Host Mobility Management with Identifier-Locator Split Protocols in Hierarchical and Flat Networks

Muhana, Magboul Ali, Muslam

This thesis is submitted in partial fulfilment of the academic requirements

for the degree of

Doctor of Philosophy in Electrical Engineering

in the Faculty of Engineering and The Built Environment

University of Cape Town

February 2012

As the candidate's supervisor, I have approved this dissertation for submission.

Name: Professor H. Anthony Chan

Signed: signature removed

Date: __ February 13 2012_____

Declaration

I hereby declare that: (1) the above thesis is my own unaided work, both in conception and execution, and that apart from the normal guidance of my supervisor, I have received no assistance apart from that stated below; (2) except as stated below, neither the substance or any part of the thesis has been submitted in the past, or is being, or is to be submitted for a degree in this University or any other University.

I am now presenting the thesis for examination for the Degree of PhD in Electrical Engineering. I also grant the University free license to reproduce the above thesis in whole or in part, for the purpose of research.

Muhana Magboul Ali Muslam	29 January 2012
Name	Date

Abstract

As the Internet increasingly becomes more mobile focused and overloaded with mobile hosts, mobile users are bound to roam freely and attach to a variety of networks. These different networks converge over an IP-based core to enable ubiquitous network access, anytime and anywhere, to support the provision of services, that is, any service, to mobile users. IP mobility management solutions, built-based on Mobile IPv6 (MIPv6) and/or Proxy Mobile IPv6 (PMIPv6) as well as Host Identity Protocol (HIP) are the main mobility solutions introduced to support host mobility on the Internet. In fact, mobility solutions, built-based on MIPv6 and PMIPv6, lack native security support and host identifiers. Thus, they experience an unsatisfactory and non-secure performance of the IP handover when used for supporting mobile host handovers between heterogeneous IPv6-networks. Execution of the many handover components such as duplicate address detection and authentication, which are time consuming, causes long handover delays, many packet losses and unnecessary signalling overheads. Furthermore, HIP and PMIPv6 on their own do not provide seamless handovers.

Therefore, in this thesis, the researcher proposed network-based mobility solutions at different layers to securely support seamless handovers between heterogeneous networks in hierarchical and flat network architectures. He analysed the handover performance of these proposed mobility solutions and their related research such as HIP and PMIPv6. In the evaluation, handover delays, packet losses and signalling overheads are investigated. The analysis demonstrated that network-based mobility solutions, such as PMIPv6, provide a better handover performance than host-based mobility solutions, such as MIPv6 and its extensions including Hierarchical MIPv6 (HMIPv6) and Mobile IPv6 Fast Handovers (FMIPv6). Therefore, the network-based approach is mainly employed for the proposed mobility solutions to further enhance the handover performance of the mobile hosts. For example, the researcher combined HIP with PMIPv6, called HIPPMIP, to provide a network-based mobility solution for HIP-enabled mobile hosts. The HIPPMIP is introduced to provide seamless network-based handover solutions for HIP-enabled mobile hosts. Thus, the latter do not perform any handover procedures such as binding updates, and the verification and validation of mobile hosts. Thereafter, the researcher proposed a network-based HIP and mobility, called MHPP, to provide seamless,

secure handovers for both HIP-enabled and non-HIP-enabled mobile hosts without unnecessary signalling overheads. MHPP also introduced a network-based HIP and mobility that securely provides seamless handover procedures without unnecessary handover-related signalling. MHPP supports host mobility in hierarchical network architectures since it has a central entity.

Furthermore, the researcher extended the MHPP, as it achieves a good handover performance in the hierarchical network architecture, and called it DM-MHPP to respond to the needs created by the evolution of the network architecture from being hierarchical to being flat. DM-MHPP co-locates the mobility functions of MHPP in a single mobility entity and is thus duplicated in different network locations to support host mobility in a flat network architecture. Thereafter, he proposed, also for flat network architectures, a signal-less distributed mobility (SL-DM) solution which uses only data packets instead of control packets for seamless, secure and scalable mobility solutions.

In all, four mobility designs were introduced: two, HIPPMIP and MHPP, for the hierarchical network architecture and the other two, DM-MHPP and SL-DM, for the flat network architecture. These designs employ a network-based mobility approach and utilise HIP technology to ensure non-perceptible disconnection of active sessions during and after handovers. The simulation is used to evaluate the handover performance, measuring the handover delay, packet loss and signalling overhead of the proposed mobility solutions and some of the related work. In addition, the researcher considered the effect of mobile host speed, number of mobile hosts simultaneously performing IP handover, number of correspondent hosts with which mobile hosts have active sessions during the handover, etcetera. The simulation results demonstrate that the proposed mobility solutions have better handover performance than similar existing mobility solutions and standard mobility solutions such as HIP and PMIPv6. Furthermore, the proposed mobility solutions provide different options in response to different needs and also serve different scenarios.

Acknowledgements

I thank you GOD for Your blessings and provision.

Thank you to my family for their generous and unlimited support.

My supervisors Professor H. Anthony Chan and Mr. Neco Venturea for their wisdom, direction, continuous encouragement to improve the quality of my research as well as their valuable advice that extended beyond the academic aspects.

Thank you to Professor Linda Xie for her authoritative influence, initiative guidance and for hosting me at her laboratory at the University of North Carolina, Charlotte.

Thank you to the National Canter for Diplomatic Studies and National Council for Training for their financial support to complete this PhD study.

The University of Cape Town, Post Graduate Funding Office, for their financial support to complete this PhD study.

Thank you to the staff of the Electrical Engineering Department, staff of the International Academic Program Office and the staff of Student Housing for their high esteem.

My colleagues at the Communications Research Group (CRG) for their initiative and constructive comments.

Thank you to my friend Mohssen Mohammed Zain for hosting the follow-up meeting and for his generous support and welcome in Cape Town.

Table of Contents

List of Figures

List of Tables

Publications

A Peer-Reviewed papers published from this thesis are documented in the following:

1. Muhana Muslam, H Anthony Chan, and Neco Ventura, “Inter-Subnet Localized Mobility Support of Host Identity Protocol,” EURASIP Journal on Wireless Communications and Networking 2011, 4 August 2011, doi:10.1186/1687-1499-2011-55.

2. Muhana Muslam, H. Anthony Chan, Linoh A. Magagula, and Neco Ventura, “Network-Based Mobility and Host Identity Protocol,” Proceedings of the IEEE Wireless Communications & Networking Conference (WCNC) 2012, Paris, 01-04 April 2012.

3. Muhana Muslam, H. Anthony Chan, and Neco Ventura, “Host Identity Protocol Extension Supporting Localized Mobility Management,” Proceedings of IEEE Consumer Communications & Networking Conference (CCNC) Workshop on Personalized Networks (PerNets 2011), Las Vegas, 9-12 January 2011.

4. Muhana Muslam, H Anthony Chan, Neco Ventura, and Linoh A. Magagula, “Hybrid HIP and PMIPv6 (HIPPMIP) Mobility Management for Handover Performance Optimization,” Proceedings of the Sixth International Conference on Wireless and Mobile Communications (ICWMC 2010), Valencia, Spain, 20-25 September 2010.

5. Muhana Muslam, Anthony Chan, and Neco Ventura, "HIP Based Micro-Mobility Management Optimization," Proceedings of the Fifth International Conference on Wireless and Mobile Communications, ICWMC, Cannes, France, August 2009. IEEE Computer Society. ISBN 9780769537504.

Glossary

AAA: Authentication, Authorization, and Accounting.

AP: Access point.

AR: Access router (AR).

BS: Base station

CH: Correspondent host.

CoA: Care-of-address.

DHT: Distributed Hash Table.

DMM: stands for Distributed Mobility Management.

ESP: Encapsulating Security Payload Protocol.

FMI: Future Mobile Internet (FMI) is an IP-based infrastructure integrating heterogeneous wireless networks to enable them to interact and interoperate.

Heterogeneous Wireless Network Environment: a network that comprises fully or partially overlapping sub-networks with different wireless technologies.

HIP: Host Identity Protocol.

HIPBE: HIP Base Exchange.

HIPPMIP: A hybrid of HIP and Proxy Mobile IPv6

IEEE: Institute of Electrical and Electronics Engineers.

IETF: Internet engineering task force.

iMAG: intelligent Mobility Access Gateway.

Initiator: A host that starts establishment of the HIP security association (HIPSA).

ITU: International Telecommunication Union.

LMA: Local Mobility Anchor

LRVS: Local Rendezvous Server.

MAG: Mobile Access Gateway

MH: Mobile host.

MHP: Mobility-enabled HIP Proxy.

MHPP: Mobility-enabled HIP Proxy Protocol.

Micro-RVS: Micro-Rendezvous Server.

Mobility Management Protocol: A protocol that enables hosts to move between different locations of the network and to preserve their active communications.

Multihoming: Ability of mobile host to sequentially or simultaneously connect to more than one network using different access technologies.

PoA: Point of Attachment is the network entity to which MH can connect either at layer 2 such as AP and BS, or layer 3 such as AR.

Responder: A host that responds to the establishment of the HIPSA.

RTT: Round Trip Time.

RVS: Rendezvous Server.

Seamless handover: Handover that preserves active sessions during the movement of MH without perceptible disruptions.

SL-DM: Signal-Less-Distributed Mobility.

TCP: Transmission Control Protocol.

UDP: User Datagram Protocol.

WLAN: Wireless Local Area Network.

Chapter 1 Introduction

In this chapter, advances in applications and networks, and how these advances relate to host mobility are discussed. The chapter begins with a discussion of impacts of the evolution of network architecture and application on mobility management. This is followed by a discussion of need for secure, seamless, scalable mobility designs and limitations of the some mobility solutions in Section 1.2 and Section 1.3 respectively. The chapter also presents a discussion of proposed mobility architectures and research contributions in the Future Mobile Internet (FMI).

1.1 Impacts of the Evolution of Network Architecture and Application on Mobility Management

Advances in the development of applications, allowed for by network developments, create new requirements that must be met by the network and its protocols. “Network applications are the raisons d'etre of a computer network. If we couldn't conceive of any useful applications, there wouldn't be any need to design networking protocols to support them” [1]. The service requirements for applications can generally be classified based on application sensitivity to data loss, bandwidth or timing (delay).

Some applications, such as Web document transfers and financial applications demand zero data loss. For example, a loss of data in a session of a financial application could have undesirable consequences for both customers and banks. On the other hand, some applications such as multimedia applications, particularly real-time audio/video or stored audio/video, could tolerate some amounts of data loss, making them loss tolerant. However, data loss might result in a small fault in the played-out audio/video.

For bandwidth-sensitive applications to be effective, some applications such as IP telephony, widely known as voice over IP (VoIP), must send their data at a certain rate, for example, 15kbps. If the required bandwidth is not available, applications either send at a different rate or fail. It is important to note that the higher the available bandwidth, the better for even the non-bandwidth-sensitive, that is, elastic applications such as remote access and Web transfers.

The third application requirement, timing or delay, is particularly relevant for certain applications such as interactive real-time applications; videoconferencing, VoIP, and multiplayer games which require restricted delay constraints on data delivery to work effectively. In particular, several of these applications tolerate at most a few hundredths of a millisecond end-to-end delays [1-3]. For example, as stated in the ITU-T G.114 standard, a one-way, end-to-end delay of more than 100-150 milliseconds in VoIP causes undesirable pauses during conversations [4]. In addition, high delays in a multiplayer game cause undesirable disruption and, thus, make the application feel less realistic. For non-real-time applications, although there is no tight restriction on the end-to-end delays, a lower delay is normally preferable. In general, as stated in the 3GPP TS22.105 specification, the end-to-end delay for multimedia applications must not exceed 400 milliseconds.

As discussed, application performance requirements are different. These requirements need to be insured by network protocols such as mobility management protocols. In summary, applications require: (i) small or no loss for good session quality; (ii) small delays especially for interactive applications; (iii) sufficient bandwidth; and (iv) little or no variance in delays for effective communication. These are some of the application requirements that mobility protocols must not violate. Again, large delays cause significant packet loss, while large bursts of packet loss disrupt the communication session between peers, rendering communication interactions unintelligible [4]; the difference in the arrival delay of ongoing traffic cannot exceed a few hundreds of milliseconds [5].

Although current applications have challenging requirements that need to be fulfilled, many other important applications such as e-Health, e-Utilities, e-Government, etcetera, will be fully deployed on the Internet because of the advances made towards a high-speed Internet. Such applications have tight quality of service (QoS) requirements [6]. Naturally, this large growth in applications adds some new constraints to packet loss, bandwidth and delay. Many of these applications need to be accessed at any place or time within the network coverage. To achieve this, mobility management architectures that can be further optimised to satisfy the requirements of the current and future applications, are strongly required. For example, to efficiently and effectively support the delay-sensitive application services during movement between different

networks, there is a need for delay-tolerant IP mobility management architectures. This optimisation must ensure at least the requirements of the different types of applications; data loss-sensitive, bandwidth-sensitive and delay-sensitive. If the approach employed in the mobility architectures does not negatively affect the application requirements, end-to-end delay, packet loss, bandwidth and variability in delay it will result in undesirable disruptions to the active session because of mobility.

As mobility management architectures struggle (are being revised) to meet application requirements, additional challenges are introduced by network advances, integration between isolated different networks and evolutions in the network architecture of hierarchical architectures.

The integration of different wireless systems to access networks will take place at the IP layer networks [7]. An illustration for such integration is displayed in Figure 1-1. In the figure, the IP bridges enable the movement of mobile hosts between different networks such as WiMAX, WiFi and the Long Term Evolution (LTE). One of the main advantages of these integrated heterogeneous wireless networks is that a user can connect to the network that best satisfies his/her needs and requirements. For example, WWANs such as the Universal Mobile Telecommunication System (UMTS) cover a wide area with relatively low-data-rates for high-speed MHs, whereas WLANs such as IEEE 802.11b cover a small area with high-data-rates [8]. In addition to this, an MH also needs to preserve its active sessions via a different interface when moving between access networks. It is questionable though, how securely an MH proves that it was communicating with a correspondent host (CH) via different access networks and different interfaces. In fact, during a movement between heterogeneous networks that result in a change of an MH IP address, the MH cannot be authenticated either by its IP address or its interface identifier. Therefore, there is a need for a permanent host identifier, which is accessible anywhere (despite the access network to which the MH is connected). Besides the host identifier, there is also a need for a secure mechanism to determine whether the newly detected MH is the same as the one that was connected to a different access network or not. The required time to perform this check depends on many factors including the component involved, the employed approach as well as the traffic load in the network during that time.

In summary, the integration of different access networks creates a need for a permanent and unique host identifier that must be accessible at any time as well as a secure handover approach. Without the host identifier and secure mechanism, MH active services could be attacked, sniffed, redirected to a victim host and/or denied.

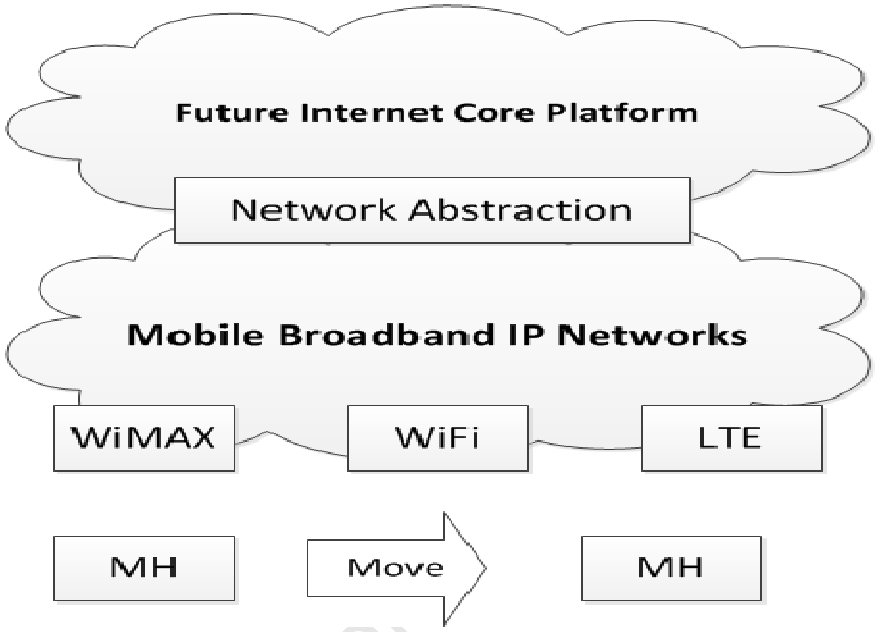


Figure 1-1 Illustration of future mobile environment

In addition to the heterogeneity in the wireless access networks and their underlying protocols, network architecture is evolving from a hierarchical to a flat infrastructure. The nature of hierarchical architecture could be utilised to efficiently and seamlessly support host mobility. This is because in hierarchical architecture, it is possible to select or identify a functional entity, to be updated on the current location of an MH between the MH and CH. Consequently, a handover performance will be optimised since the selected entity is topologically closer to the MH than CH. Unfortunately, the nature of the hierarchical architecture that allowed the selection of a central entity for handover optimisation, is no longer available in a flat architecture since entities could be distributed across different networks. This architectural evolution from hierarchical to flat networks, caused by increased data traffic volumes, creates new challenges as have been identified in [9]. The challenges include single point of failure and bottlenecks; non-optimal routing paths; scalability problems; and long handover delays. Consequently, the

handover mechanisms that have been built-based on the centralised mobility function need to be redesigned and/or carefully optimised again.

Advances in network applications always set new, diverse requirements and tight constraints while advances in the network itself create technical challenges that need to be addressed. Therefore, there is a call for the continuous optimisation of mobility solutions and/or the development of new mobility designs.

1.2 The Need for Secure, Seamless, Scalable, and Efficient Mobility Management Architectures

Although such requirements are challenging even for stationary hosts, they must be offered at least with the same quality to the MHs. That is, mobility solutions must not violate the requirements of the applications. To achieve that, there is a need for secure, seamless and scalable mobility management architectures.

As a result of IP integrating different access wireless networks, challenges such as the preserving of active sessions among heterogeneous networks; provisioning of required quality of service (QoS); and the need for permanent host identifiers to authenticate MHs from access networks, have emerged. In particular, the integration of heterogeneous access networks creates an environment where the need for host identifiers, instead of interface identifiers, in heterogeneous networks becomes mandatory. Thus, to maintain active connections, handover functionality must be able to identify MHs with more than an interface when moving between heterogeneous networks. Here strong secure mechanisms are needed. This functionality must ensure that handovers between heterogeneous networks are secure and seamless without imposing additional handover delay and signalling overhead. If the handover functionality does not achieve this, MH users experience a denial of service (DoS), Man-in-the-middle attack, or other type of security difficulties.

Many of the existing IP mobility management solutions do not have a native security mechanism. Consequently, MH active services are vulnerable to DoS, sniffing and/or any other type of attack. Therefore, secure handover support is as mandatory as a seamless function; if the

lack of a seamless handover mechanism degrades the performance of the active services, the lack of a secure handover mechanism denies access to the services. Furthermore, scalability is another important technical issue that must be considered in mobility architectural designs as the number of MHs is increasing tremendously. If these issues are not considered, mobility designs may not be so widely deployed since all the network operators plan to increase their customers who, most of them if not all, are already mobile.

Current mobility solutions do not support seamless, secure and scalable handovers to active sessions. For example, some of them support the seamlessness but do not consider the security and/or the scalability. Others do the opposite. Having solutions with different capabilities is fine if these different solutions can be integrated with one another in order to achieve better handover performance. In some cases, the optimisations introduced by integrating different mobility solutions can be limited, for example, when applicable for a specific type of MH but not for other types. Therefore, besides the integration, there is a need for the development of new mobility designs and/or enhancement of existing ones. In addition to this, there is also a need for extendable mobility architectures that do not incur long handover delays, high packet losses and unnecessary signalling overheads in a secure and scalable manner.

In the Future Mobile Internet (FMI), to effectively allow MH users to successfully access their interactive applications while moving, delay-transparent, secure, and scalable handover solutions are mandatory. This thesis responds to the need for mobility management architectures that effectively support the performance, packet loss, bandwidth, as well as delay requirements of current and future applications at the network and/or HIP layer. For example, users expect to enjoy an acceptable quality of interactive applications via the IP layer. Such a challenge, in the Future Mobile Internet, is doubled by additional factors related to MH movement between different networks that result in IP changes. This movement is widely referred to as IP handover.

Subsequently, the researcher studied IP handover-related factors, over the Proxy Mobile IPv6 (PMIPv6) and Host Identity Protocol (HIP), that can prevent the achievement of a delay-transparent performance for interactive applications thereby hindering a secure and scalable handover. Furthermore, this thesis reconsiders the architectural framework introduced by the PMIIPv6 and HIP and their enhancements. Moreover, it also looks into efficient alternative

mobility architectures in support of secure and scalable delay-transparency in IPv6 handover for current and future application services, especially for interactive applications.

1.3 Limitations of Mobility Solutions

In this section, the limitations of some important mobility solutions such as MIPv6 and HIP are discussed. The section begins with a discussion of MIP-based solutions in centralised network architectures and network flat architectures, with the technical challenges introduced by the lack of native security support and subsequently, the emergence of flat architecture for those host mobility solutions is discussed. This is followed by a discussion of the same aspects mentioned above, but this time relating to HIP-based mobility solutions. This section mainly states the problem this thesis is solving.

1.3.1 MIP-based Solutions

The Mobile IP (MIP) standard was introduced some years ago and later improved to Mobile IPv6 (MIPv6) [10] to provide mobility support for the next generation IP-based Internet. However, it has been discovered that this standard has very long handover delays and high packet losses, hence interrupting active connections during the handover event of the MH. Various MIPv6 extensions, for example HMIPv6 [11] and MIPv6 Fast Handovers [12], have also been proposed to improve MIPv6 performance, particularly in localised mobility (micromobility) environments. Unfortunately, these have inherited most of the shortfalls of MIPv6.

MIPv6 and its extensions or any IP layer mobility management protocol, semantically overload the IP addresses, that is, the IP addresses are used as both a location identifier (where I am) and a host identifier (who I am). Furthermore, the upper layers or protocols, for example TCP, UDP, etcetera, are bound to the IP addresses. Thus, when an MH changes Points of Attachment (PoA) and effectively changes its IP address, active upper layer connections are broken. This therefore, requires reconfiguration of various parameters and states of the MH in order to re-establish the broken connections at the new location; it usually takes a significant period of time, which results in long handover delays and high packet losses. Consequently, the user quality of experience of the active communication context as well as security is seriously

compromised [13].

Proxy MIPv6 (PMIPv6) [14] extends MIPv6 to provide network-based mobility support which is not implemented in the MH protocol stack. Since MH participation in mobility-related signalling is not needed, such network-based solutions optimise handover performance in terms of handover latency and signalling overhead [15]. However, PMIPv6 lacks elegant secure mobility support and still relies on the dual role of IP addresses for location and host identity. To provide a full and efficient mobility management with reliable security support and negligible handover delay for future mobile networks, the researcher hypothesises that intelligently combining PMIPv6 and secure and scalable mobility architecture with multihoming support can meet this goal.

1.3.2 HIP-based Solutions

During a communication session, an MH may move within a single domain (micro-mobility) or move to a different domain (macro-mobility) [16]. These two scenarios can be managed at different layers of the conventional TCT/IP stack [17]. Access technologies can manage intra-link mobility (L2 handover) and may assist to trigger L3 handover. The IP layer solutions are common, especially in a heterogeneous network environment. As mentioned above (1.3.1), Mobile IP (MIP) [10], which is one of the IP layer solutions, extends the ability of the Internet to support the host mobility but has security threats such as Denial of Service attacks (DoS)[13].

A solution to the problem of the dual role of IP addresses, discussed in Section 1.3.1, in IP layer mobility management protocols is to separate the functions of host identification and location identification. The Host Identity Protocol (HIP) [18], which runs in a HIP layer between the transport layer and the network layer, separates the location and identity roles of IP addresses by introducing a new namespace, the Host Identity (HI). One consequence of such a decoupling is that new solutions to the network-layer mobility and host multihoming are possible [19] and furthermore, the mobility and multihoming can be handled in a secure manner [20].

As discussed in the above paragraph, HIP provides secure mobility support in a simpler

manner than other proposed solutions [13] and the popular MIP [21, 22]. The mobility extension for HIP allows a HIP enabled mobile host to move with negligible handover latency in environments where the global mobility management is acceptable but introduces long handover latency and unnecessary control messages in a micro-mobility environment [23]. Such long handover latency increases packet loss and delay as well as decreasing the performance of the upper layer application, particularly real time applications such as Voice over IP (VoIP).

In summary, ensuring non-perceptible disconnection for active MH sessions of real time when traversing the heterogeneous wireless networks in Future Mobile Internet is a key challenge for IP mobility management protocols. Unfortunately, IP mobility management protocols, in their current form and with existing extensions, lack seamless handover [24] in a secure manner [25][26][27]. Most mobility solutions and their extensions experience long handover delay, among packet loss, and unnecessary signalling overhead [15]. Thus, IP mobility management protocols do not ensure seamless and secure IP handover to allow MHs to preserve active sessions as the MH changes location in the networks. The handover delay is still too long and cannot be elastic for real-time applications [28] and thus causes packet loss and ultimately disconnects the session. In the IP handover, many processes need to be considered such as movement detection for the MH, IP configuration and duplicate address detection, registration of the new location of the MH and the updating of all respective binding concerning the new location of the MH, as well as authentication and authorisation processes that take a considerable amount of time.

Therefore, the current IP mobility management solutions need to be improved with secure and seamless handover solutions without incurring additional handover-related signalling overhead. Many standard IP mobility protocols introduced by IETF simply enable MH to move between networks and are still reachable, but do not support seamless and secure IP handover with minimal signalling. Furthermore, many handover solutions, for example, [29][30] [31][32][33][34], are introduced to provide seamless handovers. However, these handover solutions lack native security and permanent host identifiers and thus experience additional delays and signalling overhead for the authentication procedures required for handover between the heterogeneous networks. In addition, most of these handover solutions cannot achieve a

negligible handover delay and signalling overhead while security and/or scalability are considered. Although handover performance is optimised, there is still a need for further enhancement by effectively incorporating additional elegant mobility functionalities. Particularly, to reduce handover delay as well as mobility-related signalling in both macro and micro-mobility environments while supporting security and scalability[13][21, 22][23][35].

1.4 Proposed Mobility Management Architectures (HIPPMIP, MHPP, MHPP-DM, and SL-DM)

In this thesis, four designs (Figure 1-2), with particular advantages and drawbacks, have been developed to achieve high handover performance mobility solutions in a secure and scalable manner, allowing network operators to choose a design that best matches their requirements. The designs respond to hierarchical architectures and flat architectures, and are centralised in hierarchical structures or distributed in flat structures. Three designs (HIPPMIP, MHPP and DM-MHPP) are network based, while SL-DM can be configured either as a network or host-based solution.

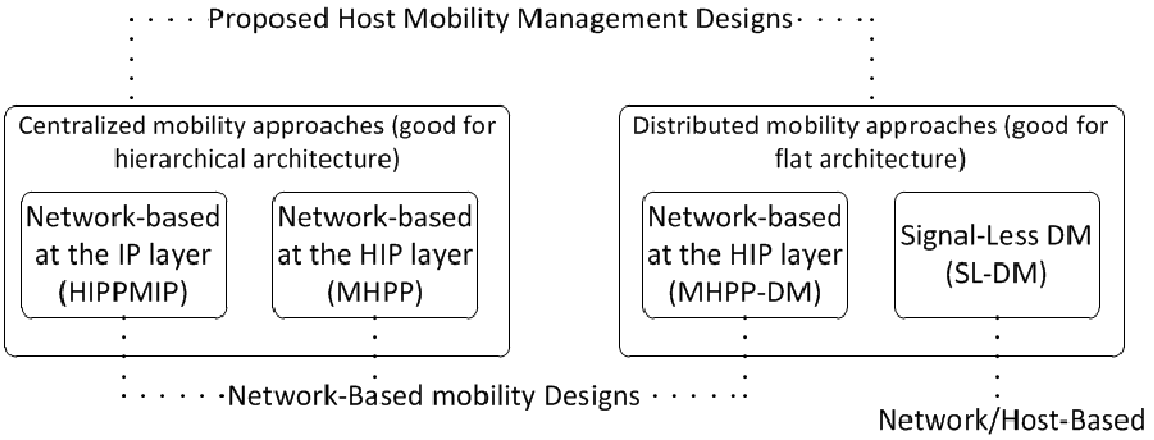


Figure 1-2 Proposed mobility designs for Future Mobile Internet

1.4.1 Centralised Solutions: HIPPMIP and MHPP

In this thesis, the researcher proposed a novel coordinated hybrid of PMIPv6 and HIP, which he called HIPPMIP, to optimise handover performance in heterogeneous wireless

networks in terms of providing efficient, secure and negligible handover delay architecture. In his HIPPMIP architecture, the MH moves while keeping its communication context active through HIP association and also maintaining a stable IP address for packet routing even under MH mobility conditions in a PMIPv6 domain.

In addition, this thesis introduces a network-based mobility management function integrated with a HIP proxy function at the access routers to support all IP hosts. The hosts do not need to possess new functions including mobility management and HIP capability other than the existing IP protocol stack. Yet they are able to experience the multihoming capability and the security level native to HIP in addition to receiving network-based mobility support. Additional mobility management functions are also included at the access routers taking advantage of the HIP proxy capability. These additional network-based functions include tracking and updating MH location, security signalling, assigning a network prefix per host identifier, and using the same network prefix within the same network domain to avoid Duplicate Address Detection (DAD), resulting in improved handover performance. They enable an MH, whether or not HIP-enabled, to use the same IP address as it changes its points of attachments within the same domain.

The above mentioned solutions are developed for the hierarchical network architecture. The latter is further extended to support the host mobility in the flat network architecture. The design for those extensions is explained below.

1.4.2 Distributed Solutions: DM-MHPP & SL-DM

For the host mobility support in flat network architectures, this thesis introduces a network-based distributed mobility management that duplicates many mobility-enabled HIP proxies in different networks to support all IP hosts. All the mobility management functions of the MHP solution are also included at the access routers, taking advantage of the HIP proxy capability. These additional network-based functions include tracking and updating the MH location, security signalling, assigning a network prefix per host identifier, and using the same network prefix within the same network domain to avoid DAD, resulting in improved handover performance. It is important to note that most of the distributed mobility solutions still

experience DAD. The mobility functions further enable an MH, whether or not HIP-enabled, to use the same IP address as it changes its points of attachments within the same domain.

A different proposed approach that enables further enhancement in the flat architecture is the signal-less DM (SL-DM). In this design that could be implemented in a host-based or network-based fashion, a distributed mobility management solution is developed, where data traffic is dynamically anchored at respective points of attachment of the MH during mobility. Handover-related messages are not necessary to facilitate the handover of the MH among the different points of attachment. In addition, the design also introduces an elegant network-based reachability mechanism for the MH. This mechanism ensures MH tracking, secure location updating, assignment of a host identifier per interface, and the use of one IP address for MH reachability within a given network domain. Ultimately, the design avoids signalling overhead, thus improving the handover performance.

In the next section the proposed alternative mobility architectural designs, in hierarchical and flat network architectures, are introduced. This is followed by the advantages that the proposed architectures could bring to network operators.

1.5 Research Contributions to Mobility Management in Future Mobile Internet

In this section, the research contributions are classified into two broad categories, that is, alternative mobility architectural designs and optimisations toward seamless handover, before being presented. The section begins with alternative mobility architectural designs, which are explained in more detail in the hierarchical and flat architectures. This is followed by optimisations toward a seamless handover.

The proposed contributions in this thesis can be outlined as follows:

Alternative mobility architectural designs

Two centralised network-based mobility designs, one at the IP layer and the other at the HIP layer, which address the handover delay, packet loss and signalling overhead are developed.

The designs have different handover performances. Each inherits the features of the layer in which it operates. For example, the network-based mobility at the IP layer extends the Proxy Mobile IPv6 (PMIPv6) to support mobility for HIP-enabled MHs, whereas the network-based mobility at the HIP layer supports the mobility for all IP MHs, HIP-enabled and non-HIP-enabled MHs. In different scenarios under different parameters such as MH speeds, traffic load and simultaneous MHs handovers, the analysis and evaluation for the handover performance of these designs is demonstrated. Both designs employ a mobility approach that uses a central mobility entity to optimise the handover of the MH. Furthermore, handover-related signalling overhead in the air interface is eliminated since both designs are built-based on the network-based approach. Moreover, the HIP nature of the network-based HIP layer ensures that the handover delay signalling overheads are kept to a minimum in the communication with third party servers for security aspects. In addition, in a network-based approach at the HIP layer the network provides mobility management and Host identity protocol (HIP) features to all IP hosts.

Network-based mobility management integrated with a network-based HIP with native security features to support all IP hosts, HIP-enabled and non-enabled hosts, provides a good performance without requiring an upgrade. Additional mobility management functions are also introduced at the access routers taking advantage of the HIP proxy capability.

Two distributed mobility designs, MHPP-extension for Distributed Mobility (DM-MHPP) and Signal-Less Distributed Mobility (SL-DM), are developed, enabling host mobility in a flat network architecture and addressing handover delay, scalability, single point of failure, packet loss and signalling overhead. Again, these designs have different handover performances and characteristics. Having different mobility designs with different advantages and disadvantages allows network operators to choose the design that best suits their requirements. In a DM-MHPP, distributed entities are introduced that provide both mobility management and Host Identity Protocol (HIP) features by the network to all IP mobile hosts. In the SL-DM, distributed mobility design that ensures efficient routing between the communication parties, MH and CH, by its dynamic traffic anchoring mechanism is introduced. Another advantage that SL-DM adds is that the SL-DM can be employed at the TCP/IP or HIP layer; SL-DM is a protocol stack-independent mobility design.

Optimisations toward a seamless handover

Two attachment detection mechanisms, one utilising the Neighbour Discovery Protocol (NDP) and the other not, are introduced to further improve handover performance. From simulation experiments, the detection mechanism that does not use the NDP has shorter handover delays and smaller packet losses than the one that uses the NDP. In the latter, the MHs successfully send their cryptographic identifier, from their HIP layer or by HIP proxy for non-HIP MH, to the mobility entity. Consequently, a secure movement between different networks can be ensured.

In addition, qualitative and quantitative investigations for HIP and some widely referenced HIP-based micro-mobility solutions as well as the researcher's Mobility-enabled HIP Proxy (MHPP) solution are conducted. Qualitative and quantitative investigations for PMIP and some widely referenced PMIP-based extensions as well as the researcher's DM-MHPP proposed solution. A MHPP-extension for inter-domain handover that can be offered for all IP MHs. An elegant reachability mechanism for flat network architecture is employed with SL-DM. Furthermore, this thesis presents a review of widely used approaches that are employed at the IP/HIP layer to the optimised handover performance of MHs in different mobility scenarios such as micro-mobility and macro-mobility.

1.6 Thesis Outline

The organisation of the remainder of this thesis is as follows:

Chapter 2 presents background information about mobility management and widely employed approaches to support host mobility. In addition, the background and overview of the Host Identity Protocol (HIP) and its extensions are introduced as a base architecture to support host mobility solutions.

Chapter 3 addresses mobility management protocols at the IP or/and HIP layer related to the researcher's proposed designs or technology these designs have utilised, and their mobility approaches as well as their seamless handover approaches. In particular, related research in the

context of addressing intra- and inter-domain handover in a secure and seamless manner with these mobility solutions is reviewed. This review advocates that the network-based mobility architecture is promising and has some advantages over the host-based approaches in terms of handover performance such as the releasing of signalling overhead on the link between the MH and the network. Furthermore, the technical challenges that need to be addressed in the area of secure, scalable and seamless mobility architecture in Future Mobile Internet, in particular, seamless vertical handover to ensure non-desirable interruptions to active service, are highlighted.

Chapter 4 introduces the proposed seamless mobility architectures referred to as Hybrid HIP and PMIPv6 (HIPPMIP), and Mobility-enabled HIP Proxy Protocol (HMPP). The HIPPMIP is a network-based architecture at the IP layer while HMPP is a network-based architecture at the HIP layer. Both mobility architectures employ a central mobility entity to manage the IP handover of MH with different handover performances. Possessing mobility architectures with different performances allows network operators to choose the one that best satisfies their needs and requirements. The design goals for each are also presented.

In addition, for HIPPMIP and HMPP, the principles of operation, signalling flow and security considerations are discussed. In HIPPMIP the handover mechanism is employed at the IP layer of the network whereas in HMPP it is employed at both the IP and HIP layer of the network. Thus, the handover procedures are executed in the network without the involvement of an MH. Consequently, active sessions of an MHs are securely and seamlessly preserved by a centralised mobility entity during movement.

Chapter 5 demonstrates the implementation and simulation issues of the proposed mobility architectures that use a central mobility entity, that is, a centralised mobility approach. It first gives a brief overview of the network simulator, that is, the OMNeT++ network simulator, particularly in the context of its wireless and mobility modelling. In addition, an overview is presented of the evaluation framework in terms of the simulation setup environment and the topologies. Issues pertaining to the implementation, configuration and simulation of HIPMIP and MHP are also presented. Moreover, this chapter also includes the performance evaluations and the handover performance results obtained from the conducted simulation experiments with a

comparative handover performance analysis between the proposed HIPMIP, MHP, HIP, Micro-HIP and PMIPv6 in terms of handover delay, packet loss and signalling overhead. Many parameters such as increasing the number of MHs and/or CHs that influence handover delay components, packet loss, and signalling overhead are investigated.

Chapter 6 presents the additional proposed seamless mobility architectures referred to as Distributed Mobility with HMPP (DM-HMPP), and Distributed Mobility without handover-related signalling/signal-less DM (SL-DM). The DM-HMPP is a network-based architecture at the HIP layer while SL-DM is a general mobility approach, which is protocol stack-independent. Both mobility architectures do not depend on a central mobility entity to manage the IP handover of MHs. Again, possessing mobility architectures with different handover performance allows network operators to choose the one that best satisfies their needs and requirements.

In addition, for DM-HMPP and SL-DM, the principles of operation, signalling flow and security considerations are discussed in Chapter 6. In DM-HMPP, the handover mechanism is employed at the HIP layer of the network. Thus, the handover procedures are executed in the network without the involvement of an MH. Consequently, MHs' active sessions are securely and seamlessly preserved by distributed mobility entities during movement. In SL-DM, the handover mechanism could be employed at the IP or HIP layer because of its Stack-independent mobility approach. Furthermore, in SL-DM, information about the IP changes of MH will not be sent in control messages, instead they are included either by the MH itself or by the network, with the data packets as an option. Thus, the handover-related messages are eliminated and MHs' active sessions are securely and seamlessly preserved during movement.

Chapter 7 demonstrates the implementation and simulation issues of the proposed mobility architectures that use distributed mobility entities, that is, a distributed mobility approach. It first provides a brief overview of the evaluation framework in terms of the simulation setup environment and topologies. Then issues related to the implementation and simulation of DM-MHPP and SL-DM are presented. Moreover, this chapter also includes the performance evaluations, and the handover performance results obtained from the conducted simulation experiments with a comparative handover performance analysis between the proposed DM-MHPP, SL-DM, MHP, HIP and PMIPv6 in terms of handover delay, packet loss and

signalling overhead. Again, but this time for the distributed mobility approach, many parameters such as increasing the number of MHs and/or CHs that influence handover delay components, packet loss, and signalling overhead are investigated.

Chapter 8 furnishes the conclusions and the contributions of this thesis. The chapter further recommends some direction for future research related to the topics investigated during this research.

Chapter 2 Mobility Management Background

This chapter commences with a discussion of the basic concepts of management for host mobility in Section 2.1. This is followed by a discussion about host mobility in the TCP/IP stack and HIP stack in Section 2.2 while Section 2.3 presents host mobility support in hierarchical and flat networks.

2.1 Basic Concepts in Host Mobility Management

This section presents a discussion of the basic concepts of management for host mobility.

2.1.1 Mobility Definitions

To make MHs reachable for a host that might be interested in communicating with them, the current location of the MH must be reported to a well-known place (server or rendezvous), which is publicly known directly or via another known server such as a domain name server. Let us assume that, MH and CH have established a session while the MH was connected to subnet11, which includes two base stations/access points at domain1 (Figure 2-1). After a few minutes from the establishment of the session while the session is active, the MH has decided to move from BS/AP1 to BS/AP2 in the same subnet. Such an MH movement, that is, L2-mobility (Figure 2-1), will not result in a change to the IP address of the MH, since the access router (AR), that is, AR1, remains the serving IP Point of Attachment (PoA). In this thesis, as in many other works, such MH movements are referred to as layer-2 handover (L2-HO). In this case, L2 mechanisms could manage the movement of the MH. If the MH has later decided to move from BS/AP2 to BS/AP3 in a different subnet, not only will L2 PoA, for example, BS/AP2, be changed but also IP PoA, for example, will be changed from AR1 to AR2. Such MH movements, that is, IP micro-mobility (Figure 2-1), result in a change to the IP address of the MH if the access routers, AR1 and AR2, advertise router advertisements in a multicast manner, that is, AR2 sends the same network prefix(es) to all hosts in its subnet (if the access routers, AR1 and AR2, employ a multicast mechanism to advertise router advertisements). If the used mode for router advertisements is the unicast mode, that is, a unique network prefix(es) sent to a specific host, an MH could return the same IP address even in IP micro-mobility because

movements between different subnets belong to the same domain. Irrespective of the router advertisement mode, without host mobility management in this scenario, data traffic from the CH to the MH will be sent to the MH's old network, in this case to subnet11. This is because the CH is only aware of the MH's old IP, which belongs to subnet11. On the other hand, if the MH has configured a new IP address, the data traffic from MH to CH will be routed to the CH with a different source IP since the packets are sent from a different location, for instance from subnet12. Consequently, the CH drops data packets that have a source IP address that does not belong to any of its (CH) active sessions.

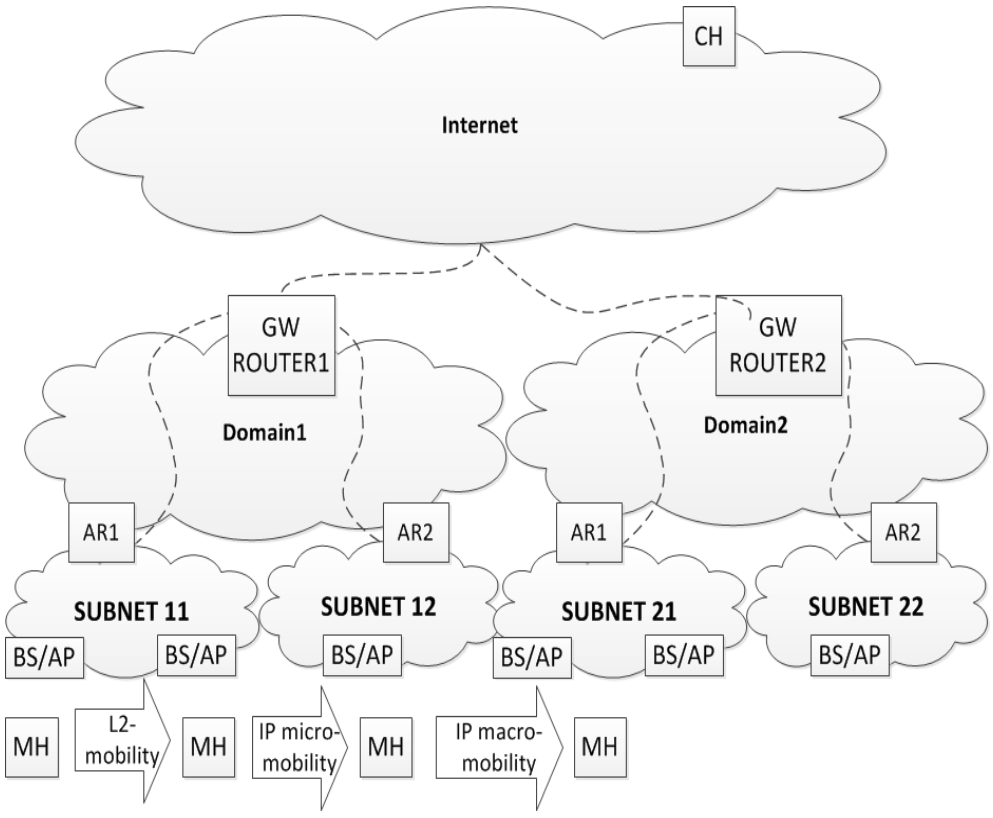


Figure 2-1 Host mobility within an administrative domain and across domains

As explained in the above mobility scenario, a host movement that results in a change of an IP address of the MH is referred to as an IP handover. A mechanism that enables an MH to perform an IP handover is known as host mobility management while a mechanism that enables subnetworks and/or whole networks is referred to as network mobility.

In some cases, network mobility support could be more challenging than host mobility

support. Nevertheless, efficient mobility architecture can be optimised to address challenges that might arise when used for network mobility support. It is important to note that this thesis is mainly concerned with host mobility support, which is one of the important aspects in forthcoming future networks.

2.1.2 Mobility Types

In this subsection, the types of mobility are identified and a brief description for each type is given. While the literature has suggested multiple ways of categorising mobility, the broad distinction between high level mobility and terminal/ host mobility is particularly useful. Thus mobility can be classified into two mobility types, namely, high level mobility and terminal/host mobility.

High level mobility includes service mobility, personal mobility and session mobility. In service mobility a user can access his/her services to which the user is subscribed to regardless of the network service provider to which the user is currently accessing or connected. Address books, call logs, media preferences, and buddy lists are a few examples of services that can be accessed irrespective of the service provider and device used. In personal mobility, presented as part of Universal Personal Telecommunications (UPT) as stated in [36], a user can be globally reached by a single ID that is unique to that user, and can originate or receive a session by accessing any of his or her terminals. Personal mobility for multimedia applications is discussed in [37]. In session mobility, a user can maintain an ongoing session while changing terminals. For example, if a user has more than one active session, for example voice and game on a smart phone, he/she can transfer one of these sessions to any convenient device. [38-40] furnish a few examples of the approaches that can be utilised for session mobility implementation. Discussions about how active sessions can be transferred between different hosts/terminals are presented in [41] with a discussion of some technical aspects pertaining to session mobility. The proxy-based, client-based, and server-based architectural solutions are also utilised to support the web session mobility and are presented in [42-44]. For example, [45] is used to support the HTTP session mobility.

Lastly, terminal/host mobility refers to the ability to maintain connectivity while changing

points of attachment as a result of user mobility or switching between partially or fully overlapped networks. The latter can take place without physical movement between the networks. In terminal mobility, the handover process can be performed "softly", where the MH connects to the new network before disconnecting from the current one, or "hardly", where it disconnects from the current network before connecting to the new network. Terminal mobility can result in a change of access point only, known as layer-2 handover, or a change of access point and access router, known as an IP or layer-3 handover.

Terminal mobility can be implemented in either a host-based or network-based mobility manner. In host-based mobility solutions, such as MIPv6 and HIP, the MH is one of the entities that participates in mobility management, but in network-based mobility solutions, such as PMIPv6, the MH does not participate in mobility management. Thus, network-based mobility solutions support MHs irrespective of the host's capabilities. Exclusion of the MHs from participating in the mobility process also accelerates deployment of the mobility solution and reduces mobility signalling overhead between the MH and access points (AP). Furthermore, a network-based mobility approach is easy to manage and control, and is sufficiently flexible to enhance or upgrade [15].

2.1.3 Mobility Scenarios (Micro and Macro Mobility)

During a communication session, an MH may move within a single domain (micro-mobility) or move to a different domain (macro-mobility) [16]. These two main scenarios can be managed at different layers of the conventional TCP/IP stack [17]. As shown in Figure 2-1, IP micro-mobility refers to an MH's movement from one subnet, for example, subnet11 to another, for example, subnet12, belonging to the same domain. In addition, IP macro-mobility refers to an MH's movement from subnet12 in domain1 to subnet21 in domain2. Such MH movements not only change the BS/AP and AR2 but also change the gateway (GW) router, for example, from GW router 1 to GW router 2.

2.2 Host Mobility Support in TCP/IP and HIP Stacks

Host mobility support is one of the key features of the next generation networks which

are the All-IP-based heterogeneous networks [7]. The duality problem of IP addresses [46] in simultaneously serving as both host identifier and locator on the Internet, is the major issue that makes host mobility support challenging. In the standard TCP/IP stack, the IP is a routing address which has to change as a mobile host (MH) moves, changing its routing path in the network. However, the socket of a network session is identified by the IP address together with the port number. Therefore, the network session will not survive such changes of the IP address. To solve this dilemma, a new namespace is introduced to identify the network session, so that the IP address is used only as a locator. This locator/identifier split approach provides a better framework to develop solutions to support mobility, multihoming, IPv4 and IPv6 interoperability as well as security.

One such locator/identifier split approach is the use of two separate IP addresses in MIP [10] to support host mobility on the Internet. A static IP address is used to identify the network session, a dynamic IP address is used for routing and a mapping between these two addresses is maintained. Another locator/identifier split approach is HIP [47, 48] which provides secure mobility support in a simpler manner than the MIP based solutions [13, 21, 22]. Yet both MIP (v4/v6) and HIP are host-based protocols, requiring new functionalities in the MH protocol stack. Although the latter approach, HIP, is relatively recent, this thesis has discussed it in some detail in Section 2.2.1, specifically the features that can facilitate and strengthen host mobility support.

2.2.1 Host Identity Protocol

The IP address has been used both as an identifier of a communication session and as a network locator; in the standard TCP/IP stack, the upper layer protocols such as TCP and UDP are bound to the IP addresses. As an MH moves and changes IP address, the reconfiguration of the IP address breaks the ongoing TCP or UDP session. HIP [48] introduces a new namespace (host identity name space) to serve as host identifier to establish and maintain a communication session between the communicating parties, while the IP address serves only as a locator of the current point of attachment (PoA) of the host. In the HIP protocol stack (Figure 2-2), a new sub-layer (i.e., Host Identity Layer) decouples the transport layer from the inter-networking layer, thus making the ongoing communication independent of the host location. This is because the transport protocols are bound to the HI (i.e. 128 bits host identity tags (HITs) for the IPv6

application and 32 local scope identifiers for the IPv4 application). In addition, the translation between the HI and the respective IP addresses takes place at the host identity layer in both sending and receiving nodes.

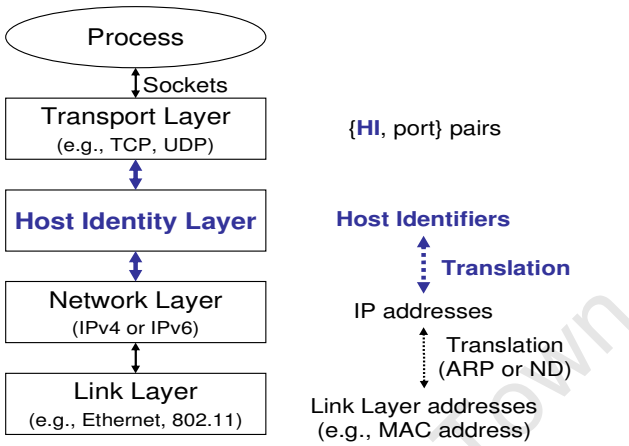


Figure 2-2 The HIP protocol stack

2.3 Host Mobility Support in Hierarchical and Flat Architectures

Regardless of whether a mobile solution uses a single IP with an identifier, HIP, or uses two IPs, one as an identifier and the other as a locator, MIP, most mobility solutions are primarily designed for hierarchical architectures. The current Internet architecture is struggling to support future requirements in many ways such as a loss of universal connectivity; inefficient support for mobility and multihoming; unwanted traffic; and a lack of authentication, privacy and accountability (application mobility, host mobility, and sub-network level mobility), hence its performance is being affected. The Future Internet Design Initiative of the USA's National Science Foundation [49], the 6th and 7th framework of the European Union [50], and the Asia consortium [51] are all indicative of the realisation of the need for 'clean slate' solutions to the problems encountered by the current Internet architecture.

Besides the evolution of access networks and their applications and requirements, the current Internet architecture is also faced with the challenge of supporting high numbers of mobile hosts that have inundated the market. While researchers are designing architecture for the future Internet, it is important to keep in mind that a significant portion of Internet users today are

mobile and expect to access their services wherever they go with the same quality as at their previous location.

This chapter has provided an overview of the concept of mobility and the types of mobility based on the different factors used to categorise mobility such as location, scope, etcetera. The particular categories of mobility solutions have directed us towards the key challenge of IP duality. This chapter, having also considered the widely used solutions to this problem, notes that the literature recommends a single IP with an identifier approach (HIP), based on the experience with hierarchical networks. The remainder of this thesis will extend the HIP approach to consider both hierarchical and flat networks.

Chapter 3 Existing Mobility Management Approaches and Limitations

In the Internet, mobility support concerns the binding of identifiers and locators of the mobile host as well as the updating of active mobility agents. The latter affects traffic routing, handover latency, signalling overheads, packet loss and packet jitter. These are the evaluation criteria on which the related work is reviewed. To efficiently perform these mobility functions, mobility solutions employ various approaches which depend on the structure of the underlying architecture, including the stack's layer of the mobility solution, and the mobility management parties, that is, entities that run the mobility protocol.

An approach that statistically defines mobility entities to be consulted for every IP handover is referred to as a centralised mobility approach. This centralised approach has been widely studied and used. Some of these solutions relating to the researcher's proposed mobility architecture with a cartelised mobility approach and/or technology, on which the proposed mobility architecture is built, are reviewed (3.1).

Recently, another approach in which there is no need to only consult with specific mobility entities has been introduced. In this case, mobility services are offered by any of the distributed mobility entities. Such an approach is referred to as the distributed mobility approach. Some of the widely referenced distributed mobility solutions that are related to the researcher's proposed mobility architecture are reviewed in (3.2), with a distributed mobility approach and/or technology on which the proposed mobility architecture is built.

Therefore, for now the mobility solutions are broadly divided into centralised and distributed approaches, based on the approach they employ to manage host mobility. Accordingly, they are reviewed and the limitations that need to be considered are also highlighted.

3.1 Centralised Mobility Approaches and Limitations

In this section, mobility solutions and their extensions that employ the centralised

approach to support the host mobility are reviewed. As host mobility can be implemented in either a host-based or network-based mobility manner, the researcher further classified the related work, that is, centralised mobility protocols, into host-based mobility protocols and network-based mobility protocols. In host-based mobility solutions, such as MIPv6 and HIP, the MH is one of the entities that participate in mobility management, but in network-based mobility solutions, such as PMIPv6, the MH does not participate in mobility management.

Regarding centralised host-based mobility solutions, the mobility solutions that run at the HIP layer of the HIP stack, such as HIP, are reviewed in (3.3.1) while the other mobility solutions that run at the IP layer of the TCP/IP stack, such as MIPv6, are only briefly mentioned in this thesis. This is because the researcher's proposed mobility designs employ HIP as a major technology, that is, the reason for the inclusion of host-based mobility solutions at the HIP layer; and a network-based approach, that is, the reason for the inclusion of network-based mobility solutions at different layers. Network-based mobility protocols are classified similar to host-based mobility solutions, that is, according to the layer of the underlying protocol stack layer at which mobility protocols are implemented. The network-based mobility solutions that run at the IP layer of the TCP/IP stack, such as MIPv6, are reviewed in (3.1.3). It is important to note that the first network-based mobility solutions that run at the HIP layer are introduced by this thesis and discussed in detail in 4.2 and analysed in 5.2.

3.1.1 Host-based Mobility Protocols at the HIP Layer

This section briefly describes the existing host-based mobility solutions for HIP and the shortcomings of these solutions. The handover latency varies in different handover scenarios [52], for example in macro-mobility and micro-mobility scenarios.

While there are some proposed solutions, there is, to date, no complete mobility management solution for HIP [53-55][25]. A local rendezvous server (LRVS)[55] has been used in the micro-mobility architecture for HIP. The LRVS extends the normal HIP rendezvous server (RVS) to perform a Network Address Translation (NAT) as well as the normal RVS functions. Once the MH enters a given local domain, it detects the LRVS in the visited network either by actively initiating a service discovery procedure or passively waiting for a service announcement

according to the HIP Service Discovery [56]. Then the MH registers itself at the LRVS. The LRVS also registers the MH's IP address and other information at the Domain Name Server that has been extended for HIP support [57]. The MH, therefore, notifies the LRVS, instead of the correspondent host (CH), to redirect the data traffic to its new location, that is, the new local IP address. However, this solution does not avoid IP address configuration and re-registration at the LRVS whenever the MH moves from one subnet to another within the same domain. The IP configuration, which requires Duplicate Address Detection (DAD), delays the handover process as the re-registration takes considerable time, further contributing to handover latency. Moreover, for the registration, the MH always sends its new IP address to the LRVS even when there is a cross-over point between the old point of attachment and the new one. So the time required to execute the re-registration at the LRVS is relatively higher than at a topologically closer cross-over point. Furthermore, before the registration is completed, the LRVS forwards the packets that are destined for the MH to the previous Access Router (AR) in which the MH was present at the time. This obviously increases packet delay and loss.

The second method for securing micro-mobility that is more realistic for hierarchical mobility domains [53], focuses on the authentication of the location binding update messages to prevent possible security issues such as man-in-the-middle attacks and DoS attacks. It uses a regional anchor point (RAP) which supports the dynamic binding between the endpoint identifiers (EIDs) and their IP addresses. Once an MH enters a given region, it does not need to register at any mobility anchor point within that region. During the security association (SA) establishment, mobility anchor points in the region learn the required security context and current location information of the MH, while the nearest anchor point only knows the shared secret key of the communication session. This solution is based on the use of Lamport one-way hash chains and secret splitting techniques to bind the messages of location updates together and to establish an SA between the MH and the nodes (e.g., anchor points in a domain) along the path of the MH and CH.

However, this solution behaves like a macro-mobility solution in many situations. For example, if the Lamport one-way hash chain reaches the seed value or a man-in-the-middle attack between the MH and the nearest anchor point (NAP) occurs, this solution requires the

creation of a new hash chain. Furthermore, the scheme still needs to reconfigure its local IP (LIP) if the MH changes its point of attachment, thus affecting handover latency, signalling overhead and packet loss as well as compromising location privacy.

Finally, a HIP based mobility management architecture solution which uses tight coupling between the Universal Mobile Telecommunication System (UMTS) and WLAN is proposed in [54]. The architecture uses an RVS in the UMTS network to manage the handover process with a strategy to establish a new connection before terminating the previous one. However, it still suffers from the same problem faced by [53, 55] in terms of IP configuration delay as a result of IP address changes. The signalling flow of this scheme is similar to the signalling flow of the scheme in [55], but uses the RVS, rather than the LRVS, to manage the mobility in a domain. Even though the handover performance is improved, it still needs to be optimised.

Finally, mHIP, a micro-mobility solution [25] for HIP, overcomes the limitations of other solutions in the micro-mobility management environment for HIP. However, it introduces other problematic issues, for example, signalling overhead after the handover completion of a specific MH and thus inefficiency affecting the handover performance of other MHs. mHIP encounters the same problems faced by [55] when there were many MHs in the network, especially in the neighbouring agents. Furthermore, in this solution, an agent acts on behalf of a corresponding host (CH). Therefore, the movement of a corresponding host (CH) is not considered by the mHIP and thus inefficiently affects the handover performance. However, even though the handover performance is improved, it is still not optimised or completed.

In [58], A. Leonardo et al. propose a mechanism to enhance MH movements in a micro-mobility environment. Their proposed solution is based on: a set of different performance evaluations; experienced results from a testbed based on the infraHIP implementation. In addition, their solution has been built-based on the usage of the HIP and mainly in the proactive update process, which allows the MH to reduce handover delays and improve the transfer of HIP sessions. However, the proactive approach in the IP handover of the MH only manages to avoid the associated delay for a specific process such as the authentication but does not remove the required control messages.

In [59], Z. Gurkas Aydin et al. proposed an enhancement for the handover performance of HIP micro-mobility. To achieve that, researchers introduced a LRVS proactive location update mechanism and a method that minimises the total radio resource utilisation in their architecture, subject to the QoS constraints of the MH, and particularly for the delay-sensitive applications. Simulation results demonstrate that the proposed mechanisms can enhance radio resource utilisation and, thus, ensure the fulfilment of the requirements for the active real-time applications of the MHs. However, this solution faces the same problem encountered by [58]

In [60], Q. Yinghui proposes HIP-based mobility management for an MH handover between heterogeneous networks. To achieve that, researchers introduced an RVS into the architecture that tightly coupled UMTS/WLAN. In addition, for Mobile IP support, each GGSN of the UMTS system is collocated with a home agent. Furthermore, the GGSNs are also co-located with an RVS. Thus the proposed architecture is backward compatible to non-HIP MHs. This research claims that the proposed solution has reduced the MH handover delays and cost when compared to Mobile IP based solutions. However, this mobility solution still experiences DAD, which are long delays, and does not support the local host mobility.

This subsection has reviewed the centralised host-based mobility solutions that run at the HIP layer (thus HIP technology) and highlighted the limitations of these mobility solutions. It is significant that the number of mobility solutions that employ HIP technology is growing as the literature increasingly recommends a single IP with an identifier approach (HIP), based on experiences with hierarchical networks. This is due to the features that HIP offers in support of mobility and mobility-related functions such as multihoming and security. The remainder of this chapter will review the network-based mobility protocols at the IP and HIP layers in (3.1.2) and (3.1.3) respectively.

3.1.2 Network-based Mobility Protocols at the IP Layer

This section briefly reviews the existing network-based mobility solutions for HIP-enabled and non-HIP MHs in (3.1.2.1) and (3.1.2.2) respectively as well as the shortcomings of these solutions.

3.1.2.1 For HIP MH

In [61], G Iapichino et al. combine PMIPv6 and HIP to achieve a secure global and localised mobility management scheme for multihomed MHs. Researchers integrate security and multihoming features of the identifier/locator split architecture introduced by HIP with the network-based mobility management scheme of PMIPv6 to inherit features of each protocol. In particular, this HIP-PMIP combination ensures an efficient micro-mobility solution for HIP MH as well as inter-PMIPv6 domain extension for PMIPv6. Consequently, the HIP-PMIP combination supports inter-technology handover and multihoming in a secure way. Performance evaluation of the HIP-PMIPv6 scheme and experimental results; and measurements of UDP throughput during MH movement from one access point to another, have demonstrated the viability of the scheme. However, this scheme still needs to authenticate MHs at a third party, for example, an AAA server, thus introducing additional signals and some delays. Furthermore, advantages of this HIP-PMIP combination can only be offered for HIP MHs but not for non-HIP MHs.

Similarly in [62], U. Cespedes et al. combine Proxy Mobile IPv6 and Host Identity Protocol (HIP) for seamless Internet access in urban vehicular scenarios. The researchers consider non-HIP hosts (legacy hosts) without mobility support, in this case mobility is supported by a vehicle's mobile router (MR), and HIP-enabled MHs. The proposed scheme has reduced signalling overheads and packet losses during intra- and inter-domain handover. However, non-HIP MHs can only roam and preserve the active communications if moved together with their MRs.

In [63], H. Bo et al. propose a network-based localised mobility management solution, by combining HIP and PMIPv6, to handle an MH handover in a secure way. Based on the conducted performance analysis for the handoff latency and handover-related signalling for HIP; and the proposed solution, research shows that better handover performance in addition to battery power savings, CPU resources as well as location privacy support can be obtained. However, this mobility solution faces the same problem expressed by [61] and [62].

3.1.2.2 For non-HIP MHs (legacy host)

Proxy MIPv6 (PMIPv6) [14] extends MIPv6 to provide network-based mobility support which is not implemented in the MH protocol stack. Since MH participation in mobility-related signalling is not needed, such network-based solutions optimise handover performance in terms of handover latency and signalling overheads [15]. However, PMIPv6 lacks elegant secure mobility support. PMIPv6 is a network-based mobility management solution that improves handover delay, packet loss and signalling overhead; yet it lacks native support for security resulting in long delays due to the establishment of security associations or authentication procedures.

Media Independent Handover (MIH) services are utilised by many mobility solutions to optimise different handover components such as security and attachment detection delay components. In [64, 65], researchers utilise the MIH services to reduce the PMIPv6's authentication delay component. The addition of MIH allows the MH to be authenticated before leaving its old network and attaching to a new one. Furthermore, to proactively establish a tunnel to redirect the traffic to the MH's new location and/or authenticate the MH when performing IP handover, [66, 67] use the MIH services to commence the handover procedures ahead of time. Consequently, the utilisation of MIH services enables the proactive start of handover procedures and hence effectively optimises handover performance in terms of handover delay and packet loss. However, using MIH services requires additional signalling messages and may add some delays due to the involvement of the MH in the handover process.

Similarly, in [68], I. Kim et al. use MIH services to achieve a low latency handover scheme for PMIPv6. The use of MIH services minimises the scanning delay component at layer 2 during network discovery in IEEE 802.11 wireless networks. Thus, the information service provided by MIH is used to efficiently trigger network discovery to speed up the handover procedures. In addition, similar to Fast Handovers for Mobile IPv6 (FMIPv6), the proposed scheme utilises proactive handover approaches by employing a buffering technique to reduce packet loss due to handover. However, a combination of different techniques from different layers may introduce unnecessary operations for handover, thereby increasing signalling overhead and delay.

In [69], I. Kim et al. utilise the MIHF services to provide a link-layer trigger mechanism. In addition, bi-casting is also used to reduce packet loss to achieve seamless handover for the PMIPv6-network. From the simulations results, handover performance is optimised, that is, the lost packets and handover delays are reduced. However, bi-casting, if not properly controlled, might result in an inefficient use of network resources. Furthermore, like PMIPv6, this mobility solution consults a third party about handover-related security aspects when the MH performs an IP handover. Thus this solution experiences a long handover delay and high signalling overhead.

The Proxy Mobile IPv6 (PMIPv6) is developed to enable the IPv6-MH to perform an IP handover in a network domain called a PMIPv6 domain. Such an IP handover is referred to as an Intra-domain handover. Some solutions aim to extend the PMIPv6 to enable the IPv6-MH to move between two different PMIPv6 domains. This is because the movement of the IPv6-MH within a PMIPv6 domain is as frequent as the movement between different PMIPv6 domains, since the PMIPv6 is selected as a candidate for the next generation wireless networks such as 802.16e and 3G/3.9G.

In this regard, Soochang Park et al. in [70], propose a network-based mobility management mechanism between different PMIPv6 domains, thus eliminating the need for an MH to have any mobility solution even for an inter-domain. To achieve that, during the inter-domain handover, routers in the home and visited PMIPv6 network domains establish tunnels, mechanism concatenated bi-directional tunnels, between the home domain and visited domain. Furthermore, in this solution, local mobility anchors (LMAs) and mobility access gateways (MAGs) in the home and visited domains carry out an exchange of signalling messages for mobility management on behalf of the IPv6 hosts. From the measurements and simulation results, the proposed scheme has reduced handover delay and packet loss. However, this solution, as with many other mobility solutions at the IP layer, experiences an additional delay component and related signalling since it lacks native security support. Another challenge is that of supporting mutlihoming in a secure way.

In [71], for inter-domain handover, G. Giaretta et al. propose the PMIPv6-MIPv6 interworking solution according to two inter-domain movement scenarios: (1) an MH with MIPv6 enters a PMIPv6 domain and then the host moves to a different PMIPv6 domain; and (2)

an MH without a MIPv6 moves between different PMIPv6 domains, home and visited. In this solution, the MIPv6 protocol is used for global mobility and the PMIPv6 is used for mobility inside the PMIPv6 domain. In the case where an MH without MIPv6 moves between the home and visited PMIPv6 domains, the LMA of the home network functions as the MIPv6's home agent (HA) so that the MH registers a new address from a new PMIPv6 network as the care-of address (CoA) of the MIPv6. However, both scenarios only work for an MH that has the MIPv6 protocol. Furthermore, registration, which is a cumbersome process, is needed for each MAG change and thus introduces unnecessary handover delay and signalling overhead.

In [72], Z. Chen et al. propose a dynamic fast authentication and authorisation scenario during inter-domain mobility, which could reduce delay between different domains. These researchers developed their fast handover scheme, which is implemented at the access router, based on a fast handover for Mobile IPv6 and a handover context transfer protocol [73]. However, secure context transfers result in long delays and introduce additional handover-related signalling overheads.

In [74], J-W Baik et al. propose the addition of a multicast server to the PMIPv6 to enable a seamless handover between different domains, utilising the multicast server to preserve the session and IP connectivity. Thus the proposed scheme enables the MH to preserve services irrespective of the domain the MH is connected to. Performance analysis demonstrates that, inter-domain handover reduces handover delays. However, this solution inherits the shortfalls from which the [72] suffers.

In [75], A. Diab et al. combine the Mobile IP fast authentication protocol (MIFA) with the hierarchical MIP (HMIP) to support fast intra- and inter-domain mobility. In this solution, researchers propose a framework to support mobility in all IP networks. From the results, the proposed solution has reduced handover delay and packet loss. Delays during inter-domain mobility are optimised to be similar to those during intra-domain mobility. However, this solution displays the same shortfalls as those in [14] .

In [76], R. Hsieh et al. propose an architecture for seamless handover, S-MIP, that is based on the hierarchical approach and a fast-handoff mechanism, in conjunction with a

handover algorithm based on pure software-based, movement tracking techniques [77]. From the analysis and discussion it seems that this proposed architecture could reduce handover delay and packet loss. However, additional delay and signalling will be experienced due to authentication of handover-related messages.

Some analysis of handover performance for host-based mobility solutions such as MIPv6 and its derivatives are also given in [78-81] and for network-based mobility solutions such as PMIPv6 are given in [82, 83]. Some information about the required QoS in mobile networks are presented in [84].

3.1.3 Network-based Mobility Protocols at the HIP Layer

Network-based mobility protocols at the HIP layer refer to a mobility solution that typically employs a Mobility-enabled HIP proxy or the addition of a HIP layer with HIP-based mobility to the network's entities to enable non-HIP MHs to move freely even when connected to a HIP-enabled CH and to continue to receive packets at the new location. In fact, to the researcher's best knowledge, this thesis proposes the first network-based mobility protocols at the HIP layer (see Section 4.2).

3.2 Distributed Mobility Approaches and Limitations

This section reviews mobility solutions and their extensions that employ a distributed approach to support the host mobility. Like centralised mobility protocols, distributed mobility protocols have been classified into host-based and network-based mobility protocols. In the distributed host-based mobility solutions, those that run at the HIP layer are reviewed in Section 3.2.1 while those that run at the IP layer of the TCP/IP stack are reviewed in Section 3.2.2. The network-based mobility solutions that run at the IP layer of the TCP/IP stack, such as MIPv6, are reviewed in Section 3.2.2. It is also important to note that the first distributed network-based mobility solutions to run at the HIP layer is introduced by this thesis, and discussed in detail in Section 6.1 and analysed in Section 7.1.

3.2.1 Host-based Mobility Protocols at the IP Layer

A number of distributed mobility management schemes have been proposed as repose for the evolution of networks from hierarchical to flat architecture. In [85], P. Bertin et al. propose a distributed, dynamic and mobility-based management solution for flat IP architecture, as implemented by [86, 87]. The proposed solution dynamically anchors the MH traffic at the access node (AN). However, when the MH visits another AN, the IP flow remains anchored at the AN, where the setup was initiated. Consequently, the traffic after the MH handover resumes a longer route for the longer lasting traffic. Such long routes can adversely affect delay-sensitive applications, especially real time applications.

In [88], G. Fabio et al. propose a solution similar to [85], using MIPv6 design principles and a Cryptographic Generated Address (CGA) to secure binding update signalling. However, the solution still anchors the traffic at the point where the traffic was initially set up.

3.2.2 Network-based Mobility Protocols at the IP Layer

In [89], M. S. Bargh et al. extend the PMIPv6 with a simultaneous binding mechanism to enhance handover performance, and reduce the handover delay and related packet loss. Using the proposed solution, some handover processes are proactively performed while the MH is attached to the current network. In this proposed solution, the previous MAG proactively prepares the MH handover, based on available information. Later, when an MH loses its IP connectivity with the current network, the MH can hand over and attach to the new network. The performance analysis demonstrates that the handover performance is optimised. Furthermore, to reduce the handover-related packet loss, an appropriate buffering mechanism is employed at the new access router. However, packets received at the new router will be delayed and/or dropped if the buffer is full.

In the IETF, many optimisations, such as those offered in [90-93], are proposed to further enhance the handover delays, packet losses and signalling overheads in the flat network architecture. However, for active real-time applications during handovers, the above mentioned proposals imply that the PMIPv6 handover performances need to be optimised and thus further research is highly required.

In [94], to enhance the mobility management protocols, W. J. Song et al. propose a

network-based mobility approach in which they introduce new functional elements to be placed either in the current network or new network, or in both, in order to reduce handover delay and packet loss. Thus, the MH resumes its active communication when it receives the buffered packets via the new network. However, in this mobility solution, the handover delays and packet loss are still considerable for ongoing real-time communications.

This chapter has reviewed the related host-based and network-based mobility solutions that employ centralised or distributed mobility approaches in Sections 3.1 and 3.2, respectively. The particular categories of mobility solutions have directed the researcher towards the key challenge of IP mobility in both hierarchical and flat network architectures. The widely-used solutions for this challenge have also been considered in this chapter. In addition, the limitations of these solutions were highlighted. In summary, reviewing of the centralised mobility solutions, host-based and network-based approaches, indicates that most of the mobility management protocols generally exploit layer-2 and layer-3 signalling messages sequentially, hence suffering the consequences of insufficient handover performance as mentioned above. In fact, it should also be appreciated that mobility protocols do not support seamless, secure and scalable handovers, particularly vertical handovers, in their current form.

Chapter 4 Network-based Mobility Solutions for HIP-enabled and Non- HIP-enabled Mobile Host

In this chapter, the researcher introduced his proposed two centralised designs, a novel coordinated hybrid of PMIPv6 and HIP; and a network-based mobility management function integrated with a HIP proxy function at the access routers to support all IP hosts. Both designs aim to optimise handover performance in heterogeneous wireless networks in terms of providing efficient, secure and negligible handover delay architectures. It is important to note that these designs are complementary and have different features. These different features satisfy different requirements for network operators. The chapter begins with a discussion of the Hybrid HIP and PMIPv6 (HIPMIP) and their details in Section 4.1 and related subsections respectively. This is followed by a discussion of the Mobility-enabled HIP Proxy (MHP) and its details in Section 4.2 and related subsections respectively.

4.1 Hybrid HIP and PMIPv6 (HIPPMIP) Mobility Management for Handover Performance Optimisation

In this section, the researcher proposes an elegant coordinated hybrid of PMIPv6 and HIP, which he called HIPPMIP, to optimise handover performance in heterogeneous wireless networks in terms of providing an efficient, secure and negligible handover delay scheme. In the researcher's HIPPMIP scheme, the MH moves while keeping its communication context active through HIP association and also maintaining a stable IP address for packet routing even under MH mobility conditions in a PMIPv6 domain.

4.1.1 Need for HIPPMIP

The handover delays, handover-related security vulnerabilities and handover-related signalling overheads are some of the main challenges in the Future Mobile Internet (FMI). The Mobile IP standard was introduced some years ago and later improved to Mobile IPv6 (MIPv6) [95] to provide mobility support for the next generation IP-based Internet. However, it has been discovered that this standard has very long handover delays and high packet losses hence

interrupts active connections during the MH handover event. Various MIPv6 extensions, for example HMIPv6 [11] and MIPv6 Fast Handovers [12], have also been proposed to improve MIPv6 performance particularly in localised mobility (micro-mobility) environments. Unfortunately, they inherit most of the shortfalls of MIPv6.

MIPv6 and its extensions or any IP layer mobility management protocol semantically overloads the IP addresses. That is, the IP addresses are used as both a location identifier (where I am) and a host identifier (who I am). Furthermore, the upper layers or protocols, for example TCP, UDP, etcetera are bound to the IP addresses. Thus, when an MH changes PoA and effectively changes its IP address, active upper layer connections are broken. This therefore, requires the reconfiguration of various parameters and states of the MH to re-establish the broken connections at the new location and it usually takes a significant time period which results in long handover delays and high packet losses. Consequently, the quality of the user experience of the active communication context as well as security is seriously compromised.

Naturally, a solution to this problem of the dual role of IP addresses in IP layer mobility management protocols is to separate the functions of host identification and location identification from each other. The HIP [18], which runs in a HIP layer between the transport layer and the internetworking layer, separates this location and identity roles of IP addresses by introducing a new namespace, the HI. One consequence of such a decoupling is that new solutions to the network-layer mobility and host multihoming are possible [19] and furthermore, the mobility and multihoming can be handled in a secure manner [13].

The Proxy Mobile IPv6 (PMIPv6) [14], a widely used network-based localised mobility management protocol, has been discovered to have lower handover delay than its host-based IP layer mobility management counterparts such as HMIPv6. However, PMIPv6 still relies on the dual role of IP addresses for location and host identity. To provide full and efficient mobility management with reliable security support and negligible handover delay for NGWNs the researcher hypothesise that intelligently combining PMIPv6 and HIP could meet this goal.

Thus, for many reasons, an integration between the HIP and PMIPv6 is needed in an IP handover between heterogeneous wireless networks:

- Vertical handover is necessary in the Future Mobile Internet and is more challenging compared to horizontal handover; therefore the host identifiers have to be handled in a secure manner between the affected heterogeneous wireless networks without introducing additional handover delay and signalling.

- To ensure that there are host identifiers, introduced by HIP, that are independent of the MH's network location and the access network through which the MH is connected.

- To enable preservation of the MH's active sessions during the actual handover as the MH performs handovers across homogeneous/heterogeneous networks.

- To provide a common framework that can utilise the MH's stack features/capabilities during IP handover across heterogeneous wireless access networks since each requires a specific handover strategy. Thus the common framework facilitates the MH's handover procedures in the diverse network environment in Future Mobile Internet to ensure a seamless, vertical handover in a secure manner.

4.1.2 Design Objectives for HIPPMIP

The design of the HIPPMIP is based on two principles: (1) distributed caches are employed to store new R1 pre-computed packets; and (2) MH will use the same IP address, as it remains within a single domain.

The caching of a new pre-computed R1 packet at the LRVS optimises the handover performance when re-keying is required because of a handover. Besides re-keying the HIP, the SA can also be timed out. In both cases, a re-establishment of the HIP SA is required.

1. To reduce the handover delay and packet loss for HIP-enabled MH in an intra-domain handover. This can be achieved by reducing the following:

    - Time taken for IP configuration

- Time taken for binding updates (Where a binding update is performed)
- Time taken for security association establishments/updates

2. To minimise the handover-related signalling overhead in the air interface between the MH and the access points.
3. To enable secure and efficient handovers between heterogeneous networks by effectively using host identifiers and host identity tags (HIT) introduced by the HIP from hosts themselves or from HIP proxies.
4. To manage proxy mobility while utilising the MH's stack capabilities such as HIP layer capabilities to maintain the same security level of the HIP.

4.1.3 Protocol Overview

The HIPPMIP is detailed and its architecture defined in [96]. HIPPMIP basically extends the PMIPv6 to efficiently manage mobility for HIP-enabled MHs. To achieve this, the HIPPMIP collocates new functionality into the PMIPv6's mobility entities. Thus, these entities are enabled to set up HI-based connections between hosts, and map HIs to IP addresses and vice versa during HIP packet exchanges between hosts as explained in the HIP architecture. Furthermore, HIPPMIP integrates PMIPv6 and HIP to manage mobility securely with negligible handover delays in a localised heterogeneous or homogeneous environment. By intelligently combining the best of both protocols, an effective handover optimisation scheme is achieved.

4.1.4 Architecture

The architectural framework of the HIPPMIP mobility management scheme in a localised domain is shown in Figure 4-1 below.

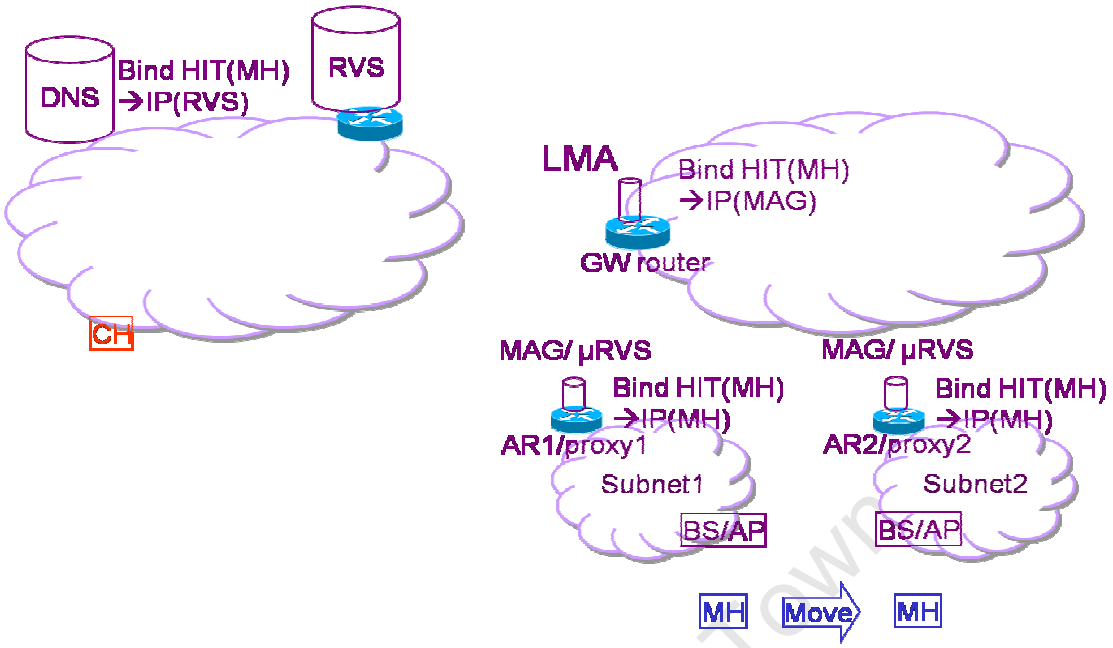


Figure 4-1 HIPPMIP architectural framework

Since PMIPv6 does not require any PMIPv6 functionality installed in the hosts, the MHs in the domain should only be HIP-aware. The PMIPv6's core functional entities, the MAGs, collocate with the HIP RVS, called micro RVS (µRVS), at the access routers and interwork towards a common goal of optimising handover performance. The architecture as shown in Figure 4-1 depicts a situation where only the host (in the PMIPv6 domain) is mobile while the CH is stationery. However, the scheme or architecture can easily extend support to a scenario where both the MH and CH are mobile.

4.1.5 Initialisation

The researcher assumes that the MH is entitled to network-based mobility services provided in the PMIPv6 domain. Thus, when the MH enters the PMIPv6 domain, the MAG (e.g., MAG 1) detects the attachment event typically through the help of MIH services (or layer-2 triggers) and sends PBU to the LMA on behalf of the MH. Typically, the collocated µRVS obtains the MH's HIT during the attachment and this HIT is sent as the MH's identifier in the PBU to the MH's LMA.

Internet MH HoA PMIPv6 domain MAG/µRVS MAG/µRVS CH Common Global RVS

Proxy-CoA LMAA Proxy-CoA Tunnel MAG MAG PBU/PBA LMA Internet CH Traffic PMIPv6 domain MH strongly relies on the self certifying cryptographic identifiers provided by HIP [18] to ensure secure and protected communication between itself and the μRVS. On receiving the PBU, the LMA sends back a PBA including the home network prefix (Per-MH-Prefix) to the MAG. The MAG then emulates the MH's home network on the access network and sends a router advertisement (RA) message to the MH. The MH configures its home address (MH's HoA) which is stable throughout the PMIPv6 domain.

The MH then notifies the μRVS of its IP MH's HoA and consequently the μRVS has the MH's HIT(s) and IP address (i.e. MH's HoA). At this point the μRVS informs the MH of its own HIT and IP address (i.e. proxy care-of-address, Proxy-CoA, of the MAG). Furthermore, the μRVS registers the MH's HIT(s) and MH's HoA(s) to a common global RVS on behalf of the MH to enable reachability of the MH. The registration procedure is defined in [97].

4.1.6 Communication Establishment

If the MH wants to set up a HIP association with a CH, it initiates a HIP Base Exchange procedure by triggering the μRVS to send an I1 packet on its behalf (by utilising the proxy capability of the collocated MAG). The μRVS, therefore, sends the I1 packet via the LMA on behalf of the MH to the common global RVS which is possibly outside of the PMIPv6 domain. The common global RVS is capable of providing a rendezvous registration to any node irrespective of its domain. For the sake of simplicity it is assumed that the CH is already registered with the common global RVS. However, if not, the registration procedure is carried out as defined in [97]. The rest of the Base Exchange is performed directly between the MH (represented by the μRVS) and the CH via their respective locators and using the normal method of routing packets to a node in a PMIPv6 domain. After the HIP association has been established, the nodes can begin sending data packets to each other. The signalling flow diagram of the above explained HIPPMIP setup is depicted in Figure 4-2 below.

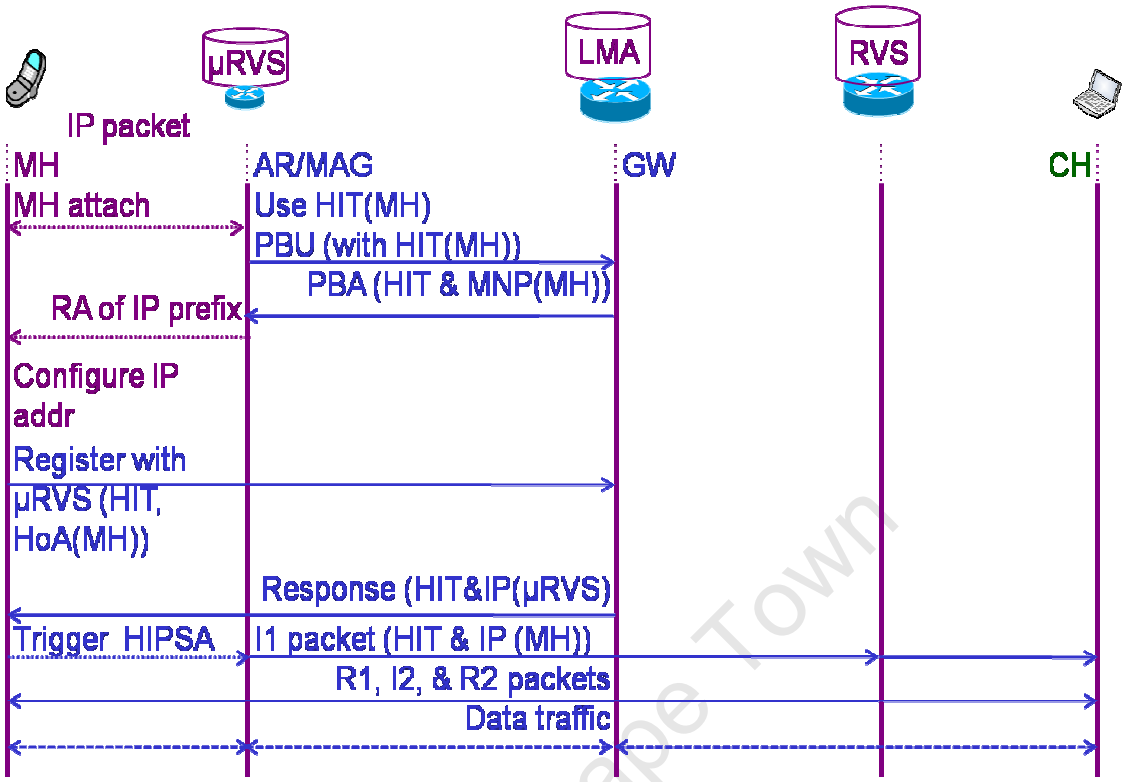


Figure 4-2 HIPPMIP initial registration and communication establishment

Alternatively, if the CH wants to initiate a HIP association with the MH, but is currently unaware of its location, it sends an I1 packet to the common global RVS that has the MH's rendezvous registration. The CH would find the common global RVS address from the MH's Domain Name Server (DNS) record as defined in [57]. The common global RVS then relays the I1 packet towards the MH. However, the LMA intercepts the packet based on the address in the destination address field since it is the topological anchor point and forwards it to the Proxy-CoA of the relevant MAG (and μRVS). The μRVS forwards the I1 packet to the relevant MH's HoA where the IP-HIT address mapping is performed. The rest of the HIP Base Exchange is carried out directly between the MH and the CH using the normal packet routing procedures applicable to a PMIPv6 domain.

4.1.7 End Host Mobility in HIPPMIP

When the MH performs a handover between any PoAs or MAGs (access networks) in the scope of a PMIPv6 domain, it continues to use the same MH's HoA since it always receives a

unique Home Network Prefix (HNP) from any MAG it attaches to in the PMIPv6 domain. Thus, the only signalling performed during handover is the exchange of the PBU and PBA to update the LMA of the current Proxy-CoA to reach the MH for packet routing purposes. Irrespective of this localised location update, the advertised MH's HNP to the MH stays the same (Per-MH-Prefix) hence the configured MH's HoA. Consequently, there is no need to update the MH's parameters at the common global RVS and respective CHs since the MH's locator (MH's HoA) and identifier (HIT) are stable as long as the MH roams within the same PMIPv6 domain. Thus, no HIP update locator packets (i.e., re-address packets) are exchanged. As a result, signalling overheads and handover delays are significantly reduced. The handover signalling call flow diagram is depicted in Figure 4-3 below.

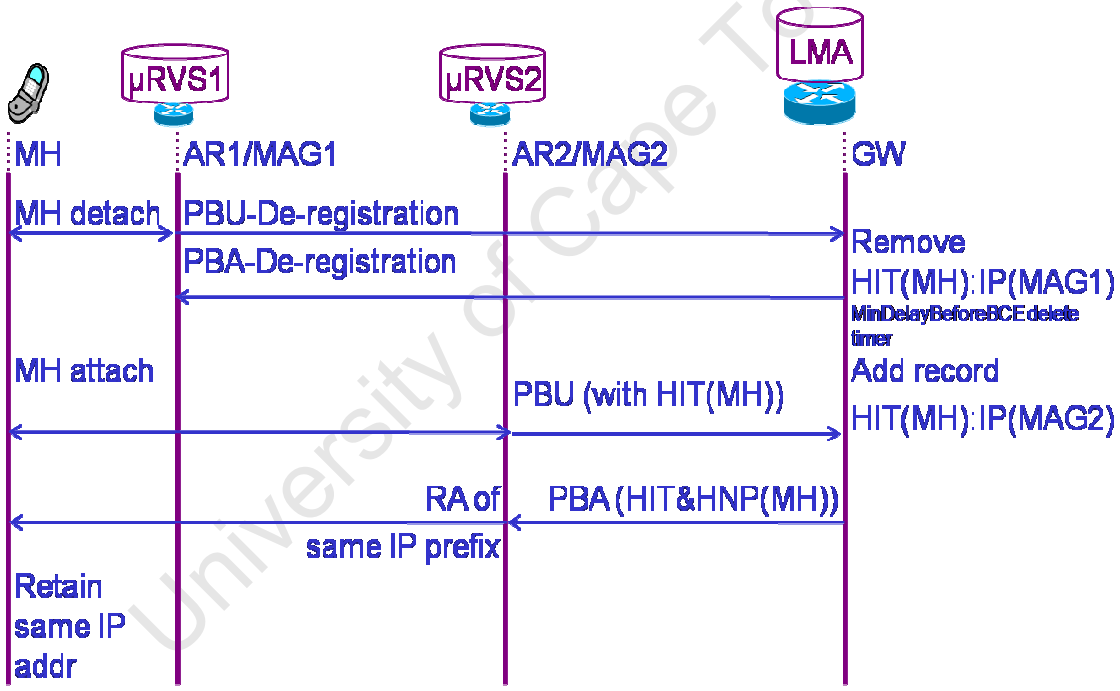


Figure 4-3 Signalling call flow diagram for HIPPMIP handover process

4.1.8 Performance Gains of HIPPMIP

HIPPMIP combines the advantages of PMIPv6 and HIP to produce a powerful mobility management scheme suitable for localised domains. Thus, HIPPMIP reduces over the air signalling overheads, maintains a stable MH locator even when the MH changes PoAs and reduces unnecessary signalling overheads over the core network as well as the localised domain.

Furthermore, HIPPMIP maintains the active communications contexts of upper layers (transport connections) by ensuring stable node identifiers over and above maintaining stable host locators during mobility and handover events. Thus, the handover is transparent as far as both the upper layers and internetworking layer are concerned implying negligible handover delay.

Consequently, packet losses are significantly reduced. With HIPPMIP, update locator packets on the RVS and CHs (peer nodes) are unnecessary hence reducing signalling overheads and delays. The PMIPv6 aspect of HIPPMIP mainly manages packet routing by addressing the IP address configuration of the MH even during mobility, thus ensuring stable MH locators while also providing localised network-based mobility management advantages. The HIP aspect, on the other hand, mainly ensures continuity of the upper layers' communication context by addressing the problem of a stable host identifier even during mobility situations. HIP also addresses authentication in an end-to-end manner to ensure secure communication even under mobility scenarios.

In an ordinary HIP handover, the time taken by the MH to register its new location address and HIT on the RVS as well as de-register from its old location can be time-consuming and cause a long handover delay for localised (micro-mobility) domains which may result in the breaking of ongoing communication. By design, HIP is mainly suitable for global mobility management and not micro-mobility management.

4.2 Mobility-enabled HIP Proxy for non-HIP-enabled and HIP-enabled MH

4.2.1 Need for Mobility-enabled HIP Proxy

The current use of an IP address in the network application session identification cannot preserve the session when the IP address changes. HIP, which is an identity-location separation protocol, provides a better framework to build solutions for mobility, multihoming and security by adding a host identity layer on top of the IP layer. Yet modifying the IP protocol stack and adding mobility as well as other solutions to all the hosts can be impractical to deploy and

interoperate with existing IP hosts.

Furthermore, HIP has security support to enable secured mobility and multihoming, both of which are essential for future Internet applications. Compared to end host mobility and multihoming with HIP, existing HIP-based micro-mobility solutions have optimised handover performance by reducing location update delays. However, all these mobility solutions are client-based mobility solutions. We observe that another fundamental issue with end host mobility and multihoming extension for HIP and HIP-based micro-mobility solutions is that handover delays can be excessive unless the support for network-based mobility is strengthened.

4.2.2 Design objectives for Mobility-enabled HIP proxy protocol (MHPP)

Like HIPPMIP, the design of the MHPP is based on two principles: (1) distributed caches are employed to store new R1 pre-computed packets; and (2) the MH will use the same IP address, as it remains within a single domain. The caching of a new pre-computed R1 packet at the LRVS optimises the handover performance when re-keying is required because of a handover. Besides re-keying the HIP, the SA can also be timed out. In both cases, the re-establishment of the HIP SA is required. In addition to the HIPPMIP's design objectives, MHPP has the following additional objectives:

1. To provide a network-based handover solution for both intra- and inter-domain movements.

2. To reduce the handover delay and packet loss for both HIP-enabled and non-HIP-enabled MHs in the intra- and inter-domain handover. This can be achieved by reducing the following:

    - Time taken for IP configuration, in the intra- and inter-domain movements.

    - Time taken for binding updates (Where a binding update is performed), in the intra- and inter-domain movements.

    - Time taken for security association establishments/updates, in the intra-

and inter-domain movements.

3. To further minimise the handover-related signalling overhead in the air interface between the MH and the access points.

4. To enable secure and efficient handovers between heterogeneous networks by effectively using host identifiers and host identity tags (HIT), introduced by HIP from networks using HIP proxies.

5. To proxy both mobility and HIP for non-HIP MH while maintaining the same security level of a HIP-enabled MH.

6. To enable simultaneous support of mobility for HIP and non-HIP MHs.

7. To reduce handover delays as well as signalling overheads due to consulting a third party on security aspects.

4.2.3 Overview of Mobility-enabled HIP Proxy

This section introduces a network-based mobility management function integrated with a HIP proxy function at the access routers to support all IP hosts. The hosts do not need to possess new functions, including mobility management and HIP capability, other than the existing IP protocol stack. Yet they are able to experience the multihoming capability and the security level native to HIP in addition to receiving network-based mobility support.

Additional mobility management functions are also included at the access routers taking advantage of the HIP proxy capability. These additional network-based functions include tracking and updating MH locations, security signalling, assigning network prefix per host identifiers and using the same network prefix within the same network domain to avoid DAD, resulting in improved handover performance. They enable an MH, whether or not HIP-enabled, to use the same IP address as it changes its points of attachments within the same domain.

4.2.4 Architecture

The architecture for network-based mobility management with a HIP proxy is illustrated

in Figure 4-4. The RVS has been defined in [98] with the DNS to provide reachability of a HIP host by maintaining a mapping between the host identity, which is called a host identification tag (HIT) and an IP address of the MH. The LRVS has also been defined to perform NAT and RVS functions in a given domain [55]. The researcher's design, called Mobility-enabled HIP proxy, adds a set of co-located mobility and HIP proxy functions at the access router. The Mobility-enabled HIP proxy performs HIP signalling on behalf of non-HIP MH so that HIP services can be offered to non-HIP enabled hosts. It also tracks the movement of the MH and updates the MH's binding record. On detection of an MH attachment, it sends an update message to the nearest anchor point, which is the cross-over point between the old point of attachment and the new point of attachment of the MH.

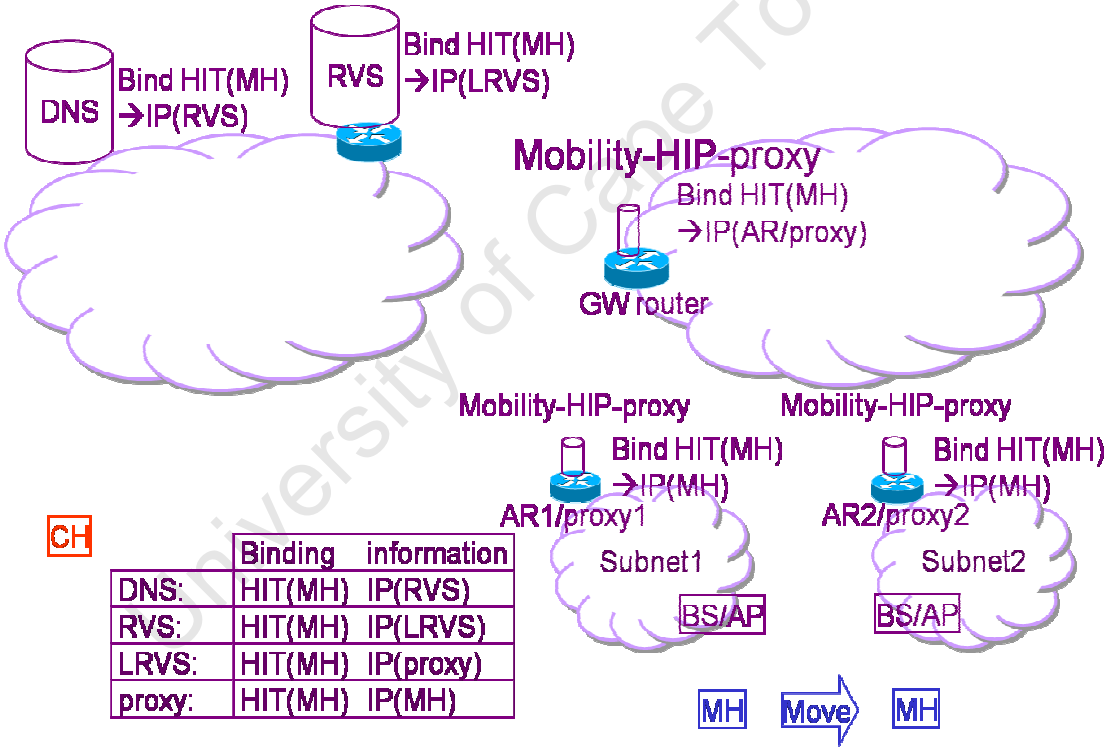


Figure 4-4 Design of network-based mobility management and HIP proxy

The binding information, which is displayed in a table in Figure 4-4, is managed in the hierarchy DNS-RVS-LRVS-proxy to enable the reachability of an MH which is registered with the Mobility-enabled HIP proxy. After registration, the Mobility-enabled HIP proxy contains the binding of the HIT of the MH, HIT(MH), to the IP address of the MH, IP(MH). The LRVS

contains the binding of the HIT of the MH, HIT(MH), to the IP address of the proxy, IP(proxy). The RVS contains the binding of the HIT of the MH, HIT(MH), to the IP address of the LRVS, IP(LRVS). The DNS contains the binding of the HIT of the MH, HIT(MH), to the IP address of the RVS, IP(RVS).

4.2.5 Registration and Reachability

Before using a HIP service, a HIP host needs to register with the service using the registration mechanism defined in [97]. The registration of an MH, which may either be or not be HIP enabled, is depicted in Figure 4-5.

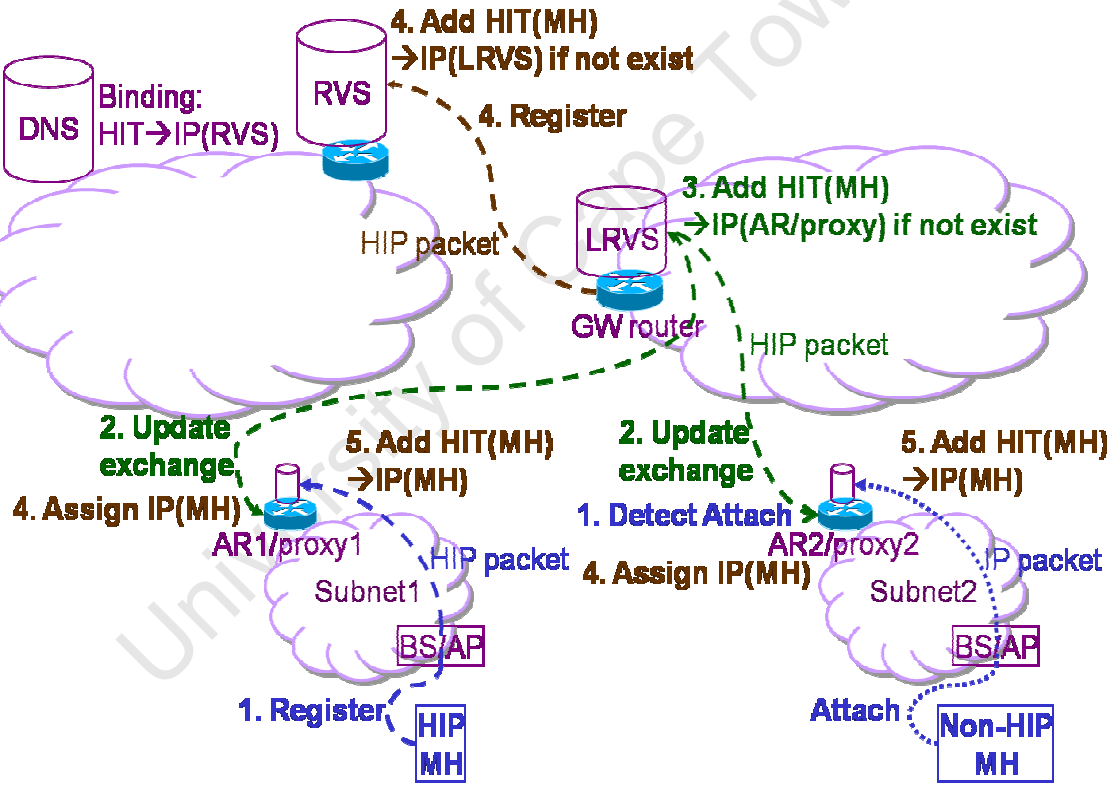


Figure 4-5 Registration of a mobile host, which is or is not HIP enabled

After registration, the MH becomes reachable from any CH which may query the DNS about the location of the MH. The DNS replies with the IP address of the RVS to which the HIT of the MH is registered.

4.2.6 Establishing Security Association

This mobility management design enables data traffic between either a HIP enabled MH or non-HIP enabled MH and a CH. A security association (SA) is set up prior to the data plane traffic. If the MH is a HIP host, the SA ends or terminates at the MH. If the MH is not a HIP host, the SA ends at the Mobility-enabled HIP proxy to which the MH is registered.

When an MH attaches to a Mobility-enabled HIP proxy, it first registers according to the registration procedure described in Section 4.2.5 above. After registration, the MH becomes reachable from the CH.

4.2.6.1 The HIP Initiation-Response Exchanges

To set up a security association in HIP, an initiator and a responder first go through a base exchange. Two pairs of initiation-response packets (I1, R1 and I2, R2) are exchanged to prepare for SA establishment. Either the MH or the CH may be the initiator, and the other one will then be the responder.

The I1 message is illustrated in Figure 4-6 for an MH which is either a HIP host or a non-HIP host. If the MH is a non-HIP host, its Mobility-enabled HIP proxy sends and receives the HIP packets.

As demonstrated in Figure 4-6, a HIP enabled CH may initiate a HIP SA from outside an MH's domain. The CH already has the IP address of the RVS at which the MH is registered, by querying the DNS. For the sake of simplicity, it is assumed that both the MH and the CH are registered at the same RVS.

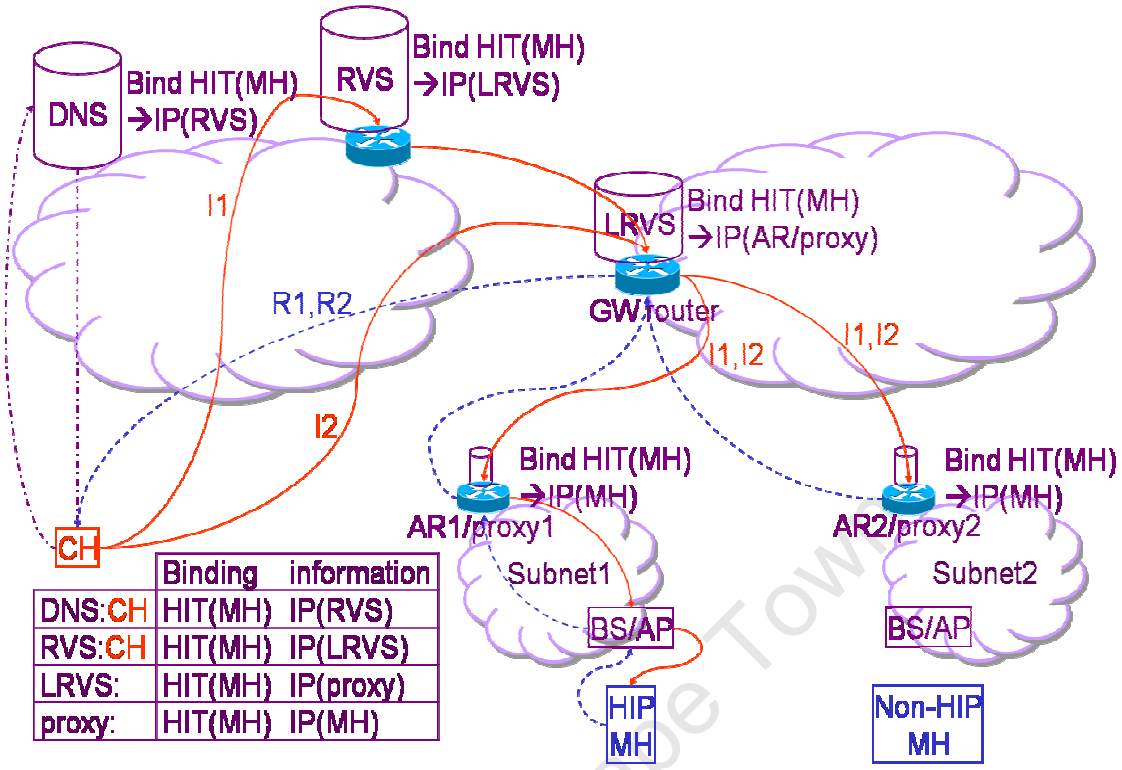


Figure 4-6 The flow of initiation-response messages for a HIP or non-HIP MH

On receiving an I1 packet from the CH, the RVS checks if the destination HIT corresponds to that of a registered MH. If so, the I1 packet is forwarded to the registered IP address of the LRVS. On receiving an I1 packet from the RVS, the LRVS checks whether the destination HIT belongs to a registered MH. If so, the packet is forwarded to the IP address of the Mobility-enabled HIP proxy. The LRVS also stores the binding HIT(CH):IP(RVS):IP(CH). On receiving an I1 packet from the LRVS, the Mobility-enabled HIP proxy checks the destination HIT in the HIP header. If the destination HIT corresponds to that of a registered HIP enabled MH, the Mobility-enabled HIP proxy (proxy1) forwards the I1 packet to the MH. The Mobility-enabled HIP proxy also stores the binding HIT(CH):IP(LRVS). The MH will store the binding HIT(CH):IP(CH), and the MH will send the reply R1.

If the destination HIT corresponds to that of a registered MH which is not HIP enabled, the Mobility-enabled HIP proxy (proxy2) stores the binding HIT(CH):IP(LRVS):IP(CH). The Mobility-enabled HIP proxy (proxy2) will send the reply R1 on behalf of the MH. For a non-HIP MH, the Mobility-enabled HIP proxy (proxy2) will respond to the I1 packet by sending a R1

packet to the CH. The I1, R1, and I2, R2 exchanged pairs are shown in Figure 4-6 for an MH which is either a HIP host or a non-HIP host. To complete HIP SA establishment for a non-HIP MH, the Mobility-enabled HIP proxy (proxy1) and the CH will exchange the remaining I2 and R2 packets. Unlike the I1 packet, the R1, I2, and R2 packets will only go through the LRVS, but not through the RVS.

4.2.6.2 ESP Security Association

After the successful exchange of the two initiation-response packet pairs, a HIP SA will be established between the initiator and responder. During the establishment of the SA, all the proxies along the path between the MH and the LRVS will be aware of the SA context. In data traffic, HIP proxy (proxy2) uses ESP to encapsulate/decapsulate non-HIP MH data packets, whereas HIP MH uses ESP to process its data.

4.2.6.3 HIP Security Association vs IP handover

In HIP, HIP SA can be used from different network locations since the HIP SA is associated with the MH's HIT, which is static, and not associated with the MH's IP address, which is dynamic. In fact, to securely re-use the already established HIP SA for non-HIP-enabled MH, mobility entities or any other entities must be able to share information and process traffic related to a specific established HIP SA.

4.2.7 Handover Mechanisms

In this section the mobile hosts' IP handover for both intra-domain (Section 4.2.1.1) and inter-domain (Section 4.2.7.2) scenarios is presented.

4.2.7.1 Intra-MHP handover

Figure 4-7 shows the handover procedure of a non-HIP enabled MH between two wireless access networks belonging to the same domain and managed by a LRVS. The MH is communicating with a HIP enabled CH, which is in a different domain. However, the MH and the CH are registered at the same RVS.

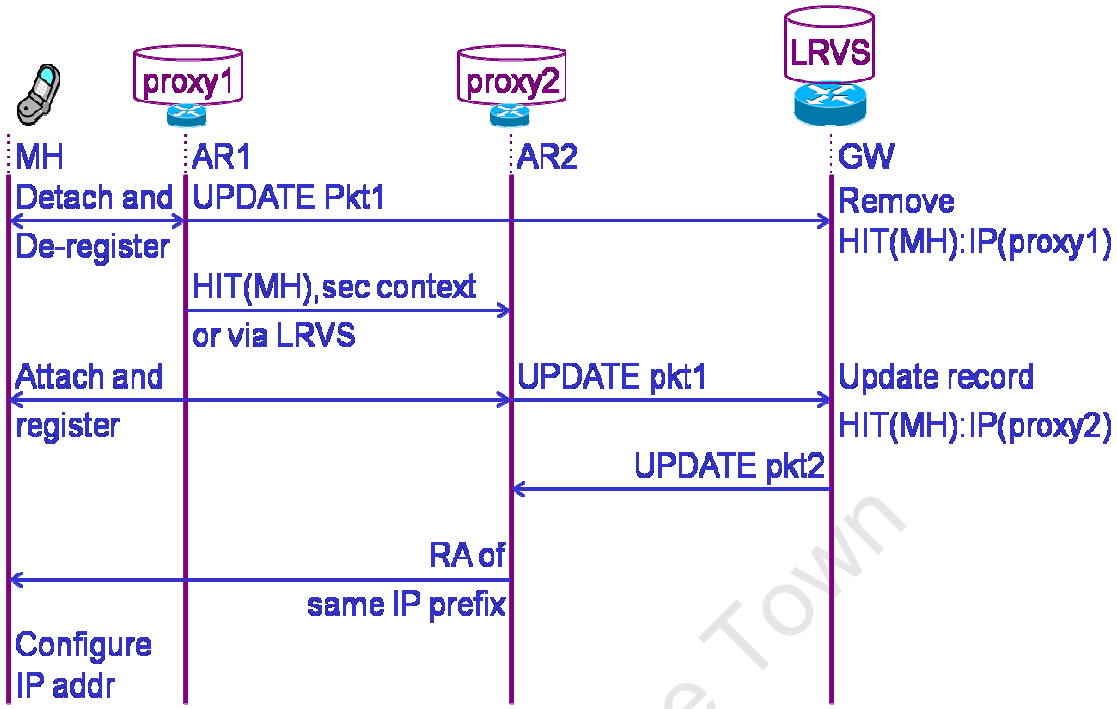


Figure 4-7 Handover procedure of an MH communicating with HIP enabled CH

The non-HIP enabled MH may change its PoA and attach to another Mobility-enabled HIP proxy (proxy2) under the same LRVS. The new access network may be of the same or different network type as the previous access network. Irrespective of the type of access network to which proxy2 is connected and irrespective of whether the MH is HIP enabled or not, proxy2 will be informed about the attachment of the arriving MH. Proxy2 acts as the HIP proxy and updates the binding record of the MH at the LRVS. To do that, it needs to know the context of the HIP SA and the HIT of the MH. Generally, a mechanism is required to securely share this security context with the proxies to which the MH moves.

When the MH performs an intra-domain handover, proxy1 detects the detachment and sends an UPDATE packet (packet1) to the LRVS to de-register its (proxy1) IP address. Proxy2 detects the attachment of the MH and sends an UPDATE packet (packet1) to the LRVS. When proxy2 receives the reply UPDATE packet (packet2) from the LRVS, it will send a Router Advertisement (RA) to the MH. The RA will have the same network prefix that the MH used to configure its IP address in the proxy1 subnet. The MH, therefore, retains the same IP address configuration so that DAD is not required. This procedure significantly reduces the handover

latency, signalling overheads, and packet loss.

When the HIP-enabled MH performs an intra-domain handover, MHP1 (i.e., old MHP) is no longer the serving MHP. The new MHP detects the attachment of the HIP-ENABLED MH and sends an UPDATE packet 1 to the LRVS. On receiving the UPDATE packet 1, the LRVS verifies the HIP-ENABLED MH and then updates the HIP-ENABLED MH's binding record. Afterwards, the LRVS responds with the UPDATE packet 2. Using the content of the UPDATE packet 2, the new MHP sends an RA, which includes the same network prefix that the HIP-ENABLED MH employed to configure its IP address during the initial registration, to the HIP-ENABLED MH. The HIP-ENABLED MH, therefore, retains the same IP address configuration. This may significantly reduce the HOL and signalling overheads due to the handover procedure. It is important to note that the proposed solution is intended for IPv6 networks. In addition, the study in this section is mainly concerned with localised mobility management where the host mobility is very high, whereas the management of inter-domain handovers is presented in the next section.

This HIP-based micro-mobility management solution reduces the HOL and signalling overheads by allowing an HIP-ENABLED MH to use the same IP address (to avoid the DAD process as it remains within a single domain) and sending the HIP-ENABLED MH 's HIT and assigned network prefix to the other MHPs (e.g., MHP2) at an appropriate time. Then, the new MHP sends both the network prefix to the HIP-ENABLED MH to retain the same IP configuration, and the UPDATE packet 1 to the LRVS to set up a new path for the ongoing traffic. The use of the same IP address supports location privacy. Furthermore, the use of HIT in the upper layer protocol instead of an IP address enables the HIP host to use the established HIP associations during and after the handover, since the communication context remains the same. Moreover, reducing the time taken to perform an HIP BE can also reduce the handover delay when the re-establishment of HIP SA is required. Having an MHP also eliminates the need for a new location reachability check between the HIP-ENABLED MH and its peer, because the new location of the HIP-ENABLED MH is known to the serving the MHP. The number of MHPs in a domain depends on the domain's size, and each subnet is managed by an MHP which acts as the authoritative MHP for that subnet. The number of HIP-ENABLED MHs in each subnet must

not exceed the capability of the MHP. This method can also manage the simultaneous move of the communicating parties and multihoming in an easy and efficient way to do so.

4.2.7.2 Inter-MHP handover

Figure 4-8 shows exchanged messages between entities in a wireless communications system as a non-HIP enabled MH performs a handover from one access network to another, which belongs to a different domain managed by a different LRVS, that is, an inter-domain handover.

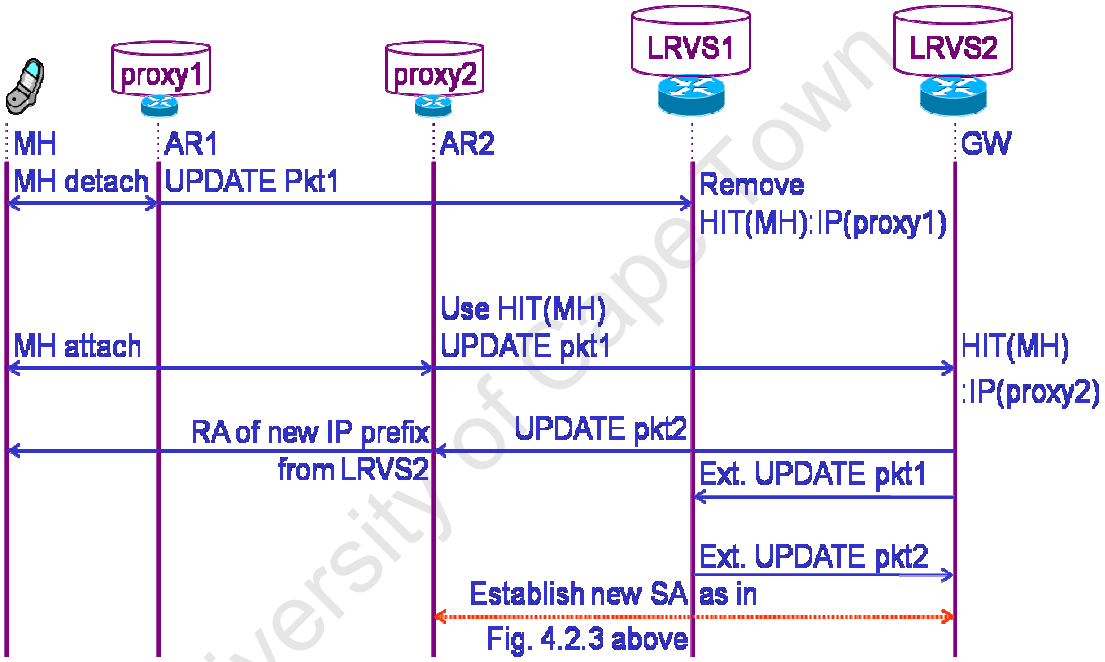


Figure 4-8 Handover procedure of a MH between different domains

The researcher extended the functions of the home network prefix (HNP) to play different roles in different domains, that is, the home domain and the visited domain. For example, HNP1, which is allocated by LRVS1 in the home domain, is used to configure a new IP on a newly attached MH. Furthermore, HNP1 returns the same IP configuration during the MH's Intra-domain handover. In addition, HNP1 in the visited domain managed by different LRVSs, LRVS2, is used to return the same IP configuration during the MH inter-domain handover. It is important to note that the same HNP serves primary roles in the home domain and secondary roles in the visited domain. Therefore, we use primary HNP and secondary HNP as terms to

differentiate between the roles that the HNP plays at a specific time.

Since the handover is not under the same LRVS, proxy1 sends UPDATE packet1 to the old LRVS (LRVS1) to remove the MH's binding, whereas proxy2 sends UPDATE packet1 to the new LRVS (LRVS2). If proxy2 has no record of the MH, it extracts the HNP that the MH used to configure the previous IP address, that is, the IP address configured in the home domain. Thereafter, proxy2 informs LRVS2 about the extracted HNP. LRVS2 then checks whether the extracted HNP is primary or secondary. If the extracted HNP is a primary HNP, the handover procedures are similar to the ones used for Intra-domain handover (Fig.4).

If the extracted HNP is a secondary HNP, LRVS2 determines the LRVS to which the secondary HNP belongs. To accomplish this, the LRVS indexes its list of neighbouring and authenticated LRVSs based on the secondary HNP. In addition, LRVS2 creates a temporary binding for the MH and sends a normal UPDATE packet (UPDATE pkt2) with the secondary HNP to proxy2. Furthermore, LRVS2 sends an extended UPDATE packet (Ex_UPDATE pkt1) to LRVS1. Ex_UPDATE pkt1 is created by adding a new flag (E) to the first UPDATE packet of HIP. The rest of the first UPDATE packet remains unchanged.

On receiving Ex_UPDATE pkt1, LRVS1 uses the secondary HNP of the MH to find the MH binding and consequently sends the MH information in an extended UPDATE packet (Ex_UPDATE pkt2) to LRVS2. Ex_UPDATE pkt2 is created by adding a new flag (E) to the second UPDATE packet of HIP. The rest of the second UPDATE packet remains unchanged. It is important to note that flag (E) enables the LRVSs to differentiate between UPDATE packet senders, Mobility-enabled HIP proxies or other LRVSs.

On receiving Ex_UPDATE pkt2, LRVS2 compares information in Ex_UPDATE pkt2 sent by LRVS1, against information in UPDATE packet1 sent by proxy2. If the necessary information from LRVS1 differs from that sent by proxy2, LRVS2 instructs proxy2 to stop serving the MH and to remove the related binding. If the required information is the same, LRVS2 converts the temporary binding for the MH to a permanent binding.

For the MH's reachablilty directly through LRVS2 (i.e. not via LRVS1), LRVS2 updates the MH binding at the RVS. From the content of the Ex_UPDATE pkt2, the LRVS can reuse the

established SA. Furthermore, LRVS2 continues to deliver the MH data in a secure way. In contrast, LRVS2 can establish a new SA if necessary. However, this new SA establishment adds some delay to the handover latency. To this end, the ongoing data traffic between the MH and its CH flows through LRVS1. In contrast, all new communications is established directly through LRVS2 and not via LRVS1.

4.2.8 Comparison of non-HIP-enabled MH and HIP-enabled MH Handover

This section furnishes a comparison between a HIP-enabled and non-HIP-enabled mobile host in terms of handover-related security and signalling.

4.2.8.1 Security between MH and MHP

A Mobility-enabled HIP proxy is co-located within the ARs that are deployed in secure private networks. In addition, HIP-enabled hosts (i.e., MH and CH) still establish an SA between themselves while MHPs only manage mobility packets using an established SA. Therefore, neither security nor reliability of the HIP MH will be compromised by introducing an MHP in a secure private network.

It is important to note that the researcher provides a network-based micro-mobility support at the HIP layer but not at the IP layer as do some proposed solutions [61, 96]. Solutions [61, 96] are about the use of PMIPv6 [14] to support HIP MHs. Yet, both solutions are using IP technology to support host mobility for the HIP MH. The main difference between providing mobility supports at the HIP layer and the IP layer is that the first can utilise all the HIP features, which are security, multihoming, interoperability between IPv6/IPv4, and mobility. Furthermore, the researcher's proposed MHPP supports the mobility of a non-HIP MH using HIP technology in a secure manner.

4.2.8.2 In Intra- and Inter-MHP handover

Unlike intra-domain handover procedures, in inter-domain the serving LRVS can be changed and thus additional signalling is required. For reachability through the new LRVS, the record of MHs serving the LRVS must be updated.

4.2.9 Performance Gains of Intra-MHP

This scheme proposes a network-based mobility management solution that employs the HIP layer to provide efficient, secure, network-based seamless mobility as well as multihoming support to all MHs, with all signalling overheads on the MH interface removed. Unlike ordinary HIP proxy solutions, this design eliminates the issue of a single-point-of-failure due to services being received only via static HIP proxies.

4.2.10 Performance Gains of Inter-MHP

Inter-MHP support enables a secure, seamless network-based handover across a large geographical area. It further enables a change of the LRVS without experiencing long handovers or violating established HIP security associations.

4.2.11 Security Considerations

HIPPMIPv6 leverages the security mechanisms of PMIPv6 in the management of an MH handover. This is because HIPPMIPv6 is built on top of the PMIPv6. Although HIPPMIP has extended the PMIPv6 to support mobility for HIP-enabled MHs, which have built-in security support, HIPPMIMv6 still relies on PMIPv6 for security concerns in terms of its management of handovers across heterogeneous wireless networks. In fact, HIPPMIP utilises two promising technologies, HIP and PMIP, but it does not introduce an entirely new mechanism to support the IP handover-related aspects of security. It is important to note that security considerations for sending MH identifiers such as HITs in the existing PMIPv6 messages for example update PBUs, is beyond the scope of this thesis. In addition, mutual authentication between the MH and the MAGs/Micro-RVS is also required.

In the MHP solution, mutual authentication between the non-HIP enabled MH and the MHP has to be considered since the non-HIP enabled MH needs to obtain a HIT and thereafter uses the assigned HIT in different networks. Security support in these networks is different and may compromise the security during and/or after the MH handover. Moreover, possible security threats may exist when MHPs are deployed in non-secure networks. In addition, mutual authentication between the HIP MH and MHPs is also required. A trust HIP security association

between the MHPs and the LRVS must exist before they exchange packets. However, the MHP has HIP features, hence it exchanges handover-related messages with the LRVS in a secure way and acts on behalf of the MH. Thus, an established trust between the MN and the HC must exist. However, the detailed studies of these security aspects are considered a part of future research.

In this HIPPMIP implementation, there has to be a third party such as an AAA server responsible for ensuring secure vertical handovers for both HIP-enabled and non-HIP enabled MHs to move between heterogeneous wireless networks. This implementation appears to be lengthy with large signalling overheads for the security process even for HIP-enabled MHs. MHPP achieves secure handover without experiencing additional delay and signalling. As the network domain grows, there is no need to deploy any specific entities for security aspects alone.

This chapter has provided a discussion on two centralised designs, a novel coordinated hybrid of PMIPv6 and HIP; and a network-based mobility management function integrated with a HIP proxy function at the access routers to support all IP hosts. The chapter has discussed the Hybrid HIP and PMIPv6 (HIPMIP) and their details in Section 4.1 and related subsections respectively. This is followed by a discussion of the Mobility-enabled HIP Proxy (MHP) and its details in Section 4.2 and related subsections respectively.

Chapter 5 Experiment, Results, and Performance Evaluation of HIPPMIP and MHPP

In this chapter, the researcher evaluated two of his proposed mobility designs/solutions, which are HIPPMIP and HMPP. These mobility solutions are evaluated by the OMNeT++ network simulator [99] (briefly presented in Section 5.1). He also presented and analysed the results obtained from the proposed mobility solutions, HIPPMIP and HMPP discussed in Section 4.1 and Section 4.2 respectively. The handover performance of HIPPMIP is evaluated and compared against the basic PMIPv6 and HIP. The performance of MHPP is also evaluated and compared against HIP, Micro-HIP, PMIPv6 and HIPPMIP. The discussion of the HIPPMIP handover performance results and analysis is presented in Section 5.2, while the MHPP handover performance results and analysis is furnished in Section 5.3.

5.1 OMNeT++ Overview

This section furnishes a brief description of the OMNeT++; the network simulator the researcher used to develop and evaluate his proposed mobility designs, and the HIPSim++ [100]; an OMNeT++-based simulation model. OMNeT++ is a discrete event and open-source network simulator for the development of models including communication networks, queuing systems, multiprocessors, centralised or parallel processes and other systems [101]. Compared to the open-source NS-2 simulator [102] and the commercial OPNET simulator [103], OMNeT++ is growing and is free to use for academic purposes, which are for non-profit purposes, under the Academic Public License.

In the OMNeT++, which is module-based, simulation models consist of modules connecting together via message passing. The base modules, that is, simple modules, are atomic modules where the behaviour of the solution/protocol is implemented using the C++. To achieve that, the simulation class library of the OMNeT++ is used. Furthermore, modules that consist of simple modules are called compound modules. These modules are connected via links, connecting gates of respective modules, and exchange messages via these links to communicate with each other. Messages include the necessary information such as user data and control data.

In OMNeT++, the messages are defined only by the determination of their fields. After that, OMNeT++ creates the corresponding C++ classes from the file containing the message definitions. In OMNeT++, the NEtwork Description (NED) language is used to describe the network topology, and the C++ language is used to implement the functionality of the design/solutions. Code-independent files, files.ini, are used to set the parameters for the simulation models.

The OMNet++ 4.0 network simulator [99] and HIPSim++ simulation framework [100], that is, a simulation toolset for the evaluation of the HIP and HIP-based solutions , are utilised to implement the HIPPMIP and Mobility-enabled HIP proxy designs. According to the IETF's HIP specifications, HIPSim++ has been built-based on the INET model [104], version 20090325. In addition, HIPSim++ includes the xMIPv6 models introduced by Dortmund University of Technology. Furthermore, the HIP simulation model has been validated against a real-life HIP testbed that employed the implementation of InfraHIP.

5.2 Evaluation of the HIPPMIP

The handover of HIPMIP, HIP and PMIPv6 is each carried out in two partially overlapping IEEE 802.11b (11 Mbps peak data rate) subnetworks. These subnetworks implement HIP, PMIPv6 and HIPPMIP. In PMIPv6 and HIPPMIP the mobility access gateways (MAGs) are co-located with the access routers while in HIPMHIP the Micro-SRVSs are co-located with the MAGs. That is, the mobility in subnetwork 1 and 2 is managed by MAG1 and MAG2, respectively, for PMIPv6, whereas in HIPPMIP it is managed by MAG1/Micro-SRV1 and MAG2/Micro-SRV2 respectively. The simulated topology is illustrated in Figure 5-1 and the simulation parameters are described in table 1.

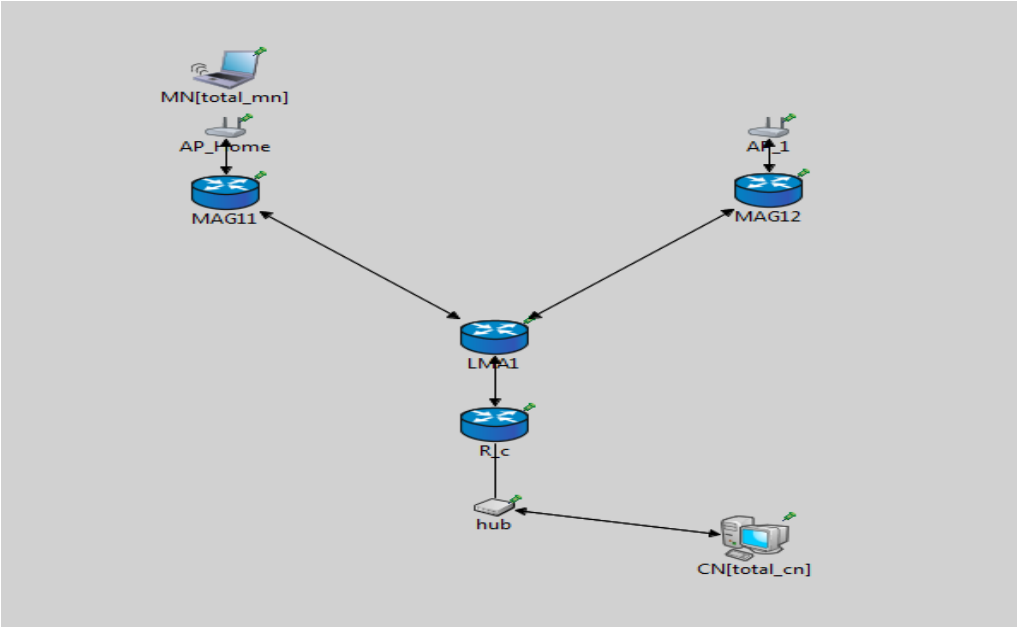


Figure 5-1 Simulation network topology of HIPPMIP

Table 1. Simulation Parameters under Which HIP, PMIP and HIPPMIP are Examined

PARAMETER	VALUE	PARAMETER	VALUE	PARAMETER	VALUE
Speed	1 m/s	Mobility Model	Rectangle	Route advertise Interval	≥ 0.3s
# of POA	2	Packet flow	Bi-dir CBR		≤ 0.7s
# of MH	1	UDP packet transmit rate	0.13 s	AP power	2.0 mW
Grid size(m^2)	850*850	Packet size	256 B	Beacon freq.	0.1s

5.2.1 Architecture of HIPPMIP's Main Mobility Functions in OMNeT++

In this section, the researcher describes the node structure in the OMNeT++ for the HIPPMIP's main mobility entities. According to HIP RFCs, HIPSim++ has provided the HIP-enabled hosts, the Initiator and the Responder, the HIP-enabled servers as well as the Rendezvous Server and DNS server for the HIP architecture. HIPSim++ has utilised the existing INET modules to implement the new functionalities introduced by the HIP. Note that the exiting modules of the INET model as well as the newly introduced modules for HIP are located in the

INET directory, called "/Node/IPv6".

To implement the HIP-enabled host functions in OMNeT++, HIPSim++ has inserted a HIP module, between the transport and network modules, into the INET existing StandardHost6 module. This HIP-enabled host can run both UDP and TCP applications. However, the host is stationary. Similarly, to implement the HIP-enabled MH functions in OMNeT++, HIPSim++ has inserted a HIP module, between the transport and network modules, into the INET existing WirelessHipHost6 module that employs the Mobility Agent for mobile operations.

To implement the new mobility functionalities proposed by the HIPPMIP, developed the PMIP MAGs and LMAs based on the INET existing modules and then inserted the micro-RVSs (Figure 5-2) into the PMIP MAGs. LMAs have also been modified to operate with the HIP RVS and micro-RVSs and to handle the host identifiers, that is, host identity tags (HIT), introduced by HIP modules.

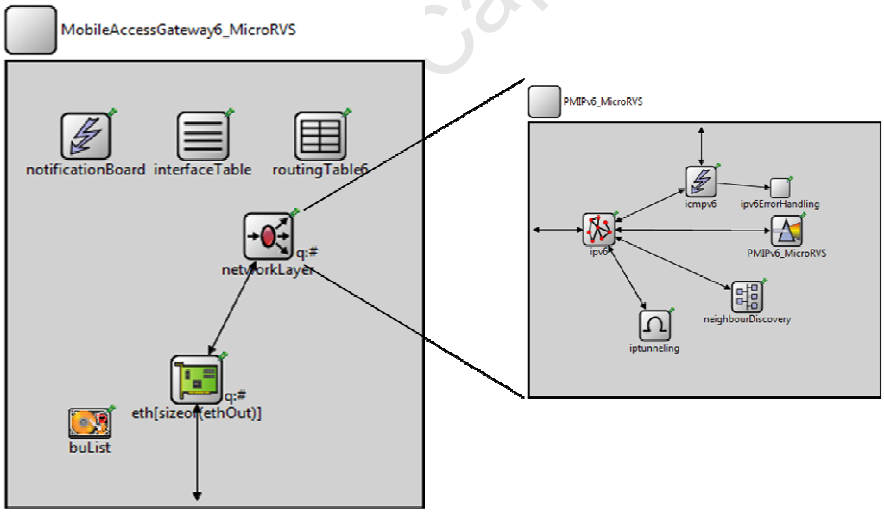


Figure 5-2 MAG with micro-RVS functionality

5.2.2 Simulation Scenarios

In the handover performance evaluation and analysis of HIPPMIP, the researcher considered a scenario whereby a HIP-enabled CH is fixed outside the access network to which the HIP MH is currently attached. Data are exchanged between the CH and the MH at a rate of 15 kbps and are in the form of 256-byte UDP packets. For the sake of simplicity, the researcher

considered only unidirectional data flow from the CH to the MH. The handover is simulated with the MH moving linearly at a constant speed of 1 m/s from one subnet to the other. The simulation parameters of this scenario are described in Table 1.

5.2.3 Performance Evaluation and Analysis of HIPPMIP

Before presenting his investigation of the handover performance for HIPPMIP and its related work, the researcher needs to first identify the evaluated parameters and define what they mean in this simulation context. During this simulation, the handover latency (HOL), lost packets and signalling overhead parameters are investigated. HOL here refers to the time difference between the time when the MH is able to receive packets in the new PoA and the time when the MH was unable to receive packets in the old PoA. The lost packets refer to the number of packets that are lost from the downstream traffic during the HOL. Signalling overhead means the number of required signalling packets per handover that are used for location updates (LUs) or IP address configuration.

In this section, the researcher presented and analysed the handover performance results obtained from the HIPPMIP, PMIPv6 and MHP. The handover delays, packet losses and signalling overheads are investigated. He has also investigated other factors that affect the MH handover performance such as the MH speed, the number of CHs communicating with the MH, and the delay owing to third party consultation.

5.2.3.1 Handover delay

Using the above mentioned simulation environment described in Section 5.2.2, the researcher examined three models (HIP, PMIPv6 and HIPPMIP). In addition, he recoded and analysed a hundred handoffs for each of the three models. The fluctuation in the handover latency (HOL) of the models over the first 20 handover (HO) instances is illustrated in Figure 5-3.

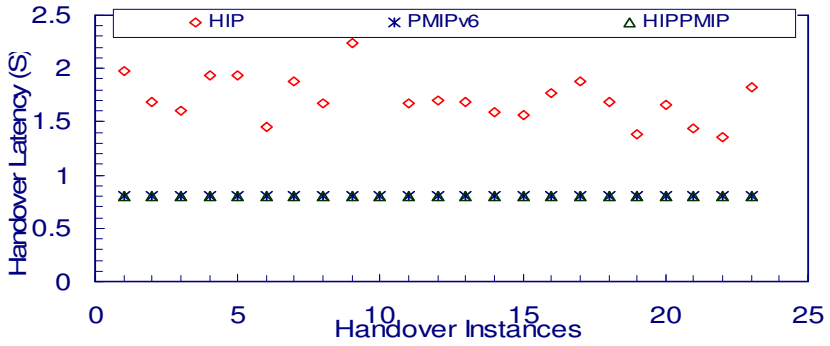


Figure 5-3 The first 20 handoffs for HIP, PMIPv6 and HIPPMIP

The researcher carried out a hundred handoffs for each of the three investigated models. As can be observed from Figure 5-3, fluctuations or differences in the values of handover latency in the three models are observed over the first 23 handover instances. The HIPPMIP is observed to have the same handover latencies, which are consistently below 1 second per handover, as PMIPv6. This is because the HIPPMIP is using PMIPv6 for mobility management.

5.2.3.2 Packet loss

Figure 5-4 depicts the packet loss of the HIP, PMIPv6 and HIPPMIP. The researcher measured the loss of data packets of a UDP application in unidirectional traffic flowing from the CH to the MH during handover. It is important to note that there is no buffering or forwarding technique used to mitigate packet loss.

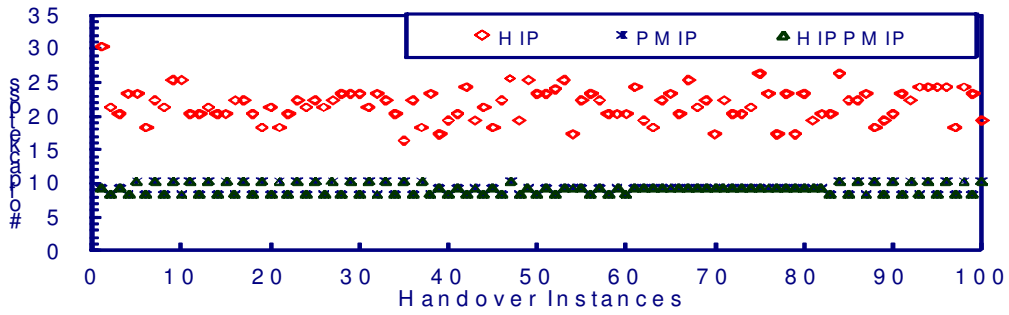


Figure 5-4 The first 100 packet loss for HIP, PMIPv6 and HIPPMIP

5.2.3.3 Signalling overhead

Handover related messages in the HIP, PMIPv6 and HIPMIP during 25000s simulation

time are depicted in Figure 5-5.

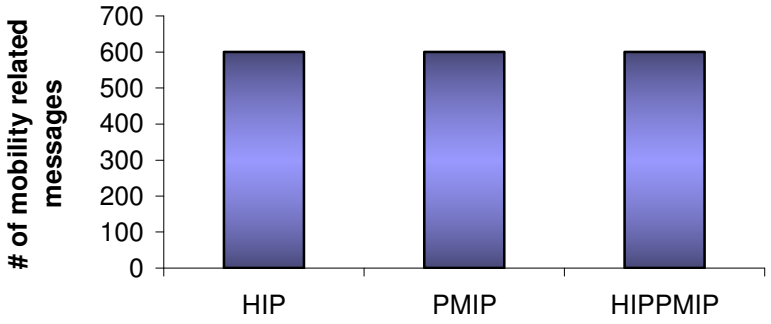


Figure 5-5 Handover-related messages of the HIP, PMIPv6 and HIPPMIP

Although PMIPv6 and HIPPMIP uses a two-way location update protocol while HIP uses a three-way protocol for location updating, it is evident from the figure above that PMIPv6 and HIPPMIP use the same number of signals as the HIP to securely manage the whole process of handover. The signalling overheads of HIP, PMIP and HIPPMIP are also described in Table 2. The first row in Table 2 shows the number of binding update messages when the MH has ongoing communications sessions with one CH. In fact for HIP, the number of binding update messages when the MH has ongoing sessions with *n* CHs is different from those used for one CH (displayed in the table). Thus, the mobility related signalling overheads of the basic HIP are highly affected by the increasing number of *n* CHs with which the MH has ongoing communication sessions. In contrast, the mobility related signalling overheads of PMIPv6 and HIPPMIP are not affected by the increasing number of CHs. This is because PMIPv6 and HIPPMIP update only the network gateway irrespective of how many CHs the MH has with ongoing communications sessions. It is important to note that the HIP does not need to consult any third party on security issues as it has capabilities of self certifying at the HIP layer. However, PMIPv6 does need to consult a third party on security aspects. This third party security consultation brings about additional signalling overheads and adds a further delay to the total handover delay. Unlike HIP, PMIPv6 and HIPPMIP avoid all signals related to DAD as well as signal overheads related to the HIP MH interface.

Table 2. Signalling Overheads of HIP, PMIPv6 and HIPPMIP

Parameters\Scheme	HIP	PMIPv6	HIPPMIP
# of UPDATE packets per IP handover when MH has ongoing communications with 1 CH.	6	6	6
Are there any signalling overheads on MH's interface?	Yes	No	No
Are there any signalling overheads due to configuration of new IP address?	Yes	No	No

The IP handover delay for HIPPMIP is compared with HIP and PMIPv6. It should be noted that in HIPPMIP, there is no need for HIP locator update packets to be sent since the MH IP address stays the same even though the MH changes its PoA due to the Per-MH-Prefix property of the PMIPv6 domain. Thus, it is not necessary to exchange packets to re-establish HIP associations. The security and authentication aspects are established when the HIP association is first established and are maintained even during and after handover since the communication contexts remain the same in as far as the transport and internetworking connections are concerned. Thus, the HIPPMIP shows lower handover delay than HIP and PMIPv6.

5.2.4 Impact of MH's Speed on HIPPMIP's Handover Performance

Figure 5-6 illustrates how different MH speeds affect the handover delay for HIP, PMIP and HIPPMIP. All measurements are taken during the constant bit rate traffic with an interval rate of 0.133333s. Each point in the graph represents an average of all the MH handovers, from the home to the visited network and vice versa, made within 2000s for each different MH speed. The number of handovers the MH performed with different speeds is different. For example with speed of 3mps, the number of handovers (HOs) is three times the number of handovers the MH has performed with a speed of 1mps. It is important to note that, in such a case, the researcher considered the average of all the MH handovers for each different speed. It is evident from the

figure and measurements that the handover performance of network-based solutions, PMIP and HIPPMIP, have less effect than that of the host-based solution, HIP. This is because in PMIPv6 and HIPPMIP, the MH that moves with a different speed does not participate in the handover procedures while it does when an HIP is used.

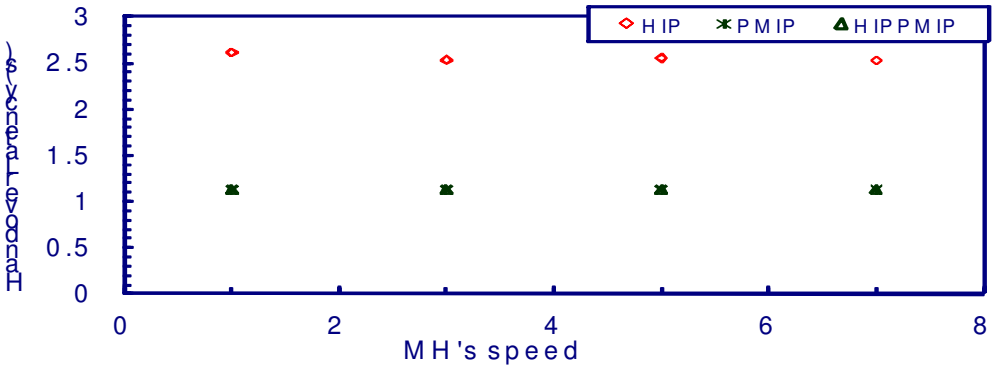


Figure 5-6 MH's speed impact on HO performance of the HIP, PMIPv6 and HIPPMIP

5.2.5 Impact of the HIPPMIP Handover Performance due to the Security Delay Component with a Third Party

Figure 5-7. illustrates the relationship between the delay owing to the security process involvement with a third party, for example, an AAA server and the handover delay of HIPPMIP. Every point on the graph represents an average of the MH handovers, layer-2 and layer3 handovers, while the MH was moving with a speed of 1mps. Like PMIPv6, the HIPPMIP is extremely affected by the third party security check delays and thus adds additional delays.

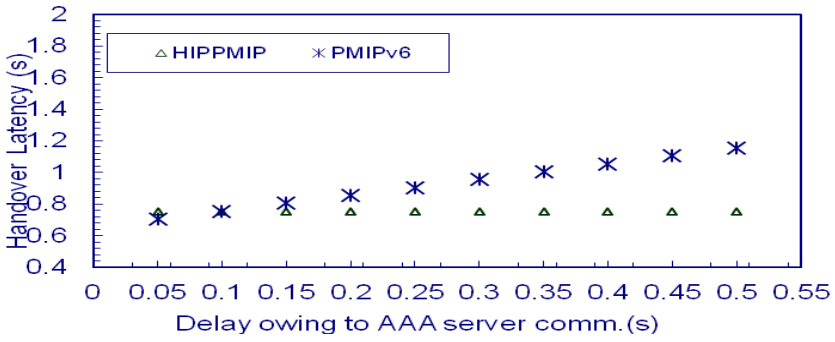


Figure 5-7 Impact of AAA server delay on HO delay of the PMIPv6 and HIPPMIP

5.2.6 Impact of Number of CHs on HIPPMIP Handover Performance

The following table, Table 3, displays the results of the impact of the number of CHs with which the MH is connected during the handover as well as the on average packet loss and handover delay for all the HIP, PMIPv6 and HIPPMIP.

Table 3. Signalling Overheads for HIP, PMIPv6 and HIPPMIP

Parameters\Scheme	**HIP**	**PMIPv6**	**HIPPMIP**
# of UPDATE packets per IP handover when MH has ongoing communications with 2 CH.	9	6	6
# of UPDATE packets per IP handover when MH has ongoing communications with *n* CH.	3*(*n* + 1)	6	6

In the above table we can observe that PMIPv6 and HIPPMIP perform better that HIP. In HIP, at a certain number of CHs, for instance, when there are more than eight CHs, the handover performance begins to perform inefficiently. This is because, in HIP, the MH exchanges many mobility-related signalling messages at the same time and therefore the network and mobility agents become saturated. In addition, the increase in handover-related messages owing to the number of CHs, with which the MH is connected, increases the delay in the queue of shared links. In fact, the queuing delay in these links starts to increase as the number of handover-related signalling increases and thus causes congestion. However, even with these congested links the CHs and MHs still continue to exchange packets of active sessions. These congested links can however cause packet loss since a handover takes longer to finish or sometimes even fails. This phenomenon is worse in the case of the HIP since it is a host-based mobility protocol. In

addition, most of the handover signalling has to be sent over wireless links between the MHs and the mobility entities in the network.

5.3 Evaluation of MHPP

The handover of MHPP, HIP and PMIPv6 is each carried out in two partially overlapping IEEE 802.11b (11 Mbps peak data rate) subnetworks. These subnetworks implement HIP, PMIPv6 and MHPP. In PMIPv6 the MAGs are co-located with the access routers while in MHPP the mobility-HIP proxies are co-located with the access routers. That is, the mobility in subnetwork 1 and 2 is managed by MAG1 and MAG2, respectively, for PMIPv6 whereas in MHPP it is managed by mobility-HIP proxy1 and mobility-HIP proxy2, respectively. The simulated topology is typical to what is explained in Figure 5-8 and the simulation parameters are described in Table 1.

Again, the OMNet++ 4.0 network simulator [99] and the HIPSim++ simulation framework [100] are utilised to implement the Mobility-enabled HIP proxy design. The handover of the Mobility-enabled HIP proxy, HIP, Micro-HIP and PMIPv6 are each carried out in two partially overlapping IEEE 802.11b (11 Mbps peak data rate) subnetworks. These subnetworks implement HIP, Micro-HIP, PMIPv6 and the Mobility-enabled HIP proxy. In PMIPv6 the MAGs are co-located with the access routers while in the Mobility-enabled HIP proxy (MHP) the mobility-HIP proxies are co-located with the access routers. That is, the mobility in subnetwork 1 and 2 is managed by MAG1 and MAG2, respectively for PMIPv6 whereas in the MHP it is managed by mobility-HIP proxy1 and mobility-HIP proxy2, respectively. The simulated topology is typical to that which is explained in Figure 5-8 and the simulation parameters are described in Table 1.

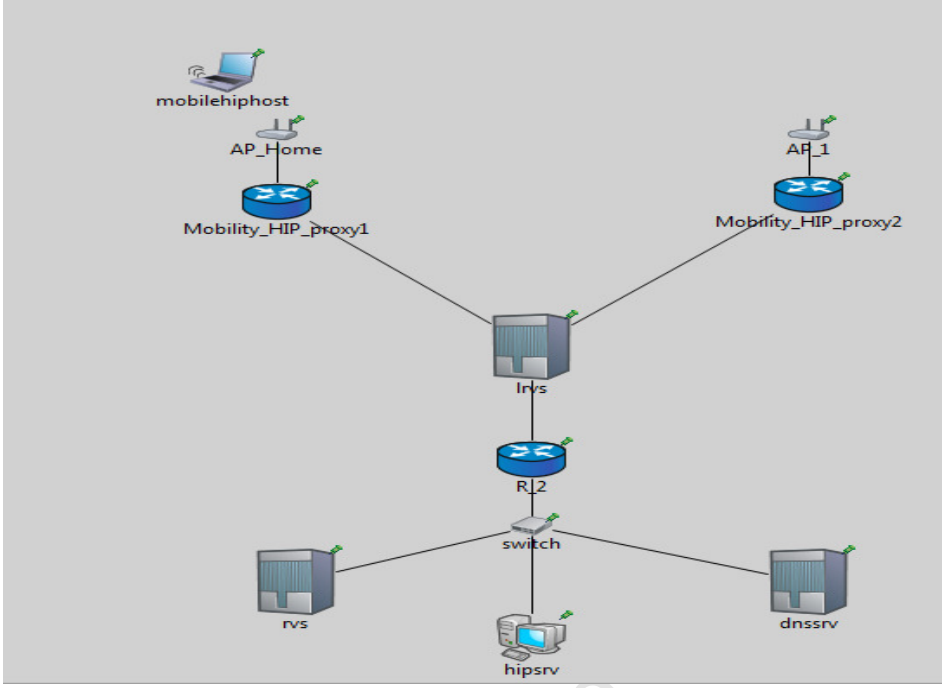


Figure 5-8 Simulation network topology of MHPP

5.3.1 Architecture of the MHP's Main Mobility Functions in OMNeT++

In this section, the researcher describes the node structure in the OMNeT++ for the main mobility entities of the MHPP. The HIP-enabled hosts, the Initiator and the Responder as well as the HIP-enabled servers, the Rendezvous Server and the DNS server of the HIP architecture, introduced by HIPSim++, are utilised and extended to develop a MHPP model.

To implement the MHP functions in OMNeT++, the researcher added mobility functions at the HIP module into the HIPSim++ existing RVSHost6 module. Figure 5-9 illustrates the internal structure of the MHP in the OMNeT++. In addition, to implement the LRVS proposed by the Micro-HIP, he has also developed the LRVSs functionality based on the HIPSim++ existing modules. LRVSs have also been modified to operate with the HIP RVS and MHPs. Figure 5-10 illustrates the internal structure of LRVS in the OMNeT++.

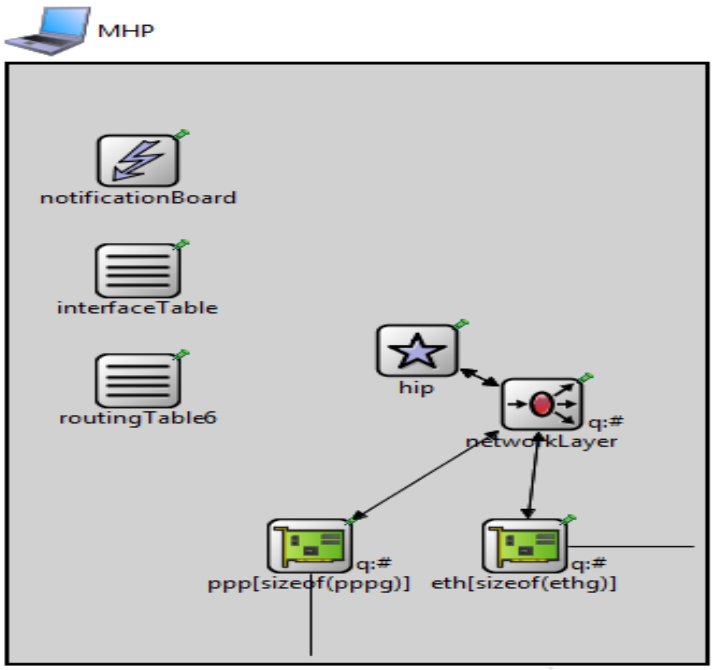


Figure 5-9 MHP structure in the OMNeT++

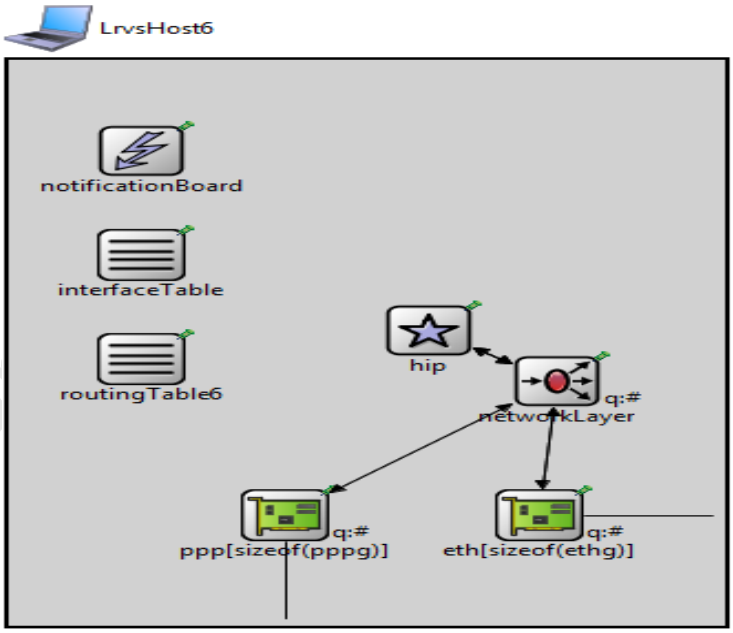


Figure 5-10 LRVS structure in the OMNeT++

5.3.2 Simulation Scenario

Similar to the scenario in which the HIPPMIP is evaluated, in the handover performance

evaluation and analysis of MHPP, the researcher considered a scenario whereby an HIP-enabled CH is fixed outside the access network to which the HIP MH is currently attached. Data are exchanged between the CH and the MH at a rate of 15 kbps and are in the form of 256-byte UDP packets. For the sake of simplicity, he considered only unidirectional data flow from the CH to the MH. The handover is simulated with the MH moving linearly at a constant speed of 1 m/s from one subnet to the other.

5.3.3 Performance Evaluation and Analysis of MHPP

To evaluate the handover performance of the MHPP, the researcher extended his simulation model [105] to incorporate a mechanism that allows the HIP-enabled MH to use the same IP address in different subnetworks under the same LRVS. He examined the new simulation model using the network topology (Section 5.3) and simulation scenario explained in (Section 5.3.2) and the simulation time extended up to 25,000s. Table 1 (Section 5.2) portrays the necessary simulation parameter configuration under which he evaluated the handover performance of the HIP, the Micro-HIP and the MHPP. Similar to the simulation environment under which the researcher examined the HIP and the Micro-HIP, he now examined the MHPP by employing two IEEE 802.11b access points, the home access point (H_AP) and the access point 1 (AP1). Furthermore, he co-located two S-RVSs, S-RVS 1 and S-RVS 2, within two ARs, AR 1 and AR 2, and partially overlapped the two subnetworks that were managed by AR 1 and AR 2. A fixed HIP CH (i.e., hipsrv), which is placed outside the access network of the MH, is used for running the UDP application and transmitting the datastream at 15 kbps with a packet size of 256 bytes to the MH.

Similar to the HPPMIP, to investigate the handover performance for the MHPP and its related work, he used the same meaning for the evaluated parameters that have been defined in Section 5.2. Furthermore, he evaluated and compared the handover performance of HIP, Micro-HIP PMIPv6 and the researcher's proposed Mobility-enabled HIP proxy in terms of metrics such as handover latency, packet loss and signalling overhead. He also defined handover latency (HOL) as the time difference between the time when the MH is able to receive packets in the new PoA and the time when the MH was unable to receive packets in the old PoA. In addition, he defined packet loss as the number of lost packets in the downstream traffic (CH to MH) during

handover. Furthermore, signalling overhead is quantified in terms of the number of mobility-related signalling messages per handover.

It is important to note that the MHPP is examined with two mechanisms for attachment detection: (1) when the MH is associated with a new layer-2 access point (N-AP), the MH triggers its ND protocol [106] to send a router solicitation (RS) packet to the MHP (i.e., the access router connected to the N-AP). It is important to note that the researcher extended the RS packet to include the HIT of the MH. During the first attachment, HIP-enabled MHs include their HITs into the RS packet while the non-HIP-enabled MHs do so if they have already received their HITs from the HIP proxy. If they have not assigned HITs yet, they set zeros as the HIT option that the researcher added to the RS packet. On receiving the RS packet with the HIT option and values set to zeros, the MHP is alerted that this is a non-HIP MH and has no HIT as yet. After that the MHP assigns and sends back a HIT for that particular MH, a non-HIP-enabled MH. Furthermore, the MHP sends an UPDATE packet with the MH HIT to the LRVS.

Another important issue to note is that the above mentioned attachment mechanism is different from the one that the researcher used for the detection of the HIP-enabled MH in [107]. The main difference is that the ND protocol is not utilised for the attachment detection mechanism in [107]. These different attachment detection mechanisms have different attachment delays. Those that utilise the ND protocol are considered experiments that the researcher used in this work.

For faster detection at the IP layer, the NDP allows the MH to not solely depend on the life time of a router advertisement but also to send router solicitations. The period that the MH waits before it becomes aware of the absence of router advertisements can be noted as delay 1 (MDD1). It is important to note that if the life time of the RA is high, the detection of the IP movement will likewise be high. In addition to this delay and according to the ND protocol, the MH should wait a random period of time between 0 and MAX_RTR_SOLICITATION_DELAY before sending an initial RS message. In the MHPP, delaying the initial RS message alleviates congestion when many MHs perform a handover to the same link at the same time. This delay is denoted as MDD2. Furthermore, responses to the router solicitation are delayed for a random period between 0 and 500ms to prevent routers on the same link from sending simultaneous

responses to the soliciting MH. This delay is denoted as MDD3.

During the attachment after a handover or any attachment after an assignment of HITs, the non-HIP-enabled MH presents its assigned HIT to the new MHP or serving MHP respectively. In contrast, a HIP-enabled MH presents its HIT even during the first attachment when it enters a new MHPP domain. Presenting the permanent and cryptographic HIT of the MH during the attachment enables the MH to securely receive its active sessions even if it is moving between heterogeneous networks, for example, moving between WiFi and WiMAX networks.

5.3.3.1 Handover delay (MHPP with attachment detection mechanism 1)

Using the above mentioned simulation environment (Section 5.2), the researcher examined the three models; HIP, Micro-HIP and MHPP. In addition, he recoded and extensively analysed a hundred handoffs for each of the three models. The fluctuation in the HOL of the models over the first 20 HO instances is shown in Figure 5-11.

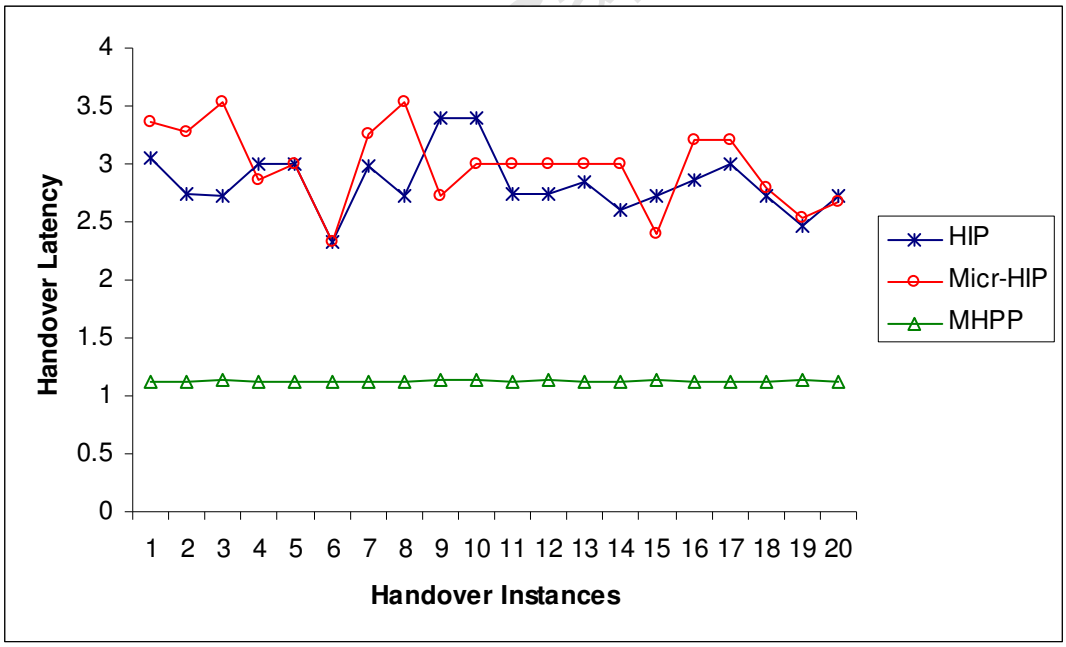


Figure 5-11 The first 20 handoffs for HIP, Micro-HIP and MHPP

One can also observe that there was a significant decrease in the HOL in MHPP. The MHPP achieved the lowest HOL that was in the fourth HO instance. Over the simulation period, different HO latencies other than those experienced by MHPP were consistently below 1.5s.

Furthermore, the MHPP has a stable HOL, while the HO latencies of the others (i.e., HIP and Micro-HIP) vary over the simulation period. This is because the MHP avoided DAD latency and movement detection (MD) latency, which are variable, but both the HIP and the Micro-HIP are still suffering from both DAD and MD latency.

The MHPP also achieved another advantage which is the reduction of LU latency. This is because in MHPP, the LU is performed by an MHP that is usually topologically closer to the LRVS than the MHs. In other words, the distance between the sender and the responder of LU messages in MHPP is shorter than the distance between senders and responders of LU messages in both the HIP and the Micro-HIP. In addition, the number of required LU messages in MHPP is less than those in the HIP and Micro-HIP.

To present a clear picture of how the MHPP managed the HO of an HIP-enabled MH, the researcher explained a close-up view of the first HO of the MHPP in Figure 5-12. This figure depicts a HIP-enabled MH that was receiving UDP data traffic from its CH. The CH was sending the data at a rate of 15Kbps from outside the MH domain. Again, it is necessary to identify which HO definitions will be used during the measurements and analysis. This is because the HOL can be defined in many ways. Some articles, including [55][15] co-relate HOL to the fetching of the first data packets at the new-POA. For example, [55] refers to the HOL as the latency (time difference) between the time of receiving the first packet at the N-PoA and the time of receiving the last packet at the previous PoA (P-PoA).

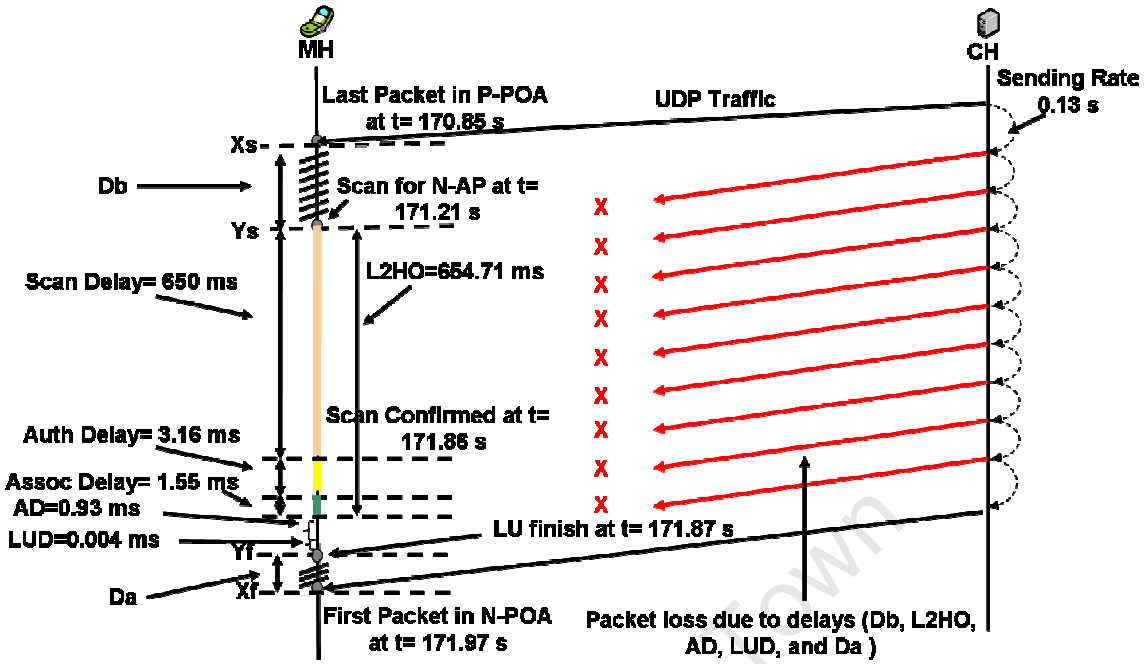


Figure 5-12 The handover of MH from the home network to the visited network

As illustrated in Figure 5-12, the MHs received the last packet in the P-POA (i.e., MHP1) at Xs = 170.85 s and the first packet in the N-PoA (i.e. MHP2) at Xf = 171.97 s. The difference between Xf and Xs is typical of the HOL mentioned above and used in [55]. From the measurements and analysis, the researcher observed that the $HOL_{Xf\text{-}Xs}$ includes two delay components, which are not related to the handover components, but are related to HO events and other parameters. He presented the delay components in Figure 5-12 as shaded areas, which are the areas between Ys and Xs as well as the areas between Xf and Yf. Therefore, he defined the HOL as latency, the time difference between the time at which the MH becomes available to receive a data packet from the N-PoA and the time at which the MH was unable to receive any data packets from the P-PoA. In other words it is the time that the MH remains unavailable to receive any data due to HO processes. This definition only includes the main HO components, such as delay of scanning (SD), authentication (AuthD), and association (AssD) in the link layer; as well as the delay of attachment detection (ADD), IP configuration and location updates (LUDs) in the network layer.

The researcher used the Ys and Yf to indicate the points of time when the first component of the HO (link layer switching) took place and when the last one (LU) finished, respectively, and

also used the $HOL_{Yf\text{-}Ys}$ to denote such delay. The $HOL_{Yf\text{-}Ys}$ in the MHPP was only due to an attachment delay (AD) and an LUD. This is because the MHPP has a mechanism that ensures the avoidance of a new IP configuration delay.

The co-relation and differences between the two HOL definitions ($HOL_{Xf\text{-}Xs}$ and $HOL_{Yf\text{-}Ys}$) are illustrated in the figure and explained hereafter. The following equations indicate the co-relation:

$$HOL_{Yf-Ys} = SD + AuthD + AssD + MDD + LUD \quad (6)$$

$$HOL_{Xf-Xs} = HOL_{Yf-Ys} + Db + Da \quad (7)$$

The delay before scanning (Db) and the delay after LU (Da) are delay components that are not related to the HO components; however, these delays occurred because of HO events and were included in the first definition of the HOL. The Db is the time difference between the time of receiving the last packet in the P-PoA and the time of starting the scanning for a new access point (N-AP). In the MHPP, the Db delay was 0.36s. The Db depends on factors including data sending rate (inter-arrival rate of the packets) at the CH, the distance between the MH and the CH and the signal strength of the N-AP. These factors also affect the Da LU, which is the time difference between the time of receiving the first packet at the N-POA and the time of the binding update completion. In the MHPP, the Da was approximately 0.1s. The combined delay due to both Db and Da was 0.46s, which is very high.

To the researcher's knowledge, neither macro-mobility management solutions (e.g., MIPv6 and HIP) nor micro-mobility management solutions (e.g., HMIPv6 and PMIPv6) addressed the Db and Da. Therefore, these solutions will experience such delays and incur a high HOL.

Micro-mobility management solutions usually anchor mobility in a domain of the MH or somewhere close to the MH to reduce the HOL. This implies that the CH location will not affect the HOL. Furthermore, when the MH has ongoing communications with many CHs, the MH only informs the mobility anchor point instead of informing all the CHs as is the case in macro-mobility solutions. It is true that the LUD will not be affected by the distance between the MH

and the CH, but both the Db and Da are directly affected by that. For example, in the MHPP micro-mobility solution, the latency due to both Db and Da was 0.46s, which is too high and will result in a relatively large HOL.

Figure 5-13 depicts the HOL ($HOL_{Yf\text{-}Ys}$) that includes only the HO components for the HIP, the Micro-HIP and MHPP. This is the average of a hundred handovers for each of the three models. The HOL measurements indicate that the HMPP outperformed both the HIP and the Micro-HIP. This is because, in the MHPP, the DAD latency is eliminated and the LU latency is significantly reduced. Note that this HOL includes both layer-2 (i.e., about 0.66s) and layer-3 HOLs. The layer 2 HOL was the same in the HIP, the Micro-HIP and the MHPP. The layer 3 HOLs of the HIP, the Micro-HIP and the MHPP were different. The difference between the HOLs of the HIP and the Micro-HIP lay in the LU latency, which was shorter in the latter than in the former. This is because the Micro-HIP anchored mobility at the domain's gateway (i.e., LRVS) instead of informing the CH, which is topologically far from the MH compared to distance of the LRVS from the MH. Unlike the HIP, the Micro-HIP eliminates signalling overheads between the domain's gateway (i.e., LRVS) and the CH.

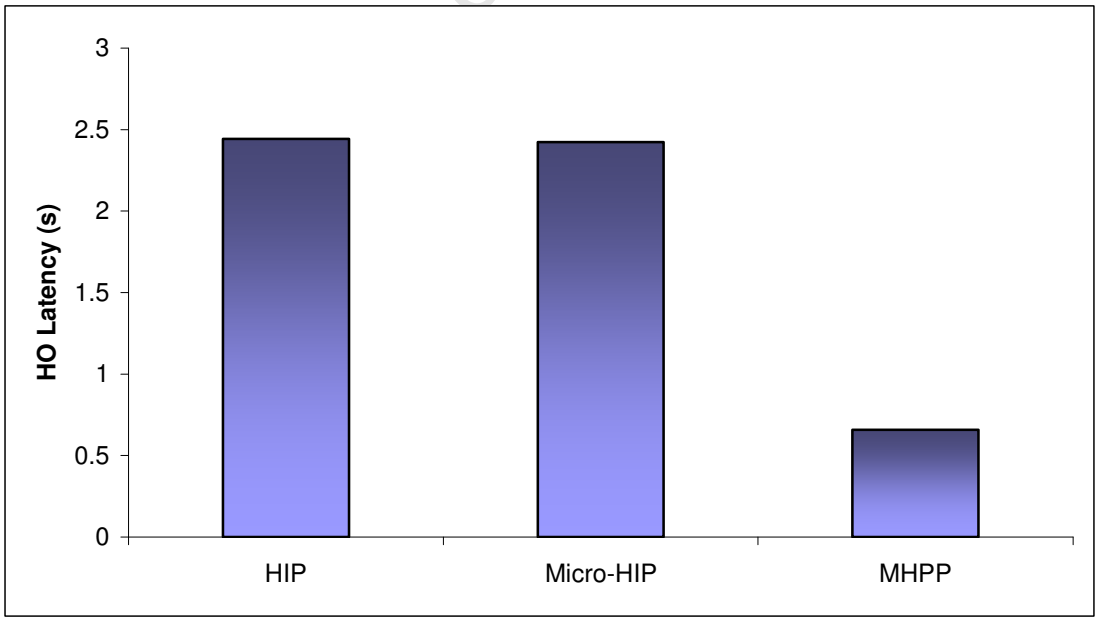


Figure 5-13 Handover latency of the HIP, Micro-HIP and MHPP

5.3.3.2 Packet loss (MHPP with attachment detection mechanism 1)

Figure 5-14 portrays the packet loss of the MHPP compared to the HIP and the Micro-HIP. The researcher measured the packet loss from traffic and the data packets of the UDP application moving between the CH and the MH during HOL. The inter-arrival rate of a data packet was kept constant in all the cases. From the packet loss measurements, he observed that the number of packet losses is proportional to the HOL. Compared to the HIP and Micro-HIP, the MHPP achieved the lowest HOL and thus the smallest number of packet losses. In MHPP, there was an average of 9 lost packets per 100 handovers, whereas the HIP and the Micro-HIP lost 22 and 21 packets respectively.

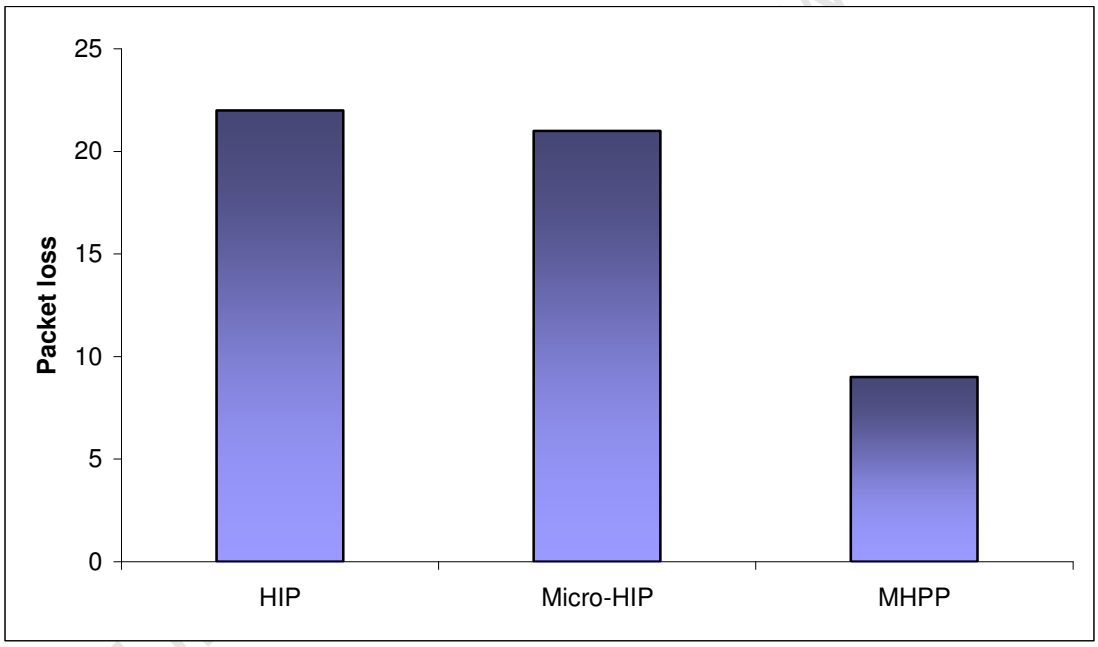


Figure 5-14 The averaged packet loss of the HIP, Micro-HIP and MHPP

5.3.3.3 Signalling Overhead (MHPP with attachment detection mechanism 1)

During a 25,000s-simulation period, the number of handover occurrences is 100. Figure 5-15 shows only the number of signals used for the LU in the HIP, the Micro-HIP and the MHPP during the entire simulation period. In the figure, it is evident that the MHPP outperformed both the HIP and the Micro-HIP in terms of LU messages. This is because the MHPP uses a two-way LU protocol while the HIP and Micro-HIP use a three-way protocol for the the LU. Unlike the

HIP and the Micro-HIP, the MHPP avoids all the signals related to the DAD as well as signal overheads related to the HIP MH interface.

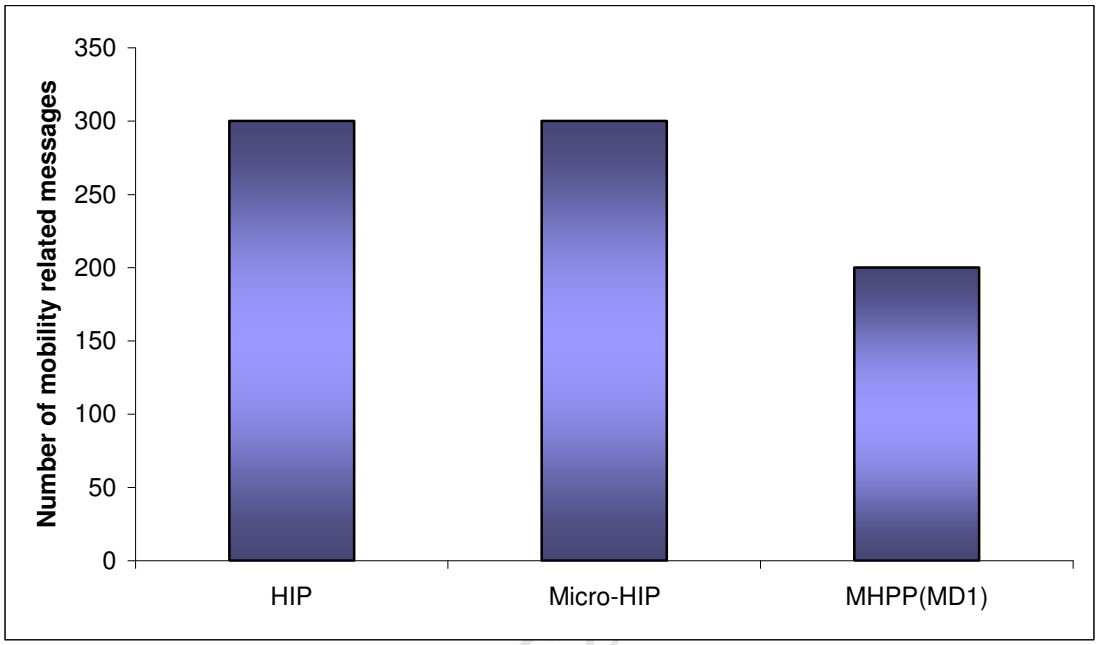


Figure 5-15 Mobility messages of the HIP, Micro-HIP and MHPP over 100 HOs

5.3.3.4 Handover Delay (MHPP with attachment detection mechanism 2)

In this subsection, the researcher presents an analysis of the handover process in the MHP with another attachment detection mechanism, called ADM2. In addition, he presented the main parts of the MHP handover in detail in Section 4.2 and then validated their measurements by means of simulation measurements for different UDP application configuration scenarios.

Figure 5-16 depicts a general view of the effect of the MHPP handovers for the MH movement between the home and visited network. In the unidirectional flow of the UDP application sent towards the MH, the researcher observed that the disruptions of the active session during the MH handover from the home and a visited network are similar to the ones during the MH handover from the visited and the home network.

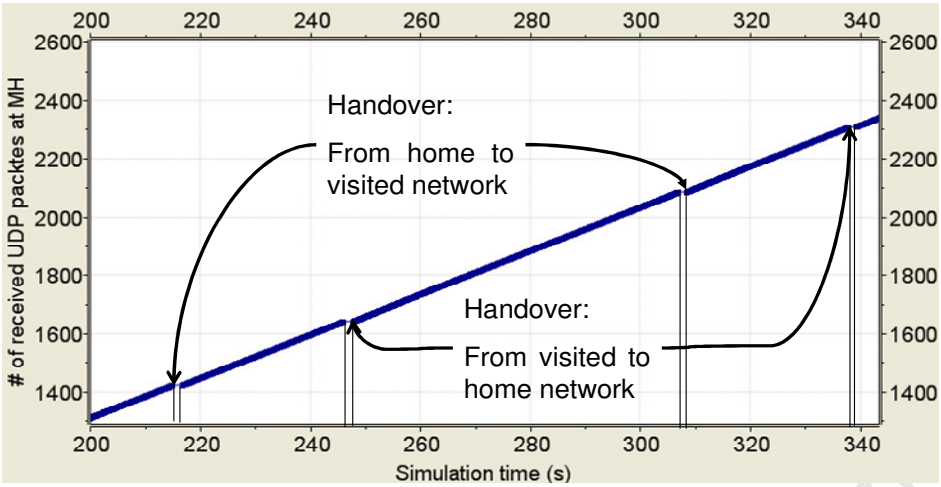


Figure 5-16 Disruptions on UDP session for the MH uses MHPP

The close-up view of the first handover of the MHPP with the attachment detection 2 is the same as the detailed view of the handover for MHPP with AD2. It is important to note that the attachment delay of AD1 is different to that of AD2. Furthermore, in using AD2, the researcher observed that the MH has received the last UDP packet via the old PoA, MHP, at 30.754s and the first UDP packet via MHP2 at 32.223s thus the delay between them is 1.469s. When an MH has attached to a new access router and has not received a router advertisement within a period of time equal to three times the existing router advertisement interval on the new link, the MH requests an RA.

Figure 5-17 illustrates unidirectional UDP packets flowing from the HIP CH to the non-HIP MH during movement from the home network to a visited network. The left side of the figure shows the mobility entities such as MHPs and the LRVS as well as some intermediate entities such as R_2. The session between the non-HIP MH CH has been initiated via MHP1. The UPD packets, while connected to the MHP flow, are indicated by the UDP packets before the HO. In the MH handover from the home network to the visited network, the MH has sent a RS, triggered by the L2 handover completion, to the MHP2 at 32.1041. Triggering the RS packet from layer 2 allows the MH to avoid a delay equal to three times the existing router advertisement interval on the new link. Furthermore, the MH has delayed randomly sending the

RS message by 340ms. On receiving the RS message, MHP2 performed a location update in 117us, which is very small. In the researcher's MHPP, an MH that has a router advertisement (RA) packet with a valid life time can receive data packets if the LRVS authenticates the MH and has accepted the binding update. On receiving the first data packet, MHP2 sends a Neighbour Solicitation message to the MH's solicited-node multicast address for the MH link-local address. The MH responds with a Neighbour Advertisement (NA) including its link-layer and sends back the MHP2 link- local address. On completing the address resolution the MH receives the first data packet via MHP2. The address resolution is completed shortly after the completion of the L2-handover. From Figure 5-17, in this handover instance, the attachment delay component lasts as long as 340ms including the location update delay, which is 117us.

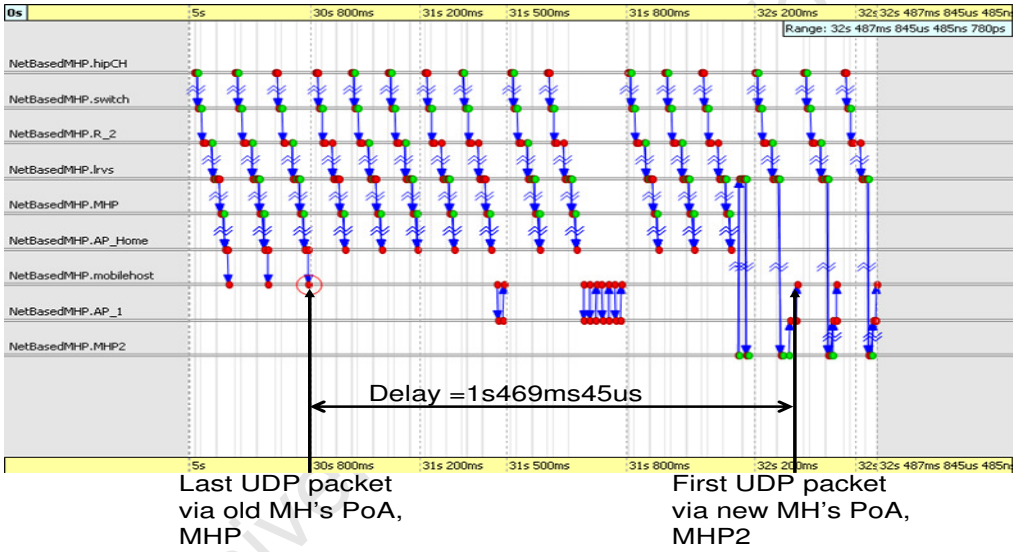


Figure 5-17 HO messages and delay of the MHPP (from "h" to "v" networks)

The network prefix in the solicited RA packet allows the MH to retain its IP address configured at the MHP1. Thus the MH has not experienced any DAD delay.

This improvement in handover performance can be attributed to the following: (1) DAD is eliminated in the MHPP; (2) The distances between the LRVS and the two mobility-HIP proxies are the same for both (back and forth) handovers between the subnetworks. Thus, the Handover Delay (HD) is very similar in both handover instances; (3) Unlike the attachment detection mechanism in [107], in this Attachment Detection (AD) time of the MH it is not the

same in all handover instances in the MHPP.

When the MH is disassociated from the old AP, AP_home, and connected to the MHP, the LVRS has erroneously forwarded the UDP packets via MHP1. These UDP packets are indicated by the UDP packets via the old MH PoA, MHP. Furthermore, layer-2 signalling between the MH and the new AP, AP_1, connected to the new MHP, MHP2 is indicated by layer-2 signalling. The location update packets MHP2 used to update the MH binding at the LRVS, are indicated by the UPDATE packets for handover. Moreover, the figure shows a delay between the first UDP packet the MH received via the new MHP and the last UDP packet the MH received via the old MHP.

From the figures in this MHPP, the MH movement from the home network to a visited network or vice versa has almost the same delay as that experienced in the movement from the visited network to the home network as shown in Figure 5-18. As explained in Section 5.3.3.1, this delay is not only affected by the handover components.

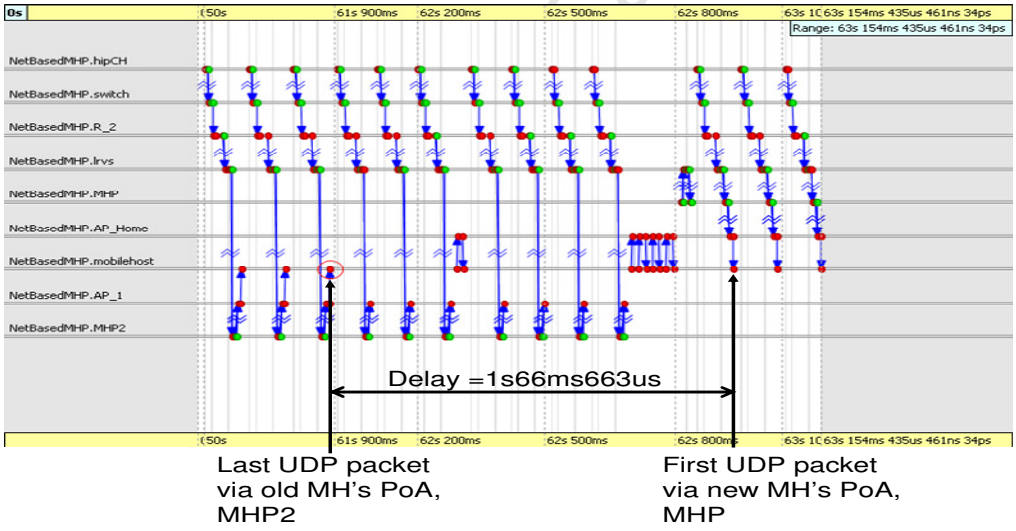


Figure 5-18 HO messages and delay of the MHPP (from "v" to "h" networks)

It is evident from the figure that the MHPP for Intra-domain HO outperformed the HIP, PMIPv6 and Micro-HIP in terms of handover related messages. Again, this is because the MHPP uses a two-way location update protocol and does not consult a third party on security matters. However, PMIPv6 does need to consult a third party to ensure secure sessions. The third party

security consultation results in additional signalling overheads (four messages per IP handover) thus adding some delay to the total HO delay.

5.3.3.5 Packet loss (MHPP with attachment detection mechanism 2)

Again, the researcher carried out a hundred handovers for each of the HIP, Micro-HIP, PMIP and MHPP. The simulation measurements indicate that the Mobility-enabled HIP proxy has the least packet loss. In fact, packet loss for this protocol (MHPP) is consistently below eight packets per handover as opposed to the other three models (HIP, Micro-HIP and PMIPv6).

5.3.3.6 Signalling overhead (MHPP with attachment detection mechanism 2)

Handover related messages in HIP, Micro-HIP, PMIPv6 and Mobility-enabled HIP proxy during 25,000s simulation time are depicted in Figure 5-19.

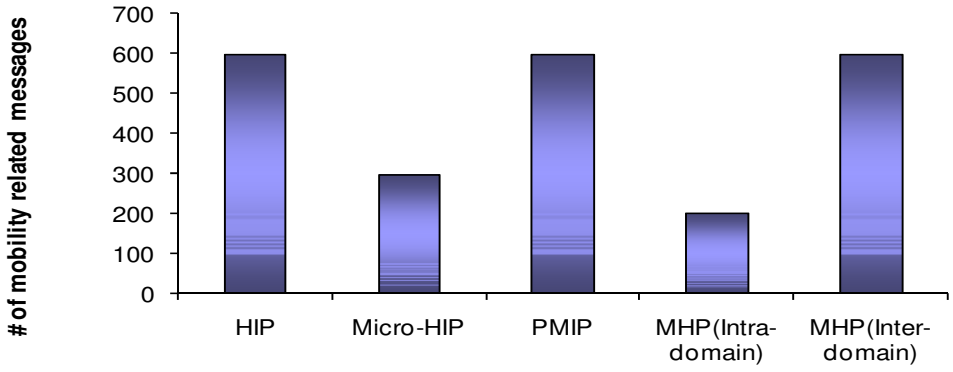


Figure 5-19 HO messages of the HIP, Micro-HIP, PMIPv6 and MHPP

It is evident from this figure that the MHPP for intra-domain HO outperformed HIP, PMIPv6 and Micro-HIP in terms of handover related messages. This is because the MHPP uses a two-way location update protocol while the HIP and Micro-HIP use a three-way protocol for location update. It is important to note that the HIP, Micro-HIP and Mobility-enabled HIP proxy are not required to consult any third party to ensure secure sessions since they have capabilities of self certifying at the HIP layer. However, PMIPv6 does need to consult a third party to ensure secure sessions. The third party security consultation results in additional signalling overheads (four messages per IP handover) thus adding some delay to the total handover delay.

The Mobility-enabled HIP proxy for inter-domain HO needs four additional messages, two messages to communicate with the old LRVS, which redirects the active session, and two messages to communicate with the RVS, which confirms the reachability through the new domain. It is important to note that the number of mobility-related messages for inter-domain HO does not depend on the number of CHs to which an MH has active sessions. The signalling overheads of the Mobility-enabled HIP proxy for intra- and inter-domain handover are shown in Table 4.

Table 4. Signalling Overheads of MHPP for Intra and Inter-Domain HO

	MHPP(Intra-domain)	**MHPP(Inter-domain)**
# of UPDATE packets per handover when communicating with 2 CHs?	2	6
# of UPDATE packets per handover when communicating with n CHs?	2	6
Signalling overheads on MH's interface?	No	No
Signalling overheads due to configuration of new IP addr?	No	No
Signalling overheads for consulting 3rd party for security?	No	No

5.3.4 Impact of MH's Speed on Handover Performance

Figure 5-20 demonstrates how different MH speeds affect the handover delay of the MHPP. All the measurements are taken during the constant bit rate traffic with an interval rate of 0.133333s. Each point in the graph represents an average of all the MH handovers, from the

home to the visited network and vice versa, made within 2,000s for each different MH speed. For example the number of HOs the MH has performed with a speed of 3mps is three times the number of handovers the MH has performed with a speed of 1mps. In this case the researcher considered the average of all the MH handovers for each different speed. In HO delay, the measurements with different MH speeds, it is interesting is that the HO delay for MH speeds of 5mps is lower than the HO delay at MH speeds of 3mps and 1mps.

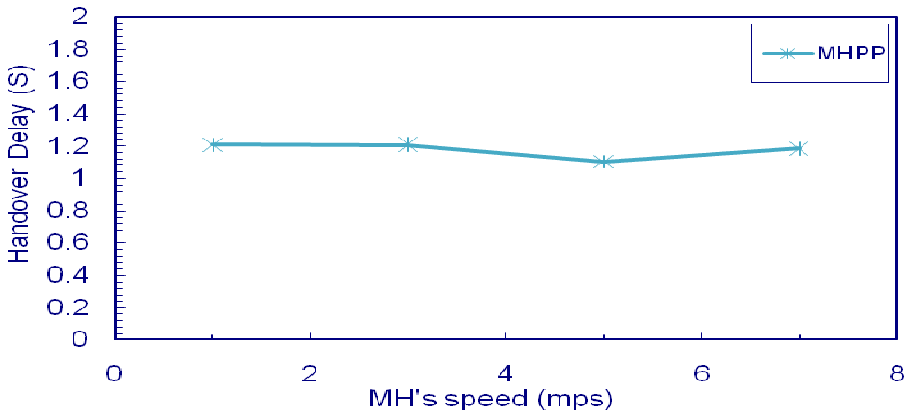


Figure 5-20 Affect of MH's speed on handover delay of MHPP

In the MHP solution, the MH only experiences handover due to: (1) layer-2 handover; (2) attachment detection delay; and (3) location update delay. To explain how each of these delay components are affected by the different MH speeds, the researcher depicts a layer-2 handover, when it started and ended as well as the scheduling of the RS message to inform MHP2 about the MH attachment in Figure 5-21 and Figure 5-22 for MH speeds of 3mps and 5mps respectively.

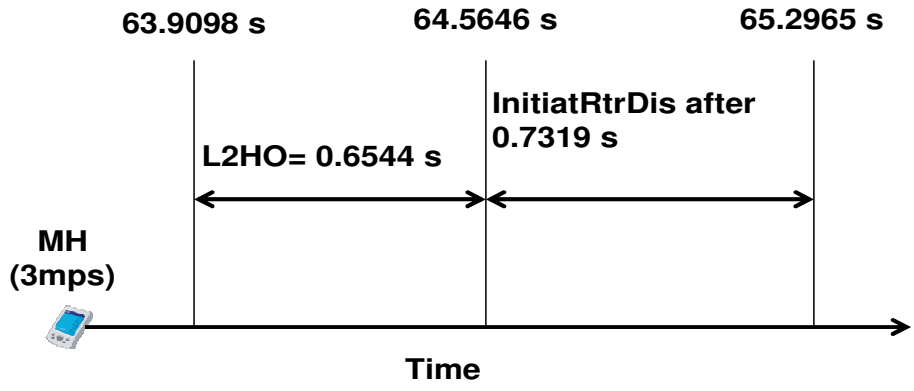


Figure 5-21 L-2 HO and attachment detection with MH's speed of 3mps

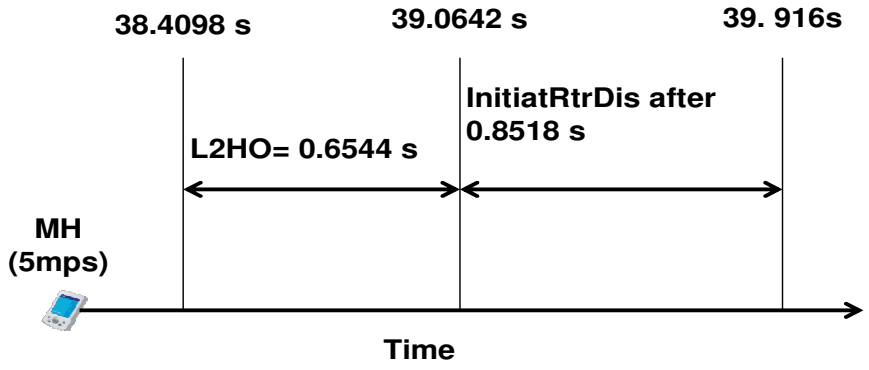


Figure 5-22 L-2 HO and attachment detection with MH's speed of 5mps

The start and end times of a layer-2 handover and the scheduling of the attachment while the MH hands over from the home to a visited network with speeds of 3mps and 5mps, are shown respectively in Figures 5-21 and 5-22. In the figures it is notable that the layer-2 delay on the MH speed of 3mps is the same as the delay on the MH speed of 5mps. In 3mps, the attachment detection is randomly scheduled to start at 65.2965, which is more than 0.7319s after the completion of layer-2 handover. Similarly, in 5mps, the attachment detection is randomly scheduled to start at 39.916, which is more than 0.8518s after the completion of layer-2 handover. From the figures the delay before the start of the attachment detection in the MH speed of 5mps is larger than the delay in the MH speed of 3mps. The difference is attributed here to the random selection of between 0 and max_solicitation_delay = 1 s. Furthermore, from the measurement it seems that sometimes a higher speed can allow the MH to receive a better SNR In this case, the MHs with a higher speed can start the handover process earlier and be more reachable at the new PoA.

However, in some cases an MH that moves with a higher speed can lose the signal from the serving AP faster than the others moving at a slower speed. Thus, the MH loses its reachability earlier and packet loss starts earlier as well. In conclusion, different MH speeds do not significantly affect handover latency and signalling overheads unless the attachment message is lost due to a higher speed of the MH in the MHP solution since it is a network-based mobility solution.

5.3.5 Impact on MHPP's Handover Performance due to Security Delay Component with a Third Party

Figure 5-23 illustrates the relationship between the increase of the delays, owing to the security process with a third party such as an AAA server, and the handover delay of PMIPv6, HIPPMIP and the Mobility-enabled HIP proxy. Each point in the graph represents an average of MH handovers, layer-2 and layer-3 handovers, calculated while the MH was moving at a speed of 1mps. It is important to note that these measurements are for PMIPv6, HIPPMIP and MHPP with the attachment detection mechanism 1. AD1 utilises the NDP, attachment mechanism 2, AD2, which is different from the one that the researcher used in [105, 107]. PMIPv6 and HIPPMIP are extremely affected by security delays because of security checks at a third party and thus experience additional delays while the Mobility-enabled HIP proxy does not.

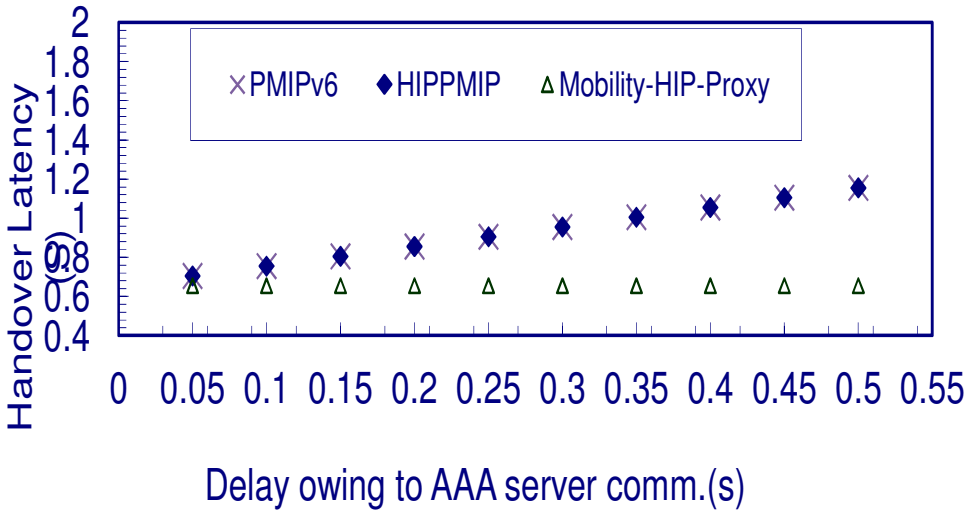


Figure 5-23 Impact of AAA delay on HOD of the PMIPv6, HIPPMIP and MHPP

5.3.6 Impact of Number of CHs on MHPP's Handover Performance

The following section briefly compares the basic handover latency involved in HIP, Micro-HIP and MHPP. The researcher developed an analytic model based on the explanations provided in figures 5-24, 5-25 and 5-26 to measure the HOL and the mobility-related signalling overheads of HIP, Micro-HIP and MHPP respectively. Note that CH1 and CH2 can reside in the

same or in different domains. Another issue to be considered is which one of the CHs will be the first to inform. However, the receipt of the UPDATE packets depends on the distance between the MH and the respective CH. The sequence of the UPDATE packets in Figure 5-24 is one of the possible exchanges that can take place in real networks.

In the evaluation of the handover performance of HIP, the researcher assumed that the HIP MH registered at the RVS with binding contains the MH HIT and IP addresses of the MH which can currently be reached. He also assumed that the MH has ongoing communications with both CH1 and CH2 as indicated in Figure 5-24.

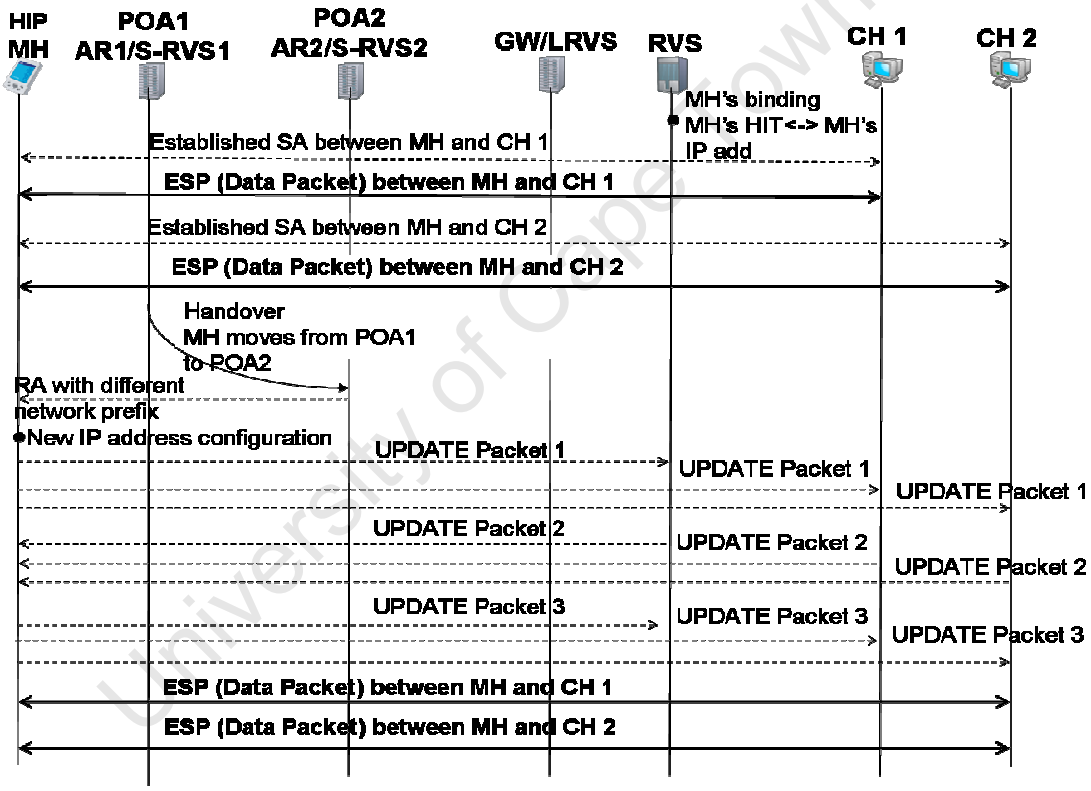


Figure 5-24 HIP HO procedures while MH has communications with CH1 and CH2

When a HIP host moves from one PoA to another, the following HOL components are involved:

- Latency due to the MH movement detection (MD) at the IP layer in the MH stack, L_{MD}.

- Latency due to the MH configuring its current IP address at the new location, L_{IP_CONF}.

- Latency due to the HIP MH sending the update message with a locator parameter (carried in the first UPDATE packet) to update the CHs, L_{LU1_CH} .

- Latency due to the sending of the second UPDATE packet from the CH to the MH to verify the new locator, L_{LU2_CH}.

- Latency due to the sending of the third UPDATE packet from the the MH to the CHs to confirm verification of the new locator, L_{LU3_CH}.

Thus, the HOL due to the basic HIP mobility management protocol is as follows:

$$L_{HIP(MH, CHi)} = L_{MDi} + L_{IP\_CONFi} + L_{LU1\_CHi} + L_{LU2\_CHi} + L_{LU3\_CHi} \quad (1)$$

where i = 1... n; n is the number of CHs with which the MH has ongoing communications. In addition, n must be greater than or equal to 1. This is because no UPDATE packets are needed when the MH has no connection with the CH (i.e. $n = 0$).

After the handover latency (HOL), both CH1 and CH2 redirect their data traffic to the new location of the MH. Yet, the RVS can only direct any host that intends to establish a new communication with the handed-over MH to the old PoA of the MH. This situation continues until the MH updates its record at the RVS. The following latencies affect the required time for the MH binding update at the RVS:

- Latency due to the HIP MH sending the update message with a locator parameter (carried in the first UPDATE packet) to update the RVS, L_{LU1_RVS}.

- Latency due to the sending of the second UPDATE packet from the RVS to the MH to verify the new locator, L_{LU2_RVS}.

- Latency due to the sending of the third UPDATE packet from the MH to the RVS to confirm the verification of the new locator, L_{LU3_RVS}.

$$L_{HIP(MH,RVS)} = , L_{IP\_CONFi\_} + , L_{MDi\ \_} + , L_{LU1\_RVS} + , L_{LU2\_RVS} + , L_{LU3\_RVS} \quad (2)$$

Figure 5-25 illustrates the signalling flow of the MH handover using the HIP while the MH has ongoing communications with both CH1 and CH2. When conducting two ongoing communications, MHs have to exchange six messages (i.e. three UPDATE packets with each of the CHs). In addition, the MH needs to exchange an additional three UPDATE packets with the RVS to update its binding. The number of messages required to update the MH binding at its registered RVS, and to inform the CHs, CH1 and CH2, with which it has ongoing communications, are nine UPDATE packets. The analytic model for the HIP shows that the number of CHs with which MH has ongoing communications significantly increase the number of UPDATE packets. Having an MH that has two communications with CH1 and CH2 as well as a binding record at the RVS, the number of UPDATE packets can be calculated by the following simple equation:

$$N_{UP\_HIP} = 3*(n+1) \quad (3)$$

where n is the number of CHs with which the MH has ongoing communications, while 3 indicates the number of required UPDATE packets to inform each CH or to update the MH binding at the RVS.

In the evaluation of the handover performance of Micro-HIP, using the same assumptions mentioned before for the HIP, the researcher developed another analytic model to measure the HOL and mobility-related signalling overheads of Micro-HIP while the MH was conducting two ongoing communications with both CH1 and CH2 as shown in Figure 5-25. From the figure, when an MH performs a handover from PoA1 to PoA2, the following HOL components are involved:

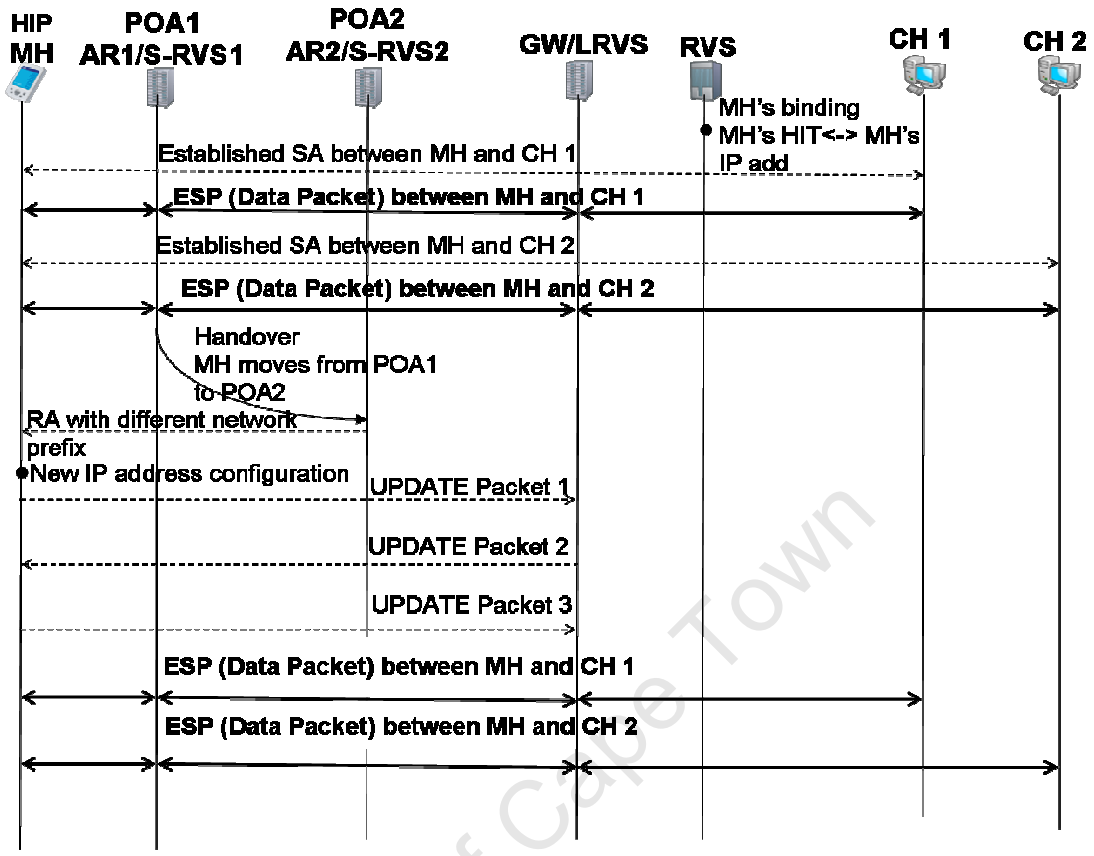


Figure 5-25 Micro-HIP HO procedures while MH communicating with CH1 and CH2

- Latency due to the MH MD at the IP layer in the MH stack, L_{MD}.
- Latency due to the IP address configuration of the MH at the new PoA, $L_{IP\text{-}CONF}$.
- Latency due to the HIP MH sending the update message with a locator parameter (carried in the first UPDATE packet) to update the relevant components (LRVS), L_{LU1_LRVS}.
- Latency due to the sending of the second UPDATE packet from the LRVS to the MH to verify the new locator, L_{LU2_LRVS}.
- Latency due to the sending of the third UPDATE packet from the MH to the LRVS to confirm the verification of the new locator, L_{LU3_LRVS}.

Thus, the HOL for a Micro-HIP protocol is as follows:

$$L_{Micro\text{-}HIP} = L_{IP\text{-}CONF} + L_{MD} + L_{LU1\_LRVS} + L_{LU2\_LRVS} + L_{LU3\_LRVS} \quad (4)$$

Unlike the HIP, the use of the Micro-HIP allows the MH to only inform the LRVS about the new IP address. Three UPDATE packets as shown in Figure 5-25 are enough to redirect the data traffic to the MH's new location. Evidently, by the explanations on Figure 5-25 and the developed analytic models for the HIP and Micro-HIP, the HOL and mobility related signalling overheads of the Micro-HIP are partially optimised. The HIP and Micro-HIP have signalling overheads on the MH interface, although they further incur signalling overheads of the new IP configurations because of the MH handover.

Figure 5-26 shows an explanation of handover management using the MHPP while the MH conducts ongoing communications with two CHs, CH1 and CH2. Based on the same assumptions used before for the HIP and Micro-HIP, the researcher developed an analytic model to measure the HOL and mobility-related signalling overheads while the MH was conducting ongoing communications with CH1 and CH2.

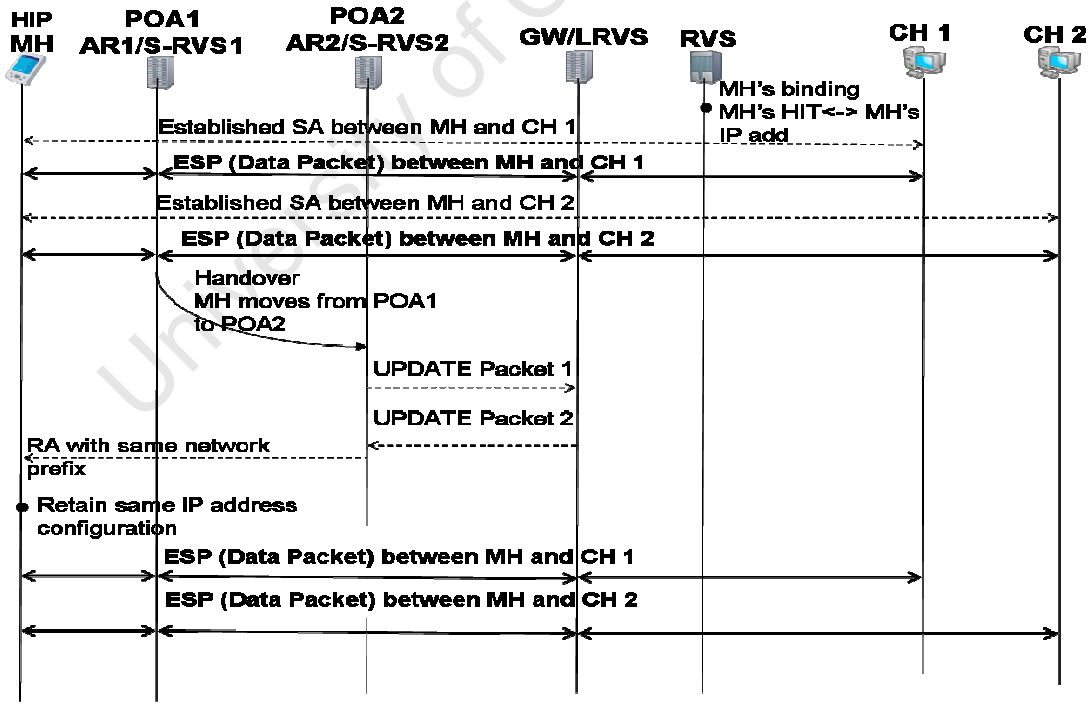


Figure 5-26 MHPP for HO procedures while MH communicating with CH1 and CH2

The MHPP has the following components contributing to the HOL:

• Latency due to the MH attachment detection (AD) at the IP layer in the POA stack, for which reason it is called an attachment rather than a MD, L_{AD}.

• Latency due to the two-way handshake readdressing protocol, between the S-RVS and the LRVS, $L_{LU1} + L_{LU2}$.

Thus, the HOL due to the MHPP is as follows:

$$L_{MHPP} = L_{AD} + L_{LU1} + L_{LU2} \quad (5)$$

A comparison between Equations 1, 4, and 5 that describe the HOL of the HIP, Micro-HIP and MHPP, respectively, shows the advantages of the last, that is, Equation 5. The advantages of the MHPP are better than those of the HIP and Micro-HIP. The MHPP reduces LU latency and the number of required UPDATE packets as well as eliminates messages and latency related to the configuration of the new IP address.

Unlike the HIP and Micro-HIP, the MHPP does not involve the MH in mobility-related signalling. As shown in Figure 5-26, the new PoA (i.e. PoA2) only exchanges two UPDATE packets with the LRVS to redirect the MH traffic through POA2. To clearly show the differences between the HIP, Micro-HIP and MHPP, the researcher summarised the mobility-related signalling overheads in Table 5. Evidently, judging by the developed models, the MHPP overcomes the shortcomings of the HIP and Micro-HIP solutions to efficiently manage mobility in a localised domain.

Table 5. Signalling overheads of HIP, Micro-HIP and our MHPP

Parameters\Scheme	**HIP**	**Micro-HIP**	**MHPP**
# of UPDATE packets per handover when MH has ongoing communications with 2 CH.	9	6	2
# of UPDATE packets per handover when MH has ongoing communications with *n*	3*(*n* + 1)	6	2

CH.			
Are there any signalling overheads on MH's interface?	Yes	Yes	No
Are there any signalling overheads due to configuration of new IP address?	Yes	Yes	No

The first column in Table 5 displays the number of binding update messages when the MH has ongoing communication sessions with two CHs. In addition, it indicates the number of binding update messages when the MH has ongoing sessions with n CHs in the second column of the table. It is important to note that the mobility-related signalling overheads of the basic HIP are highly affected by increasing the number of CHs with which the MH conducts ongoing communication sessions. In contrast, the mobility-related signalling overheads of the Micro-HIP and MHPP are unaffected by increasing the number of CHs. This is because the Micro-HIP and MHPP update only the network gateway, irrespective of how many CHs and ongoing communication sessions there may be. It is also important to note that the HIP, Micro-HIP and MHPP need not consult any third party on security issues as they have capabilities of self certifying because of the HIP layer. However, solutions [96][61] need to consult a third party on security aspects. This third-party security consultation incurs a cost of additional signalling overheads and adds some delay to the total HOL.

In this chapter the researcher explained the simulation framework and implementation of his proposed network-based mobility solutions, HIPPMIP and MHPP. The chapter begins with a brief overview of the OMNeT++ network simulator, which he used for the development of the simulation models and performance evaluation of the proposed mobility solutions. The overview centred particularly on the implementation of the mobility solutions' mobility entities and simulators' mobility-related library. Furthermore, he presented simulated network topologies for HIPPMIP and MHPP as well as the necessary parameters under which the proposed mobility solutions and their related work were investigated. Moreover, he presented and analysed the

obtained results from simulations of HIPPMIP and MHPP models and compared them with those obtained from HIP, PMIPv6 and Micro-HIP models. The performance analysis shows that HIPPMIP and MHPP outperformed HIP, PMIP and Micro-HIP models. Unlike HIPPMIP, MHPP support legacy MH and also eliminates further handover components.

Chapter 6 Distributed Mobility Management

In this chapter, the researcher introduced two distributed designs, a Distributed Mobility Management with Network-Based Host Identity Protocol (DM-MHPP) and a Signal-Less Distributed Mobility Solution (SL-DM) to support all IP hosts. Both designs aim to optimise handover performance in heterogeneous flat wireless networks in terms of providing efficient, secure and scalable handover delay architectures. It is important to note that these designs are complementary and have different features. These different features satisfy different requirements for network operators. The chapter begins with a discussion of the DM-MHPP and its details in Section 6.1 and related subsections. This is followed by a discussion of the SL-DM and its details in Section 6.2 and related subsections.

6.1 Distributed Mobility Management with Network-Based Host Identity Protocol (DM-MHPP)

In this section, the researcher proposes an elegant distributed mobility management with network-based HIP, called DM-MHPP, to optimise handover performance in flat heterogeneous wireless networks in terms of providing an efficient, secure and scalable handover delay solution. In the researcher's DM-MHPP solution, the MH moves while keeping its sessions active through a HIP association and by also maintaining a stable IP address for packet routing even under MH mobility conditions in a MHPP domain.

6.1.1 Need for DM-MHPP

Network architecture is evolving from a hierarchical to a flat infrastructure. The nature of a hierarchical architecture can be harnessed to efficiently and seamlessly support the host mobility. This is because it is possible to select/identify a functional entity, which can be updated on the MH's current location between the MH and CH. Consequently, a handover performance will be optimised since the selected entity is topologically closer than the CH to the MH. Unfortunately, that specific aspect of a hierarchical architecture's nature that allows the selection of a central entity for handover optimisation, is no longer available in a flat architecture since

entities are distributed across different networks. This architectural evolution from hierarchical to flat networks caused by increased data traffic volumes creates new challenges as identified in [9]. These challenges include single points of failure and bottlenecks, non-optimal routing paths, scalability problems and long handover delays. Consequently, the handover mechanisms that have been built-based on the centralised mobility function need to be redesigned and/or carefully optimised again.

The MHPP provides a seamless and secure handover for the MH in the hierarchical network architecture. However, the MHPP cannot ensure the same handover performance in the flat network architecture since the MHPP has been built to utilise the features offered by the hierarchical architecture. In the MHPP, the mobility entities perform many handover components such as the security process by themselves without incurring additional delays and signals. Furthermore, the MHPP ensures a secure multihoming irrespective of the underlying architecture. In other words, the security and multihoming support provided by the MHPP can be preserved irrespective of the network architecture in which it is employed. Therefore, the MHPP is extended to ensure the seamlessness and scalability in the flat network architecture, also adding security and multihoming features.

6.1.2 Design Objectives for DM-MHPP

The design of the researcher's DH-MHPP is based on distributed mobility entities to independently provide the HIP and the mobility for the HIP MHs and non-HIP MHs. In addition to the design objectives presented in Section 4.1.2.

The distribution of the mobility entities in different locations respond to the handover-related needs introduced by the network evolution from hierarchical to flat, to optimise the handover performance. The main objectives are presented below.

1. To reduce handover delays and packet loss for the HIP-enabled and non-HIP-enabled MH in the flat network architecture. This can be achieved by introducing independent mobility entities, seamless association transfer protocols, reducing the time consuming handover delay components such as IP configuration and

security association establishment and/or update.

2. To keep handover-related signalling overheads minimal in the air interface between the MH and the access points as well as on the core network.

3. To utilise the MH protocol stack capabilities such as host identifiers and host identity tags (HIT) introduced by the HIP to strengthen the IP handover.

4. To provide scalable mobility designs while preserving security, seamlessness and multihoming support.

Like the MHPP, but in a flat network architecture, to provide network-based mobility management while utilising the MH stack capabilities such as the HIP layer capabilities to maintain the same security level of the HIP.

6.1.3 Protocol Overview

This section introduces a network-based distributed mobility management solution that duplicates many Mobility-enabled HIP proxies in different networks to support all IP hosts. All the mobility management functions of the MHPP described in Section 4.2 are also included at the access routers taking advantage of the HIP proxy capability. These additional network-based functions include tracking and updating the MH location, security signalling, assigning a network prefix per host identifier and using the same network prefix within the same network domain to avoid DAD, resulting in improved handover performance in the flat network architecture. They enable an MH, whether or not HIP-enabled, to use the same IP address as it changes its points of attachments within the flat network architecture.

6.1.4 Mobility Management Architecture

The architecture for network-based distributed mobility management with a HIP proxy is shown in Figure 6-1. The RVS has been defined in [98] with the DNS to provide reachability of a HIP host by maintaining a mapping between the host identity, called a HIT, and the IP address of the MH. The researcher's design, called distributed Mobility-enabled HIP proxy, adds a set of co-located mobility and HIP proxy functions at the access router. Like the MHPP for the

hierarchical network architecture, the Mobility-enabled HIP proxy performs HIP signalling on behalf of non-HIP MH so that HIP services can be offered to non-HIP enabled hosts. It also tracks the movement of the MH and updates the MH binding record if the MH is moving away from the network during an established session even while the session is active. On detection of the MH attachment, the MHP checks whether the MH is HIP-enabled or not. If not, the MHP assigns a HIT and returns it to the MH. The MHP uses the HIT, from the HIP MH or the assigned one for non-HIP MH, to check whether the MH is registered or not. If it is not registered, the MHP sends an update message to the RVS, which is the intermediate location information between the MHP entities and the DNS servers.

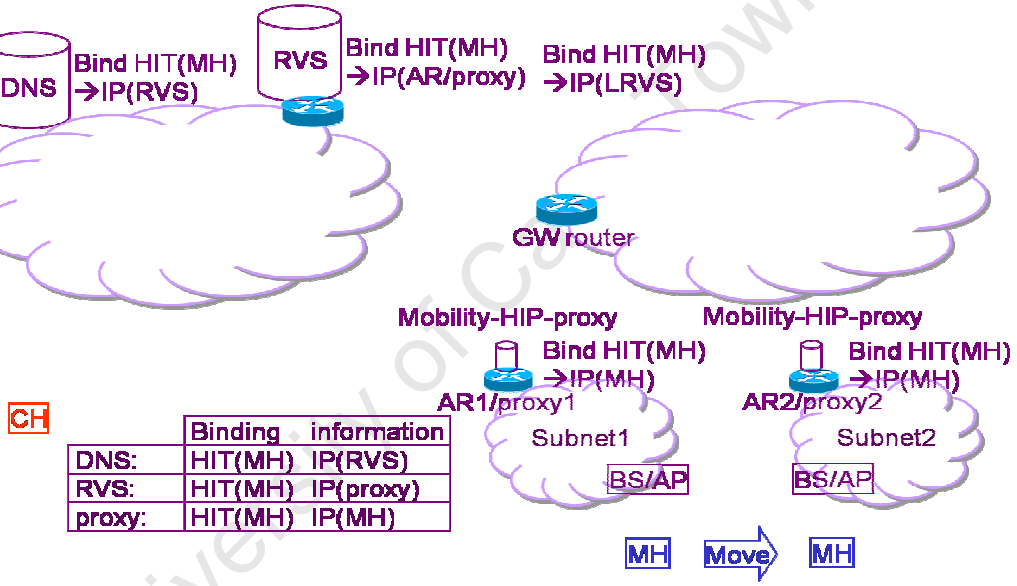


Figure 6-1 Design of network-based distributed mobility management and HIP proxy

The binding information, which is shown in a table in Figure 6-1, is managed in the hierarchy DNS-RVS- proxy to enable the reachability of an MH which is registered with the Mobility-enabled HIP proxy. After registration, the Mobility-enabled HIP proxy contains the binding of the HIT of the MH, HIT(MH), to the IP address of the MH, IP(MH). The RVS contains the binding of the HIT of the MH, HIT(MH), to the IP address of the proxy, IP(proxy). The DNS contains the binding of the HIT of the MH, HIT(MH), to the IP address of the RVS, IP(RVS).

6.1.5 Registration and Reachability

Before using an HIP service, an HIP host needs to register with the service using the registration mechanism defined in [97]. The registration of an MH, which may either be HIP enabled or not, is illustrated in Figure 6-2.

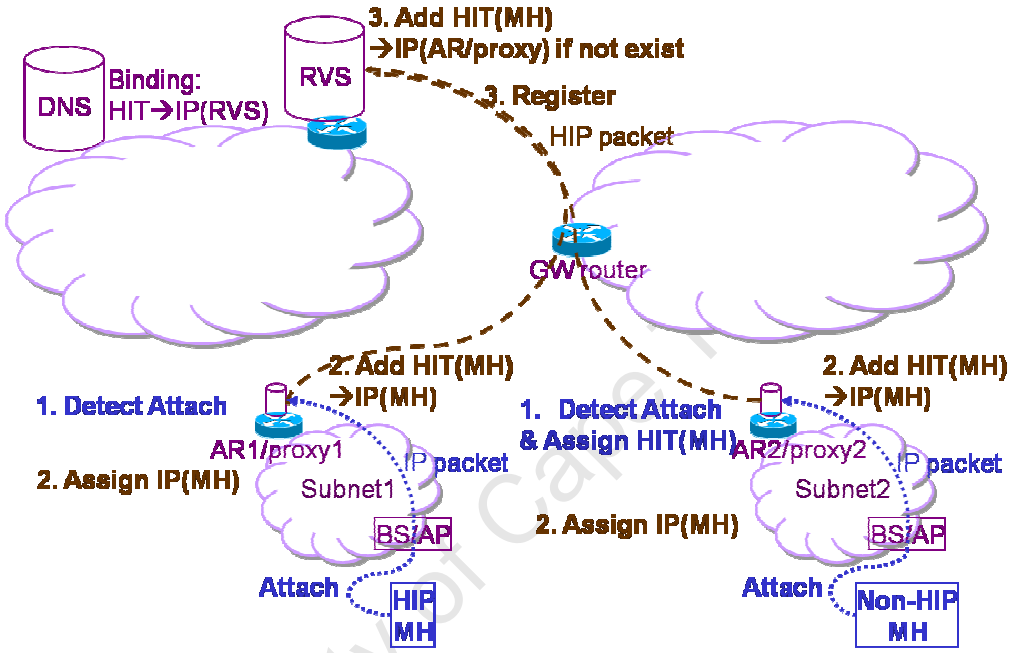


Figure 6-2 Registration of a mobile host, which is HIP enabled or not

After registration, the MH becomes reachable from any CH that may query the DNS about the location of the MH. The DNS replies with the IP address of the RVS to which the HIT of the MH is registered (Figure 6-2).

Furthermore, Figure 6-3 illustrates an example flow diagram of DM-MHPP operations for the attachment of a HIP enabled MH and a non-HIP enabled MH.

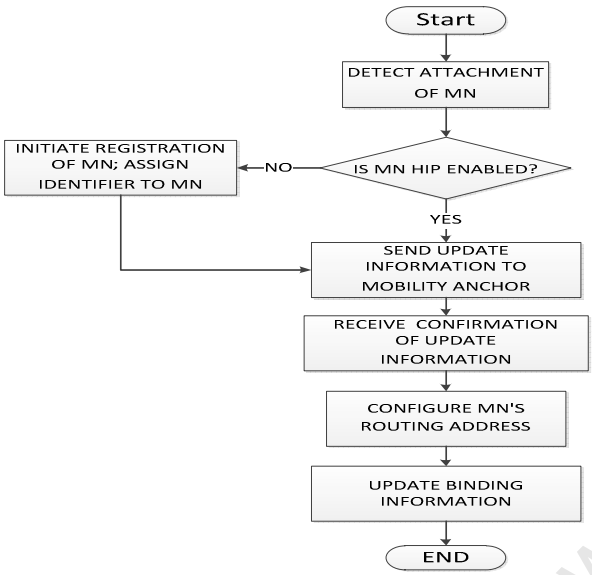


Figure 6-3 Attachment detection for a HIP and a non-HIP MH

6.1.6 Establishing Security Association

Like the MHPP in the hierarchical architecture, this distributed mobility management design enables data traffic between either an HIP enabled MH or non-HIP enabled MH and a CH. An SA is set up prior to the data plane traffic. If the MH is a HIP host, the SA ends or terminates at the MH. If the MH is not a HIP host, the SA ends at the Mobility-enabled HIP proxy to which the MH is registered.

When an MH attaches to a Mobility-enabled HIP proxy, it first registers according to the registration procedure described in Section 6.1.3. After registration, the MH becomes reachable from the CH.

6.1.6.1 The HIP Initiation-Response exchanges

Two pairs of initiation-response packets (I1, R1 and I2, R2) are exchanged to prepare for an SA establishment. Either the MH or the CH may be the initiator, and the other one will then be the responder. The I1 message is shown in Figure 6-4 for a MH which is a HIP host and Figure 6-5 for a non-HIP host. If the MH is a non-HIP host, its Mobility-enabled HIP proxy sends and receives the HIP packets. As demonstrated in Figure 6-4, a HIP enabled CH may initiate a HIP SA from outside the MH domain. By querying the DNS, the CH already has the IP

address of the RVS at which the MH is registered. For the sake of simplicity, it is assumed that both the MH and the CH are registered at the same RVS.

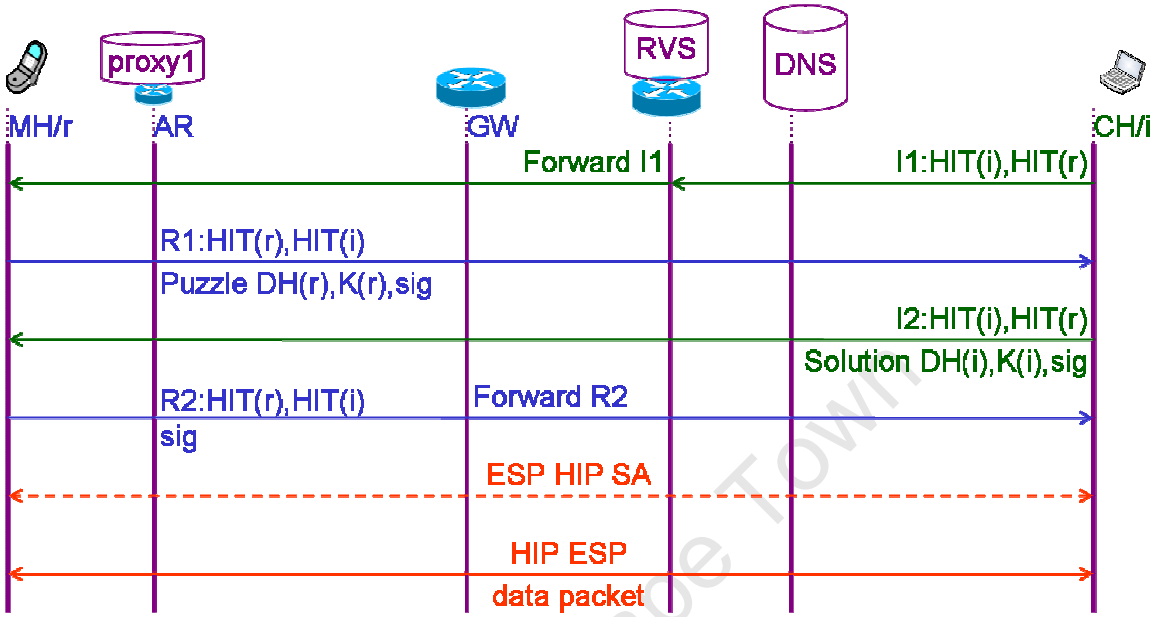


Figure 6-4 The flow of 2 pairs of initiation-response messages for an HIP MH

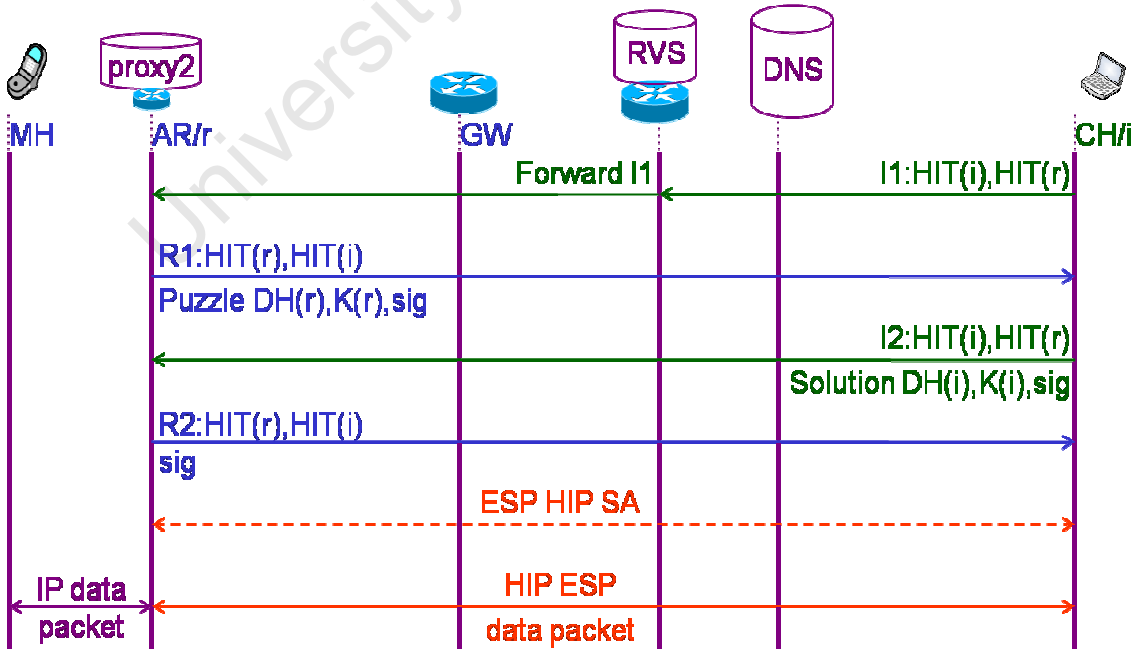


Figure 6-5 The flow of 2 pairs of initiation-response messages for non-HIP MH

Figure 6-6 illustrates an example flow diagram of MHP operations in establishing an HIP base exchange (HIPBE) between a HIP enabled MH and a HIP enabled CH. In addition, the figure illustrates an example flow diagram of MHP operations in establishing an HIPBE between a non-HIP enabled MH and an HIP enabled CH.

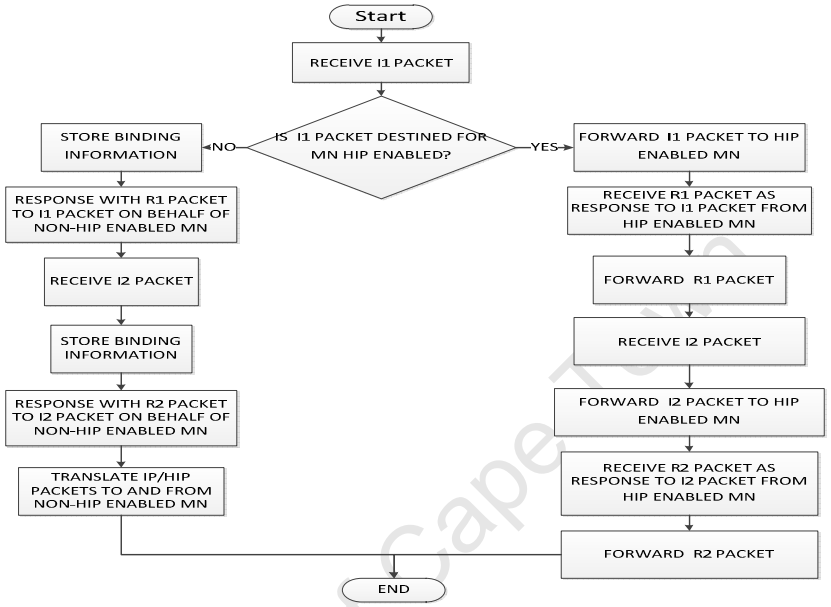


Figure 6-6 HIP SA establishment detection for a HIP and a non-HIP MH

On receiving an I1 packet from the CH, the RVS checks if the destination HIT corresponds to that of a registered MH. If so, the I1 packet is forwarded to the registered IP address of the proxy. On receiving an I1 packet from the RVS, the Mobility-enabled HIP proxy checks the destination HIT in the HIP header. If the destination HIT corresponds to that of a registered HIP enabled MH, the Mobility-enabled HIP proxy (proxy1) forwards the I1 packet to the MH. The Mobility-enabled HIP proxy does not store any binding in the case of the HIP MH. The MH will store the binding HIT(CH):IP(CH), and the MH will send the reply R1. If the destination HIT corresponds to that of a registered MH which is not HIP enabled, the Mobility-enabled HIP proxy (proxy2) stores the binding HIT(CH): IP(CH). The Mobility-enabled HIP proxy (proxy2) will send the reply R1 on behalf of the MH.

The I1, R1, and I2, R2 exchanged pairs are shown in Figure 6-4 and Figure 6-5 for a MH which is a HIP host and a non-HIP host respectively. To complete the HIP SA establishment for

a non-HIP MH, the Mobility-enabled HIP proxy (proxy1) and the CH will exchange the remaining I2 and R2 packets. Unlike I1 packet, R1, I2 and R2 packets will not go through the RVS.

6.1.6.2 ESP Security Association

After the successful exchange of the two initiation-response packet pairs, a HIP SA will be established between the initiator and responder. In data traffic, the HIP proxy (proxy2) uses the HIP SA and ESP to encapsulate/decapsulate non-HIP MH data packets, whereas the HIP MH uses its HIP SA and ESP to process its data. Figure 6-7 demonstrates how the HIP SA is used based on the traffic type, HIP or IP traffic. In addition, it illustrates an example flow diagram of MHP operations as a MHP receives a packet for and from a MH.

When the MHP receives HIP packets destined for one of its MHs, it checks first whether the packets are sent for a HIP or non-HIP MH. When the MHP receives packets from a non-HIP, the MHP determines first whether packets need HIP services or not. To achieve this, there are two solutions: (1) Enable the network-layer of the MHP to pass the received packets to the HIP layer. The HIP identifies the IP flow to which the received packets belong and accordingly offers HIP services if needed; (2) add a flag, for example, a HIP flag to the packets of a packet flow that requires HIP services. The MHP then offers the HIP services if the HIP flag is set to 1.

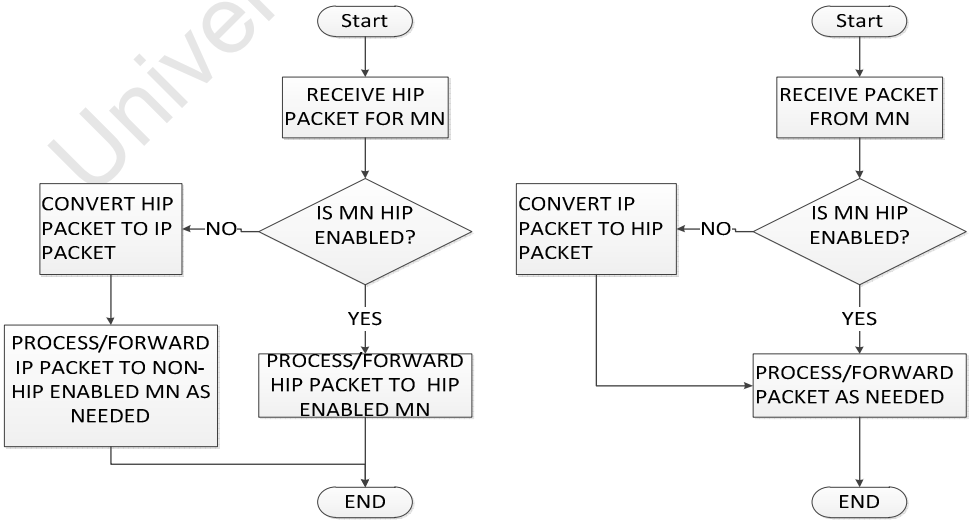


Figure 6-7 HIP SA for data processing, encapsulation and decapsulation

6.1.6.3 HIP Security Association re-use due to handover

The re-use of the established HIPSA allows the MH to avoid some delay and signals and thus enable the seamless IP handover in a secure way. In addition, the researcher's proposed DM-MHPP ensures another way to at least obtain some of the necessary security information from the local server, while the full authentication is being performed at the original servers as explained in the HIP RFCs. In this case, at the server, for example as responder in a remote network location, the average of the end-to-end delay for the inter-domain will be about 110ms [108] that can lead to a long handover delay. In addition, [109] reported that the one-way delay is about 70ms where there is no congestion while [110] reported that from 90 to 95% of the links have a round trip time (RTT) of less than 500ms. Specifically, in the regional connections, a RTT of less than 200ms is experienced in more than 75 to 90% of links. Therefore, the re-use of the established HIP SA or local server for the SA establishment/update further reduce the associated delay and signalling overhead.

6.1.7 Handover

Figure 6-8 shows the handover procedure of a MH, which is either HIP MH or non-HIP enabled MH, between two wireless access networks belonging to the domain managed by the same GW. The MH is communicating with a HIP enabled CH (not included in the figure) which lies in a different domain.

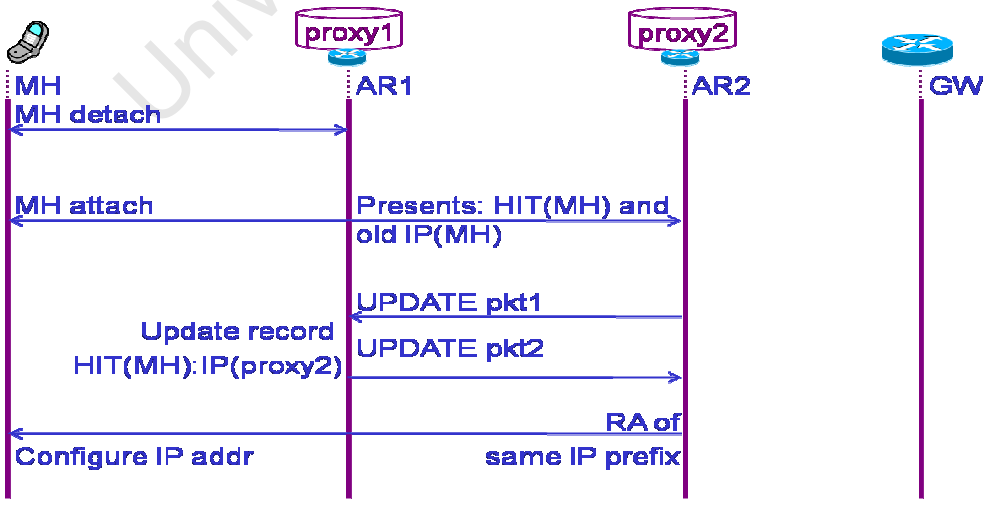


Figure 6-8 DM-MHPP for MH's handover

The MH may change its point of attachment (PoA) and attach to another Mobility-enabled HIP proxy (proxy2) under the same GW. The new access network may be the same or a different network type as the previous access network. Irrespective of the type of access network to which proxy2 is connected and irrespective of whether the MH is HIP enabled or not, proxy2 will be informed about the attachment of the arriving MH. During this attachment the MH presents its HIT and previous IP to proxy2. Proxy2 then determines the previous proxy, proxy1, from the network prefix of the MH's previous IP and then acts as the HIP proxy and updates the binding record of the MH at proxy1. Communicating with proxy1 allows proxy2 to securely know the context of the established HIP SA.

Note that in a secure private network, for non-HIP MH, HIP communications can be terminated at proxy1 and then exchanged with a MH as IP communications via proxy2. That is, proxy1 performs HIP proxy functions while proxy2 performs mobility support. The advantages of this approach are: (1) non-HIP MH can move to any mobility-enabled access router and still preserve its active sessions with HIP CHs; (2) it allows load balancing, for example, if the proxy is heavily loaded it can assign some of the load to other HIP proxies. However, this approach can result in inefficient routing if the distance between proxy1 and proxy2 is large while the distance between the GW and proxy2 is small. In the DM-MHPP, all HIP communications are handled in the new proxy, proxy2. One of the main advantages of the DM-MHPP is that it can ensure efficient routing and reduces vulnerability between the MH and the proxy.

When the MH performs the handover from a network through which the MH has established the active session, proxy2 detects the attachment of the MH and sends an UPDATE packet (packet1) to proxy1. When proxy2 receives the reply UPDATE packet (packet2) from proxy1, it will send a RA to the MH. The RA will have the same network prefix that the MH used to configure its IP address in the proxy1 subnet. The MH, therefore, retains the same IP address configuration so that a DAD is not needed. This procedure significantly reduces handover latency, signalling overheads and packet loss.

Figure 6-9 shows exchanged messages between entities in a wireless communications system as a non-HIP enabled MH performs a handover from one access network to another, through which the active session is established.

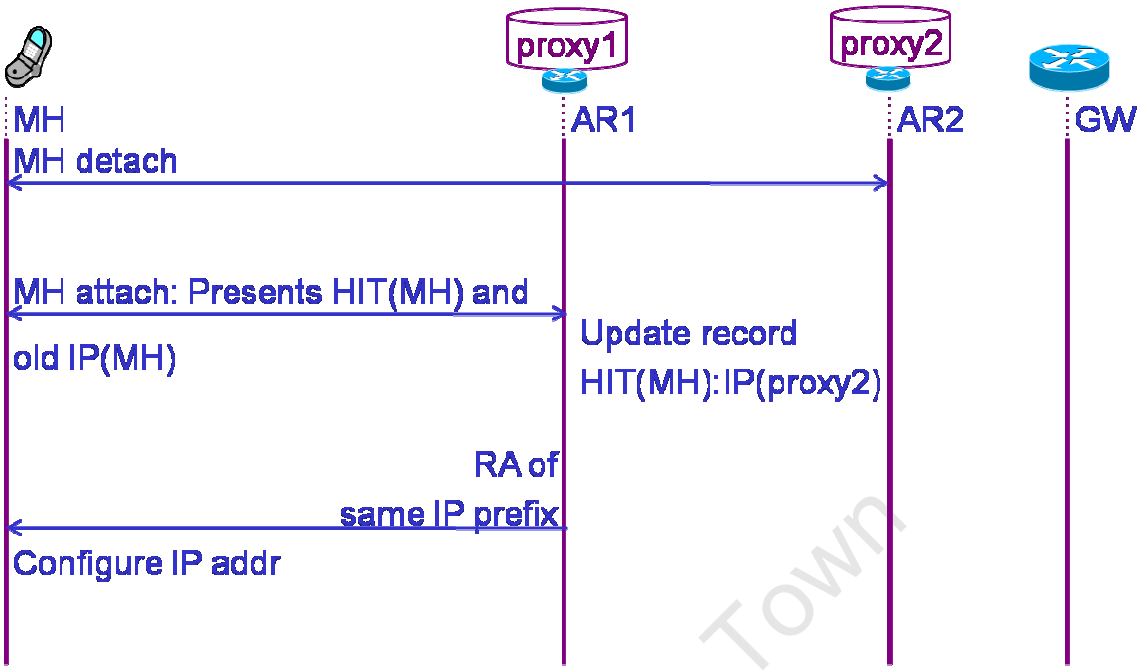


Figure 6-9 HO procedure of a MH using DM-MHPP

When the MH returns to the proxy, through which the active session is established, the proxy checks its cache binding to identify the MH and where its active sessions are established. If the sessions were established via the new proxy, the latter updates the record of the MH and starts serving it instead of forwarding it to another proxy. It is important to note that the proxy does not send any handover-related signalling and thus the location update delay is eliminated. Furthermore, there is no need to update the MH record at the RVS since the MH is still reachable via the registered proxy at the RVSs.

6.1.8 Performance Gains of DM-MHPP

The DM-MHPP distributes MHPs introduced by the MHPP and equips them with additional functions to produce a powerful mobility management solution suitable for flat network architecture. Thus, the DM-MHPP reduces over the air signalling overheads, maintains a stable MH locator even when the MH changes MHPs and reduces unnecessary signalling overheads over the core network through which established sessions are communicated. Furthermore, the DM-MHPP makes the IP handover in flat architecture transparent to the upper layer protocols and thus securely preserves the active sessions.

Consequently, IP handover performance is significantly optimised. Like the MHPP and HIPPMIP, the DM-MHPP updates locator packets at the HIP RVS. CHs are also unneccessary hence reducing signalling overheads and delays. The network-based aspect of the DM-MHPP locally manages handover-related packets and packet routing before and after the handover, thus ensuring efficient routing. The HIP aspect, on the other hand, mainly provides its security capabilities and multihoming insured by the HIP secure and permanent host identifier. In basic MHPP (4.2) handover, the time taken by the MH to register its new location address and HIT to the LRVS as well as deregister from its old location can be a single point of failure.

6.2 Signal-Less Distributed Mobility Solution (SL-DM)

This section introduces a distributed mobility management solution, which can be implemented either as a host-based or network-based solution, where data traffic dynamically anchored at respective points of attachment on the mobile host (MH) during mobility. This section also introduces an elegant network-based reachability mechanism for the MH. This mechanism ensures MH tracking, secure location updating, assignment of a host identifier per interface and the use of a single IP address for MH reachability within a given network domain.

6.2.1 Need for SL-DM

Again, to provide host mobility in a flat architecture and to satisfy the requirements of future applications, the IETF is revising mobility management designed for the hierarchical network architecture. In this architecture, mobility solutions use a central entity to manage the movement of the MH between different networks. The challenges of centralised mobility management (CMM) in a flat architecture have been identified in [9]. These challenges include single points of failure and bottlenecks, non-optimal routing paths, scalability problems and long handover delays.

To solve the aforementioned challenges and effectively support mobile users, the distribution of mobility management functions in the flat architecture is required. To achieve this, various distributed mobility management (DMM) solutions have been proposed. However, existing DMM solutions encounter a non-optimal route for the ongoing traffic when the MH is

away from its initial point of traffic establishment. This is because the existing DMM solutions anchor the traffic flows at the point where the session was initially established.

Using the existing DMM solutions, the active session experiences a non-optimal route especially for ongoing traffic when a MH moves from one network to another. Furthermore, the solutions are applicable to a small coverage topological area due to the non-optimal route that can be caused by the traffic anchoring method used in the solutions.

To address the non-optimal route and signalling overhead of existing DMM solutions, the researcher proposes an elegant SL-DM solution that can be implemented either in a host-based or network-based way. The proposed solutions: (1) dynamically anchor the traffic flow to the MH's current point of attachment; and (2) remove the handover-related signalling.

6.2.2 Design Objectives for SL-DM

Like the DM-MHPP, the design of the researcher's network-based implementation of the SL-DM is based on two principles: (1) distributed mobility entities to manage the IP handover for the HIP and non-HIP MHs. In addition, the SL-DM aims to provide signal-less mobility architectures that efficiently and securely manage the MH handover. In addition to the design objectives of the DM-MHPP, the SL-DM has the following additional objectives:

1. To provide a handover solution for the IP handover in a flat network architecture that can be configured as a network-based or host-based solution to ensure the required QoS.

2. To provide seamless IP handover for both HIP-enabled MH and non-HIP-enabled MH in flat network architectures.

3. To provide a signal-less IP handover in the flat network architecture and thus eliminate the hanover-related signalling overheads in the air interface between the MH and the access points even for the host-based implementation of the SL-DM.

4. To ensure secure and scalable IP handovers between heterogeneous networks by effectively using the MH protocol stack capabilities.

5. To dynamically anchor data traffic to the mobility entities that result in an efficient routing.

6. To simultaneously provide mobility support for different types of MHs, for example, HIP and non-HIP MH.

6.2.3 Protocol Overview

A signal-less distributed mobility solution is a distributed mobility solution that does not explicitly exchange the handover-related signals, hence the name signal-less mobility solution. Furthermore, this mobility solution is designed for the flat network architecture, where there is a need for the dynamic anchoring of data traffic at respective points of attachment on the MH during mobility. In the SL-DM, handover-related messages do not necessarily facilitate the handover of the MH among the different points of attachment. Ultimately, the proposed SL-DM and reachablity mechanism improve the handover performance.

The handover performance of the HIPPMIP, MHPP and DM-MHPP indicates that there is a need for stack-independent mobility solutions without incurring signalling overheads. Therefore, the researcher developed the SL-DM and made it flexible for implementation either in a network-based and/or host-based manner. The SL-DM aims to eliminate the handover-related messages and to ensure dynamic traffic routing in the flat network architecture to improve the MH handover performance. The proposed mechanism ensures fast detection, and an elegant way of exchanging the necessary information for handover execution. In the SL-DM, this information is handled inside the first few data packets. Thus, the proposed mechanism reduces handover delays and eliminates handover-related messages. It is important to note that the inclusion of the handover-related information in the data packets was carefully considered. Thus it does not exceed the maximum transmission units and does not violate the handover-related security aspects.

The following section describes the host-based and network-based implementations of the proposed SL-DM solution. The researcher discusses these models in terms of their principles of operation and their signalling and packet routing before and after the IP handover. In addition the

shortcomings and consequences of handover-related signals as well as their inclusion inside the data packets are discussed.

6.2.4 Mobility Management Architecture

The architecture for host-based and network-based mobility management is shown in Figure 6-10 and is described below. The network-based architecture introduces intelligent mobility access gateways (iMAGs) as depicted in Figure 6-10. In this architecture the communicating hosts, for example MH2 and CH2, rely on the iMAGs to carry the proposed mobility management functions.

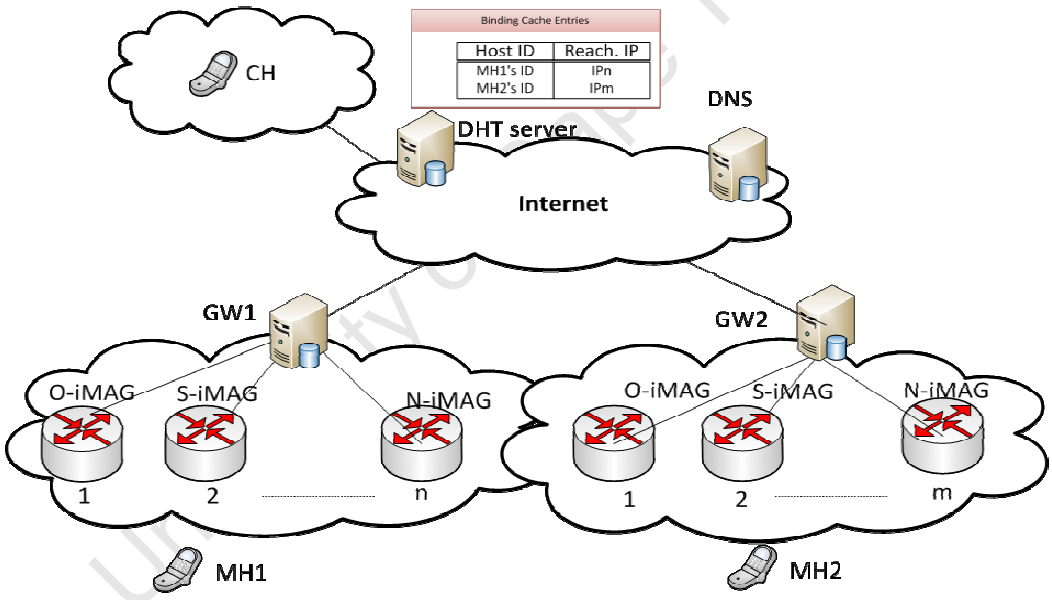


Figure 6-10 The distributed iMAG architecture

The iMAG allocates the MH's IP prefix/address and maintains the binding cache for the registered MHs. The iMAG tracks the MH movement in the network. Furthermore, the iMAG swaps the source and destination addresses of a data packet that includes certain parameters, which are an IP option that contains an IP address belonging to a different subnet or network and a mobility proxy flag (MP).

The host-based architecture has normal access routers as depicted in Figure 6-10. In this architecture the communicating hosts, for example MH1 and CH1 are directly involved in carrying out mobility management functions and do not rely on iMAGs.

6.2.5 Registration and Reachability

When an MH enters the distributed iMAG domain, the iMAG detects the MH attachment and allocates an IP prefix. The MH configures an IP address from the allocated prefix. In fact, the MH attaches to the O-iMAG, which assigns the prefix P1 to the MH, which in turn configures the IP address. Thereafter, the O-iMAG registers the MH at a DHT server. The registration of the MH is described below. The signalling flow diagram of the registration of the MH is illustrated in Figure 6-11.

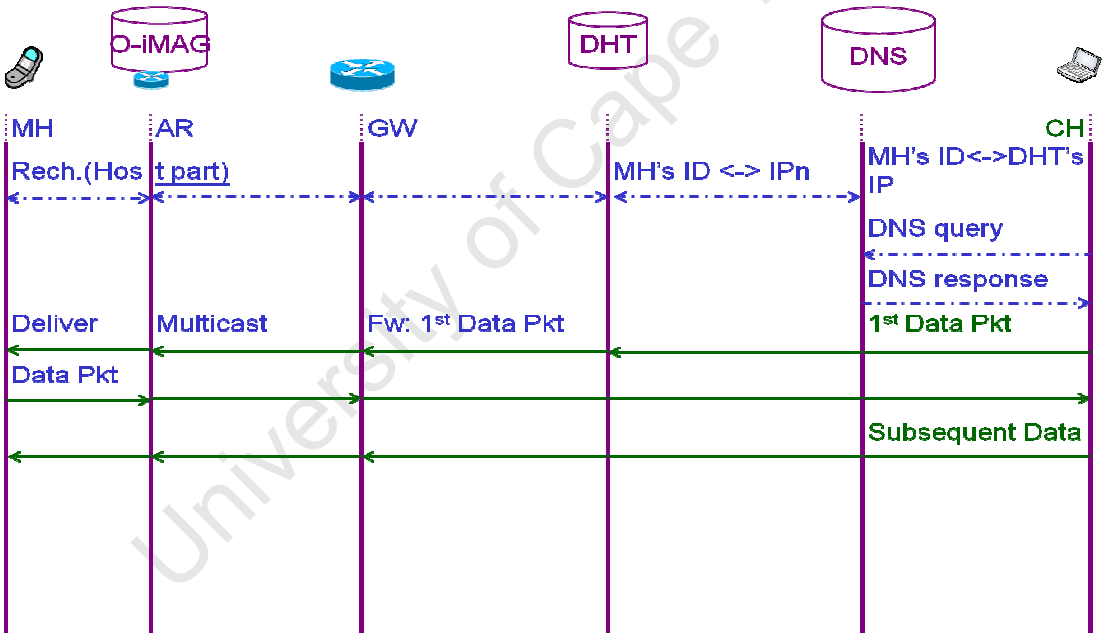


Figure 6-11 Registration signalling between the relevant elements in the network

Figure 6-12 illustrates how a CH establishes communication sessions with an MH, which supports the proposed mechanism. The CH queries the DNS about the MH IP address. The DNS responds with the IP address of a distributed hash table (DHT) server with which the MH is registered. The DHT is located between the DNS and the current MH location. This location ensures a secure and scalable reachability procedure as well as minimises the active involvement

of the DNS in packet forwarding.

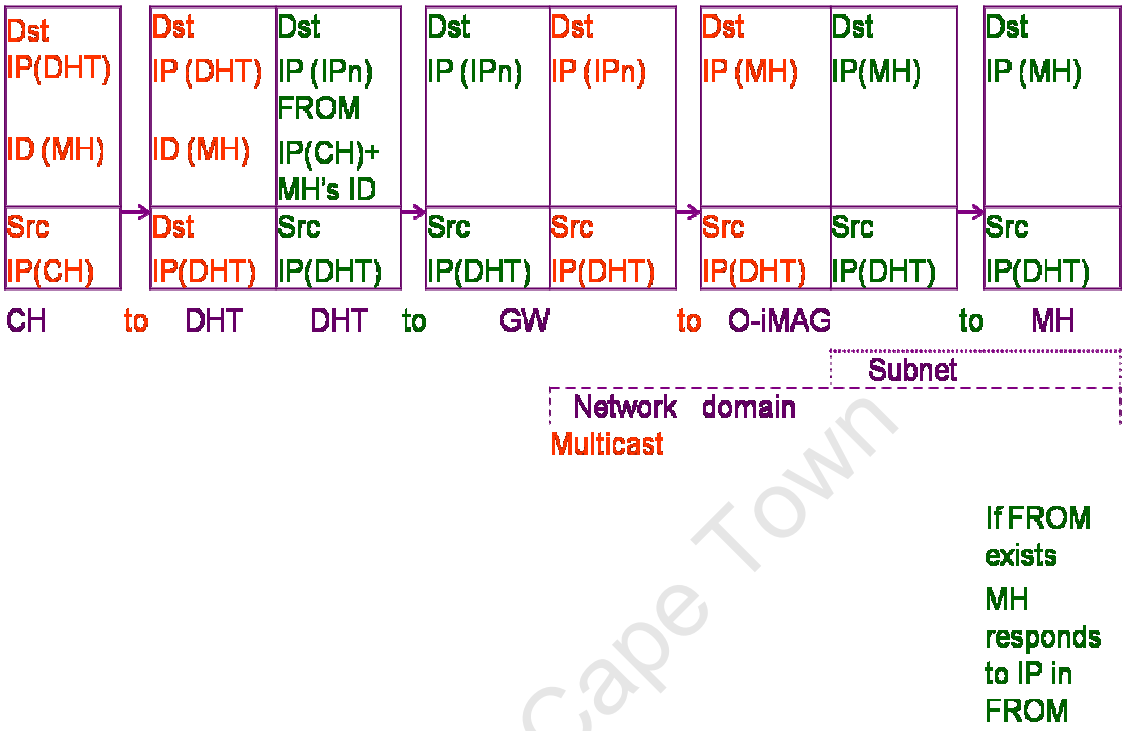


Figure 6-12 First data packet from the CH establishing a session with the MH

On receiving the DNS response, the CH sends the first data packet to the MH through the DHT server where the MH is registered. The DHT server forwards the packet to the MH's current location. The MH's current location is identified by a multicast address, for example, IPn, which belongs to the domain of iMAGs where the MH is attached. In other words, IPn refers to a domain's reachability address. For example, if IPn is a reachability address of "domain *n*", all MHs attached to domain *n* use IPn as the identifier for their current locations. On receiving a packet from the DHT server, the MH or iMAG checks the field of the original sender in the received packet. Thereafter, the MH or iMAG communicates directly with the sender (i.e., CH or CH's iMAG) instead of the DHT server. Figure 6-13 depicts such communications. During the establishment of a communication session between MH and CH, the iMAG functions according to whether the mobility management approach in the architecture is host-based or network-based. For example, in the host-based approach is followed, the iMAG behaves like a normal access router. Whereas, in the network-based approach, the iMAG has extra functionalities for the

management of mobility on behalf of the MH.

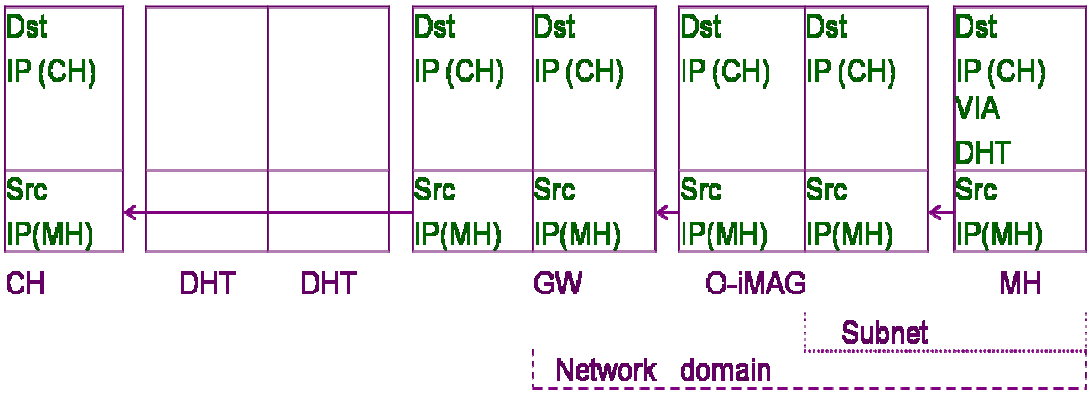


Figure 6-13 Data packet from the MH to the CH

6.2.6 Establishing Communication Sessions

When a CH wants to communicate with an MH, the CH queries the DNS about the IP address of the MH. The DNS responds with the IP address of a server, for example, the DHT server, where the MH is registered. The DHT is selected for the reachability in between the DNS and the current MH location since it (DHS) supports the scalability. It is important to note that this mobility solution implicitly detects the protocol stack of the MH and then accordingly utilises the features of the stack towards a secure, scalable and seamless handover.

6.2.7 Handover

In the host-based approach, when the MH moves from the O-iMAG to S-iMAG, it receives a new prefix and configures another IP address, IP2 address as demonstrated in Figure 6-14 and Figure 6-15. Figures 6-14 and 6-15 show host-based scenarios where the MH moves inside and outside the domain reachable by IPn and IPm respectively. When the MH moves within the IPn domain, there is no need for reachability update messages. However, when the MH moves out of the IPn domain, the MH sends reachability update messages as shown in Figure 6-15. The O-iMAG tracks the MH movement and acquires the address of the S-iMAG. Thereafter, the O-iMAG uses the acquired address to forward the packet when the MH moves out of its range.

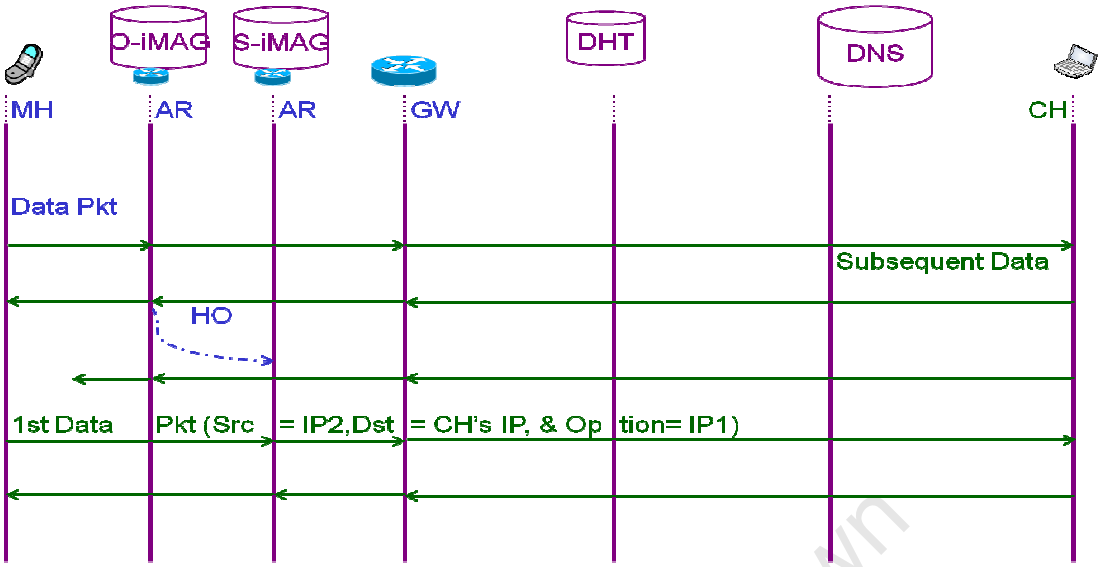


Figure 6-14 Packet flow after MH handover within the IPn domain

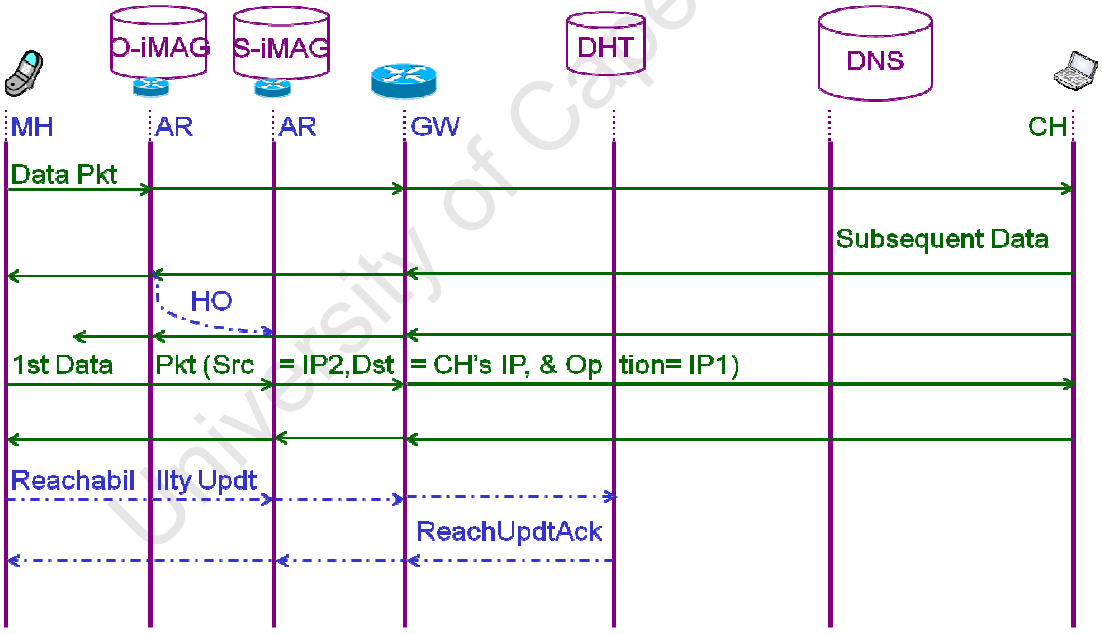


Figure 6-15 Packet flow after MH leaves the IPn domain

At S-iMAG, the MH uses IP2 as the source address for active and newly established communication sessions. For active sessions, initiated at O-iMAG with source address IP1, the MH includes IP1 in the IP option of the first few data packets. In this host-based approach, the iMAG serves as a normal access router for all data packets to and from the MH.

On receiving a data packet with a source IP address that does not match any of its active sessions, the CH checks whether the packet has information in the IP option field. If the field includes an IP address that matches one of the active sessions, the CH knows that the MH has moved to a new location. From the IP address in the option field, the CH identifies the IP flow where the data packets belong. Thus, the CH creates a binding between the source IP of the received packet and IP address in the option field. To present the packet to the upper layer, the CH swaps the source address of the packet, IP2, with the IP address in the option field, IP1.

For outgoing traffic from the CH to the MH, the upper layer protocols at the CH use IP1 as the destination address. The network layer uses the stored binding to swap the destination address from IP1 to IP2. The subsequent packets from the CH to the MH, therefore, are sent directly to the MH's current PoA. This procedure prevents the triangle routing problem where packets have to move through the anchor where the communication was initially established.

In the network-based approach, mobility management is implemented at the iMAGs instead of the MH and/or CH. Similar to the host-based approach, when the MH moves from O-iMAG to S-iMAG, the MH configures a new address (i.e., IP2). The S-iMAG creates a binding association for the MH that includes MH ID, previous IP address, IP1 and the current IP address, IP2. The MH sends the uplink traffic to the CH using IP1 as the source address. On receiving the packet from the MH with a source address, IP1, which does not belong to its prefixes, the S-iMAG looks if there is a binding cache entry for the source address. If the entry exists, the S-iMAG swaps the source IP address (IP1) with the new IP address that the MH has configured in the S-iMAG's network (e.g., IP2). Furthermore, the S-iMAG includes IP1 in an option field. The S-iMAG then forwards the packet to the IP address of the CH. Thus, the overload of functionalities at the MH is reduced since the MH does not perform the swapping process. When the packet arrives at the CH network, the iMAG of the CH receives the packet. The iMAG of the CH then checks if the packet includes an IP option field. If there is an option field, the iMAG of the CH swaps the source IP address with the IP address included in the option field. Furthermore, the iMAG of the CH maintains the mapping of the two addresses and forwards the packet to the CH as illustrated in Figure 6-16 and Figure 6-17.

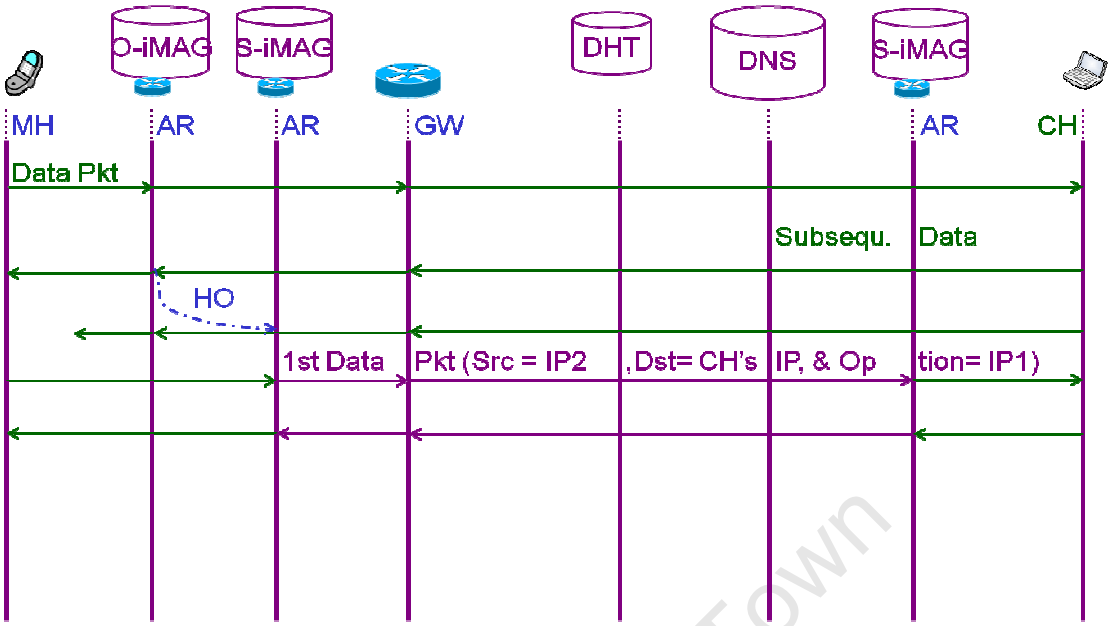


Figure 6-16 Network-based for MH movement in the same range of IPn

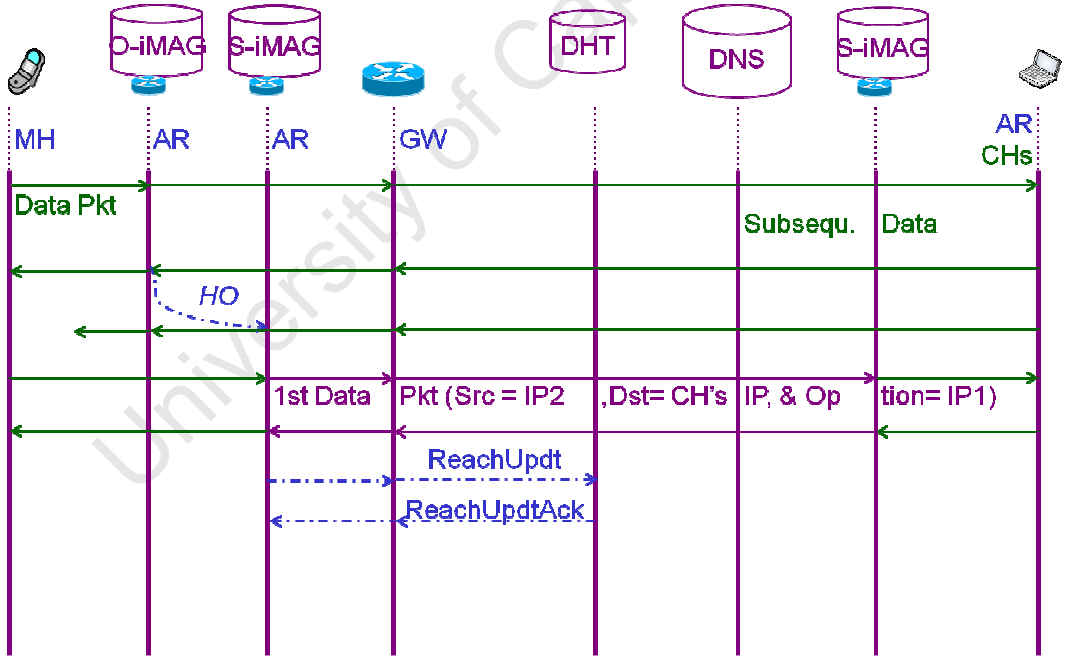


Figure 6-17 Network-based for MH movement in a different range of IPn

When the CH sends a packet to the MH, it uses IP1 as the destination address. On receiving the packet from the CH, the iMAG of the CH checks if there is an existing mapping for the packet's destination address in its cache entries. If the mapping exists, the iMAG swaps

the destination address (IP1) with the corresponding address in the cache entry. The iMAG further includes the original packet destination address (IP1) into the IP option field and then forwards the packet to the S-iMAG of the MH as illustrated in Figure 6-16 and Figure 6-17. On receiving the data packet, the S-iMAG of the MH checks if there is an IP option field. If this field exists, the S-iMAG replaces the destination address of the packet with the address in the option field and then forwards the packet to the MH. If the option field is not found, S-iMAG does nothing but simply forwards the packet to the final destination (MH) or an intermediate router. Ultimately, the MH receives the data packet as if it was directly sent from the CH.

6.2.8 Performance Gains of SL-DM

The SL-DM is a promising approach to current and future wireless networks. The SL-DM is expected to meet the demands of the anticipated increase in data traffic by providing scalable, secure and seamless mobility support for the MH. This approach proposes a distributed mobility management solution that: (1) eliminates the need for handover-related signalling; (2) eliminates the static anchoring traffic and thus reduces the long routing path for long-lasting traffic; (3) eliminates the delay pertaining to duplicate address detection (DAD); and (4) ensures efficient reachability for the MH in the flat architecture. Furthermore, SL-DM is a protocol-stack independent solution that fully utilises the features of the underlying stack.

This chapter has provided a discussion on two distributed designs, a Distributed Mobility Management with Network-Based Host Identity Protocol (DM-MHPP) and a Signal-Less Distributed Mobility Solution (SL-DM) to support all IP hosts. The chapter has discussed the DM-MHPP and its details in Section 6.1 and related subsections. This is followed by a discussion of the SL-DM and its details in Section 6.2 and related subsections.

Chapter 7 Experiment, Results, and Performance Evaluation of DM-MHPP and SL-DM

In this chapter, the researcher evaluates two of his proposed mobility designs/solutions, that is, the DM-MHPP and SL-DM. These mobility solutions are also evaluated by the OMNeT++ network simulator [99] (briefly presented in Section 5.1). He also presented and analysed the results obtained from the proposed mobility solutions, The DM-MHPP and SL-DM are discussed in Sections 6.1 and 6.2, respectively. The handover performance of DM-MHPP is evaluated and compared against its related work. The performance of SL-DM is also evaluated and compared against its related work. A discussion of the DM-MHPP's handover performance results and analysis is furnished in Section 7.1, while the SL-DM's handover performance results and analysis are discussed in Section 7.2.

7.1 Evaluation of the DM-MHPP

Like the HIPPMIP and MHPP, the handover of the DM-MHIPP is carried out in two partially overlapping IEEE 802.11b (11 Mbps peak data rate) subnetworks. In DM-MHPP, the mobility-enabled HIP proxies are co-located with the distributed access routers. That is, mobility in the subnetworks 1 and 2 is managed by MHP1 and MHP2, respectively, for DM-MHPP. The simulated topology is illustrated in Figure 7-1 and the simulation parameters are described in Table 6.

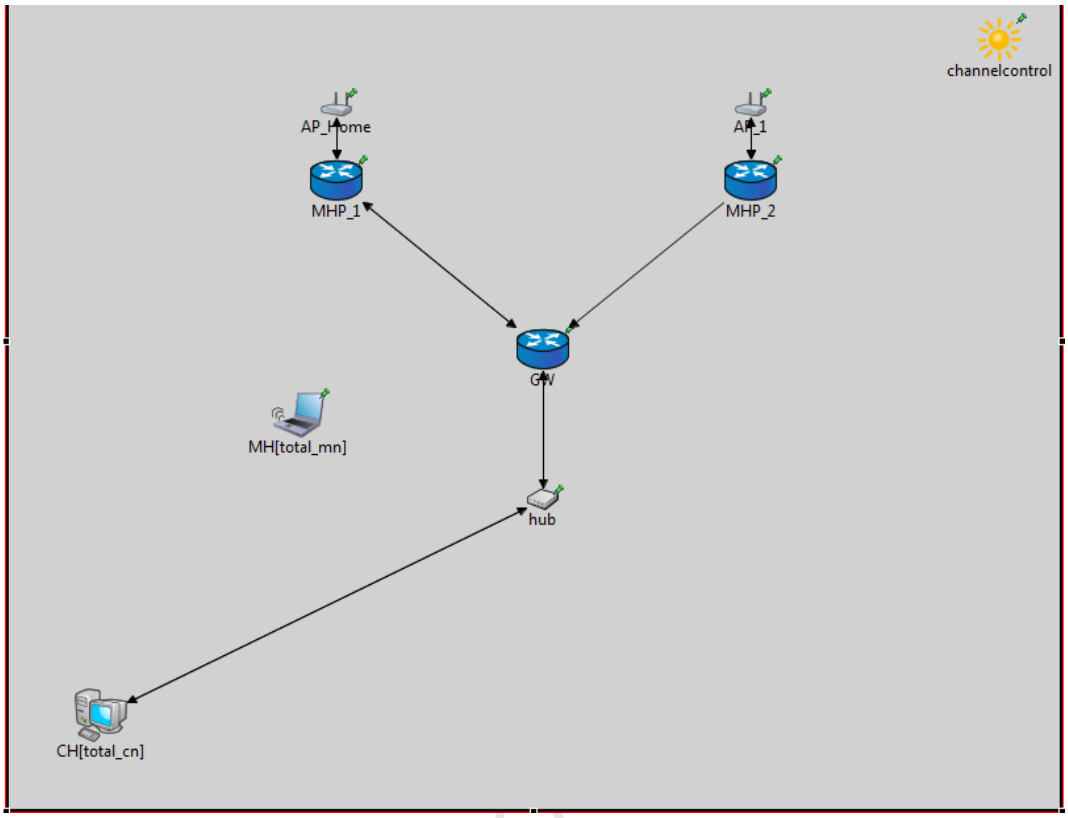


Figure 7-1 Simulation network topology of DM-MHPP

Table 6. Simulation parameters under which HIP, DM-MHPP and DM-MHPP are examined

PARAMETER	VALUE	PARAMETER	VALUE	PARAMETER	VALUE
Speed	1 m/s	Mobility Model	Rectangle	Route advertise Interval	≥ 0.3s
# of POA	2	Packet flow	Bi-dir CBR		≤ 0.7s
# of MH	1	UDP packet transmit rate	0.13 s	AP power	2.0 mW
Grid size(m^2)	850*850	Packet size	256 B	Beacon freq.	0.1s

7.1.1 Architecture of DM-MHPP's Main Mobility Functions in OMNeT++

In this section, the researcher describes the node structure in the OMNeT++ for the DM-MHPP's main mobility entities. To implement the new mobility functionalities proposed by the DM-MHPP, he has extended the MHPP mobility entities that are mobility-enabled HIP proxies (MHPs) on INET modules. For DM-MHPP, MHPs have also been modified to operate with the HIP RVS, instead of the LRVS, utilising the host identifiers, that is, HITs introduced by HIP modules. The modified MHP is illustrated in Figure 7-2.

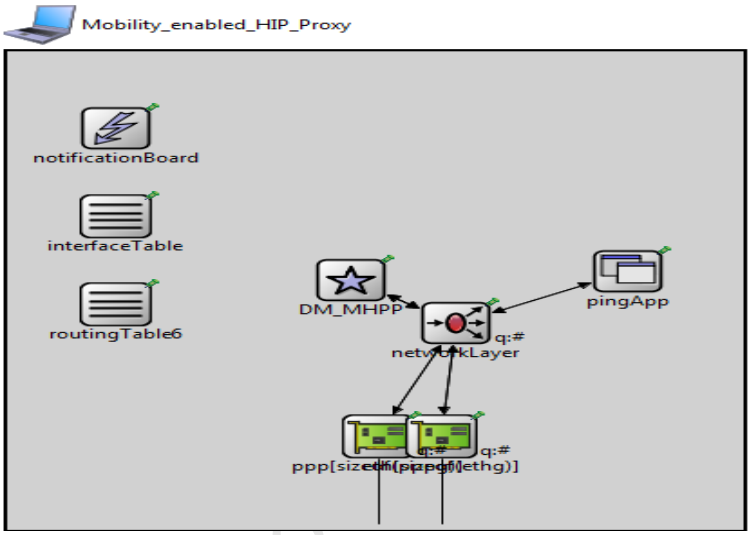


Figure 7-2 MHP with distributed mobility functionality

7.1.2 Simulation Scenarios

The simulation environment under which the researcher examined the DM-MHPP constitutes two IEEE 802.11b subnetworks with MHPs co-located within the access routers. The two subnetworks partially overlapped. A fixed HIP CH (i.e., hipsrv) is placed outside the access network of the MH and runs a UDP application to transmit a datastream at 15 Kbps with a packet size of 256 Byte to the MH. The simulation runs for 25,000 seconds while the MH speed is fixed at 1 m/s as it moves from subnet 1 that is managed by MHP1 to subnet 2 that is managed by MHP2 and vice versa. The simulation parameters of this scenario are described in Table 1.

7.1.3 Performance Evaluation and Analysis of DM-MHPP

In this section, the researcher presented and analyses the handover performance results

obtained from the MHPP and DM-MHPP. The handover delays, packet loss and signalling overheads are investigated. He has also investigated other factors that affect MH handover performance such as the number of MHs simultaneously performing handover while communicating with different CHs. In addition, end-to-end delays before and after the MH handover are investigated. It is important to note that handover delay, packet loss and handover-related signalling in this simulation context have the same meaning as defined in Section 5.2.3.

7.1.3.1 Handover delay

Using the above mentioned simulation environment (Section 7.1.2) that is similar to the one specified in Section 5.3.2, the researcher examined the model (DM-MHPP). In addition, he recoded and analysed a hundred handovers for the DM-MHPP. The fluctuation in the HOL of the DM-MHPP and MHPP over the first 23 HO instances is depicted in Figure 7-3.

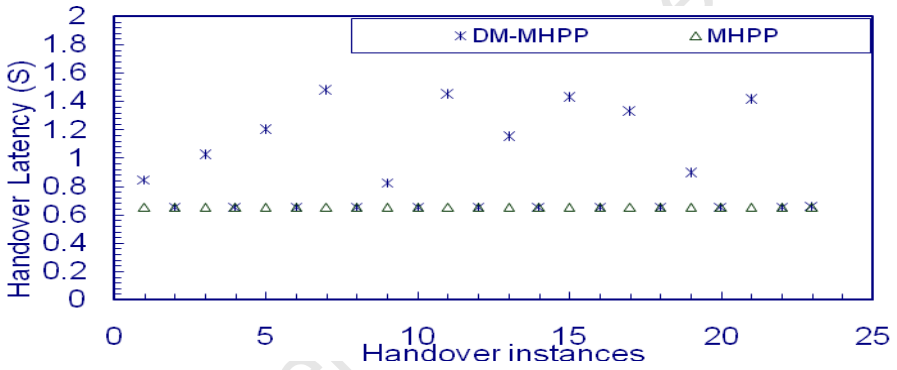


Figure 7-3 The first 23 handoffs for DM-MHPP and MHPP

The researcher carried out a hundred handovers for each of the two investigated models. As evident in Figure 7-3, fluctuations or differences in the values of handover latency in the two models are observed over the first 23 handover instances. It is observed that the DM-MHPP exhibits varying handover latencies, which vary between 0.6s and 1.8s in the handover from a visited network to the home network and from the home to a visited network respectively. This is because the DM-MHPP communicates with the PoA of the session, that is, the PoA in the home position when the MH moves from the home to a visited network, to redirect the data traffic via the new PoA, that is, the PoA in the visited network. It is also evident from the measurements presented in the figure, in the IP handover towards the PoA session, that the handover delay due

to location updates has been completely eliminated. This is because in the DM-MHPP, when returning to the PoA of the session, the MHP stops forwarding the data traffic and thus serves as an authoritative MHP. These services are provided for HIP and non-HIP MHs.

Before dwelling on the details of Figure 7-4 it is necessary to refer to the PoA through which the session of the MH is established as the PoA of the session. The figure displays the RTT while the MH is connected to the PoA of the session as well as RTT when the MH is absent. It is evident that the RTT when the MH is absent from the PoA of the session is longer than the RTT while the MH is connected. In other words, Figure 7-4 indicates the RTT of the DM-MHPP over the simulation time of 25,000 seconds. It is further evident that while the MH is connected to a PoA different from the PoA of the session, the RTT is higher than that while the MH is connected to the PoA of the session.

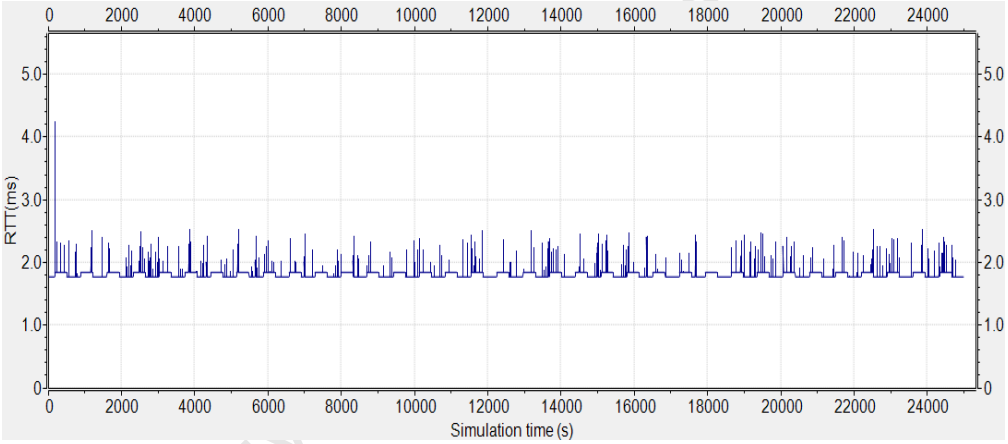


Figure 7-4 The RTT before and after the MH's handover using DM-MHPP

The close-up views of the IP handovers of the DM-MHPP while the MH is moving away from and towards the PoA of an active session, are shown in Figures 7-4 and 7-5 respectively. Both figures depict a session between the non-HIP MH CH initiated via MHP1. In Figure 7-5, the UPD packets of the flow while the MH is connected to MHP1 are called the "UDP packets before HO". In addition, the figure shows the packets after the IP handover and calls them the UDP packets after HO. Furthermore, the figure depicts the lost UDP packets, called UDP packets lost due to HO, because of the MH handover as well as the location update packets, called UPDATE packets for HO, to inform the PoA of the session. Moreover, in Figure 7-.5 in the

handover while the MH moves away from the PoA of an active session, the MH has received the last UDP packet via the old PoA, MHP, at 190.729s and the first UDP packet via MHP2 at 192.064 and thus the delay between them is 1.335s. It is evident in Figure 7-5 that there is no need to delete the MH binding since the PoA of the active sessions will continue to serve its sessions even if the MH is absent. Ultimately, signalling overhead related to the deletion process is eliminated.

The same information presented in Figure 7-5 is also presented in Figure 7-6 but in this case for the IP handover towards the PoA of active sessions. Furthermore, Figure 7-5 indicates unidirectional UDP packet flow from the HIP CH to non-HIP MH during movement from a visited to the home network. The left side of the figure displays the MHPs, MH and CH. In the MH handover towards the PoA of the session, the MH has received the last UDP packet via the old PoA, MHP2, at 519.788s and the first UDP packet via MHP1 at 521.521 and thus the delay between them is 1.733. It is also evident from the measurements represented in Figure 7-5 that the location-related packets and delays are eliminated.

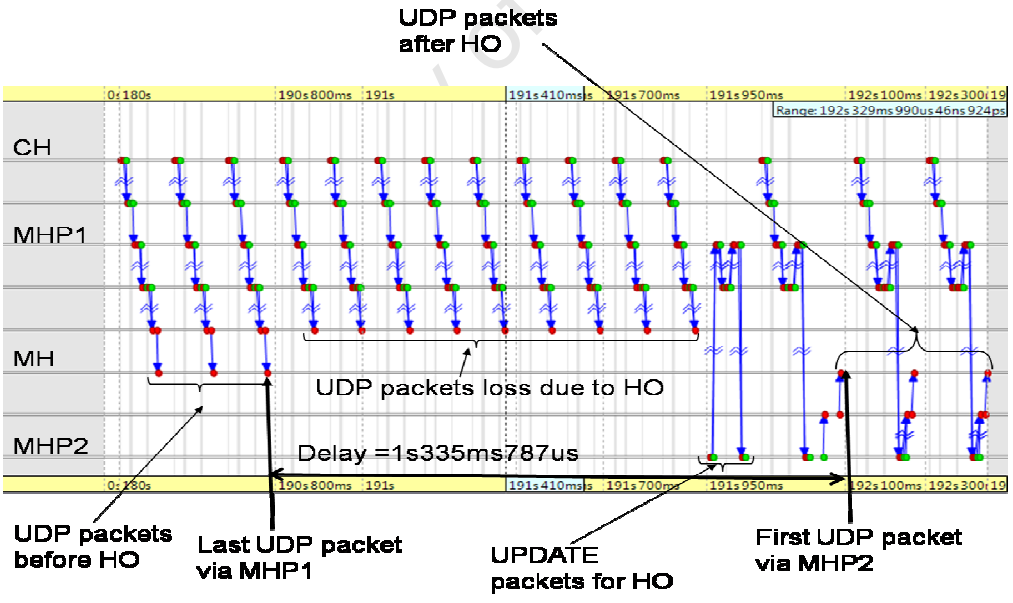


Figure 7-5 A close-up view for the HO of the MH from a "h" to a "v" networks

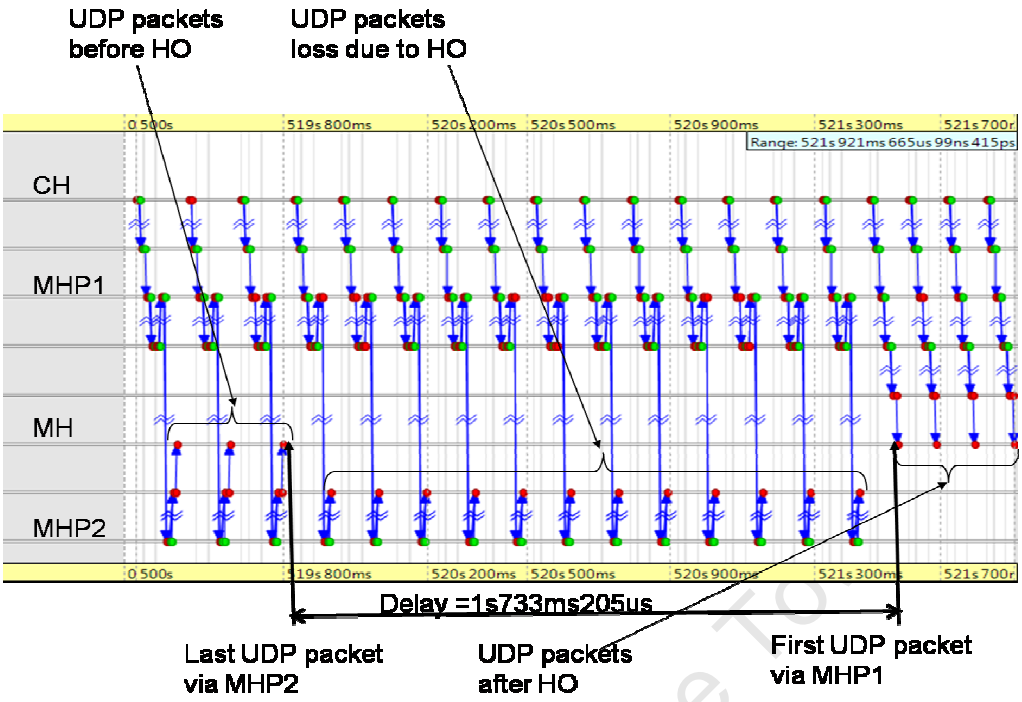


Figure 7-6 A close-up view of the HO of the MH from a "v"to the "h" network

7.1.3.2 Packet loss

Figure 7-7 depicts the packet loss of the DM-MHPP and MHPP. The researcher measured the loss of data packets of a UDP application in the unidirectional traffic going from the CH to the MH during IP handover. Again, in these measurements there is no buffering or forwarding technique used to mitigate the packet loss. Like the handover delay, packet loss in DM-MHPP is small when MHs move towards the PoA of the session while packet loss is high when the MH moves away from it.

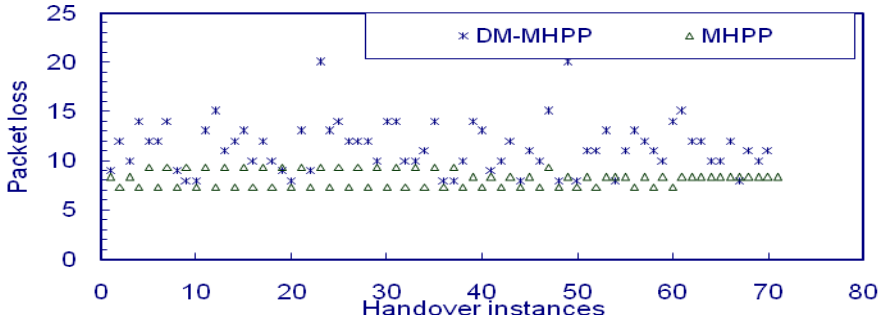


Figure 7-7 The first 70 packet loss for DM-MHPP and MHPP

7.1.3.3 Signalling overhead

Handover related messages in the DM-MHPP and MHPP are portrayed in Figure 7-8. In the DM-MHPP during 25,000s simulation time, the MH performed 70 handovers. Thus Figure 7-8 depicts the handover-related messages for the MHPP and DM-MHPP over the first 70 handovers. It is evident from the figure that the DM-MHPP has outperformed the MHPP in the handover-related signalling since the DM-MHPP does not use any handover-related messages when the MH moves to the PoA of the session. It is important to note that a case where the MH performs a handover during active sessions established through different PoAs is not present in the said figure.

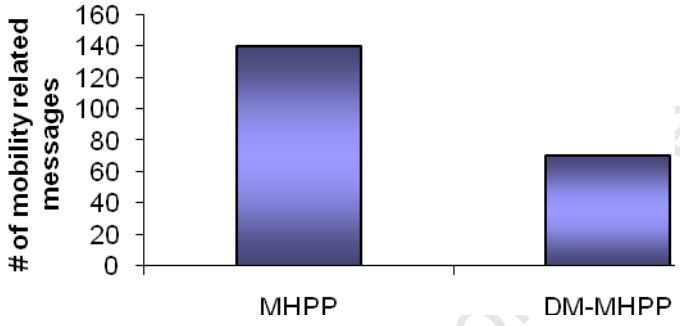


Figure 7-8 Handover-related messages of the MHPP and DM-MHPP

Furthermore, signalling overheads of HIP, PMIP, HIPPMIP, MHPP and DM-MHPP are described in Table 7. The first row in Table 7 indicates the number of binding update messages when the MH has ongoing communications sessions with one CH. In fact for DM-MHPP, the number of binding update messages when the MH has ongoing sessions with *n* CHs is the same as a case where the MH has a session with one CH. Thus, the mobility related signalling overheads of the DM-MHPP is not affected by the increasing number of CHs with which the MH has ongoing communication sessions. This is because the DM-MHPP updates only the PoA through which the active sessions are established and not the CHs. Furthermore, the DM-MHPP does not require a consultation with any third party on security aspects as it has capabilities of self certifying at the HIP layer. Moreover, DM-MHPP avoids all signals related to DAD and signal overheads on the HIP MH interface.

Table 7. Signalling overheads of HIP, PMIPv6, HIPPMIP, MHPP and DM-MHPP.

Parameters\Scheme	HIP	PMIPv6	HIPPMIP	MHPP	DM-MHPP
# of UPDATE packets per IP handover when MH has ongoing communications with 1 CH.	6	6	6	2	2 (for Home_to_visted handover only)
Are there any signalling overheads on MH's interface?	Yes	No	No	No	No
Are there any signalling overheads due to configuration of new IP address?	Yes	No	No	No	No
Are there any signalling overheads due to contact with centralised mobility entity?	Yes	Yes	Yes	Yes	No

7.1.4 Impact of MH speed on DM-MHPP Handover Performance

The impact of the different MH speeds on the handover delay for the DM-MHP when the MH moves away from the PoA of the active sessions is the same as for the MHPP, depicted in Figure 5-20. However, the impact of the MH speeds on the handover delay for the DM-MHPP when the MH moves to the PoA of the active sessions is negligible. This is because when the MH is detected at the PoA of the active sessions it just stops forwarding the traffic of the MH via another PoA. In other words, when the MH moves to the PoA of the active sessions, the DM-MHPP is less affected by the MH speeds compared to the handover performance of the MHPP and also the case where the MH moves away from the PoA of the active sessions.

7.1.5 Impact of DM-MHPP's Handover Performance due to Security Delay Component with a Third Party

Figure 7-9 illustrates the relationship between the delay owing to the security process with a third party, for example an AAA server, and the handover delay of the DM-MHPP and MHPP. Every point on the graph represents an average of the MH handovers, layer-2 and layer-3 handovers, measured while the MH was moving with a speed of 1mps. Like the MHPP, the DM-MHPP is not affected by a third party security delay since the security checks are not performed at the third party and thus avoids additional delay.

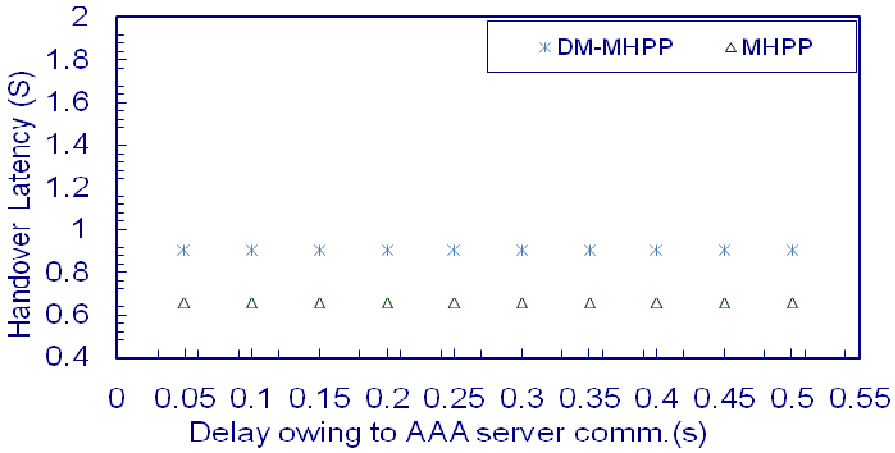


Figure 7-9 Impact of AAA server delay on HO delay of the DM-MHPP and MHPP

7.1.6 Impact of Number of CHs on DM-MHPP's Handover Performance

Table 8 below portrays the results of the impact of the number of CHs, with which the MH is connected during the handover, and an average packet loss and handover delay for the HIP, PMIPv6, HIPPMIP, MHPP and DM-MHPP.

Table 8. Signalling overheads for one MH with more than one CH using HIP, PMIPv6, HIPPMIP, MHP and DM-MHPP

Parameters\Scheme	HIP	PMIPv6	HIPPMIP	MHPP	DM-MHPP
# of UPDATE packets per IP handover when MH has ongoing communications	9	6	6	2	2

with 2 CH.					
# of UPDATE packets per IP handover when MH has ongoing communications with *n* CH.	3*(*n* + 1)	6	6	2	2

From the above table it is evident that PMIPv6 and HIPPMIP perform better than HIP. In the HIP, at a certain number of CHs, in this case more than eight, the handover performance begins to be affected inefficiently. This is because, in HIP, the MH exchanges many mobility-related signalling messages at the same time and therefore the network and mobility agents become saturated. In addition, the increase in handover-related messages owing to the number of CHs, with which the MH is connected, increases the delay in the queue of shared links. In fact, the queuing delay in these links starts to increase as the number of handover-related signalling increases and thus causes congestion. However, even under these congested conditions the CHs and MHs continue to exchange the data packets of active sessions. These congested links can cause packet loss since handover takes a longer time to complete or sometimes even fails. This phenomenon is worse in the case of the HIP since it is a host-based mobility protocol. In addition, most of the handover signalling has to be sent over wireless links between the MHs and the mobility entities in the network.

7.1.7 Impact of Number of MHs on DM-MHPP's Handover Performance

This section briefly discusses the impact of the number of MHs on the handover performance of the DM-MHPP. Like the HIPPMIP and MHPP, this evaluation is performed based on the model presented in Figure 7-10. This figure depicts scenarios under which the DM-MHPP is investigated; the scenarios are divided into two groups. The first group contains more than one MH communicating with one CH as illustrated in Figure 7-10(a). The second group contains more than one MH communicating with more than one CH as portrayed in Figure 7-10(b). In these two scenarios, the effect of the increasing number of MHs and/or increasing

number of CHs on handover delay and signalling overhead are studied. In addition, the researcher investigated the DM-MHPP and presented a comparison with other mobility protocols at the end of the chapter. In particular, handover delay components such as location update delays and security delays are identified and how they are affected by the number of MHs and/or CHs are investigated. The analysis of the DM-MHPP in the scenarios, Figures 10(a) and 10(b) is presented below.

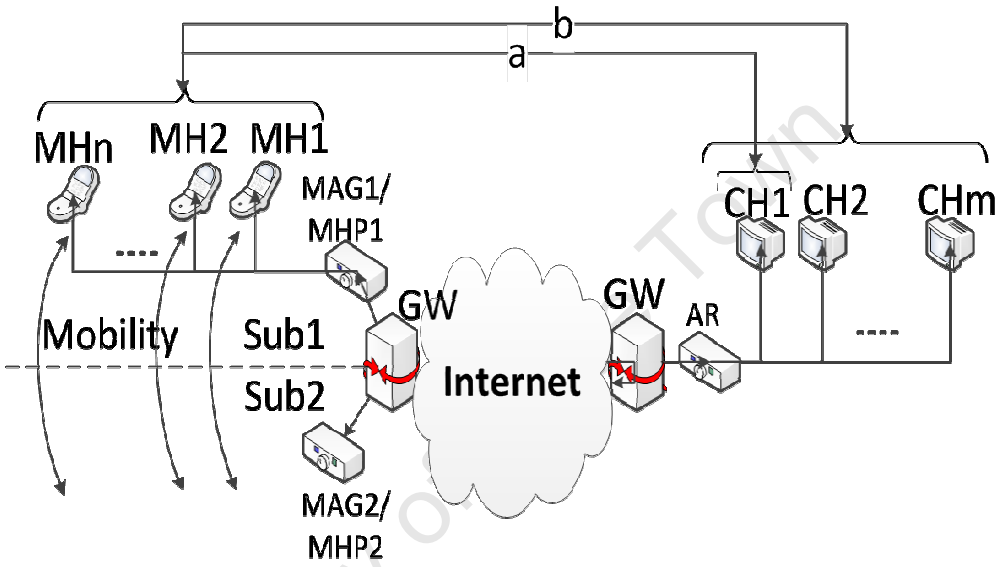


Figure 7-10 Scenarios under which mobility protocols are invistigaated

Figure 7-11 illustrates the signalling and data flow of the DM-MHPP for *n* MHs and 1 CH. Security delay components are eliminated from the figure because of the HIP capabilities. Thus, the handover delay and signalling overhead are improved. Furthermore, unlike PMIPv6 and PMIPv6-based solutions such as HIPMIP, it is evident that the number of MHs that are moving at the same time towards the same PoA, MHP2, neither affects the handover delay nor the signalling overhead. This is because the MH identifiers and HITs, are aggregated by MHP2 into one UPDATE packet, UPDATE packet1, and sends it to the PoA of the active sessions. Similarly, the PoA of the active sessions aggregates the HITs of authenticated, authorised and successfully accepted MHs into one UPDATE packet, UPDATE packet2 and sends it back to the MHP2. This aggregation allows MHs to save significant amounts of signals as well as to avoid delays due to the sending and processing of handover-related messages simultaneously.

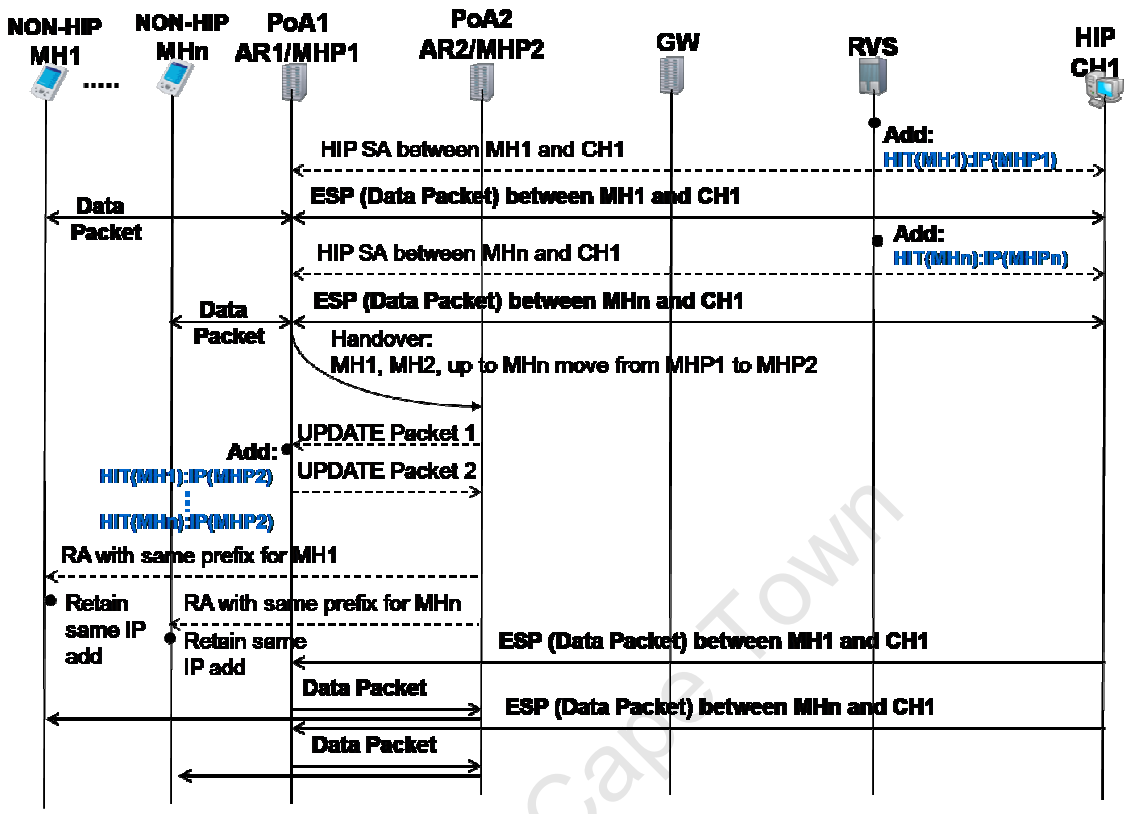


Figure 7-11 DM-MHPP for HO of *n* MHs during *n* sessions with 1 CH

Furthermore, a case whereby the DM-MHPP is used to manage *n* MHs to communicate with *m* CHs are also investigated and exhibited in Figure 7-12. It is evident from this figure that neither an increase in the number of MHs nor CHs affect the handover performance of the DM-MHPP. This is because the IP handover information for MHs that perform handover at the same time will be sent in only two UPDATE packets, thus avoiding sending separate UPDATE packets per MH.

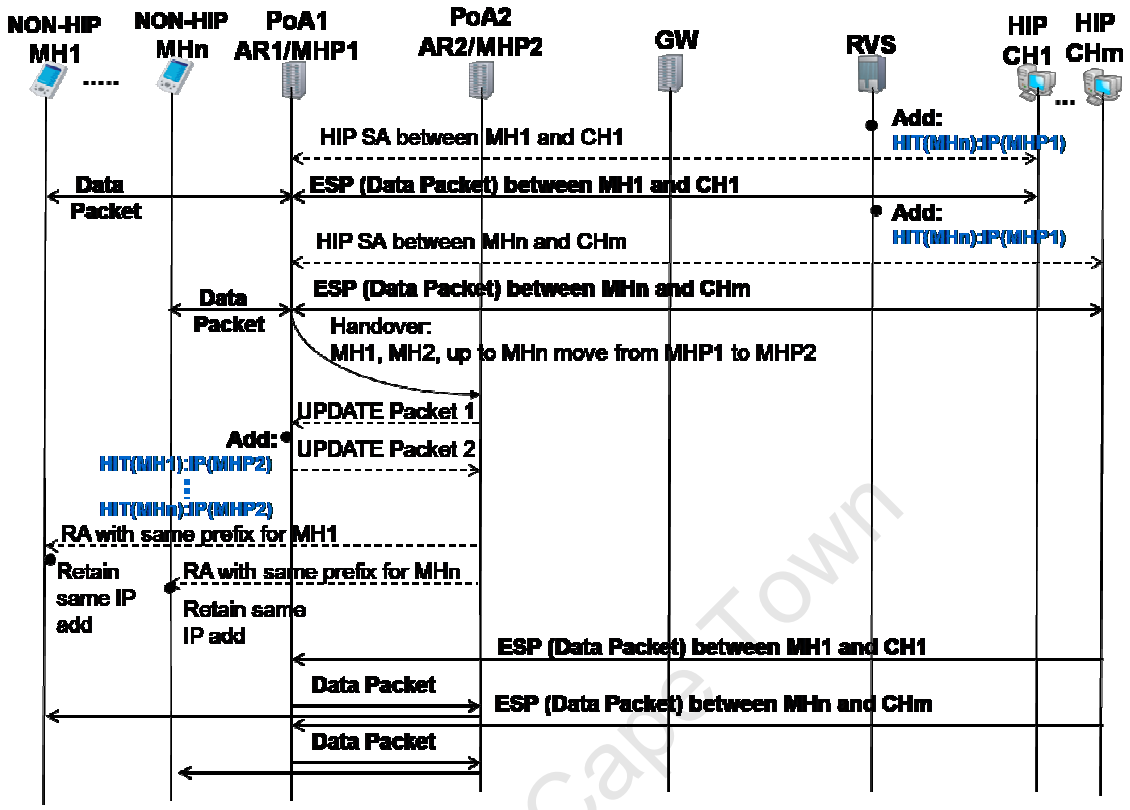


Figure 7-12 DM-DMPP for HO of *n* MHs during *n* sessions with *m* CHs

7.2 Evaluation of SL-DM

Like the HIPPMIP, MHPP and DM-MHPP the OMNet++ 4.0 network simulator [99] and the HIPSim++ simulation framework [100] are utilised to implement the Signal-Less Distributed Mobility (SL-DM) design. The handover of the SL-DM is carried out in two partially overlapping IEEE 802.11b (11 Mbps peak data rate) subnetworks. These subnetworks implement intelligent mobility access gateways (iMAGs) for the network-based implementation of the SL-DM. In the SL-DM the iMAGs are co-located with the access routers. That is, mobility in subnetwork 1 and 2 is managed by iMAG1 and iMAG2, respectively, for SL-DM. The simulated topology is typical to what is explained in Figure 7-13 and the simulation parameters are the same as those described in Table 1.

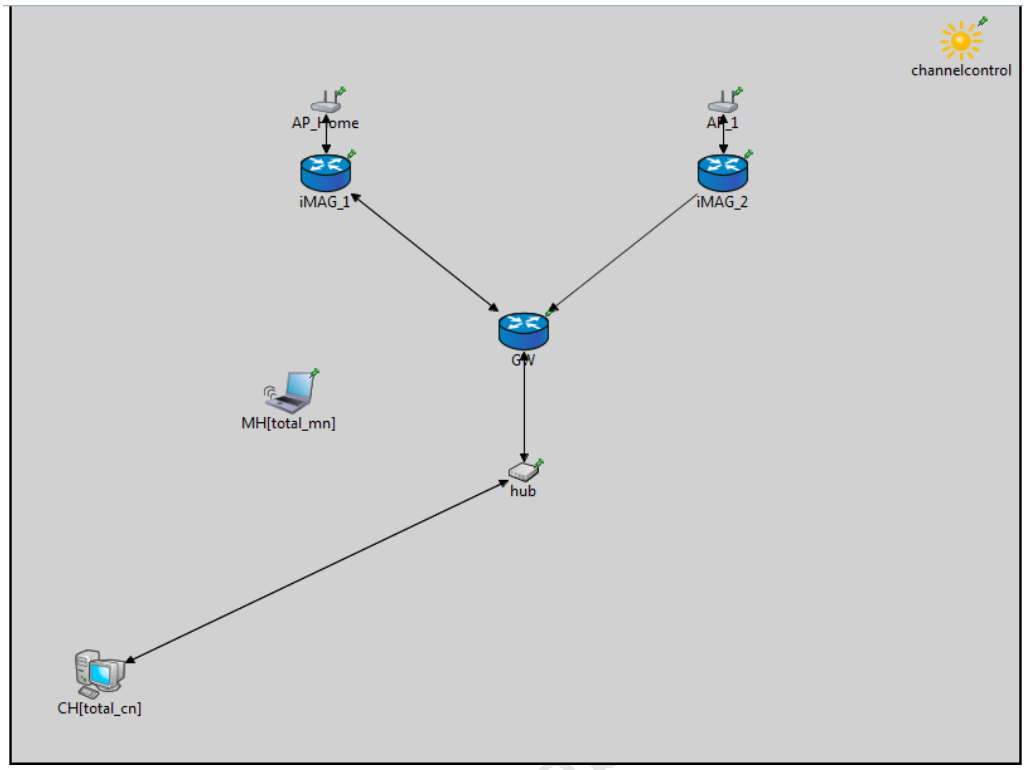


Figure 7-13 Simulation network topology of SL-DM

7.2.1 Architecture of SL-DM's Main Mobility Functions in OMNeT++

In this section, the researcher describes the node structure in the OMNeT++ for the SL-DM's main mobility entities. The module libraries of the INET and HIPSim++ are utilised and extended to develop the SL-DM model. To implement the iMAG functions in OMNeT++, he added mobility functions at the MAG module into the INET++'s MAGHost6 module that he developed for the PMIPv6 implementation. Figure 7-14 illustrates the internal structure of the iMAG in the OMNeT++. The iMAGs have also been modified to operate with the HIP RVS and/or distributed hash table (DHT) servers.

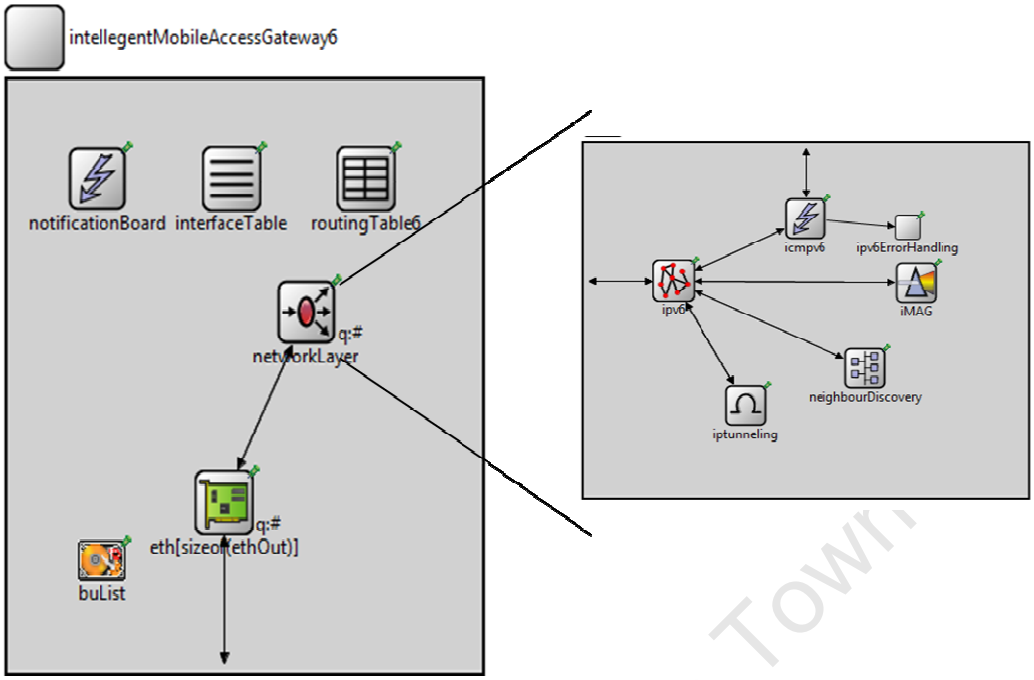


Figure 7-14 iMAG structure in the OMNeT++

7.2.2 Simulation Scenario

Similar to the scenario in which the HIPPMIP, MHPP and DM-MHPP are evaluated, in the handover performance evaluation and analysis of the SL-DM, the researcher considered a scenario whereby a CH is fixed outside the network domain of the MH. The CH and the MH exchange 256-byte UDP packets at a rate of 15 kbps. Again, for the sake of simplicity, he only considered a unidirectional data flow from the CH to the MH. The handover is simulated with the MH moving linearly at a constant speed of 1 m/s from one subnet to the other.

7.2.3 Performance Evaluation and Analysis of SL-DM

To evaluate the handover performance of the SL-DM, the researcher extended his PMIPv6 simulation model to incorporate a mechanism that allows the MH to perform an IP handover and to use the same IP address in different subnetworks in the flat architecture. Like the HPPMIP, MHPP and DM-MHPP, to investigate the handover performance for the SL-DM, he used the same meaning of the evaluated parameters that had been defined in (5.2). It is important to note that the SL-DM can be implanted either in a host-based or a network-based manner.

However, the network-based implementation is examined while the host-based is considered as future research.

7.2.3.1 Handover delay

Using the above mentioned simulation environment described in Section 7.2, the researcher examined the network-based implementation of the SL-DM. In addition, he recoded and extensively analysed a hundred handoffs for each of the three models (DM-MHPP, MHPP and SL-DM). The fluctuation in the handover delay of the model over the first 23 handover (HO) instances is depicted in Figure 7-15.

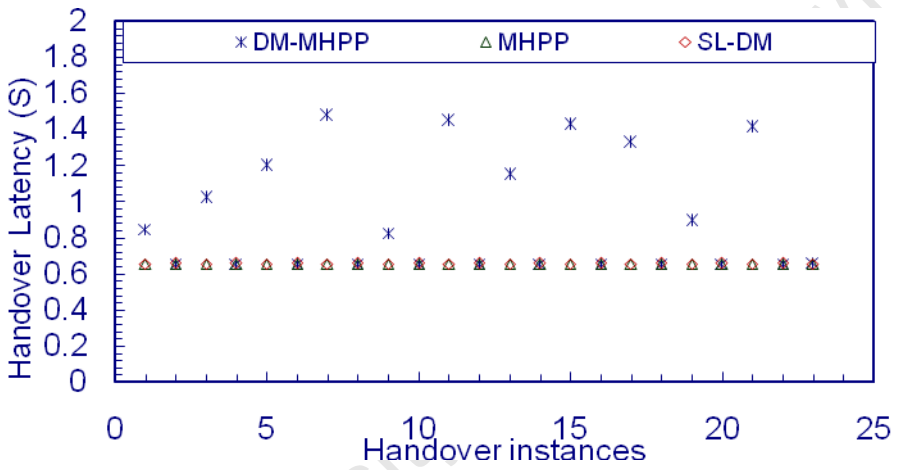


Figure 7-15 The first 23 handovers for DM-MHPP, MHPP and SL-DM

It can also be observed that there was a significant decrease in the handover delay in the SL-DM. It achieved a small handover delay that is close to a layer-2 handover delay. It is important to note that in this implementation the CH is informed about the MH's new location using data packets instead of handover-related control packets. Although the CH is informed instead of the central mobility entity like in the MHPP, the handover delays of the MHPP and SL-DM are close to each other. These results indicate that the SL-DM has achieved a good handover performance without considering any central entity for host mobility support. Furthermore, the SL-DM has a stable handover delay since it has avoided a DAD delay, which is variable, a delay of both the authentication and authorisation as well as some other delays related to the location update. The SL-DM has also achieved another advantage, which is the reduction

of the LU delay. This is because in the MHPP and DM-MHPP, explicit LU messages are exchanged. In this case these LU messages need to be authenticated and acknowledged. However, in the SL-DM these LU messages are eliminated and thus the necessary information for the MH's new location is included inside the data packets. Having an option for new location information carried in authenticated packets eliminates the need for authentication of the handover-related packets and reduces the time of a location update. Therefore, the handover performance of the SL-DM in terms of delay and signalling is optimised.

7.2.3.2 Packet loss

Figure 7-16 depicts the packet loss of the SL-DM compared with the HIP and DM-MHPP. The researcher measured the packet loss from the traffic, data packets of the UDP application, moving between the CH and MH during handover delay. The inter-arrival rate of the data packets remained constant in all the cases. From the packet loss measurements of the SL-DM, he observed that the amount of packet loss is also proportional to the handover delay. Compared with the HIP and DM-MHPP, the SL-DM achieved a good handover delay and thus the smallest amount of packet loss.

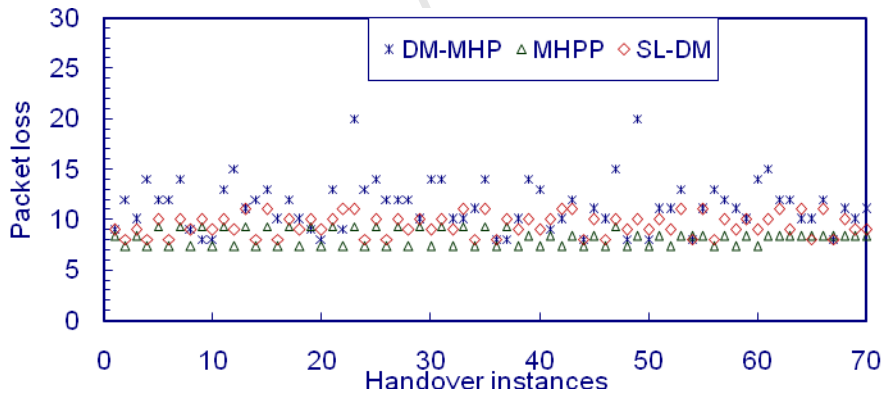


Figure 7-16 The averaged packet loss of the DM-MHPP, MHPP and SL-DM

7.2.3.3 Signalling overhead

Table 9 shows the number of signals used for the IP handover in the MHPP and SL-DM during the entire simulation time. From the figure, it can be noted that the SL-DM does not exchange any handover-related control packets and thus significantly outperformed both the HIP

and the DM-MHP in terms of handover-related messages. This is because the SL-DM inserts the necessary information for the IP handover inside data packets. MHPP for intra- and inter-domain handover use explicit handover-related control packets/messages. Unlike the MHPP, the SL-DM avoids all the signals related to the IP handover such as signals for location updates and signal overheads related to the MH interface. The SL-DM for the IP handover in flat network architecture needs a zero message to redirect the active session to the new location of the MH. It is important to note that this happens irrespective of the number of CHs to which an MH has active sessions. Signalling overheads of the SL-DM compared with signalling overheads of the MHPP for intra- and inter-domain handover are shown in the table.

Table 9. Signalling Overheads of Mobility-Enabled SL-DM as well as MHPP for Intra-Domain and Inter-Domain Handover

	MHPP(Intra)	**MHPP(Inter)**	**SL-DM**
# of UPDATE packets per handover when communicating with 2 CHs?	2	6	0
# of UPDATE packets per handover when communicating with n CHs?	2	6	0
Signalling overheads on MH's interface?	No	No	No
Signalling overheads due to configuration of new IP address?	No	No	No
Signalling overheads for consulting 3rd party for security?	No	No	No

7.2.4 Impact on SL-DM's Handover performance Due to Security Delay Component with a Third Party

Figure 7-17 illustrates the relationship in the increase of the delay owing to the security process with a third party, for example an AAA server, and the handover delay of the MHPP, DM-MHPP and SL-DM. Each point of the handover delay in the graph represents an average of the MH handovers measured while the MH was moving with a speed of 1mps. It is important to note that these measurements are taken for the MHPP, DM-MHPP and SL-DM. Neither the DM-MHPP and MHPP nor the SL-DM are affected by security delays at a third party since the DM-MHPP uses HIP capabilities and the SL-DM uses already secured communication for the exchange of information for IP handover purposes.

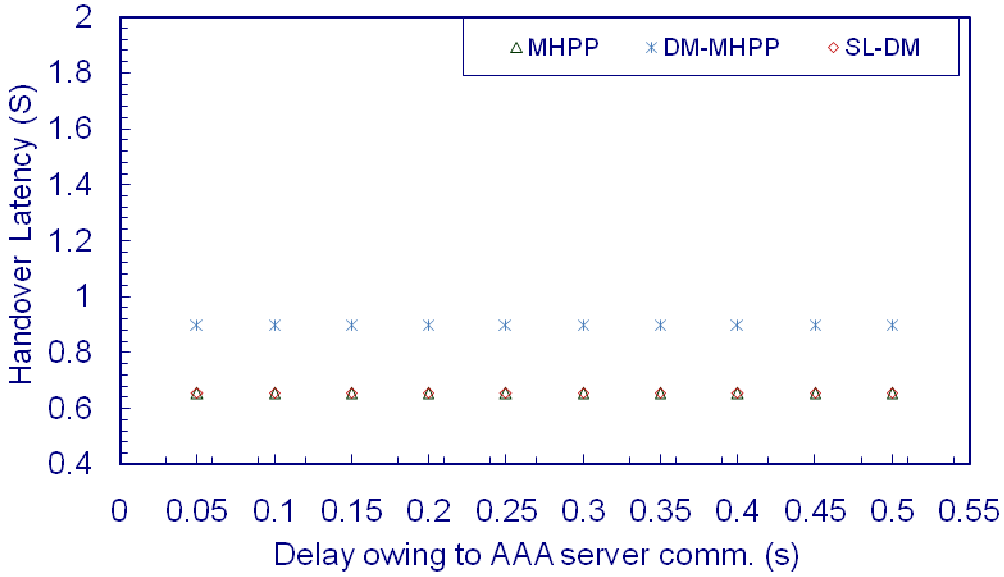


Figure 7-17 Impact of AAA delay on HOD of the MHPP, DM-MHPP and SL-DM

7.2.5 Impact of Number of MHs on SL-DM's Handover Performance

This section evaluates the handover performance of the SL-DM. The researcher developed an analytic model based on the scenarios explained in Figure 7-10. The main purpose is to measure the handover performance of the SL-DM where many MHs are communicating with a different number of CHs. Note that CH1 and CH2 can be in the same or in different

domains. Another issue to be considered is that it is immaterial which one of the CHs will be the first to inform. Again, the receipt of the UPDATE packets depends on the distance between the MH and the respective CH. The sequence of the data packets where *n* MHs communicate with one CH is depicted in Figure 7-18 while the sequence where *n* MHs communicate with *m* CHs is portrayed in Figure 7-19.

In the evaluation of the handover performance of the SL-DM, the researcher assumed that the HIP MH registered at the RVS/DHT with a binding contains the MH identifier and IP addresses present in the domain to which the MH is connected. As demonstrated in Figure 7-18, *n* MHs have ongoing communications with one CH1 and the MHs moved at the same time to the same PoA. It is evident that the increase in the number of the MH does not affect the handover delay and signalling overhead since the SL-DM includes the handover-related information inside the data packets. Ultimately, the use of data traffic for the exchange of IP handover information enables the SL-DM to serve many MHs even if they move at the same time.

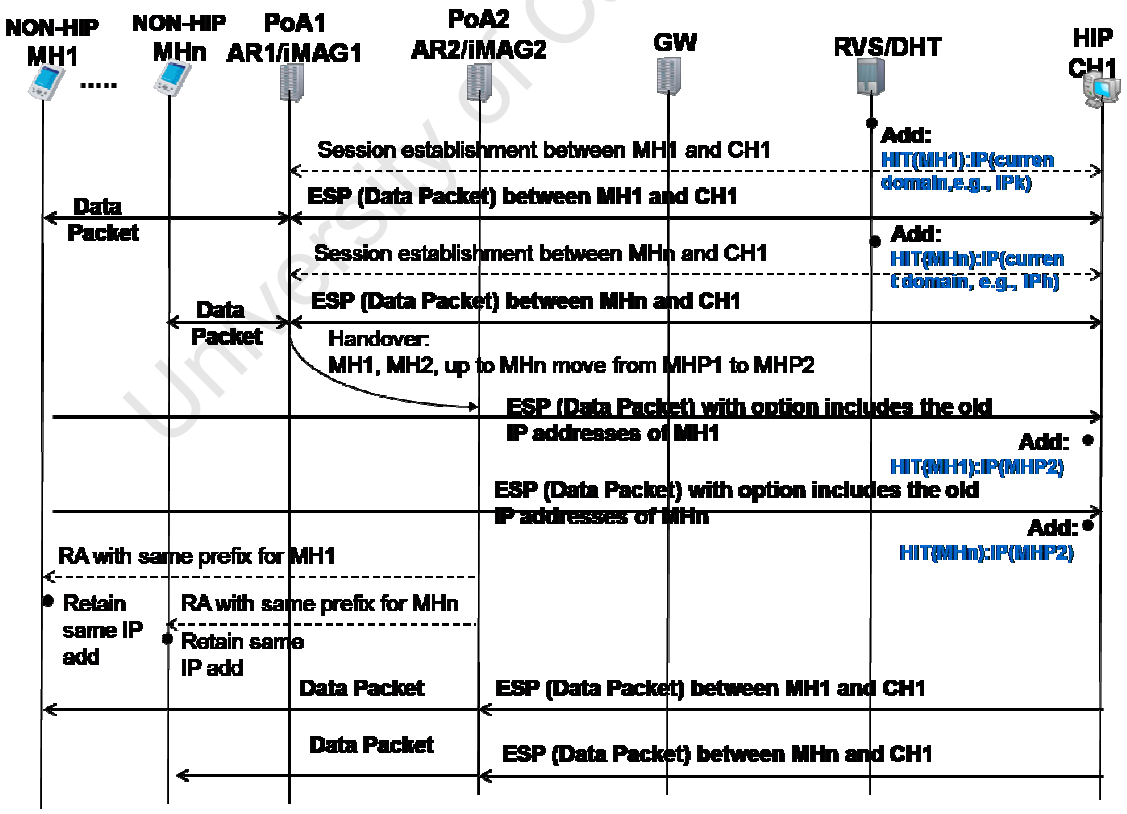


Figure 7-18 SL-DM for HO of *n* MHs at the same time during *n* sessions with 1 CH

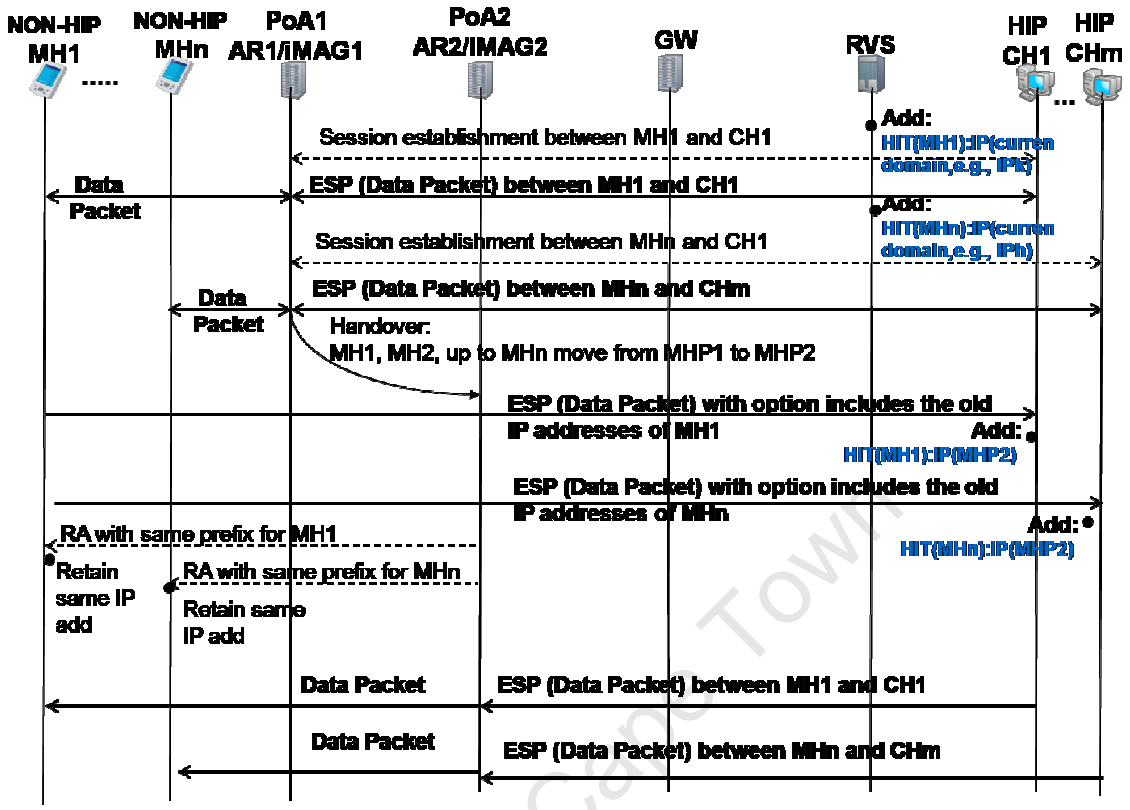


Figure 7-19 SL-DM for HO of *n* MHs at the same time during *n* sessions with *m* CHs

Furthermore, a case whereby the SL-DM is used to manage *n* MHs communicate with *m* CHs are also investigated. It is evident from the figure that neither the increase in the number of MHs nor CHs affect the handover performance of the SL-DM. This is because the IP handover information for each MH will be sent in the traffic between the respective MH and CH. For example, in the IP handover of MH1, MH1's handover information is included inside the data traffic between MH1 and CH1, that is, the host to which MH1 has an active session with during the handover.

In this chapter the researcher has evaluated two of his proposed mobility designs/solutions, that are, the DM-MHPP and SL-DM. These mobility solutions are also evaluated by the OMNeT++ network simulator presented in Section 5.1. He also presented and analysed the results obtained from the proposed mobility solutions, The DM-MHPP and SL-DM are discussed in Sections 6.1 and 6.2, respectively. The handover performance of DM-MHPP is evaluated and compared against its related work. The performance of SL-DM is also evaluated

and compared against its related work. A discussion of the DM-MHPP's handover performance results and analysis is furnished in Section 7.1, while the SL-DM's handover performance results and analysis are discussed in Section 7.2.

Chapter 8 Conclusions and Recommendations

In this thesis, the researcher introduced two designs: a novel coordinated hybrid of PMIPv6 and HIP and a network-based mobility management function integrated with a HIP proxy function at the access routers to support all IP hosts, to optimise the handover performance in heterogeneous wireless networks in terms of providing efficient, secure and negligible handover delay architecture.

Many mobility management solutions have been introduced to support IP handover between heterogeneous wireless networks. However, these mobility solutions in their current form cannot provide a seamless handover in a secure and scalable manner. Various extensions, host-based and network-based, toward a seamless handover have been introduced in the literature to further enhance different handover-related aspects such as delay, packet loss, security and scalability. However, tolerant delay and packet loss handover mechanisms while ensuring security and scalability are urgently needed.

A network-based handover design for a seamless handover between heterogeneous wireless networks in hierarchical and flat architectures has been proposed in this thesis to further improve the IP handover performance. The designs employ HIP technology and different initiation mechanisms for the handover between homogenous and heterogeneous wireless networks. Therefore, many time consuming handover components such as security processes are eliminated while the MH transparently and securely preserves its active sessions. Ultimately, the signalling delay for security aspects during the actual handover are eliminated, thereby reducing the handover delay and packet loss. In addition, the network-based nature of the mechanisms ensures many advantages such as removing the handover-related signalling in the air interface.

The contributions of this thesis are summarised in Section 8.1, while the directions for future research are presented in Section 8.2.

8.1 Summary of the Contributions (HIPPMIP+ MHPP + DM-MHPP + SL-MD)

In this thesis, the researcher proposes four designs for host mobility support in the Future Mobile Internet. Each of the four introduced mobility designs employ different technologies to achieve a seamless vertical handover and thus reduce handover delay and packet loss while ensuring minimal signalling overhead in a secure and scalable manner. To achieve such a handover performance, the network-based mobility style is leveraged by the researcher's proposed mobility designs.

A network-based mobility management solution that integrates the HIP and PMIPv6, known as HIPPMIPv6, is introduced to optimise IP of the MH handover performance in terms of handover delay, packet loss and signalling overhead. This mobility solution provides a framework that supports a seamless vertical intra-domain handover in a secure manner. The HIPPMIP utilises the benefits of these two protocols to achieve its goal. An architectural framework of the scheme has been presented and discussed in order to demonstrate that it does indeed result in a secure handover with a small handover delay in a localised domain. The performance evaluation of the HIPPMIP in comparison to PMIPv6 and HIP in terms of handover delay performance, is shown to perform better, yet maintaining a signalling overhead and delay due to a third party consultation; this requires further optimisation.

Furthermore, existing mobility management and ID-locator split schemes have the following limitations: (1) Existing mobility management with HIP requires hosts to have HIP capabilities and also incur long handover delays; (2) HIP Proxy proposals provide HIP to all IP-based hosts but the existing mobility management solutions for HIP incur long handover delays; (3) Existing Proxy Mobile IP (PMIP), Mobile IP (MIP) and each mobility solution that leverages PMIP and/or MIP lack native security support.

To address these issues, the researcher co-located a network-based mobility management function and a proxy HIP function at the access router so that no new physical network elements are needed. These logical functions securely and efficiently manage the handover of the MH in

homogenous or heterogeneous networks. This solution inherits advantages of both the network-based approach and HIP technology. The Mobility-enabled HIP proxy acts as a HIP proxy for non HIP enabled hosts and offers network-based mobility support for both non HIP-enabled and HIP-enabled MHs. The simulation results show that the Mobility-enabled HIP proxy handover performance in terms of handover latency, packets lost and signalling overhead is much better compared to HIP, Micro-HIP and PMIPv6. In addition, the results show that the Mobility-enabled HIP proxy achieves smaller handover latency than PMIPv6 because the functional entities (i.e., LMA and MAG) of PMIPv6 need to communicate with a third party (i.e., AAA server) to authenticate the MH in question while the Mobility-enabled HIP proxy function identifies the MH itself by using HIP technology. Moreover, the Mobility-enabled HIP proxy solution supports intra- and inter-domain HO, whereas basic PMIPv6 does not support inter-domain HO.

The MHPP, which is an enhanced mobility design discovered from the HIPPMIP, has offered an elegant mobility architecture that can be deployed in hierarchical network architecture. To optimise the scalability of the MHPP, a distributed mobility extension for the MHPP is introduced, known as DM-MHPP. This is to prevent performance bottlenecks, for example, in situations where the number of MHs simultaneously performing handover is large. However, this DM-MHPP must still maintain the level of handover performance of the MHP which include the exchange of handover-related signalling without increasing handover delay, packet loss and the signals themselves.

To achieve this, the MHPP, which is a network-based mobility management solution, is extended to employ the distributed mobility approach and called DM-MHPP. In, DM-MHP, distributed entities that provide both mobility management and HIP features by the network to all IP hosts are introduced to optimise the MH IP handover performance in the flat network architecture. This distribute mobility solution provides a framework, for the flat network architecture, that supports a seamless vertical handover in a secure manner. The DM-MHPP utilises the benefits of the MHP protocol to achieve its goal. The performance evaluation of the DM-MHPP in comparison to similar mobility solutions demonstrates that it does indeed perform better.

Another distributed mobility design, the SL-DM, is introduced, enabling host mobility in flat network architecture and addressing handover delay, scalability, single point of failure, packet loss and signalling overhead. This distributed mobility design has different handover performances and characteristics compared to DM-MHP. In the SL-DM, distributed mobility design that ensures efficient routing between the communication parties, MH and CH, by its dynamic traffic anchoring mechanism is introduced. Another advantage that SL-DM adds is that the SL-DM can be employed at TCP/IP layer or HIP layer; SL-DM is a protocol stack-independent mobility design.

Two attachment detection mechanisms, one utilising the NDP while the other does not, are introduced to further improve handover performance. Simulations experiments indicate that the detection mechanism that does not use the NDP has shorter handover delays and smaller packet losses than the one that uses the NDP. In the latter, the MHs successfully send their cryptographic identifier, from their HIP layer or given by the HIP proxy for non-HIP MH, to the mobility entity. Consequently, a secure movement between different networks can be ensured.

Qualitative and quantitative investigations for HIP and some widely referenced HIP-based micro-mobility solutions as well as the researcher's Mobility-enabled HIP Proxy (MHPP) are discussed. In addition, qualitative and quantitative investigations for PMIP and some widely referenced PMIP-based extensions as well as the researcher's DM-MHPP are also discussed. Furthermore, a MHPP-extension for inter-domain handover can be offered for all IP MHs. Moreover, an elegant reachability mechanism for flat network architecture is introduced and investigated with SL-DM.

8.2 Future Work

Future work will involve an addition of mechanisms to each of the introduced mobility designs, HIPPMIP, MHPP, DM-MHPP and SL-DM that avail services, for example MIH services, making available information about network characteristics, neighbouring networks and associated characteristics as well as indications that a handover should take place, mainly for inter-domain handovers between different administrative domains.

In this thesis, the performance evaluation of the SL-DM, which is protocol stack-independent of the HIP stack is studied. Therefore, an investigation of the SL-DM on top of the TCP/IP stack is one of the important aspects that need further research. Furthermore, comparisons between HIP stack-based SL-DM and TCP/IP stack-based SL-DM also need further research. These distributed architectures will help to identify the optimal mobility designs that suit a certain environment for mobile network operators. Furthermore, they will provide alternative frameworks to face the increasing number of MHs that simultaneously perform a handover.

In addition, some aspects that need further research are the study of the mechanisms and alternatives that enable simultaneous support of different mobility solutions, the use of different ways for routing advertisement and the exchange of messages for different types of hosts such as HIP-enabled MHs and non-HIP-enabled MHs. All these aspects can be considered for each of the proposed mobility designs.

The addition of elegant and dynamic mechanisms to also consider are the required Quality of Experience (QoE) when MHs perform an IP handover without incurring additional handover delay, and signalling. Consideration of a QoE concerns the reservation of the required resource in the new wireless network so as to ensure the required quality for the active applications/services during the MH handover.

In this thesis, an elegant proposed reachability mechanism for flat network architecture is investigated when employed with SL-DM. Therefore, investigation of this proposed reachability mechanism with DM-MHPP and/or with other distributed mobility solutions need further research. This reachability mechanism will help to reduce the signalling cost to the MH location update and thus face challenges introduced by the increase of the number of MHs and expected increase of data traffic in the Future Mobile Internet. However, this reachability mechanism for the flat network architecture must be secure and maintain minimal signalling overload without affecting the handover performance of the MHs.

References

[1] J. F. Kurose and K. W. Ross, " Computer Networking: A Top-Down Approach," 5th Edition, Addison-Wesley, 2009.

[2] R. Ramjee, J. Kurose, D. Towsley and H. Schulzrinne, "Adaptive playout mechanisms for packetized audio applications in wide-area networks," in INFOCOM '94. Networking for Global Communications., 13th Proceedings IEEE, 1994, pp. 680-688 vol.2.

[3] L. Gautier, C. Diot and J. Kurose, "End-to-end transmission control mechanisms for multiparty interactive applications on the internet," in INFOCOM '99. Eighteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE, 1999, pp. 1470-1479 vol.3.

[4] International Telecommunication Union –Telecommunication Standardization Section Recommendation G.114, "One-way Transmission Time," vol. 2011, 2003/May, 2003. HTTP://

[5] R. Steinmetz, "Human perception of jitter and media synchronization," Selected Areas in Communications, IEEE Journal on, vol. 14, pp. 61-72, 1996.

[6] P. Tran-Gia, T. Hoßfeld, M. Menth and R. Pries, "Emerging issues in current Future Internet design," E & i Elektrotechnik Und Informationstechnik, vol. 126, pp. 241-249, 2009.

[7] F. M. Chiussi, D. A. Khotimsky and S. Krishnan, "Mobility management in third-generation all-IP networks," Communications Magazine, IEEE, vol. 40, pp. 124-135, 2002.

[8] I. F. Akyildiz, Jiang Xie and S. Mohanty, "A survey of mobility management in next-generation all-IP-based wireless systems," Wireless Communications, IEEE, vol. 11, pp. 16-28, 2004.

[9] H. A. Chan, "Problem statement for distributed and dynamic mobility management," Draft-Chan-Distributed-Mobility-Ps-02 (Work in Progress), March, 2011.

[10] D. Johnson, C. Perkins and J. Arkko, "Mobility support in IPv6," Rfc-3775, June2004.

[11] H. Soliman, L. Bellier and K. E. Malki, "Hierarchical mobile IPv6 mobility management (HMIPv6)," Rfc-4140, August 2005.

[12] R. Koodli, "Mobile IPv6 fast handovers," Rfc-5568, July 2009.

[13] A. Gurtov, "Host Identity Protocol (HIP): Towards the Secure Mobile Internet, " Wiley and Sons, 2008.

[14] S. Gundavelli, K. Chowdhury, V. Devarapalli, B. Patil and K. Leung, "Proxy mobile IPv6," Rfc-5213, August 2008.

[15] Ki-Sik Kong, Wonjun Lee, Youn-Hee Han, Myung-Ki Shin and HeungRyeol You, "Mobility management for all-IP mobile networks: mobile IPv6 vs. proxy mobile IPv6,"

Wireless Communications, IEEE, vol. 15, pp. 36-45, 2008.

[16] A. T. Campbell and J. Gomez-Castellanos, “IP micro-mobility protocols,” ACM SIGMOBILE Mobile Computing and Communications Review, vol. 4, pp. 45-53, 2000.

[17] Deguang Le, Xiaoming Fu and Dieter Hogrefe, “A review of mobility support paradigms for the internet,” Communications Surveys & Tutorials, IEEE, vol. 8, pp. 38-51, 2006.

[18] R. Moskowitz, P. Jokela, P. Nikander and T. Henderson, “Host identity protocol,” Rfc-5201, April 2008.

[19] P. Nikander, J. Arkko and T. Henderson, “End-host mobility and multihoming with the host identity protocol,” Rfc-5206, April 2008.

[20] P. Jokela, P. Nik, J. Melen, J. Ylitalo and J. Wall, “Host identity protocol: Achieving IPv4 - IPv6 handovers without tunneling,” in In Proc. of Evolute Workshop 2003: “Beyond 3G Evolution of Systems and Services, 2003 .

[21] A. Khurri, E. Vorobyeva and A. Gurtov, “Performance of host identity protocol on lightweight hardware,” in Proceedings of 2nd ACM/IEEE International Workshop on Mobility in the Evolving Internet Architecture, Kyoto, Japan, 2007, pp. 4:1-4:8.

[22] P. Jokela, T. Rinta-aho, T. Jokikyyny, J. Wall, M. Kuparinen, H. Mahkonen, J. Melen, T. Kauppinen and J. Korhonen, “Handover performance with HIP and MIPv6,” in Wireless Communication Systems, 2004, 1st International Symposium on, 2004, pp. 324-328.

[23] T. R. Henderson, J. M. Ahrenholz and J. H. Kim, “Experience with the host identity protocol for secure host mobility and multihoming,” in Wireless Communications and Networking Conference, 2003. WCNC 2003. 2003 IEEE, 2003, pp. 2120-2125 vol.3.

[24] A. Dutta, Ed., V. Fajardo, Y. Ohba, K. Taniuchi and H. Schulzrinne, “A framework of Media-Independent Pre-Authentication (MPA) for inter-domain handover optimization,” Rfc-6252, June 2011.

[25] J. Y. H. So and Jidong Wang, “Micro-HIP A HIP-based micro-mobility solution,” in Communications Workshops, 2008. ICC Workshops '08. IEEE International Conference on, 2008, pp. 430-435.

[26] A. R. Prasad, A. Zugenmaier and P. Schoo, “Next generation communications and secure seamless handover,” in Security and Privacy for Emerging Areas in Communication Networks, 2005. Workshop of the 1st International Conference on, 2005, pp. 267-274.

[27] K. Pahlavan, P. Krishnamurthy, A. Hatami, M. Ylianttila, J. P. Makela, R. Pichna and J. Vallstron, “Handoff in hybrid mobile data networks,” Personal Communications, IEEE, vol. 7, pp. 34-47, 2000.

[28] T. C. Hung, L. Phuc, T. T. T. Uyen, H. W. Jung and Y. Kang, “Improving handover performance in mobile IPv6,” in Advanced Communication Technology, 2008. ICACT 2008. 10th International Conference on, 2008, pp. 1828-1831.

[29] N. Capela, J. Soares, P. Neves and S. Sargento, "An architecture for optimized inter-technology handovers: Experimental study," in Communications (ICC), 2011 IEEE International Conference on, 2011, pp. 1-6.

[30] S. Mohanty and I. F. Akyildiz, "A Cross-Layer (Layer 2 + 3) Handoff Management Protocol for Next-Generation Wireless Systems," Mobile Computing, IEEE Transactions on, vol. 5, pp. 1347-1360, 2006.

[31] L. A. Magagula, O. E. Falowo and H. A. Chan, "PMIPv6 and MIH-enhanced PMIPv6 for mobility management in heterogeneous wireless networks," in AFRICON, 2009. AFRICON '09. 2009, pp. 1-5.

[32] A. Altaf, F. Iqbal and M. Y. Javed, "S3H: A secure seamless and soft handover between WiMax and 3G networks," in Convergence and Hybrid Information Technology, 2008. ICHIT '08. International Conference on, 2008, pp. 530-534.

[33] A. A. Tabassam, H. Trsek, S. Heiss and J. Jasperneite, "Fast and seamless handover for secure mobile industrial applications with 802.11r," in Local Computer Networks, 2009. LCN 2009. IEEE 34th Conference on, 2009, pp. 750-757.

[34] S. Kim and J. A. Copeland, "TCP for seamless vertical handoff in hybrid mobile data networks," in Global Telecommunications Conference, 2003. GLOBECOM '03. IEEE, 2003, pp. 661-665 Vol.2.

[35] J. Kempf, "Problem statement for network-based localized mobility management (NETLMM)," Rfc-4830, April 2007.

[36] M. Zaid, "Personal mobility in PCS." Personal Communications, IEEE, vol. 1, pp. 12, 1994.

[37] H. Schulzrinne, F. Oertel, C. Zahl and G. F. Berlin, "Personal Mobility for Multimedia Services in the Internet," in European Workshop on Interactive Distributed Multimediu System and Services (IDMS), (Berlin, Germany), Mar. 1996.

[38] R. Sparks, "The session initiation protocol (SIP) refer method," Rfc-3515, April 2003.

[39] F. Cuervo, N. Greene, A. Rayhan, C. Huitema, B. Rosen and J. Segers, "Megaco protocol version 1.0," Rfc-3015, November 2000.

[40] J. Rosenberg, J. Peterson, H. Schulzrinne and G. Camarillo, "Best current practices for third party call control (3pcc) in the session initiation protocol (SIP)," Rfc-7325, April 2004.

[41] R. Shacham, H. Schulzrinne, S. Thakolsri and W. Kellerer, "Ubiquitous device personalization and use: The next generation of IP multimedia communications," ACM Transactions on Multimedia Computing, Communications, and Applications (TOMCCAP), vol. 3, pp. 12, 2007.

[42] G. Canfora, G. Di Santo, G. Venturi, E. Zimeo and M. Zito, "Proxy-based hand-off of web sessions for user mobility," in Mobile and Ubiquitous Systems: Networking and Services, 2005. MobiQuitous 2005. the Second Annual International Conference on, 2005, pp. 363-372.

[43] M. D. Hsieh, T. P. Wang, C. S. Tsai and C. C. Tseng, "Stateful session handoff for mobile WWW," Inf. Sci., vol. 176, pp. 1241-1265, 2006.

[44] H. Song, H. Chu and S. Kurakake, "Browser session preservation and migration," Poster Session of WWW, pp. 2, 2002.

[45] X. Wu and H. Schulzrinne, "Use SIP MESSAGE method for shared web browsing," Draft-wu-sipping-webshare-00, November 2001.

[46] P. Pacyna, "Advances in mobility management for the NG Internet," China Communications, vol. 3, pp. 76-90, 2006.

[47] R. Moskowitz, P. Jokela, P. Nikander and T. Henderson, "Host identity protocol," Rfc-6253, April 2008.

[48] P. Nikander and R. Moskowitz, "Host Identity Protocol (HIP) Architecture," Rfc-4423, May 2006.

[49] National science foundation future internet design initiative. [Online]., Available: Http://www.Nets-Find.Net/, visited on 12/02/2012.

[50] European future internet portal. [Online]., Available: Http://www.Futureinternet.Eu/, visited on 12/02/2012.

[51] Asia future internet forum. [Online]., Available: Http://www.Asiafi.Net/,12/02/2012 .

[52] S. Yankov and S. Wiethoelter, "Handover blackout duration of layer 3 mobility management schemes," Technical Report TKN-06-002,Telecommunication Networks Group, Technische Universität Berlin, May 2006.

[53] J. Ylitalo, J. Melén, P. Nikander and V. Torvinen, "Re-thinking security in IP based micro-mobility," Information Security, pp. 318-329, 2004.

[54] J. Y. H. So and J. Wang, "HIP based mobility management for UMTS/WLAN integrated networks," in Australian Telecommunication Networks and Applications Conference, 2006 .

[55] S. Novaczki, L. Bokor and S. Imre, "Micromobility support in HIP: Survey and extension of host identity protocol," in Electrotechnical Conference, 2006. MELECON 2006. IEEE Mediterranean, 2006, pp. 651-654.

[56] P. Jokela, J. Melen and J. Ylitalo, "HIP Service Discovery," InternetDraft, draft-jokela-hip-service-discovery-00, Work in Progress, June 2006.

[57] P. Nikander and J. Laganier, "Host identity protocol (HIP) domain name system (DNS) extensions," Rfc-5205, April 2008.

[58] A. Leonardo and H. Chaouchi, "Host identity protocol proactive mobility management experimentation," in Telecommunications (AICT), 2010 Sixth Advanced International Conference on, 2010, pp. 462-467.

[59] Z. Gurkas Aydin, T. Ali-Yahiya, H. Chaouchi and H. Zaim, "QoS mobility-aware algorithm using early update for host identity protocol," in Personal Indoor and Mobile Radio Communications (PIMRC), 2010 IEEE 21st International Symposium on, 2010, pp. 2014-2018.

[60] Yinghui Qiu, "HIP based mobility management for heterogeneous networks," in Wireless Communications, Networking and Mobile Computing (WiCOM), 2011 7th International Conference on, 2011, pp. 1-4.

[61] G. Iapichino and C. Bonnet, "Host identity protocol and proxy mobile IPv6: A secure global and localized mobility management scheme for multihomed mobile nodes," in Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE, 2009, pp. 1-6.

[62] S. Cespedes U. and Xuemin Shen, "An efficient hybrid HIP-PMIPv6 scheme for seamless internet access in urban vehicular scenarios," in GLOBECOM 2010, 2010 IEEE Global Telecommunications Conference, 2010, pp. 1-5.

[63] Bo Hu, Tao Yuan, Zhangfeng Hu and Shanzhi Chen, "L-HIP: A localized mobility management extension for host identity protocol," in Wireless Communications Networking and Mobile Computing (WiCOM), 2010 6th International Conference on, 2010, pp. 1-4.

[64] L. A. Magagula and H. A. Chan, "IEEE802.21 optimized handover delay for proxy mobile IPV6," in Military Communications Conference, 2008. MILCOM 2008. IEEE, 2008, pp. 1-7.

[65] L. A. Magagula and H. A. Chan, "Early discovery and pre-authentication in proxy MIPv6 for reducing handover delay," in Broadband Communications, Information Technology & Biomedical Applications, 2008 Third International Conference on, 2008, pp. 280-285.

[66] J. Seil, K. Namhi and K. Younghan, "Enhanced Predictive Handover for Fast Proxy Mobile IPv6," IEICE Trans. Commun., vol. 92, pp. 3504-3507, 2009.

[67] K. TANIUCHI, A. DUTTA, V. FAJARDO and Y. OBA, " Media Independent Pre-authentication supporting fast-handoff in PMIPv6," Draft-Taniuchi-Netlmm-Mpa-proxymipv6-00, February 2007.

[68] I. Kim, Y. Jung and Y. T. Kim, "Low Latency Proactive Handover Scheme for Proxy MIPv6 with MIH," 11th Asia-Pacific Symposium on Network Operations and Management (APNOMS 008), pp. 344-353, October2008..

[69] Ji-In Kim, Seok-Joo Koh and Nam-Seok Ko, "B-PMIPv6: PMIPv6 with bicasting for soft handover," in Advanced Communication Technology, 2009. ICACT 2009. 11th International Conference on, 2009, pp. 218-221.

[70] Soochang Park, Euisin Lee, Fucai Yu, Sungkee Noh and Sang-Ha Kim, "Inter-domain roaming mechanism transparent to IPv6-node among PMIPv6 networks," in Vehicular Technology Conference (VTC 2010-Spring), 2010 IEEE 71st, 2010, pp. 1-5.

[71] G. Giaretta, "Interactions between PMIPv6 and MIPv6: scenarios and related issues " Draft-Ietf-Netlmm-Mip-Interactions-07, October 2010.

[72] Zhikui Chen and Xiaodi Huang, "Dynamic fast authentication and authorization during inter-domain mobility," in Wireless Communications, Networking and Mobile Computing, 2008. WiCOM '08. 4th International Conference on, 2008, pp. 1-4.

[73] J. Loughney, M. Nakhjiri, C. Perkins and R. Koodli, "Context transfer protocol (CXTP)," Rfc-4067, July 2005.

[74] Jung-Woo Baik, Ju-Hyun Kim, June Sup Lee and Kyung-Geun Lee, "Inter-domain mobility support scheme using multicast in proxy mobile IPv6," in Consumer Communications and Networking Conference, 2009. CCNC 2009. 6th IEEE, 2009, pp. 1-2.

[75] A. Diab, A. Mitschele-Thiel and R. Boeringer, "A framework to support fast inter-domain mobility in all-IP networks," in Personal, Indoor and Mobile Radio Communications, 2006 IEEE 17th International Symposium on, 2006, pp. 1-5.

[76] R. Hsieh, Z. G. Zhou and A. Seneviratne, "S-MIP: A seamless handoff architecture for mobile IP," in INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies, 2003, pp. 1774-1784 vol.3.

[77] Z. G. Zhou, A. Seneviratne, R. Chan and P. Chumchu, "A software based indoor relative location management system," Procedings of Wireless and Optical Communications, 2002.

[78] S. Pack and Y. Choi, "Performance analysis of fast handover in mobile IPv6 networks," PersonalWireless Communications, pp. 679-691, 2003.

[79] R. Hsieh, A. Seneviratne, H. Soliman and K. El-Malki, "Performance analysis on hierarchical mobile IPv6 with fast-handoff over end-to-end TCP," in Global Telecommunications Conference, 2002. GLOBECOM'02. IEEE, 2002, pp. 2488-2492 vol. 3.

[80] N. Montavont and T. Noël, "Analysis and evaluation of mobile IPv6 handovers over wireless LAN," Mobile Networks and Applications, vol. 8, pp. 643-653, 2003.

[81] S. Haseeb and A. F. Ismail, "Handoff latency analysis of mobile IPv6 protocol variations," Comput. Commun., vol. 30, pp. 849-855, 2007.

[82] M. S. Kim, S. K. Lee, D. Cypher and N. Golmie, "Fast handover latency analysis in proxy mobile IPv6," in GLOBECOM 2010, 2010 IEEE Global Telecommunications Conference, 2010, pp. 1-5.

[83] K. S. Kong, W. Lee, Y. H. Han and M. K. Shin, "Handover latency analysis of a network-based localized mobility management protocol," in Communications, 2008. ICC'08. IEEE International Conference on, 2008, pp. 5838-5843.

[84] D. Chalmers and M. Sloman, "A survey of quality of service in mobile computing environments," Communications Surveys & Tutorials, IEEE, vol. 2, pp. 2-10, 1999.

[85] P. Bertin, Servane Bonjour and J. -. Bonnin, "A distributed dynamic mobility management scheme designed for flat IP architectures," in New Technologies, Mobility and Security, 2008. NTMS '08. 2008, pp. 1-5.

[86] P. Bertin, S. Bonjour and J. -. Bonnin, “An evaluation of dynamic mobility anchoring,” in Vehicular Technology Conference Fall (VTC 2009-Fall), 2009 IEEE 70th, 2009, pp. 1-5.

[87] P. Bertin, S. Bonjour and J. -. Bonnin, “Distributed or centralized mobility?” in Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE, 2009, pp. 1-6.

[88] F. Giust, A. de la Oliva and C. J. Bernardos, “Flat access and mobility architecture: An IPv6 distributed client mobility management solution,” in Computer Communications Workshops (INFOCOM WKSHPS), 2011 IEEE Conference on, 2011, pp. 361-366.

[89] M. S. Bargh, B. Hulsebosch, H. Eertink, G. Heijenk, J. Idserda, J. Laganier, A. R. Prasad and A. Zugenmaier, “Reducing handover latency in future IP-based wireless networks: Proxy mobile IPv6 with simultaneous bindings,” in World of Wireless, Mobile and Multimedia Networks, 2008. WoWMoM 2008. 2008 International Symposium on a, 2008, pp. 1-10.

[90] A. Dutta, S. Das, H. Yokota, T. Chiba and H. Schulzrinne, “Proxy MIP Extension for inter-MAG Route Optimization,” Draft-Dutta-Netext-Pmipro-00, Work-in-Progress, October 2009.

[91] C. Bernardos, A. de la Oliva, J. Zuniga, T. Melia and S. Das, “PMIPv6 operation with IEEE 802.21,” Draft-Bernardos-Netext-pmipv6-Mih-01, October 2009.

[92] H. Chan, F. Xia, J. Xiang and H. Ahmed, “Distributed local mobility anchors,” draft-chan-netext-distributed-lma-03, March 2010.

[93] M. Liebsch, S. Jeong and Q. Wu, “PMIPv6 localized routing problem statement,” Rfc-6279, June 2009.

[94] W. Song, Jong-Moon Chung, Daeyoung Lee, Chaegwon Lim, Sungho Choi and Taesun Yeoum, “Improvements to seamless vertical handover between mobile WiMAX and 3GPP UTRAN through the evolved packet core,” Communications Magazine, IEEE, vol. 47, pp. 66-73, 2009.

[95] D. Johnson, C. Perkins and J. Arkko, “Mobility support in IPv6,” Rfc-3775, June 2004.

[96] M. Muslam, H. A. Chan, N. Ventura and L. A. Magagula, “Hybrid HIP and PMIPv6 (HIPPMIP) mobility management for handover performance optimization,” in Wireless and Mobile Communications (ICWMC), 2010 6th International Conference on, 2010, pp. 232-237.

[97] J. Laganier, T. Koponen and L. Eggert, “Host identity protocol (HIP) registration extension,” Rfc-5203, April 2008.

[98] J. Laganier and L. Eggert, “Host identity protocol (HIP) rendezvous extension,” Rfc-5204, April 2008.

[99] OMNet++ open source network simulater., “Official website: http://www.omnetpp.org,”visited on 12/02/2012 .

[100] L. Bokor, S. Nováczki, L. T. Zeke and G. Jeney, “Design and evaluation of host identity protocol (HIP) simulation framework for INET/OMNeT,” in Proceedings of the 12th ACM

International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems, 2009, pp. 124-133.

[101] A. Varga and R. Hornig, "An overview of the OMNeT simulation environment," in Proceedings of the 1st International Conference on Simulation Tools and Techniques for Communications, Networks and Systems & Workshops, 2008, pp. 60.

[102] The Network Simulator – ns-2, "Official homepage: http://nsnam.isi.edu/nsnam/index.php/Main_Page," visited on 12/02/2012.

[103] I. OPNET Technologies, "Official homepage: http://www.opnet.com," visited on 12/02/2012.

[104] The INET Framework for OMNeT++, "Official homepage: http://www.omnetpp.org/doc/INET/neddoc/index.html," visited on 12/02/2012 .

[105] M. Muslam, H. A. Chan and N. Ventura, "Host identity protocol extension supporting localized mobility management," in Consumer Communications and Networking Conference (CCNC), 2011 IEEE, 2011, pp. 106-110.

[106] T. Narten, E. Nordmark and W. Simpson, "Neighbor Discovery for IP Version 6 (IPv6)," Rfc-2461, December 1998.

[107] M. M. Muslam, H. A. Chan and N. Ventura, "Inter-Subnet Localized Mobility Support of Host Identity Protocol," EURASIP Journal on Wireless Communications and Networking 2011, 4 August 2011, doi:10.1186/1687-1499-2011-55.

[108] C. Bovy, H. Mertodimedjo, G. Hooghiemstra, H. Uijterwaal and P. Van Mieghem, "Analysis of end-to-end delay measurements in internet," in Proc. of the Passive and Active Measurement Workshop-PAM'2002, 2002 .

[109] S. Mukkamalla and B. Raman, "Scaling and Latency Issues in Mobile-IP," http://www.cs.berkeley.edu/ adj/cs294-1.s98/projects/MobileIP/sld001.htm , April 1998.

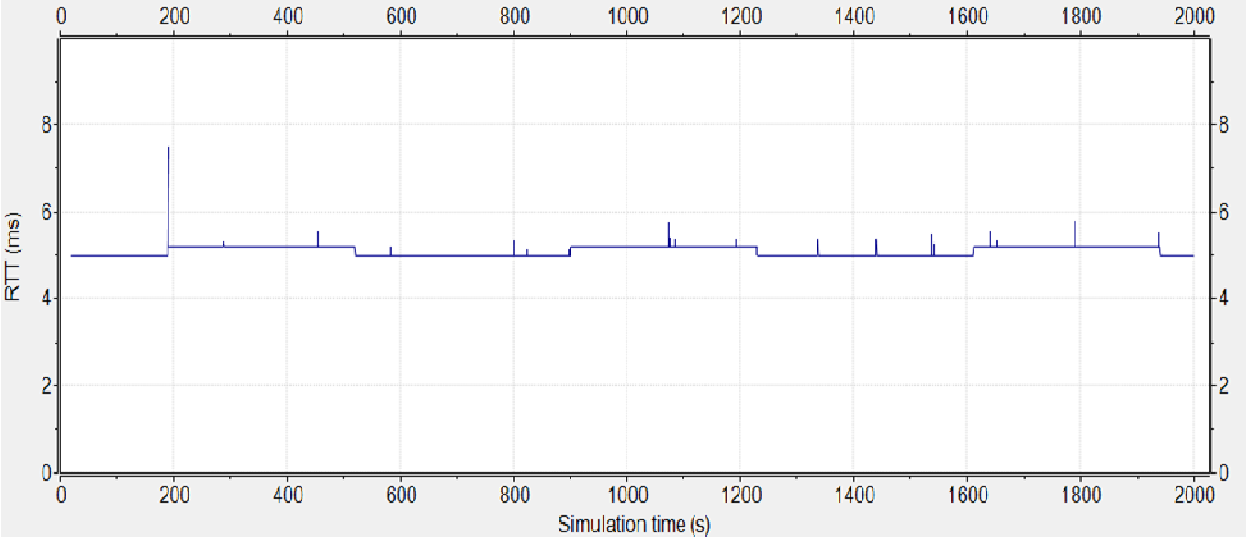
[110] H. Jiang and C. Dovrolis, "Passive estimation of TCP round-trip times," ACM SIGCOMM Computer Communication Review, vol. 32, pp. 75-88, 2002.

Appendix A: Influence of different traffic loads on DM-MHPP behaviour

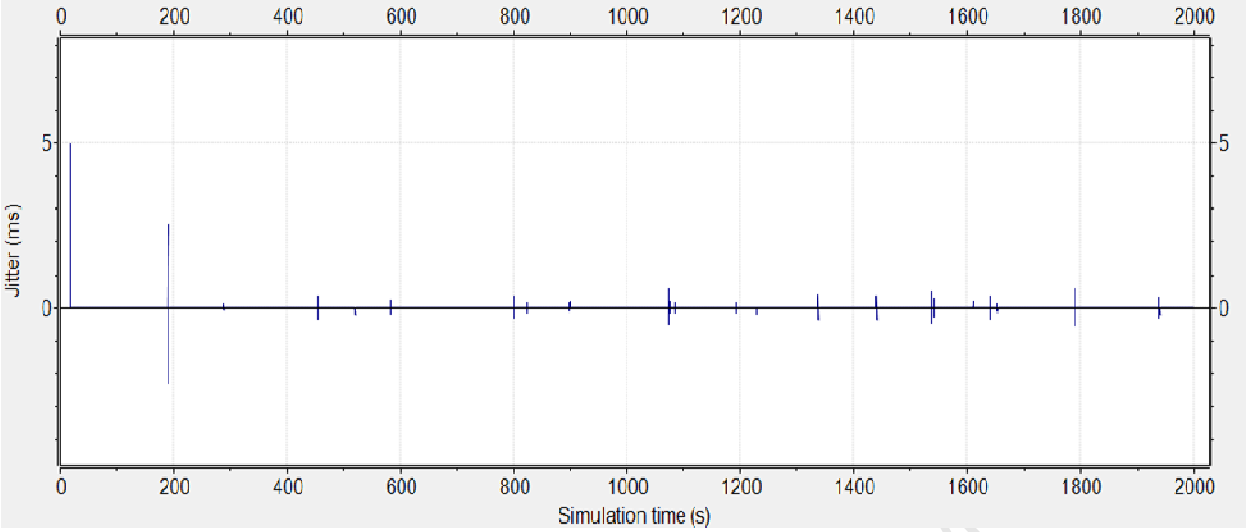
A.1 DM-MHPP

// Mobility-enabled HIP proxy for non-HIP-enabled and HIP-enabled //

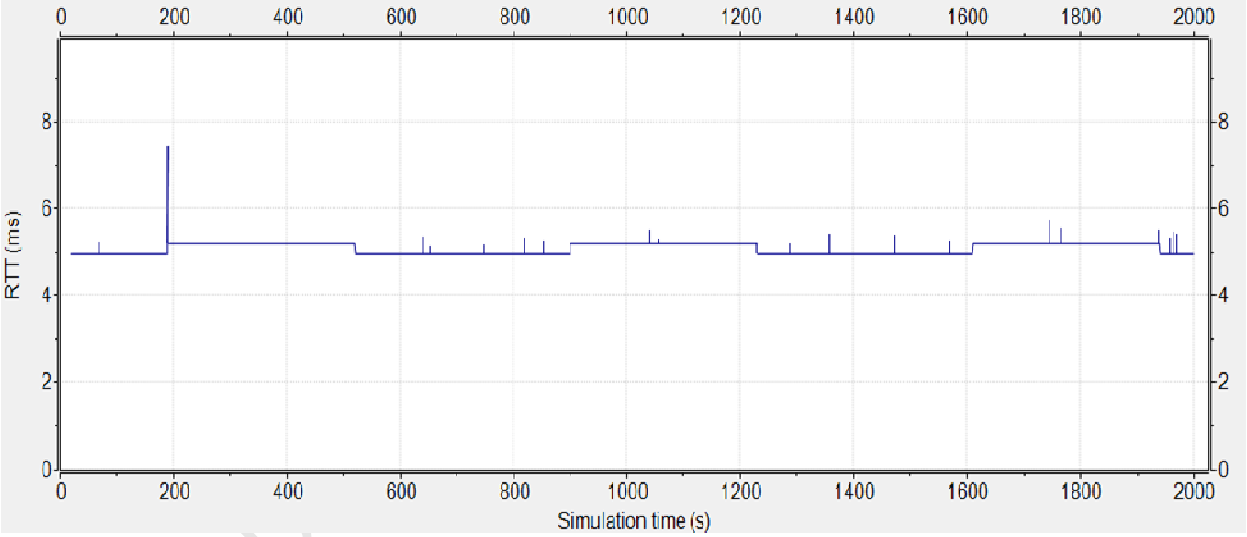
The following figures (A0-1, A0-3, A0-5, A0-7 and A0-9) show the influence of the different packet inter-arrival rates on the RTT before and after the handover of mobile host using DM-MHPP and moving between home and visited networks. Figures A 0-2, A 0-4, A 0-6, A 0-8 and A 0-10 show the influence of the different packet inter-arrival rates on the jitter for DM-MHPP. From the figures and the measurements, it is evident that DM-MHPP handover jitter in not varying due to different inter-arrival rates and thus meet the requirements for application that do not accept varying in packet delays.



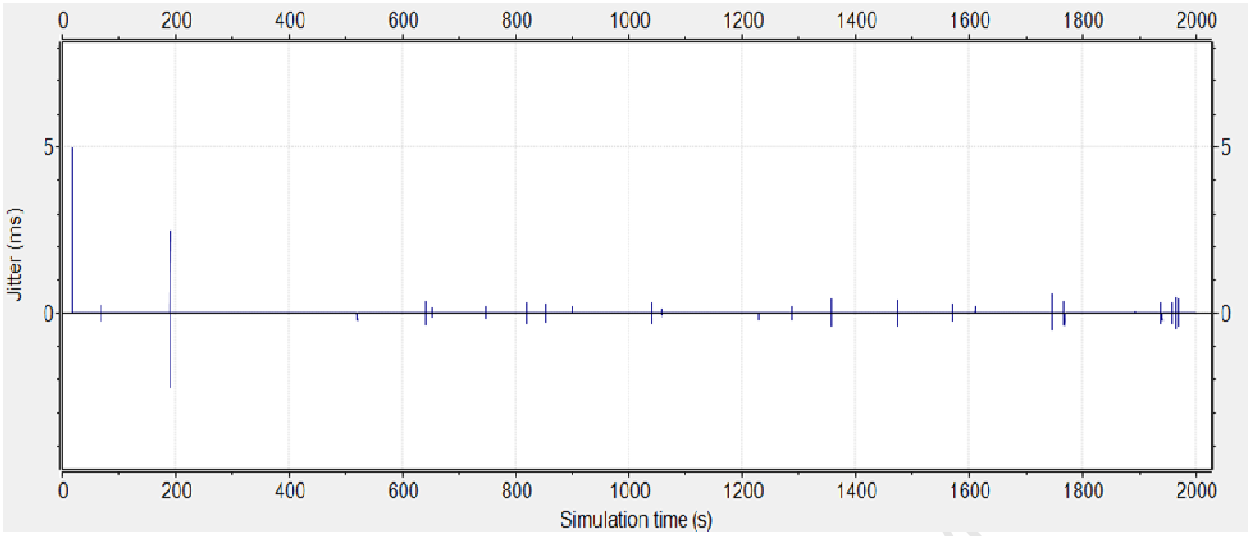
A 3. MH RTT in DM-MHPP scenario for packet interval of 100 ms.



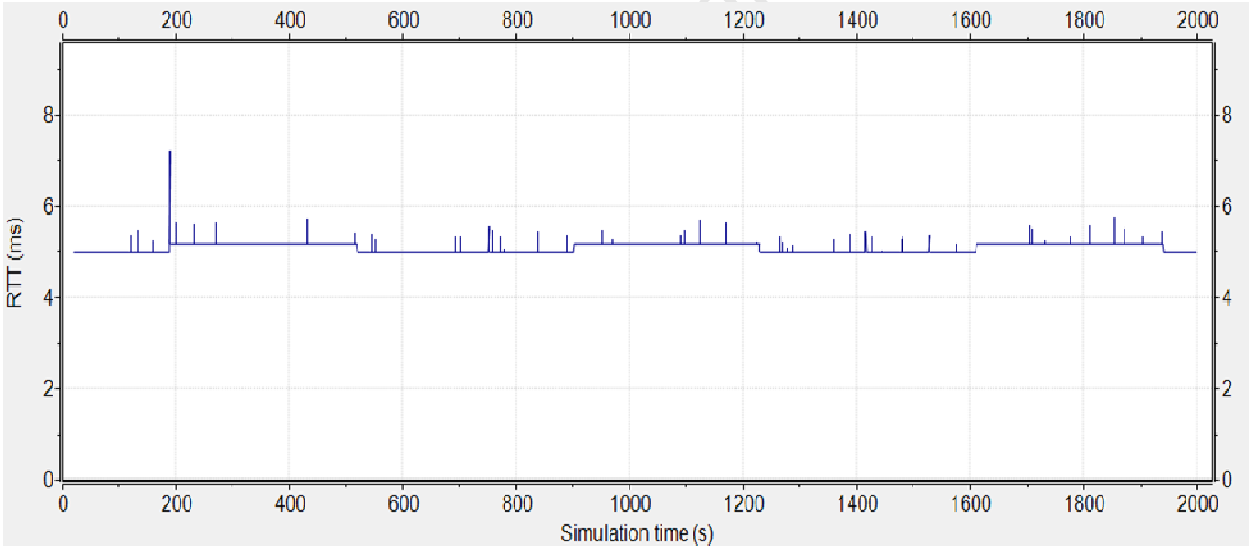
A 4. MH Jitter in DM-MHPP scenario for packet interval of 100 ms.



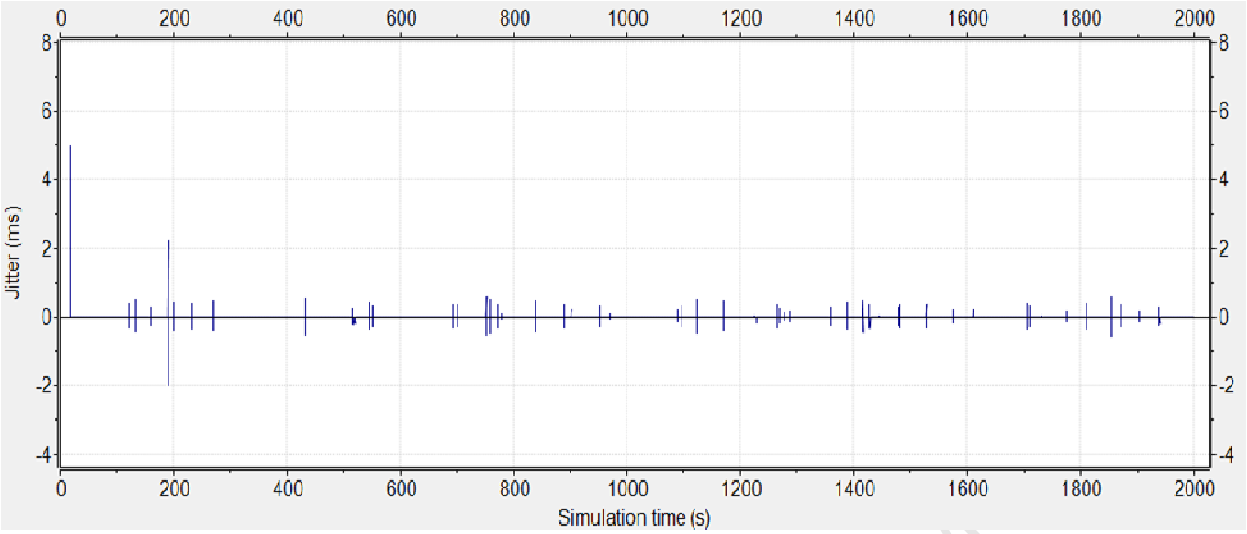
A 5. MH RTT in DM-MHPP scenario for packet interval of 80 ms.



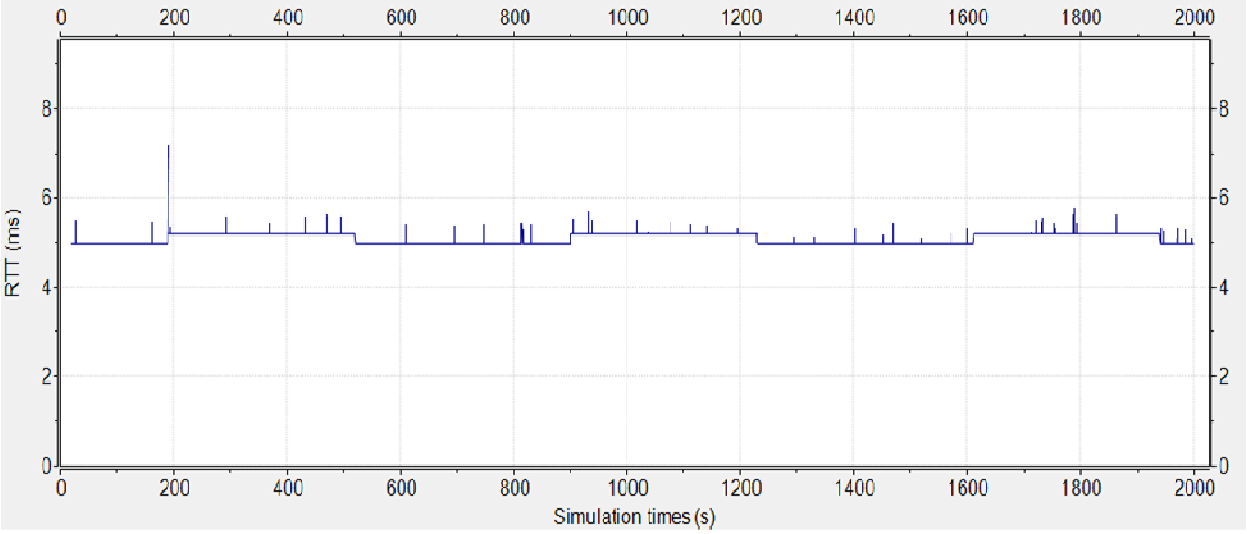
A 6. MH Jitter in DM-MHPP scenario for packet interval of 80 ms.



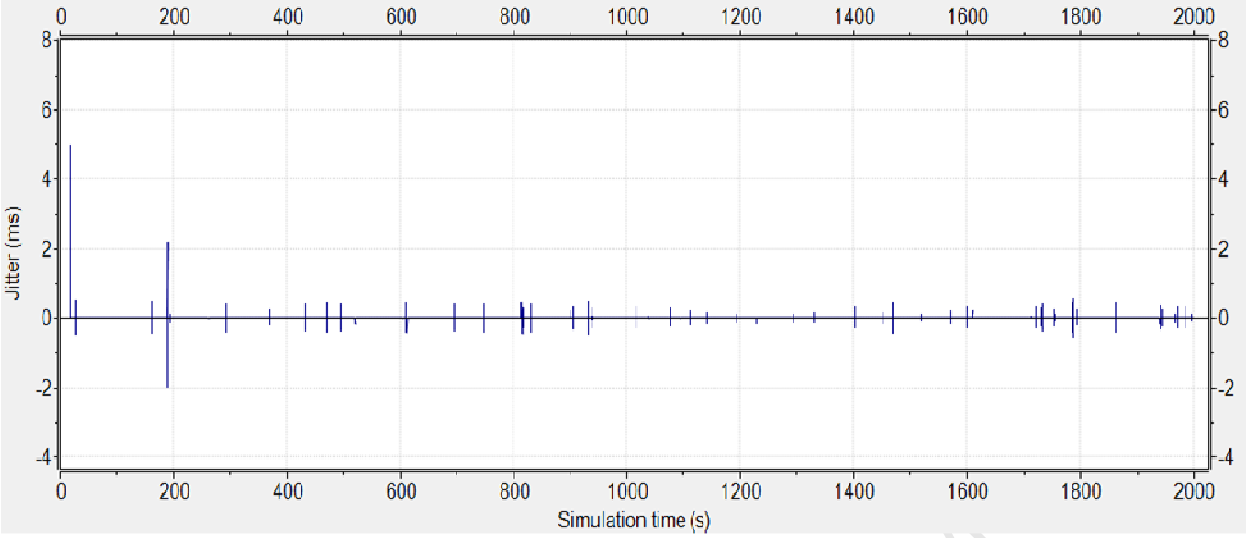
A 7. MH RTT in DM-MHPP scenario for packet interval of 60 ms.



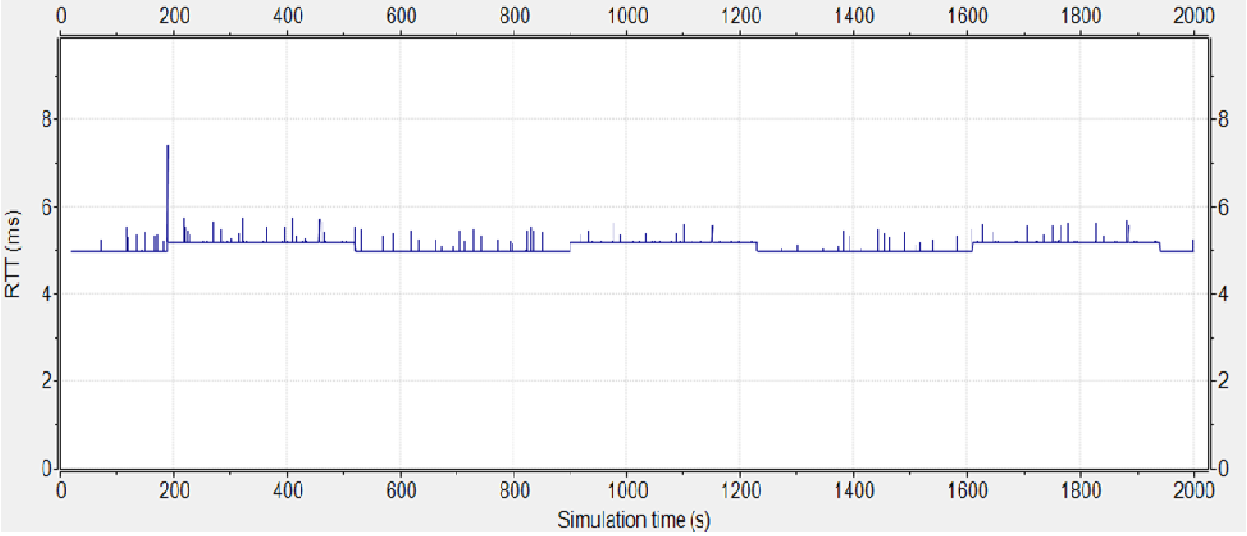
A 8. MH Jitter in DM-MHPP scenario for packet interval of 60 ms.



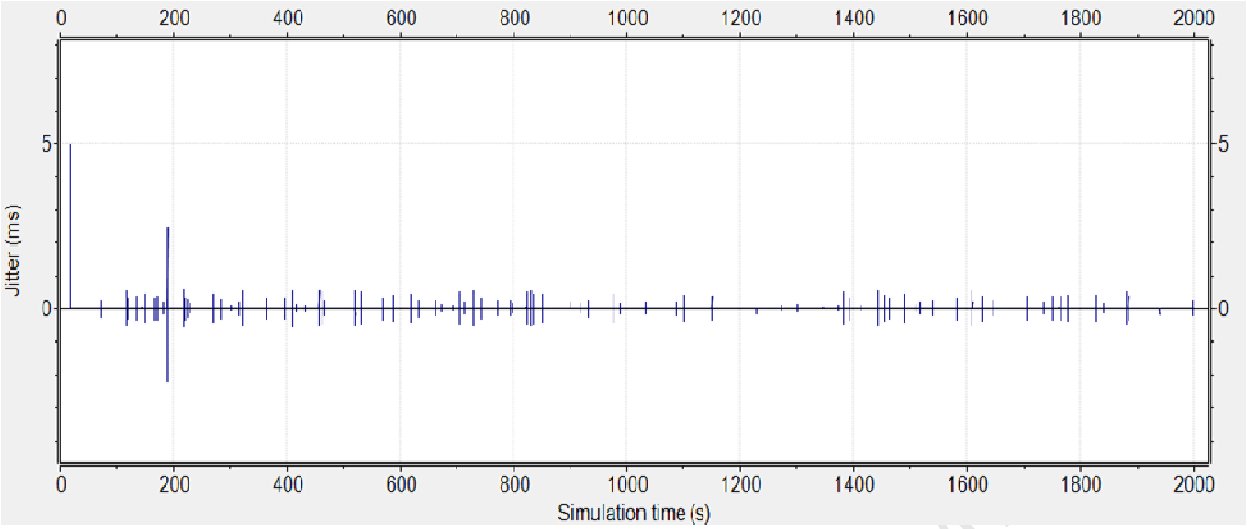
A 9. MH RTT in DM-MHPP scenario for packet interval of 40 ms.



A 10. MH Jitter in DM-MHPP scenario for packet interval of 40 ms.



A 11. MH RTT in DM-MHPP scenario for packet interval of 20 ms.



A 12. MH Jitter in DM-MHPP scenario for packet interval of 20 ms.

Appendix B:

Accompanying CD-ROM

The submission of this thesis is accompanied with a CD-ROM containing the following items:

• Simulation Frameworks - Developed simulation framework for each of the proposed solutions is included. Specifically the simulations frameworks for the following:

– HIPPMIP

– MHPP

– DM-MHPP

– SLDM

• Results data- Raw data obtained from the performance evaluation for each of the developed designs.

• Thesis documents - Source files and Portable Document Format (PDF) copies of the thesis document and abstract.