology. However, with this heterogeneity, several challenges arise in the choice of network architecture design and mobility protocol [3].

Various studies such as that done by J. Abeille et. al. [4] have established that mobility is more efficient when divided into local and global mobility, where the former

refers to a MN performing a handover within a restricted administrative domain and the latter refers to mobility when the MN moves across administrative or geographical boundaries. Mobile IPv6 (MIPv6) is a mature protocol standardised by the Internet Engineering Task Force (IETF) to maintain IP connectivity everywhere which is more effective when used as a global mobility protocol. However, even though MIPv6 is a well known mature standard for IPv6 mobility support, it suffers from considerable handover latencies, signalling overhead, high packet losses and adds complexity in the MN by requiring an active IPv6 stack. This has led to the IETF standardising more host-based protocols such as Fast Mobile IPv6 (FMIPv6) [6] and Hierarchical Mobile IPv6 (HMIPv6) [7] which are optimisations of MIPv6 with the expectation of improving its performance.

Due to the poor performance of MIPv6 and the added complexity in the MN, the IETF Network-based Localised Mobility Management Working Group (NeTLMM WG) [8] further standardised Proxy Mobile IPv6 (PMIPv6) which is a localised network-based mobility scheme. PMIPv6 is an enhancement of MIPv6 supporting mobility for IPv6 nodes with the help of proxy agents in the network. The functional entities in PMIPv6 are the Local Mobility Anchor (LMA) and Mobile Access Gateway (MAG). The LMA is a topological anchor point for the MN's Home Network Prefix (HNP) and manages the location of the MN. The MAG keeps track of the MN's movements and handles all mobility related signalling on behalf of the MN and as a result, an IPv6 stack is not required in the MN. The main reasons that led to the idea of splitting mobility management into local and global mobility was to keep the same IP address in the mobility domain without involving the MN in any mobility related signalling [5].

One of the significant goals of the EPC is to provide seamless service continuity for multi-mode devices when they move from one radio access technology to the other [9]. Two distinct mobility approaches were specified for mobility between 3GPP and non-3GPP access networks in the EPC, namely the network-based mobility protocol PMIPv6 [10] and host-based mobility protocol Dual-Stack Mobile IPv6 (DSMIPv6)[11], which is a constituent of Mobile IPv6 (MIPv6). The EPC supports PMIPv6 and MIPv6 together, which may cause service interruption. Thus investigations are needed to understand how the protocols interact and how different scenarios can be enabled [12]. Hence, the IETF NetLMM WG has drafted several proposals discussing the interworking between PMIPv6 and MIPv6 [8]. These drafts identify three interworking scenarios: hierarchical interworking scenario, co-existence scenario and the transition scenario [12]. Figure 1.1 illustrates the hierarchical interworking scenario, where PMIPv6 is used as a network-based local mobility management protocol and MIPv6 is used as a global mobility management protocol. MIPv6 manages the MN when it roams across different access networks whereas PMIPv6 manages the mobility within an access network.

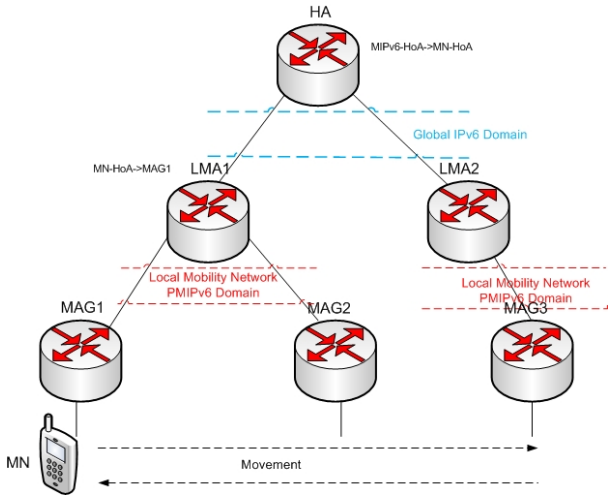


Figure 1.1: Hierarchical interworking scenario

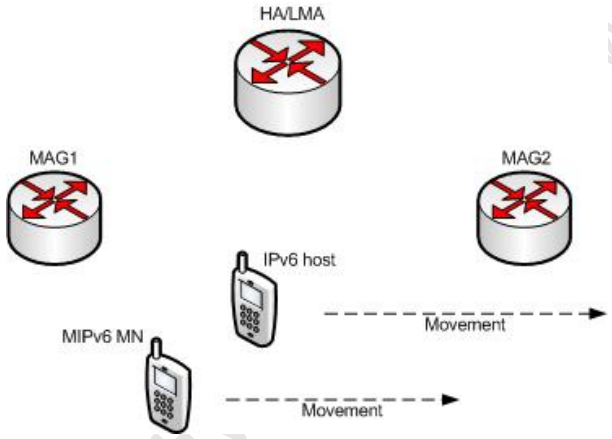


Figure 1.2: Co-existence interworking scenario

Figure 1.2 illustrates the co-existence scenario, where some MNs handle their own mobility by using MIPv6 while others rely on the network to manage their mobility using PMIPv6. The MIPv6 home agent and a PMIPv6 Local Mobility Anchor can be co-located or separate, this will not have an effect on the mobility of the nodes.

Figure 1.3 illustrates the transition scenario where a MN moves between different access networks, some supporting a network-based solution (PMIPv6), while the another supports a host-based solution. Hence, the MN is moving from an access network supporting PMIPv6 to another access network supporting MIPv6. This scenario is similar to the network architecture of the EPC with various access technologies managed by different service providers supporting different mobility management protocols. Furthermore, for the EPS to reach the goal of Fixed Mobile Convergence (FMC), the significance of this scenario becomes imperative. A detailed comprehension of the transition scenario will help provide a good network layer mobility management solution that is independent of the access technology while providing a lot of flexibility to operators.

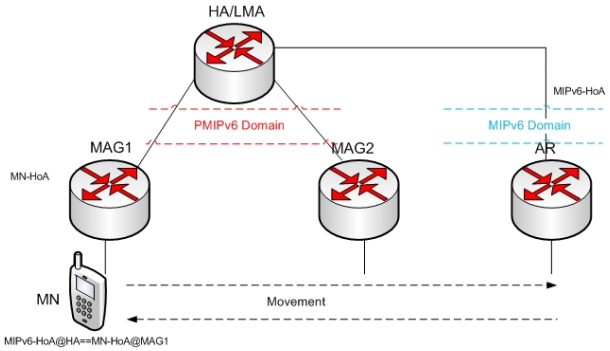


Figure 1.3: Transition interworking scenario

1.1 Problem Definition

This thesis analyses the mobility protocols developed for local and global mobility. It investigates the interworking or interaction of Mobile IPv6 and Proxy Mobile IPv6 in the Evolved Packet System with the aim of providing seamless mobility with efficient quality of service anywhere and anytime. As a result of the heterogeneity in the EPS and the need to provide seamless service continuity for multi-mode terminals, several mobility management challenges need to be resolved. These challenges consists of incompatibility between the mobility protocols supported and addresses being managed by two different entities i.e. the Local Mobility Anchor and Home Agent.

In the transition scenario, a MN moves between an access network that supports PMIPv6 (e.g. LTE) to another access network that supports MIPv6 (e.g. WIMAX) or vice versa, the MN's session continuity may be compromised. PMIPv6 is an enhancement of MIPv6 as it reuses some of its core functionality and messages, thus interworking between PMIPv6 and MIPv6 would appear straightforward and simple. However despite the similarity, several issues discovered in the transition scenario need to be investigated for interworking:

1. Proxy Mobile IPv6 and Mobile IPv6 have compatibility issues since they use different lookup keys to search for binding cache entries.

2. Addresses known by MIPv6 (e.g. Home address) are not necessarily known by PMIPv6, which causes communication problems that lead to dropped IP sessions.

3. If a single binding cache is shared between the Local Mobility Anchor(PMIPv6) and the Home Agent(MIPv6), PMIPv6 registration messages may be deleted by MIPv6 de-registration messages which would discontinue the MN's IP session.

4. Race condition problems may occur due to registration messages being sent by different entities (i.e. MAG and MN). The sequence and arrival of messages is

crucial because packets destined for the MN may not be delivered.

These problems need to be solved to achieve seamless handover when the MN moves among different access technologies.

1.2 Thesis Objectives

As explained in the previous section, heterogeneity brings about several challenges in the choice of network architecture design and mobility protocol. The Evolved Packet System is an all-IP network which supports various radio access technologies and mobility management protocols. Hence, this study investigates the interaction and thereafter, the performance of Mobile IPv6 and Proxy Mobile IPv6 when they are deployed in the same network. The thesis objectives can be summarised as follows:

- Give a theoretical analysis to compare the performances of MIPv6 and PMIPv6 and to investigate their benefits and drawbacks. The comparison would then be used to model a hybrid interworking scheme which allows operators to combine the advantages of network and host-based mobility management.
- Simulate the transition scenario where the MN moves across two access networks, one supporting MIPv6 while the other supports PMIPv6 to identify how the protocols interact.
- Provide a solution for issues identified in Chapter 2 without modifying the initial design of the mobility protocols to allow continuous session mobility.
- Provide a comparative study based on defined performance metrics such as handover latency, end-to-end delay, jitter, packet loss and throughput between the proposed scheme, the hierarchical interworking scenario and MIPv6. Handover latency and packet loss usually occur when a MN moves across subnets causing an interruption of packet flow. During this phase, the MN is unreachable by both the Correspondent Node (CN) and its HA until a binding update message is sent. Hence, the reduction of handover latency and packet loss is significant for real time applications like Voice over IP (VOIP), Video on Demand (VoD) and Internet Protocol Television (IPTV). In addition, various applications are time-consuming due to some network properties such as propagation delay, queueing delay and limited bandwidth. These metrics will be used to determine how the interworking scheme performs.

1.3 Scope and Limitations

The EPC supports other protocols like GPRS Tunnelling Protocol (GTP) however, this study concentrates only on IETF protocols. GTP is a link layer protocol used for mobility between 3GPP networks (e.g. GPRS and UMTS). Link layer mobility solutions for seamless mobility in heterogeneous access networks are complex and since the EPC is heading to an all-IP network, network layer solutions are developed for mobility regardless of the access technology. Thus, this thesis is confined to the network layer for resolving mobility management issues.
To support Fixed Mobile Convergence, various access networks and both IPv4 and IPv6 nodes are supported. However this study only considers IPv6 nodes and the scope is restricted to a homogeneous environment, for example two WLAN networks administered by different network operators. The EPS supports DSMIPv6 which is a constituent of MIPv6. However in this study, with regard to a host mobility protocol, only MIPv6 (IPv6 network) is considered, the IPv4 network is out of the scope of this study.
Due to the nature of the study, the following assumptions have been made:

- Stateful Address Configuration is supported on the home link (PMIPv6) of the MN and because the study is simulation-based, addresses are configured statically.
- The Authentication, Authorisation and Accounting (AAA) server is supported in order to authenticate the MN during the initial attachment to the network.
- The study is restricted to a single HA or LMA. This means that the issue of the wrong HA or LMA after handover is ignored and the security of the MAG is out of the scope of this research.

1.4 Thesis Outline

The remainder of this document is organised as follows:

Chapter 2 provides a theoretical overview necessary to grasp ideas presented in the upcoming chapters. The incorporation of MIPv6 and PMIPv6 in the EPS architecture is discussed thoroughly to understand how different interworking scenarios can be enabled. In addition, various existing papers relevant to this project are observed. These papers provide a good motivation of the study being carried out.

Chapter 3 presents the proposed hybrid network/host mobility management scheme for the Evolved Packet System in order to provide seamless service continuity for multi-mode terminals ubiquitously.

Chapter 4 presents the framework and modelling used to carry out the study. The design of the network topology and mobility aspects are described. In addition, metrics used to evaluate the performance of the proposed work are discussed.

Chapter 5 provides the results as consequence of simulations conducted. The results are thoroughly analysed and contrasted with benchmark schemes, followed by a discussion.

Chapter 6 presents the conclusions drawn from the evaluation of results. Furthermore, recommendations are made for future work to enhance the proposed interworking scheme.

Chapter 2

Literature Review

2.1 Introduction

The Evolved Packet System was designed by 3GPP to link the Internet with mobile communications, combining high speed radio access technologies (RATs) to enable a variety of mobile broadband services and applications to be experienced by operators and end users alike. The standardisation allows interoperability in a multi-vendor operating environment, where nodes from different vendors interwork with each other. As a result of the EPS design requirements, it was evident that IETF-based protocols would play a key role. Given that the EPS is a multiple access paradigm, mobility management becomes significant to ensure that end-users roam about freely in the network, while making use of mobile broadband services. Hence, it became important to support multiple mobility management protocols to handle mobility between 3GPP and non-3GPP networks [37]. Mobile IPv6 is a mature global mobility protocol standardised by the IETF to maintain IP connectivity when the MN moves between subnets. It is a host-based layer 3 protocol that requires the MN's involvement in mobility related signalling. This requires an active IPv6 stack in the MN which induces high handover latencies, signalling overhead and packet losses. PMIPv6 was later standardised by the IETF NETLMM to reduce signalling overhead by using network-based mobility management which does not require the MN's involvement i.e., no IPv6 stack is required in the MN. However, PMIPv6 only supports mobility within a localised domain and lacks support for global mobility. Given that the EPS supports heterogeneity to converge multiple operators, some non-3GPP networks support host-based mobility schemes while others support network-based mobility schemes. Thus a MN can move from a access network that supports a host mobility protocol (e.g. MIPv6) to an access network that supports a network mobility protocol (e.g. PMIPv6); therefore it is the responsibility of the EPC to ensure that IP session continuity is maintained. This chapter will present background information to clearly grasp the fundamental concepts of mobility management. Moreover, MIPv6 and PMIPv6 have

subtle differences which will be presented to illustrate the challenges that occur when there is an interaction between the protocols.

2.2 Background Information

2.2.1 Networking Fundamentals

The EPS incorporates a number of interworking technologies and protocols. Thus to manage the complexity of heterogeneity, the concept of layering is introduced. The functionalities of a network architecture can be grouped according to the Open System Interconnection model (OSI). The OSI model logically sub-divides a communication model into layers to simplify the network architecture design. This hierarchical approach of the OSI stack allows for different protocols to be implemented at each layer. These protocols are independent of each other which allows implementations at specific layers to be changed without affecting the rest of the stack.

Each MN in the Internet has at least one IP address used to locate the MN in the network. The shortage of IPv4 addresses led to the development of IPv6 due to a rapid increase of mobile devices in the Internet, thus solving several limitations found in IPv4 such as the support for extension headers (routing, fragmentation and security). Each IPv6 address consists of a prefix and an interface identifier. The prefix identifies the network subnet the node is connected to, while the interface identifier identifies the interface to which the IPv6 address is assigned. When the MN enters a network for the first time, it bootstraps its MIPv6 or PMIPv6 parameters in order to gain entry. The MN is then required to configure an IPv6 address using a Dynamic Host Configuration Protocol (DHCP). The DHCP can be implemented to support either stateless or stateful auto address configuration. The stateless mechanisms allows the MN to generate its own address by using locally available information as well as information gathered from router advertisements, whereas in stateful address autoconfiguration the MN obtains configuration parameters from a server. The server maintains a database of addresses and keeps track of the address the MN is using. A MN would configure a unique IP address by appending its interface identifier to the prefixes advertised by routers, and to ensure uniqueness of an IP address, duplicate address detection (DAD) is performed defined in the Neighbour Discovery (ND) protocol.

In a wireless environment, a MN typically consists of two attachment points: An Access Point (AP) and an Access Router (AR). An Access Point (AP) or base station is a link layer device that allows connectivity between wired devices and a wireless network. Hence data can be relayed between wireless and wired devices and an Access Router

(AR) provides routing services for one or more APs.

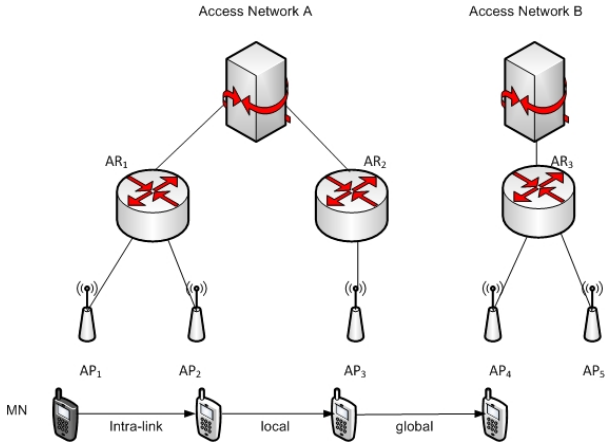


Figure 2.1: Local and global mobility

In most network architectures, mobility is restricted to different domains. Figure 2.1 illustrates a basic reference topology of two access networks. A MN moving between two APs (AP_1 and AP_2) under the same AR represents link-layer mobility which involves layer 2 mechanisms. It occurs between wireless APs within the same link and no IP subnet configuration is needed upon the MN's movement because the link does not change. Mobility between two APs (AP_2 and AP_3) belonging to different ARs constitutes local mobility which typically occurs within an access network. This kind of mobility is restricted within an administrative domain while global mobility occurs when the MN moves between two different access networks (AP_3 and AP_4). Global mobility maintains session continuity when the MN changes access network and it usually spans across administrative boundaries. Examples of protocols that could be supported are GTP, PMIPv6 and MIPv6 for intra-link, local and global mobility respectively.

2.2.2 Host-based Mobility Management

The EPS supports two host mobility management protocols, namely MIPv4 and MIPv6. These host mobility management protocols are mature standards designed to keep the end user connected irrespective of the users location by providing the MN with full responsibility for all mobility related signalling. The MN directly communicates with a router on the MN's home link over the air interface with its IPv6 stack active. Even though host-based mobility schemes exhibit poor performance due to signalling, they play a fundamental role in mobility management. Mobile IPv6 and Dual-Stack IPv6 are discussed thoroughly to expose the underlying differences of the protocols.

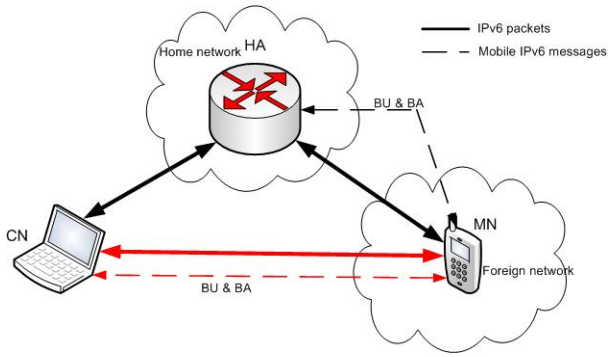


Figure 2.2: MIPv6 Operation

2.2.2.1 Mobile IPv6

Mobile IPv6 (MIPv6) is a network layer mobility protocol, a successor of MIPv4 providing mechanisms to ensure that the MN is always reachable via its home address (HoA) which is a permanent address [13]. MIPv6 contains three functional core entities as shown in Figure 2.2:

- Mobile Node (MN): Which is a IPv6 node that can change its point of attachment and obtain a new IP address as a result of its new location.
- Correspondent Node (CN): Any node that communicates with the MN
- Home Agent (HA) of the MN: Which is a router responsible for intercepting packets and forwarding them to the MN's current location.

The MN is always expected to be reachable using its HoA, which is an IP address configured from the MN's Home subnet prefix on its home link. While the MN is home, all packets from the CN are destined to the MN's HoA. If the MN enters a foreign link, it obtains a Care-of-Address (CoA) which is an IP address configured from the subnet prefix of the foreign link using conventional IPv6 mechanisms such as stateful or stateless address configuration. The CoA represents the MN's current point of attachment (PoA) in the network where the MN is reached when away from home. The association or relationship between the MN's HoA with its CoA is known as a binding. This allows the HA to forward packets to the MN's current location. When the MN is in a foreign network, it registers its CoA with the HA on the home link. This registration is performed by sending a binding update (BU) message to the HA. Upon reception of the BU, the HA responds with a binding acknowledgement (BA) message to confirm receipt of the BU. Thereafter, using neighbour discover mechanisms, the HA intercepts any IPv6 packets destined for the MN's HoA and tunnels them to the MN's primary CoA. The routing of packets where the HA always intercepts packets from the CN is known as triangular routing as shown in Figure 2.2. This mechanism suffers from high delays and as a result,

route optimisation was designed to allow the CN to directly send packets to the MN causing a reduction in delays [13].

Mobile IPv6 provides global mobility i.e. a node can move to any network, however it suffers from high signalling overhead when the MN changes subnets frequently, especially when the CN node needs to be notified. High latencies are also problematic with MIPv6 when the distance between the MN and HA is large. This led to the development of localised mobility protocols such as Hierarchical Mobile IPv6 (HMIPv6) and Fast Mobile IPv6 (FMIPv6). However due to the added complexity in the MN, PMIPv6 was designed to reduce the handover latency experienced by the MN, and to remove any mobility related signalling found in the MN.

2.2.2.2 Dual-Stack Mobile IPv6

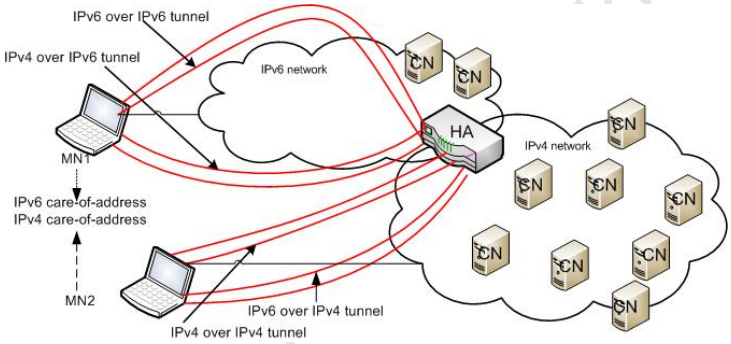


Figure 2.3: Dual-Stack IPv6 operation

Many applications and access networks still support IPv4 only, thus a rapid transition to IPv6 is not possible. Traditional IPv4 nodes and applications need to be accounted for in IPv6 deployments which make dual nodes i.e. nodes supporting both IPv4 and IPv6 important. Dual-Stack Mobile IPv6 is an extension of Mobile IPv6 to allow dual-nodes to move across any network as depicted in Figure 2.3. This means that IPv4 traffic can traverse through an IPv6 tunnel and IPv6 traffic can traverse through a IPv4 tunnel. This requires the MN to have the ability to simultaneously manage both IPv4 and IPv6 home or care of addresses while updating their home agents bindings accordingly [34].

A MN contains both IPv4 and IPv6 home addresses while the HA is a dual stack node connected to both the IPv4 and IPv6 Internet. When MN1 visits an IPv6 foreign network, it configures a CoA and registers it with the HA which it bounds to the MN's IPv4 and IPv6 HoAs. The IPv4 traffic moves through the IPv4 over IPv6 tunnel while IPv6 traffic goes through the IPv6 over IPv6 tunnel. Similarly with MN2, when it moves into an IPv4 foreign network, it configures and registers its IPv4 CoA with the HA. Thereafter,

traffic traverses through the IPv6 over IPv4 tunnel or the IPv4 over IPv4 tunnel. With this process, mobile nodes only require MIPv6 to manage mobility to move within both IPV4 and IPv6 Internet, hence eliminating the need to use two mobility management protocols (MIPv4 and MIPv6) simultaneously [11].

2.2.3 Network-Based Mobility Management

When the MN changes its point of attachment, upon detecting the MN's location, the network provides the same IP address as it had on its previous point of attachment. The network also updates the mobility anchor in order for packets to be routed to the right location of the MN. The key idea here is that the MN keeps its initial IP address while moving across multiple access routers. Thus the mobility is hidden from the IP layer and those above it. The next subsection discusses examples of network-based mobility schemes supported by the EPS i.e. PMIPv6 and GTP [37].

2.2.3.1 Proxy Mobile IPv6

Proxy Mobile IPv6 (PMIPv6) [10] is a protocol designed to enable the network to manage all mobility related signalling without the MN's participation. The core functional entities include the Local Mobility Anchor (LMA) and the Mobile Access Gateway (MAG).
The LMA acts as the home agent of the MN and is a topological anchor point for the MN's Home Network Prefix (HNP) also managing the location of the MN. The MAG's role is to detect the MN movements as well as initiating binding registrations with the LMA. With PMIPv6, the MN need not have an IPv6 stack, since all mobility signalling is handled by the MAG. The basic operation of PMIPv6 is shown in Figure 2.4.

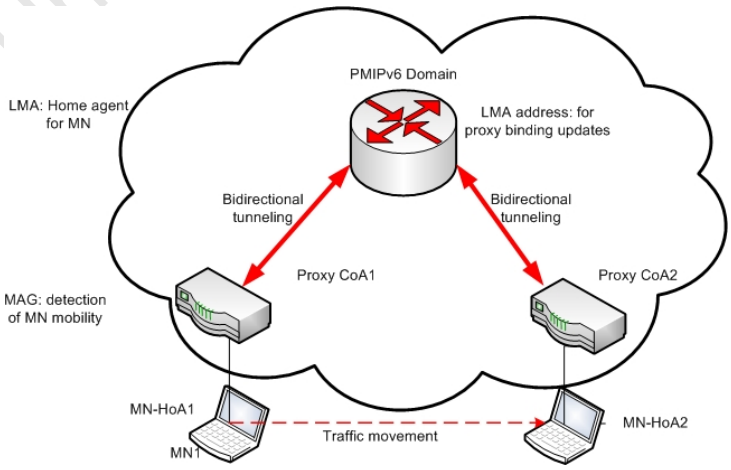


Figure 2.4: Proxy Mobile IPv6 operation

When the MN enters a PMIPv6 domain, the MAG on the access link checks if the MN

is authorised by acquiring its identity. As shown in Figure 2.4, there are three different entities with three different addresses, namely the LMA address, Proxy CoA and the MN HoA. The LMA address is a global address configured to the LMA while the proxy CoA is the global address configured to the MAG which are used as the end point of the bi-directional tunnel established between the LMA and MAG. The tunnel is used to traverse proxy binding update (PBU) messages between the two entities. The LMA views the Proxy CoA as the MN's care-of-address and registers it in the binding cache for that MN. The MN-HoA is the permanent IP address assigned to the MN while it is still attached to the access network. Unlike MIPv6, the mobility entities (i.e. LMA and MAG) may not know the exact home address of the MN instead the HNP is always known.

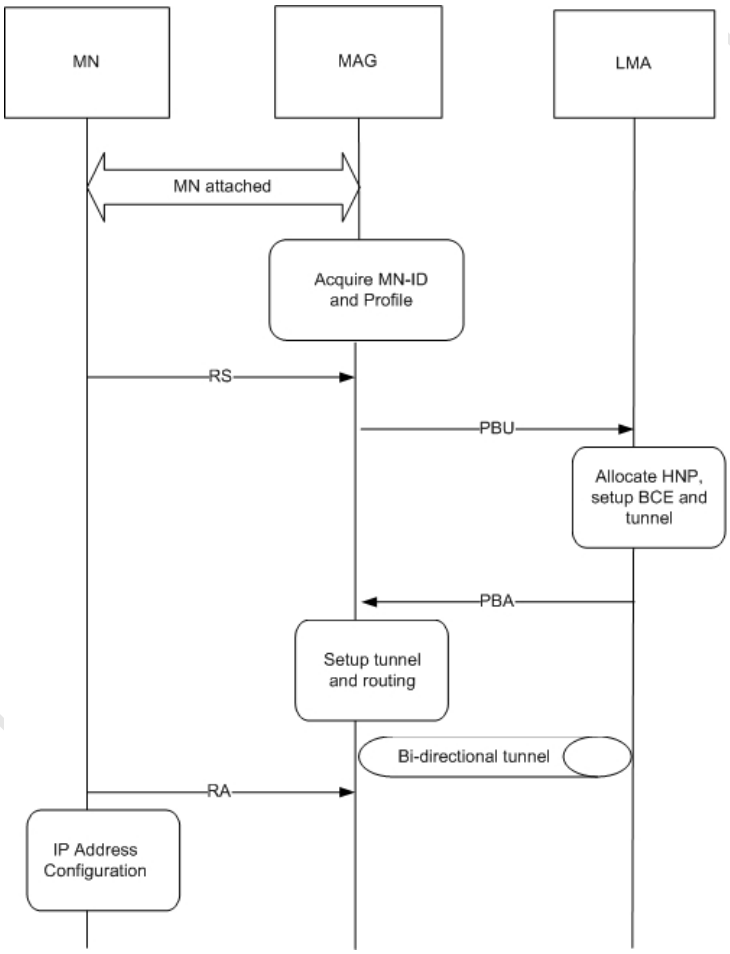


Figure 2.5: Mobile node Attachment

Figure 2.5 illustrates the signal flow of a MN during its initial attachment to a PMIPv6 domain. Upon attachment to the MAG access link, the MN discovers a new attachment by sending a Router Solicitation message (RS) to the MAG. After the MN attaches, the MAG uses the MN-ID and profile to correspond with the AAA (policy server) to authorise the MN. Given that the MAG keeps track of the MN's movement, it sends a PBU to the

LMA for an update on the MN's location. Upon accepting the PBU message, the LMA responds with a PBA including the MN Home Network Prefix (HNP). It creates a binding cache entry and sets up a bi-directional tunnel with the MAG for the transportation of packets. Subsequently, the MAG has enough information for emulating the MN's home link and sends a Router Advertisement (RA) message to advertise the HNP. The MN configures a HoA on its interface using stateful or stateless address configuration modes. After successful IP address configuration, the MN would have a valid address from its HNP at its current point of attachment. This address will from hereon stay the same while the MN is moving within the PMIPv6 domain. Traffic from external networks is sent to the LMA which carries it through the bi-directional tunnel setup with the MAG. The MAG then forwards the packets on its access link towards the MN.

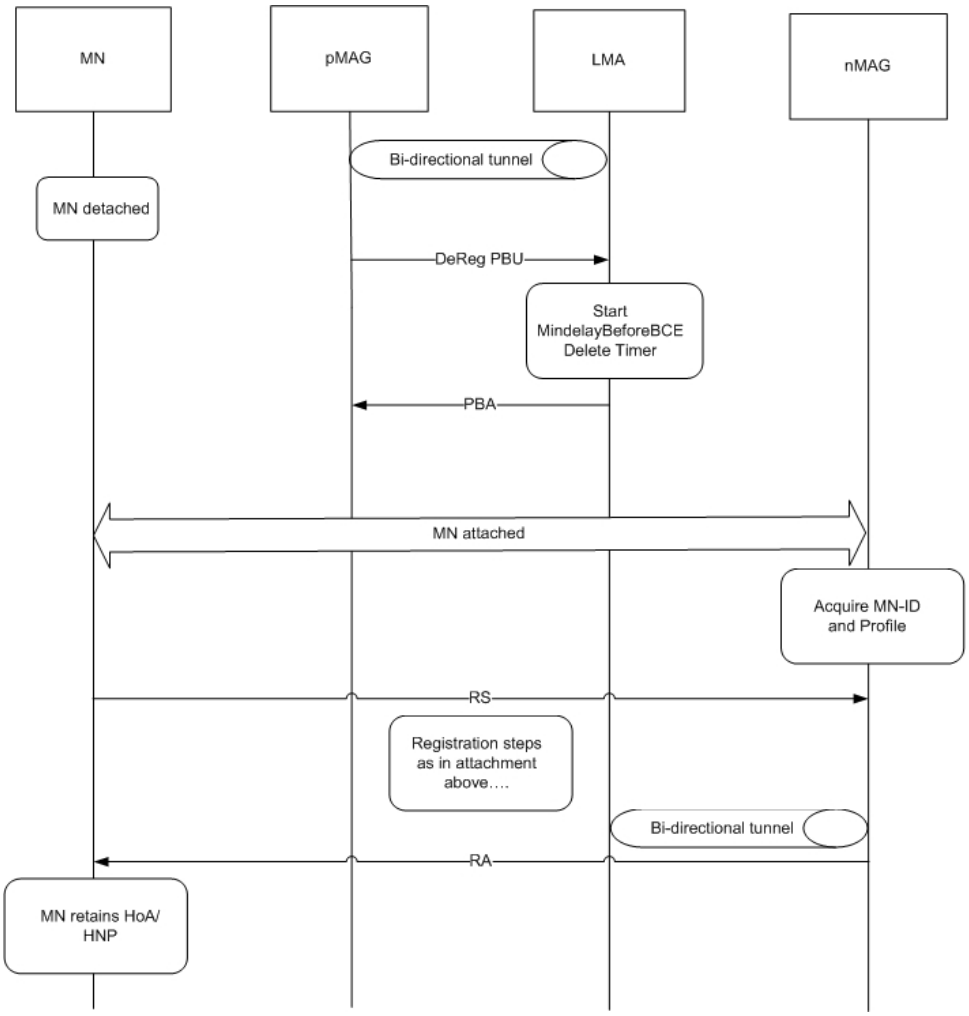


Figure 2.6: Mobile node Handoff

Figure 2.6 shows the signalling call flow of a MN moving between two different MAGs. When the MN switches between MAGs because of reachability or decrease in signal strength with its previous MAG (pMAG), it is important to maintain session continuity. Prior to the MN leaving its pMAG, the LMA uses a timer to update the next MAG

(nMAG) with the MN's profile so that no information is lost during the exchange. After being fully updated, the nMAG continues the MN's session.

2.2.3.2 GPRS Tunnelling Protocol

The GPRS Tunnelling Protocol (GTP) is a link layer protocol developed within GSM standards to handle mobility, bearer management and tunnelling of user data for the General Packet Radio Service (GPRS) network. The protocol was further enhanced for usage in 3G UMTS and has now migrated to the EPS where it is used for mobility between 3GPP networks. GTP can be subdivided into three separate protocols, the control-plane part (GTP-C), user-plane part (GTP-U) and GTP-prime (GTP') which is used for charging [37].

GTP-C is the main control part used within the GPRS core network for signalling between the Gateway GPRS Support Node (GGSN) and the Serving GPRS Support Node (SGSN). It allows the SGSN to activate sessions on behalf of the MN as well as adjusting QoS parameters while managing tunnels for individual terminals.

GTP-U uses tunnelling mechanisms to carry user data within the GPRS core network and between the core network and the radio access network. Packets can be in a form of IPv4, IPv6 or Point-to-Point protocol (PPP). GTP' is used to transmit charging information between charging functions within the GPRS core network.

2.3 Related Work

2.3.1 Comparison between MIPv6 and PMIPv6

Mobile IPv6 is a host-based solution for handling global mobility for hosts in IPv6 networks [44]. This means that every time the MN enters a new IP subnet, the MN requires an active IPv6 stack to register its location. It employs a shared-prefix model in which multiple MNs in the same subnet are configured with the same IPv6 network prefix. Consequently, movement detection and Duplicate Address Detection (DAD) are essential during every subnet change which introduces more delays and hence degrade the performance significantly. Additionally, the MN is reachable globally irrespective of its current point-of-attachment, however three problems have been identified [26]:

- Binding Update Latency: When the HA is located far away from the MN's current location, the binding update message takes a considerable amount of time before it reaches the HA and thus, packets are still sent to the MN's old address. Consequently, these packets are then dropped which results as a waste of resources.

- Signalling overhead: The amount of signalling required when the MN moves between access routers can be large, including configuring a new IP address every time the MN enters a new foreign network. This kind of signalling impacts the networks bandwidth usage and real time services negatively.

- Location privacy: Since the MN changes its CoA every time it enters a new foreign network, this can expose the MN's topological location to the CN which makes the MNs' addresses vulnerable to attacks.

In contrast, PMIPv6 provides a localised network-based solution which employs a per-MN-prefix model. Here each MN is given a unique HNP which they use while in the PMIPv6 domain. As a result, no network layer movement detection and address configuration processes are required while in the localised domain, apart from the initial attachment to the network. Hence, a significant reduction in the handover latency and signalling overhead is achieved which means better performance overall. Unlike MIPv6, where a bi-directional tunnel is established between the HA and MN over the air interface, for PMIPv6, the tunnel is established between the LMA and MAG and which requires no involvement from the MN. This hides the location of the MN from any malicious attacks. K. Kong et. al. [33] proved using qualitative and quantitative analysis the superiority of PMIPv6 over other host-based schemes in a localised domain. Their results show that MIPv6 is most affected by the change in wireless link delay as it requires the largest number of messages while PMIPv6 is the least affected due to the MN's non-involvement in mobility-related signalling. In addition, the delay between the MN and CN does not affect the handover latency of PMIPv6 given that no registration with the CN is required however, for MIPv6, the handover latency increases with the delay between the MN and CN. Lastly, MIPv6 portrays an increase in movement detection delay which results in an increase of handover latency. Having shown that MIPv6 is best suited for global mobility and PMIPv6 for local mobility, this thesis combines the advantages of both protocols for seamless handover in a heterogeneous domain. A summary of the comparison between MIPv6 and PMIPv6 is given in Table 2.1 below.

2.3.1.1 Difference in Message Formats

Proxy MIPv6 reuses most of the core functionality and messages of MIPv6, however despite their similarities there are various differences in the way the protocols are designed. Binding Updates (BU) are sent by the MN with respect to MIPv6 while Proxy Binding Updates (PBU) are sent by the MAG in the case of PMIPv6. Given that these messages are sent by different entities, the format and timing of the messages differ which becomes problematic when the protocols are interworked.

Table 2.1: Comparison between PMIPv6 and MIPv6

Category	MIPv6	PMIPv6
Mobility Scope	Global Mobility	Localised mobility
Functional entity	HA	LMA
Topological entity	AR	MAG
Mobile Node modification	Yes	No
Location registration message	Binding Update	Proxy Binding Update
Relation between tunnel & binding cache entry	1:1 relation	1:m relation
Tunnelling over wireless link	Required	Not required
Router Advertisement type	Broadcast	Unicast
Lookup key in binding cache	HoA	MN identifier
Addressing model	shared-prefix model	Per-MN-prefix model
Supported link type	Any type of link	Point-to-point link
Route Optimisation	Supported	Not supported
Movement Detection	Required	Not required
Duplicate Address Detection	Performed at every subnet	Performed once
Return routability	Required	Not required

A proxy binding update message sent by the MAG is similar to the binding update sent by the MN except from a few additional flags. Every binding update message contains a lifetime and sequence number. Where the lifetime value is a 16-bit unsigned integer which signifies the time remaining before the binding cache entry expires or is deemed invalid. The sequence number is used both by the MN and CN to know the order in which the binding update and/or binding acknowledgement was received. MIPv6 uses the sequence number field as a way to process binding registrations in the order at which they were sent by the MN. It is the responsibility of the MN and HA to manage a counter over the lifetime of a binding. However, as the MN moves between different MAGs in a PMIPv6 domain and with the absence of context transfer mechanisms in the MAG, the serving MAG is unable to determine the sequence number that it needs to use in the signalling messages. Thus, PMIPv6 opted to use timestamps where the MN will insert the current time at which the message was sent and the receiving node will check that the current timestamp is greater than all stamps received.

The binding cache entries for MIPv6 includes the MN's HoA, CoA, sequence number and lifetime while PMIPv6 cache entry includes the HNP, MN-ID, PCoA and a timestamp for the entry. This implies that the binding cache entries in the HA and LMA for MIPv6 and PMIPv6 respectively are different, which will have a significant impact in the interaction of the protocols.

2.3.2 The Evolved Packet System

3GPP's need to sustain a competitive wireless network, for the years 2010 to 2020, has been the key driver in the standardisation of the Evolved Packet System [2]. An overview of the EPS is presented as well as how PMIPv6 and DSMIPv6 are integrated into the architecture.

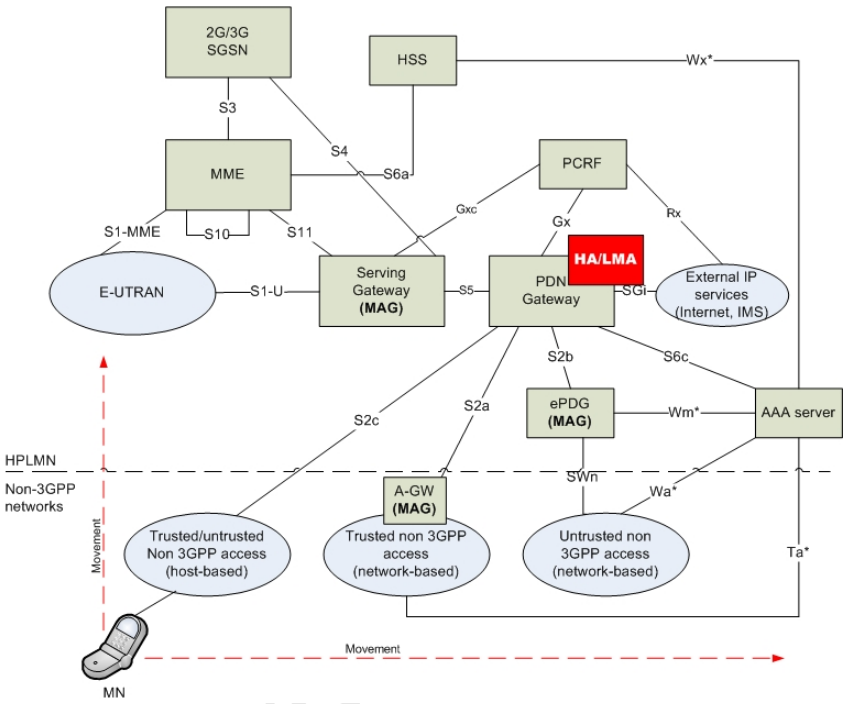


Figure 2.7: The PMIPv6/DSMIPv6-based mobility architecture of the Evolved Packet System

Figure 2.7 illustrates the architecture of the Evolved Packet System. The MN, E-UTRAN and EPC form the IP connectivity Layer which is commonly known as the Evolved Packet System. The IP connectivity layer is only optimised for IP based connectivity where no circuit switched nodes and interfaces are present. The IP Multimedia Subsystem (IMS) is an example of an overlay network that provides services on top of the IP network. For example, to support voice services, the IMS can provide Voice over IP (VoIP) and interconnectivity to legacy circuit switched networks, PSTN and ISDN through Media Gateways it controls [22].

The E-UTRAN consists of eNodeBs connected by the X2 interface in a mesh network and all radio functionality terminates at this node. Its functionality includes performing radio resource management for LTE which includes radio bearer control, radio admission control and scheduling. The Mobility Management Entity (MME) is the main control element in the EPC. It operates only on the Control Plane (CP) and plays no involvement in the User Plane (UP), i.e. user IP packets do not go through the MME. The

main functions performed by the MME include authentication and authorisation, mobility management, management of subscription profiles and service connectivity. The Serving Gateway terminates the S1-U user plane interface towards the eNodeBs and functions as a anchor point during intra-LTE handovers as well as handovers between LTE and other 3GPP accesses technologies. It additionally supports transport level QoS by marking IP packets with suitable DiffServ code points based on the parameters associated with the corresponding packet bearer [37]. The Packet Data Network Gateway (PDN-GW) is a user-plane node which provides IP connectivity to external networks such as the Internet and IMS through the SGi interface. The PDN-GW plays a significant role by operating as an anchor for mobility between 3GPP and non-3GPP networks (such as WIMAX and CDMA2000) and for supporting QoS for IP services provided to the user. Other functions include IP address allocation, packet filtering, charging and policy-based control of user-specific IP flows. The EPS is an all-IP network which means all protocols are transported over IP networks and as a result any messaging between logical entities is over an IP network.

Figure 2.7 also presents the PMIPv6 and MIPv6 functional entities. Over non-3GPP access, host and network-based mobility protocols are supported. The EPS distinguishes between "trusted"and "untrusted"non-3GPP networks. For untrusted networks, the evolved Packet Data Gateway (ePDG) secures the connection by means of an IPsec tunnel between itself and the MN. Given that the EPS supports different mobility protocols in different access technologies, it is the task of the PDN-GW to ensure that IP session continuity is provided. The S5, S2a and S2b are PMIP interfaces which provide tunnel management and user plane tunnelling between the S-GW and PDN-GW, trusted non-3GPP access and PDN-GW, ePDG and PDN-GW respectively. During PMIP mobility, the S-GW and PDG act as MAGs whilst the PDN-GW acts as the LMA. When the MN's parameters have been bootstrapped with the LMA, a bidirectional tunnel is created on the S5, S2a and S2b interfaces in order to relay packets to the MN depending on the location of the MN. Moreover, the S2c interface supports DSMIP which is defined between the MN and the PDN-GW. It provides the user plane with related control and mobility support between the MN and PDN-GW. During DSMIP mobility, the PDN-GW acts as the HA of the MN and the S2c interface provides functionality in order to support tunnelling between the HA and MN for packet forwarding.

2.3.3 Considerations for Interworking PMIPv6 with MIPv6

The Evolved Packet System's goal to achieve seamless macro and micro mobility, requires PMIPv6 and MIPv6 to interact especially for handovers between 3GPP and non-3GPP access networks. Chapter 1 introduced three interworking scenarios where PMIPv6 and

MIPv6 interact. The hierarchical and co-existence scenarios portrayed no significant issues, however the transition scenario, poses several challenges that need to be resolved for seamless handover. The PDN-GW functions both as the LMA and HA in case of PMIPv6 and MIPv6 mobility and for interworking the two protocols, the HA and LMA are required to share a binding cache. However, sharing a binding cache poses problems which impact the service continuity of the MN. The issues that arise are:

- **HoA management and lookup key in the binding cache**
  In MIPv6, the lookup key in the Binding Cache is the Home Address of the MN, it excludes the MN-ID in the Binding Update (BU) Message to the Home Agent as defined by C. Perkins et. al. [13]. However for PMIPv6, the Proxy Binding Update (PBU) contains the MN's Home Network Prefix (HNP) and MN-ID. The HoA is not included in the message as it's not explicitly known by the MAG and subsequently by the LMA. The lookup key for the LMA Binding Cache Entry (BCE) is therefore the HNP or the MN-ID as defined by S. Gundevalli et. al. [10]. This means that the lookup keys for MIPv6 and PMIPv6 registrations are different, which implies that as the MN moves from its home network (PMIPv6 domain) to a foreign network (MIPv6 domain), the BU sent by the MN will not be recognised by the HA as an update of Proxy Binding cache entry which included the HNP and MN-ID. Consequently, a new BU entry is created. If the HA and LMA are implemented as two separate entities, they will not recognise each others binding updates. As a result, the continuity of the session will always be interrupted as a new session will always be created [12].

- **MIPv6 de-registration Binding Update deletes PMIPv6 binding cache entry**
  When the MN moves from a foreign MIPv6 network into a PMIPv6 domain, the MN bootstraps its parameters with the MAG and after successful authentication, it sends a PBU to the LMA. The LMA updates its Cache with an entry including the MAG address and responds with a PBA. The MAG emulates the MN home link and once the MN has detected this, sends a de-registration BU to its HA. It is essential to ensure that the MIPv6 de-registration does not delete the PMIPv6 registration just created by the MAG.

- **Race condition between Binding Update and Proxy Binding Update (Sequence numbers and Timestamps)**
  Re-ordering of registration messages are handled differently for both MIPv6 and PMIPv6. For the former, Binding Update Messages are sent by the MN to the HA and ordered by sequence numbers while the latter uses Proxy Binding Update Messages sent by the MAG and ordered by timestamps. When a MN moves from

an access network managed by MIPv6 to another managed by PMIPv6, the delay incurred in the mobility signalling may have adverse consequences. For instance, when the MN enters a foreign network (MIPv6 domain), the MAG sends a de-registration PBU to the LMA while the MN registers a BU with the HA. If the PBU from the MAG is delayed and is received after the BU from the MN, the LMA wrongly updates the MN's binding update entry as if the MN was still in the home network (PMIPv6 domain). As a result, packets destined for the MN will be lost.

- **Use of wrong HA or LMA after Handover**
  This issue only arises when multiple LMAs are deployed in a PMIPv6 home domain. If the MN moves from a MIPv6 foreign network to a PMIPv6 domain, the MAG should send the PBU to the correct LMA which is collocated with the MN's HA that maintains the active binding cache entry of the MN. If a different LMA is assigned to the MAG, the MN will not be in its home link. The MIPv6 binding will still be active even when the MN moves to another LMA, however the outcome will be undesirable. This also applies when the MN moves from a PMIPv6 to a MIPv6 domain, the MN would have to choose the correct HA.

- **Thread of compromised MAG**
  Both network-based(PMIPv6) and host-based(MIPv6) security associations are used to update the same binding cache entry at the LMA/HA. This could compromise the security of the MAG which would have serious implications on the functionality of the LMA.

2.3.4 Interaction between PMIPv6 and MIPv6

The EPS was one architecture that was identified as deploying MIPv6 together with PMIPv6. These two protocols play a fundamental role in improving mobility management and providing ubiquitous computing to the user. Giaretta et. al. [12] suggested that the MIPv6 home link be implemented as a PMIPv6 domain when interworking MIPv6 and PMIPv6. For mobility between a PMIPv6 domain to a non-PMIPv6 domain, they proposed that the MN establish an IPsec security association with the HA/LMA before the MN sends a BU, as this has a significant impact on the handover latency experienced by the MN. This means that the MN will have an active MIPv6 stack while in the PMIPv6 domain, however it will appear to the MN as if it is attached to the home link. During the security association, the MN discovers the IP address of the HA/LMA using DHCPv6 mechanisms. The network is configured to let the MN discover the same HA/LMA that was serving as the LMA in the PMIPv6 domain to ensure service continuity. The issue of how the MN discovers the correct HA/LMA after handover is out of the scope of this paper, however Gou et. al. addresses this problem.

The discovery of the MN's home address and identifier are all bound to a security association, however with respect to the EPCs trusted non-3GPP networks, no IPSec tunnel is needed, the MN merely requires authorisation to access the non-3GPP network.

Lee et. al. [27] proposed an interworking scheme which enables the MN to move from a PMIPv6 domain to a non-PMIPv6 domain and vice versa. Their scheme consists of an integrated functional architecture, a common lookup key and a HNP allocation mechanism. The integrated functional architecture consists of a DHCP function, LMA function and a HA function sharing the same binding cache. The DHCP function is used by the LMA function to discover the MN-HoA since it is not inherently known by the LMA. The common lookup key used in the cache is the MN-HoA and in order to distinguish between the entries, a flag is used. Their results showed that their scheme has the smallest handover latency and highest throughput by comparison with MIPv6 and the hierarchical interworking scenario.
This scheme does not require any special security mechanism, however this implementation was not designed for any specific architecture.

2.3.4.1 Hierarchical interworking scenario

Yan et. al. [51] designed and implemented a Hybrid MIPv6/PMIPv6 based mobility management architecture, where they consider MIPv6 and PMIPv6 for global and local mobility respectively. The proposed scheme is designed to minimise any modification to legacy networks and always guarantee global mobility management without additional latency during the handover process. The proposed network architecture is similar to the HMIPv6/MIPv6 interaction where the MN moves between different PMIPv6 local domains assisted globally by MIPv6 as shown in Figure 2.8. The HA logically coexists with the LMA (hLMA/HA) and the AAA server is deployed in each domain to provide the necessary authentication and information storage.

From the network topology, the MN moves from the visited local mobility domain (vLMD) to the home local mobility domain (hLMD). The MN is initially attached to MAG1 and a bi-directional tunnel is established between vLMA and MAG1. Subsequent to the tunnel, the HNP is assigned to MN. This new prefix triggers the movement detection of MIPv6 of which a CoA is configured, which is made known to the hLMA/HA. Knowing the MN's HNP and CoA, the hLMA/HA receives packets from the correspondent node and redirects them to the vLMA which is the anchor point of this CoA.

However in this scenario, packets sent to the MN have to be initially directed to the vLMA using the MIPv6 tunnel and then encapsulated in the PMIPv6 tunnel and finally sent

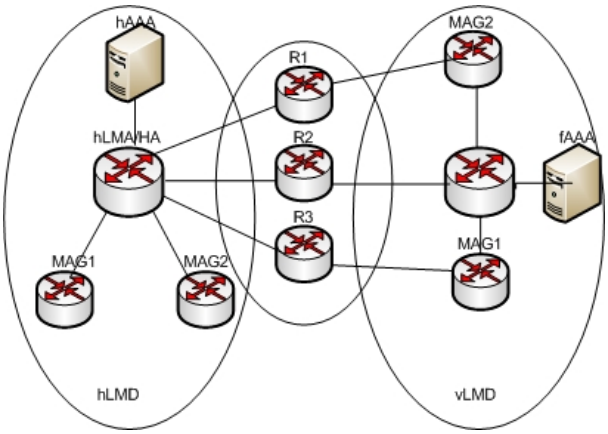


Figure 2.8: Network architecture of Multi-HAs/LMAs on Interaction between PMIPv6 and MIPv6

to the MN. The tunnelling overhead is increased due to the attachment of an additional mobility header at the vLMA prior to the MIPv6 header to enable packets to be delivered to the MAG.
This scenario is a sub-scenario of the hierarchical scenario discussed in Chapter 1. It divides mobility into layers where PMIPv6 is used for local mobility and MIPv6 for global mobility. Due to the similarities the hierarchical scenario has to the transition scenario, it will be used as a benchmark to compare the performance of the proposed scheme.

2.3.4.2 Address Discovery

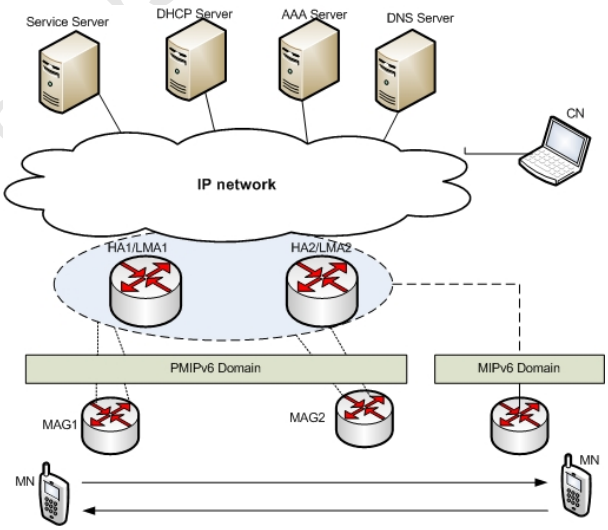


Figure 2.9: Network architecture of Multi-HAs/LMAs on Interaction between PMIPv6 and MIPv6

H. Gou et. al. [16] proposed an address discovery scheme in a MIPv6-PMIPv6 interworking scenario. They consider a network that contains multiple HA/LMAs deployed in

the same network, where the MN moves from a PMIPv6 domain to a MIPv6 domain or vice versa. The key focus of their proposal is to solve the problem of choosing the correct HA/LMA after handover, because if the MN doesn't send BU messages to the HA that is collocated with the LMA which maintains the active proxy binding cache entry, packets destined to the MN HoA will be dropped. The considered network architecture consists of DHCP and DNS servers for address configuration, an Authorisation Authentication and Accounting (AAA) server for authenticating the MN, two different MAGs (MAG1 and MAG2) connected to the LMAs (LMA1 and LMA2) which constitutes a PMIPv6 domain and for the non-PMIPv6 domain which supports MIPv6 consists of a HA1, HA2 and AR as shown in Figure 2.9.

The proposed mechanism introduces two new messages (i.e. HA_Address_Register_req/ HA_Address_Register_rsp and LMA_Address_Req/LMA_Address_Rsp) in every scenario. These messages are included as an option in the authentication messages and given that the MN needs authorisation before acquiring access, this scheme does not add any significant signalling overhead. The HA/LMA is implemented as one node entity which means that the HA and the LMA share the same address, as a result no conflict would occur in providing the same HNP.
The network architecture used is based on an experimental testbed, however no results such as handover latency, packet loss and signalling overhead or the access technologies used have been provided to show how the scheme performs.

2.3.4.3 Proxy Mobile IPv6 indication and discovery

Han et. al. [17] proposed a Hybrid Proxy Mobile IPv6 Indication mechanism that helps to indicate the type of protocol selected by the network or the mobile node while moving from a MIPv6 to a PMIPv6 domain. The main focus of this paper is based on deciding who manages the signalling for a MN that contains a MIPv6 stack when it moves into a PMIPv6 network, either the MN itself or the MAG on behalf of the MN. The scheme uses router advertisement (RA) messages where they modified the Prefix Information option as well as the router solicitation (RS) message. It provides the MN with the responsibility of selecting the preferred mobility management protocol and prefix type without modifying legacy or conventional mechanisms to maintain IP session continuity when the MN moves into a PMIPv6 domain with its IPv6 stack active.

Given that in a PMIPv6 domain, the network manages all mobility related signalling on behalf of the MN and as such, Han et. al. examines mechanisms by which the MN is informed of PMIPv6, as well as means to actively discover such capability in the network. Having to make the MN aware of PMIPv6 support in the access network enables

better decision making in terms of network selection, attach procedure, choice of mobility management, service/session and application configuration abilities [14].

2.4 Discussion

Handover as defined in [56] *"is the process in which the radio access network changes the radio transmitters or radio access mode or radio system used to provide the bearer services, while maintaining a defined bearer service QoS."*
Consequently, handover plays a significant role in the movement of the MN for any cellular system. This chapter, looked at work closely related to the topic of this thesis. It is clear that wireless communications are heading to an all-IP network, where network and application convergence becomes imperative. Such an all-IP network is the Evolved Packet System which is envisioned to provide mobile broadband services with high data rates and reduced delays. The EPS is identified by the author as one of the architectures where MIPv6 and PMIPv6 are deployed together, thus the need to research all possible deployment scenarios where PMIPv6 and MIPv6 are interworked to provide seamless service continuity. Three main interworking scenarios have been identified, hierarchical, co-existence and transition. An example of the transition scenario with respect to the EPS is when a MN moves from a 3GPP network supporting PMIPv6 to a non-3GPP network supporting MIPv6, where several issues arose that compromised session continuity.
The next chapter will propose an interworking scheme that will take full advantage of the benefits of MIPv6 and PMIPv6 to enable seamless wireless communications.

Chapter 3

The Proposed Hybrid Network/Host Mobility Management Scheme

3.1 Introduction

The EPS was designed to allow a common way of accessing PDNs irrespective of the access technology used. This implies that IP address assignment, user subscription management, security, charging, policy control and access to IP networks are managed independent of the access technology used [37]. Hence the EPC permits interworking between 3GPP networks(LTE, HSPDA and GSM) and non-3GPP networks (WLAN, WIMAX and fixed access).

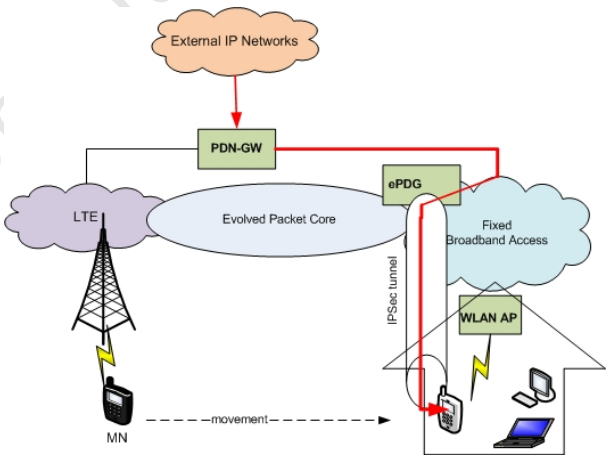


Figure 3.1: Interworking between 3GPP access and non-3GPP access

An example use case scenario is depicted in Figure 3.1. A user has a mobile device that can connect to LTE and WLAN amongst a multitude of other technologies. The user is connected to a LTE network and decides to move indoors. In the house, there is a WLAN AP connected to a fixed broadband network. Depending on a number of prefer-

ences, the device can choose to change accesses from LTE to WLAN. For this reason, the EPS consists of logical entities designed to maintain the user's sessions during handover between two distinct access technologies.
The key logical entity designed to handle mobility in the EPS is the Packet Data Network Gateway (PDN-GW). Mobile IPv6 and Proxy Mobile IPv6 are host and network-based mobility protocols supported by the EPS to provide mobility in IPv6 networks. Therefore, in the used case scenario, the device can either use MIPv6 or PMIPv6 depending on which is supported on the network to switch between the two access technologies. As a consequence of the EPS supporting both MIPv6 and PMIPv6, investigations are needed to comprehend how the protocols would interwork. Due to PMIPv6 being an enhancement of MIPv6, most of the core functionalities and messages of MIPv6 are reused. Therefore, interworking between PMIPv6 and MIPv6 would seem clear-cut without any alteration. However, regardless of their similarities, several issues discussed in chapter 2 developed when the protocols interact.

In order to adhere to 3GPP's design goals for the EPS, all these issues that heterogeneity poses which adversely affect the user's broadband experience need to be resolved. This motivates the significance of this thesis. And seeing that mobility management is efficiently handled by separating local and global mobility, and in addition to MIPv6 and PMIPv6 being the most promising mobility protocols to realise the next generation all-IP mobile Internet, a hybrid PMIPv6/MIPv6 mobility management scheme is proposed to take full advantage of both protocols to enhance the performance of the network.

3.2 EPS non-optimised Handover with non-3GPP networks

As discussed in Chapter 2, the EPC distinguishes non-3GPP networks into trusted and untrusted networks. Untrusted non-3GPP networks are subject to a security mechanism before the MN is granted access into the core network. Internet Protocol Security (IPSec) is the protocol supported by the EPS to provide security for user traffic in the network. It functions at the IP layer providing security services for both IPv4 and IPv6 [37]. Several interfaces in the EPS support IPSec to maintain communication privacy between various entities. For example, the SWu interface uses IPSec to protect user plane traffic between the MN and ePDG as well as the S2c interface which uses IPSec to protect DSMIPv6 signalling between the MN and PDN GW as shown in Figure 3.1.

IPSec makes use of two protocols to provide traffic security namely, Authentication Header (AH) and Encapsulating Security Payload (ESP). The AH provides connection-

less integrity which gives the recipient the ability to detect any modified data, and data origin authentication which allows the recipient to verify the identity of the sender. The ESP provides confidentiality by transforming IP packets using an encryption algorithm so that the packets become unintelligible to third parties. Together both the AH and ESP assist in Access Control by distributing cryptographic keys and managing traffic flows. Security parameters such as keys and encryption algorithms classify communication between nodes. To manage these parameters, IPSec employs Security Associations (SA) defined as the relationship between two entities communicating using IPSec. Each IPSec SA is uniquely recognised by a Security Parameter Index (SPI) as well as a destination IP address and security protocol (either AH or ESP). The SPI is used as a key to index all SAs maintained by IPSec nodes. The Internet Key Exchange (IKE) is used to setup and maintain IPSec SAs between entities. This security mechanism plays a crucial role during handover with untrusted non-3GPP networks because all untrusted non-3GPP networks are confined to using IPSec for authorisation. All user-plane traffic from the PDG-GW traverse through ePDG and then through the IPSec tunnel to the MN. This tunnel protects the DSMIPv6 signalling as well the user traffic between the HA and MN.

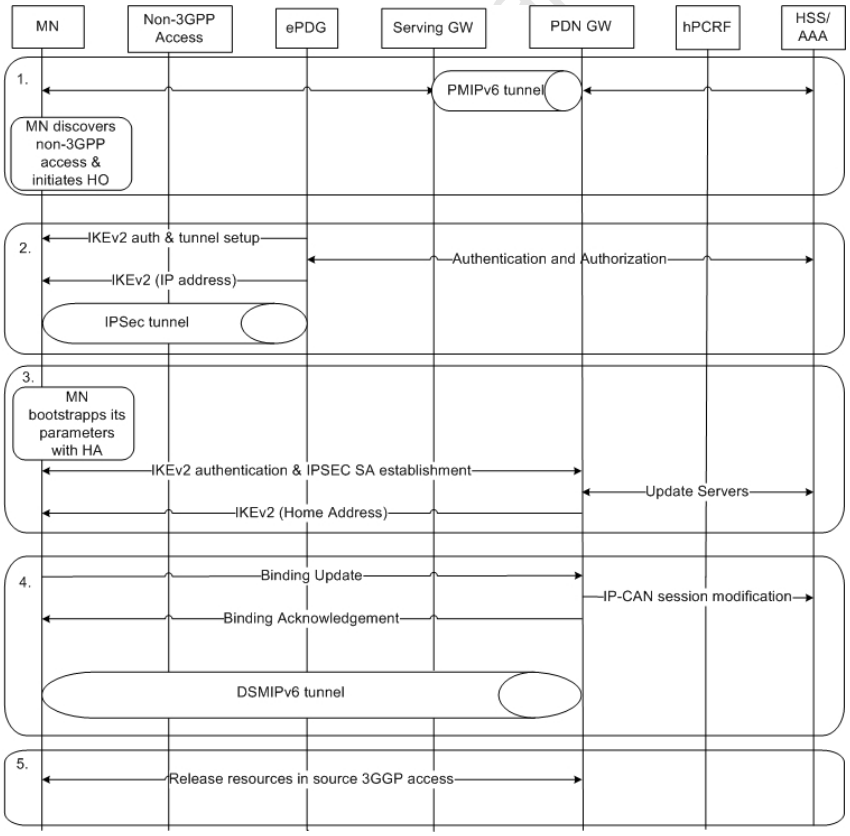


Figure 3.2: Handover from 3GPP access to untrusted non-3GPP access

Figure 3.2 provides a generic overview of the signalling involved when the MN moves from a 3GPP access network to an untrusted non-3GPP network as defined by the 3GPP

Technical Specification [55]. The figure is described in detail as follows:

1. The MN is initially attached to a 3GPP network supporting PMIPv6 and decides to handover the session to a untrusted non-3GPP network.

2. The MN discovers a non-3GPP network (e.g. WLAN) and decides to hand over the session.

3. If the target network is untrusted, the MN should establish the IPSec tunnel towards the ePDG. The MN then initiates an IKEv2 procedure to authenticate and set up an IPSec SA and after successful authentication, a IPSec tunnel is created between the MN and ePDG. In addition, the ePDG allocates a local IP address to the MN.

4. The MN bootstraps its DSMIPv6 parameters, which includes finding the correct PDG-GW which contains the HA functionality. The MN performs a IKEv2 procedure with the PDN-GW to set up an IPSec Security Association for DSMIPv6. The PDN-GW then returns the same IP address the MN had when it was in 3GPP access (MN's home link).

5. Next the MN sends a binding update message to the PDN-GW (Home Agent). The PDN-GW notifies the PCRF of the new access type and responds with a binding acknowledgement message. A bi-directional tunnel is then created between the MN and the PDG-GW in order to continue its IP sessions. Binding update and acknowledgement messages together with the DSMIPv6-tunnelled user plane are transferred within the IPSec tunnel established between the MN and ePDG.

6. To complete the process, the PDN-GW notifies the source 3GPP network that the MN has moved to another network.

This handover procedure only specifies what should happen when the MN moves between two networks supporting different mobility schemes. It does not specify if the PDN-GW combines or separates the binding caches of the HA and LMA nor is it specified how the MN-HoA is maintained when the MN switches networks. All of the identified issues have not yet been resolved, thus further research is required to solve these problems so that all the design goals 3GPP had for the EPS are met.

3.3 Proposed Scheme

To provide seamless mobility between two distinct access technologies supporting different mobility protocols, the proposed scheme consists of a mutual binding cache for the HA and LMA, a HNP allocation mechanism and handover signalling between a MIPv6 domain and PMIPv6 domain. In order for MIPv6 and PMIPv6 to be deployed together, a binding

cache should be shared between HA and LMA. This allows one binding cache entry to be recognised by both entities for each MN. This facilitates seamless session continuity as the MN moves from one domain to another, as both the HA and LMA will be managing the same IP session initiated by the MN. Given that the HNP allocation varies for both protocols, the proposed scheme allows the HA and LMA to allocate the same HoA. All these mechanisms will assist the MN to move between a PMIPv6 domain and a MIPv6 domain without losing the preceding session.

3.3.1 Mutual Binding Cache

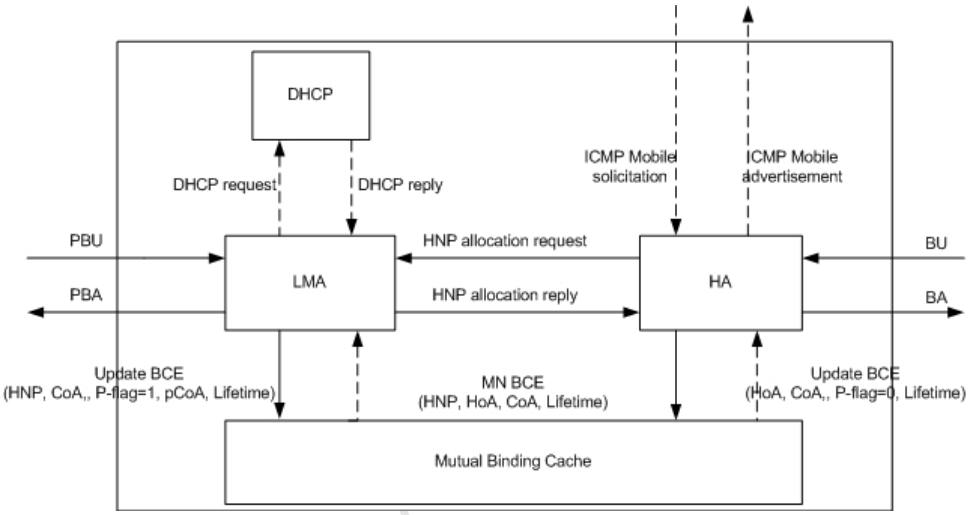


Figure 3.3: Mutual Binding Cache

Untrusted non-3GPP networks are confined to security measures via the ePDG before accessing the core network, whereas in trusted non-3GPP networks the MN merely requires access authorisation from the non-3GPP network concerned. With this in mind, careful consideration must be taken in designing the interworking mechanism for the EPS.
To interwork PMIPv6 and MIPv6, a mutual binding cache is proposed by the author to be shared between the LMA and HA which requires the respective entities to be collocated as shown in Figure 3.3. The functionality of both these entities are included in the PDN-GW. The architecture consists of a combination of a LMA, HA ,DHCP server and mutual binding cache. Seeing that the LMA and consequently the MAG are unaware of the MN-HoA, the LMA requests the MN-HoA configuration from the DHCP server which than responds. Currently, the EPS supports stateless address configuration using a DHCP server [37], however, for the proposed interworking scheme it is suggested that Stateful Address Configuration also be supported on the MN's home link (PMIPv6 domain). This allows the LMA to configure the MN's HoA from the HNP it allocated. Thus, the MAG incorporates the DHCP relay server to support the address configuration. As a result of the LMA having no knowledge of the MN-HoA, the Stateful DHCP server allows the

LMA to configure the MN-HoA and thus the MN-HoA will always be known by the LMA.

During the MN's initial attachment to the PMIPv6 domain, the DHCP server configures the MN-HoA using the MN-ID and interface information. This IP address evidently becomes the MN's HoA which is included in the PBA message to the MAG. The HoA configured to the MN's interface must be the same in the MIPv6 and PMIPv6 domain, which requires an interaction between the HA and LMA to allocate the same HNP as shown in Figure 3.3.

The use of the DHCP server to configure the MN's HoA address is viable when the MN moves into trusted non-3GPP networks.
Given that the security mechanism is inevitable with untrusted non-3GPP networks, to avoid any added signalling overhead, the author of this document proposes that the MN configures its own HoA similar to that used in the previous network in the IKEv2 INTERNAL_IP6_ADDRESS attribute during the IKEv2 exchange with the HA/LMA [15]. Furthermore, as a result of the LMA not knowing the MN-HoA, the configuration of the MN's HoA is handled differently for trusted and untrusted non-3GPP networks.

3.3.2 Common Lookup - key

Given that the LMA and HA are using a mutual binding cache, a common lookup key is required to search the cache for update entries so that the HA and LMA can keep track of the same MN-HoA. Since PMIPv6 is an extension of MIPv6, the Binding Cache Entries are comparable. The lookup key for PMIPv6 is either the MN-HNP or MN-ID whereas for MIPv6, the MN-HoA is used. This implies that the lookup key for PMIPv6 and MIPv6 are different and because of this, when the MN moves from a PMIPv6 domain to a MIPv6 domain, the binding update sent by the MN is not recognised by the HA as an update to the proxy binding cache entry containing the MN's HNP, and as a result a new cache entry is created dropping the previous session. Hence, the author proposes to use the MN-HoA as a common lookup key in the mutual binding cache, because the LMA can configure the MN-HoA using DHCP mechanisms in the initial attachment as shown in Figure 3.3, and consequently, the MN-HoA becomes common to both the HA and LMA which is used as the common lookup key. In order to distinguish between a Proxy Binding Update (PBU) and a Binding Update (BU), a Proxy Registration (P) flag defined in PMIPv6 mobility options is used [10]. The P-flag is set when the binding cache entry is updated by a PBU (PMIPv6) otherwise a BU (MIPv6) is registered.

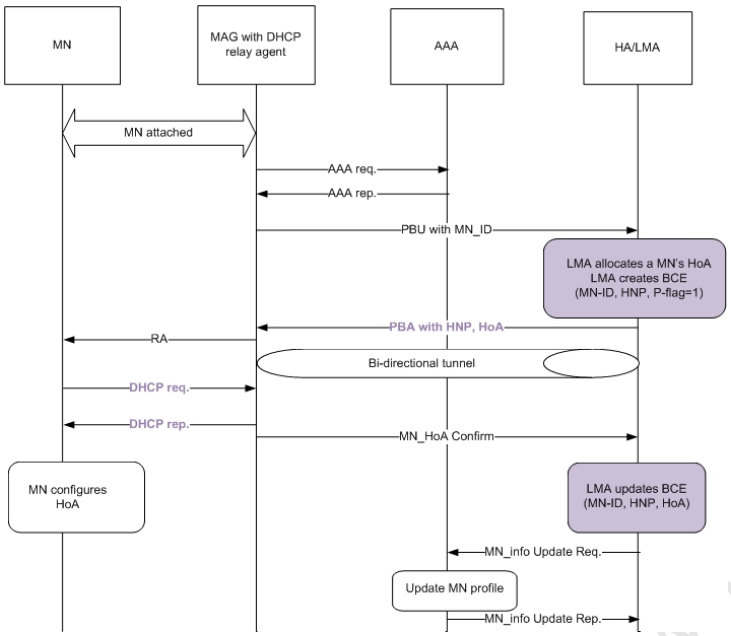


Figure 3.4: Initial attach of MN to PMIPv6 domain

3.3.3 Initial Attachment methodology to PMIPv6 domain

Figure 3.4 illustrates the signalling diagram of the MN as it enters the PMIPv6 domain. The coloured parts of the figure indicate the additional information added by the author. When the MN initially attaches to an access link of a MAG, the MAG authenticates the MN by corresponding with the AAA server. Upon acquiring all the necessary information, the MAG sends a PBU message including the MN-ID to the LMA. Thereafter, the LMA allocates a HNP for the MN and creates a binding cache entry that contains the MN-ID, HNP and the P-flag is set to 1. The LMA configures the MN-HoA and responds with PBA message including the HNP and HoA, plus a bidirectional tunnel is created between the MAG and LMA for the relaying of packets. Upon receiving the PBA message, the MAG emulates the MN's home link and sends Router Advertisement (RA) messages notifying the MN of its HNP and that Stateful IP address configuration is supported. The MN exchanges messages with the DHCP server (MAG with relay agent) to discover the HoA configured by the LMA and for reassurance, the MAG confirms the HoA allocation with the LMA. Lastly, the AAA server is updated with the latest information concerning the MN.

3.3.4 Initial Attachment methodology to MIPv6 domain

The initial procedure when the MN moves into a MIPv6 domain is shown in Figure 3.5. When a MN enters a foreign network, it configures a Care-of-address (CoA) from the foreign subnet prefix. Thereafter, the MN sends a Internet Control Message Protocol (ICMP) Mobile Prefix Solicitation message to the HA. The ICMPv6 is defined to carry

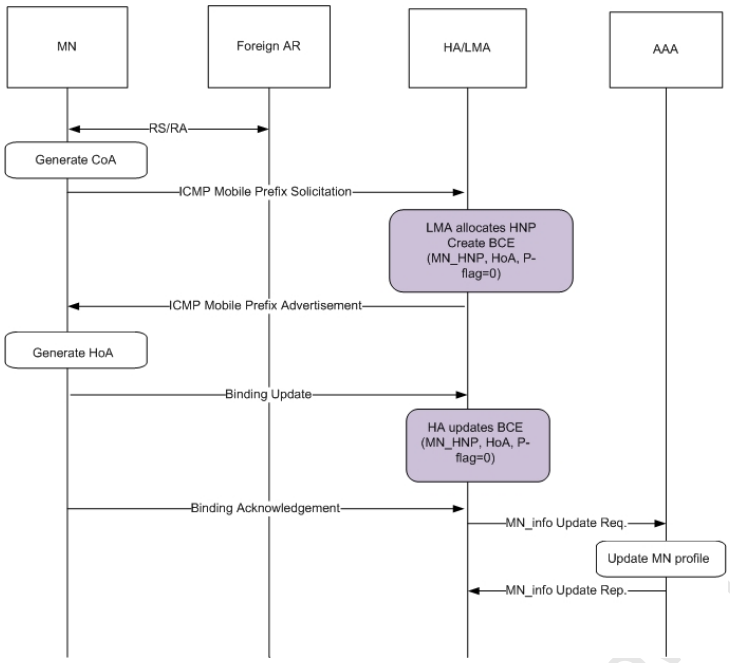


Figure 3.5: Initial attach of MN to MIPv6 domain

IP control messages between network entities. The HA/LMA allocates the HNP and responds ICMP advertisement message which includes the HNP. A temporary binding cache entry is created by the HA/LMA including the HNP. Subsequently, the MN configures a HoA from the HNP and sends a BU to notify the HA of its location. The HA updates the MN-HoA in the binding cache and sets the P-flag to 0. Finally, the AAA server gets updated with the most recent information regarding the MN.

3.3.5 Mobility from PMIPv6 Domain to MIPv6 Domain

Figure 3.6 illustrates the procedure when the MN hands over from a PMIPv6 Domain to a MIPv6 Domain. When the MN initially entered the PMIPv6 domain, the LMA created a Binding Cache Entry setting the P-flag to 1. When the MN moves out of the PMIPv6 domain, a MAG sends a de-registration PBU to the LMA and upon reception, starts a BCE-delete timer as defined by the PMIPv6 standard [10]. Meanwhile, the MN realises that it has entered a foreign network and sends a RS message to the Access Router which replies with a RA message. The MN then sends a registration BU to the HA. Upon reception of the message, the HA is able to find the MN BCE in the mutual binding cache using the MN-HoA as a key, updates the cache and cancels the BCE-timer. The HA responds with a BA and sets the P-flag to 0 while it informs the AAA server of the latest information regarding the MN.

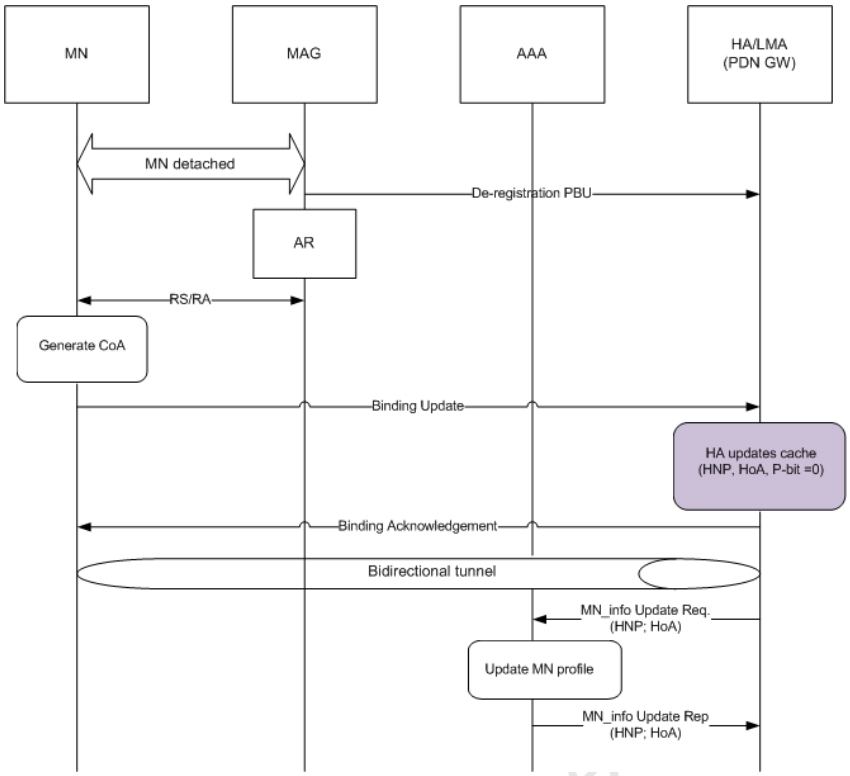


Figure 3.6: Mobility from PMIPv6 Domain to non-PMIPv6 Domain

3.3.6 Mobility from MIPv6 Domain to PMIPv6 Domain

Figure 3.7 below illustrates the signalling when the MN moves between a MIPv6 Domain to a PMIPv6 Domain. When the MN enters a PMIPv6 domain and attaches to a MAG, the MAG tries to authenticate the MN by communicating with the AAA server. Upon the MN's approval, the MAG sends a PBU message to LMA. The LMA replies with PBA which includes the MN's HNP and HoA. Given that a PBU message was sent, the LMA sets the P-flag to 1. Thereafter, the MAG sends a RA message and a bi-directional tunnel between the MAG and LMA is created. As soon as the MN realises that it has moved into its home subnet, it sends a de-registration BU to HA, however the HA ignores this message since the P-flag is already set to 1.

3.4 Discussion

This chapter introduced handover procedures that allow seamless mobility between different access technologies supported by two distinct mobility protocols. A mutual binding cache was proposed by the author to be shared between the HA and LMA. This allowed the two entities to identify the MN's BCE as the MN moved from one domain to another. This implies that the HA and LMA are collocated within the PDN-GW to manage mobility within the EPS. The most significant facet of this proposal is to resume the MN's IP

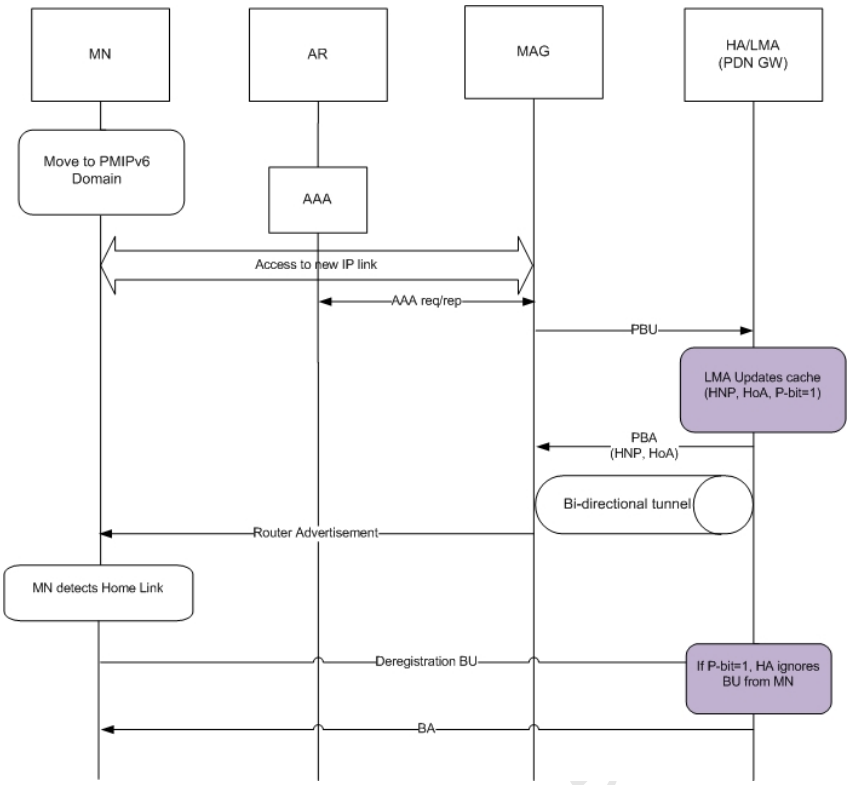


Figure 3.7: Mobility from non-PMIPv6 Domain to PMIPv6 Domain

session from its previous network by keeping the same HoA irrespective of the mobility scheme. To evaluate the performance of the scheme, the author opted to measure handover latency and packet loss as the MN switches between APs because these metrics are significant as they provide quantitative measures that contribute to the quality of service experienced by the user. When these measures are notably elevated, they will affect the overall throughput of the system and for this reason, they should be kept at a minimum to comply with the Evolved Packet Systems standard. The following chapters address the evaluation of this proposal as well as its performance compared to other schemes.

Chapter 4

Network Framework and Modelling

4.1 Introduction

Modelling plays a key role in the design stage to understand how systems work and perform before they are implemented. The model is an abstraction of the system where parameters can be changed, metrics tested and the results fully analysed. Thus, if modelling is performed accurately it could significantly save costs in system development.

The evaluation of the proposed interworking scheme is possibly better modelled in a simulation environment rather than an experimental physical testbed. The reason for this is due to the limitations of an experimental setup. When comparing a network simulation to a physical network testbed, the following conclusions can be made:

- Experimentation has drawbacks of cost and time as they depend on the availability of the hardware, software and further development.
- Using simulation based tools, the scale and complexity of the network is not limited by cost or the availability of resources.
- Simulations are an abstraction of the model and can be used to gain insight into large complex systems by estimating their performance.

It was therefore decided to use a simulator to model the interworking scheme and in order to evaluate the model, performance metrics are defined to analyse the results extracted from the simulation.
This chapter provides the modelling work done for this thesis study to allow multi-mode terminals to roam freely within or across administrative domains. A description of the design and implementation of Mobile IPv6 and Proxy Mobile IPv6 is discussed. Furthermore, the simulation model of the proposed network/host mobility management scheme is specified with the modules used.

4.2 Performance Metrics

Handover in a heterogeneous environment may cause user applications to be disrupted. Seamless handover depends on the mobility solution used as well as movement detection mechanisms available in the network. In order to determine if the users quality of experience was affected during handover, a quantitative analysis is performed. In this section, we define performance metrics which are used during the evaluation of existing scenarios as well as the proposed scheme.

4.2.1 Throughput

LTE networks strive to provide high data rates for mobile users and low end-to-end delays for real time communications. Therefore, it is worth investigating how handover impacts the systems throughput.

Throughput can be defined as the average rate of successful packets transferred in the network. In this thesis, packets will be transmitted using two commonly known transport protocols, namely User Datagram Protocol (UDP) and Transmission Control Protocol (TCP). TCP is a reliable connection-oriented transport protocol [28] which discovers error-prone packets and retransmits them to the receiver in the order in which they were sent. UDP however, is an unreliable transport protocol which does not guarantee the receipt of packets. As a result, an evaluation is made to observe if UDP and TCP throughput is affected by the proposed hybrid network/host mobility management scheme.

4.2.2 Packet Loss

Packet loss represents the number of packets not received by the destination node. Dropped packets could be attributed to network saturation caused by queue overflows as well error-prone packets received by the destination node. The effect of packet loss depends on the application. For example, lost RTP packets used for video streaming may cause synchronisation errors during playback while TCP packets lost in the network layer are retransmitted in the transport layer. Therefore, when a MN moves from one basestation to another, it loses connectivity with the previous basestation and then links up with the next basestation. During this time, the previous basestation would not be able to reach the MN due to loss of connectivity which results in packet loss. This means that handover delay is proportional to packet loss, because the longer handover delay, the higher the packet loss.

4.2.3 Handover Latency

Handover latency is the time the MN loses connectivity from its previous base-station to the time it regains connectivity with the next base-station. The latency also includes movement detection, the decision process, the new address creation/validation if needed and the redirection latency that includes a round trip time with the correspondent node [38]. If the MN is a multi-node terminal, it can still receive or send data packets with the active interface while the other is disabled. High handover latencies have an impact on real time communications as they cause packet loss and transmission delay at the IP layer. Furthermore, it is important to make sure that the proposed scheme does not add any additional delay. In this thesis, only hard handovers (break-before-make) are considered where the MN breaks the connection with the source basestation before the connection to the target basestation is made.

4.2.4 End-to-end Delay

Delay is the time taken for a packet to be successfully transmitted from the sender to the receiver. End-to-end delay is primarily caused by the ratio of propagation delay which is the time taken for the transmission of an electrical signal over optic fibre or copper cables, serialisation delay which is the amount of time needed to transmit an IP packet in a serial manner and queueing delay as a result of network congestion. Certain applications such as FTP transfers are delay insensitive, however VoIP applications are affected by packet delays and reduce the quality of the conversation.

4.2.5 Jitter (Variation of delay)

Jitter is caused when the arrival times of packets vary due to different queueing and processing times. Although the source generates packets at regular intervals (say 20 ms), the destination will typically not receive packets at regular intervals due to the effects of jitter. The general approach of handling jitter is to retain incoming frames in a buffer long enough for the slowest frames to arrive in time, so that they can be played in the exact order in which they were transmitted. VoIP applications are affected by jitter as the time between packets affects the voice at the receiver.

4.3 Simulation Objectives

The main objectives of the simulation are:

- To design a mutual binding cache which is accessed by the HA and LMA independently, which allows the MN to move between different domains (i.e. PMIPv6

and MIPv6) without having to re-establish a session. This mechanism should be implemented without inducing any additional latencies during the handover process. This will be observed when the proposed network/host scheme is compared to Mobile IPv6 and the hierarchical scenario.

- To determine the performance of the Network/Host interworking scheme using the defined performance metrics and comparing the results to the hierarchical and Mobile IPv6 scenarios. All mobility protocol implementations need to be designed according to their respective technical specifications.

4.4 Simulation Modelling

In the event of choosing the most suitable evaluation platform, various simulators needed to be evaluated. The main discrete event simulators namely NS-2 [39], OPNET [40], QUALNET [45] and OMNET++ [52] were considered. Key differences of the aforementioned simulators are summarised in the table below.

Table 4.1: Characteristics of various simulation tools

Factors	NS-2	OPNET 15.0	QUALNET	OMNET++
Cost	Open source	License	License	Free for academics
Programming Language	C++/OTcl	C++	C++	C++
Graphical User Interface	No	Yes	Yes	Yes
IPv6	Yes	Yes	Yes	Yes
Mobility	MIPv4/MIPv6/ PMIPv6	MIPv4/MIPv6	MIPv6	MIPv4

In order to support mobility using different mobility protocols namely PMIPv6 and MIPv6, the ideal simulator should provide the following capability:

Mobility support: A MN must be able to roam freely with the possibility of a handover despite the access network or mobility protocol used.

As seen from Table 4.1, NS-2 is the only simulation tool that supports both protocols. All the other simulators require MIPv6 or PMIPv6 to be implemented which could consume a considerable amount of time. Furthermore, one requires a license to obtain the relevant modules. Compared to other simulators, NS-2 uses open source software which is easier and advantageous given that commercial tools have an access limitation to the code. For all these reasons, NS-2 was chosen as the suitable simulator to use for this thesis.

NS-2 is an event-driven object oriented network simulator which is widely used in academic research. It is supported by two programming languages namely C++ and Object-oriented Tool Command Language (OTcl) linked together using TclCL. The internal mechanisms of the simulation is described in C++ while OTcl configures the network and schedules discrete time events. For this thesis, NS-2 version 2.31 was installed on a Acer Pentium 1.73GHz running Debian Linux 2.6.24, as it contains the necessary modules needed to simulate the proposed scheme.

4.5 Simulation Protocol Design Overview

For the interworking of the protocol extensions, NS-2.31 was used in the experimental setup as it supports basic wireless mobile IPv6 extensions.

4.5.1 Mobile IPv6 Implementation

Dean Christakos [18] and his colleagues from National Institute of Standards Technology (NIST) developed the MIPv6 Module for NS-2.31. This module emulates MIPv6 protocol as standardised in [13]. It consists of the following major attributes:

- **MIPv6Agent**: Controls packet processing by sending and receiving packets to handle mobility. It generates binding messages such as Binding Updates and Binding Acknowledgements.
- **MIPv6 Classifier**: MIPv6-enabled nodes such as the home agent and mobile nodes use the MIPv6 classifier instead of the default hierarchical classifier which is a kind of routing that breaks the topology into several layers of hierarchy, reducing the routing table. It processes packets that need to be re-routed according to the MIPv6 protocol before being routed through the address classifier.
- **Handover class**: This class implements all the necessary functionality needed for handovers to occur. Every time the MN enters a new subnet, the handover class receives a new prefix signifying the MN's change of address.
- **Neighbour Discovery protocol:** Provides Layer 3 movement detection by providing the necessary signalling when the Access Router (AR) is unreachable. The Access Points (APs) periodically sends Router Advertisement (RA) messages and responds to Router Solicitation (RS) messages to the MN informing it of the new network prefix.
- **Packet headers**: A new packet header and packet type have been created for binding updates and acknowledges. These headers are only used for signalling between the MN and the MIPv6Agent which processes all packets.

4.5.2 Proxy Mobile IPv6 Implementation

HyonYoung Choi [21] developed a PMIPv6 module using the NIST mobility package for NS-2.29. It contains the following major objects:

- **LMAAgent & MAGAgent:** These agents emulate the functionality of the LMA and MAG respectively. The LMA provides home network prefixes for the MN. The MAG maintains a binding update list for the MN and performs all mobility related signalling on behalf of the MN.
- **PMIPv6 & IP6Encap packet headers:** A packet header forms part of the packet containing attributes such as packet unique ID and IP address. The PMIPv6 and IP6Encap packet headers form part of binding update messages and encapsulation of IP-to-IP tunnelling of packets from the correspondent node respectively.
- **PMIPv6Src & PMIPv6Dest classifiers:** Classifiers are packet forwarding objects with multiple connecting targets. The PMIPv6Src receives packets and forwards them according to a predefined criterion to the PMIPv6Dest which relays the packets to the MN.
- **PMIPv6Encapsulator & PMIPv6Decapsulator tunnelling objects:** Tunnelling objects are used for data packet encapsulation and decapsulation as packets traverse through the network.

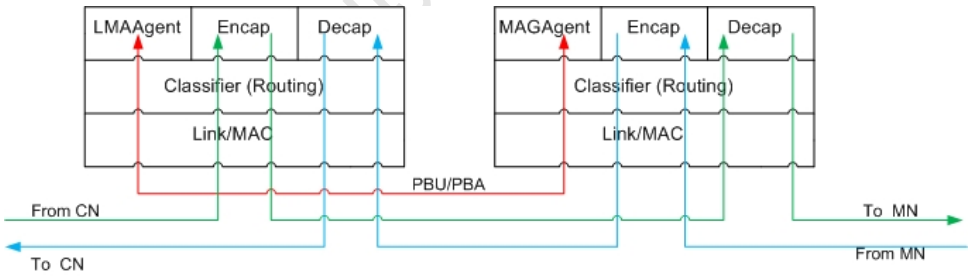


Figure 4.1: PMIPv6 code data process

Figure 4.1 illustrates the process of data as it traverses from the CN to the MN and vice versa. Packets from the CN are encapsulated by the LMA and tunnelled to the MAG through the bi-directional tunnel. Thereafter, the MAG decapsulates the packets and forwards them to the MN.

Note that these two modules are designed for two different versions of NS-2, namely NS-2.29 and NS-2.31 which are significant in modelling the proposed scheme. Therefore, the author of this document ported all the relevant modules from NS-2.29 to NS-2.31. The author chose NS-2.31 as it was more stable and contained the most recent modules.

4.6 Simulation Environment

4.6.1 Wireless Access Network

To support wireless communications and mobility in NS-2, the CMU Monarch Project [47] extended NS-2 with new functional entities at the physical, link and routing layers of the simulation environment. With these entities, nodes could be configured with wireless parameters which provide detailed modelling of wireless subnets and ad-hoc networks. NIST further extended the work done in the CMU Monarch Project by adding more modules to the 802.11 standard. They added beacon messages which are sent periodically at a predefined interval. The APs use these beacons to synchronise the MN's and to make their presence known to them. Connection at the link layer (Layer 2) is also made possible, which is achieved with Association Request and Response messages. These provide the MN with the capability to connect to an AP at Layer 2 or to be rejected by the AP when accessing a network. Evaluations of handovers are required when the mobility of MNs are observed. Thus, NIST made it possible to simulate multiple APs in any given topology where a MN could scan for a specific AP to connect too.

4.6.2 Routing and Address update

Routing of packets is managed differently in NS-2 with respect to wired and wireless nodes. In a wired environment, the routes are statically initialised at the beginning of the simulation and the classifiers are updated accordingly. However in a wireless network, a routing agent dynamically manages packet routes as a result of a change in topology and routing. An example of a routing protocol supported by NS-2 is NOAH which is a protocol that supports direct communication between wireless mobile nodes and base-station nodes.

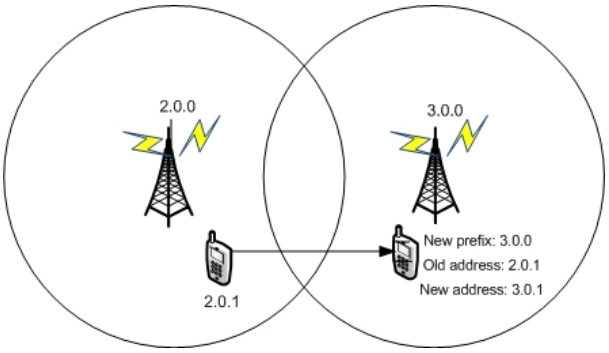
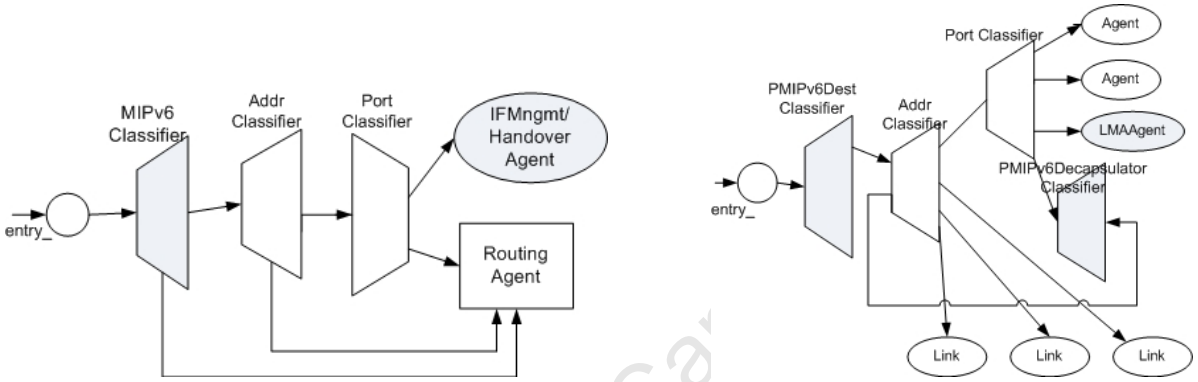


Figure 4.2: Mobile node address change

A wireless topology can change at any given time, therefore as the MN moves between different subnets, the node should be capable of changing its address according to its new

subnet prefix. As a result, NIST modified the NOAH routing protocol so as to reach the MN new address when it switches between APs. Figure 4.2 illustrates the change in address when a MN switches APs. Subsequent to Layer 2 handover, the Neighbour Discovery protocol is used to receive new prefix information from which the MN address is obtained. Thereafter, the node address in the agents located in the MN's are updated as well as the base-station information in the routing protocol.

4.7 Architecture of the Interworking Model



(a) MIPv6 node structure (b) LMA node structure

Figure 4.3: Node architectures of MIPv6 and PMIPv6 capable nodes

PMIPv6 and MIPv6 implementations are independent of each other. This suggests that the HA and LMA with their binding caches are implemented separately. Each protocol has its unique design which entails that incoming packets from the CN are handled differently. Figure 4.3 illustrates the node structure for a MIPv6 capable node and a LMA with respect to PMIPv6. In the Evolved Packet System, the logical entity that handles mobility is the Packet Data Network Gateway (PDN-GW). The PDN-GW is equipped with the functionality of both the LMA and HA to manage mobility within the EPS. Thus to interwork the two protocols, the HA and LMA are collocated and implemented in different nodes sharing the same binding cache as depicted in Figure 3.3 on page 31. With regard to the EPS, the HA, LMA and the mutual binding cache would reside in the PDN-GW. A C++ data structure i.e. a linked list is used to represent the mutual binding cache for the processing of update messages. Packets from the CN are intercepted by either the HA or LMA and forwarded to the current location of the MN.

Due to the added complexity (i.e. active IPv6 stack) of the MN when using the MIPv6 protocol, the MN design is different from that of PMIPv6. Therefore, the author of this document decided to use a multi-interface node depicted in Figure 4.4. A multi-interface node is typically used in a heterogeneous environment to enable the MN to connect to dif-

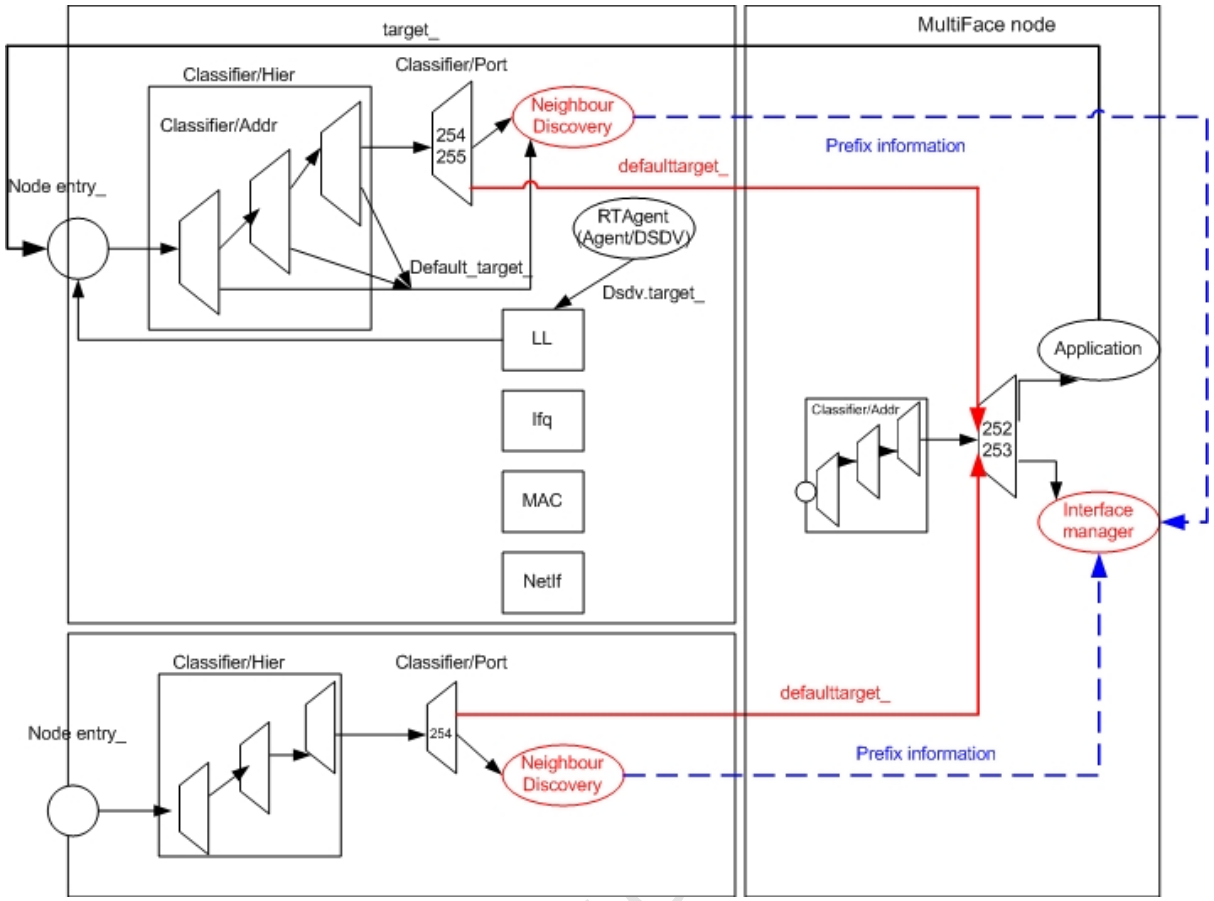


Figure 4.4: Schematic of multi-interface node in NS-2

ferent access technologies. This was advantageous, because when the MN is in a MIPv6 domain, it would use one interface and when it roams into the PMIPv6 domain, the second interface would be enabled while the other is disabled. Thus, the multi-interface node was extended by the author to support PMIPv6.

The multi-interface node was designed as a virtual node linking nodes of similar technology or different technologies [50]. The other nodes are considered as interfaces of the multi-interface node. The Neighbour Discovery agent located in the interface nodes is used for network layer movement detection i.e. new and expired prefixes as the MN changes subnets.

4.8 Simulation Topology

Simulations are performed using the simulation network topology depicted in Figure 4.5. The simulation model consists of a correspondent node (CN) for sending data packets over UDP or TCP to the MN, a HA and LMA for redirecting packets to the MN. Table 4.2 below illustrates the configuration parameters of the nodes when simulations are carried out.

Table 4.2: Configuration of parameters for simulations

Attribute	**value**
Wireless technology	-
Technology	WiFi (802.11b)
Data rate (Mb/s)	11
Link	-
Data rate (Mb/s)	100
Delay (s)	0.03
Application	-
Packet size (bytes)	500
Transport	UDP,TCP
Sender	CN
Mobility	-
Mobility protocol	MIPv6, PMIPv6
Duplicate Address Detection	disabled
RA interval (s)	0.05
MN speed (m/s)	5
Movement direction	Linear

The distance between the access routers including the MAGs is 75m with a coverage area of 50m. All scenarios use the 802.11b technology with a data rate of 11 Mb/s. Due to the limitations of the simulator, the functionality of the HA resides in the AP.

The MN is equipped with two interfaces, one supporting MIPv6 while the other supports PMIPv6. In the simulation model, the MN moves linearly at a speed of $5m/s$ from the HA in the MIPv6 domain to MAG2 in the PMIPv6 domain. Mobile users can move at different speeds which would affect the handover latency experienced by the MN, however the speed of the MN is not the primary focus of this thesis. The MN should be able to switch domains as the speed varies given that the HA and MAG always keep track of the MN's movements.
In each scenario, the access routers send router advertisement messages at an interval of $0.05s$ to the MN. As defined by the MIPv6 standards, the minimum router advertisement (RA) interval is $0.03s$ while the maximum RA interval is $0.07s$ with an advertisement lifetime of $1s$. In order to perform a comparison study between the proposed scheme and other scenarios, the randomness of the RA interval is removed setting the minimum and maximum interval to an average value of $0.05s$.

All the network nodes are connected together using $100Mbps$ links as a representation of an ethernet connection. The link delay of $30ms$ between the network nodes symbolises any effects of congestion due to background traffic, packet queueing and buffering in the link. The MIPv6 module was tested with different link delay values and it was

discovered by NIST[18] that it worked as expected with a link delay of 30ms. Therefore a constant link delay value of 30ms was used in the simulation for both MIPv6 and PMIPv6.

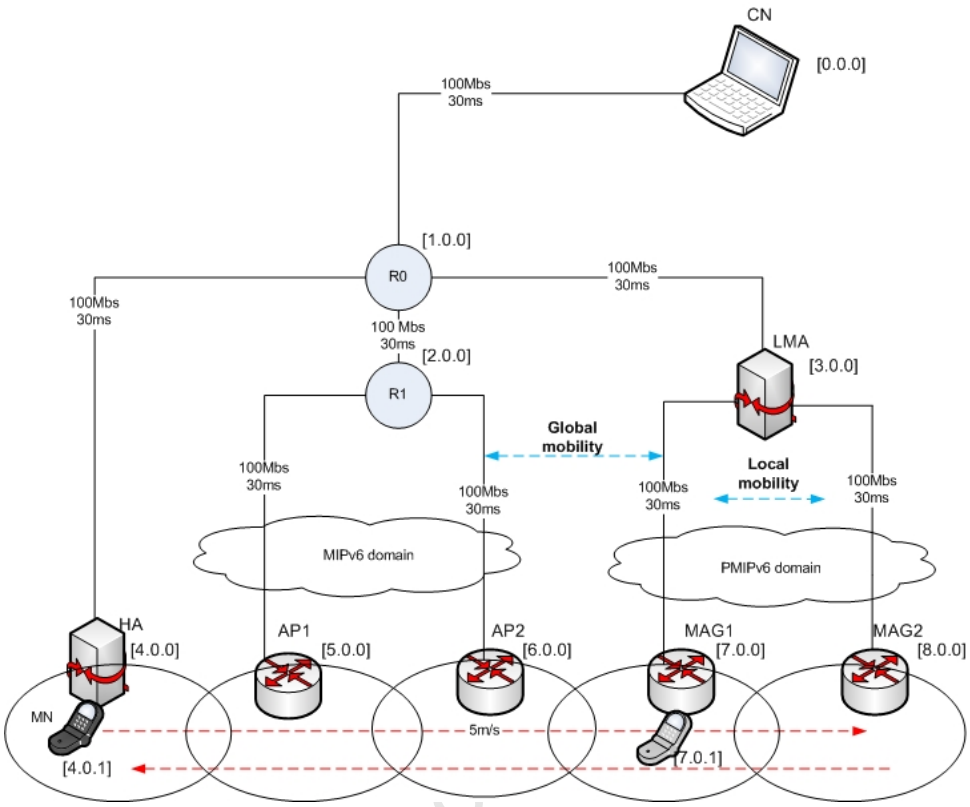


Figure 4.5: Simulation network topology

The CN is equipped with a TCP or UDP source node for transmitting File Transfer Protocol (FTP) or Constant Bit Rate (CBR) packets to the MN which contains the sink agent. The CBR application is configured with a constant data rate of 448kbps and a UDP packet size of 500 bytes which is a representative of a video packet. The average packet size of a video stream and an audio stream differ. Video packet sizes are generally large ranging from 800 to 1500 bytes while audio packet sizes are usually small with sizes of 480 bytes or less [31]. Hence a UDP packet size of 500 bytes was chosen, however a different value could also be used because video packets vary. The data rate (or bite rate) is the number of bits that pass a given point in a network in a given amount of time, usually in seconds. A higher data rate means that the video contains more information resulting in better quality, thus the author assumes that the CN is sending video packets of a good quality.

Initially the MN is attached to the HA and its HoA [4.0.1] is associated with the HA network prefix([4.0.0]). As the MN switches APs it generates a CoA from the AP prefix information as discussed in section 4.5.2. This kind of addressing corresponds to the hier-

archical routing supported in NS-2. Hierarchical routing was devised to reduce memory requirements of simulations over large topologies. A topology is broken down into layers of hierarchy thus reducing the routing table. Given that this simulation is based on a small-scale network and addresses are configured statically before the simulation is run, the implementation of a DHCP server is not required. Every time the MN changes APs, a binding update is sent to the HA or LMA depending on the location of the MN and the MN's routing table is updated accordingly. Furthermore, when the MN moves from a PMIPv6 domain to a MIPv6 domain or vice versa, the traffic from the CN is redirected to the current location of the MN. Either the HA or LMA will encapsulate the packets from the CN and the MAG or MN would decapsulate the packet relative to the MN's present location. As a result, every time a binding update is sent, the mutual binding cache gets updated.

4.8.1 Simulation scenarios

A comparative study is performed to validate the proposed scheme. The hierarchical scenario discussed in Chapter 1 as well as MIPv6 are simulated and compared to the proposed scheme. The hierarchical scenario is similar to the network topology shown in Figure 4.5, however the HA and LMA binding caches are implemented separately.

4.9 Simulation Challenges

NS-2 is a very mature network simulator which is widely adopted in research. However NS-2 is not backward compatible, which means any new modules from newer versions of NS-2 will not function with older versions or vice versa. For example, NS-2.29 contains the NIST mobility package and this package only works for this version. PMIPv6 was developed for NS-2.29, as a result considerations were needed to port the PMIPv6 module to be compatible with NS-2.31. The author successfully ported all NS-2.29 modules to NS-2.31 and therefore all simulations are based on NS-2.31.

In order to support MIPv6, NS-2 includes extensions to study mobility in wide area IPv6 Networks (mobiwan). However this module is obsolete as it was created for NS-2.1b6. Nonetheless, a MIPv6 module from Dean Christakos [18] for NS-2.31 was used for this study. After successfully porting PMIPv6, the author of this document needed to make sure that PMIPv6 and MIPv6 could be run simultaneously on the same simulation script and this was done successfully.

4.10 Discussion

The preceding section detailed how MIPv6 and PMIPv6 were simulated. It was essential to chose the most appropriate simulator to carry out experiments. As such, NS-2 was identified as the simulator that contained all the relevant modules. Therefore the topology illustrated in Figure 4.5 was modelled to closely resemble a real-world mobility scenario with two networks supporting a host or network mobility protocol. The author successfully ported all the relevant modules from NS-2.29 to NS-2.31. The author then developed the mutual binding cache so that messages from MIPv6 and PMIPv6 can be processed. Furthermore, TCL scripts were written by the author to simulate MIPv6 and PMIPv6 simultaneously.

The deployment of MIPv6 and PMIPv6 was identified in the EPS where operators are converging to a single IP core network. Thus, network and service operators would be able to maximise profits by using legacy (e.g GSM) and new access technologies (e.g LTE) while users experience ubiquitous computing at optimum prices.

Using the simulation network model in Figure 4.5 a performance evaluation of the proposed scheme will be conducted using the metrics identified. The following chapter will discuss and thoroughly analyse the results obtained from the simulation model.

Chapter 5

Results and Analysis

5.1 Introduction

This chapter presents the performance of the proposed interworking scheme from the simulation network topology presented in Chapter 4. The results of the proposed scheme are obtained from the performance metrics identified in the previous chapter and compared to the hierarchical and MIPv6 scenarios. The main motivation of the interworking scheme is to allow the MN to roam about freely between a MIPv6 and PMIPv6 domain while continuing its IP session without incurring any additional delays. The mobility framework was tested on real and non-real time applications using UDP and TCP as transport protocols to inspect the impact of handover.

The results shown in this section are for the MN moving from a MIPv6 domain to a PMIPv6 domain. Results for handover from a PMIPv6 domain to a MIPv6 domain can be found in Appendix A.

5.2 Handover Performance Evaluation with Real Time Applications

Real time applications such as VoIP, video conferencing and IPTV are confined to stringent quality of service (QoS) parameters. Such applications are usually grouped into different classes according to their QoS requirements. For example, WiMAX supports a variety of applications with varied QoS parameters. It divides these applications into unsolicited grant service for VoIP, real-time polling service for streaming audio, extended real-time polling service for VoIP with activity detection, non-real time polling service for file transfer protocol (FTP) and best effort for data transfers and web browsing [19]. These real time applications are affected differently by various factors due to the nature

of wireless networks. For instance, delays of up to 150ms and above are detectable by humans and can impair the interactivity of conversations. People are far less tolerant to audio degradation (audio with missing snipits of information i.e. chopped) than video degradation by comparison, thus to meet the stringent QoS requirements, the minimisation of network latency, jitter and packet loss becomes a priority.

The following experiments investigate the performance of the proposed hybrid network/host mobility management scheme when the MN switches between network subnets during a real-time broadband application. The performance of the evaluated scheme is examined using predefined primary metrics: Throughput, handover latency, packet loss, end-to-end delay and jitter.

5.2.1 Handover Latency

An application that closely resembles a real-time application in NS-2 is a Constant Bit Rate (CBR) application. In this experiment, a CBR application is configured with a packet size of 500 bytes which is sent periodically at an interval of 0.05 seconds.

Handover latency for this experiment was determined to be the time difference between the last CBR packet sent by the previous access point to the first packet received by the new access point. Thus, according to the simulation model shown in Figure 4.5, we expect to see four handovers during the simulation of a period of 70s.

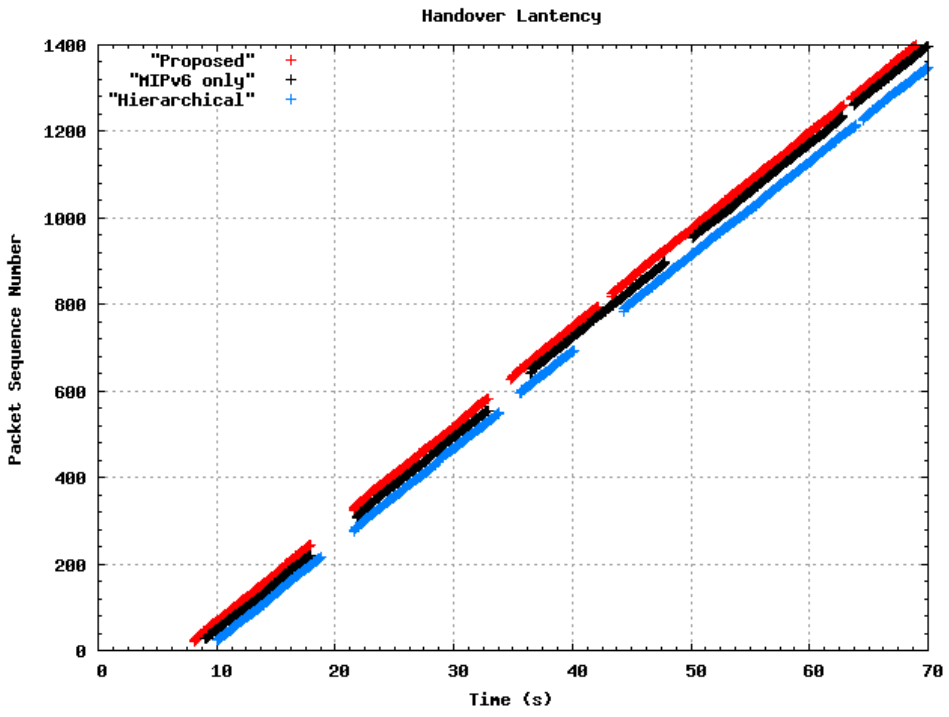


Figure 5.1: Handover delay for CBR application

Figure 5.1 compares the handover latencies experienced by the MN during the simula-

tion among MIPv6, hierarchical scenario and the proposed scheme. The MN is initially in the MIPv6 domain and moves towards the PMIPv6 at a constant speed of $5m/s$. At $9s$, the MN starts receiving CBR packets from the CN. The discontinuities in Figure 5.1 illustrate the handover period during which no CBR packets are received by the MN. The quantitative analysis of the handover latency experienced by the MN is tabulated in Table 5.1. The handover latency in the MIPv6 domain is decreasing due to predictive

Table 5.1: Handover latency (s) between APs

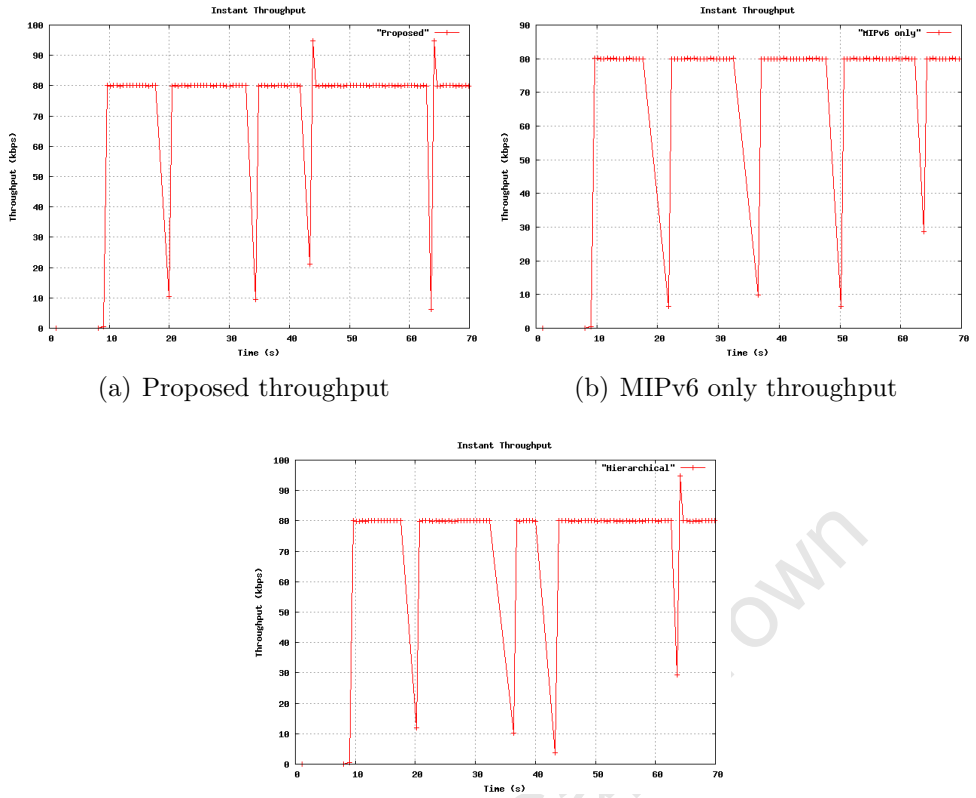
	Proposed Scheme	MIPv6 only	Hierarchical
HA→ AP1	3.66	3.94	2.69
AP1→ AP2	1.98	3.65	1.75
AP2→ MAG1	1.61	2.35	4.16
MAG1→ MAG2	0.652	0.949	0.651

layer 2 mechanisms where the MN anticipates the loss of signal and begins to discover other potential APs. Nonetheless, the handover delay in the MIPv6 domain is longer compared to that in the PMIPv6 domain. The proposed and hierarchical scenarios have shorter latencies of about $0.651s$ in the PMIPv6 domain due to the MAGs immediate location registration which is based on layer 2 triggering. Furthermore, unlike MIPv6, PMIPv6 does not require any movement detection except when the MN initially enters the domain and in addition, the MN keeps the same IP address while roaming in the PMIPv6 domain. All these factors contribute to the reduction of latency in PMIPv6 compared to MIPv6.

A delay of more than $150ms$ in a real-time application such as VoIP becomes detectable and considered unacceptable [24]. From these results, one can see that the proposed, MIPv6 only and hierarchical do not perform adequately enough when the MN is roaming the MIPv6 domain. Furthermore, these results point out the superiority of PMIPv6 over MIPv6 with the significant difference in handover latency.

5.2.2 Throughput

Figure 5.2 illustrates the throughput of the various scenarios over a period of $70s$. As can be seen from Figure 5.2, the MN gets disconnected and loses its signal around $17.8s$, $32.9s$, $42.2s$ and $62.8s$. During these periods, no packets are received resulting in a significant decrease of throughput. The proposed, MIPv6 and hierarchical scenario portray similar throughput patterns with a maximum of $80.0233kbps$. However the average throughput values of the proposed scheme, MIPv6 and hierarchical scenarios are 73.387, 65.954 and 67.813 *kbps* respectively. The proposed scheme has a higher average throughput because of the lower handover latencies experienced when the MN moves between subnets.



(a) Proposed throughput

(b) MIPv6 only throughput

(c) Hierarchical throughput

Figure 5.2: Throughput for CBR application

As can be observed from Figure 5.2, the throughput is adversely affected by the handover latency. An increase in handover latency results in a reduction of average throughput. The mutual binding cache of the proposed scheme does not affect the overall throughput by comparison to MIPv6 and the hierarchical scenario. This implies that the proposed scheme is a viable solution to solving IP session continuity for multi-mode terminals roaming in different access technologies.

5.2.3 Packet Loss

Packet loss occurring in real-time applications affects the quality of service of the application. For example, packets lost during a VoIP conversation causes voice clipping and skips which may be unpleasant , whereas loss in video applications can be tolerable to a certain extend. Real-time packet losses can be classified into random and bursts, where the former describes randomly distributed lost packets over a period of time and the latter defines a cluster or a burst of packets lost during a short period of time. Techniques such as Packet Loss Concealment (PLC) reduce packet loss in VoIP by masking the effects of discarded packets. This technique however, depends on the type of codec used. This experiment will examine packets lost during the handover period when the

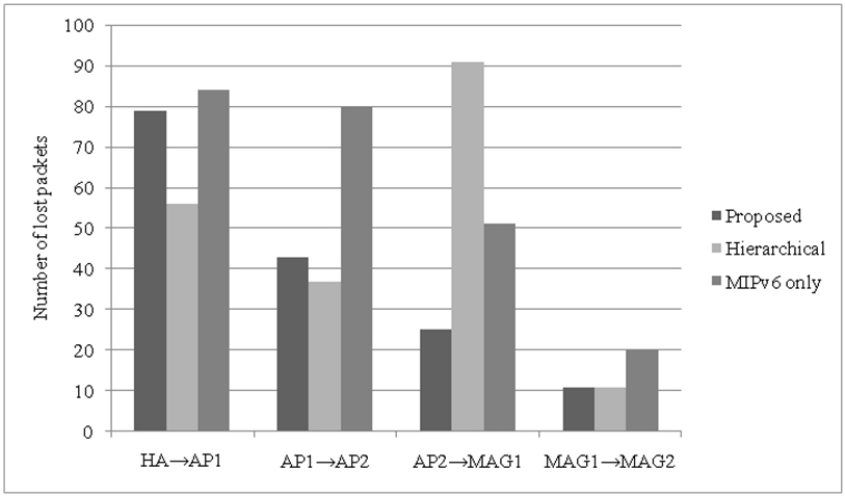


Figure 5.3: Packet loss for CBR application

MN moves between subnets. Obviously during handover, the MNs signal is temporarily discontinued until it can connect to the next AP. During this time interval, no packets are received by the MN as observed in Figure 5.2 with a throughput of $0kbps$. Figure 5.3 depicts and compares the number of lost packets during the handover period. In this experiment, CBR packets are sent uniformly as a result, packets lost during handover should be proportional to the handover latency of the respective scenarios in Figure 5.1. Furthermore, the longer the handover latency the more packets are lost. In the PMIPv6 domain, the packet loss incurred in the proposed and hierarchical scheme has improved by 55 ٪from MIPv6 due to PMIPv6's layer 2 triggering and efficient IP address management. The proposed scheme is comparable to the hierarchical and MIPv6 scenario and in some cases performs better losing fewer packets especially when transitioning between the MIPv6 and PMIPv6 domain (AP2 → MAG1).

5.2.4 Packet Delay

The correspondent node (CN) generates packets which are transmitted to the mobile node via intermediate nodes in the network. In the Evolved Packet System, packets from a source located in an external network are forwarded to the Packet Data Network Gateway (PDN-GW) which routes the packets to the MAGs located in the evolved Packet Data Gateway(ePDG) or Serving Gateway (S-GW) then to the MN with respect to MIPv6 or directly to the MN with regard to MIPv6. As the packets traverse through the intermediate nodes, the end-to-end delay is the total sum of all the delays experienced at each hop on the way to the MN. Thus, the end-to-end delay is the sum of the transmission delay, propagation delay and queueing delay.

Figure 5.4 depicts the end-to-end delay as the MN moves from a MIPv6 domain to a PMIPv6 domain. The end-to-end delay is increases from $0.0919s$ to $0.1812s$ in the

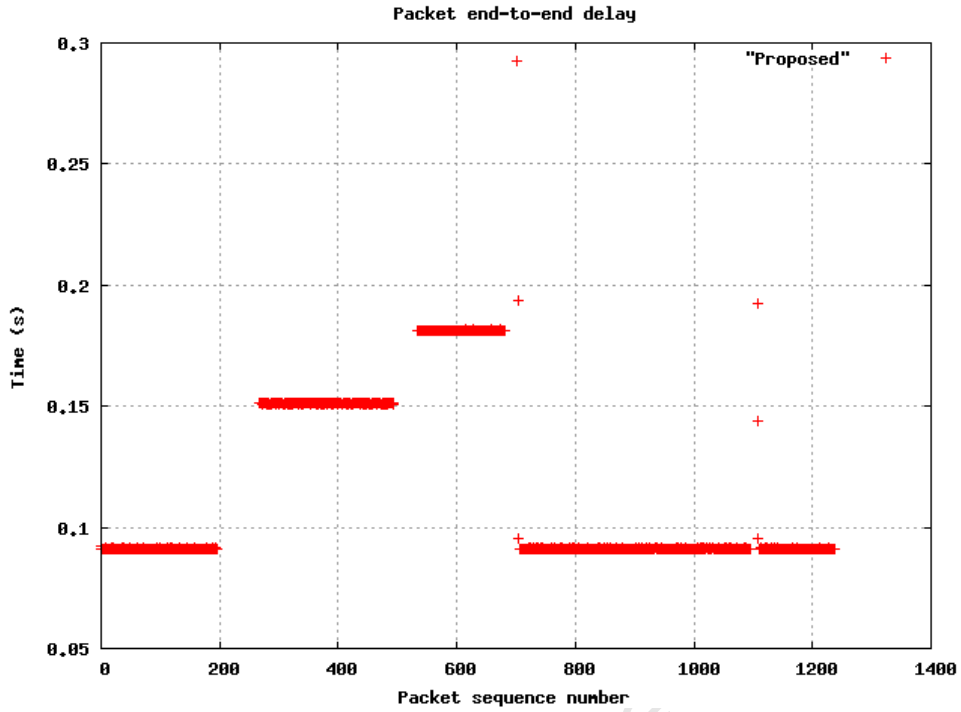


Figure 5.4: Packet end-to-end delay for CBR application

MIPv6 domain and reduces to 0.0908s in the PMIPv6 domain. When the MN is in the MIPv6 domain, packets are routed from the CN to the HA and then redirected to AP1 or AP2 depending on the location of the MN, which causes to the increase of delay in the MIPv6 domain. When the MN is in the PMIPv6 domain, the number of hops from the CN node decreases which results in a reduction of delay. The maximum delay experienced in the proposed scheme is about 0.1812s (181.2ms) which is more than the recommended value of 150ms set by the International Telecommunications Union-Telecommunications (ITU-T) [24]. The delay is primarily caused by triangular routing, where data packets are forwarded to the HA first which in turn redirects the packets to the MN. To avoid the triangular routing in MIPv6, route optimisation can be used where the CN forwards packets directly to the MN.

5.2.5 Jitter

The CN sends packets periodically to the MN, however the rate at which the MN receives the packets may vary. This variation is known as jitter which could be caused by network congestion, improper queueing and configuration errors. Jitter causes transmission errors because packets sent by the source may not be received in the same order at the receiver. Packets would arrive out of sequence which would cause degradation in the quality of the application. In order to compensate for the variation in delay, a jitter buffer can be utilised to temporarily hold the packets and output a steady stream of packets organised

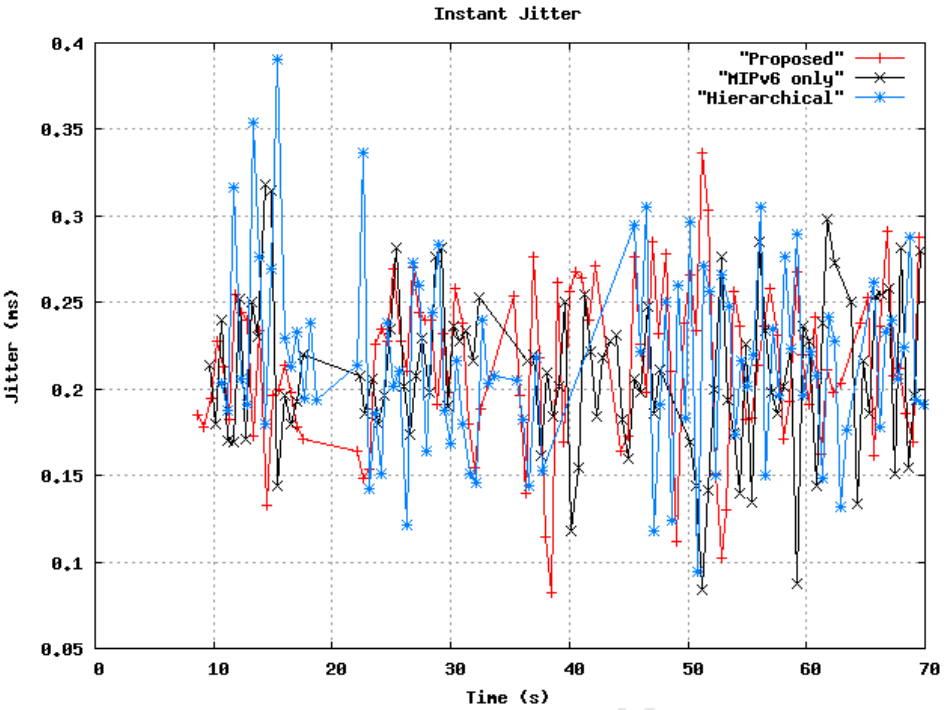


Figure 5.5: Instant jitter for CBR application

in the correct sequence in which they were sent. Furthermore, the size of the buffer is significant because a large buffer adds to the end-to-end delay while a smaller buffer may cause buffer underflows or overflows. With underflows, the buffer is empty when the codec needs to play out samples whereas overflows occur when the buffer is full and packets cannot be enqueued [49]. Therefore the network needs to be carefully analysed so that the desired buffer is designed at the receiver so that packets arrive in the correct sequence at the right time.

Figure 5.5 compares the instant jitter of the proposed scheme at any given time. Thus, in order to observe how the proposed scheme performs, a mean value of the jitter is calculated. The average jitter values calculated are $0.2135ms$, $0.2089ms$ and $0.2168ms$ while the variance is $0.0022ms^2$, $0.0022ms^2$ and $0.003ms^2$ for the proposed scheme, MIPv6 only and hierarchical scenarios respectively. The packets arrive at the MN at an average delay of $0.2135ms$ for the proposed scheme. This means that packets arrive $0.2135ms$ later then expected by the MN. Hence, The results indicate that MIPv6 slightly outperforms the proposed scheme, because in MIPv6, packets are managed only by the home agent. Which means the packets from the home agent are directly sent to the MN. With respect to the proposed scheme, packets are managed by the home agent and the local mobility anchor depending on which network the MN is connected too. The time it takes to switch packet management from the home agent to the local mobility anchor or vice versa contributes to the variation of delay experienced by the data packets. However, comparing the proposed scheme with MIPv6 and the hierarchical scenario it can be seen

that it does not introduce any significant jitter.

It has been shown using extensive testing that voice quality degrades significantly when jitter exceeds $30ms$. Therefore, $30ms$ is the value used as the threshold with respect to VoIP QoS restrictions [49]. According to this threshold, the proposed scheme performs well with an average jitter of $0.2135ms$.

5.3 Handover Performance Evaluation with non-Real Time Applications

Transmission Control Protocol (TCP) is a connection-oriented protocol that connects several network hosts for exchanging data within the Internet. Various Internet applications such as World Wide Web, e-mail, and file transfer rely on TCP for delivery. It prioritises accurate delivery over timely delivery and as a result TCP incurs long end-to-end delays as it waits for the re-transmission of lost packets, and thus, not optimised for real-time applications. TCP uses end-to-end flow control and congestion control mechanisms to manage the speed of data packets from the source. Congestion control is essential for handling network congestion, lossy links and transmission timeouts and also aids to the reliability of TCP. For this experiment, handover latency and average throughput are evaluated as the MN downloads a 5MB file from the CN.

5.3.1 Handover Latency

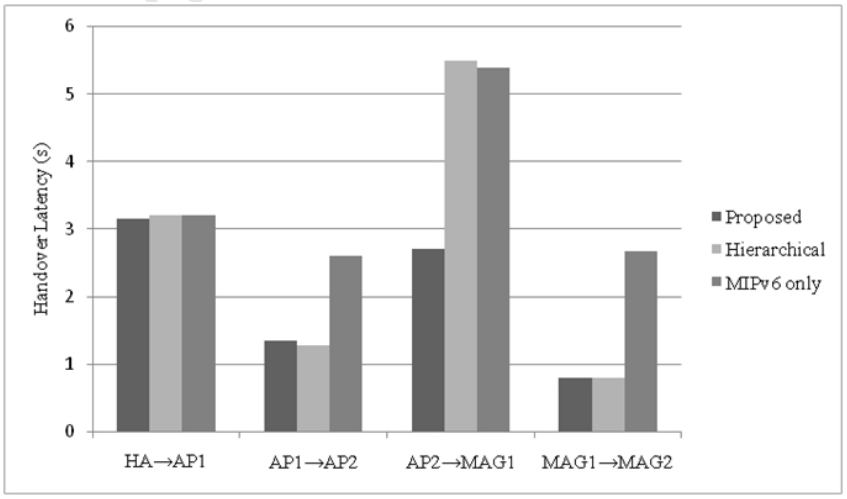


Figure 5.6: Handover delay for FTP application

Figure 5.6 illustrates the handover latency of a file transfer Protocol application using TCP as the transport protocol. As illustrated in Figure 5.6, the handover latency in

the MIPv6 domain is high compared to that of PMIPv6 for all the scenarios due to the time it takes the CN to send packets to the HA and from the HA to the MN (triangular routing). When the MN switches to the PMIPv6 domain (AP2→ MAG1), the proposed scheme performs better with a handover latency of 2.720s. Meanwhile, when the MN is roaming in the PMIPv6 domain, the handover latency has significantly reduced to 0.815s for the proposed and hierarchical scenario due to PMIPv6 addressing properties.

5.3.2 Throughput

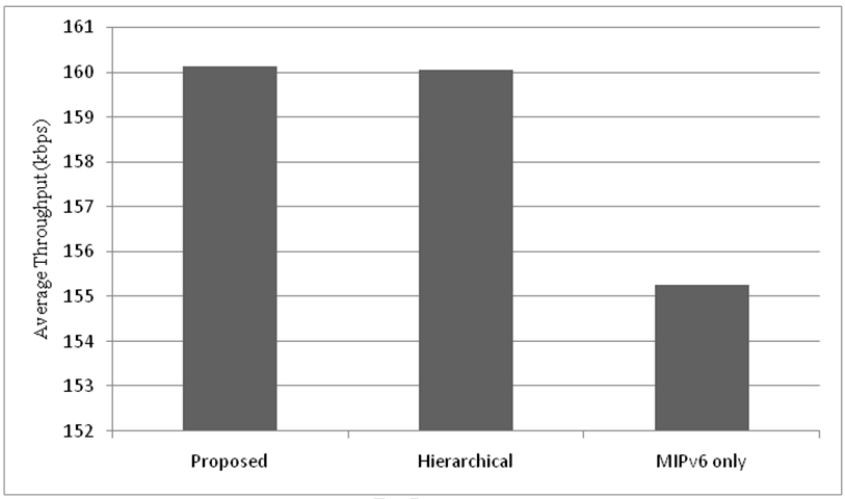


Figure 5.7: Throughput for FTP application

Figure 5.7 illustrates the average throughput of the MN when it moves from a MIPv6 domain to a PMIPv6 domain. The proposed scheme and the hierarchical scenario have the same average throughput of about 160$kbps$ which is more than the MIPv6 scenario with an average throughput of 155.261$kbps$. The average throughput of the proposed scheme and hierarchical scenario is slightly higher due to PMIPv6 scheme which utilises wireless resources efficiently. The advantage of PMIPv6 not involving the MN in any mobility related signalling leads to less signalling traffic over the air interface which avails more bandwidth for user applications, and hence, an increased average throughput for the proposed scheme and hierarchical scenario.

5.4 Results for mobility from PMIPv6 domain to MIPv6 domain

This section illustrates the results obtained when the MN moves from a PMIPv6 domain to a MIPv6 domain. These results are essentially similar to those described when the MN moves from a MIPv6 domain to a PMIPv6 domain, however the MN is moving in

the opposite direction representing mobility from a 3GPP home network to a non-3GPP foreign network with respect to the Evolved Packet System. Figures 5.8, 5.9, 5.10, 5.11 and 5.12 show the handover latency, end-to-end delay, throughput over a period of 70s, lost packets and jitter.

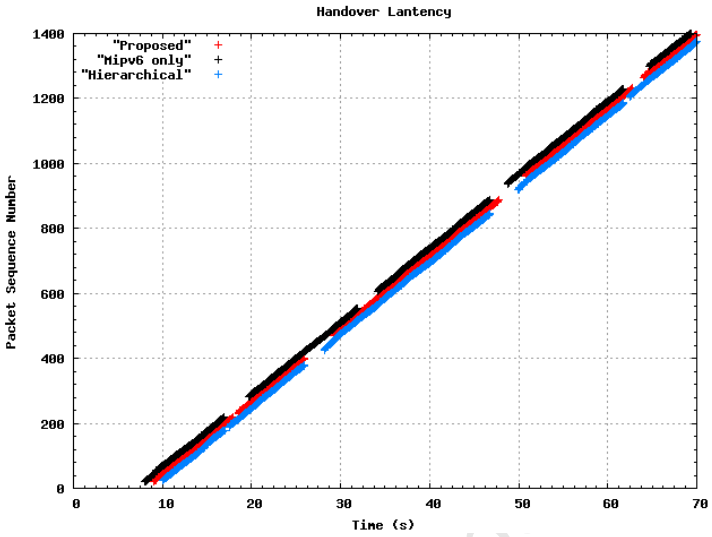


Figure 5.8: Handover delay for CBR application from PMIPv6 domain to MIPv6 domain

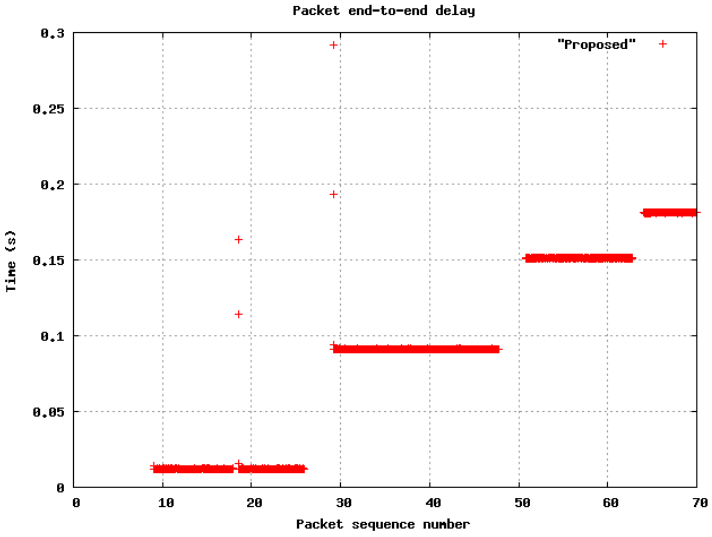
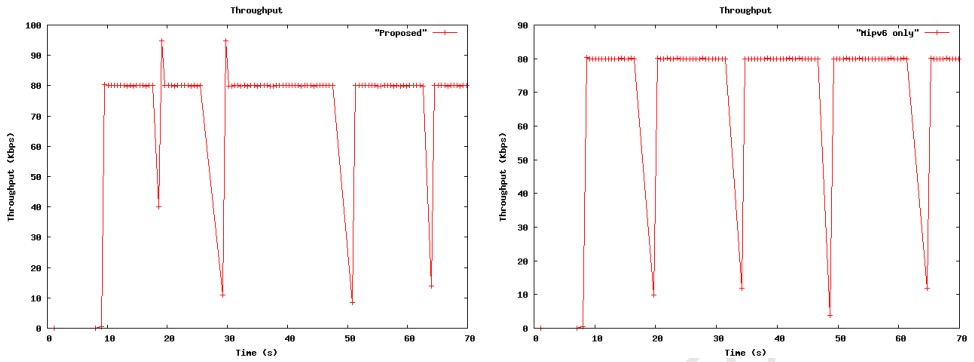


Figure 5.9: Packet end-to-end delay for CBR application from PMIPv6 domain to MIPv6 domain

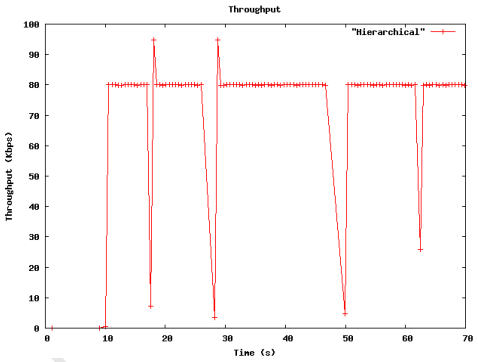
The discontinuities in Figure 5.8 represent the handover latency when the MN switches between subnets. During these periods, no packets are received resulting in high packet losses. The end-to-end delay in Figure 5.9 increases when the MN leaves the PMIPv6 domain. When the MN is in the MIPv6 domain, packets are initially sent to the HA then redirected to the MN which accounts for the increase in delay when in the MIPv6 domain.

Figure 5.10 below illustrates that the maximum throughput achieved when the MN moves from a PMIPv6 domain to a MIPv6 domain. The throughput value of 80.0233$kbps$ is similar to the the throughput recorded when the MN moves from a MIPv6 domain to a PMIPv6 domain. This indicates that throughput is not affected by the direction in which the MN is moving.



(a) Proposed throughput

(b) MIPv6 only throughput



(c) Hierarchical throughput

Figure 5.10: Throughput for CBR application from PMIPv6 domain to MIPv6 domain

Figure 5.11 below depicts the packets lost when the MN moves between a PMIPv6 domain and a MIPv6 domain. The packets lost in the PMIPv6 domain are significantly lower than in the MIPv6 domain. Therefore, if the handover latency is reduced, the total number of lost packets will decrease, due to the basestations being able to connect to the MN sooner. Lastly, the jitter values recorded for the MN moving from a PMIPv6 domain to a MIPv6 domain depict a similar pattern as those obtained when the MN moves from a MIPv6 to a PMIPv6 domain. The jitter values shown in Figure 5.12 are acceptable given that they do not exceed the threshold of 30ms as discussed previously.

5.5 Discussion

The interworking mobility management scheme was proposed to allow mobile users to move between heterogeneous networks without any mobility restrictions. Therefore,

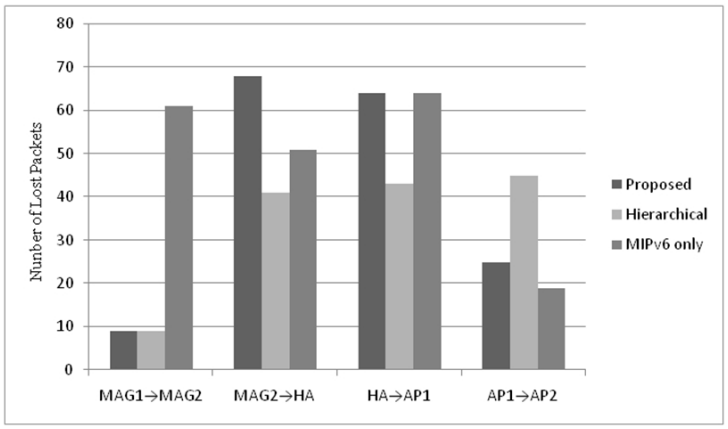


Figure 5.11: Packet loss for CBR application from PMIPv6 domain to MIPv6 domain

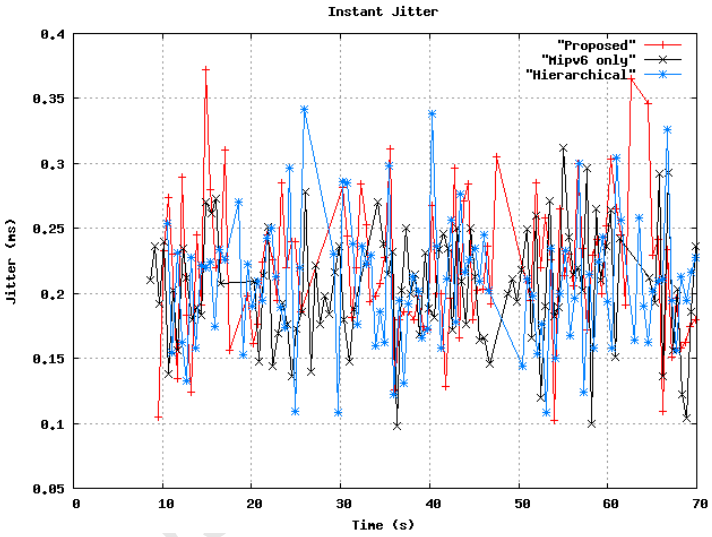


Figure 5.12: Instant jitter for CBR application from PMIPv6 domain to MIPv6 domain

experiments were designed to emulate the mobility management functionalities of the Evolved Packet Systems logical entities. The handover latency and packet loss figures achieved by the proposed scheme are comparable to the hierarchical scenario and in some cases performs better. In addition, the average UDP and TCP throughput results of the proposed scheme are higher compared to other schemes. TCP throughput is higher than UDP throughput because of mechanisms TCP contains to retransmit lost packets. With regard to end-to-end latency, the proposed scheme has an additional 30*ms* delay over the recommended 150*ms* set by the ITU-T. This extra delay is caused by triangular routing which is solved using route optimisation by reducing the number of hops from the CN to the MN. The variation of delay (jitter) was also identified as having an impact on real time applications. The proposed scheme experiences a small amount of jitter when compared to the 30*ms* recommendation Cisco uses during their quality of service design.

Results show that the proposed scheme can be used to interwork MIPv6 and PMIPv6, and

as expected, PMIPv6 performs better than MIPv6 with a reduction of handover latency and packet loss. Having evaluated the performance of the proposed interworking scheme, the next chapter concludes and provides future work needed to enhance the scheme.

Chapter 6

Conclusions and Future Work

6.1 Conclusions

The Evolved Packet System was identified as a next generation network standardised to support a variety of access technologies. The Third Generation Partnership Project (3GPP) target was to introduce a competitive, low-latency, higher data-rate, all-IP core network with the capability of supporting real-time applications over multiple access technologies. Furthermore, we observed that two distinct mobility approaches were specified for the EPS to achieve seamless mobility between access networks supported by the EPC, namely the network-based mobility protocol PMIPv6 and the host-based mobility protocol DSMIPv6. Thus, a mobile user should be able to roam freely among the access networks while maintaining their IP session connectivity.

Mobile IPv6 is a well-known mature host-based mobility standard for IPv6 networks solving many issues identified in IPv4, however, it still suffers from problems such as handover latency, signalling overhead and packet loss. Due to these drawbacks, the Internet Engineering Task Force Working Group (IETF WG) later introduced a network based mobility protocol, PMIPv6, which reuses most of the functionality contained in MIPv6. It is an enhancement of MIPv6 and provides network-based localised mobility.

Seeing that MIPv6 and PMIPv6 are both supported by the EPC, a mobile user may move from an access network supporting MIPv6 to an access network that supports PMIPv6. Thus, considerations were required to understand the interaction of the protocols and how different scenarios could be enabled [12]. A thorough literature review revealed various issues that occur when the two protocols interwork. The author found that the two mobility schemes were incompatible and modifications were required to enable them to interact. Therefore, a hybrid network/host mobility management scheme was proposed to enable the mobile user to roam between the two respective mobility schemes solving

the identified incompatibility issues.

A software simulation framework consisting of MIPv6 and PMIPv6 was successfully implemented using NS-2. The framework was used to quantitatively evaluate the performance of the hybrid interworking scheme as the mobile user switches subnets. Results were compared to other schemes to gauge the performance of the proposal. Based on the findings in the preceding chapter, the following conclusions have been drawn:

- With the stringent QoS requirements on real time applications, the Mobile IPv6 standard performs inadequately during handover. This is consistent with the original observations in literature. Proxy Mobile IPv6 performs far better than MIPv6 as inspected from the findings. Thus, it is concluded that PMIPv6 is a superior mobility scheme over MIPv6 in a localised domain.

- Because we wanted to perform seamless handover when the MN moves between different subnets supporting different mobility management schemes, a mutual binding cache was designed and implemented to allow the MN to maintain its IP connectivity while traversing through the network. To use this mutual binding cache, a common lookup key was required to search entries corresponding to the MN in the binding cache. We observed from the results that the mutual binding cache had no negative effect on throughput of the MN, rather a higher average throughput and in some cases better handover latencies and packet losses were obtained.

- During MIPv6 handover, the packet delay increases as the number of Access Points (AP) increases. In the absence of route optimisation, packets are routed in a triangular manner which causes additional packet delays. And given that the recommended threshold of packet delay is less than 150ms for VoIP applications, the increasing packet delay due to the number of AP is at risk of exceeding this threshold which would impact the quality of the application.

- Global mobility or macro mobility (i.e. when the MN from the MIPv6 domain to PMIPv6 domain) is excessive compared to handover within a localised domain. It is essential to minimise the handover latency during a global handover because it has a negative impact on all real time applications. One of the key goals of the EPS is to provide low latencies, and in order for this goal to become a reality, the large global handover caused by MIPv6 needs to be addressed.

- It can be observed from the simulation framework that the MN can maintain IP connectivity while moving from the MIPv6 domain to the PMIPv6 and vice versa. Maintaining IP connectivity is essential for providing ubiquitous computing. Given that the EPS is a multi-access paradigm with support of external networks such as

the IMS, it is the Evolved Packet Core's fundamental task to provide mobile users with ubiquitous access to network services, as well as session continuity across the different access technologies.

- The proposed scheme performs considerably well in terms of the instant jitter achieved. The reduction of jitter is required to avoid, transmission errors and to ensure that packets are received in the correct order.

- The TCP throughput at the MN for the proposed scheme was $160kbps$ which was comparible to the hierarchical scenario but better than MIPv6. TCP guarantees the arrival of packets in the correct order with no duplication which contributes to the number of successful packets received by the MN.

6.2 Recommendations & Future Work

This study encompasses a broad spectrum of networking technologies by integrating two well-known mobility approaches, Mobile IPv6 and Proxy Mobile IPv6. While conducting this work, various avenues for further research became evident. A brief outline of associated to future work is listed below:

- The proposed architecture does not consider use of wrong HA or LMA after handover. More HA/LMAs can be added and the issue of choosing the correct HA/LMA after handover can be resolved. Because if the MN chooses the wrong HA/LMA after handover, data packets destined to the MN will be lost because signalling messages are sent to the incorrect HA or LMA.

- Future work can also evaluate the security of the Mobile Access Gateway (MAG), because both PMIPv6 and MIPv6 security associations are used to update the same binding cache which could compromise the security of the MAG and have serious implications on the functionality of the Local Mobility Anchor (LMA).

- Simulations were carried out in a homogeneous environment using the WiFi 802.11b standard. Other access technologies such as WiMAX and UMTS could have been used to test the handover performance of the hybrid interworking scheme. Given that PMIPv6 was ported and made compatible with the WiFi standard, the same would have to be done with WIMAX or UMTS standards.

- Reduce the handover latency of MIPv6 by introducing its optimisations (e.g. Fast Mobile IPv6 or Hierarchical Mobile IPv6). These optimisations reduce the handover latency and packet losses experienced within MIPv6.

- Use route optimisation to minimise the packet delay. PMIPv6 does not support route optimisation, however research is being carried out to enable it to support this feature [30]. If both MIPv6 and PMIPv6 support route optimisation, the packet delay would be drastically reduced.

- In this research, real time applications were transported using UDP to emulate encoded video streams. Real time applications usually use the Real Time Protocol (RTP), so future evaluations should use RTP to extend the results obtained.

- Given that the work was simulation based, a test-bed can be designed to accurately emulate a real scenario using the IMS software present in the University of Cape Town's (UCT) Centre of Excellence (CoE) together with FOCUS EPS software.

Bibliography

[1] F. Siddiqui, S. Zeadally, "Mobility management across hybrid wireless networks: Trends and challenges",DOI 10.1016/j.comcom.2005.09.003, Elsevier, 2005.

[2] I. Ali, A. Casati, K. Chowdhry, K. Nishida, E. Parsons, S. Schmid, R. Vaidya, "Network-Based Mobility Management in the Evolved 3GPP core Network", *IEEE Communications Megazine*, 2009.

[3] T. Chiba, H. Yokota & A. Idoue, "Mobility Management Schemes for Heterogeneity Support in Next Generation Wireless Networks.

[4] J. Abeille, R. Aguiar, T. Melia, I. Soto & P. Stupar "MobiSplit: a scalable approach to emerging mobility networks", *MobiArch*, 2006.

[5] T. Balan & F. Sandu, "LTE Mobility Solutions at Network Level for Global Convergence," IGI Global, DOI: 10.4018/978-1-61520-674-2.ch019, 2010.

[6] R. Koodli, " Mobile IPv6 Fast Handovers", MISHOP Working Group, draft-ietf-mipshop-fmipv6-rfc4068bis-07.txt, April 2008.

[7] H. Soliman, C. Castellucia, K. El Malki & L. Bellier, "Hierarchical Mobile IPv6 (HMIPv6)", RFC 4140, August 2005.

[8] IETF netlmnn WG charter, http://www.ietf.org/html.charters/netlmm-charter.html.

[9] 3GPP TS 22.278 Tech. Spec., "Service Requirements for Evolution of the 3GPP System, Stage 1, Release 8,"June 2008.

[10] S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury, B. Patil, "Proxy Mobile IPv6"RFC 5213, August 2008.

[11] "Mobile IPv6 Support for Dual Stack Hosts and routers", Work in Progress; IETF Internet draft, draft-ietf-next-nemo-v4traversal-05.txt.

[12] G. Giaretta, "Interactions between PMIPv6 and MIPv6: scenarios and related issues,"IETF Internet draft-giaretta-netlmm-mip-interactions-04, June 2009.

[13] D. Johnson, C. Perkins, & J. Arkko, "Mobility Support in IPv6,"RFC 3775, June 2004.

[14] D. Damic, "Proxy Mobile IPv6 indication and discovery", IETF Internet draft, draft-damic-6man-pmip6-ind-00.txt, March 2009.

[15] G. Giaretta & V. Devarapalli, "Mobile IPv6 Bootstrapping in Split Scenario ", RFC 5026. October 2007.

[16] G. Hua, W. Lingjiao, D. Bin, L. Chuan, L. Zhengchun,"LMA/HA Discovery Mechanism on the Interaction between MIPv6 and PMIPv6, *IEEE Computer Society Press*, DOI 10.1169/NCM.2008.238.

[17] B. Han, J. Lee & T. Chung, "Hybrid PMIPv6 Indication Mechanism for Interaction between MIPv6 and PMIPv6", *The International Conference on Mobile Technology, Applications & Systems (Mobility Conference)*, Ilan, Taiwan, September 2008.

[18] Dean Christakos's Website, http://dean.christako.com retrieved May 2010.

[19] F. Masuabi, "An Evaluation of VoIP quality of service over WiMAX", Undergraduate Thesis, 2008.

[20] H. Chan, " Proxy Mobile IP with Distributed Mobility Anchors", *GlobeCom Workshop on Wireless Seamless Mobility*, December 2010.

[21] H. Choi, "PMIPv6 implementation in NS", http://commani.net/pmip6ns/download.html retrieved April 2009.

[22] H. Holma & A. Toskala, "LTE for UMTS OFDMA and SCFDMA Based Radio Access".John Wiley & Sons Ltd.2009.

[23] H. Kim, M. Yu, J. Lee, Y. Yu, S. Choi,"Network based Global Mobility Management in NGN,", IEEE Computer Society, DOI 10.1109/NCM.2008.238.

[24] ITU-T Recommendation G114: one way transmission delay; (02/1996)

[25] Academic dictionaries and encyclopedias http://en.academic.ru/dic.nsf/enwiki/1125318, retrieved October 2010.

[26] J. Kempf, K. Leung & P. Roberts, "Problem Statements for Network-based Localised Mobility Management (NETLMM)", IETF RFC 4830 April 2007.

[27] K. Lee, W. Seo, D.nKum, &Y. Cho, "Global Mobility Management Scheme with Interworking between PMIPv6 and MIPv6".IEEE Computer Society.WiMob.2008.

[28] H. Soliman, "Mobile IPv6: Mobility in a Wireless Internet ", Addison-Wesley,Pearson Education, Inc.2004.

[29] H. Yokota & A. Idoue "Emerging Standards for Mobility Management in Next-Generation All-IP Networks, *ICMU*, 2006.

[30] J. Song, H. Kim & S. Han, "Route Optimization in PMIPv6 Environment", Computer and Information Technology, *Ninth IEEE International conference*, October 2009.

[31] *Jitter and Latency.* Available: http://www.asnettechnologies.co.nz [15 November 2010].

[32] K. Fall & K. Varadhan, " The ns Manual", January 2009. Accessed from: http://www.isi.edu/nsnam/ns/ns-documentation. html

[33] K. Kong, W. Lee, Y. Han, M. Shin & H. You, "Mobility Management for All-IP Mobile Networks: Mobile IPv6 vs Proxy Mobile IPv6",*IEEE Wireless Communications*, April 2008.

[34] K. Mitsuya, R. Wakikawa & J. Murai, "Implementation and design of Dual Stack Mobile IPv6," *asiabsdcon*, 2007.

[35] L. Bhebhe, "Multi-Access Mobility in Heterogeneous Wireless Networks Today and Tomorrow", DOI 10.1109, *WiMob*, 2008.133.

[36] M. Fischer, F. Andersen, A. Kospel, G. Schafer, M. Schlager, "A Distributed IP Mobility Approach for 3G SAE".

[37] M. Olsson, S. Sultana, S. Rommer, L. Frid, & C. Mulligan, "*SAE and the Evolved Packet Core. Driving the Mobile Broadband Revolution*", Elsevier Ltd.2009.

[38] N. Montavont, R. Rouil & N. Golmie, "Effects of router configuration and link layer trigger parameters on handover performance", 2000.

[39] Network Simulator NS-2. http://www.isi.edu/nsnam/ns/, retrieved April 2009.

[40] OPNET Application and Network Performance. http://www.opnet.com/, retrieved April 2009.

[41] PMIPv6 for ns-2 Downloads. http://commani.net/pmip6ns/download.html retrieved April 2009.

[42] R. Droms, J. Bound, B. Volz, T. Lemon, C. Perkins & M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", July 2003.

[43] R. Rouil, "A Mobility Solution for Next-Generation Multi-Technology Networks", Ph.D. Thesis, Université de Rennes, 2009.

[44] S. Hyeon, Y. Han, H. Lee & H. Choi "Empirical Performance Evaluation of IETF Mobile IPv6 and Proxy Mobile IPv6", Computer-Communication Networks.

[45] Scalable Network Technologies (SNT). Qualnet. http://www.scalable-networks.com, retrieved April 2009.

[46] S. Kent & R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, November 1998.

[47] The Monarch Project. [Online] Available: http://www.monarch.cs.rice.edu/cmu-ns.html. Accessed 2010.

[48] T. Issariyakul & E. Hossain, "*Introduction to Network Simulator NS2* ". Springer. 2009.

[49] T. Szigeti & C. Hattingh "Quality of Service Design Overview", cisco press. Accessed from: http:
www.ciscopress.com/articles

[50] The Network Simulator NS-2 NIST add-on, "IEEE 802.21 model (based on IEEE P802.21/D03.00)", January 2007.

[51] Z. Yang, H. Zhou, HC Wang, H. Zhang & S. Zhang, "Design and Implementation of a Hybrid MIPv6/PMIPv6 Based Mobility Management Architecture", *Mathematical and Computer Modelling* (2010), doi:10.1016/j.mcm.2010.03.028.

[52] OMNeT++ Community http://www.omnetpp.org/, retrieved April 2009.

[53] Qualcomm, "Evolved Packet System (EPS): An Overview of 3GPP's Network Evolution", Qualcomm, Incorporated, December 2007.

[54] 3GPP TS 23.401: "GPRS Enhancements for E-UTRAN Access", June 2008.

[55] 3GPP TS 23.402: "Architecture Enhancements for non-3GPP accesses", November 2007.

[56] 3GPP TS 22.129: "Handover requirements between UTRAN and GERAN or other radio systems ", March 2006.

Appendix A

802.11b Configuration in NS-2

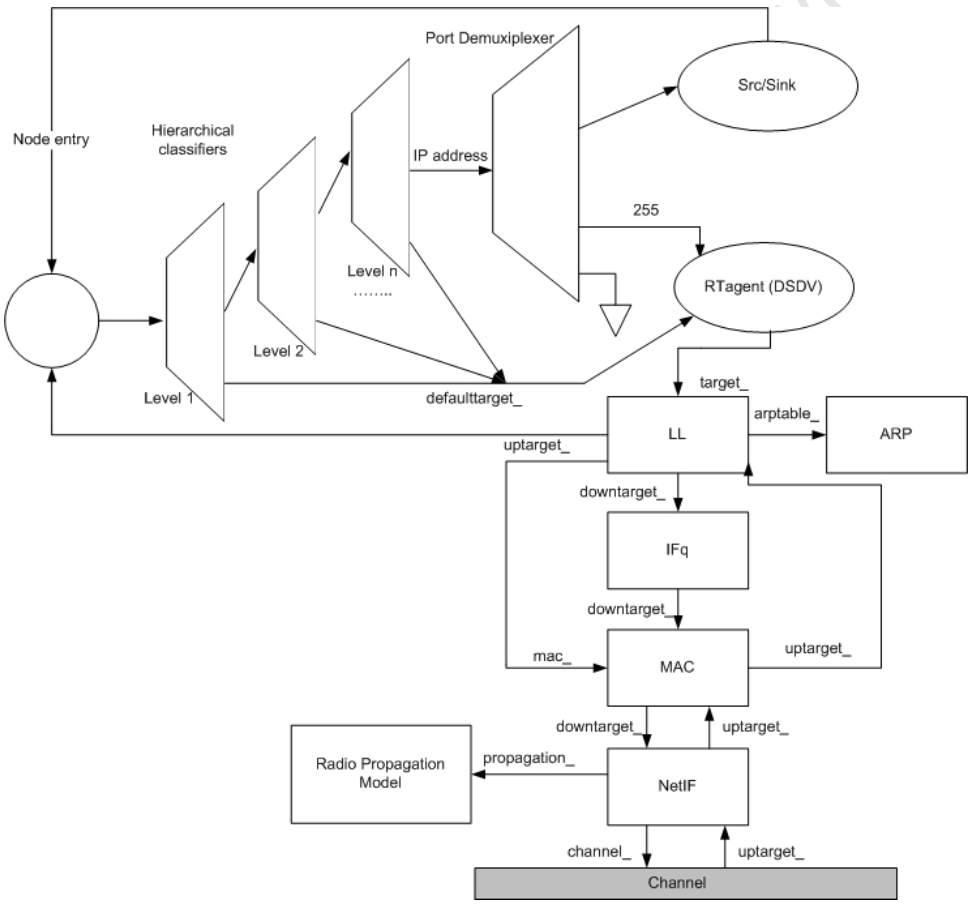


Figure A.1: Schematic of BaseStationNode in NS-2

The network stack of the WLAN 802.11b basestation node is described below.

Link layer The ARP module is connected to the LL which resolves all IP hardware (MAC) address conversions. Usually for all outgoing packets into the channel, the Routing Agent hands down the packets to the LL. Thereafter, the LL hands down packets to the interface queue. For all incoming packets out of the channel, the MAC layer hands up

packets to the LL which are then handed off at the node_entry_point.

ARP The Address Resolution Protocol (implemented in BSD style) module receives any queries from the Link layer. If ARP has the hardware address for destination, it writes it into the mac header of the packet. Otherwise it broadcasts an ARP query, and caches the packet temporarily. For each unknown destination hardware address, there is a buffer for a single packet. When additional packets to the same destination are sent to the ARP, the earlier buffered packet is dropped.

Interface Queue The **class PriQueue** is implemented as a priority queue which gives priority to routing protocol packets, inserting them at the head of the queue. It supports running a filter over all packets in the queue and removes those with a specified destination address.

Mac layer The IEEE 802.11 distribution coordination function (DCF) MAC protocol has been implemented by the CMU. It uses a RTS/CTS/DATA/ACK for all unicast packets and sends out data for broadcast packets. The implementation uses both physical and virtual carrier sense.

Network Interface This layer serves as a hardware interface which is used by the mobilenode to access the channel. The wireless shared media interface is implemented as **class Phy/WirelessPhy**. This interface is subject to collisions and the radio propagation model receives packets transmitted by other node interfaces to the channel. The interface stamps each transmitted packet with the meta-data related to the transmitting interface like the transmission power, wavelength etc. This meta-data in **pkt** header is used by the propagation model in receiving network interface to determine if the packet has minimum power to be received and/or captured and/or detected (carrier sense) by the receiving node. The model approximates the DSSS radio interface (Lucent WaveLan direct-sequence spread-spectrum).

Radio Propagation Model It uses Friss-space attenuation ($1/r^2$) at near distances and an approximation to Two ray Ground ($1/r^4$) at far distances. The approximation assumes specular reflection off a flat ground plane.

Antenna An omni-directional antenna having unity gain is used by mobilenodes.

A.1 Wireless Configuration

The network components discussed above such as Link layer or Mac layer are configured as follows:

```
# parameter for wireless nodes
set opt(chan)           Channel/WirelessChannel    ;# channel type for 802.11
set opt(prop)           Propagation/TwoRayGround   ;# radio-propagation model 802.11
set opt(netif)          Phy/WirelessPhy            ;# network interface type 802.11
set opt(mac)            Mac/802_11                 ;# MAC type 802.11
set opt(ifq)            Queue/DropTailHSNTG/PriQueueHSNTG    ;# interface queue type 802.11
#set opt(ifq)            Queue/DropTail/PriQueue    ;# interface queue type 802.11
set opt(ll)             LL                         ;# link layer type 802.11
set opt(ant)            Antenna/OmniAntenna        ;# antenna model 802.11
set opt(ifqlen)         50                         ;# max packet in ifq 802.11
set opt(adhocRouting)   DSDV                       ;# routing protocol 802.11
```

Figure A.2: Wireless configuration

A.1.1 Radio Range Configuration

```
#define coverage area for base station: 50m coverage
Phy/WirelessPhy set Pt_ 0.0134
Phy/WirelessPhy set freq_ 2412e+6
Phy/WirelessPhy set RXThresh_ 5.25089e-10
Phy/WirelessPhy set CSThresh_ [expr 0.9* [Phy/WirelessPhy set RXThresh_]]
```

Figure A.3: Basestation coverage area

Appendix B

Compilation and Analysis of NS-2 Trace data

Network Simulator (Version 2) is an event driven simulation tool where network simulation is written in a scripting format using the Tcl language. In NS-2, the network topology, network components (nodes, links, TCP and UDP) are created according to the simulation design and configured in a particular order. During a simulation, changes in any Tcl objects and events are recorded to a trace file for post-processing and analysis. There are two types of monitoring tools available in NS-2. First, *traces* which record every individual packets arrival, departure, or when they are dropped at a link or queue. Second, *monitors* which record counts of various quantities such as bytes, byte arrivals, lost packets etc. NS-2 also includes an animation tool called NAM which is used to view network simulation traces as well as real world packet trace data. It is used to visualise the network topology and how packets flow from the source until they reach their destination. To collect relevant data or results from the trace file AWK scripts are used. AWK is a simple programming language designed for processing text files and is used to filter large amounts of data.

The events of a trace file are written in a specific format depending on whether the simulation is wired or wireless. In order to trace wireless objects, the following command is used:

$ns use-newtrace

An example of the trace format is shown below:

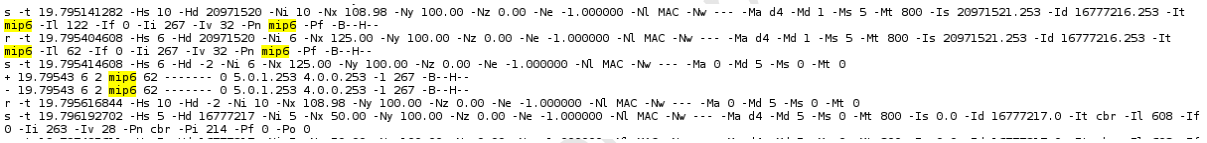
s -t 9.160202680 -Hs 5 -Hd 16777217 -Ni 5 -Nx 50.00 -Ny 100.00 -Nz 0.00 -Ne -1.000000 -Nl MAC -Nw — -Ma d4 -Md 5 -Ms 0 -Mt 800 -Is 0.0 -Id 16777217.0 -It cbr -Il 608 -If 0 -Ii 29 -Iv 29 -Pn cbr -Pi 2 -Pf 0 -Po 0

r -t 9.160819441 -Hs 10 -Hd 16777217 -Ni 10 -Nx 60.00 -Ny 100.00 -Nz 0.00 -Ne -1.000000 -Nl MAC -Nw — -Ma d4 -Md 5 -Ms 0 -Mt 800 -Is 0.0 -Id 16777217.0 -It cbr -Il 548 -If 0 -Ii 29 -Iv 29 -Pn cbr -Pi 2 -Pf 1 -Po 0

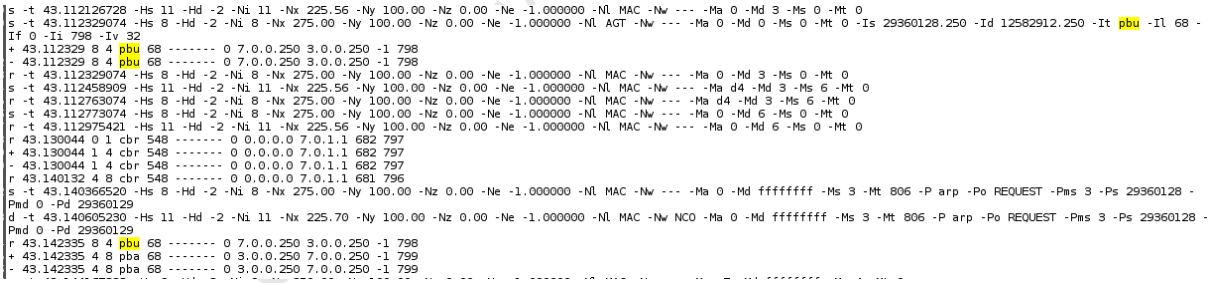
Useful information such as timestamps, packet IDs, sequence numbers are taken from this trace where results corresponding to the perfomance metrics can be recorded and analysed.
Each NS-2 tcl script is executed from the Linux shell command prompt. For example, the interworking tcl script is executed as follows;

$ns wrapper-test.tcl > info

After the simulation, an output tracefile is generated as shown in Figure B.1 from which AWK files are used to generate useful results. Figure B.1 illustrates the binding messages during the simulation. As can be seen from the figure, both MIPv6 and PMIPv6 messages are recorded.



(a) Binding update messages



(b) Proxy binding update messages

Figure B.1: Binding messages from output tracefile

Appendix C

Source Code for Simulation Experiments

C.1 Network Layer Mobility Protocols

C.1.1 Mobile IPv6

Filenames:classifier-mip6.h classifier-mip6.h mip6.h mip6.cc mip6-pkt.h, handover-unified.h handover-unified.cc

C.1.2 Proxy Mobile IPv6

Filenames: pmip6.h pmip6.cc

C.2 Tcl Scripts

Filenames: mip_pmip.tcl pmip_mip.tcl

C.3 Awk Scripts

Filenames: Throughput.awk Jitter.awk AverageStats.awk

Appendix D

Publications

F.M. Masuabi & N. Ventura, "A Hybrid Network/Host Mobility Management Scheme for NGNs", *SATNAC*, September 2010.

Abstract—Next Generation Networks are becoming more and more converged. Like the System Architecture Evolution (SAE) which encourages Fixed Mobile Convergence. It is a packet switched network which connects different radio access technologies. With this heterogeneity, mobility management becomes an issue as the goal is to always achieve seamless mobility. However, various access technologies support different layer 3 schemes, such as PMIPv6 which is network-based and MIPv6 which is host based. With the heterogeneity that the SAE adopts, there are several deployment scenarios where PMIPv6 will interact with MIPv6. We propose a hybrid network/host mobility management scheme which will allow the user to roam amongst networks supporting either protocol.

Appendix E

Accompanying CD-ROM

The contents of the CD-ROM are as follows:

- A soft copy of thesis document in PDF format
- Simulation software including all source files
- Research articles and papers used and listed in References
- Publication from this thesis