# Mobility Management across Converged IP-based Heterogeneous Access Networks

by

**Qazi Bouland Mussabbir**

**School of Engineering and Design**

**Brunel University**

A Thesis Submitted for the degree of

***Doctor of Philosophy***

**July 2010**

**Supervised by: Dr. Thomas Owens**

**Dr. Wenbing Yao**

## ABSTRACT

In order to satisfy customer demand for a high performance “global” mobility service, network operators (ISPs, carriers, mobile operators, etc.) are facing the need to evolve to a converged “all-IP” centric heterogeneous access infrastructure. However, the integration of such heterogeneous access networks (e.g. 802.11, 802.16e, UMTS etc) brings major mobility issues. This thesis tackles issues plaguing existing mobility management solutions in converged IP-based heterogeneous networks. In order to do so, the thesis firstly proposes a cross-layer mechanism using the upcoming IEEE802.21 MIH services to make intelligent and optimized handovers. In this respect, FMIPv6 is integrated with the IEEE802.21 mechanism to provide seamless mobility during the overall handover process. The proposed solution is then applied in a simulated vehicular environment to optimize the NEMO handover process. It is shown through analysis and simulations of the signalling process that the overall expected handover (both L2 and L3) latency in FMIPv6 can be reduced by the proposed mechanism by 69%. Secondly, it is expected that the operator of a Next Generation Network will provide mobility as a service that will generate significant revenues. As a result, dynamic service bootstrapping and authorization mechanisms must be in place to efficiently deploy a mobility service (without static provisioning), which will allow only legitimate users to access the service. A GNU Linux based test-bed has been implemented to demonstrate this. The experiments presented show the handover performance of the secured FMIPv6 over the implemented test-bed compared to plain FMIPv6 and MIPv6 by providing quantitative measurements and results on the quality of experience perceived by the users of IPv6 multimedia applications. The results show the inclusion of the additional signalling of the proposed architecture for the purpose of authorization and bootstrapping (i.e. key distribution using HOKEY) has no adverse effect on the overall handover process. Also, using a formal security analysis tool, it is shown that the proposed mechanism is safe/secure from the induced security threats. Lastly, a novel IEEE802.21 assisted EAP based re-authentication scheme over a service authorization and bootstrapping framework is presented. AAA based authentication mechanisms like EAP incur signalling overheads due to large RTTs. As a result, overall handover latency also increases. Therefore, a fast re-authentication scheme is presented which utilizes IEEE802.21 MIH services to minimize the EAP authentication process delays and as a result reduce the overall handover latency. Analysis of the signalling process based on analytical results shows that the overall handover latency for mobility protocols will be approximately reduced by 70% by the proposed scheme.

# Acknowledgements

First and foremost, I would like to thank my supervisors, Dr Thomas Owens and Dr Wenbing Yao, for their assistance and guidance during the course of my PhD research. In retrospect, the journey towards the degree has been a very challenging yet enjoyable one. I am personally thankful and indebted to Dr. Wenbing Yao, for teaching me the art of academic research. Without her kindness, generosity, and patience, this PhD research work would simply have not been possible. I am grateful to Dr Thomas Owens for providing and assisting me with his renowned expertise in wireless communications, and guiding me through the arduous and mammoth process of writing the thesis.

My sincere gratitude goes out to all the partners in the ENABLE Project, especially the R&D team from Huawei and Telecom Italia for providing valuable technical knowledge and skills.

I like to take this opportunity to thank my family members, especially my parents, who have gone to extreme ends to make sure I receive my education at the highest level. Truly, without their unconditional love and support, I would not have reached this point in life. I would like to thank my sister, who has been a constant source of encouragement. Lastly, but not the least, I am sincerely thankful to my loving wife, without whose love and courtship, I would not be the man I am today.

# *Table of Contents*

# *List of Figures*

# *List of Tables*

# Nomenclature

| | |
|---|---|
| ***3G*** | Third Generation |
| ***3GPP*** | Third Generation Partnership Project |
| ***4G Systems*** | Fourth Generation Systems |
| ***AAA*** | Authentication, Access and Accounting |
| ***ADSL*** | Asymmetric Digital Subscriber Line |
| ***ASA*** | Access Service Authoriser |
| ***ASP*** | Access Service Provider |
| ***AP*** | Access Point |
| ***BAA*** | Bootstrapping Authorisation Agent |
| ***BC*** | Bootstrapping Client |
| ***BCA*** | Bootstrapping Configuration Agent |
| ***BT*** | Bootstrapping Target |
| ***BS*** | Base Station |
| ***BU*** | Binding Update |
| ***CoA*** | Care-of-Address |
| ***EAP*** | Extensible Authentication Protocol |
| ***DoS*** | Denial of service |
| ***DSL*** | Digital subscriber line |
| ***HoA*** | Home Address |
| ***HoKEY*** | Handover Key |
| ***DVB-H*** | Digital Video Broadcasting - Handheld |
| ***GSM*** | Global System for Mobile communications |
| ***GPRS*** | General Packet Radio Service |

| | |
|---|---|
| ***HSPA*** | High Speed Packet Access |
| ***HIP*** | Host Identity Protocol |
| ***HSDPA*** | High-Speed Downlink Packet Access |
| ***IETF*** | Internet Engineering Task Force |
| ***IP*** | Internet protocol |
| ***IPSec*** | IP security |
| ***ISP*** | Internet service provider |
| ***IST*** | Information society technologies |
| ***ITU-T*** | International Telecommunication Union |
| ***LAN*** | Local Area Network |
| ***MAC*** | Medium access control |
| ***MSA*** | Mobility Service Authorizer |
| ***MSP*** | Mobility Service Provider |
| ***MSCTP*** | Mobile Stream Control Transmission Protocol |
| ***MN*** | MN |
| ***NAS*** | Network Access Server |
| ***NAT*** | Network address translation |
| ***NGN*** | Next Generation Network |
| ***PDA*** | Personal digital assistant |
| ***RSS*** | Required Signal Strength |
| ***RTP*** | Real-time transport protocol |
| ***RTT*** | Round-trip time |
| ***SCTP*** | Stream Control Transmission Protocol |
| ***SIP*** | Session Initiation Protocol |
| ***SHIM6*** | Site Multihoming for IPv6 Intermediation |

| | |
|---|---|
| ***PoA*** | Point-of-Attachment |
| ***PoS*** | Point-of-Service |
| ***UMTS*** | Universal Mobile Telecommunications System |
| ***WLAN*** | Wireless Local Area Network |
| **VoIP** | Voice Over Internet Protocol |
| ***QoS*** | Quality of Service |
| ***W-CDMA*** | Wideband code division multiple access |

# CHAPTER 1 - INTRODUCTION

## 1.1 Introduction

Mobile communications is entering a new era where service provision in mobility is evolving to exploit the capabilities of converged 'all-IP' centric networks. The rapid proliferation of mobile devices along with the presence of a plethora of distinct cellular telecommunications, wireless local area networks and broadcast to hand-held device standards, e.g. GSM, GPRS, EDGE, UMTS, 802.11a/b/g/n, DVB-H, etc has led to a massive growth in users accessing the Internet from portable hand-held devices. According to reports, mobile Internet service providers have over 100 million customers worldwide using more than 300 active networks [1]. By January 2009, there were 247 commercial HSDPA networks launched in 110 countries with an estimated 65 million HSPA users [2]. Vodafone, the world's second largest Telecommunications operator, reported an increase of 55% in revenues from data traffic from March 2007 to March 2008. Informa Telecoms & Media forecasts that the volume of data transported over wireless connections will increase by 1000% between 2007 and 2012 [1]. The consumer demand for a truly mobile broadband experience, which involves a combination of wired broadband data speeds, global coverage and mobility, and ubiquitous access to services across heterogeneous networks, is changing the wireless landscape and providing the incentive for a migration towards the so called Fourth-Generation (4G) networks (WiMAX, 3GPP LTE, LTE Advanced etc). Thus, the demand for global mobility and “any time- anywhere” type services is paving the way for Next Generation Networks (NGN) which essentially represent the integration of existing (2/2.5, 3G, WLANs etc) and upcoming(i.e. 4G based) heterogeneous access networks where the underlying converged infrastructure is completely IP based. That said there seems to be confusion amongst researchers about how 4G networks and NGN should be defined. Apart from representing the natural evolution of 3G systems, 4G by definition means a fully IP-based convergence of existing and new wired and wireless networks (i.e. LTE, 802.16m etc.), as well as of the computers, consumer-electronics, and communications technology generally, necessary for the provision of IP based data services at data rates of 100 Mbit/s to 1Gbit/s. Therefore, 4G and NGN essentially represent the same concepts and this thesis will use these terms interchangeably.

The vision of Next Generation Networks (i.e. 4G) is inherently of an intricate mesh of multi-access and multi-operator convergence. It is assumed that every end-device will be multi modal (i.e. different interfaces for each of the access technologies). End users will have different technology options with which to access the Internet while mobile, in a market where service providers (fixed and mobile), in some cases joined in consortium co-exist with smaller and often unmanaged entities (e.g. private or home WLANs). Another element to be considered is the presence of on-board vehicular networks placed in trains, cars, buses or other moving vehicles. Typically these networks use 802.11 WLAN infrastructure and offer connectivity to travellers or exchange information between on-board devices, e.g., satellite navigation systems, sensors, etc. In such a context, providing users with seamless mobility with zero service interruption across such a heterogeneous access environment is becoming a necessity. Given below in Figure 1.1 is a depiction of the envisaged network scenario for Next-Generation Networks.

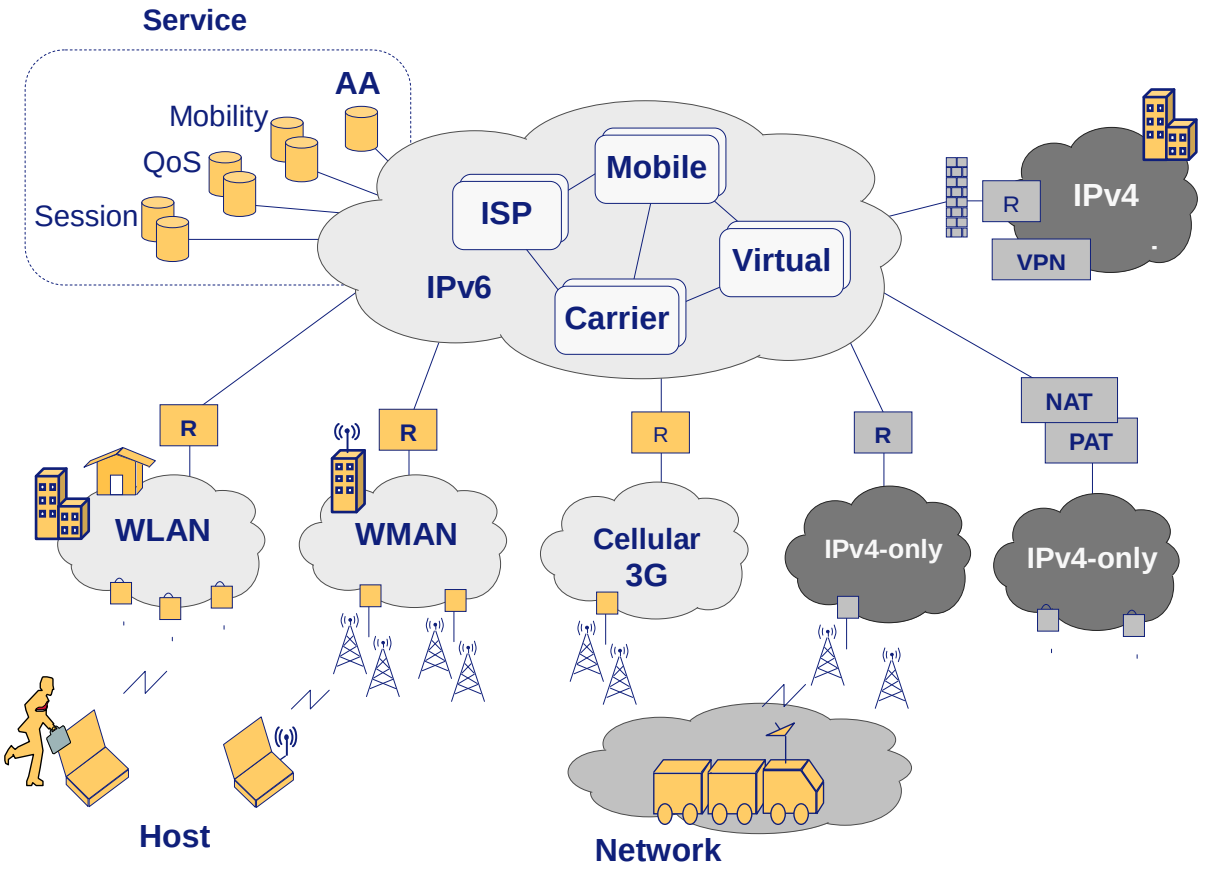


Figure 1.1: Envisaged Network Deployment for Next Generation Networks

Seamless mobility requires seamless handover. Providing such handover in an integrated multi-access environment is challenging but very important. Essentially, vertical handover, which means inter-technology handover and which may also be between different operator domains, will be a particularly complicated process. Handover between cells of the same technology is called horizontal handover and is said to be intra-technology in nature; this of course may also be across different operator domains. Any handover whether inter or intra technology can be broadly classified as providing either micro or macro-mobility. Micro-mobility refers to mobility inside a given domain that is between subnets, while macro-mobility refers to mobility between different administrative domains. Various handover scenarios could be envisaged based on the mobility requirements of 4G networks. Examples of such mobility scenarios are given in section 2.2 of this thesis.

IPv6 [16] has been chosen not only for the core backbone infrastructure of 4G but also for its ubiquitous inter-networking layer for the provisioning of seamless mobility between the integrated heterogeneous access networks. Another reason for choosing IPv6 is because of the rapidly depleting IPv4 [17] address pool. However, interworking with IPv4 based networks will also be supported in 4G with plans for a smooth migration to IPv6. Network Layer/Layer 3 (i.e.IPv6) mobility will be fundamental in providing global mobility, i.e. the ability to move freely within large geographical areas and still be reachable/addressable in the Internet for uninterrupted services. It must be noted that there have been extensive discussions about which is the most suitable layer in the TCP/IP protocol stack [18] for dealing with mobility efficiently. Mobility solutions exist in all the layers of the protocol stack. Examples of mobility management protocols at different layers are Session Initiation Protocol (SIP) [4], Host Identity Protocol (HIP) [5], etc. As such, different levels of convergence could be defined. The choice of the layer used to implement handover and thus mobility is driven by design trade-offs. Different wireless access network technologies, e.g., 802.16e, UMTS, come with technology specific standardised mobility solutions. That is to say that they each provide distinct handover mechanisms for intra-technology handover. Each type of access technology has distinct advantages/disadvantages and applications scope in terms of coverage, data transfer speed, frequency, spectrum availability, etc. It is reasonable to state that convergence at layer 2, i.e., the link layer, would require every individual standard to drastically modify its existing access technologies and that it would be unwise and costly to converge at the link layer. On the other hand, real-time applications are very

sensitive to handover latency, packet loss, etc., and may want to handle mobility themselves to dynamically adapt to the changing context using mobility protocols such as SIP. However applications come and go and it would be a significant burden for each one to develop its own mobility protocol. The same is true for mobility management or convergence at the transport layer. Taking this into account and given the ubiquitous interworking nature of IP, solutions based on network layer mobility may seem natural. However, multiple mobility protocols may exist and operate at the same time so such solutions would cause maintenance and scalability "nightmares" for operators and users alike.

A number of network layer mobility management solutions have been proposed to provide mobility and handover management services. Amongst candidate technologies, Mobile IPv6 (MIPv6) [6][3] has been widely accepted by academia and industry alike and standardized by the Internet Engineering Task Force (IETF) as a viable option for delivering the required ubiquitous mobility services across integrated heterogeneous networks. MIPv6 arbitrarily allows a mobile node (MN) to change its location on the Internet due to a change in its link while roaming between access networks belonging to different subnets of administrative domains. A graphical illustration of how MIPv6 works is given in Figure 1.2.

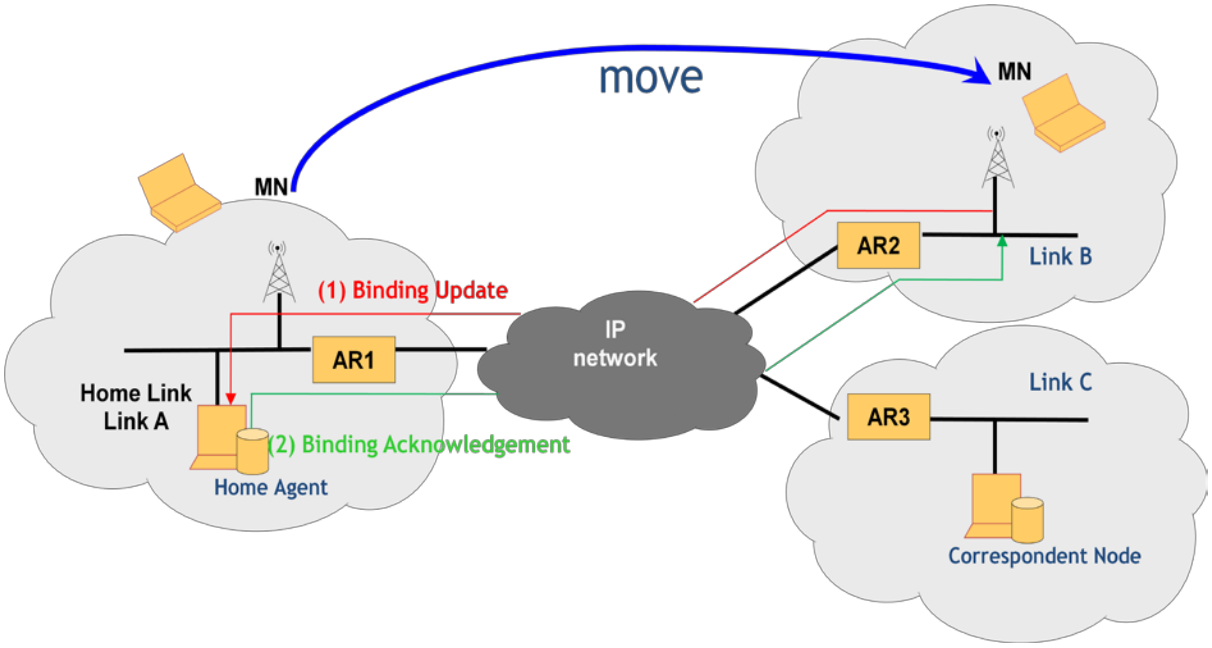


Figure 1.2: Mobile IPv6 overview

Its main objective is to maintain session continuity between the MNs and Corresponding Nodes (CNs) with which the MN is communicating with while it changes its Point-of-Attachment (PoA), i.e. APs, BSs [7]. The MN updates its change in IP subnet at an anchor point known as the Home Agent (HA) by sending a prefix-scope Binding Update (BU) message that associates its Care-of-Address (CoA) which is its current IP address with its Home Address (HoA) [7]. The HA intercepts any packet destined for the MN and tunnels it to the MN's current CoA.

### 1.1.1 Research Issues

There are many obstacles and issues that will have to be resolved to realise the efficient deployment of large scale 'All-IP' based converged heterogeneous networks. This thesis focuses on mobility management for optimized handover mechanisms at the network/IP layer. This includes providing security management in terms of authentication and authorization to allow IP mobility to be provided as a commercial service by a network operator/service provider. Other mobility management issues such as radio interference and management, power control, etc. are beyond the scope of this thesis.

#### 1.1.1.1 Long Handover Latencies for Mobile IPv6 based Mobility protocols

Unfortunately, the overall handover latency of the MIPv6 protocol is unacceptable for most time delay sensitive applications such as VoIP, video conferencing and streaming multimedia. Handover performance plays a crucial role in the QoS provisioning of real-time multimedia services/applications. For such reasons the IETF *Mobility for IP: Performance, Signalling, and Handoff Optimization (MIPSHOP)* Working Group (WG) has developed MIPv6 extension protocols which include, Fast Handovers for MIPv6 (FMIPv6) [7], Proxy Mobile IPv6 (PMIPv6) [8] and Hierarchical MIPv6 (HMIPv6) [9], for reducing the signalling overhead and handover latency incurred by MIPv6. FMIPv6 has proven to be a strong contender among mobility optimization protocols by providing a ‘make-before-break’ type handover solution with the assistance of layer 2 (L2) triggering mechanisms. Using anticipation mechanisms (i.e. L2 triggers), FMIPv6 prepares for handovers in advance. FMIPv6 aims at reducing the handover latency by formulating a prospective IPv6 address known as a New Care-of-Address (NCoA), while it is still present on the current/previous AR's (pAR) link [7]. Details of the FMIPv6 protocol operations are given in chapter 2. However, it must be noted that HMIPv6 or FMIPv6 alone, or a combination of them both (HFMIPv6 [81]) is not sufficient to reduce packet losses

and handover latency enough to efficiently provide the required QoS for delay sensitive real-time multimedia traffic.

#### 1.1.1.2 Need for Cross Layer interactions for Intelligent Media Independent Handover Management

One of the major drawbacks of mobility management mechanisms in a multi-access environment is the lack of interaction between different layers of the protocol stack. The mobility management protocols at layer 3 (L3) or above are not capable of making intelligent handover decisions without cross-layer interactions with other layers below or above it. For instance, providing link layer or various network information (e.g. Layer 2 triggers, network neighbourhood information such as PoA MAC addresses, PoA channel ranges, Network Type, Security details etc) to Layer 3 or higher mobility protocols would allow for informed and intelligent/optimized handovers across heterogeneous access networks.

The IEEE802.21 standard WG, named the Media Independent Handover (MIH) Standard WG [13], officially established in 2004, is developing a standard that provides generic link layer intelligence and other network related information to upper layers to optimize handover between different heterogeneous media, such as 3GPP/3GPP2, and both wired and wireless media of the IEEE802 standard family [13]. In order words, the IEEE802.21 standard is developing solutions to enable efficient cross-layer mechanisms. At the moment, there is a lack of clearly defined handover optimization mechanisms in IETF and IEEE802 standards (e.g. 802.11, 802.16). By taking into account the details of the interworking of MIPv6 extension protocols such as FMIPv6 with IEEE802.21 MIH services, optimized handover solutions could be defined. Moreover, the current 802.21 draft standard does not take into account mobility management in vehicular environments. Already, CALM (Continuous Air interface for Long and Medium range) which is a family of umbrella protocols developed in ISO/TC204/WG16 ("Wide Area ITS Communications") is developing standards in order "*to provide a uniform environment for vehicle data communications that allows vehicles to stay connected using the best communications technology available both in the vehicle and in the infrastructure wherever the vehicle is located*" [14]. In fact, in CALM, MIPv6 and Network Mobility (NEMO) [15] are included as two viable options for supporting host mobility and network mobility respectively in vehicular environments. Considering the overlap of work between CALM and IEEE802.21, with

respect to defining cross-layer solutions for optimized handover mechanisms, there is a great need to link the work done by both the standards. Therefore, extensive research needs to be done if MIH services are to be provided in vehicular environments.

#### 1.1.1.3 Mobility Service Bootstrapping Problem

In order to successfully deploy Mobile IPv6 based mobility solutions across large scale IPv6 heterogeneous networks, it is crucial to develop mechanisms to dynamically and securely provide the end hosts with the necessary information for service access based on some long term credential, which is typically a shared secret or a X.509 certificate. However, in the current MIPv6 specification defined in [6], the MN is assumed to be statically provisioned with the necessary information (i.e. HoA, HA address and necessary security associations with the HA). From an operational point of view, such an assumption prevents any large scale MIPv6 deployment since it is not feasible or scalable to manually configure thousands of users and HAs. The availability of a dynamic solution, which is also known as “MIPv6 Bootstrapping” [20] is, therefore, a fundamental building block for enabling large scale MIPv6 deployment.

#### 1.1.1.4 Need for a Mobility Service Authorization Framework

It is becoming clearer to operators that mobility will become an inherent part of 4G networks. A big proportion of their revenues will come from considering and providing mobility as a service. As a result basic Mobile IPv6 could be enriched with a set of additional features such as HMIPv6, or FMIPv6. For instance, FMIPv6, which offers an enhancement to the MIPv6 features, could be considered as a “premium” type service from an operator’s point of view. Therefore, it must be noted that Mobile IPv6 and its extension protocols (FMIPv6 in our case) or any other services such as multi-homing, video streaming/conferencing, needs extensive authentication and authorization to maintain efficient accounting information and prevent potential security threats being introduced by such services. Authorization is often a neglected problem. The main focus of the existing bootstrapping architecture is to establish related information and security associations between the involved parties to authenticate successfully. However it is not clear whether a MN which is able authenticate successfully with a HA, should be automatically allowed to access a service in mobility. Consider a scenario where a MN interacts with a HA to utilize a MIPv6 service to maintain session continuity. The HA could be located in the access network and an additional authorization step from the user's home domain

would be necessary to ensure the user is in fact authorized to obtain the requested service and start credit control and accounting. This leads to the notion that authenticating for initial network access in a visited domain does not necessarily mean that the user is authorized to use other network services. In other words, authentication and authorization should be decoupled for efficient service provisioning.

#### 1.1.1.5 IEEE802.21 assisted fast Re-authentication

Wireless handovers between PoAs (APs, Bss) across heterogeneous networks are typically a complicated process that involves several layers of protocol execution, which results in long latencies causing undesirable service disruptions. Apart from the mobility protocol signalling, additional latencies are incurred due to AAA services for re-authentication purposes. At the moment, there is a great lack in research on how IEEE802.21 MIH services could assist in optimizing the AAA based re-authentication process to reduce the overall handover latency. Moreover, operators may treat the IEEE802.21 assisted fast re-authentication mechanism as a "premium" service. As a result, an efficient scheme should be in place for IEEEE802.21 assisted fast re-authentication service authorization and bootstrapping.

## 1.2 Thesis Contributions

This thesis takes into account the challenges/issues described in the previous section as the driving forces behind the motivation to pursue detailed research, which aims at enabling efficient mobility management across heterogeneous IPv6 based networks. During the course of the research period, the thesis has contributed relevant research to the body of literature in the field and to standardisation. These contributions are detailed below:

### 1.2.1 Handover Enhancement for Mobile IPv6 based Solutions using IEEE802.21 MIH Service

Enhancement of Mobile IPv6 based solutions (namely FMIPv6) is proposed to allow for seamless mobility across heterogeneous networks using IEEE802.21 Media Independent Handover (MIH) services. A detailed cross-layer mechanism has been defined which greatly reduces the FMIPv6 (also applicable to other MIPv6 solutions) overall handover latency (i.e. both at Layer 2 and Layer 3) with the assistance of existing and newly defined MIH service

primitives. With the aid of the lower three layers' knowledge of the MN/Mobile Router (MR) and the neighbouring access networks, the radio access discovery and candidate AR discovery issues (refer to chapter 2, section 2.7.1) of FMIPv6 are tackled. FMIPv6 has been applied in simulated vehicular environments to optimize the handover procedure by using IEEE802.21 MIH services. FMIPv6 is used to enhance the performance of handover in Mobile IPv6 (MIPv6) and its basic extension for Network Mobility (NEMO), the fundamental mobility management protocols used in vehicular networks.

The thesis shows through analysis and simulations using Network Simulation (NS2) that the proposed mechanism will significantly reduce the overall expected handover latency (both at Layer 2 and Layer 3) in FMIPv6.

### 1.2.2 Experimental Evaluation of secured FMIPv6 over a Generic Authorization and Bootstrapping Architecture

A novel service authorization and bootstrapping architecture is presented in order to provide the MN with the necessary configuration parameters and distributed keying materials to successfully bootstrap FMIPv6 services across heterogeneous access networks in terms of authentication and authorization.

In this respect, experimental analysis is provided through implementation of a practical Linux operating system based test-bed. The purpose of the experiments carried out on the test bed was to investigate the handover performance of the proposed secured FMIPv6 mechanism compared to plain FMIPv6 and MIPv6 by providing quantitative measurements of the quality perceived by the users of the IPv6 multimedia applications subject to handover.

### 1.2.3 IEEE802.21 assisted Re-Authentication scheme over a service authorization and bootstrapping framework

A novel IEEE802.21 assisted Re-Authentication scheme over a service authorization and bootstrapping framework is presented to reduce the signalling overhead during the re-authentication process, and as a result reduce the overall handover delay. The thesis shows

through analysis that the proposed mechanism will enhance the re-authentication process and significantly reduce the overall expected handover latency.

## 1.3 The EU IST 'ENABLE' Project

This thesis has been partly affiliated with and produced within the EU IST F6 framework 'ENABLE' project. The project included nine worldwide partners including Brunel University. The partners were Telecom Italia (Italy), Siemens (Germany), IABG (Germany), University of Murcia (Spain), Consulintel (Spain), TSSG (Ireland), Georg-August-University of Goettingen (Germany), Huawei Technologies (China). Brunel has actively collaborated with its project partners to fulfil the goal of ENABLE which has been to research, develop, test, integrate and evaluate mechanisms and technologies for the successful deployment of efficient and operational mobility as a service in large scale IPv6 based heterogeneous networks [118].

## 1.4 Thesis Structure

This thesis is organized into eight chapters:

- ***Chapter 2*** provides the background to the pursued research.
- ***Chapter 3*** gives a comprehensive survey of the related work on mobility management in heterogeneous networks.
- ***Chapter 4*** investigates the potential of applying FMIPv6 in vehicular environments by optimizing the handover procedure using IEEE802.21 MIH services.
- ***Chapter 5*** presents a novel service bootstrapping and authorization architecture for FMIPv6 in order to provide the MN with necessary configuration parameters and distributed keying materials to secure FMIPv6 messages in terms of authentication and authorization.
- ***Chapter 6*** presents a novel IEEE802.21 assisted Re-Authentication scheme over a service authorization and bootstrapping framework. The purpose of the proposed scheme is to reduce the signalling latency during the re-authentication process, and as a result reduce

the overall handover delay. Also, the proposed scheme enables 802.21 service authorization and enables SAs to be established for securely exchanging MIH services.

- ***Chapter 7*** presents proposals for future work and conclusions.

## 1.5 Publications

**Transactions/Journals Papers**

- Q.B.Mussabbir, W.Yao, Z.Niu and X.Fu, "Optimized FMIPv6 using IEEE802.21 MIH Services in Vehicular Networks", IEEE Transactions on Vehicular Technology, Volume 56, Issue 6, November 2007, Page(s):3397-3407

**Conference Papers**

- Q. B.Mussabbir and W.Yao, "Optimized FMIPv6 handover using IEEE802.21 MIH services", In *Proceedings of ACM/IEEE International Workshop on Mobility in the Evolving internet Architecture*, MobiArch, San Francisco, 2006

- Q.B.Mussabbir, W.Yao and J.Cosmas, "IEEE802.21 Assisted Network Layer Mobility Support", Accepted in *The Third International Conference on Mobile Computing and Ubiquitous Networking*, ICMU, London 2006

## 1.6 Chapter Summary

This chapter has introduced the thesis and presented the current research issues of its research area of mobility management in Next Generation Networks. The original contributions made by the thesis to its research area have been summarized.

# CHAPTER 2 - BACKGROUND

## 2.1 Supported Services and Devices in Next Generation Networks

In chapter 1(see section 1.1) the envisaged network scenario for NGNs was highlighted. Before delving deeper into the realms of mobility management, it is important to highlight the services and terminals that will be supported in NGNs. It is quite difficult and risky to lay down customer needs for the future. However, a basic knowledge of the type of services, terminals and business entities that will exist in NGNs, can be derived from the concept of integrated heterogeneous access networks. The end-users should be able to utilize all the services and applications which are common in today's networks (mostly in wired networks such as ADSL, LAN etc) and are typical across the wired Internet. Tables 2.1 and 2.2 highlight a list of the core services and devices which will exist in 4G networks. It must be noted that the list in the tables is not exhaustive because future services and devices which were not envisioned at the time of writing are not included.

| | ***Popular Internet Service*** | ***Multimedia Services*** | ***Upcoming Services in NGNs*** |
|---|---|---|---|
| ***Overall Services*** | Web, E-mail, Chat and Instant Messenger, P2P Applications (Limewire Bittorrent), Enterprise Applications (e.g. SAP), VPN Access, Telnet, FTP, ssh, .... | Video-Conferencing, VoIP, Audio/Video Streaming, Video on Demand (VoD), Online Gaming Real-time Information Sharing, .... | Location-Based Services, Mobility Services (e.g. MIPv6, FMIPv6 etc), Multihoming, .... |

Table 2.1: Services for NGN

| | ***Handheld*** | ***Other*** |
|---|---|---|
| ***Target Devices*** | Laptops, PDAs, Cameras, Mobile Phones, Portable Game Devices, Multimedia Devices | Sensory Devices, Satellite Navigation Systems |

Table 2.2: Target Devices

The purpose of an integrated multi-access network is to allow users to be able to roam across different access technologies and administrative domains and utilize a wide array of ubiquitous services irrespective of their geographic location. Mobility is the core underlying principal of heterogeneous access networks which allows users to roam freely across multi-access environments. As a result, mobility will be the "*De-Facto*" service and it is only rational for Telecom operators to generate a massive revenue stream from it if they can. In other words, customers will have to subscribe and pay for services which will allow them seamless (i.e. without any service interruption) roaming in multi-access environments using mobility protocols such as Mobile IPv6, FMIPv6 etc. Therefore, it is important that an efficient business model is in place to provide solutions for mobility service bootstrapping (i.e. configuration and SA parameter provisioning) and access control ( authentication and authorization) mechanisms.

## 2.2 Business Models

It is clear that NGNs will support a wealth of services (shown in Table 2.1). Such a magnitude of services calls for clearly defined business models which will allow operators to provide such services efficiently to their customers. The complex network scenario envisaged for NGNs has led the IETF to define specialized business entities to provide mobility services. Such business entities may in turn require sophisticated business relationships among themselves. Since the core of this thesis focuses on mobility management for 4G networks, the simplified business model shown in Figure 2.1 is applicable only for mobility services.

The four clearly distinguishable macro entities shown in Figure 2.1 are the End users, Access Service Providers (ASP), Access Service Authorizer (ASA), Mobility Service Providers (MSP) and Mobility Service Authorizer (MSA).

The ASP provides network access services to the end-users (i.e. IP connectivity). The end-users maintain their subscriptions to a "Home" ASP which stores the user's service profile and contractual agreements. The user's ASA is responsible for granting authorization to the user's network access, even in a roaming scenario where the user is in a foreign ASP network. The "Home" ASP is also the user's ASA. Possible examples of ASPs are ISPs, mobile operator networks, virtual providers (Wireless ISPs), corporate networks etc.

Similarly the mobility service has been separated with specialized business roles. The MSP delivers IP mobility services to end-users. The MSP hosts the necessary mobility management infrastructure such as Home Agents or global mobility anchor points. The MSP stores the user's service profile and contractual agreements. The “Home” MSP also constitutes the MSA which is in charge of authorizing the user for mobility services such MIPv6, FMIPv6 etc. The “Home” MSA may delegate mobility services to one or many MSPs (through “service roaming” agreements) as deemed necessary.

In Figure 2.1, the Roaming Broker (RB) will act as a trusted third party and central hub among the service providers. This will avoid the establishment and maintenance of number of one-to-one relationships between service providers. The RB can be used by both network services (i.e. ASP – RB – ASA) and mobility services (i.e. MSP – RB – MSA).The iPass is an example of a Roaming Broker for access service.

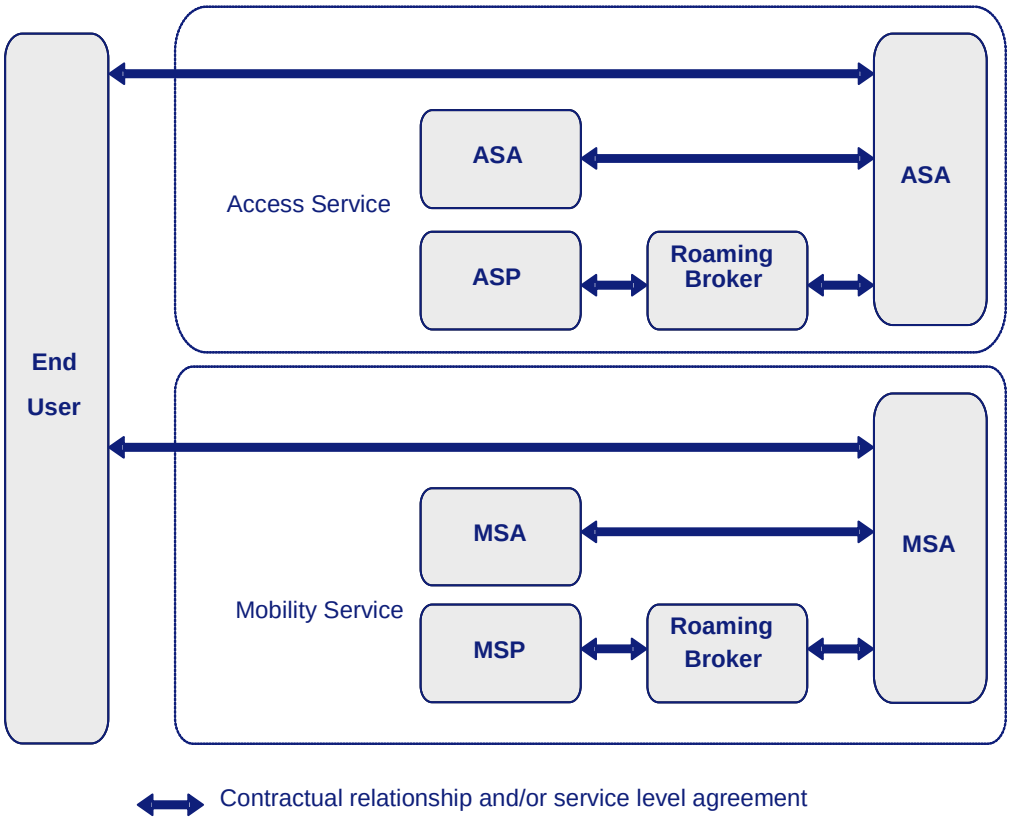


Figure: 2.1. Foreseen Business Entities

The end-user category is quite varied and involves many actors which can be easily classified. The groups defined below are not necessarily separate and a user may belong to more than one group. For example, cellular users may want to leverage their corporate network while they are at work.

***Cellular users*** are customers of mobile operators. Cellular users use an (U) SIM to access the mobile network (e.g. GSM/UMTS networks)

***Private citizens*** use the Internet providers network (ISP, carrier, Wireless ISP, etc) using technologies such as dial-up, ADSL, Wireless MAN, hotspots, etc.

***Employees*** who use their corporate networks from work using both wired and wireless technologies.

## 2.3 Mobility Scenarios

### 2.3.1 Access Technologies

The mobility scenarios in 4G networks will comprise of various access technologies. In Table 2.3, a list of the main access technologies involved in the mobility scenarios are provided. Note that the list is not exhaustive as future access technologies are not considered.

| | ***Local Area Networks*** | ***Cellular*** | ***Wireless Metropolitan Networks*** | ***Satellite*** |
|---|---|---|---|---|
| ***Main Access Technologies*** | Wired Networks (e.g. Ethernet), Wireless LAN (IEEE 802.11x), Bluetooth, Ultra Wide Band (UWB), Fibre Optics... | GSM, GPRS/UMTS (2.5/3G), 3GPP LTE (4G), ... | IEEE802.16REVd (i.e. Wireless DSL), IEEE802.16e, IEEE 802.16m, Pre-standard Solutions (e.g. Samsung WiBro), ... | DVB-S, DVB-S2, DVB-RCS, SCPC, ..... |

Table 2.3: Access Technologies

### 2.3.2 Mobility Definitions

Different kinds of mobility definitions could be derived based on the network deployment scenarios.

**Global Mobility** occurs when the MN moves between access technologies involving a change in the IP link or subnet. Generally such mobility incurs both layer 2 and 3 mobility mechanisms.

**Intra-link Mobility** is the movement of MNs between different wireless APs within the same IP subnet. This kind of mobility involves only layer 2 mechanisms. Intra-link is often referred as intra-subnet handover since no IP link re-configuration is required upon movement. However some IP signalling may be needed to confirm whether or not the change in APs resulted in a change of IP subnets.

**Localized Mobility** occurs when the MNs movement is restricted over an access network. The area in which the MN moves may be restricted by geographical topology. However the actual geographical area could be very large, depending on the mapping between the wireless coverage area and network topology. Figure 2.2 illustrates the concepts behind the three mobility scenarios described.

## 2.4 Types of Handovers

### 2.4.1 Intra-subnet/Inter-subnet and Intra-technology/Inter-technology handover

Mobility between two access networks that are part of the same IP subnet and same broadcast domain is known as Intra-subnet handover.

An Inter-subnet handover results in the movement between two access networks that belong to two different IP subnets. This causes the L3 identifier (i.e. IP address) to change, giving rise to a need for a mobility management protocol to maintain session continuity. Inter-subnet handover involves both layer 2 and 3 mobility mechanisms and triggers delays which results in packet loss and jitter (i.e. QoS degradation).

When a MN moves between the same access-technologies, it is known as Intra-technology handover. Inter-technology handover occurs when a MN moves between different access-technologies (e.g. 802.11g to 802.16e). During an Inter-technology handover, a MN may move out of the coverage or footprint area of the radio access of one technology (e.g. 802.11g) and move into the coverage area of a different access technology (e.g. 802.16e). Inter-technology handover causes a change in the communication interface (i.e. L2 Identifier) being used by the MN.

Different combinations of Intra/Inter-subnet and Intra/Inter-technology handovers may exist. For example, an Intra-subnet handover may be accompanied by an Inter-technology handover, or, vice-versa. Alternatively an intra-technology handover may involve intra-subnet or inter-subnet mobility, which may be associated with a change in the L3 identifier of the MN.

### 2.4.2 Intra domain/Inter domain handover

A domain by definition could have several meanings. However, for the purpose of roaming, a domain could be defined as a single administrative entity which manages one or many networks. The administrative entity which may be a service provider, an enterprise or any organization is responsible for authenticating and authorizing a MN to access the various networks.

When a MN's movement is confined within a single administrative domain, it is referred as Intra-domain mobility. Intra-domain mobility could involve Intra/Inter-subnet, Intra/Inter-technology handover.

Inter-domain handover by definition provides mobility between two administrative domains. By default, Inter-domain handover is subjected to Inter-subnet handover since the two different domains exclusively have two different subnets. In addition it may be associated with either Intra or Inter-technology handover. Therefore, Inter-domain handover will consist of all the transitions/steps a subnet handover goes through with the addition of authentication to the new domain. The extra procedures will bring additional latencies during the overall handover process (i.e. L2 + L3). Figure 2.2 depicts the Intra and Inter-domain handovers consisting of Intra/Inter-subnet, Intra/Inter-technology handovers.

Based on the classification of various types of mobility and handover, different requirements on mobility management can be derived. For example, each of the categories of mobility has a

specific tolerance to packet loss during handover latency. Based on these tolerances a certain minimum mobility support will be required, which could be one of following:

**Seamless handover**: In this case, the handover occurs with no delay, and consequently no packet loss.

**Lossless handover**: In this case, the handover occurs with some delay, but mechanisms are in place to prevent packet loss.

**Session Continuity**: In this case, the handover occurs with some delay and some packet loss; however, the session will survive the handover and continue afterwards.

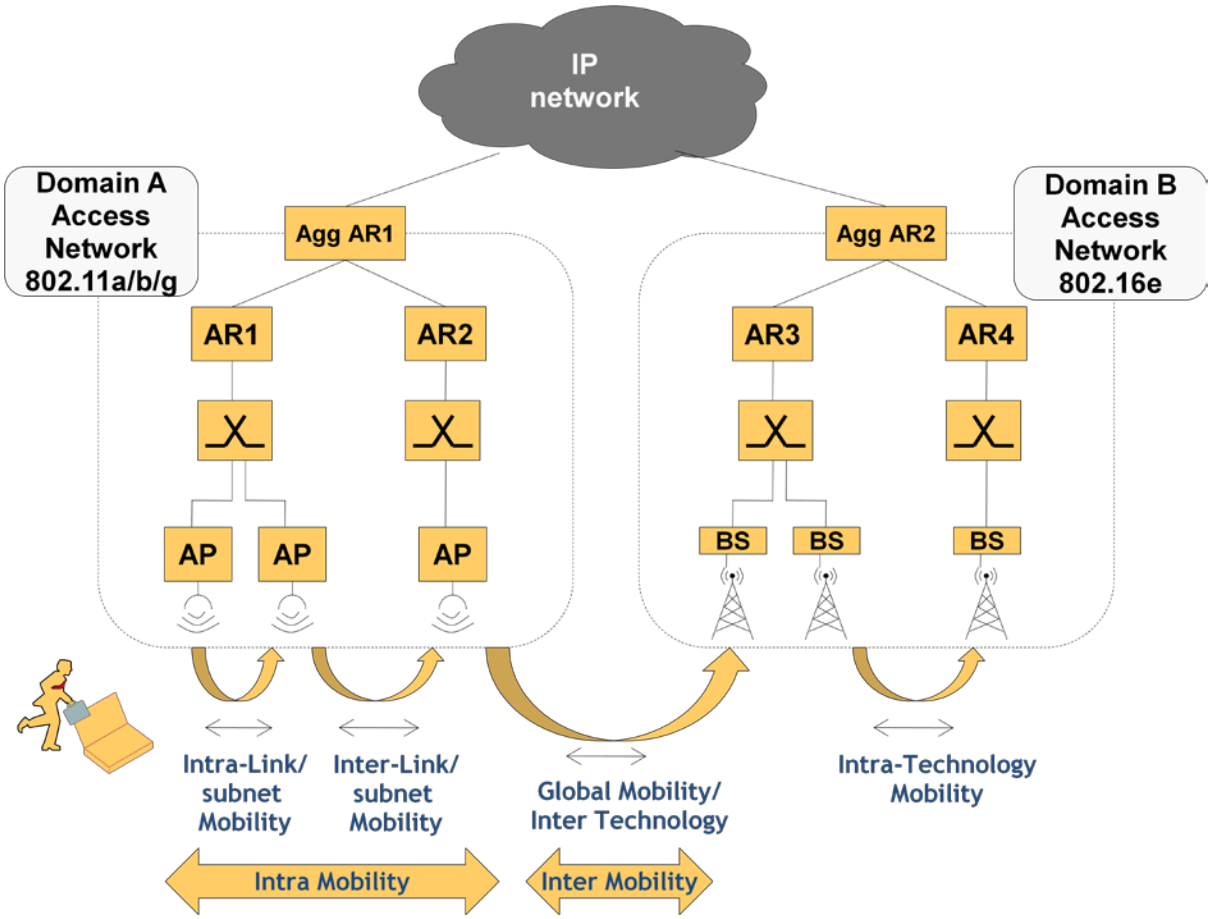


Figure 2.2: Various type of mobility

## 2.5 IP/Network Layer Mobility Management Protocols

### 2.5.1 Mobile IPv6 Handover Mechanisms

Due to various limitation of the IPv4 protocol, IPv6 has been chosen as the convergence layer for future heterogeneous access networks. Consequently, MIPv6 is meant to replace the IETF defined MIPv4 standard as the base mobility management protocol for NGNs. MIPv6 is incorporated by substantial changes to MIPv4, such as elimination of the Foreign Agent (FA) entity, security enhancements and route optimization.

The MIPv6 specification defined by the IETF provides transparent host mobility within IPv6 networks. MIPv6 assists a MN to freely move between IP subnets without change in its original IPv6 address configuration. This means that the MN is always addressable in the Internet by its Home Address (HoA). The HoA is the IPv6 address assigned to the MN in its home network. While away from the home network, a MN can still be reachable in the Internet, since packets can be routed to its HoA. In this way, mobility transparency of higher layer protocols (e.g. Transport layer or higher) is achieved.

MIPv6 arbitrarily allows a MN to change its location in the Internet when it moves from one IPv6 subnet to another. During such mobility, the MN will perform the MIPv6 handover procedure. The overall handover procedure of MIPv6 involves several stages which are listed below. Figure 2.3 illustrates the overall message flow for the MIPv6 protocol operation.

#### 2.5.1.1 Movement Detection

Movement Detection refers to the process by which a MN detects whether or not it has moved to a different IPv6 subnet. As a general rule, such movement can be detected when two events have taken place.

1. The current default router is not reachable, and
2. A new prefix has appeared on the link

The first event can be observed when a MN performs Neighbour Reach-ability Detection (NUD) on a continual basis to determine whether the current default router is still bi-directionally reachable. Briefly speaking, NUD works by maintaining a 'Neighbour Cache' to determine the

link layer address of the next hop node (either an on-link router or its current router). A detailed explanation of NUD can be found in [16][109][110]. The second event occurs in two ways: 1) The MN sends a Router Solicitation (RS) message, and, in response receives a Router Advertisement (RA) containing new prefix information; 2) The MN receives unsolicited RAs when it moves to a new network before the RA interval of the previously connected AR has terminated. The amount of time that elapses before a RA is received depends on the advertisement frequency. MIPv6 has a minimum RA interval time of 0.05 seconds.

#### 2.5.1.2 Address Configuration

When a MN moves into a new IPv6 subnet (i.e. foreign network), it must configure itself with an IPv6 address to use on the new network. This process of forming a new IPv6 address is known as Care-of-Address (CoA) configuration. The MN may use both stateless and stateful address auto-configuration mechanisms to form the CoA.

Stateless auto-configuration requires no manual configuration of hosts and minimal configuration of servers. A MN combines local information such as RA prefix information and a unique host identifier to form an IPv6 address (i.e. CoA in a MIPv6 scenario). Stateful auto-configuration allows a MN to obtain an IPv6 address or configuration parameters from a DHCPv6 [19] server.

Upon formation of a CoA, the MN must perform Duplicate Address Detection (DAD) in order to validate its new CoA, which is essentially a link local IPv6 address, against any other node that may have been assigned the same IPv6 address. In [16], a detailed explanation of DAD is provided.

#### 2.5.1.3 Binding Update and Binding Acknowledgement

Following the address auto-configuration, the MN must inform it's HA of its new CoA by sending a Binding Update (BU) message. The BU message is one of several MIPv6 message options encoded in a new header known as a *mobility header*. The purpose of the BU is to inform the HA of the MN's current address (i.e. CoA). The HA binds the MN's HoA with the CoA and stores it in a *binding cache.* When the HA receives a BU, it performs a number of actions before it can accept the BU message. Firstly, it checks the binding cache to see if an entry exists. If an entry does exist, then that entry is updated with the new information received. If there are no

entries, then a new one is created. The HA also defends the MN's HoA by performing DAD to validate that no other node on the home network has configured an IPv6 address that collides with the MN's HoA. The HA, upon validating the BU, sends back a Binding Acknowledgement (BA) message to the MN to indicate whether or not the BU has been accepted. Like the BU, the BA is also a mobility header. If accepted, the MN starts to receive IP packets in the foreign network.

#### 2.5.1.4 Authentication and Authorization

When an Inter-domain handover is encountered, the MN will have to utilize some form of AAA infrastructure to gain authentication and authorization for network access. Also, since MIPv6 will be considered as a separate specialized service, additional latencies will be incurred for authenticating and authorizing a MN for mobility services. Authentication and authorization for initial network access will occur before the MIPv6 service is requested by the MN. The details of the AAA infrastructure interaction which is necessary in order to authenticate and authorize the MN for network access and mobility services is explained in chapter 5.

#### 2.5.1.5 Message flow for MIPv6

In Figure 2.3, the detailed message flow of MIPv6 is presented, which also highlights the overall handover latency.

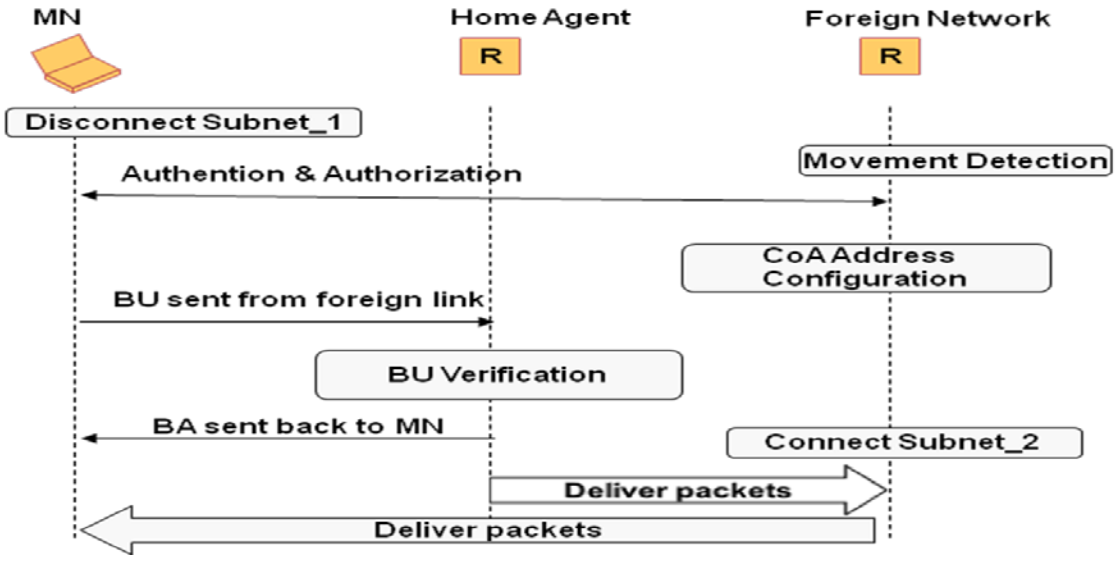


Figure 2.3: MIPv6 Message Flow

### 2.5.2 Fast Handovers for MIPv6

The latencies involved in the movement detection, CoA configuration, and CoA testing (i.e. DAD) in MIPv6 could be reduced if there is knowledge of the neighbouring ARs and subnet affiliations prior to handover. Such information would allow a MN to anticipate its attachment to a new router by asking its default router to provide the subnet prefix, IP address and MAC address of a target router attached to a neighbouring access point. The procedure of anticipating network layer mobility results in a *make-before-break* handover. In the following sections, the overall handover procedure for FMIPv6 is presented as a sequence of events. Figure 2.4 presents an overview of FMIPv6 handover and Figure 2.5 illustrates the overall message flows involved.

#### 2.5.2.1 Anticipation and Handover Initiation

FMIPv6 is designed to allow MNs to anticipate and initiate an IP layer handover through the use of link layer triggers. These link layer triggers are delivered to the network layer modules as events reporting changes with regard to the link and physical layer conditions. For instance, when the MN detects that its signal quality with its attached AP is going down or about to go down, the link layer sends a trigger to the network layer which in turn starts the IP layer movement anticipation and initiation.

During the anticipation phase, the MN sends a Router Solicitation for a Proxy Advertisement (RtSolPr) message to the default access router to resolve one or more AP Identifiers (AP-ID) to subnet-specific items of information [7]. The default router known as the pAR (Previous Access Router) replies with a Proxy Router Advertisement (PrRtAdv) message which contains the neighbouring router's advertisement that includes one or more [AP-ID, AR-Info] tuples [7]. Using this information the MN forms a new CoA (NCoA) while still being a part of the pAR's link. Hence, the latency incurred as a result of discovering a new prefix (in other words due to router discovery in MIPv6) is eliminated [7].

#### 2.5.2.2 Updating the Previous Access Router

After anticipating an IP layer handover, the MN will send a Fast Binding Update (FBU) message which contains the NCoA to the pAR. The purpose of the pAR is to provide local HA functionality to redirect the MN's traffic to its new location belonging in the nAR's link. The

pAR upon receiving the FBU will send a Handover Initiate (HI) message containing the prospective NCoA to the new AR (nAR) [127].

The HI message serves two purposes: firstly it establishes a tunnel between the pAR and nAR [127]. The purpose of the tunnel is to forward packets arriving at the Previous Care-of-Address (PCoA) to the NCoA. Such a tunnel remains active until the MN moves to the nAR's link and completes binding updates with its correspondents [7] [127]. Secondly, after the tunnel is set up, the nAR determines whether it is aware of any address duplication for the NCoA [7][127]. The nAR sends a DAD probe for the NCoA to verify uniqueness. If there is no collision, the nAR starts defending it. Otherwise, the nAR will assign a new NCoA on behalf of the MN. In either case, the nAR will respond back to the pAR with a Handover Acknowledgement (HAcK) message [7] [127]. If the nAR assigns the NCoA, the HAcK message will contain the assigned NCoA. Upon receiving the HAcK message, the pAR sends a Fast Binding Acknowledgement (FBack) to the MN. If HAck contains an assigned NCoA, the FBack must include it, and the MN must use the address provided in the FBack [7] [127].

#### 2.5.2.3 Moving to the New Access Router's link

As soon as the MN establishes link connectivity with nAR, it immediately sends an Unsolicited Neighbour Advertisement (UNA) message. When the nAR receives the UNA message, it immediately starts forwarding arriving and buffered packets to the MN. The UNA message is used to inform the nAR that the MN is now attached to its link and requests any buffered packets to be forwarded to the MN. This scenario is only valid when the MN receives the FBack message while it was still connected to the pAR's link. In the event the MN moves without receiving an FBack, the MN can start using its NCoA after sending a FBU from the nAR's link [7] [127]. If the nAR provides a different IP address to the MN to use, it should send a Router Advertisement with the "Neighbor Advertisement Acknowledge (NAACK)" option which contains an alternate IP address for the MN [7] [127]. In this case, the MN will resend the FBU. The nAR will tunnel the FBU to the pAR. If the nAR is already proxying the NCoA as a result of the HI and HAcK exchanged before the MN moved [7] [127], then, the pAR will only send the FBack message to the MN. If the nAR is not proxying the NCoA, then the pAR and nAR will exchange HI, HaCK and FBack messages as described in [7]. Hence, two types of operational modes in FMIPv6 can be defined based on the scenarios described above:

- the Predictive mode, and,
- the Reactive mode.

In the Predictive mode, the FBU is sent from the pAR's link and the FBack is also received in the pAR's link before it moves to the new link [7]. In the Reactive mode, the FBU is sent from the nAR's link [7]. The reactive mode also includes the case when FBU is sent from the pAR's link but the Fast Binding Acknowledgement (FBack) has not been received yet [7]. Therefore, in the reactive mode, long handover delays would be induced due to NCoA configuration and Binding Updates. Due to this reason, it is desirable that the FMIPv6 protocol always operates in the predictive mode. Given below is a diagram which illustrates the operations of the FMIPv6 protocol.

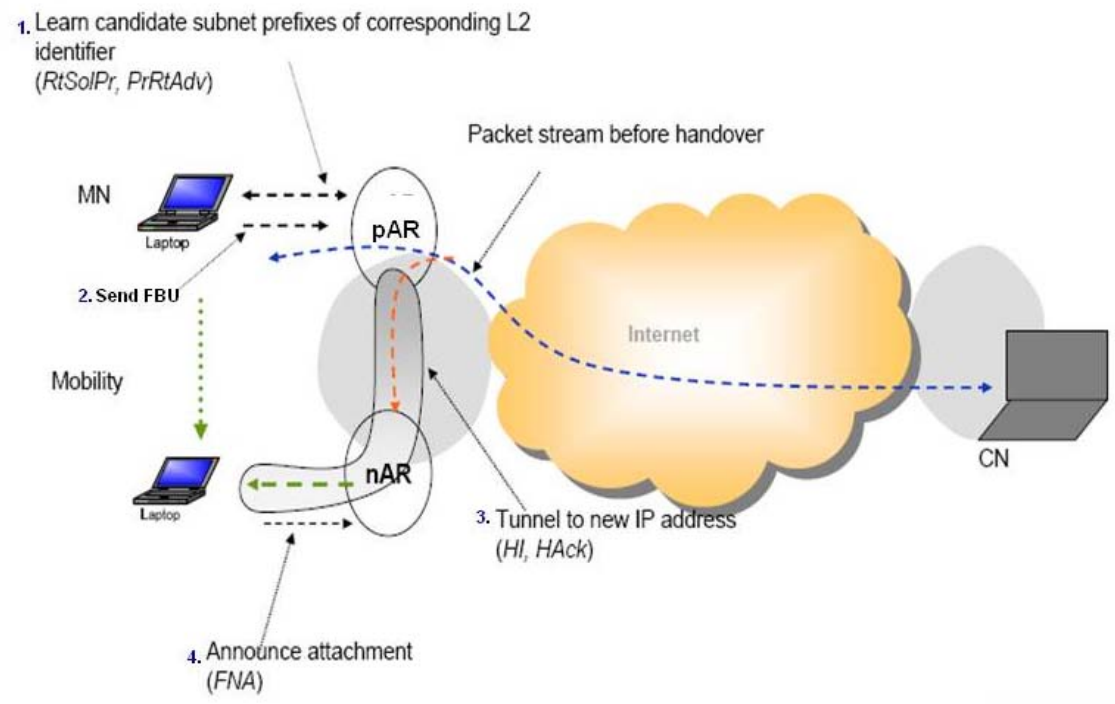


Figure 2.4: Overview of FMIPv6

In Figure 2.5, the detailed message flow of FMIPv6 is illustrated (as explained earlier) which also highlights the overall handover latency.

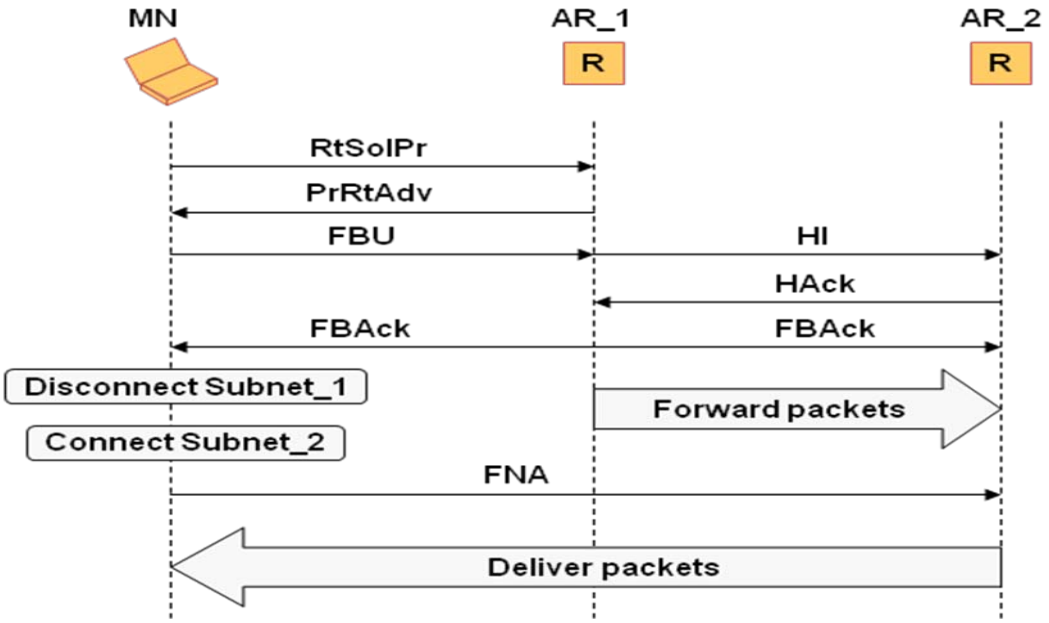


Figure 2.5: FMIPv6 Message Flow

### 2.5.3 Network Mobility (NEMO)

In order to address the requirement for transparent Internet access for mobile networks, the IETF has standardized the NEMO Basic Support Protocol. By definition, a mobile network (or Network that moves) is a network whose point of attachment to the Internet varies with time [128]. In terms of architecture, a mobile network is composed of Mobile Network Nodes (MNN) with some of the nodes (typically the most capable) acting as gateways to external nodes and infrastructure based networks such as the Internet. Like MIPv6, NEMO consists of a mobility anchor point (i.e. HA) in the home network with which it maintains a HoA. The MNN within NEMO that connects to the Internet is called the Mobile Router (MR) [128]. The handover procedure of NEMO is very similar to that of MIPv6. When a mobile network moves away from its home network, the MR acquires a CoA and sends a BU message on behalf of all the MNNs, which associates its Care of Address (CoA) with the network prefix [128]. Essentially, it creates a bi-directional tunnel between the HA and CoA of the MR [128]. The handover process of NEMO is very similar to that of MIPv6 and involves Movement Detection, Address Configuration and Sending Binding Updates. Figure 2.6 illustrates an overview of NEMO.

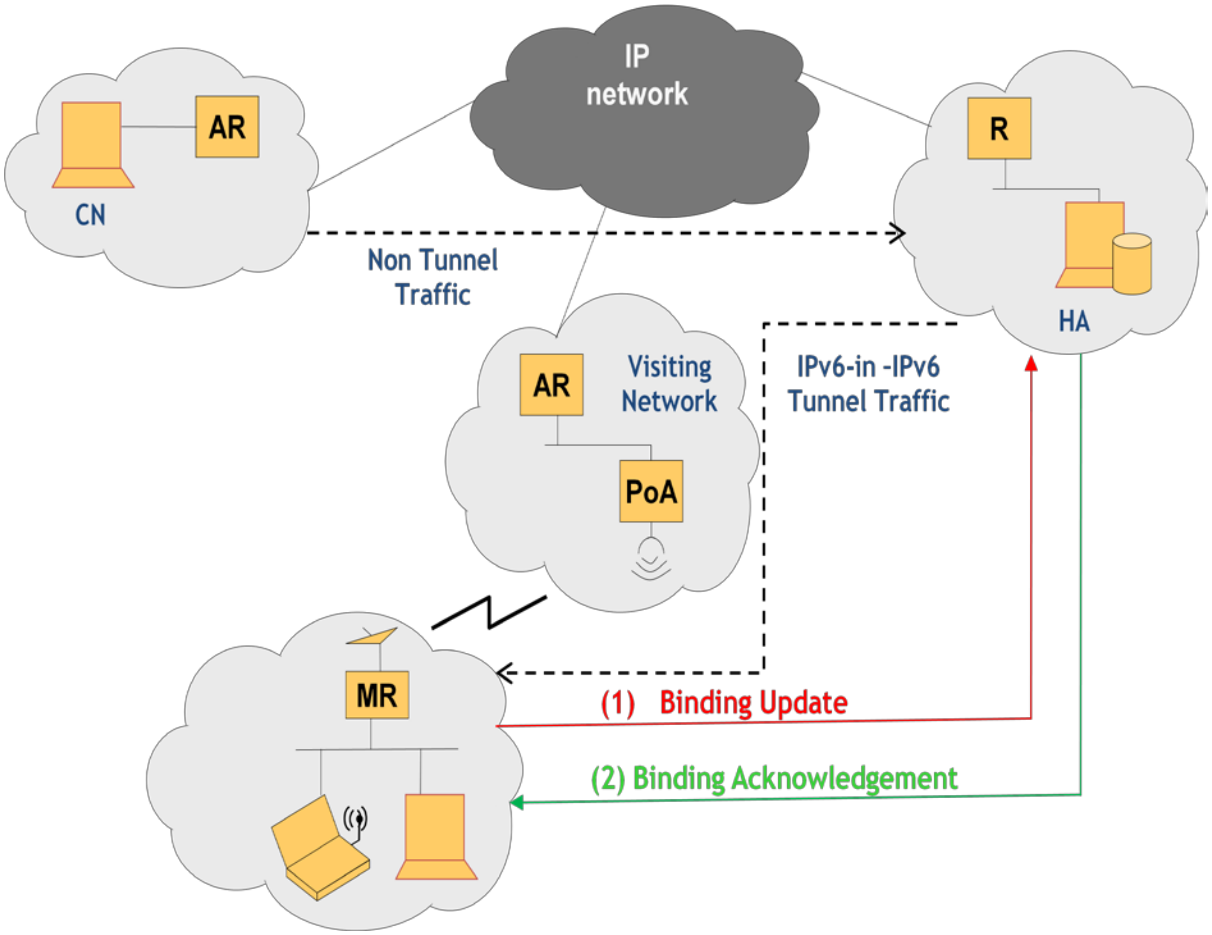


Figure 2.6: NEMO operations overview [10]

## 2.6 IEEE802.21 Media Independent Handover Framework

The IEEE802.21 WG, named the "Media Independent Handover (MIH) Standard WG [8], and officially formed in 2004 is developing a standard that provides generic link layer intelligence and other network related information to upper layers to optimize handovers between different heterogeneous media, such as 3GPP/3GPP2, and both wired and wireless media of the IEEE802.21 family" [13]. The framework relies on the presence of a mobility management protocol stack (e.g. MIPv6, FMIPv6 etc) to enable session continuity while the MN moves across heterogeneous access networks [13]. The IEEE802.21 WG has defined a new logical entity within the protocol stack of the network elements with a set of handover-enabling functions to assist in Inter-technology (i.e. Vertical) handovers.

### 2.6.1 IEEE 802.21 Media Independent Handover Function

The IEEE802.21 standard maintains that information about the condition and configuration of the surrounding networks will be received and transmitted by the MIHF, regardless of where it may be residing(i.e. on the MN or the access network).

The IEEE802.21 MIHF is a logical component that resides between L2 and the IP layer. Using Service Access Points (SAPs), both asynchronous and synchronous services are provided by the MIHF. Essentially, the SAPs are a list of primitives, where each primitive contains parameters that are defined utilising abstract data types. A unified SAP known as the MIH_SAP provides MIH services (i.e. Independent of access technologies) to upper layers. On the other hand, the lowers layers and provided services thorough media dependant SAPs known as MIH_Link_SAPs.

Three primary services that facilitate handovers between heterogeneous networks are defined by MIHF: MIH Event Services (MIES), MIH Command Services (MICS) and MIH Information Services (MIIS). Figure 2.7 shows the MIH Framework. A detailed discussion of each of the services is presented below.

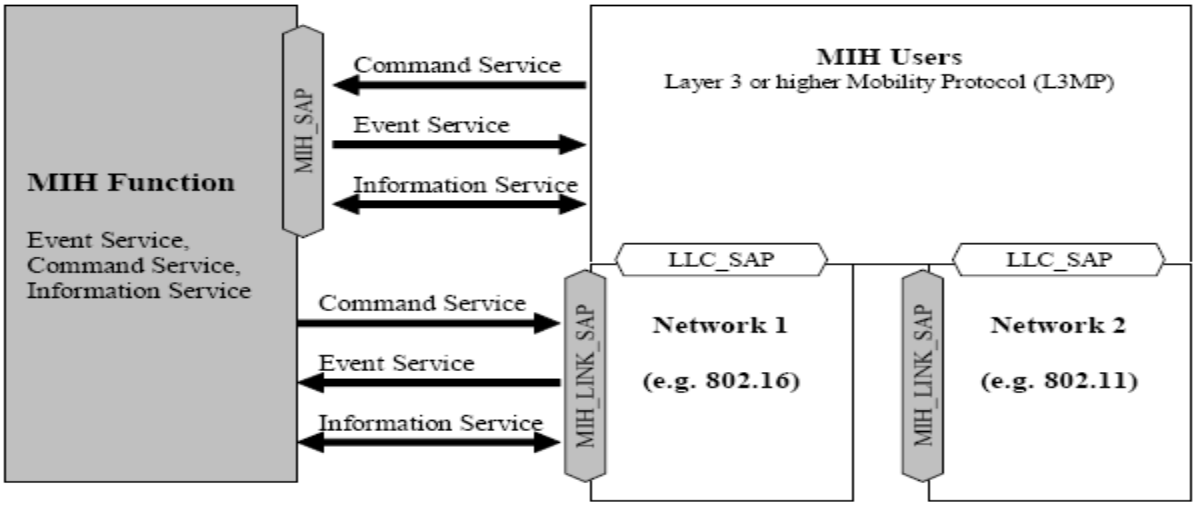


Figure 2.7: IEEE 802.21 Media Independent Handover Framework [13]

**Media Independent Event Service (MIES)** "provides an event reporting, event filtering and event classification service corresponding to the dynamic changes in link characteristics, link

quality and link status. The Event Service is also used to indicate management actions and command status on behalf of the" [13] management entity residing on the MN or a network entity. The MIES reports both local and remote events to the upper layers. A transport protocol is required in order to support remote events. Events originate from MIHF or lower layers within the protocol stack of a MN or network entity [13]. In the case of local events, the message propagates from the lower layer (i.e. PHY, MAC) to the MIHF and from there to the upper layers located within the same protocol stack [13]. In case of remote events, messages traverse across the network medium from one MIH entity to another located remotely [13]. Link Events originate from layers below the MIHF and terminate at the MIHF [13]. The Link Events are media-specific triggers which include, but are not limited to, various IEEE802 defined and 3GPP/3GPP2 defined interfaces [13]. The upper layer entities (i.e. MIH users) receive events through an event subscription mechanism. The event subscription consists of the Link Event subscription and the MIH Event subscription. Link Event subscription takes place when the MIHF subscribes with the link source entities (MAC or PHY layers) for Link Event notifications. MIH Event subscriptions are performed by the MIH users with the MIHF to select which events they will receive.

The MIES is used to anticipate handovers. For example, an indication that the link with which the MN is connected will cease to carry layer 2 data frames in the near future can be used by the MIH users to prepare for handover to a new PoA [13]. Some of the events that have been specified by IEEE 802.21 are "Link Up", "Link Down", "Link Detect", "Link Parameter Reports" and "Link Going Down". Mobility management protocols can use some of these events, for example, "Link Down" or "Link Going Down" as handover triggers. The MIES together with the QoS requirements of the applications, the reported link status, quality and characteristics, will be very useful for the mobility management entity to make handover decisions, i.e. decide which network and PoA the MN should switch to, and when the MN should make the handover.

**Media Independent Command Service (MICS)** uses the MIHF primitives to send commands from higher layers (e.g. Policy Engines, Mobility protocols) to lower layers [13]. The higher layers would pass commands regarding mobility and connectivity to lower layers, based on the status of the connected interfaces. In other words, MICS controls, reconfigures or selects an appropriate link through a list of pre-defined handover commands [13]. MIH user invoked

commands are known as MIH Commands. Commands originating from the MIHF are known as Link Commands. MICS can be both local and remote in nature. Local command messages propagate from the MIH users to the MIHF and from there to the lowers layers located within the same protocol stack. In case of remote commands, the messages traverse across the network medium from one MIH entity to another with the assistance of the MIH protocol. A typical use case of MICS is to inform the link layer to get ready before the actual handover happens, and to give the command to the link layer to switch from one network interface to another. It also allows the mobility management protocols to enquire about the link layer's status before making the handover decision.

**Media Independent Information Service (MIIS)** provides a framework and mechanism for an MIHF entity to discover available neighbouring network information within a geographical area to facilitate the handover process. In order to represent the information across different access technologies, the MIIS specifies a common way of representing this information by using a standard format such as XML (Extensible Markup Language), ASN.1 (Abstract Syntax Notation One), or TLV (Type Length Value), and this information can be obtained through a certain query/response mechanism [13]. Both static and dynamic information is provided by the MIIS. Examples of this static information include the names of service providers, MAC addresses, and channel information of the MN's current network neighbourhood. Dynamic information includes link layer parameters such as, data rate, throughput, and other higher layer service information needed to make an intelligent handover decision.

In the current 802.21 MIIS specification, a MN gets the heterogeneous neighbourhood information by requesting Information Elements (IEs) from the Information Server (IS). It also allows the neighbourhood information to be delivered to the MN using pre-defined Information Reports/IE Containers to effectively represent the heterogeneous neighbourhood information in TLV format. In the IEEE 802.21 draft, the defined IEs provide mostly static L2 information. The neighbouring network information discovered and obtained by the MIIS can be used in conjunction with user and network operator policies for optimum network selection. MIIS relies on existing media specific transport and security mechanisms or L3 transport and security mechanisms to deliver access to surrounding network information [13].

### 2.6.2 The MIH Protocol

The MIH protocol allows two remote MIH entities to exchange messages to support MIHF services. Remote MIHF can send each other reports and other information by utilizing the MIES, MICS and MIIS. MIH protocol is responsible for encapsulating the MIH services in MIH Frames and sending them over the physical link. Each of the physical links will require a slightly different method, but the reference models defined in [13] will take care of it. MIH protocol transactions are recognized through sequences of messages with a Transaction-ID. MIH protocol also uses a message acknowledgement service when the underlying transport used for the remote communication does not provide reliability. However, the acknowledgement service is not needed when the underlying transport provides reliable transport services. A detailed explanation of the MIH protocol can be found in [13].

#### 2.6.2.1 MIH protocol Frame Format

In Figure 2.8, a general frame format for the MIH protocol is shown. In the MIH protocol messages, all TLV definitions are assigned a boundary of one octet, and, as a result no padding is required. The frame carries a MIH Header, Source MIHF Identifier TLV, a Destination MIHF Identifier TLV, followed by the MIH service specific TLVs [13]. A detailed description of each of the components of the MIH protocol is provided in [13].

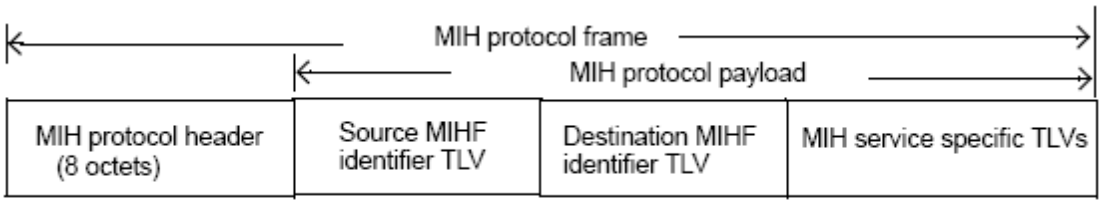


Figure 2.8: MIH Protocol Frame Format [13]

## 2.7 Motivation

This section aims to provide the motivation behind pursuing the field of research of this thesis; i.e. *Mobility Management across Converged –IP Based Heterogeneous Access Networks*. The motivation stems from the issues that need to be tackled for efficient mobility management to

enable the deployment of large IPv6 heterogeneous networks. In chapter 1(section 1.1.1), general details of the research issues were presented. In this section the motivation for the research undertaken in this thesis is presented in terms of the underlying issues that it aims to resolve.

### 2.7.1 Handover Enhancements for FMIPv6

The handover process for MIPv6 and FMIPv6 presented in section 2.5 of this chapter, gives an insight into the overall handover latencies incurred for each of the mobility protocols (i.e. MIPv6 and FMIPv6). The handover service for MIPv6 does not assure seamless movement and causes non-negligible handover latency without connectivity which causes data packets to be lost. The handover latency is mainly caused by *movement detection*, *address configuration*, and, *sending binding updates and Binding Acknowledgements*. The acceptable handover latency depends on the type of application in use. In section 2.4, handovers were classified based on packet loss tolerance. MIPv6 is not capable of providing transparent seamless mobility to most multimedia applications (real-time or non-real-time), such as VoIP, and Video Conferencing. However, MIPv6 is a matured solution and extensive research has been conducted by academics, industry and standards organizations, into enhancing its handover latency. As a result, MIPv6 handovers can be considered an exhausted area of research. An overview of the related work on MIPv6 handovers and their optimization is presented in the next chapter. It must be noted, that, MIPV6 is a base mobility protocol from which other extension protocols like HMIPv6 and FMIPv6 derive. In the context of NGNs, MIPv6 will exist as the fundamental mobility protocol which will provide basic mobility services for any roaming users requiring session continuity. Extension protocols like FMIPv6, which are designed to reduce the handover latencies of MIPv6 can be thought of as "*premium*" type services for users requiring seamless mobility.

Compared to MIPv6, FMIPv6 is relatively new and has not enjoyed the same mainstream attention that MIPv6 enjoyed. At the moment there seems to be great interest in FMIPv6 among the research community for its "*make-before-break*" handover capabilities which rely on lower layer triggers and neighbouring network information. As a result, FMIPv6 holds great potential for applying cross-layer information and network intelligence (i.e. neighbouring network information) to provide seamless mobility. Therefore, this thesis has chosen FMIPv6 as the protocol for its solutions for providing mobility management across heterogeneous networks.

Even though FMIPv6 stands as a promising solution for seamless mobility there are issues which need to be tackled for it to be successfully deployed in NGNs.

The FMIPv6 specification focuses on the protocol operation itself and neglects issues such as radio access network discovery and candidate AR discovery (i.e. how the network prefixes for the ARs are mapped with the corresponding L2 identifier). Although the anticipation mechanism specified by FMIPv6 is useful, it introduces additional problems.

**Need for standardized L2 triggers:** FMIPv6 relies on L2 triggers to anticipate and perform "make-before-break" type handovers. However, the FMIPv6 only mentions the use of L2 triggers it does not specify or define any such L2 triggers. Therefore, it is essential that standardized L2 triggers are defined to assist FMIPv6 in providing seamless mobility.

**Neighbouring access network discovery**: FMIPv6 does not address any radio access network discovery mechanism. Discovering the available PoAs by actively scanning all the channels provided by the neighbouring networks takes a considerable amount of time which makes a significant contribution to the overall handover latency. For example, in 802.11b, the L2 scanning can take 400ms to 800ms [57] and takes 90% of overall L2 handover time.

**Information exchange with neighbouring ARs**: How neighbouring ARs exchange information to construct PrRtAdv messages is not specified in the RFC of FMIPv6. The IETF SEAMOBY WG has developed the Candidate Access Router Discovery (CARD) protocol [101] to address this issue. However, it does not support the sharing of L2 information between the ARs.

**Reduced cost of anticipation**: There are three FMIPv6 signalling messages involved in the anticipation phase: Router Solicitation for Proxy Advertisement (RtSolPr), Proxy Router Advertisement (PrRtAdv) and Fast Binding Update (FBU). These messages are used for assisting IP movement detection and NCoA configuration. In FMIPv6, the L2 handover is triggered by the degraded link condition. It is likely that the MN will not be connected to the pAR long enough to send and receive all FMIPv6 messages. When anticipation is used, the MN may not have sufficient time to update the pAR with the FBU. As a result, if the MN has already lost connection with pAR, it will then be forced to operate in the reactive mode and the handover latency will increase consequently.

### 2.7.2 IEEE802.21 Assisted Cross Layer Techniques for FMIPv6 Optimization

FMIPv6 alone is not capable of tackling the advanced mobility scenarios in NGNs. There is great interest in the research community to interwork IEEE802.21 MIH services (e.g. MIES, MICS and MIIIS) with mobility management protocols to assist in seamless mobility. The potential of IEEE802.21 MIH services can help in tackling the FMIPv6 issues by providing:

**Generic L2 triggers** by utilizing the MIES. Various L2 triggers (e.g. Link Going Down, Link Up, etc) have been clearly defined by IEEE802.21 which can assist FMIPv6 in resolving the need for standardized L2 triggers

**Neighbouring Network Information** (both L2 and L3) information provided by the MIIS can help FMIPv6 tackle the issues related to radio access discovery, candidate AR discovery, and anticipation mechanisms.

**Intelligent Network Selection** can be possible with help of both MICS and MIIS. The diverse static information provided by MIIS, together with the dynamic neighbouring information (e.g. QoS information such as packet loss, available data rates etc) collected by MICS from candidate PoAs, can be utilized for intelligent network selection.

At the moment, there is lack of clearly defined and detailed interworking mechanisms between IEEE802.21 and FMIPv6 from standards bodies such as the IETF and IEEE. Moreover, the services defined by IEEE802.21 alone are not sufficient for intelligent seamless handovers across heterogeneous access networks. Current mobility decision engines do not take user, application, and context information into account. As a result, there is a need to define cross layer mechanisms which allow mobility or policy decision engines to acquire user, application, and context information to make informed and intelligent handover decisions.

Network Mobility will play an intrinsic part in 4G networks. Users are demanding Internet access not only from fixed locations (e.g., at home, at work, in hotels, etc), but also in public transportation systems (e.g. planes, trains, and buses). At the moment, NEMO has been specified by the IETF for supporting network mobility in vehicular environments. However, handover optimization for network mobility is often neglected and few research contributions address this. The handover latency for NEMO has been presented in section 2.5. Like MIPv6, NEMO suffers from long handover delays associated with movement detection; address configuration and

sending binding updates. For delay sensitive applications (real-time multimedia, time critical safety and traffic applications) such delays are unacceptable. In order to provide seamless mobility, it is essential that the handover latencies of NEMO be reduced. As a result, the potential for realising fast handovers in NEMO must be examined. In this regard, FMIPv6 can be used to support network mobility with minor protocol modifications. Also, IEEE802.21 MIH services could be utilized to support FMIPv6 to further optimize handovers in vehicular environments.

### 2.7.3 Service Authorization and Bootstrapping Framework for Mobility Services

Mobility will be a fundamental feature of NGNs. As a result, operators will charge users for mobility services and it is expected that a huge proportion of the operators' revenues will come from them. As mentioned earlier, the basic MIPv6 could be enriched with a set of additional features that provide optimized handovers services. For example, FMIPv6 which offers enhancements to the MIPv6 features can be considered a "premium" type service. Therefore, it must be noted that Mobile IPv6 and its extension protocols (FMIPv6 in our case) or any other services such as IEEE802.21 MIH Services, multi-homing, video streaming/conferencing need extensive authentication and authorization to maintain efficient accounting information and prevent potential security threats introduced by such services from being realised.

Based on the business entities described in section 2.2, various complicated scenarios could be envisaged taking into account whether the ASA or MSA are the same entity or not. In order to successfully deploy an efficient mobility service authorization framework, the business entities would have to be integrated within an AAA infrastructure. Therefore, a detailed service authorization framework needs to be defined taking into account all the required components; i.e., business entities such as ASA, ASP, MSA, and MSP, integrated within an AAA infrastructure.

### 2.7.4 IEEE802.21 assisted fast Re-Authentication for Handover Enhancements

It must be noted that additional latencies are incurred for network access authentication/re-authentication due to AAA services during handovers across heterogeneous networks. This is

due to the fact that existing re-authentication implementations run a full authentication method (a very time-consuming process) when a MN encounters a new authenticator (i.e. PoA), irrespective of whether it has been authenticated to the network domain recently and has unexpired keying material.

Moreover, different access technologies have different authentication techniques, which make the overall handover process more intrinsic and prone to long latencies. As a result a method independent re-authentication mechanism is required which will utilize cross-layer information, such as, information on candidate PoA, candidate PoA IP and MAC address, etc, to optimize and reduce handovers delays associated with re-authentication mechanisms in a heterogeneous access environment. Also, optimized re-authentication mechanisms could be considered as a “premium” service. Therefore, IEEE802.21 assisted fast re-authentications mechanisms will need to operate over an efficient service authorization and bootstrapping framework.

# CHAPTER 3- Survey of Research on Mobility Management across Heterogeneous IP-based Access Networks

## 3.1 Introduction

Mobility management across converged IP-based heterogeneous access networks is an area of active investigation by researchers in academia and industry. This chapter attempts to report, as far as possible, some of the related work that is of relevance to the research undertaken in this thesis.

## 3.2 Related Work on Mobility Protocol Optimizations

### 3.2.1 Host Mobility Management

As mentioned earlier in chapter 1, MIPv6 has been widely studied and is accepted as the fundamental underlying protocol for providing global mobility across converged IP-based heterogeneous networks (i.e. NGNs). Various results obtained from practical implementation or simulations, such as [73][74][76] respectively, have suggested the overall handover latency for MIPv6 is unacceptable for real-time or streaming multimedia traffic (e.g. VoIP, video-conferring, on-demand video etc). For instance, the authors of both [73] and [74] have found that MIPv6 takes an average of 3-4 seconds for a vertical MIPv6 handover to complete. Others studies such as [77][78] [79] have provided similar results.

The IETF has defined extension protocols, such as HMIPv6, PMIPv6 and FMIPv6 to tackle the issues associated with MIPv6 handovers, such as movement detection, CoA acquiring/forming and CoA registration delay to the HA and CN(s). Research conducted to optimize the issues associated with MIPv6 handover is reviewed in the following subsections.

**CoA Registration and Signalling Overhead Optimization**

In order to reduce the CoA registration (i.e. BU) delay and its associated signalling overhead, HMIPv6 has been defined. The introduction of a hierarchy only makes sense if the Mobility Anchor Points (MAP) are located between the MNs location and the HA/ CN locations. In [80], an analytical study has shown that the HMIPv6 outperforms MIPv6 by reducing the overall

handover latency when the MN roams within a single (i.e. micro) MAP. The research reported in [85] defines an optimized HMIPv6 handover mechanism where each AR collects information broadcast by neighbouring ARs. For this to work a neighbour AR discovery scheme was proposed. When a MN senses that it will perform a handover to a new network, it performs an Address Auto-configuration procedure on its Local CoA (LCoA) (Regional CoA and LCoA in case of handover to a new MAP domain) in advance using the neighbour AR information received from the current AR [85]. These features allow for a reduction in the average handover latency of 550ms for intra-MAP handovers and roughly 800ms for inter-MAP cases. Without such reductions the delays would cause unacceptable service disruptions during handovers in NGNs.

In [81], a fast macro handover scheme (FMHS) is proposed that reduces BU cost, in which a MN sends a BU message including the newly obtained Regional CoA (RCoA) to the previous MAP instead of its own home agent (HA) where several MAPs exist in the administration domain. The FMHS reduces by about 56% the binding update cost and shortens macro-handover delays compared to HMIPv6.

PMIPv6 is a network-based mobility protocol defined by the IETF NETLMM WG. Network-based mobility management enables IP mobility for a host without requiring its participation in any mobility-related signalling [8]. The network is responsible for managing IP mobility on behalf of the host by extending the MIPv6 signaling [8]. The mobility entities in the network track the movements of the MN and initiate the required mobility signalling on its behalf [8]. PMIPv6 is similar to HMIPv6 in the sense that it aims to optimize the handover latency by reducing the CoA registration and signalling overheads associated with MIPv6.

In [84], an experimental evaluation of MIPv6 and PMIPv6 is presented, which gives qualitative and quantitative analysis that highlights the main desirable features and key strengths of PMIPv6. However, the average latency is found to be 711 ms, which is quite high and unacceptable for many of the services in NGNs.

**CoA Formation and Movement Detection enhancement:**

The FMIPv6 protocol aims to reduce the handover latencies associated with the CoA formation and Movement Detection phases in MIPv6, with the aid of anticipation mechanisms using L2 triggers. A detailed explanation of the FMIPv6 handover process is provided in chapter 2

(section 2.5.2) of this thesis. The amount of research conducted in the area of mobility management using FMIPv6 across heterogeneous networks is much less compared MIPv6 and HMIPv6. A few of the relevant works are summarized in this subsection.

In [93] and [94], experimental evaluations of FMIPv6 over WLANs are reported. The test-bed was developed by implementing FMIPv6 as an open source code project [52]. The experiments conducted addressed both predictive and reactive handover. The FMIPv6 predictive handover was shown to have zero packet loss with an average of 33.2ms handover latency. An average of 1.52 seconds is required for a reactive handover. However, [93] and [94] report low handover latencies which are achieved by modifying the wireless drivers and using a secondary wireless interface for scanning purposes only. Such modifications are quite unrealistic (i.e. it cannot be expected that MNs will have a secondary interface just to reduce the L2 scanning time).

The current FMIPv6 specification defines a general and non-standardized L2 trigger model for seamless handover operation, but it does not address the exact timing and definitive criteria of the L2 triggers which have a significant effect on the handover performance of FMIPv6. In [73], a solution is proposed which considers the available timing and accurate criteria of L2 triggers. With the definitive L2 triggers, a practical mechanism has been defined which allows for low overall handover latency and packet loss during handovers. In order to study the impact of such definitive L2 triggers, an FMIPv6 test-bed was developed. The results obtained from it suggest that the overall FMIPv6 handover latency (for predictive cases) is roughly 1 second. Such delays are still very high and would cause undesirable service disruptions during handovers.

In [92], the Access Router Information Protocol (ARIP) is proposed which tackles the candidate AR discovery and radio access network discovery issues described in chapter 2 (see section 2.7) in one protocol suite. ARIP is designed to cope with heterogeneous networks as well as homogeneous networks and to be closely coupled with FMIPv6. The proposed mechanism has been evaluated by developing a practical test-bed which has shown the overall handover latency to be reduced to 250ms. In [101], the CARD protocol has been defined to address the issue of candidate AR discovery. However, the solutions proposed in [92] and [101] require major changes at the ARs and adds additional complexities to the network infrastructure.

Solutions which reap the individual benefits of both FMIPv6 and HMIPv6 in a single optimized handover solution have been proposed in [95] and [96]. However, such solutions are either based

on theoretical analysis or simulation models which fails to consider realistic deployment scenarios and also all the intricate layers of the overall handover process (e.g. scanning, network access authentication, etc).

Since FMIPv6 has been chosen for this thesis as the mobility protocol that will be investigated for handover optimization across NGNs, it is necessary to present the related work on securing FMIPv6 signalling. At the moment, the current FMIPv6 specification specifies a companion protocol SEND [37] to be applied to secure the FMIPv6 signalling procedure. However, it is unknown whether SEND will always be available on access networks where FMIPv6 is likely to be deployed. Since NGNs will be highly dependent on the AAA infrastructure, it is only rational to design solutions which are AAA reliant, in order to secure FMIPv6 signalling (e.g. FBU and UNA).

### 3.2.2 Mobility Management in Vehicular Environments

It has been mentioned earlier in chapters 1 and 2 that NEMO has been chosen as the underlying mobility protocol to provide a uniform environment for vehicular data communications that allows vehicles to stay connected using the best communications technology available both in the vehicle and in the infrastructure, wherever the vehicle is located. In fact, under CALM, MIPv6 and NEMO defined by the IETF are selected as two options for supporting host mobility and network mobility in vehicular communications. CALM has defined mechanisms for cross-layer interactions in [99] and [100]. However, the services provided by CALM are quite abstract and no concrete solution has been defined as of yet. Also, CALM makes no assumptions based on the long handover latencies associated with NEMO.

Quite a few papers which deal with tackling the handover latencies of NEMO have been published. In [87], a GNU/Linux OS based test-bed deployed in Louis Pasteur University's campus in France, demonstrated the applicability and feasibility of NEMO in real world deployments. However, [87] it failed to provide any quantitative results for NEMO handover latency.

In [88], a test-bed has implemented the NEMO basic support protocol and has identified problems in the architecture which affect the handover and routing performance. The handover latency found for the basic NEMO is roughly 2.7 seconds. Such delays would bring undesirable service disruptions during handovers in NGNs. To address the identified handoff performance

issue, the use of make-before-break handoffs with two network interfaces for NEMO has been proposed. A comparison study of handovers with NEMO with MIPv6 has shown that the optimized scheme provides near-optimal performance [88]. Several Route Optimization (RO) techniques have been proposed in the context of single-level and nested mobile networks, such as [89], [90], and [91] respectively. However, such solutions either require significant support from the network infrastructure, or introduce additional signalling overhead on the wireless link.

## • 3.3 Cross-layer Mechanisms to Enhance Handovers for NGNs

The literature that is available regarding cross layer mechanisms to enhance the Vertical Handovers for 4G networks is discussed in the following sub-sections.

### 3.3.1 Related Work on Optimizing Mobility Protocols utilizing IEEE802.21 MIH services

Formed in 2004, the IEEE802.21 standard WG is relatively new. So far, a lot of research effort has been made within the IEEE 802.21 WG itself, for standardization of the MIHF framework. The IEEE802.21 WG has liaised with the IETF MIPSHOP WG to define protocols for transport and other functions like discovery and security for 802.21 MIH services at Layer 3 in [11], [12], [58], [59] and [24]. However, very little research has been done to integrate the IEEE802.21 MIH services with mobility managements protocols (e.g. MIPv6, HMIPv6, FMIPv6 etc.) to optimize the overall handover process. In this subsection, an attempt is made to summarize some of the recent related research.

In [98], an enhanced handover scheme for MIPv6 across a heterogeneous access environment using IEEE802.21 MIH services to reduce the latencies associated with DAD is proposed. By utilizing the Layer 2 triggers, the proposed scheme reduces DAD delays, and the number of Layer 3 message exchanges during Mobile IPv6 handover is greatly reduced.

A HMIPv6 based solution using IEEE802.21 MIH services to design an efficient handover scheme is provided in [83], by defining various handover scenarios and strategies to deal with each scenario.

In [82], a fast vertical handover HMIPv6 (FVH-HMIPv6) solution has been proposed which uses IEEE802.21 cross-layer information to obtain domain prefixes of MAPs belonging to

heterogeneous neighbouring access networks, which is critical to the HMIPv6 handover latency. It is shown through analysis that FVH-HMIPv6 great reduces the handover latency compared to the original HMIPv6.

In [86], a novel PMIPv6 based solution is presented using MIH services to reduce the overall channel scanning time which can substantially reduce the Layer 2 handover delay. By using MIH services, a QoS-aware target PoS selection may be performed based on the information obtained from the negotiation. By utilizing ideas of FMIPv6, a proactive handover scheme for PMIPv6 was proposed. An efficient buffering scheme to allow reduction of packet loss during handover is also presented. The results show that the 802.21 MIH assisted PMIPv6 solution reduced the overall handover delay by 50% compared to basic PMIPv6.

### 3.3.2 Existing Research on Optimizing Re-Authentication latencies during Vertical Handovers

Very little research has been conducted to reduce the handover delays associated with the re-authentication process across heterogeneous access networks. The IETF has provided some solutions to reduce the handover delay when Extensible Authentication Protocol (EAP) (see chapter 5 section 5.3.2 for a detailed explanation of EAP) authentication is required. The PANA WG has proposed mechanisms to pre-authenticate users to a new domain while connected to their current PoA in [53]. On the other hand, the HOKEY WG has defined mechanisms in [60], [61], [62], and [63] for providing fast re-authentication mechanisms without re-executing a full EAP method and re-using EAP derived keying material for handovers. However, such solutions, which are either method specific or method independent in nature, suffer from issues such as high signalling overheads and require major changes to the EAP protocol.

## • 3.4 The Need for Further Research in Mobility Management across heterogeneous IP-based access networks

It is evident from 3.2.1 and 3.2.2 that most of the research efforts in [73-97] are focused mainly on optimizing the operation of the actual mobility protocol itself. None of the research work presented in the previous subsections (i.e.3.2.1 and 3.2.2) utilizes a cross-layer mechanism which would assist in optimizing the overall handover process. Moreover, as explained in earlier

chapters, cross-layer interaction will be crucial for enhancing mobility management for NGNs. Therefore, based on the related work presented in the previous sub-sections 3.2 and 3.3, there is scope for extensive research, such as:

- FMIPv6 has been acknowledged to be one of the most promising mobility management solutions for NGNs. Even though there is a lot of discussion in the research community at the moment (particularly in the IETF) centring around FMIPv6, there is no existing academic literature regarding optimizing the FMIPv6 handover process using cross-layer mechanisms (e.g. IEEE802.21 MIH services). As a result, extensive research is required to integrate FMIPv6 with the IEEE802.21 MIHF framework. Such work would also help the IEEE802.21 standard to define a much needed detailed analysis of the overall integrated FMIPv6 handover process, in terms of message flows and required service primitives.

- Mobility management in vehicular environments using cross layer mechanisms is a research area that has been completely neglected. Much work is needed to optimize the long latencies incurred by the NEMO handover process. Therefore, it is fundamental that fast handover mechanisms (e.g. FMIPv6) are in place to optimize the NEMO handover process using IEEE802.21 MIH services. However, at the moment no such work exists.

- As mentioned in chapter 2, mobility will be provided as a service in NGNs, which will be a major source of revenue for operators. Therefore a service authorization and bootstrapping architecture is required for the mobility protocols (e.g. FMIPv6). There is no existing work that defines a generic framework through which mobility protocols, like the FMIPv6 service could be authorized and bootstrapped (e.g. establishing SAs). This would allow for securing FMIPv6 signalling by dynamically establishing SAs between the MN and ARs.

It can be concluded that very little research has been done in the area of enhancing the EAP re-authentication mechanism to further optimize the overall handover process in NGNs. At the moment, no research work has been conducted which applies the cross-layers information (e.g. IEEE802.21 MIH services) to reduce the overall network access re-authentication delay. As a

result, an IEEE802.21 assisted re-authentication mechanism must be defined to optimize the handover process across heterogeneous access networks.

# Chapter 4- Optimized FMIPv6 using IEEE802.21 MIH Services in Vehicular Networks

## 4.1 Introduction

The provisioning of seamless mobility to vehicles across heterogeneous access networks is essential for the next generation's vehicular communication networks. A variety of access network technologies (e.g. 802.11a/b/g, WiFi, 802.11p, WAVE, 802.16 WiMAX, GPRS and UMTS networks) are converging their core network infrastructure to the Internet Protocol (IPv4/6) suite. While IPv6 is being chosen as an underlying convergence protocol for vehicle networking, the introduction of high speed Wireless Access in Vehicular Environments (WAVE) is necessitated by the need to support 'breakthrough' safety and commercial applications in Intelligent Transportation Systems (ITS). In particular, the new emerging 'infotainment' applications call for the vehicular networks to support multimedia and real-time services.

In order to enable MNs and networked vehicles to seamlessly roam across heterogeneous networks while enjoying a plethora of 'all-IP-based' services, there are many challenges arising from the need for inter-technology 'vertical' handovers. As mentioned in earlier chapters, Mobile IPv6 has been widely accepted for providing IP mobility solutions across heterogeneous access platforms. Since MIPv6 was designed to support the mobility of single mobile hosts, the IETF NEMO (Network Mobility) WG has extended it to support the mobility of moving networks.

As an extension to the Mobile IPv6 protocol, the NEMO Basic Support [15] is concerned with the mobility of an entire network which dynamically changes its Point-of-Attachment (PoA) (i.e. Access Points, Base Stations) and thus its reachability in the Internet. Its main objective is to maintain session continuity between the Mobile Network Nodes (MNNs) and CNs while the Mobile Router (MR) changes its PoA. The MNNs behind the MR are IPv6 nodes and do not need to register or bind their home addresses with the HA individually. The MR, acting as a gateway between the inter-vehicle network and the network infrastructure, updates its change in IP subnets at the HA by sending a prefix-scope BU message that associates its CoA with the Mobile Network Prefix (MNP) used by MNNs.

CALM (Continuous Air interface for Long and Medium range) is a family of umbrella protocols being developed in ISO/TC204/WG16 ("Wide Area ITS Communications") in order "*to provide a uniform environment for vehicle data communications that allows vehicles to stay connected using the best communications technology available both in the vehicle and in the infrastructure wherever the vehicle is located*" [14]. In fact, under CALM, MIPv6 and NEMO are selected as two options for supporting host mobility and network mobility in vehicular communications.

Handover performance plays a crucial role in the Quality of Service (QoS) provisioning for real-time services in heterogeneous networks. The period during which the MN/MR looses connectivity with its current link till the time it receives the first IP packet after connecting to the new link is known as the *handover latency*. The overall handover latency in NEMO and MIPv6 consists of Layer 2 (L2) latency and Layer 3 (L3) latency. The L2 handover latency is the period when the MN/MR is disconnected from the air-link of the current Access Router (AR) till the time it successfully accesses the air-link of the new AR. The L3 handover latency is comprised of the latencies incurred during the IP layer movement detection, network re-authentication, CoA configuration and BU. The Fast Handover for Mobile IPv6 (FMIPv6) protocol, which was developed within the IETF MIPSHOP (Mobility for IP: Performance, Signalling and Handoff Optimization) WG can reduce handover delays in MIPv6 with the help of L2 triggers.

FMIPv6 reduces the handover delay by exploiting various L2 triggers to prepare a New CoA (NCoA) at the new AR (nAR) while being connected to the link of the previous AR (pAR). It relies on the pAR to resolve the network prefix of the nAR based on the L2 identifier reported by the link layer triggers in the MN. Note that although FMIPv6 was originally designed to reduce the handover delay in MIPv6, it can also be used to support NEMO after minor extensions. The idea is very simple: the traffic addressed to MNNs in a Mobile Network would need to be tunnelled to the MR's CoA; the MR here will be treated like a MN by FMIPv6 for traffic redirection between the pAR and the nAR using the binding of the Previous CoA (PCoA) and the NCoA maintained at the pAR. The overall handover process (i.e. handover message signalling) would be identical to the procedure described in the original FMIPv6 RFC [7] with minor extensions. Details of the FMIPv6 extensions will be discussed later in sub-section 4.3.

As mentioned earlier in the previous chapters, the Media Independent Handover (MIH) Standard WG is developing a standard, namely, IEEE802.21 that provides generic link layer intelligence

and other network related information to upper layers to optimize handovers between heterogeneous media, such as 3GPP/3GPP2, and both wired and wireless media of the IEEE802.21 family. Considering the overlap of work in IEEE802.21 and CALM with respect to vertical handovers using cross layer mechanisms, a liaison between the two groups responsible is being discussed. The IETF MIPSHOP WG has liaised with the IEEE802.21 WG to investigate the delivery and security issues of transporting MIH services over IP.

In this chapter, the potential of applying FMIPv6 in vehicular environments is investigated. By optimising the handover procedure of the FMIPv6 protocol in vehicular environments using IEEE802.21 Media Independent Handover (MIH) services, with the aid of the lower three layers' information on the MN/MR and the neighbouring access networks, the radio access discovery and candidate AR discovery issues of FMIPv6 are tackled. An 'Information Element Container' is designed to store static and dynamic L2 and L3 information of neighbouring access networks, and the use a special cache maintained by the MN/MR is proposed to reduce the anticipation time in FMIPv6, thus increasing the probability of the predictive mode of operation.

Furthermore, a cross-layer mechanism is proposed for making intelligent handover decisions in FMIPv6. Lower layer information on the available links obtained by MIH services as well as the higher layer information such as Quality of Service (QoS) parameter requirements of the applications is used by a Policy Engine (PE) to make intelligent handover decisions. It will be shown through analysis and simulations of the signalling process that the overall expected handover (both L2 and L3) latency in FMIPv6 can be reduced by the proposed mechanism.

## 4.2 Problem statement

The latencies incurred during a typical NEMO handover are unacceptable for multimedia and delay sensitive vehicular (e.g. safety) applications. In order to fully appreciate the proposed mechanism of applying FMIPv6 using IEEE802.21 MIH services in vehicular environments, it essential to understand the issues associated with NEMO handovers. A detailed message flow of the overall NEMO handover process is illustrated in Figure 4.1. Please note that in chapter 2, an overview of the NEMO protocol has been provided.

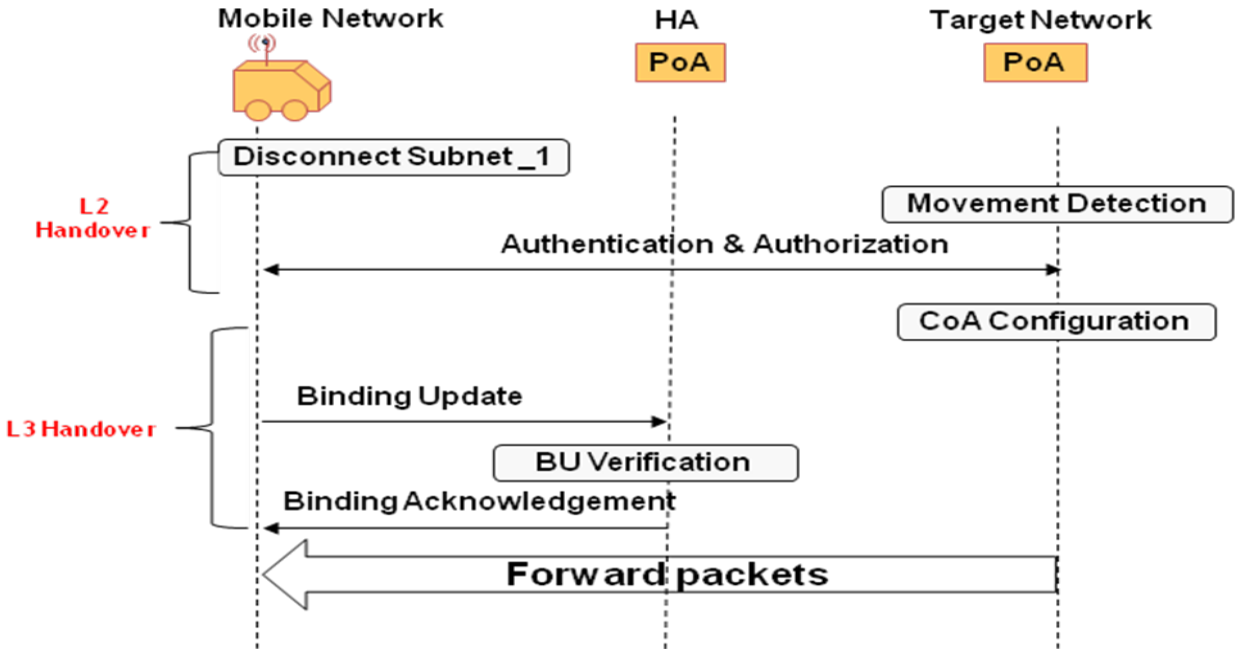


Figure 4.1: NEMO Handover Message Flow

Based on the message flow shown in Figure 4.1, the handover procedure is explained in the following steps:

- Service Authentication and Authorization: When a handover is encountered, some form of AAA infrastructure will be utilized to grant the MR authentication and authorization for network access. This step will only be encountered when the MR needs to be authenticated and authorized for services such as network access and mobility services.
- IP Movement Detection: consisting of determining if an IP subnet change has occurred. Like MIPv6, NEMO also relies on RA messages for IP movement detection.
- New Address Configuration: When the vehicle moves to a new IPv6 subnet, the MR generates a new CoA with the new subnet prefix contained in the RA packet. In order to verify the uniqueness of this CoA, it should run DAD.
- Binding Update: After the CoA has been formulated and configured, the MR sends a BU message to inform its' HA of the change of location. The HA validates the BU message in exactly the same way as in MIPv6. After BU validation, the HA sends a BA message back to the MR. Upon reception of the BA message, the MR starts receiving IP packets in the new subnet.

In Figure 4.2, an illustration of the NEMO handover process with respect to time is shown.

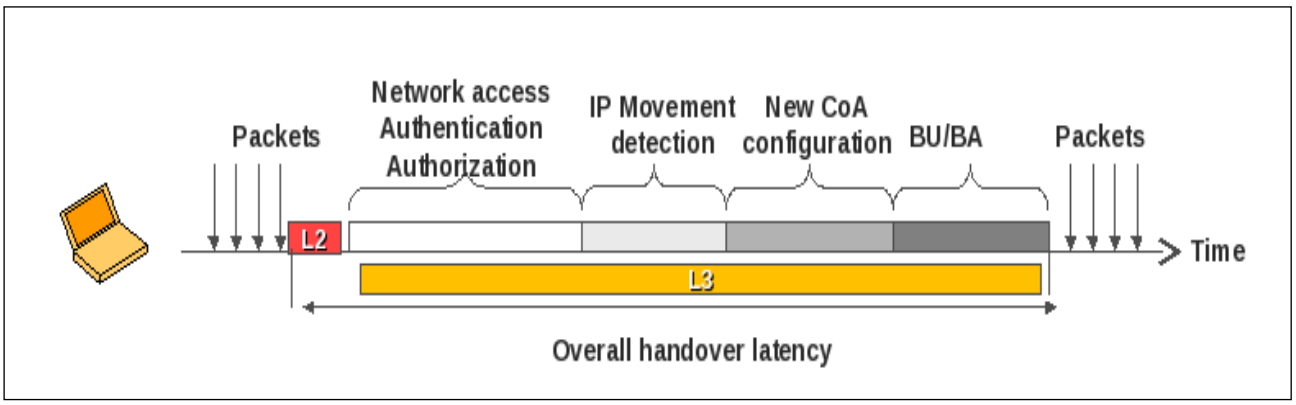


Figure 4.2: NEMO handover process with respect to time

## 4.3 Improving FMIPv6 performance with IEEE 802.21 Services in Vehicular Networks

In chapter 2, a detailed explanation of the handover issues related with FMIPv6 as a standalone protocol has been provided. The main issues that were identified were *neighbouring access network discovery, information exchange with neighbouring ARs*, and *the cost of anticipation*. It has also been mentioned earlier in chapters 1 and 2, how IEEE802.21 MIH services could be utilised to provide a cross-layer mechanism to optimize FMIPv6 handovers and tackle the issues associated with them. Before delving deeper in order to understand the proposed mechanism, it is important to present the overall network architecture. In the following section the architectural model for the proposed mechanism is presented.

### 4.3.1Architectural Overview

The network architecture considered in this chapter is illustrated in Figure 4.3. In general, handover is an intricate process which requires co-operation of both the network infrastructure and the MN in order to meet the demands of network operators and end-users [13]. As illustrated in the architectural model in Figure 4.3, the MIHF instances on different network entities are communicating with each other for various purposes. Note that this architectural model is an instantiation of the communication model developed in this chapter.

The different network entities along with their functional components are defined as follows:

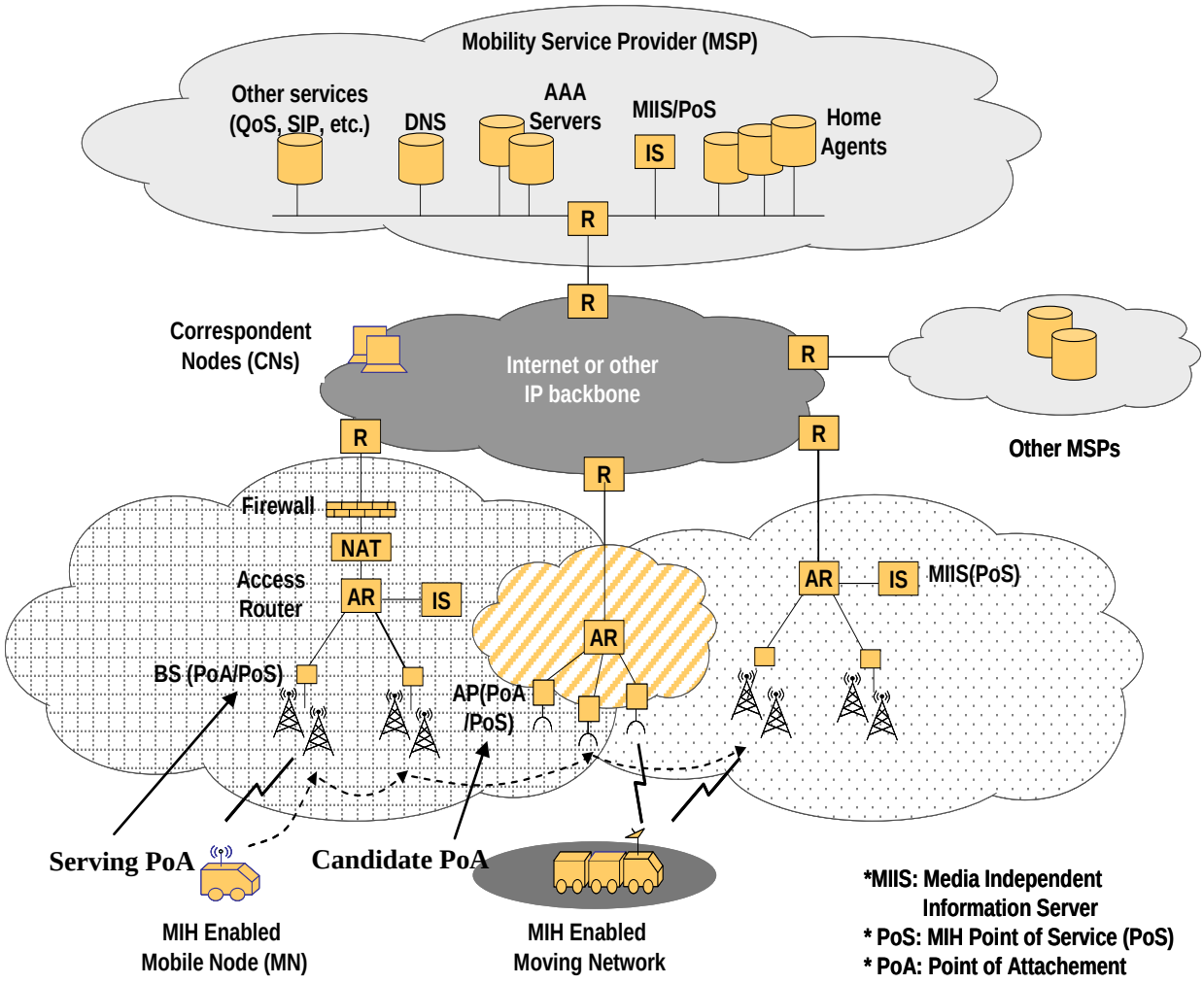


Figure 4.3: Architectural Overview

- **MRs/MNs**

The MRs/MNs are assumed to be MIH capable multi-modal devices with a protocol stack that is described in [13].

- **MIH Point of Service (MIH PoS) on the network entity - Serving PoA**

This a network-side MIHF instance that exchanges MIH messages with a MR-based MIHF. For every MIH enabled MN it communicates with, this network entity contains an MIH PoS. More than one MIH service can be hosted by a single MIH PoS. The same MIH network entity is capable of including multiple MIH PoSs to provide MIH services to respective MNs [13]. In Figure 4.3, the MIH PoS is collocated with a PoA (i.e. AP or BS).

- **MIH Point of Service (MIH PoS) on the network entity - Candidate PoAs**

This is a network-side MIHF instance that includes a candidate PoA for the Mobile device. A candidate PoA is an attachment point the mobile device is aware of but not currently attached to. However, when the handover happens, it may become the target PoA.

- **Information Server (IS)**

The IS is a network entity which serves as a MIH PoS but is located deeper in the access network. The IS could be thought of as the network knowledge reservoir which can be used to provide essential network related information, e.g., list of network providers, PoA MAC address, channel information, higher layer services etc, which may allow for optimized/enhanced network selection [13].

- **ARs**

In the proposed mechanism, the ARs are referred to the pAR and the nAR. The ARs are MIHF enabled and assumed to have the protocol stack of a normal IP AR.

### 4.3.2 Extending FMIPv6 to Support Network Mobility Solution – NEMO

As mentioned in section 4.1, FMIPv6 could be used to support network mobility, but needs minor extensions in order to fulfil the mobility requirements of a vehicular environment. The necessary extensions will include extending the FBU, HI, HAck, FBack and UNA messages defined in the FMIPv6 specification [7]. The extensions are as follows:

***The FBU message*** **-** A new Flag Option(R) will be needed in the original FBU message to distinguish whether the message sender is a single MN or a MR of a mobile network. The R flag is set to be 0 for a MN and 1 for a MR. A new Mobility Header Option will be needed to carry the Mobile Network Prefix (MNP). Upon receiving a FBU message, the PAR will first check the R flag. If R is 0, i.e. the FBU is sent from a MN, and the FMIPv6 will operate as originally defined.

If R is 1, the pAR will understand that the FBU is sent from a MR of a mobile network and that it needs to forward incoming packets that are destined to the mobile network of the MR. If the MR is operating in *explicit mode*, it will include the MNP as a mobility header option in the FBU. The pAR, upon receiving the FBU will then find out the MNP from the Mobile Header

option and tunnel the packets with this MNP (destined to the MNNs in the mobile network) to the nAR during handovers.

On the other hand, if the MR is operating in *implicit mode*, then, the MR does not include any MNP, and the pAR can use any mechanism (e.g. static configuration) to determine the route to the MNNs. The MNP message format is provided in [15]. The rest of the message processing and operation is the same as that described in [7].

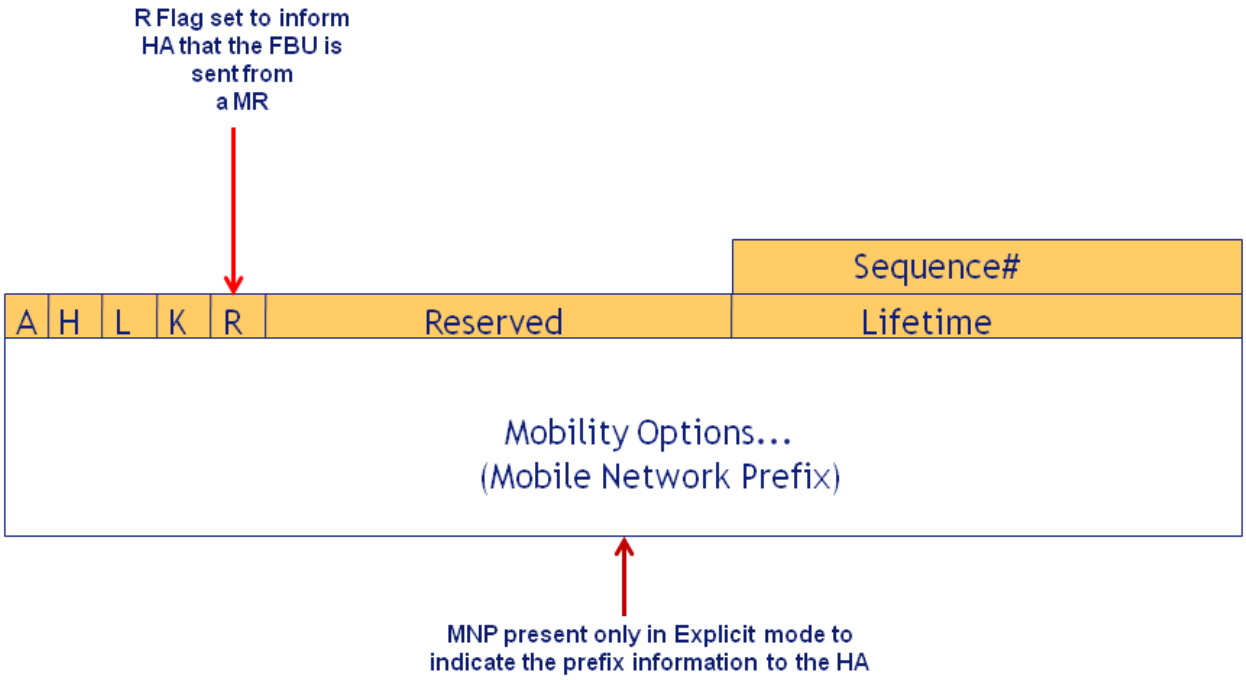


Figure 4.4: FBU message extension

***The FBack Message*** - A new Flag Option(R) will be needed in the original FBack message to distinguish whether the FBack message receiver is a single MN or a MR of a mobile network. The R flag is included to indicate that the Home Agent which processed the corresponding BU supports MRs. If the FBU is accepted but the NCoA is invalid (i.e. status is 1), then a new NCoA is supplied as an "alternate" CoA. Also, if the MNP is not accepted by the nAR, then a new MNP option will be included in the FBack message. The rest of the message processing and operation is the same as that described in [7].

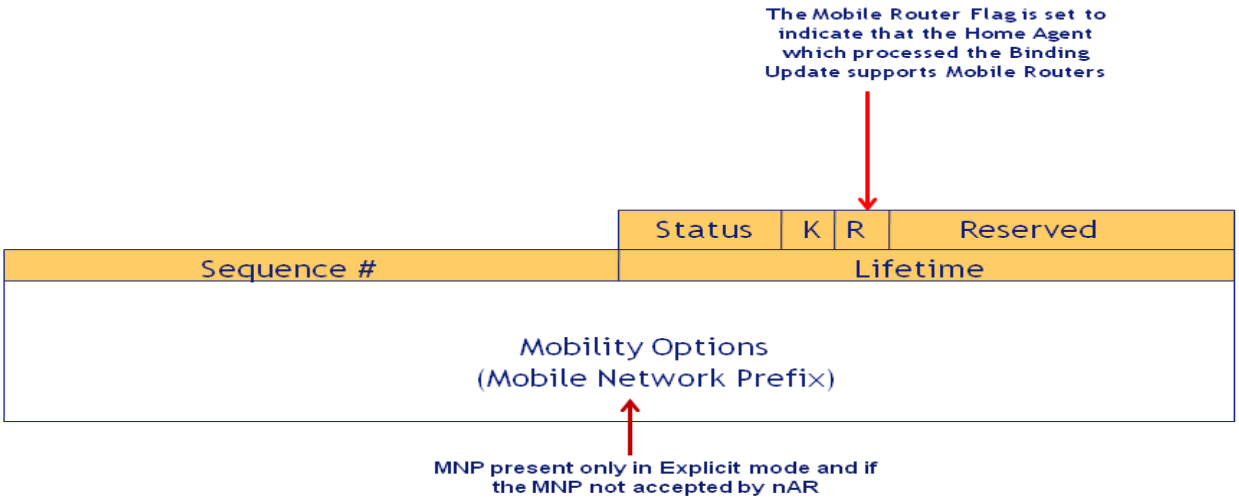


Figure 4.5: FBack message extension

***The HI message*** – The NCoA can be transmitted between the pAR and the nAR using one of the "Options" fields of the HI message. If the MR is operating in *implicit* mode, then the MNP is also included as an option. Both the pAR and the nAR could maintain a Prefix Table [7] for preventing a clash between a newly claimed MNP and a MNP that is being used. The mechanism for tackling duplicate MNPs is out of the scope of this thesis. The rest of the message processing and operation is the same as that described in [7].

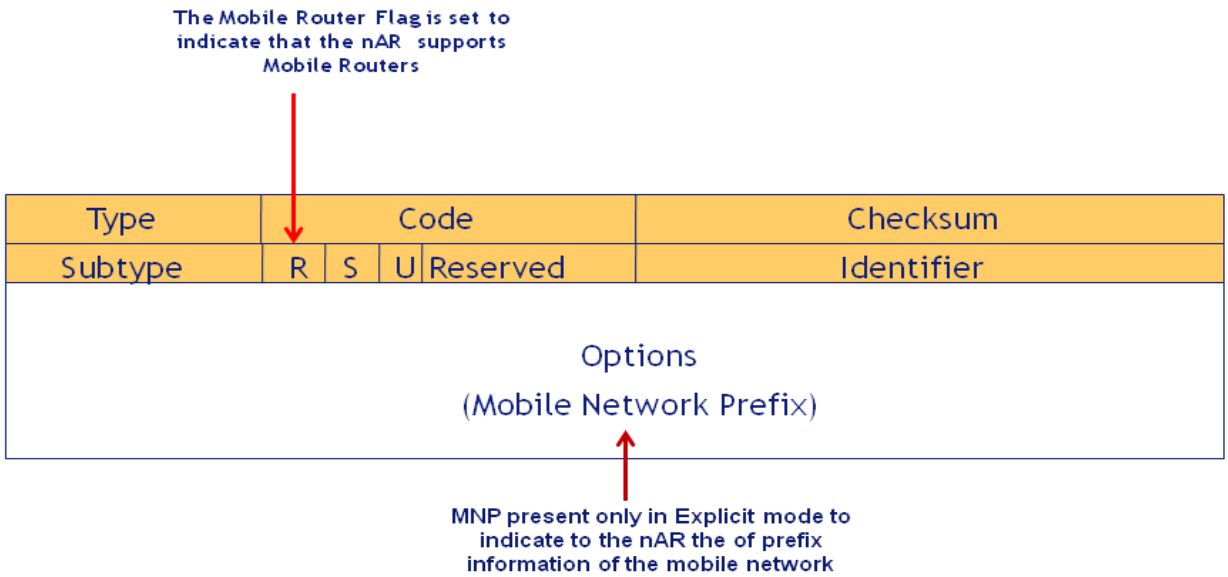


Figure 4.6: HI message extension

***The HAck message*** - should contain new status results indicating success or failure in accepting the NCoA and MNPs maintained by the MR. If the nAR does not accept the MNPs, then it will include new MNPs. The rest of the message processing and operation is the same as that described in [7].

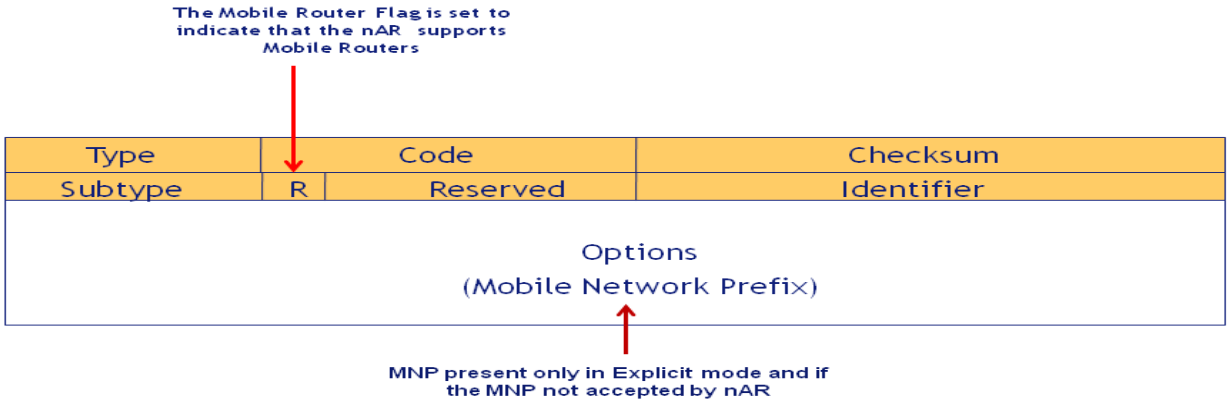


Figure 4.7: HAck message extension

***The UNA Message:*** In the Predictive mode of operation, the UNA message processing and operation is the same as that described in [7]. However, in the Reactive mode of operation, the UNA will include the MNP as a mobility header option. In case of address collision, the nAR may wish to assign a MNP to the MR different from the one in the UNA message. In such a case, the nAR must send a Router Advertisement with a NAACK option containing a new MNP. As mentioned earlier, the mechanism for tackling duplicate MNPs is out of the scope of this thesis.

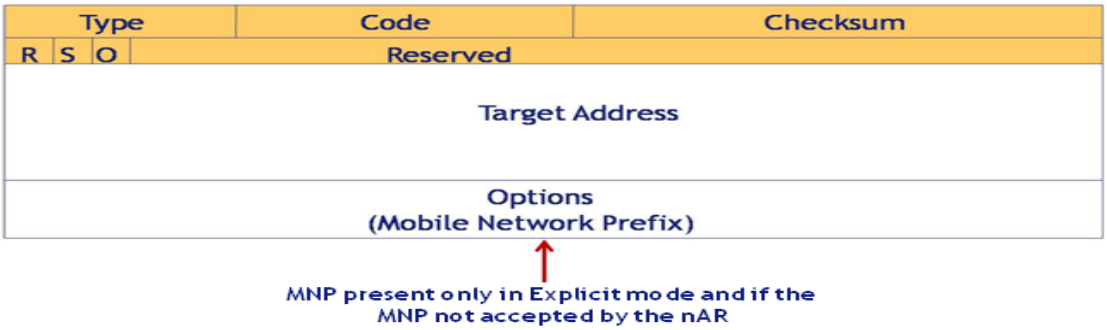


Figure 4.8: UNA message extension

### 4.3.3 Overview of the 802.21 Assisted FMIPv6 Mechanism

In this section, IEEE802.21 MIH services have been utilized to assist FMIPv6 to enhance the overall handover performance in vehicular environments by addressing the issues discussed in Section 4.2 as follows:

**1)** A Heterogeneous Network Information (HNI) Container has been defined to facilitate the storage and retrieval of the L2 and L3 static information of neighbouring networks obtained through the IEEE 802.21 MIIS. The IE known as the 'Subnet Prefix' is used to provide subnet prefixes of neighbouring ARs. Alongside the L2 information, they form the proposed pre-defined Heterogeneous Network Information (HNI) container/report. The IEEE 802.21 draft has defined a PoA container and an Access Network Container (ANE) [13] which includes many IEs such as MAC address, channel range, Network Type, Cost, Roaming Agreements, and Network Security. Instead of including all of the IEs from these two containers only the ones which can further optimize the proposed mechanism have been selected and put in a single IE container which is known as the HNI container. Having a single predefined HNI container will be ideal in vehicular environments and will help in reducing the message overheads, processing and lookup/indexing times.

The handover latency caused by the radio access discovery in FMIPv6 will be eliminated by using the L2 link information retrieved from the MIIS. Furthermore, from the L3 information of corresponding PoAs, the MN will learn of subnet prefixes of the nAR and form the NCoA prior to handover. This eliminates the router discovery time and optimizes the L3 handover latency in FMIPv6. Note that the HNI Report maintained by an IS will be similar to the mapping table maintained by the ARs for resolving L2 Identifiers of corresponding subnet prefixes. This could eliminate the need for ARs to exchange neighbouring information for maintaining the mapping table thereby tackling the candidate AR discovery issue in FMIPv6.

**2)** In order to reduce the adverse impact of the long anticipation time in FMIPv6, a Neighbouring Network Report (NNR) Cache is created to be held in the MR for storing and maintaining the HNI Report. This would help to reduce the number of signalling messages during the anticipation phase thereby reducing the overall anticipation time. The HNI Report will be delivered to the MN through the 'MIH_Get_Information' service primitives. By reducing the

anticipation time, the probability of operations in predictive mode is increased. Also the CoA configuration time can be reduced, thus the L3 handover latency is reduced.

**3)** The MICS is used to collect/obtain dynamic QoS link layer parameters directly from MIH enabled Candidate PoAs. Dynamic neighbouring network information includes packet loss rate, average packet transfer delay, signal-to-noise ratio (SNR), available data rates, etc.

**4)** A new MICS service primitive is defined for requesting application QoS requirements, and a new MIES is defined for delivering the application QoS parameters to the policy engine. A cross-layer mechanism is proposed for intelligent handover decision making by using the static and dynamic information of neighbouring networks, the local link condition and application QoS requirements.

### 4.3.4 The IEEE 802.21 MIH Services To Be Used

A subset of existing IEEE802.21 MIH services is utilized to enhance the handover process in FMIPv6. Their corresponding primitives and parameters are listed in Table 4.1.

| **Primitives** | **Service** | **Parameter** |
|---|---|---|
| MIH_Link_Going_Down | MIES | MN MAC Addr, MAC Addr of Curent PoA |
| MIH_Link_Up | MIES | MN MAC Addr, MAC Addr of new PoA, Link ID |
| MIH_Link_Down | MIES | MN MAC Addr, MAC Addr of new PoA, Reason |
| MIH_MN_HO_Commit | MICS | Old Link ID, New Link ID |
| MIH_MN_HO_Candidate_Query (extended) | MICS | SNR, Available Data Rate, number of associated users, Throughput, Packet Error Rate, CoS Minimum Packet Transfer Delay, CoS Average Packet Transfer Delay, CoS Maximum Packet Transfer Delay, CoS Packet Loss |
| MIH_N2N_HO_Candidate_Query | MICS | SNR, Available Data Rate, number of associated users, Throughput, Packet Error Rate, CoS Minimum Packet Transfer Delay, CoS Average Packet Transfer Delay, CoS Maximum Packet Transfer Delay, CoS Packet Loss |

Table 4.1: Existing MIH Service Primitives Used

In Table 4.2 the new MIH service primitives that have been defined for handover decision making are presented.

| **Primitives** | **Service** | **Parameters** |
|---|---|---|
| MIH_App_Par | MIES | Required data rate, delay, jitter, priority of applications |
| MIH_App_req | MICS | SNR, Required data rate, throughput , jitter, delay |

Table 4.2: Newly Defined MIH Service Primitives Used

### 4.3.5The Structure of the HNI Report

The MIIS 'HNI' report will be delivered through a request/response mechanism and will be represented in a standard format such as XML, ASN.1 or TLV. Table 4.3 shows the HNI request message in TLV format by which the MN/MR can obtain the HNI_report by specifying the Link Type and Operator Identifiers as parameters.

| Type = TYPE_ IE_HNI_REPORT | Length = Variable |
|---|---|
| Type_IE_Container_HNI Report | |

Table 4.3: HNI Request

Table 4.4 shows the HNI response message. The HNI Report containing the IEs will be produced and stored in an IS.

| Type = TYPE_IE_HNI_REPORT | Length = Variable |
|---|---|
| HNI Container #1 | |
| PoA MAC Address IE | |
| POA Channel Range IE | |
| POA MAC Type IE | |
| POA PHY Type IE | |

| PoA Subnet Prefix IE |
|---|
| PoA Subnet Prefix IE |
| Network Type IE |
| Roaming Partners IE |
| Cost IE |
| Network Security IE |
| HNI Container #2 |
| ... ... ... |

Table 4.4: HNI Response

## 4. 4 Detailed Handover Procedure of the 802.21 Assisted FMIPv6

In this section a detailed explanation of the overall handover procedure of the proposed mechanism is presented. Figure 4.10 provides an overview of the message flow, where as Figures 4.11 and 4.12 provide a detailed illustration of the overall message flow.

### 4.4.1 MIH Capability Discovery

At the very beginning, when the MR is activated or switched on, it will need to discover its peer MIHFs in the access network in which it is currently residing. The MIH Capability Discovery service primitive is used by the MIHF to convey the supported MIH capabilities about Event Service, Command Service, and Information Service to the MIH Users (i.e. Upper layers).

As explained in Chapter 4, the MIHF discovery can be done either at layer 2 or layer 3. The MR can discover the MIHF capabilities of its peers (e.g. MIH PoSs, MIIS, ARs, etc.) using unsolicited mechanisms by listening to a media-specific broadcast message such as a Beacon Frame [21] in IEEE 802.11 or a DCD [22] in IEEE 802.16.

The MIH entities will periodically broadcast their capabilities over the data plane using the '*MIH_Capability_Discovery*' response message. Alternatively, the MR can discover its peers MIHF capabilities by broadcasting or unicasting a '*MIH_Capability_Discovery*' request message to either its broadcast domain or a known MIHF address. In response, only the MIH network

entities (MIH PoSs, MIIS and ARs) will respond with a '*MIH_Capability_Discovery*' response message. A detailed explanation and the message format of '*MIH_Capability_Discovery*' request/response are provided in [13].

### 4.4.2 Events Subscription

After the MIH Capability Discovery procedure, the FMIPv6 protocol in the MR will register for MIES notifications (i.e. L2 triggers) within its local stack. This will be done via a MIH Event Subscription service primitive that is listed in Table 4.1. A detailed explanation of MIH Event Subscription mechanism is presented in [13].

### 4.4.3 IS Discovery and Usage

The MR can discover valid ISs through either layer 2 or layer 3 mechanisms. At the time of writing, Dynamic Host Control Protocol (DHCP) is one of the candidate solutions for discovering the IS [23, 24]. Figure 4.9 shows the three phases related to the MIIS usage scenario: IS Discovery, SA bootstrap, IS Query/Response. The MIIS serves the upper layer entity that implements network selection and handover algorithms, i.e. the Mobility Management Entity (MME).

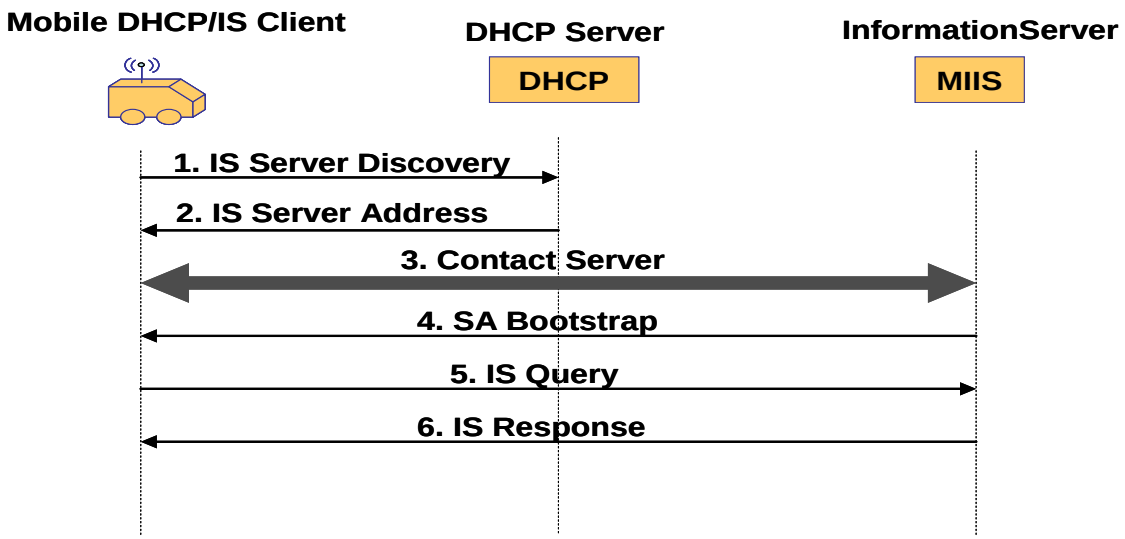


Figure 4.9: Is Discovery and Usage

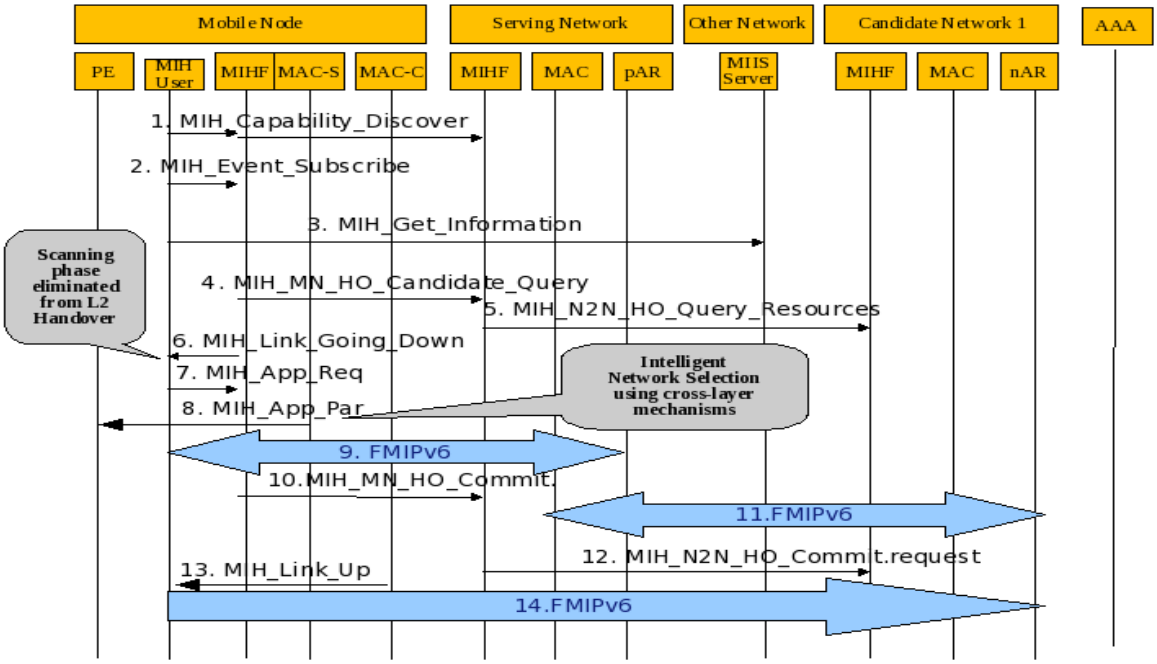


Figure 4.10: Overview of the proposed mechanism's message flow

### 4.4.4 SA Bootstrap

Before the MME can exchange any messages with the IS server, a set of Security Associations (SA) has to be established. Authentication and encryption parameters must be provided by each SA to preserve mobile device anonymity and prevent eavesdropping. The SA negotiation mechanism depends on the transport layer used and the required security services [23]. For Instance, TLS (Transport Layer Security) will be recommended for use if upper layer protocols use TCP, while ESP (Encapsulation Security Payload) using IPSec/IKE will work in most situations without the need to worry about the upper layer protocols, as long as the IS protocol identifiers are handled by IKE [23].

### 4.4.5. Retrieval of Neighbouring Network Information from the IS

It must be noted that the communications between the MR and the IS will be handled by the MIH protocol as specified in the IEEE802.21 draft. The MIH protocol defines the frame structure for exchanging messages between MIH functional entities. The payload of the MIH message contains service specific TLVs. Details of the MIH protocol message structure are provided in [13].

After the IS discovery and SA association phase, the MR will send a MIH message that carries the '*MIH_Get_ Information*' request TLV as its payload to request the HNI Report from the IS. The HNI Report will then be delivered in a returned MIH message from the IS to the MR in the format shown in Table 4.4. The contents of the report will be processed by the MR and stored in its NNR cache.

A time stamp is suggested to be maintained by the MN for periodic access to the IS. This would help the MN renew its contents and also check whether it is in the same or different IS domain.

### 4.4.6. Handover Operations

In the proposed 802.21 assisted FMIP6, the RtSolPr/PrRtAdv messages are replaced with '*MIH_Get_Information*' request/reply messages which are exchanged before the L2 trigger occurs. This is different from the original FMIPv6 in which the RtSolPr/PrRtAdv messages only occur after L2 triggers (i.e. when the MR senses that the signal strength of its existing link is becoming too weak). Later, when the signal strength of the current PoA becomes weak, the MIES will be informed by the link layer of the MR.

The MIES will scope and filter this link layer information against the rules set by the MIH user (FMIPv6 in this case), and then produce a '*MIH_Link_Going_Down*' event indication message, and send it to network layer where the FMIPv6 protocol resides. Upon receiving this event notification, the MR checks its NNR Cache and selects an appropriate PoA to handover to. Since the MR already knows the radio link information (i.e. MAC address and channel range of PoAs, etc.) of the candidate access networks from the HNI Report, the time to discover them is eliminated.

In IEEE802.11 networks for example, there will be no need to use the 'scanning' mechanism to find the neighbouring APs. After the MN discovers all the necessary information about the neighbouring access networks using the HNI Report, the MR will have to select a target PoA from a list of candidate PoAs belonging to different neighbouring access networks. In order to efficiently and intelligently select an appropriate PoA, a cross-layer mechanism is proposed in the next section.

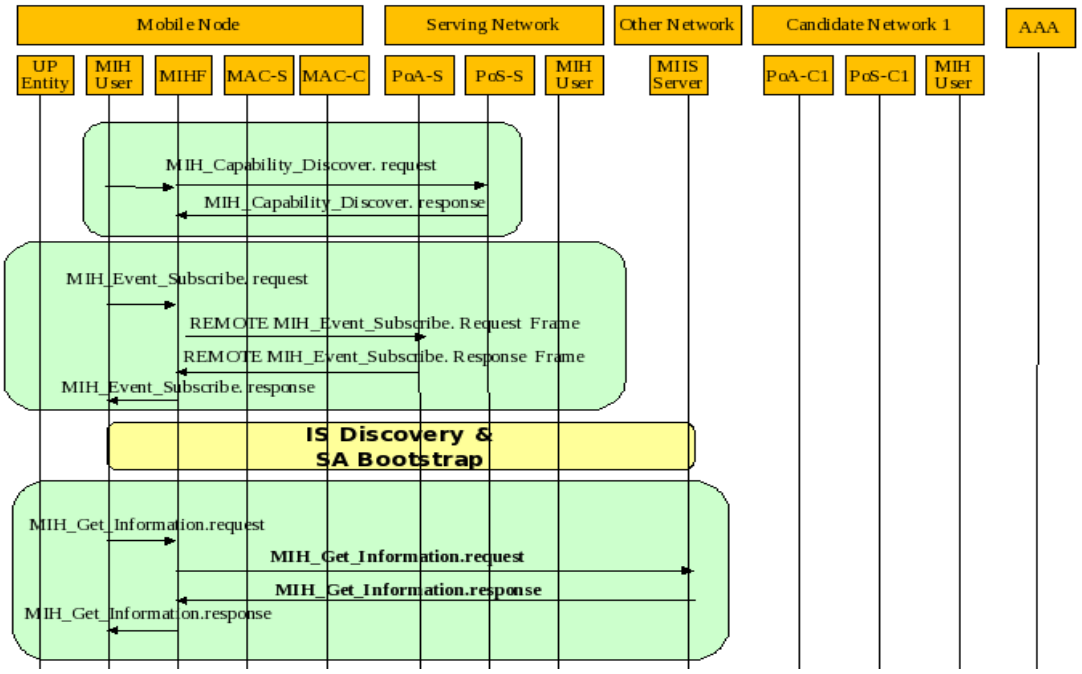


Figure: 4.11: Detailed message flow of the proposed mechanism (i)

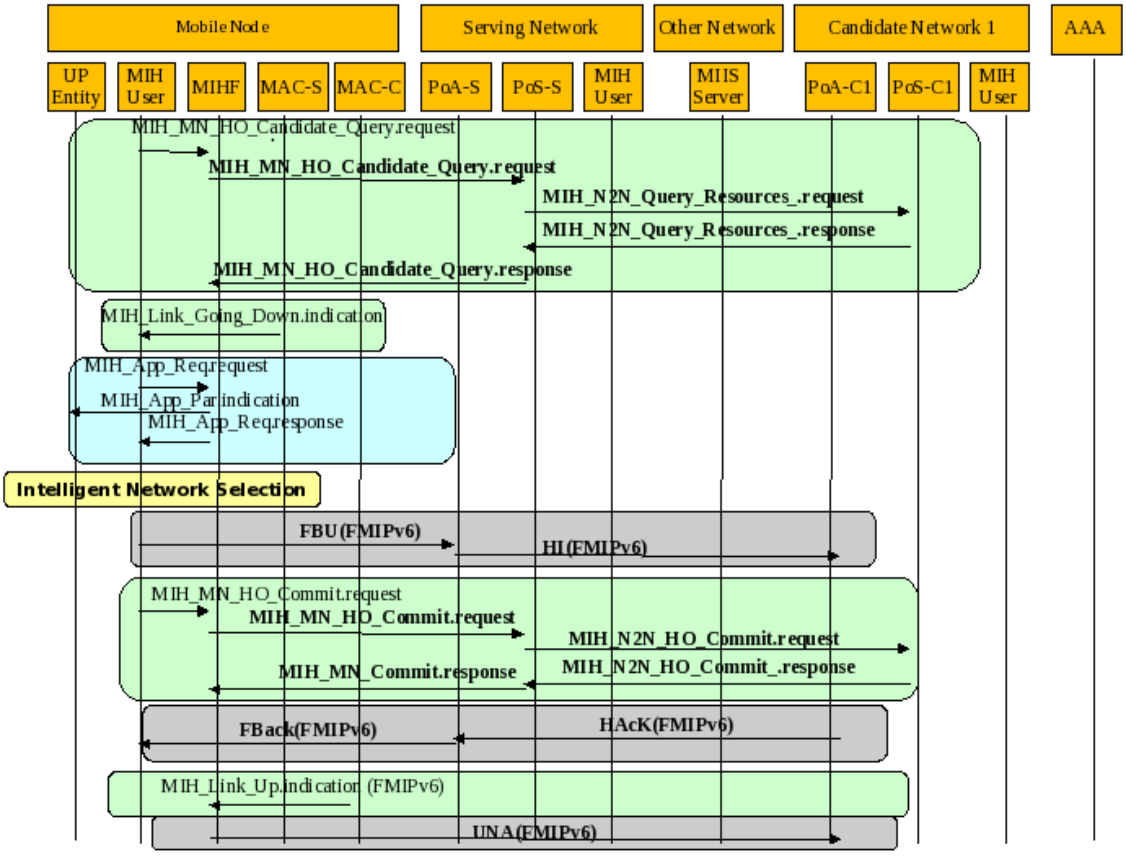


Figure 4.12: Detailed message flow of the proposed mechanism (ii)

### 4.4.7. Intelligent Handover Decision making using Cross Layer Mechanisms

The decision to select the appropriate (i.e. optimal) network is based on a policy engine which takes into account the QoS parameter requirements of the application and matches them with the dynamic QoS link parameters from the lower layers (L2 and below) of the available networks. As mentioned before, it is clearly specified in [13] that dynamic link layer parameters (e.g. QoS parameters such as Throughput, Average Packet Transfer Delay, Packet Loss Rate, SNR, etc.) have to be obtained based on direct interaction with the access networks and MIIS may not to be able to help much in this regard. Such dynamic QoS link parameters will have to be delivered to the MN through the MICS. As a result the IEEE802.21 standard has defined the *'MIH_MN_HO_Candidate_Query*' and *'MIH_N2N_HO_Query_Resources*' MICS service primitives. The *'MIH_MN_HO_Candidate_Query*' is used by MIH users on the MN/MR to inform the MIHF to query candidates for possible handover initiation. In other words, the *'MIH_MN_HO_Candidate_Query*' primitive is generated when a MIH User in the MR wants to query other candidate networks for possible handover initiation. The 'QoSResourceRequirement' parameter in '*MIH_MN_HO_Candidate_Query*' message, which provides information about the minimal QoS resources required at the candidate network, is not specified by the IEEE 802.21 standard. For this purpose, the service primitive '*MIH_MN_HO_Candidate_Query*' defined in [13] has been extended to include the list of resources shown in Table 4.2 as the 'QoSResourceRequirement'. The '*MIH_MN_HO_Candidate_Query*' service primitive works in a request/reply fashion and is carried as the payload of a MIH message as service specific TLV.

Upon choosing a PoA from the HNI Container/Report in the NNR solely on the grounds of the static L2 and L3 information (e.g., MAC address, channel range, subnet prefix), the PE in the MR will use the extended '*MIH_MN_HO_Candidate_Query*' service primitive via the MIHF to send a request to the serving PoA.

After the Serving PoA receives the '*MIH_MN_HO_Candidate_Query*' request, it will use the '*MIH_N2N_HO_Query_Resources*' request message to query to one or more candidate PoAs about their available link resources and IP address related information, and to prepare available resources in the candidate Networks. The Candidate PoAs respond with '*MIH_N2N_HO_Query_Resources*' responses and the serving PoA notifies the MR of the

resulting resource availability at the candidate networks through a '*MIH_MN_HO_Candidate_Quer*y' response message.

After receiving the '*MIH_MN_HO_Candidate_Query'* response, the PE receives the QoS requirements of the applications. Using the newly defined MICS service primitive '*MIH_App_Req*', the QoS requirement parameters are delivered from the application layer to the MIH Layer. After which, the newly defined MIES service primitive '*MIH_App_Parameter*' is triggered to deliver the application QoS parameter requirements to the PE. Figure 4.13 illustrates how the newly defined MIH service primitives help the PE in the MN/MR acquire the dynamic QoS parameters of neighbour networks.

The PE takes the application QoS parameter requirements and compares them with the dynamic QoS parameters from the lower layers of the candidate access networks. The "best" PoA to attach to can be selected according to the rules or policies input by the users. It is very important for the MN/MR to have a good network selection strategy. Note that the network selection results may vary drastically when different criteria are applied.

From the user's perspective, network selection could be carried out for the purposes of:

- Improving performance that matches the subscriber's QoS requirements (Handover QoS, Application QoS).
- Optimising cost.
- Optimising power consumption.
- Improving security.
- Obtaining better services.

From the network operators' perspective, apart from the above mentioned criteria, the network operators would also need to consider optimizing the overall network performance, e.g. balancing the load in the network. It is important to understand that the handover policies should also be made according to these criteria.

In Figure 4.13 the IEs related to each network selection criterion are shown. When the MN chooses to select a network based on one of the criteria, e.g. to optimize its power consumption, it must retrieve the information about network type, along with the network operator ID, and the

access network ID, as knowledge of the types of access network available will allow the MR to judge the potential level of power consumption of a particular connection. A finer decision could be made if the MR also retrieves the information of neighbouring PoA's, the network QoS, and available MIH services. The network selection algorithm could be as simple as comparing the IEs value with desired thresholds and scoring each available network using a weighted linear equation. The final network selection decision could be made based on the final score. Note that more sophisticated and complicated algorithms can be implemented in the PE to make intelligent decisions. Discussion of the details of such complex policies and algorithms is out of the scope of this thesis. The overall cross-layer mechanism is depicted in Figure 4.14 below.

| | QoS Performance | Cost | Power Consumption | Security | Services |
|---|---|---|---|---|---|
| Network Type | M | M | M | M | M |
| Network Operator ID | M | M | M | M | M |
| Network Cost | | Y | | | |
| Service Provider ID | | M | | | Y |
| Available Service ID1 | | M | | | Y |
| Service Cost | | Y | | | Y |
| Roaming Partner ID | | M | | M | |
| Roaming Cost | | Y | | | |
| Access Network ID | M | M | M | M | M |
| Network Security (EAP) | | | | Y | |
| MIH Serivices | | | Y | | Y |
| Network QoS | Y | | Y | | |
| PoA Info | Y | | Y | | |

***IE needed for different network selection criteria. (M stands for "Must have", and Y stands for "Good to have")***

Figure 4.13: Intelligent Network Selection criteria

## 4.4.8. Handover Operations – Switching Link

After selecting an appropriate radio access network, the MME in the MN/MR utilizes MIHF MICS and generates a link switch command using '*MIH_MN_HO_Commit*' and '*MIH_N2N_HO_Commit*' primitives as described in [13]. The parameters are shown in Table 4.1. Prior to sending the '*MIH_MN_HO_Commit*' command, the MR uses the L3 information, the PoA Subnet Prefix, to form an NCoA, and sends a FBU to its default AR (pAR). There is no

longer any need to send the RtSolPr/PrRtAdv messages for router discovery as the candidate AR information (i.e. 'Subnet Prefix' IE) is already in the NNR Cache. The CoA address configuration procedure that is related to the candidate AR discovery or RtSolPr/PrRtAdv messages is eliminated. During the anticipation phase, only the FBU message will be sent to the pAR. Unlike the original FMIPv6 operation, the proposed mechanism needs only a single signalling overhead that will be incurred during the anticipation phase. The probability of a Predictive Mode of operation in FMIP6 will be increased, and the L3 handover latency in FMIPv6 will be optimized. After receiving the FBack (Fast Binding Acknowledgement) message on the pAR's link, and the necessary L2 authentication and association procedure, a '*MIH_Link_Up*' event notification will be sent to inform the FMIP6 that a L2 connection with the target PoA is established. After the '*MIH_Link_Up*' notification, the UNA (Unsolicited Neighbour Advertisement) message is immediately sent and the traffic starts to flow from the new link. Figure 4.14 shows the operation of the cross layer mechanism for selecting the optimal network with the assistance of the newly defined MIH services.

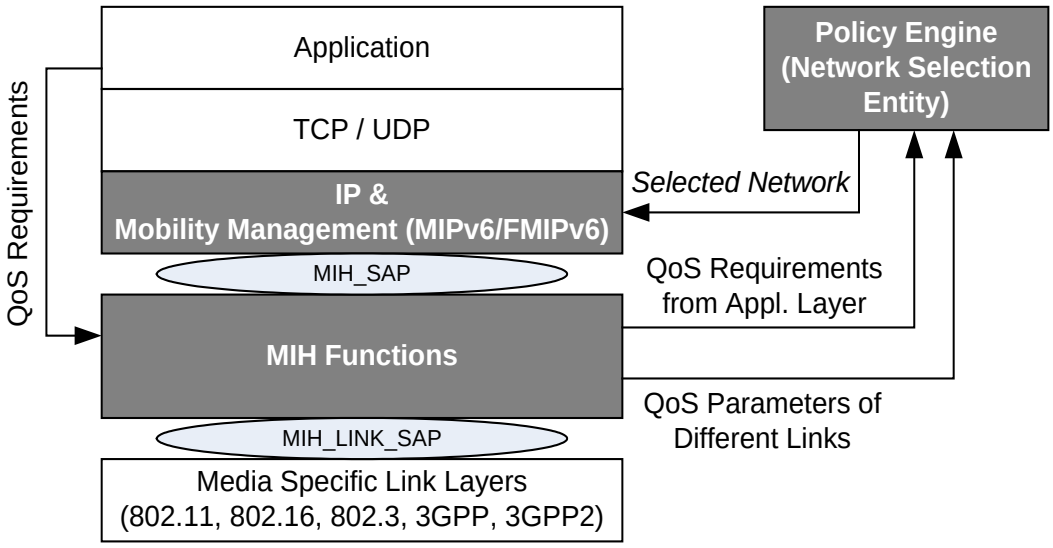


Figure: 4.14: Cross-layer mechanism for Intelligent Handover Selection

## 4. 5 Handover Performance Evaluation

As explained in Section 4.3, FMIPv6 can improve the handover performance of MIPv6 as well as NEMO. The proposed IEEE 802.21 assisted FMIPv6 mechanism should also enable NEMO handover procedures to be optimised. In this section the handover delay of the original NEMO, original FMIPv6, and IEEE 802.21 assisted FMIPv6 are analysed. The overall handover latency (both L2 and L3), i.e. the time interval between the moment the MN/MR loses connectivity with its current PoA till the moment it receives the first IP packets in the new subnet is analysed. For this reason, both the L2 and L3 handover are addressed.

### 4.5.1Numerical Analysis

The fundamental aspects of the IEEE802.21 assisted FMIPv6 handover optimization presented earlier in this chapter ( see section 4.3 and 4.4) are focused on reducing the adverse effects of the long anticipation phase, and its ability to tackle the neighbouring access network discovery issue (see chapter 2, section 2.7.1) suffered by the original FMIPv6. As mentioned earlier in section 4.4, the neighbouring network discovery issue is resolved by removing the L2 scanning time from the overall handover process. On the other hand, the long anticipation cost of FMIPv6 is resolved by eliminating the RtSolPr and PrRtAdv messages from the overall FMIPv6 handover signalling, which in effect increases the probability of a predictive mode of operation. The numerical analysis presented in the following sub-sections take into account the overall handover signalling process which highlights the impact of both the neighbouring radio/access discovery process and the cost of anticipation.

The total cost of the overall handover signalling process is derived in order to evaluate the effects of the anticipation phase on the proposed IEEE802.21 assisted FMIPv6 handover in comparison to other mobility management protocols (i.e. original FMIPv6 and NEMO). In this respect, a model based on the probability of a predictive mode failure is used which highlights the impact of the FMIPv6 anticipation phase. The overall handover latency is dependent on not only the mobility management signalling delays but also on other factors such as throughput, data rate, packet loss, network complexity etc. As a result, an extended handover evaluation is derived based on stochastic analysis which takes into account the effects of throughput, data rate, and network complexity on the overall handover latency.

#### 4.5.1.1 Handover Latency in NEMO

The handover latency for both FMIPv6 and NEMO can be expressed as:-

$$d_t = D_{L2} + D_{L3} \quad (1)$$

where $d_t$ **i**s the overall handover latency time, including both L2 and L3 latencies. Here $D_{L3}$ is the time period when the connected MN/MR is unable to send or receive any IP packets due to handover action. $D_{L2}$ is the time period the MN/MR loses connectivity with its current air link (i.e. PoA) till the time it connects to a new PoA. The overall handover procedure in both NEMO and FMIPv6 is started when L2 handover is initiated.

The L2 handover latency in an IEEE802.11 WLAN, for example, could occur in two distinct phases: the discovery phase and the re-authentication phase. During the 'discovery' phase, when the MR detects that the signal strength from the current AP is degraded to an unacceptable level, the MR/MN will start to scan available neighbouring APs and generate a list of APs prioritized by their corresponding signal strength. The 'Re-authentication' phase involves exchanging authentication and association messages between the MR and the AP. Extensive details of the L2 handover in IEEE802.11 can be found in [24]. The 802.11 L2 handover delay can be expressed as:

$$D_{L2} = D_{Discovery} + D_{Re\text{-}authentication} + D_{Association} = \mu \quad + \Psi \quad (2)$$

Where, $\Psi$ is equal to the PoA switching delay (i.e. new AP re-association and authentication latency) and $\mu$ is equal to L2 Scanning latency which could be expressed as:-

$$\mu = (N_{PoA}) \text{ X } (t_{SC})$$

where $N_{PoA}$ is the total number of PoAs and $t_{SC}$ is the delay to discover/scan a single PoA. For a MR in NEMO, the first step in the L3 handover is to perform the movement detection, during which the MR sends a Router Solicitation (RS) to the nAR. Upon reception of the RS, the nAR sends a Router Advertisement (RA) to the MR. After receiving the RA, the MR will know that it has moved. The delay caused by movement detection can be expressed as:

$$\left.\begin{array}{l} D_{MV} = D_{RD} + D_{CoA} + D_{DAD} \\ \text{where} \\ D_{RD} = D_{RS} + D_{RA} \end{array}\right\} \quad (3)$$

Here $D_{MV}$ is the time required for a MR to detect its movement and to form a new CoA. $D_{RD}$ is the router discovery time and includes the delays caused by sending the RS (i.e. $D_{RS}$) and the RA (i.e. $D_{RA}$). $D_{MV}$ also includes the time the MR takes to form a new CoA (i.e. $D_{CoA}$) and to perform Duplicate Address Detection (DAD), i.e. $D_{DAD}$.

After movement detection, the MR must send a BU to inform the HA and the CN of its new location (i.e. NCoA). The time taken to do this is expressed as $D_{BU\ (MN\text{-}HA)}$. The total handover signalling latency can be expressed as the sum of the L2 and L3 handover latency as:

$$d_t = D_{HO\text{-}NEMO} = \tag{4}$$

In NEMO, there is no scope for anticipating a handover. As a result, it can be inferred that in NEMO, there is no provision for a predictive mode of operation. The total cost of the NEM0 handover is:-

$$\left.\begin{aligned} C_{c\text{-}nemo} &= \\ &= (\ +2\ \theta.\beta)\ +2\theta.\beta+\theta.\beta+\theta.\beta\ ) \\ &= (\ +2\ \theta.\beta)+4\ \theta.\beta\ ) \end{aligned}\right\} \tag{5}$$

Where, $\theta$ is the unit signalling cost and $\beta$ is the weight for a wireless link to highlight the delays associated with shared medium access delay and collisions. Note that the latencies incurred due to L2 scanning have been included in the overall signalling cost because it is a fundamental proponent in the proposed mechanism and as well as the overall handover latency.

### 4.5.1.2 Handover Latency in FMIPv6

The handover latency in FMIPv6 is also comprised of both L2 and L3 latency. However, the delays associated with movement detection, new CoA configuration, and DAD, are eliminated in FMIPv6. FMIPv6 performs the handover initiation prior to the L2 handover. The handover initiation time includes the CoA configuration and BU times. After the L2 handover, the MR sends a UNA message to the nAR to inform it of its presence and then performs the BU operations. In equation (6), the overall handover latency in FMIPv6 is given as:

$$D_{HO\text{-}FMIPv6} = D_{L2} + D_{MN\_nAR} \tag{6}$$

In equation (6), $D_{MN\text{-}nAR}$ is the delay caused by sending the UNA message from the MR to the nAR. In the reactive mode, this will take a single Round Trip Time (RTT) since the MR will have to wait for the NAACK (Neighbour Advertisement Acknowledgement) message after sending the UNA. The Handover Initiation (HI) anticipation time is equal to the time required to send the RtSolPr, PrRtAdv, FBU, and FBack messages (i.e. the anticipation phase).

Note that it is not necessary to include the FBack in the HI time as it is not required to be received on the current link. However, for operations in predictive mode, it is mandatory for the FBack message to be received while being connected to the pAR's link. The handover initiation in case of predictive handover, is divided into two independent components; $T_{HI}$, the procedure to be executed by MN itself with the PAR and NAR, and $T_{HII}$, which is executed by the signalling process between the pAR and nAR.

$$T_{HI} = D_{PrRD} + D_{FMIPv6} = D_{RtSolPr} + D_{PrRtAdv} + D_{FBU} + D_{FBack} \quad (7)$$

Here, $D_{PrRD}$ is the time spent sending the RtSolPr and PrRtAdv messages. $D_{FMIPv6}$ is the time it takes to send the FBU and receive the FBack message.

$$T_{HII} = D_{HI} + D_{HAck} + \omega + D_{LU/DAD} \quad (8)$$

where $D_{HI} + D_{HAck}$ is the total time taken to exchange the HI and HAck messages between the pAR and nAR. The value of $\omega$ is the weighing factor of tunnelling between the pAR and nAR. $D_{LU/DAD}$ is the delay associated with the duplicate address detection at the nAR for the testing the uniqueness of the NCoA. The total FMIPv6 handover signalling latency can be expressed as:

$$D_{HO\text{-}P\text{-}FMIPv6} = \quad (9)$$

For a reactive handover, the total handover signalling latency is as follows:-

$$D_{HO\text{-}R\text{-}FMIPv6} = + D_{FBU} + D_{FBack} + D_{HI} + D_{HAck} + \omega + D_{LU/DAD} \quad (10)$$

In FMIPv6, the effects of the anticipation phase on the overall handover signalling latency must be taken into account. During an anticipation phase, there will be mobility management signalling exchanges between the MN and pAR. A failure in the predictive mode of operation will only occur if the MN leaves the overlapped area between the pAR and nAR before all the required signalling during the anticipation phase (i.e. the RtSolPr, PrRtAdv, FBU, and FBack messages) has been executed. The probability of a predictive mode of failure according to [106] is calculated as:

(11)

and if

where $\boldsymbol{T}$ represents a random variable for the time from a L2 *Link Going Down* trigger to a *Link Down* and is assumed to be exponentially distributed. $\boldsymbol{T_{pre}}$ is the time taken to send the required anticipation messages, and is time when the Link Down trigger is received by FMIPv6. $\boldsymbol{\theta}$ represents a decreasing factor, which is introduced to consider a variety of decreasing patterns as explained in [106] [107]. Based on equations (9) (10) and (11), the total handover signalling cost is derived as:

$$\boldsymbol{C_{c\text{-}fmip} = (1- Pr_{react}). C_{pred} + Pr_{react}. C_{react}} \quad (12)$$

$$\boldsymbol{= (1- Pr_{react}). C_{pred} + (1- ). C_{react}} \quad (13)$$

where

$$\boldsymbol{C_{pred} = C_{pre} + C_{L2} + C_{new}} \quad (14)$$

In equation (13), $\boldsymbol{C_{pred}}$ and $\boldsymbol{C_{react}}$ are the total handover signalling costs for predictive and reactive handovers respectively. In equation (14), $\boldsymbol{C_{pre}}$ is time required to exchange the RtSolPr PrRtAdv, FBU and FBack messages. $\boldsymbol{C_{L2}}$ is the cost of the L2 latency (i.e ) and $\boldsymbol{C_{new}}$ is the time required for the MN to send the UNA message when it connects to the nAR's link (i.e. $\boldsymbol{D_{MN\_nAR}}$ ). As a result from equation (14), the following can be derived:

$$
\left.
\begin{aligned}
C_{pred} &= C_{pre} + C_{L2} + D_{MN\_nAR} \\
&= max\{D_{RtSolPr} + D_{PrRtAdv} + D_{FBU} + D_{FBack} \\
&+D_{HI} + D_{HAck} + \omega + D_{LU/DAD}\} + \quad + D_{MN\_nAR} \\
&= max\{ 2\,\theta.\beta + 2\,\theta.\beta + 2\,\theta + \omega + \theta.\beta \} + \quad + 2\theta.\beta + \theta.\beta \\
&= max\{ 5\theta( \beta + - ) + \omega \} + \quad 3\,\theta.\beta
\end{aligned}
\right\} \qquad (15)
$$

where

$$C_{pre} =$$

and

$$C_{pre} < T$$

In equation (15), $C_{pre}$ is considered as the maximum acceptable value during which all the anticipation phase messages must be executed for a successful predictive operation. From equation (12), the total cost of the reactive handover is as follows:

$$C_{react} = C_{prt} + D_{MN\_Nar} + C_{rt} \qquad (16)$$

Where, $C_{prt}$ is the time taken for the MN to exchange the FMIPv6 signalling prior to moving to the nAR's link. In this instance, $C_{prt}$ would include the time to exchange the RtSolPr and PrRtAdv messages before being abruptly disconnected. Due to the reactive nature of the handover, the MN will not have sufficient time to send the FBU and FBack messages. $C_{rt}$ is the time to exchange the messages after the MN connects to the nAR's link. $C_{rt}$ could be expressed as follows:

$$C_{rt} = D_{FBU} + D_{FBack} + D_{HI} + D_{HAck} + \omega + D_{LU/DAD} \qquad (17)$$

$$
\left.
\begin{aligned}
C_{react} &= ( D_{RtSolPr} + D_{PrRtAdv} ) + \quad + D_{MN\_nAR} + D_{FBU} + D_{FBack} \\
&+D_{HI} + D_{HAck} + \omega + D_{LU/DAD} \\
&= (2\,\theta.\beta) + \quad + 2\,\theta.\beta + \theta.\beta + 2\,\theta.\beta + 2\,\theta + \omega + \theta.\beta \\
&=(2\,\theta.\beta) + \quad + 2\theta\,( 3\beta + 1 ) + \omega
\end{aligned}
\right\} \qquad (18)
$$

From equations (15) and (18), the total handover signalling cost $C_{c\text{-}fmip}$ is calculated as:

$$C_{c\text{-}fmip} = (max\{ 5\theta( \beta + - ) + \omega \} + \quad 3\ \theta.\beta). (1- Pr_{react}))$$

$$+((2\ \theta.\beta) + \quad + 2\theta\ (\ 3\beta + 1\ ) + \omega\ )\ (1- \quad ) \qquad (19)$$

### 4.5.1.3 Handover Latency of the 802.21 assisted FMIPv6

In the proposed mechanism, L2 handover latency is significantly reduced by removing the radio access network discovery delay (i.e. scanning time). The handover initiation/anticipation time is reduced by removing the RtSolPr and PrRtAdv delays from $D_{PrRD}$.

$$T_{HI(opt)} = D_{FBU} + D_{FBack} = D_{FMIPv6} \qquad (20)$$

The 'discovery' phase will be eliminated from the L2 handover time in the proposed mechanism. Therefore, the total optimized handover signalling latency is expressed as:

$$D_{HO\text{-}FMIPv6(opt)} = \qquad (21)$$

The total handover signalling cost for the proposed IEEE802.21 assisted FMIPv6 can be expressed as:-

$$C_{c\text{-}pr\text{-}fmip} = (1- Pr_{react}).\ C_{pred} + Pr_{react}\ .C_{react} \qquad (22)$$

where

$$\left.\begin{aligned} C_{pred} &= max\ \{D_{FBU} + D_{FBack} \\ &\quad + D_{HI} + D_{HAck} + \omega + D_{LU/DAD}\} + \quad + D_{MN\_nAR} \\ &= max\{\ \theta(3\beta + 2\ )\ + \omega\ \} + \quad + 3\theta.\beta \end{aligned}\right\} \qquad (23)$$

where

$$C_{pre} =$$

and $C_{pred} < T$

Note, that the RtSolPr and PrRtAdv have been eliminated from the predictive cost (i.e. $C_{pred}$), thus reducing the overall handover cost (i.e. $C_{c\text{-}pr\text{-}fmip}$). Naturally, the latencies incurred during the anticipation phase are also reduced which increases the probability of a predictive mode of operation. From equations (18) and (23) $C_{c\text{-}pr\text{-}fmip}$ can be calculated as:

$$C_{c\text{-}pr\text{-}fmip} = (max\{\ \theta(3\beta + 2)\ + \omega\ \} + \quad + 3\theta.\beta\ )\ \}\ ).$$

$$(1- Pr_{react}))$$

$$+((2\theta.\beta)+\quad +2\theta(3\beta+1)+\omega)(1-\qquad) \tag{24}$$

It can be inferred from equations (19) and (24) that $C_{c\text{-}pr\text{-}fmip} < C_{c\text{-}fmip}$, which highlights the fact that the overall handover cost for the proposed IEEE802.21 assisted FMIPv6 mechanism is less than the original FMIPv6. Also, the signalling cost during the anticipation phase is reduced in the proposed mechanism, which increases the probability of a predictive mode of operation.

Table 4.5 compares the handover latencies of the original NEMO, FMIPv6, and the 802.21 assisted FMIPv6.

| ***Handover Mechanism*** | ***Handover Latency Cost*** | ***Handover Initiation Time*** |
|---|---|---|
| ***NEMO*** | $(\quad + 2\ \theta.\beta) + 4\ \theta.\beta\ )$ | *None* |
| ***FMIPv6*** | $(max\{\ 5\theta(\ \beta + -\ ) + \omega\ \} + \quad 3\ \theta.\beta).$ $(1\text{-}Pr_{react}))$ $+((2\ \theta.\beta) + \quad + 2\theta\ (\ 3\beta + 1\ ) + \omega\ )\ (1\text{-}\ )$ | $D_{PrRD} + D_{FMIPv6}$ |
| ***802.21 assisted FMIPv6*** | $(max\{\ \theta(3\beta + 2)\ + \omega\ \} + \quad + 3\theta.\beta\ )\}).$ $(1- Pr_{react}))$ $+((2\theta.\beta)+\quad +2\theta(3\beta+1)+\omega)(1-\qquad)$ | $D_{FMIPv6}$ |

Table 4.5: Comparison of Handover Latencies of NEMO, FMIPv6, and the 802.21 assisted FMIPv6

#### 4.5.1.4 Extended Handover Performance Evaluation

An extended analysis of the handover latency of FMIPv6 (see section 4.5.1.2) of the proposed IEEE802.21 assisted FMIPv6 mechanism (see section 4.5.5) provides a more thorough and detailed handover evaluation. The overall handover delays expressed in equations (9) and (21) can be broken into the following latency contributing components:

$$H_{LF} = L_{Queue} + L_{Proc} + L_{sig/Tran} \quad (25)$$

In equation (25), $L_{Proc}$ is the packet processing delay both at the MN and intermediate nodes (e.g. ARs). An example of $L_{Proc}$ is when the ARs check for bit-level errors in the packet that occurred during transmission as well as the time taken to determine the packet's next destination. Additional processing delays may be incurred if the FMIPv6 messages are secured using mechanisms such as SEND. $L_{sig/Tran}$ is the delay associated with transmitting packets across the physical access medium. The only variable delay component in equation (25) is the queuing delay (i.e. $L_{Queue}$). The queuing delays are very hard to predict and are heavily dependent on the network load. So investigation into how to reduce the queuing latency is an important aspect of QoS research.

From equation (25), the signalling latency involves the delays associated with exchanging the mobility management messages. The handover signalling latencies for NEMO, FMIPv6 and 802.21 assisted FMIPv6 are derived in equations (4), (9) and (21) respectively. As a result, $L_{sig/Tran}$ can be represented as:

$$L_{sig/Tran} = \quad (26)$$

In this thesis, the queuing latency along with various parameters such as throughput, data rate, packet loss, network complexity are considered, and, its impact on the overall IEEE802.21 assisted FMIPv6 handover latency are investigated. The processing latency (i.e. $L_{Proc}$) is not considered since it is fixed in nature and depends on the deployed system. The Transmission delay ($L_{sig/Tran}$) which is indirectly dependent on the queuing latency is considered through other parameters such as the throughput and data rate.

### 4.5.1.5 Queuing Latency

To estimate, the queuing latency, $L_{Queue}$, it is assumed that there are $n$ transit ARs in the path between the source and destination. $L_i$ is the latency at the $i^{th}$ transit AR. Then the total queuing delay $L_{Queue}$ is calculated as:

$$L_{Queue} = \qquad (27)$$

The queuing latency at $L_i$ relies on the packet arrival rate which is denoted by $\lambda$. The probability of the having $j$ number of packets arriving at any instant is given in [108] and expressed as:

$$Pj = \text{————} = \text{————}. \quad .j = 0,1,...k \qquad (28)$$

where $k$ is the maximum(finite) number of packets residing in a queue. The parameter $\chi$ expresses the density of the queue (i.e. the number of packets that could reside in the queue). If $t_s$ represents the packet servicing time, the value of $\chi$ is given in [108] as:

$$\chi = \lambda / t_s \qquad (29)$$

Based on the probability function shown in equation (28), the expected length of the queue $Q_L$ at any time is expressed as:

$$Q_L = \qquad (30)$$

The probability $\eta$ of a packet being accepted by the queue is given by:

$$\eta = 1 - P_K \qquad (31)$$

Where $P_K$ is the probability of the maximum number of packets in the queue. As a result, the queuing time $L_i$ at the $i^{th}$ AR expressed in equation (27) can be derived as:

$$L_i = Q_L / \eta \qquad (32)$$

The overall queuing latency has a significant impact on other network parameters such as throughput /data rate, network complexity and packet loss, all of which individually have an effect on the overall handover latency (i.e. $H_{LF}$ shown in equation (25)). As a result, the effects

of the throughput/data rate, network complexity and packet loss on the overall handover latency are highlighted in the following subsections.

## Throughput and data rate

The throughput and data rate which are heavily reliant on the average session arrival rate and the queuing length (i.e. buffer length) are investigated in this section. In other words, the effects of the queuing latency on throughput and data rate are evaluated. The throughput of a network is defined as the average number of successfully received packets per time slot. The packet arrival rate of IP packets at the ARs (i.e. pAR and nAR), would largely contribute to the queuing latency. The average throughput in essence is directly related to the average arrival rate and hence the queuing length. When the network is not overloaded, an increment in packet arrival rate at the ARs means an equal level of departure rate (i.e. transmission rate) towards the MNs and other end devices. Since a wireless network is a shared medium, it can be assumed that the bandwidth (i.e. data rate) is distributed fairly. As the packet arrival rate increases, more data needs to be transmitted across the physical medium towards the MNs and end-devices. This leads to a decrease in both the average available throughput and data rate. If the data rate, amount of information, and number of packets successfully transmitted are defined as ***R(bps)***, ***T(bit)*** and ***n*** respectively, the normalized throughput ***S*** is given as:

$$S = \frac{\quad}{\quad} \tag{33}$$

When no transmission packets are generated or all transmission packets are destroyed by collision, ***S*** is equal to 0. In an idealized situation, the normalized throughput value of ***S*** is equal to 1. When ***S*** =1, all the bit are transmitted correctly. When ***S*** >1, then, the aggregate throughput of the system decreases. As a result, the network approaches its channel capacity (i.e. $Q_L$ in equation (30) reaches a value of ***K***) which leads to a decline in the available data rate. In this instance, the transmission delay which is a function of the data rate and amount of traffic to be transmitted (i.e. packet length and number of packets) will also be affected. The transmission delay $T_d$ can be derived as follows:

$$T_d = (n-1)\frac{\quad}{\quad} + 2\frac{\quad}{\quad} \tag{34}$$

Where  is the length of the packet. ***R*** is the data rate of the wired link and $R_W$ is the data rate of the wireless link between the MN and AR.  It can be inferred from equation (34) that when the data rate decreases, the transmission delay $T_d$ increases. The transmission delay has a very negative impact on the overall FMIPv6 handover (see equation (9) and (21)). For example, the amount of time it would require to complete all the FMIPv6 signalling along with all the IEEE802.21 MIH messages would increase proportionally as the transmission delay increases.

**Complexity**

The complexity of the network is defined as the latencies incurred due to an increase in the number of end-devices (e.g. MNs, MRs) accompanied by the level of RSS  and the speed of an individual mobile device at any given instance.  As the number of the MNs/MRs increases, the network tends to become congested.  The average packet arrival rate would increase. This would cause the queuing length to become longer and eventually lead to delays caused by queuing and processing latencies. The average throughput and data rate would decrease which would cause transmission delays.

The handover decision method in FMIPv6 relies on attempts to predict the travelling distance in a cell coverage area by using the rate of change of ***RSS***. The relationship between ***RSS*** (in mW) and the distance between a PoA and the MR/MN at any point inside the WLAN coverage area can be obtained by using the path loss model in [111] and is  as follows:

$$RSS = E^* \kappa^{\wedge} - u^*10^{\wedge}(\epsilon/10) \quad (35)$$

Where ***E*** (in MW) is the transmit power of PoA. The path loss exponent (a value between 2 and 4 chosen depending on the transmission environment) is determined by ***u*** and ***ϵ*** which are Gaussian distribution random variables with a mean of zero and a standard deviation of up to 12 dB. The transmit power is given in [111] as:

$$Tpw = N\ (\ Ц(Packets/s)^*\ K(bits)/\ R(bps) \quad (36)$$

Where ***N*** is the number of connections, ***Ц*** is the transmission rate, ***K*** is the packet size and ***R*** is the data rate. As the speed of a MN increases, the rate of RSS decay increases. Also, the path loss increases as the distance between the MN and PoA increases [111]. In such a case, the

probability of a successful handover is greatly reduced. The average handover latency increases accordingly and is given in [111] as:

$$H_{LF} = (T^* \ H_{succ}) + (t^*(1- H_{succ}))+(dist/vel) \quad (37)$$

Where $H_{succ}$ is the probability of a successful handover, $T$ is the time taken for successful handover and $t$ is time taken for an unsuccessful handover.

**Packet drop**

The latencies caused by packet processing, queuing delays, etc, restrict ARs from allowing all the packets to pass through. As a result, some packets destined to various MNs/MRs are dropped. The average traffic load at an AR is given by:

$$a = m.\lambda.T \quad (38)$$

where, $\lambda$ is the average packet arrival rate , $T$ is the time unit required to transmit the complete packet and $m$ is the total number of MNs. A packet is queued when all the outgoing routes (i.e. channels) are busy and dropped if the queue is full. Therefore, the packet dropping probability is provided in [108] and is expressed as:

$$P(S) = \frac{\quad}{\quad} \quad (39)$$

Where, $S$ is the maximum number of outgoing channels for all i = 0, 1,.....$S$. An increase in packet loss will inherently mean an increase in the packet re-transmission rate. As a result, the queuing length at the ARs will also increase, leading to queuing and transmission delays, eventually causing an increase in the overall handover latency.

### 4.5.2 Analysis of Simulation Results

To evaluate the proposed mechanism, simulations were performed using the mobility package provided by the NIST Seamless and Secure Mobility project [25]. The mobility package is developed for an NS2 utility with 802.16 and 802.21 extensions. Initially, the FMIPv6 protocol was implemented according to RFC 4068 [7]. The handover procedure of FMIPv6 was then extended with the help of the IEEE802.21 MIH services provided by the NIST mobility package. To simulate the basic NEMO protocol, the simulation package developed by Wuhan University

[26] which is based on the NS2 utility patched with Mobiwan extensions has been used. The results obtained in this section are benchmarked with other well known models from both industry and academia for the purpose of getting a clear analysis of the handover process. The network scenario simulated is shown in Figure 4.15. The network scenario consists of an area of 2000 meters by 2000 meters in which one WiMAX (IEEE 802.16) cell and one IEEE802.11b WLAN Basic Service Set (BSS) are located. The WiMAX cell has a radius of 1000 meters, whilst the coverage area of the WLAN has a radius of 50 meters. The WLAN BSS is inside the WiMAX cell. It is assumed that the WiMAX cell and the WLAN BSS are managed by one mobility service provider.

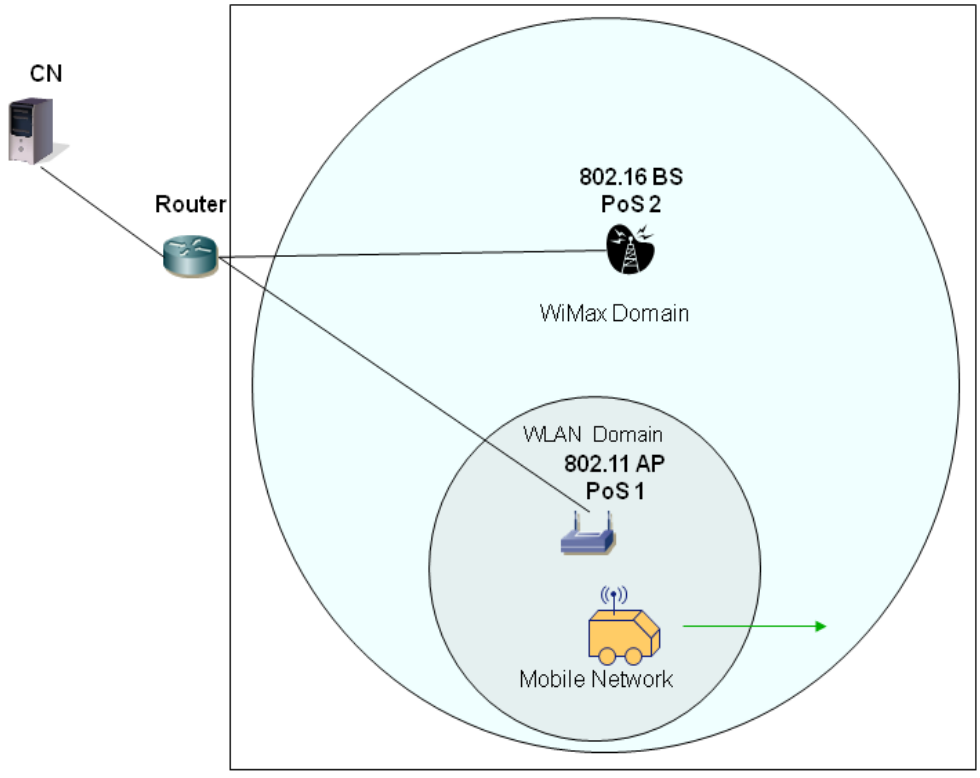


Figure 4.15: Network Simulation Topology

| Parameters | Variable Used |
|---|---|
| **Network Topology** | |
| **WLAN cell coverage** | **Disk with radius = 50 meters** |
| **WiMax cell coverage** | **Disk with radius = 1000 meters** |
| **802.11 MAC Sublayer Configuration** | |
| **Data rate(Mb/s)** | **11** |
| **Default propagation model** | **TwoRayGround** |
| **Packet loss** | **0-40%** |
| **802.16 MAC Sublayer Configuration** | |
| **Default Scanning mode** | **Active** |
| **Links** | |
| **Speed(Mb/s)** | **100** |
| **Delay(s)** | **0.01** |
| **Traffic** | |
| **Video Packet** | **4960 bytes** |
| **Audio Packet** | **320 bytes** |
| **Video packet rate** | **100 packets/s** |
| **Audio packet rate** | **200 packets/s** |
| **Mobility Model** | |
| **Velocity(m/s)** | **5m/s-25m/s** |
| **Path** | **Random** |

Figure 4.16: Simulation Parameters

The WiMAX network is the home domain where the HA is located. Each domain has one PoA which is connected to the core network through a 100Mbps connection. A correspondent node (CN) is connected to the core network through 100Mbps Ethernet. A WiMAX/WLAN dual mode MN/MR is communicating with a CN while moving in the above area at a random speed between 5 meter/s and 25 meter/s. Each time it enters and leaves the WLAN area handover procedures will be initiated.

Based on the FMIPv6 package and 802.21 along with the 802.16 NS2 extension developed by NIST [25], simulations were carried out in NS2. The simulations focused on evaluating the handover performance in terms of handover latency, packet loss and handover signalling.

Two types of traffic flows are transmitted between the MN and the CN. One is a video stream with a packet size of 4960 bytes and a packet rate of 100 packets/s. The other is an audio flow with a packet size of 320 bytes and a packet rate of 200 packets/s. The simulation time is set at 200s. For each mean speed simulated, the results given are the average of 10 simulations.

Handover Latency

The handover latency is defined as the time interval elapsed between the departure of data from the source to its arrival at the destination. In other words, it is the time when the MR looses connectivity with its attached PoA till the time it receives a data packet from the newly attached PoA.

The overall handover latency for the basic NEMO protocol is shown in Figure 4.17. It can be seen that, the average overall handover latency for the basic NEMO is 2.5sec/2500ms. Such a handover delay indicates that NEMO is unsuitable for handling real-time or multimedia traffic and providing seamless mobility.

The results shown in figure 4.17 reflect the nature of the results in [111], where an increase in MR/MN speed means that the distance from the attached PoA increases which leads to a decrease in the RSS level. At the same time the path loss increases, which leads to channel interference, low SNR and throughput. As a result, the transmission delay along with packet re-transmissions will increase, leading to lower probability of a successful handover as shown in equation (37). Moreover, the long handover latency is due to the fact that NEMO incurs very

time consuming L3 handover delays due to movement detection and CoA configuration as shown in equation (5).

| | ***Velocity 5m/s*** | ***Velocity 10m/s*** | ***Velocity 15m/s*** | ***Velocity 20m/s*** | ***Velocity 25m/s*** |
|---|---|---|---|---|---|
| ***Handover Latency*** | 1.1sec | 2.2sec | 2.5sec | 2.8sec | 3.0sec |

Figure 4.17: NEMO Handover Latency

From the simulation results presented in Figure 4.18, it is obvious that the handover process of FMIPv6 can be significantly improved by using the IEEE 802.21 MIH services. The average handover latencies for the audio and video traffic using the proposed mechanism are 0.31 sec/310ms and 0.33sec/330ms respectively.

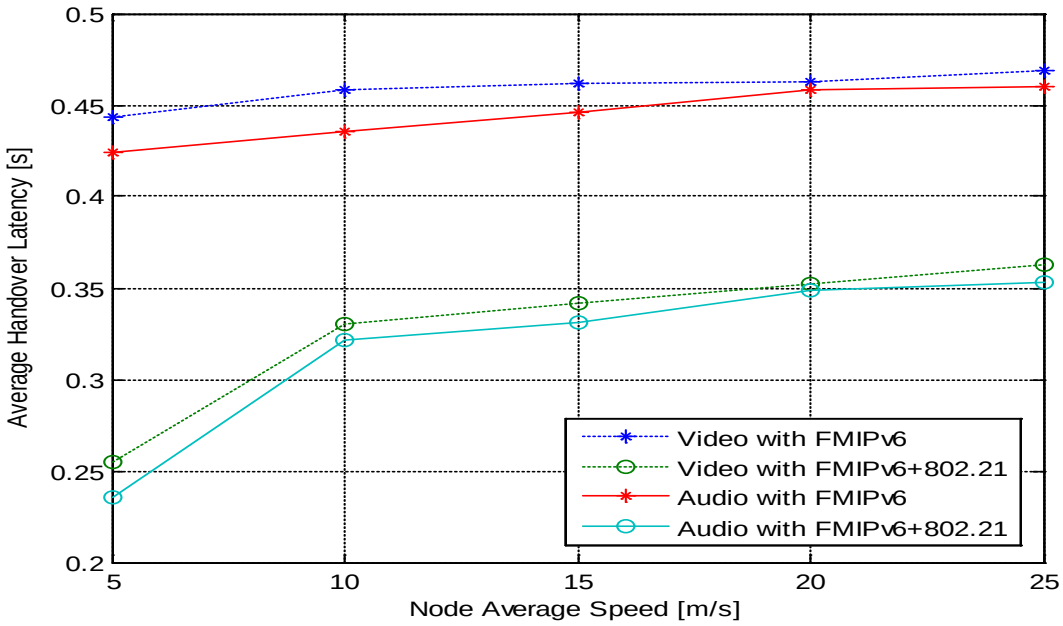


Figure 4.18: Average Handover latency

On the other hand, the average overall handover latencies for audio and video traffic of the original FMIPv6 are 0.45sec/450ms and 0.46sec/460ms. The results in Figure 4.18 suggest that the overall handover latency is roughly reduced by 140ms by using the proposed mechanism. This is due to the fact that the proposed mechanism eliminates the scanning phase from the L2 handover which drastically reduces the overall handover latency. Unsurprisingly, the handover

latency increases in NEMO (Figure 4.17), the original FMIPv6, and the proposed mechanism (i.e. IEEE 802.21 assisted FMIPv6) as the speed of the MN/MR increases.

The results shown in [113] are very similar to the simulation results presented in this chapter. The simulation tool used in [113] is different to the one used in this thesis. However, the models and scenarios considered in [113] are very similar to the one discussed in this chapter. Under similar conditions, the overall handover latency for the IEEE802.21 assisted FMIPv6 handover with respect to various MN/MR speeds outperforms the handover latency presented in [113] by 230ms on an average. Moreover, [113] does not consider vehicular environments. The proposed IEEE802.21 assisted FMIPv6 in this chapter greatly reduces the overall handover latency compared to [113] at similar velocities (i.e. lower/nomadic speed). The reason for such a reduction in the overall handover latency in Figure 4.18 when compared to [113] is due to the fact that the scanning time has been eliminated as shown in equation (20).

As shown in Figure 4.18, the overall handover latency increases with speed. With an increase in speed, the MR/MN moves further away from the PoA. As a result, the received signal strength (RSS) deteriorates more quickly resulting in lower throughput, which would eventually lead to an increase in transmission delay. This is highlighted in equations (34) and (35). The results shown in Figure 4.18 highlight the results obtained in [111]. In [111], it is shown that as the MN moves further away from its attached PoA, there is a decrease in RSS and at the same time the path loss decreases. As a result the network will suffer from channel interference, low SNR and throughput, all of which would lead to an increase in the overall handover latency. The results presented in Figure 4.18 hold true to the concept presented in [111], and show that as the speed of the MR/MNs increases and the MR/MNs move further away from the attached PoA, the RSS and path loss of the channel increases. This would cause transmission delays and if there is a sudden surge of packet arrivals at the ARs then there will be queuing and processing delays. When the MR/MN is far away from the attached PoA then the probability of a successful handover is minimized which will lead to a reduction in the average handover delay as shown in equation (37).

The results in Figure 4.18 support the FMIPv6 handover analysis in [117]. Using mathematical modelling, the results derived in [117] show that as the L2 handover increases (i.e. Link switching delay) the overall handover delay drastically increases. However, the model used in

[117] does not take into consideration the L2 scanning time, which is a fundamental component of the overall handover latency. In [117], when the link switching delay is increased to 1 second (i.e. a much more realistic value for L2 handover), even with the exclusion of the scanning time, the overall handover greatly increases. In Figure 4.18, the results obtained for the original FMIPv6 include the scanning time in the overall handover, whereas the proposed IEEE802.21 assisted FMIPv6 eliminates the scanning phase. As a result, the overall handover latency for the proposed mechanism of this chapter (see Figure 4.18) is greatly reduced due to a lower L2 handover delay which is coherent with the findings of [117]. However, the increase in the overall handover latency shown in [117] with respect to the L2 switching time is of order of the seconds, which is a lot higher than the results obtained in this chapter. The variations in results for the overall handover latency in Figure 4.18 and in [117] are due to the fact that [117] it takes the delays associated with the NCoA configuration time into account (i.e. The $\boldsymbol{T_{HII}}$ shown in equation (8) in this chapter), even in the case of a predictive handover. Moreover, some of the parameters considered in the mathematical analysis in [117], such as 'ζ' (i.e. the weighting factor of packet tunnelling between the pAR and nAR which adds a delay of 1.2 seconds) and the buffered packets forwarding delay from the pAR to the nAR , have not been considered in the simulation due to its limitations in mimicking all the aspects of real world situations. However, considering delays such as $\boldsymbol{T_{HII}}$ in the simulations would not be realistic since the predictive handover in FMIPv6 does not include the $\boldsymbol{T_{HII}}$ times in the overall handover latency. In this respect, the results shown in Figure 4.18 present a much more realistic and reasonable set of results.

In Figure 4.19, the L2 handover/setup times for the three solutions are shown against the overall handover latency values. As expected the overall handover latency increases with the L2 handover delay. As can be seen, the L2 handover/setup time has very little effect on the overall handover latency of the proposed mechanism when compared with NEMO and the original FMIPv6 protocol. This is because the scanning phase has been eliminated from the L2 handover time in the proposed mechanism.

The results in Figure 4.19 correspond to the numerical analysis presented in section 4.5 and the empirical values presented in [57] which suggests that the scanning phase comprises 90% of the overall L2 handover delay. The results in Figure 4.19 support the results in [117] which

demonstrate that the L2 handover time plays a very fundamental role in increasing the overall handover.

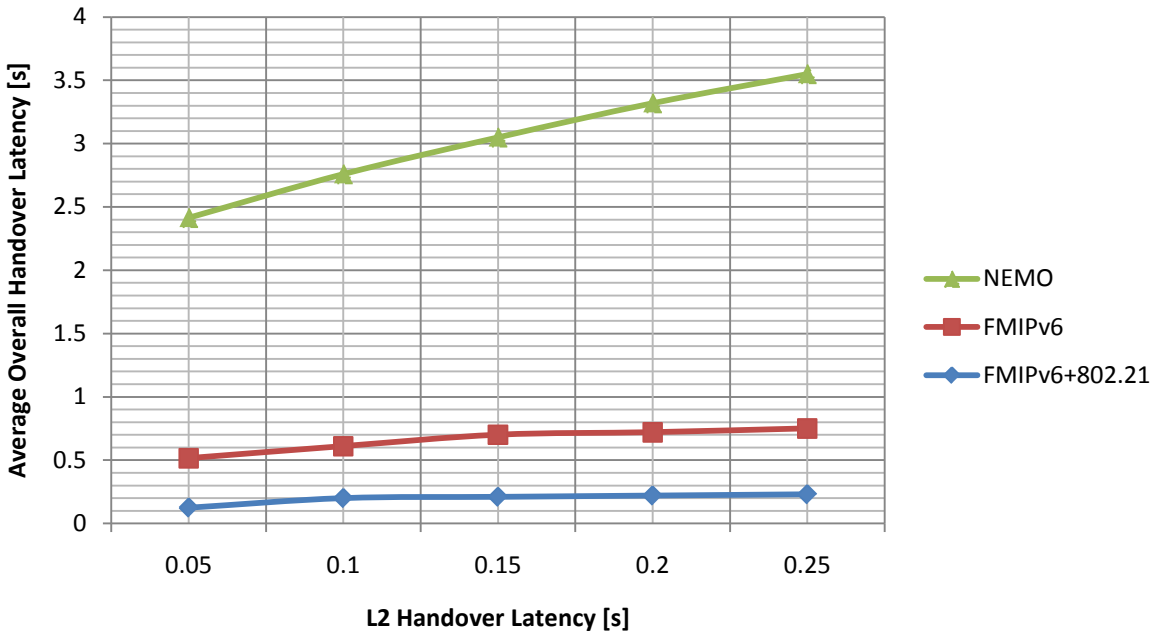


Figure 4.19: The L2 handover/setup times for three solutions

Packet Loss

Packet loss mainly refers to the amount of data that did not make it to the destination (i.e. MR) in a specified period. Packet loss is directly proportional to the QoS applicable.

Figure 4.20 shows that 802.21 assisted FMIPv6 looses less packets than the original FMIPv6 when speed increases. When the MN/MR moves at high speed, the FMIPv6 handover process might not be completed at the pAR's link, hence packets received by the pAR could be dropped. Also, as the distance from the PoA increases, the throughput of the link degrades causing further packet losses. When the MN moves further away from the attached PoA, the received RSS and the SNR decrease.

Based on research results in [111], the average packet loss increases with a smaller SNR. This is due to the fact that when the SNR is smaller, the channel interference increases, which leads to corrupted packets and hence packet loss. In [113], under a similar simulation condition compared to the one presented in this chapter, it is seen that the packet loss increases with the speed of the

MN. The results presented in figure 4.20 have a 27% lower packet loss rate in comparison to the results presented in [113]. Moreover, [113] does not consider vehicular environments. However, the results in Figure 4.20 are coherent with the findings of both [111] and [113], where packet loss increases with node speed.

The original FMIPv6 mechanisms incur on average a 79% increase in packet loss for both audio and video multimedia traffic compared to the proposed mechanism. Such packet loss is clearly undesirable and will cause service interruptions.

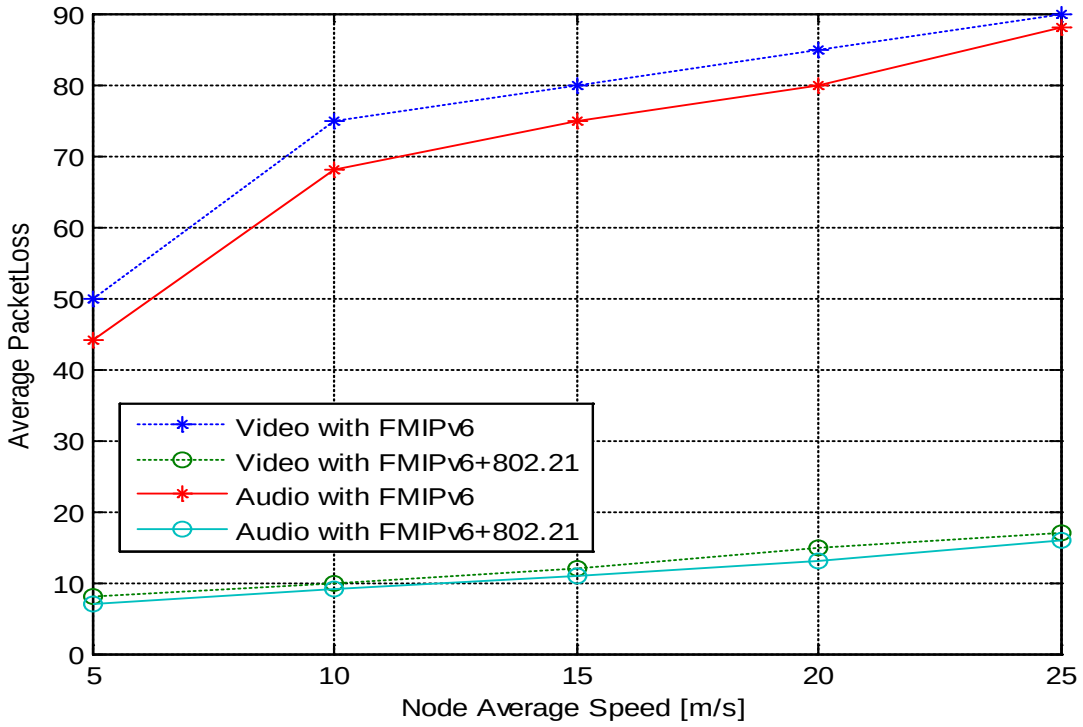


Figure 4.20: Average Packet Loss

Signalling Overhead

The overall signalling overhead here is the average signalling overhead (in bits) at the network layer and above during each handover interval. Figure 4.21 shows that the 802.21 assisted FMIPv6 has about 50% less signalling overhead than the original FMIPv6. This is aligned with the analysis of the proposed mechanism in section 4.5. The IEEE802.21 assisted FMIPv6

presented in this chapter increases the likelihood of a predictive handover in comparison with the basic FMIPv6. In Figure 4.21, as the speed increases, the probability of reactive handover increases. As a result, FMIPv6 signalling across the network also increases. When there are many MR/MNs present, then the probability of predictive handover decreases which causes the signalling load to drastically increase due to re-transmissions (see equation (32)). The results shown in Figure 4.21 support the findings in [79], where an increase in the number of MNs leads to more frequent handovers causing a linear increase in signalling load.

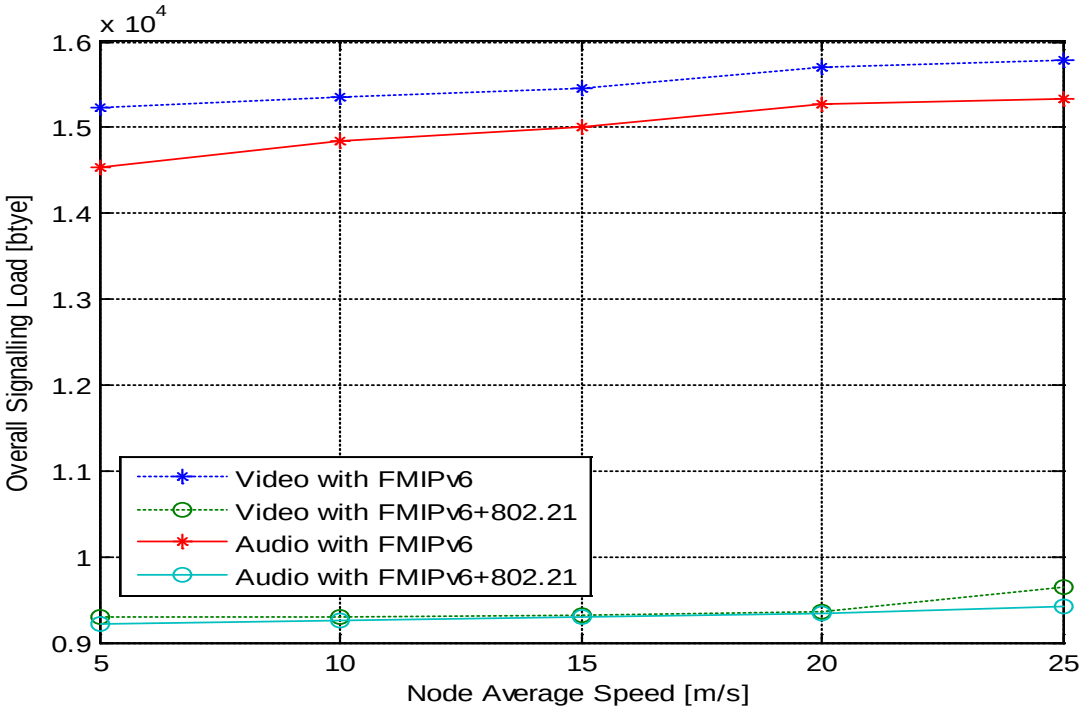


Figure 4.21: Overall Signalling Load

## 4. 6 Summary

In this chapter, a mechanism has been proposed which optimizes the FMIPv6 handover procedure with the assistance of IEEE802.21 MIH services for vehicular networking. To do so, MIH services have been exploited. Most notably, the 802.21 MIIS has been utilised and L3 information on neighbouring access networks in the MIIS service has been taken into account. A new Information Report, the 'HNI Container/Report', has been defined to contain L2 and L3 information of neighbouring access networks which can help the FMIPv6 protocol tackle issues

such as radio access discovery and candidate AR discovery. Moreover, it is proposed to store the contents of the HNI Container/Report in the NNR cache which can be maintained in the volatile memory of the MN. This eliminates the need to send RtSolPr/PrRtAdv messages which in turn reduces signalling overheads and the long anticipation time imposed by FMIPv6. It is shown analytically and through simulation results that when the proposed mechanism is applied to FMIPv6, it increases the probability of the predictive mode of operation and reduces the overall handover latency by reducing both the L2 and the L3 handover latency. The proposed mechanism outperforms the original FMIPv6 protocol and NEMO basic support.

The handover decision is made by a policy engine where a cross-layer mechanism is adopted. New MIH service primitives are defined to support intelligent handover decision making. The cross-layer mechanism takes into account QoS parameter requirements from the applications and compares them with the dynamic parameters of the available access networks. The parameters are then matched with pre-defined policies to optimize the handover decision.

# Chapter 5 Experimental Evaluation of Secured FMIPv6 over a Generic Authorization and Bootstrapping Architecture

## 5.1 Introduction

In order to successfully provide the “anywhere-anytime” type of services for NGNs, it is necessary for mobile and wireless operators to provide solutions which fulfil the mobility requirements of both the customers and operators. While roaming between heterogeneous access networks belonging to multiple administrative domains, users are demanding uninterrupted (i.e. session continuation at the least) usage of popular services like VoIP, video-conferencing, on-demand download, multimedia streaming, etc. It is becoming clear to operators that mobility (i.e. MIPv6) will become an inherent part of next-generation networks and a big proportion of the revenues will come from providing it as a service. This also comprises the enrichment of basic mobility service provided by MIPv6 with a set of additional features by enabling auto configuration and activation of specific “premium” services (e.g. multihoming, FMIPv6, etc.) based on policies and customer profiles maintained by the operators.

In the classical sense, strong inter-domain security mechanisms that allow roaming users to establish a security context between the end host and some device in the access network (e.g. APs, BSs etc), are provided by the network access authentication procedures [122]. The protocols which execute after the network access authentication also require security contexts to be established since the communicating end-points are different [122]. Furthermore, usage of different protocols may require different authorization decisions. For example, a user wishing to use MIPv6 services in a visiting domain would need an additional authorization statement from its home domain to ensure that the user is authorized to utilize MIPv6 functionalities and start the appropriate credit control and accounting [122].

The fear of becoming just a “bit-pipe” is driving operators to introduce additional services in their network [122]. As more and more services are introduced, the pressure to market the product faster, and at the same time reduce operational costs prevents operators from making static configurations per service for individual end hosts [122]. Also, from an operational point of view, static configuration is not feasible for an operator which may have millions of

subscribers. Hence the goal is to develop solutions which would allow end hosts to dynamically and securely obtain information for accessing services, based on long-term credentials. The long-term credential is typically a shared secret, a password or a X.509 certificate, which enables a client to carry out a "bootstrapping" process that distributes necessary information for service access [122]. Bootstrapping refers to the "*process of creating state* (*typically security associations* (*SA*), *configuration and authorization) information between two or more entities based on a trust relationship between a trusted third party and two or more entities"* [31].

The issue with bootstrapping is twofold. Firstly, the key distribution problem to ensure secure access to services (i.e. creating a SA between client and service) is challenging [122]. Secondly, there is a great need to define an efficient service authorization framework for real world deployments. As a result, the authentication and authorization must be decoupled. Allowing for authorization to be decoupled from authentication allows network administrators and service providers to enforce policy rules which meet the unique needs of a particular operational environment. The simplistic approach of performing authorization based on initial network authentication is no longer considered valid in terms of providing resilient security mechanisms. That is, even if the client possesses credentials to authenticate itself correctly, it is still necessary to verify whether the client is authorized to access a particular service. For example, if FMIPv6 is considered as a mobility service, then it is necessary for the MN and ARs (i.e.pAR and nAR) to share a secret (i.e. key) in order to setup SAs. This is necessary to protect the FMIPv6 signalling messages. However, simply possessing the shared secret does not imply that the MN is authorized to access the FMIPv6 service. In addition to the key distribution problem, the MN needs to be provisioned with a set of parameters [122]. The bootstrapping process allows the MN to obtain the necessary information to successfully and securely utilize FMIPv6 with the ARs.

The MIPv6 and DiME WGs have already published numerous IETF documents which provide solutions to the bootstrapping particularities in the context of MIPv6 only. The solutions provided by the IETF, such as references [28], [29], [30], [31], [32], and [33], utilize the AAA infrastructure (i.e. RADIUS or Diameter) along with the Extensible Authentication Protocol (EAP) [34] for bootstrapping MIPv6. Besides the IETF, other standards organizations like the 3GPP are currently investigating bootstrapping solutions with their Generic Bootstrapping Architecture (GBA) [35].

However, at the moment there is lack of a clearly defined generic service bootstrapping and authorization framework for integrated heterogeneous access networks. Moreover, FMIPv6 service bootstrapping is completely neglected. Even though FMIPv6 has been widely studied and accepted in research and standards bodies, there has been no work done on FMIPv6 bootstrapping; i.e. dynamic key SA establishment and authorization.

The ongoing work has led the EU-IST funded project ENABLE (Enabling Efficient and Operational Mobility in Large Scale Heterogeneous IPv6 Networks) to define successful solutions to enable efficient and operational mobility in large heterogeneous IP networks. As mentioned earlier in Chapter 1, this thesis has been partly affiliated with the ENABLE project and has contributed to define mechanisms which enrich the basic mobility service provided by MIPv6 with a set of additional features by enabling on-demand activation and auto-configuration of specific “premium” network services (e.g. FMIPv6 in our case, HMIPv6, multi-homing, IEEE802.21 MIH Services, etc). As a result, a Generic Authorization and Bootstrapping Architecture (GSABA), particularly for mobility services, has been defined [50].

In this chapter, a novel FMIPv6 bootstrapping and authorization architecture is presented in order to provide the MN with necessary configuration parameters and distributed keying materials to secure FMIPv6 messages in terms of authentication and authorization. In this respect, a practical Linux operating system based FMIPv6 bootstrapping and authorization test-bed has been implemented to provide experimental analysis. The purpose of the experiments is to investigate the handover performance of the secured FMIPv6 mechanism compared to plain FMIPv6 and MIPv6 by providing quantitative measurements and results on the quality of experience perceived by the users of IPv6 multimedia applications. Also, a security analysis of the secured FMIPv6 along with the newly defined protocol/interfaces of the GSABA architecture has been done, using the AVISA tool [36].

## 5.2 Problem Statement

As mentioned earlier, the problem with FMIPv6 bootstrapping lies with its inability to efficiently provide service authentication and authorization.

### 5.2.1 Insecure FMIPv6 Signalling

The MNs and ARs (i.e. pAR and nAR), must share credentials and cryptographic material needed for protecting the FMIPv6 signalling. The reception of a FBU triggers the pAR and nAR, with the assistance of the HI/HAcK messages to establish a tunnel for fast traffic redirection during handovers. Without proper security mechanisms in place, a malicious node may steal or redirect a victim node's traffic at will. To avoid such attacks, the pAR must ensure that the FBU packet arrived from a node that legitimately owns the PCoA. In other words, the FBU must be successfully authenticated by the pAR. Also, when the MN moves to nAR's link, it sends an UNA message. The UNA must also be authenticated by the nAR since the UNA could be faked and redirected to a malicious node. In order to tackle the issue, the current FMIPv6 specification [7] specifies a companion protocol SEND [37] to be applied to secure the FMIPv6 signalling procedure.

FMIPv6 uses the SEND protocol to exchange an encrypted shared handover key between the MN and pAR. The exchange of the handover key is done using the RtSolPr and PrRtAdv messages which are secured using the SEND protocol. Firstly, in order for the MN to utilise SEND, the relevant key pairs and CGA addresses are generated by the MN [129]. Utilising the same public key algorithm as used for SEND, a public/private key pair is then generated for protecting the shared handover key [129]. A RtSolPr is sent by the MN which contains the public key to encrypt the handover key. The RtSolPr also contains the source address of the MN's care-of CGA, which is signed with the CGA key of the MN. The RtSolPr is verified by the pAR by using SEND. The public key is used to encrypt the handover key which is then sent via the PrRtAdv message. The shared handover key is then decrypted by the MN to produce an authorization MAC [129]. However, it must be noted that SEND fails to specify mechanisms for protecting the UNA message.

SEND is sufficient for advancing FMIPv6 as a proposed standard. However, it is unknown whether SEND will always be available on access networks where FMIPv6 is likely to be deployed. Moreover, SEND makes no provision for protecting the UNA message. At the same time, it must be noted that IKEv2 has been ruled out as a solution for providing dynamic SA associations in FMIPv6, since it is not practical to run IKEv2 with every AR to create IPsec SAs, given that the AR changes may occur frequently. It is more likely that FMIPv6 will be used in

deployments (e.g. WiFi, WiMAX) where an AAA infrastructure will be used. So it would be good to develop a mechanism that leverages the AAA infrastructure in place and sets up SAs between the MN and the ARs dynamically [123]. As a result, the IETF has proposed the Handover Key (HOKEY) [38] protocol to secure FMIPv6 signalling. The HOKEY protocol is a key management protocol to establish a handover key between a MN and an AR for the purpose of securing FMIPv6 signalling messages [123]. This key can be used to protect the signalling message between the MN and the serving AR [123]. However, this handover key cannot be used to protect signalling messages sent by the MN to a new AR. As a result, if the UNA is left unsecured it is vulnerable to security threats, e.g. the UNA message sent to the nAR may be faked and then the packets could be redirected to the wrong MN [123]. However, the HOKEY protocol can be easily extended to provide mechanisms to protect the UNA message. Detailed explanation of HOKEY is provided in section 5.5.4.

### 5.2.2 Need for a Service Authorization Framework

As mentioned earlier, the second issue associated with FMIPv6 bootstrapping is authorization. Service authorization is, often, a neglected problem. In an ideal scenario, a MN has to be both successfully authenticated and authorized for a mobility service (i.e. FMIPv6). However, existing bootstrapping architectures focus on establishing security associations between involved parties. It is not clear, whether a MN that is able to authenticate for a mobility service, should automatically be authorized to use that service. In essence, there is a great need to define a framework that will inherently decouple service authentication and authorization.

## 5.3 Initial Architectural Overview

Before delving into the detailed specification of the GSABA architecture, it essential to understand the fundamental components upon which the GSABA architecture is built. A high level depiction of the initial architecture is presented in Figure 5.1. The most relevant interfaces between the nodes of the identified business entities, i.e., ASA, ASP, MSA and MSP (refer to chapter 2 section 2.2), along with the components of the GSABA framework are represented in Figure 5.3. The nodes that have been identified in this high level architecture are:

- **DHCP/Relay Agents:** Most of today's IP network deploys DHCP servers to configure network access for users. In the GSABA architecture, DHCPv6 is leveraged to deliver

HA information and discover service authorization servers.

- **Network Access Server (NASes):** New clients arriving at a network are authenticated by the NASes with the help of an AAA server. The NASs may be Layer 2 APs controlling the access of wireless clients, or an AR capable of performing IP-based admission control [49].
- **AAA:** The AAA nodes are used to authenticate the credentials provided by the clients, as well as to authorize access to network, mobility and other services, based on the user's profile. The AAA nodes also offer accounting facilities, allowing the business entities to charge according to service usage. AAA nodes may be redirect, relay, proxy or backend servers [49].
- **Databases:** The AAA backend servers usually interact with an external directory or database that maintains user's profiles and accounting data [49].
- **HAs/ARs:** The HAs/ARs are responsible for providing the mobility service (e.g. MIPv6, FMIPv6) to the MNs. The HA's/ARs are responsible for authenticating the MNs for mobility services in order to establish a secure tunnel for traffic forwarding.

It must be noted that the AAA infrastructure plays a fundamental role in the GSABA architecture. The next section provides an overview of the AAA infrastructure.

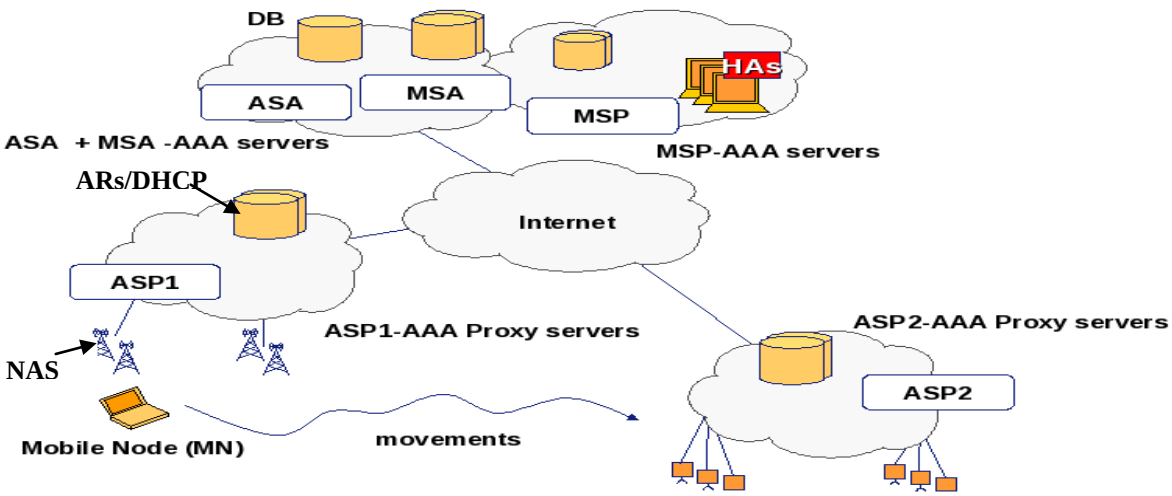


Figure 5.1: Network Architecture (Integrated Scenario)

### 5.3.1 Overview of the AAA infrastructure

AAA is an architectural framework used by operators to utilize three independent security functions in a modular manner which allows configuration of access control on network devices, such as routers and switches. The three security functions are:

**Authentication** provides mechanisms to identify subscribers before allowing them to use the network services. Authentication techniques used include login, password, challenge and response, message support and encryption.

**Authorization** provides mechanisms for remote access-control and authorization of services (e.g. MIPv6, FMIPv6, multihoming, etc.) based on user profiles and credentials.

**Accounting** provides methods for collecting and sending security server information such as user identities, start and stop times of services, executed protocols, numbers of packet and bytes exchanged, etc. Such information is used for billing, auditing and reporting purposes.

The AAA consists of three main components. They are:

- ***The AAA Protocol*** is used in the core network and runs between NAS and AAA server. Examples of AAA protocols are RADIUS [38], TACACS [39], Diameter [40], etc. However, the most widely used AAA protocol is RADIUS.
- ***The Access Network Protocol (ANP)*** is used between the NAS and the IP client. Examples of ANPs include 802.1X, PANA and PPP.
- ***The Authentication Method*** is the algorithm that the IP client and the AAA servers utilize for authentication purposes. It is typically based on a shared secret (e.g. login, password) between the client and its home operator. Many of the authentication methods support mutual authentication. The Extensible Authentication Protocol (EAP) defined in [34] is an authentication framework which supports many authentication methods. EAP is discussed in detail in the next section.

The three major components of the AAA architecture are illustrated in Figure 5.2. The MN roams into a visiting domain and requests access to the NAS using the ANP. The request is forwarded by the NAS to the AAA server located in the visiting (i.e. local) domain (shown as

AAAL in Figure 5.2). Based on the user/MN's identity, the AAAL forwards the request via the AAA protocol to the home AAA (AAAH) server located in the home domain. The authentication method is implemented only in the MN and AAAH, while the NAS simply acts a kind of gatekeeper, which is realized using an IEEE802.1X device The AAA protocol and ANP carry authentication data during the authentication phase. Based on the user's profile, the AAAH grants or denies access to the MN and may configure some services such as QoS, MIPv6 etc.

### 5.3.2 Overview of EAP

EAP, defined in [34], is a universal authentication framework typically used in PPP connection and wireless networks. EAP can be used for wired LAN and is not limited only to WLANs. The EAP peer is located in the client; the NAS contains the EAP authenticator and EAP server is located in a back-end AAA server. IEEE 802.1X defines a protocol called EAP over LAN to pass EAP messages ***between the authenticator and the client***. IEEE 802.1X provides the description for EAPOL only and does not describe the frame formats for the technology specific lower layer. For example, in 802.11, the EAPOL frames are encapsulated in IEEE 802.11 frames. Packets are exchanged via the AAA protocols between the EAP authenticator and EAP server. The EAP authenticator acts a pass-through device and does not know about the authentication methods.

Currently, there are many different EAP methods. Methods defined as IETF RFCs include EAP-MD5 [41], EAP-TLS [42], EAP-TTLS [43], PEAPv2 [44], EAP-IKEv2 [45], EAP-SIM [46], etc. The IEFT have defined an EAP Key Management Framework [47] for the generation and management of service keys within EAP architecture. Handover Keys to protect the signalling of mobility management protocols such as MIPv6 and FMIPv6 can be derived from such service specific keys.

The authentication framework selected for the proposed GSABA architecture is EAP. Since EAP enables different authentication methods to be used that run over multiple access technologies (or work over IP using PANA [48]), it is ideal for NGNs which are essentially an integration of heterogeneous access networks. Also, due to the extensible and flexible nature of EAP, it can be easily extended to piggyback service bootstrapping configuration parameters (HA address, Home address, authorization information) within an EAP exchange [49]. Moreover, EAP authentication can leverage the EAP Key Management to derive various service specific keys (e.g. keys to

protect FMIPv6 and service authorization signalling as is seen later in this chapter). EAP based solutions can be easily extended to become a generic service bootstrapping framework to provide configuration parameters and keys to establish SAs between end-points for secure communications [49].

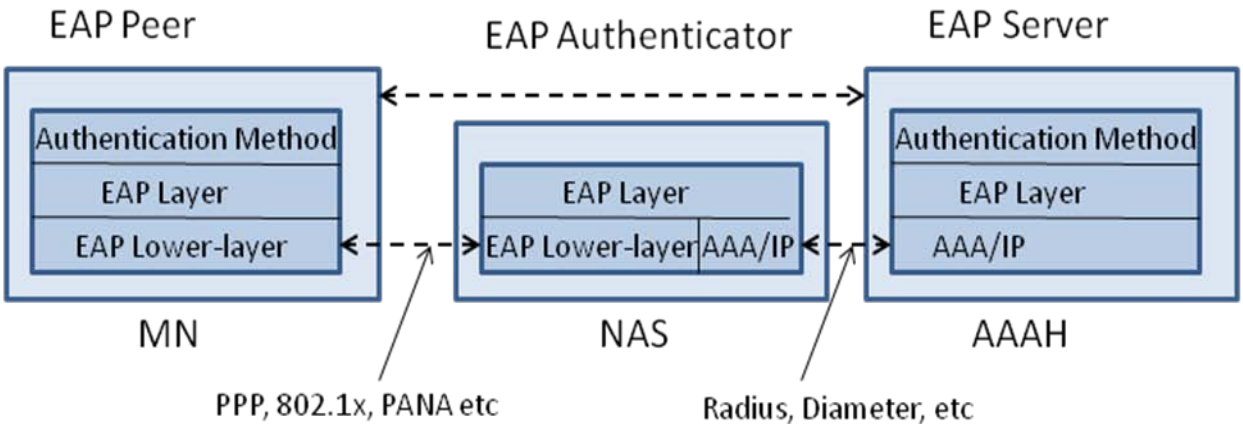


Figure 5.2: AAA Architecture

## 5.4 Network Scenario

In order to appreciate the specifics of the GSABA architecture, it is essential to understand the network scenarios under which GSABA will be deployed.

The most relevant entities to be taken into account in the proposed network scenarios are described below:

- **ASA (Access Service Authorizer)**: a network operator that authenticates a MN to establish its authorization right to receive IP service. AAA servers (ASA-AAA) are used to manage the authentication and authorization of the domain. The ASA maintains a local database, which stores the user's profile with specific access rights and policies.
- **ASP (Access Service Provider):** a network operator that provides direct IP packet forwarding and receiving from the end host. Before the MN can be granted access, the ASP must receive authorization from the user’s ASA. After the MN has been granted

access, the ASP may apply its own policies, along with service policies of ASA. The policies applied by the ASP must not conflict with the policies of the ASA. For example, ASP should not provide a MN with access to a service when it has been explicitly forbidden by the ASA.

- **MSA (Mobility Service Authorizer):** a service provider that authorizes mobility (i.e.MIPv6) service. AAA servers (MSA-AAA) are used to manage the authentication and authorization of the MSA domain. The MSA maintains a local database, which stores the user's profile with specific mobility access rights and policies.
- **MSP (Mobility Service Provider):** a service provider that provides MIPv6 service (i.e. HAs). In order to use the mobility service, the MN must be authenticated and must obtain an explicit authorization. For that reason, the MSP communicates with the user's MSA via the AAA infrastructure.

In order to authenticate and authorize a user's services, all of the entities (i.e. ASA, ASP, MSA and MSP) must communicate and trust each other. For this purpose, it is assumed that roaming agreements are in place. Based on the relationship of the MSA, MSP, ASA and ASP, two scenarios can be classified:

**Split Scenario:** When the Access Service Authorizer (ASA) is in a different administrative domain from the Mobility service Authorizer (MSA), it is called a 'split' scenario. An example of a typical split scenario is a MN that gets an opportunistic connectivity from a hotspot (e.g. coffee shop, conference), but depends on a third party (e.g. its home network) for global mobility. Different sub-scenarios can be considered based on the relationship between the MSA and MSP. They are:

- ***MSA and MSP are the same entity.***
- ***MSP is a third party entity (separated from the MSA).***

**Integrated Scenario:** When the ASA and the MSA belong to the same administrative domain, this is known as the 'Integrated' scenario. That is to say that the ASA and the MSA are the same entity, known as the MASA (Mobility and Access Service Authorizer). An example of an integrated scenario would be when a user has a subscription with an operator that typically provides both network access and mobility service. The AAA server authorizing mobility service

may or may not be co-located with the AAA server that authorizes network access. Based on the relationships between the ASP, the MSP and the MASA, various sub-scenarios can be classified:

- ***The ASP is the MSP and the MASA is a separate entity:*** In this case, the ASP and the MSP belong to the same domain and the MN is allocated a local HA in the ASP network.
- ***The MASA is the MSP, while the ASP is a separate entity:*** In this case, the MASA allocates the HA (i.e. in the home domain) and delivers the mobility service through the MSP.
- ***The MASA, MSP and ASP are separate entities:*** This scenario will occur when the ASP cannot provide MIPv6 service (e.g. the ASP does not own a HA) and, the MASA decides to redirect the MN to a third party MSP which is closer to the ASP network.
- ***The MASA is the MSP and the ASP:*** In this case, the MN is connected to the network of its own access provider which also provides mobility service.

Further variations of the two bootstrapping scenarios (i.e. Integrated and Split) can be derived based on whether EAP is being used. Detailed descriptions of the 'split' and 'integrated' bootstrapping scenarios can be found in [49] and [50] respectively. It is beyond the scope of this chapter to consider both the scenarios along with their sub-scenarios.

For simplicity reasons, this chapter considers the integrated scenario with EAP-capable access networks. Figure 5.1 shows an 'integrated' network scenario with EAP available. Here the Access Service Provider (ASP) and the Mobility Service Provider (MSP) are responsible for network (i.e. IP connectivity) and mobile services (MIPv6) respectively.

## 5.5 Detailed Architectural Overview

The logical components involved in our architecture are illustrated in Figure 5.3. The GSABA architecture is instantiated to fit the needs and requirements defined by the IETF MIPv6 WG. As a result the GSABA architecture is designed to accommodate the complex network scenarios envisaged by the MIPv6 WG which may require sophisticated business relationships among the network entities defined in section 5.2. Crucial to the architecture are components whose functionalities are described below:

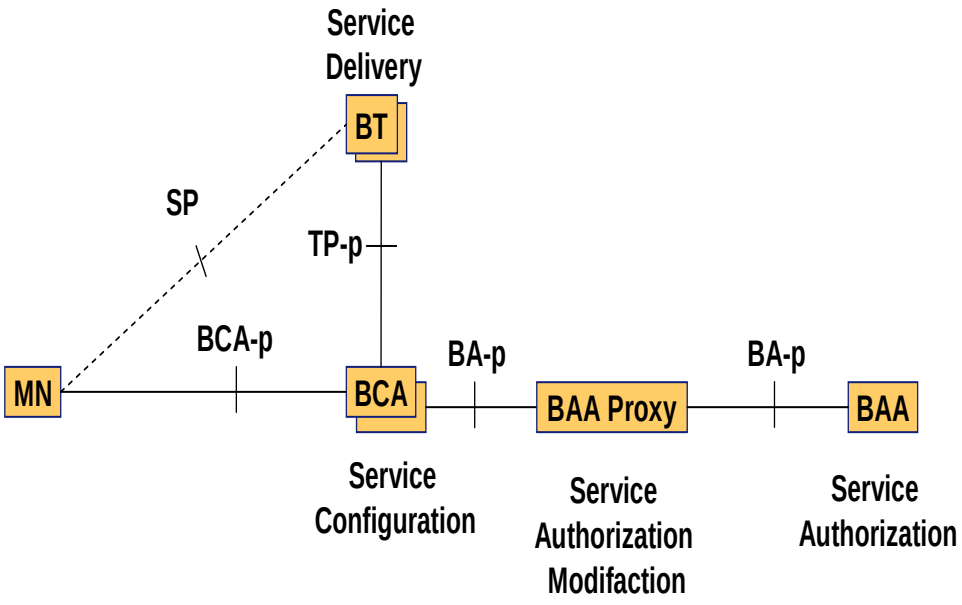


Figure 5.3: Architectural components [50]

- **The Bootstrapping Configuration Agent (BCA)** provides the required bootstrapping configuration information to the MN. For FMIPv6, this would imply the IP address of the pAR and SA parameters.
- **The Bootstrapping Authorization Agent (BAA)** is responsible for asserting the authorization statements. Based on the available profiles for the MNs, the authorization statements and parameters are produced by the BAA that are conveyed to the MN. Additionally, the BAA is required to authenticate the MN.
- **The Bootstrapping Target (BT)** is known as the 'service providing' entity. The BT is responsible for providing the service requested by the MN. The BT could be considered as the ARs (i.e. pAR and nAR) providing the FMIPv6 service to the MN.
- **The BAA Proxy** is required in the roaming case, where its function is to provide forwarding of service requests and maybe modification of the policies asserted by the BAA.

### 5.5.1 Interface Description

**The Bootstrapping Target Protocol (Tp-p):** This interface is used between the BTs and the BCA in the GSABA Proxy/GSABA Server for exchanging information which are relevant for

FMIPv6 signalling, and authorizing the BT to provide the MN with access to FMIPv6 service. Such information may be provided as Attribute Value Pairs (AVPs) or XML.

**The Bootstrapping Protocol (BCA-p):** This interface is used for the communication between the MN and the GSABA proxy. The MN is informed of the authorization decision taken by the BAA and BAA proxy via the BCA-p interface. This information may be provided as AVPs or XML. The Candidate transport protocols for the BCA-p include EAP/PANA, DHCP, HTTP, and TLS.

**The Bootstrapping Agent Protocol (BA-p):** This interface is used for communication between the BAA Proxy and the BAA. The BA-p allows information exchange between the BAA entities for decision-making purposes and delivers the decisions to the BCA. The information may be provided as AVPs or XML.

**The Service Related Protocol (SP):** This interface is utilised between the MN and BT (i.e. the pAR and nAR). Ideally, this is a service specific protocol (i.e. FMIPv6 signalling in this case) and should be left largely unmodified. The interface is therefore indicated by a dashed line in Figure 5.4

### 5.5.2 AAA Integration

Most of today's telecommunication and ISPs utilize the AAA infrastructure for their services. In order to provide users the facility to roam between access networks, AAA broker services are in place to support the peering between different providers. Established business relations are in place which has an effect on routing AAA messages. In this chapter, the defined architecture utilizes and integrates with the AAA infrastructures to reduce the deployment and operational costs.

Figure 5.4 illustrates the integration of the GSABA architecture with the AAA infrastructure. The BCA and BAA are co-located in an AAA proxy (i.e. GSABA proxy). The BAA is located in an AAA server (i.e.GSABA server). Only the extensions which are in the scope of AAA infrastructures will be applied to the GSABA architecture. The authorization decisions are taken by the GSABA server and are relayed to the GSABA proxy in the ASP domain. The proposed GSABA architecture is based on the following assumptions:

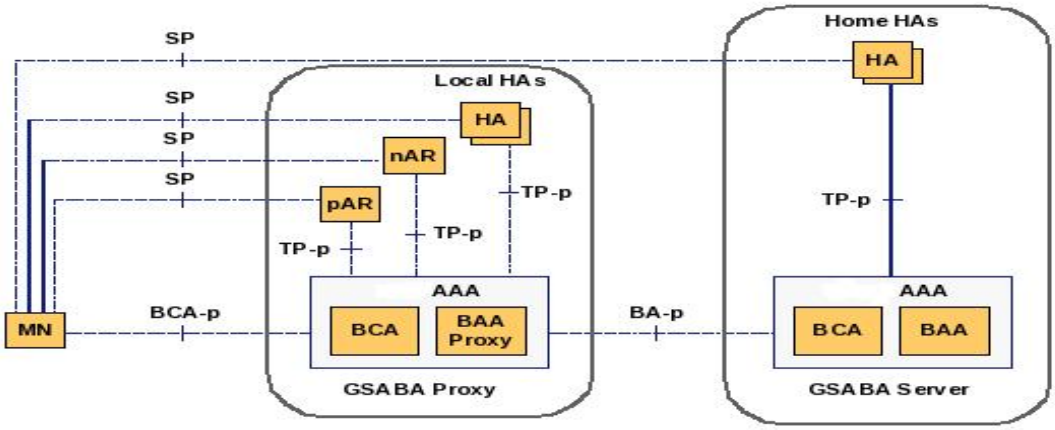


Figure 5.4: GSABA Architecture with AAA infrastructure [50]

- The GSABA proxy and the BT are located in the same domain.
- If the service provider is not the service authorizer, then the GSABA proxy can modify the authorization statements provided by GSABA server before delivering them to the BT.
- The ASA is assumed to be the home domain. In general, the ASA may or may not be the same entity which is responsible for authorizing the service to be bootstrapped [50]. However, this thesis considers only the Integrated scenario (i.e. ASA = MSA)
- The GSABA is intended to be used with a wide variety of services (e.g. MIPv6, HMIPv6, PMIPv6, multi-homing, etc). However, as mentioned earlier this thesis only considers FMIPv6.

Taking these assumptions into account, the entities of the GSABA architecture are presented:

**The GSABA Proxy:** The authorization statement is acquired from the GSABA server by GSABA Proxy for the utilization of FMIPv6 service. The authorization statements together with the needed configuration parameters are eventually delivered to the MN and the BTs. Essentially, the GSABA Proxy is an AAA server in which the BCA and BAA Proxy components are collocated. The GSABA proxy will reside in service providing domain. The authorization statements are gathered by the GSABA proxy from the GSABA server for providing the FMIPv6 service using the BA-p interface and utilising the AAA Proxy functionalities, which is similar in nature to that of an AAA server without little or no modification.

**The GSABA server** is responsible for providing the utmost decision of authorizing the requested mobility service. The GSABA server will reside in the domain that authorizes the service. In order to increase efficiency, the GSABA could optionally deliver the MN profile to the GSABA proxy instead of the authorization statement. This would allow the GSABA proxy to make authorization statements directly instead of contacting the GSABA server in the home domain every single time a service request arrives from the MN.

**ARs (i.e. The BT)** are the service providing servers (i.e. the pAR and nAR) that provide the FMIPv6 service to authorized users. The BT consists of a Service Target component and the Bootstrapping Target component. The Service Target component is responsible for providing the actual service to the MN. On the other hand, the Bootstrapping Target component is connected to the GSABA-enabled AAA proxy/severs through TP-p to acquire FMIPv6 authorization and configuration information regarding specific MNs.

**The MN** consumes the service (i.e. FMIPv6) provided by the BTs after obtaining the service configuration parameters and authorization statements from the GSABA proxy/servers.

### 5.5.3 High Level Message Flow

In this section, the overall message flow of the GSABA architecture is presented to explain the interaction between different entities to provide the FMIPv6 service bootstrapping. In the message flow provided in Figure 5.5, the following assumptions are made:

- The GSABA Proxy and the GSABA server are located in the same domain.
- The GSABA server resides in the domain that authorises service utilisation. The authorisation decisions are made locally. It is assumed to be in the “home” domain, i.e. the domain with which the MN has a relationship (i.e. a subscription based on a contract).

The overall message flow is illustrated in Figure 5.5 below which shows:

**Step 1**: The MN discovers the GSABA Proxy located in the ASP domain, e.g. using DHCP or the address could be discovered using a DNS query by using the SRV records.

**Step 2**: After discovering the GSABA Proxy, the MN needs to be authenticated by the GSABA Proxy. This is could be achieved in two ways.

- Directly by using full EAP based authentication with the GSABA proxy as the authenticator

and the GSABA server as the back-end authentication server, and the MN as the supplicant.

- Utilizing the initial network access so that the MN can be indirectly authenticated by the GSABA proxy. For this to be possible, the GSABA AAA proxy needs to be located in the ASP.

In either case, a new key known as the GSABA key is generated by the MN and the GSABA server. After a successful EAP method authentication, the GSABA key may be derived from the EMSK [51] generated, which is then delivered to the GSABA proxy. The GSABA key along with the MN's profile is delivered to the GSABA proxy. With the MN's profile the GSABA Proxy is able to generate authorization decisions locally and does not need to contact the GSABA server.

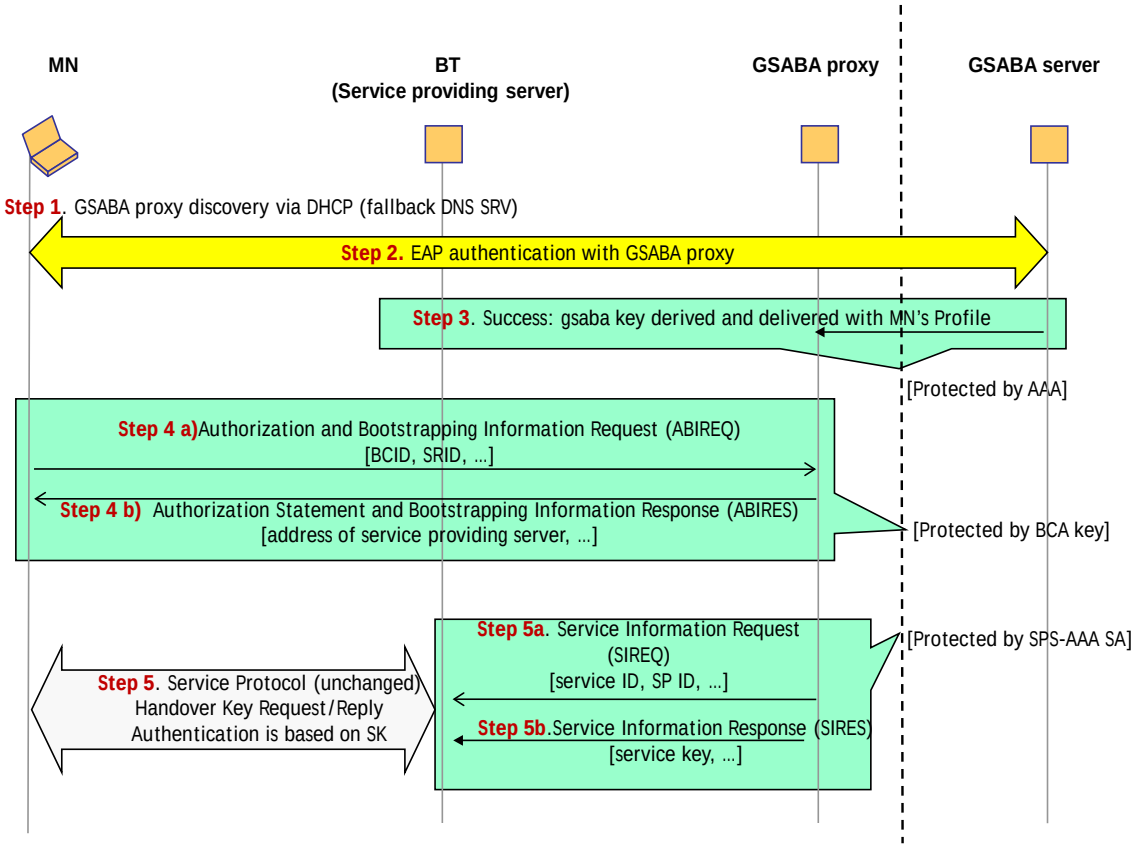


Figure 5.5: Message flow of the GSABA mechanism [50]

**Step 3:** Both the GSABA proxy and the MN have the new GSABA key at the end of a successful authentication. Other keys which are used to the protect the communication channel to the MN (i.e. the BCA key for the BCA interface between the GSABA Proxy and the MN, and the Service Key for the SP interface between the BT and the MN) are derived from the GSABA key [50]. Additionally, the GSABA Proxy and the MN generate a unique identifier (called the "bootstrapping client identifier" (BCID)) by which the GSABA key is identified [50]. The BCID aides in maintaining privacy by preventing the real user identifier, e.g. the NAI, from being transmitted in clear over the air interface.

The customer profile, which contains the service authorization information for all authorized services, is delivered to the GSABA proxy. Once the MN's profile is available to the GSABA Proxy, it is able to generate the authorization decision locally and does not need to contact the backend AAA server for each service request. After successful authentication the MN and the GSABA AAA proxy have the new GSABA key. The communication channel between the MN and the GSABA Proxy (i.e. the BCA-p interface) is protected using the GSABA key. Additionally, the BCID is generated by the MN and the GSABA Proxy with which the GSABA key, and as a result the MN as well, are identified [50].

**Step 4a:** To successfully bootstrap a service (e.g. FMIPv6), the MN sends an Authorization and Bootstrapping Information Request (ABIREQ) message to the GSABA Proxy. In order to identify the ABIREQ message, the BCID is used.

The ABIREQ message will contain the following set of information.

- The BCID
- The identifier of the service the MN wishes to use (i.e. the Service Request Identifier – SRID) [50]
- Service Identifier (Service ID-SID) to be used on the SP interface
- Additional service specific information such as capabilities and service preferences

**Step 4b:** Upon receiving an ABIREQ, the GSABA Proxy replies back with an Authorization and Bootstrapping Information Response (ABIRES) message which contains the required parameters to the MN [50].

The ABIRES message will contain the following set of parameters:

a) Authorization statement: “success”, “not available”, “not allowed”

b) Address of the service providing server (i.e. BT), which can be, for example, a Fully Qualified Domain Name (FQDN) or an IP routable address.

c) A key and an identifier (i.e. SID) used for accessing the service

d) Additional service specific information

**Step 5:** Once the MN has obtained all the necessary information for accessing the service (i.e. FMIPv6), it can start to setup a SA with the service providing server (i.e.BT). As soon as the BT gets the service request and cannot match the SID used in the request sent by the MN to any of the locally present SIDs, it contacts the GSABA proxy and queries regarding the received SID via a Service Request (SIREQ) message (step 5a). The minimum information contained in the SIREQ is the BT ID and the SID. Upon receiving the SIREQ, the GSABA proxy replies with a Service Information Response (SIRES) message (step 5b), which contains a handover key (HK) to be used for the verification (i.e. authentication) of the service protocol (i.e.FMIPv6 signalling). The HK is derived from the GSABA key and is shared by the MN and the GSABA proxy [50].

The entire process of obtaining the HK by utilizing the MN’s request/response and SIREQ/SIRES is achieved through the HOKEY process. The next section discusses the HOKEY process in detail.

### 5.5.4 Securing FMIPv6 Signalling with HOKEY

A draft [38] describes the HOKEY protocol used to establish a handover key between a MN and an AR for the purpose of securing FMIPv6 signalling messages. This key can be used to protect the signalling message between the MN and the pAR. This handover key cannot be used to protect signalling messages sent by a MN to a nAR, e.g. the UNA message sent to the new AR may be faked and then the packets are redirected to the wrong MN.

However, the HOKEY protocol can be easily extended to provide mechanisms to protect the UNA message. Details of such extensions are provided in 5.5.4.

The goals for the deployment of HOKEY are provided in [50].

### 5.5.4.1 Overview of HOKEY

In [38], it is assumed that the MN shares a key, called the Handover Master Key (HMK), with the Handover Key Server (HKS) [123]. The HMK can be thought as a GSABA key or a Usage Specific Root Key (USRK) and the Handover Key Server may be a GSABA proxy or a GSABA server [123]. A Handover Integrity Key (HIK) is derived from HMK at the MN and the GSABA proxy [123].

The HIK is used to provide integrity protection for messages exchanged between the MN and the GSABA Proxy [50]. Using the ABIRES/ABIREQ messages, the HIK is used to protect the data exchanged between the MN and the GSABA proxy through the BCA-p interface and can be thought as the BCA Key. Also, the actual Handover Key (HK), which is used to protect the signalling exchange between the MN and the AR is also derived from the HMK.

The derivation of these keys (i.e. HIK and HK) is described in detail in [38]. During the handover message exchange, the HKS should deliver the HK to the AR. Figure 5.6 illustrates the detailed message flow of the HOKEY procedure. As described in [38], the HKReq and HKRsp are realized via new Mobility Header types. The messages SIREQ and SIRES could be realized via an AAA protocol.

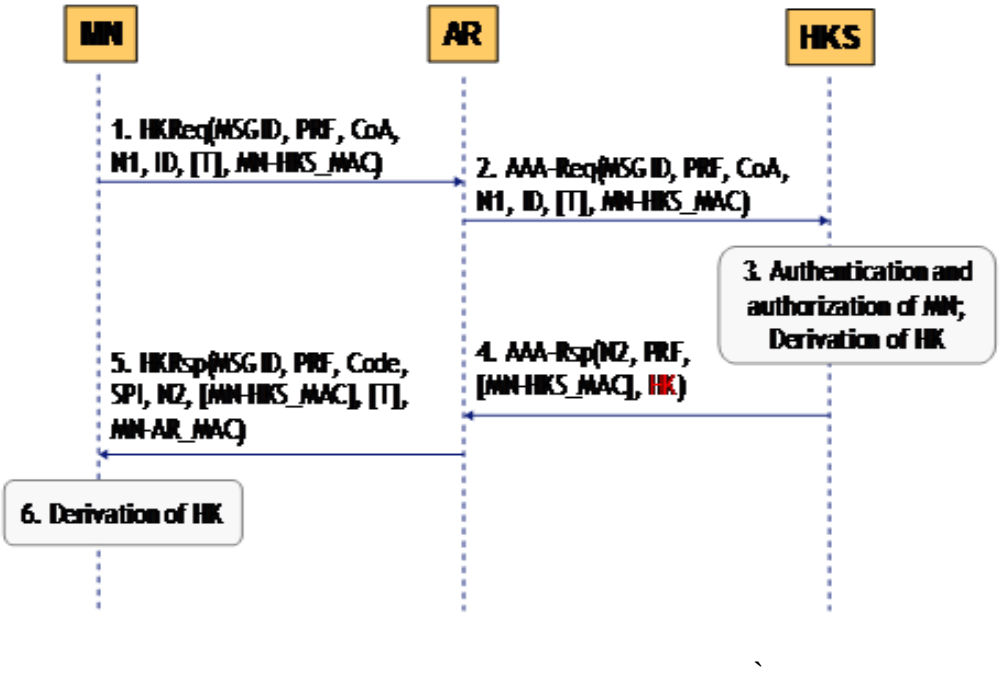


Figure 5.6: Message exchange in the HOKEY protocol

In Figure 5.6, the fields shown in "[]" are optional fields. The following parameters are given in the messages exchanged:

- MSGID represents the message ID which the MN selects in the Handover Key Request (HKReq).
- The algorithm chosen by the MN is denoted by the PRF.
- CoA is the care-of-address of the MN which is carried in the HKReq message.
- N1 and N2 are sent by the MN as nonces to the GSABA Proxy.
- The authentication data in the HKReq and HKResp messages are carried by the MN-HKS_MAC and MN-AR_MAC respectively.
- The optional timestamp used for replay protection is denoted by T.
- The SPI in the HKResp together with the AR IP address uniquely identifies the security association.
- The NAI of the MN is indicated in the ID field.
- The status code is indicated by the code field.

The following steps are required in the HOKEY process:

- **Step 1:** In order to start the HOKEY process, the MN sends the HKReq message.
- **Step 2:** The AR forwards the HKReq message via the SIREQ message to the GSABA Proxy, as only the GSABA Proxy can verify the MAC and generate a new HK.
- **Step 3:** The GSABA Proxy authenticates the MN via the MN-HKS_MAC option and checks whether the MN is authorized for fast handover. If so, the GSABA Proxy derives the HK via the following process:

  $$\boldsymbol{HK = gprf+(HMK, N1 \mid N2 \mid MN\ ID \mid AR\ ID \mid "Handover\ Key")}$$ [123]

  where "|" indicates concatenation and gprf+ is the key derivation function defined in [38]. The gprf+ is used to derive the HK (), which is an ASCII string with 12-characters and no null termination [50].

- **Step 4**: The GSABA Proxy replies with a SIRES message, containing the Handover Key (HK) and the AAA nonce N2 as well as the HK lifetime and the chosen PRF. The AR and the HKS share a SA protecting the AAA messages.

- **Step 5:** After the AR obtains the HK, the AR sends an HKResp message to the MN, which contains besides other parameters, N2 and MN-AR_MAC, which are protected using the HK.
- **Step 6:** The MN derives the HK using the same process as the GSABA Proxy. Now the MN and the AR share the same key (HK) for protecting the FMIPv6 signalling messages.

More detailed information on the protocol can be found in [38]. Figure 5.5 is based on the following assumptions:

- The FMIPv6 service is requested only after the MIPv6 service has been bootstrapped.
- The GSABA proxy downloads the user profile.
- The Handover key is derived before the handover procedures begin.

Figures 5.7 and 5.8 illustrate the message exchange during the FMIPv6 service bootstrapping in the predictive mode of operation. In this proposed scenario, MIPv6 is not important so the HA is not shown.

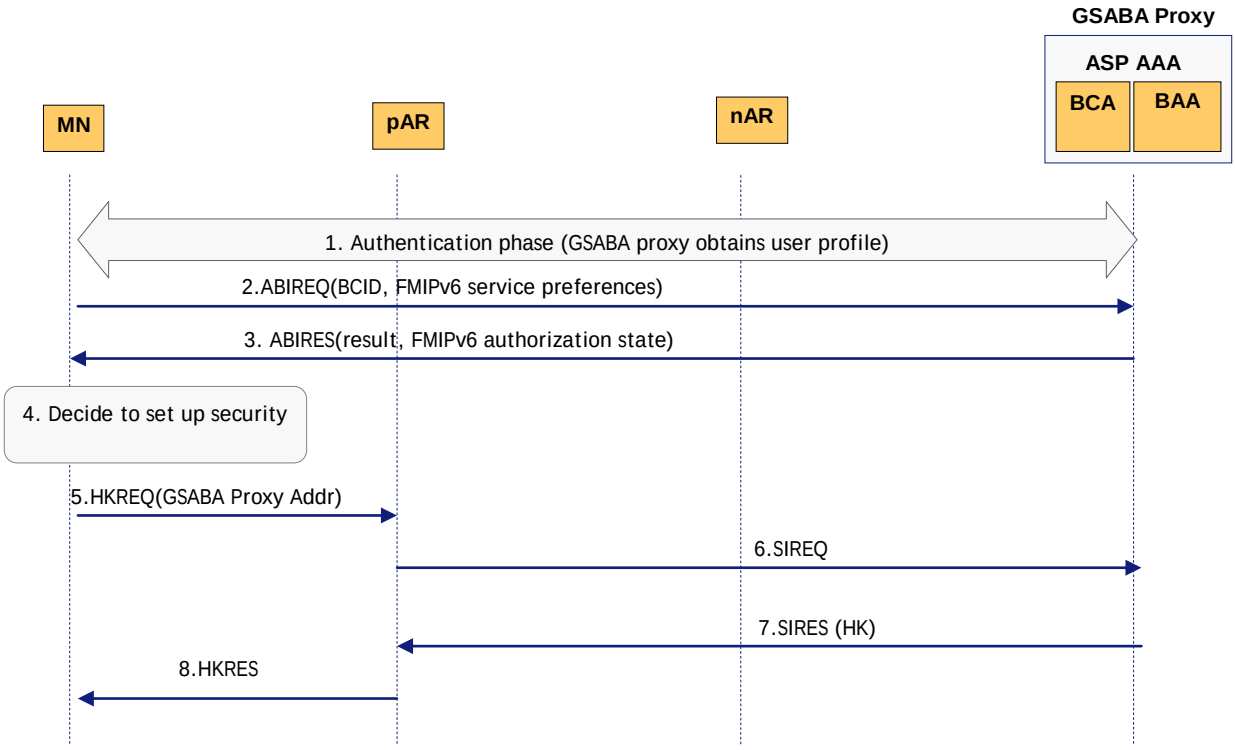


Figure 5.7: Message exchange during the FMIPv6 service bootstrapping (a) [50]

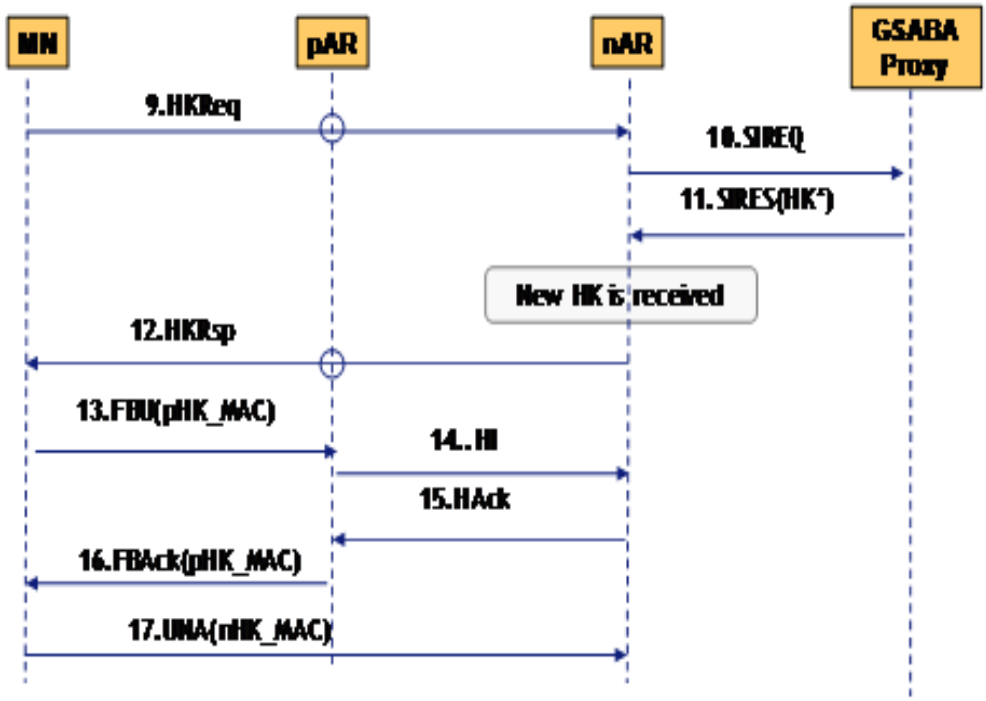


Figure 5.8: Message exchange during the FMIPv6 service bootstrapping (b) [50]

As mentioned earlier, the user profile is downloaded on the GSABA Proxy during the network access. After the GSABA Proxy has been discovered, the MN requests FMIPv6 services by sending an ABIREQ to the GSABA Proxy (i.e. The ASP AAA in this case) [50]. In the message, the MN must specify its identifier (i.e. BCID), and must indicate its interest in using the FMIPv6 service [50]. The GSABA Proxy checks the downloaded user profile and sends an authorization statement using the ABIRES message.

After successful authorization, the MN starts the process of establishing SAs with the ARs by sending the HKReq to the pAR. Upon receiving the HKReq, the pAR sends a SIREQ message to the GSABA Proxy. The GSABA Proxy checks the authorization state and generates a new Handover Key (HK) and sends it via the SIRES message. After receiving the MN's authorization state and the HK, the pAR responds to the MN with a HKRES message.

Besides the field specified in HOKEY, the HKReq message introduces new fields: the GSABA Proxy address field to allow the nAR to be informed on how to get the handover key and a pre-keying flag (P) [123]. The pre-keying flag (P) notifies the AR that the HOKEY procedure occurs

in pre-keying mode, not during the initial bootstrapping, and that the nAR should perform verification on the uniqueness of the NCoA for the MN [123]. After receiving the HKReq, the nAR sends a SIREQ message to the GSABA Proxy. The GSABA Proxy checks the authorization state and generates a new Handover Key (HK') and sends it via an SIRES message to the MN.

Through the process of HOKEY, the MN acquires the handover keys to be used to protect the FMIPv6 signalling (i.e. FBU and UNA messages) with both the pAR and nAR before the fast handover procedure begins. There are many advantages in setting up a security association between the MN and the AR before fast handover:

- "It allows the leveraging of the AAA infrastructure that is already in place to establish session keys for securing FMIPv6 signalling messages" [50].
- "The handover key derivation does not impact handoff latency" [50].
- "The compromise of one AR or a particular handover key does not lead to the compromise of the keys shared between the MN with any other AR" [50].

The MN sends a FBU to the pAR when it is willing to handover to the nAR. The FBU includes a message authentication code (MAC), which is generated using the HK. The MAC may be carried re-using the Authentication Option specified in [38]. After moving to the nAR's link, the MN sends the UNA message which includes a MAC, generated using the HK'.

## 5.6 Experimentation Analysis and Results

In this section, experimentation results are presented. Two separate cases of tests were performed. The first case is a security analysis of the HOKEY protocol, which is an integral part of the GSABA architecture. The security analysis has been performed using the AVISPA tool which provides industrial-strength technology for the analysis of the security strengths/weaknesses of large-scale Internet security-sensitive protocols. The second is to develop a GSABA testbed providing FMIPv6 services. The reason for this testbed is:

The GSABA architecture is a novel concept in its own right; in terms of providing mechanisms to securely bootstrap and authorize mobility services (i.e. FMIPv6 in this case) through newly defined protocols such as the BCA-p and HOKEY protocol. Such a concept needed to come to life for feasibility and proof of concept for the purpose of contributing to the relevant standard bodies and research community.

The GSABA architecture brings with it additional components, messages and signalling (e.g ABIRES/ABIREQ, HKReq/HKResp). With the incursion of such complexities, the effect on handover latencies (i.e. if any) needed to be investigated in comparison with FMIPv6 (without GSABA) and MIPv6.

### 5.6.1 Security Verification of HOKEY using AVISPA

In order to analyze the security of HOKEY, the Automatic Validation of Internet Protocols and Applications (AVISPA) tool has been used. AVISPA is a push-button tool which analyzes and validates security-sensitive protocols. AVISPA uses High Level Protocol Specification Language (HLPSL) [36], which an expressive, modular, role-based, formal language that allows for specification of protocols and their associated security properties [36].

The AVISPA tool interprets a user-defined security problem into an equivalent translation known as Intermediate Format (IF). For analysis, IF specifications can be provided as inputs to different back-end automation tools [124]. For formal analysis, On-the-fly-Model-Checker OFMC [36] and Constraint-Logic-based Attack Searcher CL-AtSe[36] are used, which are two matured back-ends for the tool, and are capable of performing protocol falsification and bounded verification via infinite numbers of sessions.

#### 5.6.1.1 Security Requirements

In order for HOKEY to be considered secured, a handover procedure must satisfy the following fundamental security requirements:

- Authentication: MN and the ARs (i.e. pAR and nAR) must mutually authenticate each other via HIK and HK/HK'. Moreover, the MN must be authenticated by the AR to use

the FMIPv6 service.

- Confidentiality: The contents of the HKReq and HKResp exchanged between the MN and ARs (pAR and nAR) must be kept secret from malicious attacks. The handovers keys (i.e. HK and HK') must only be shared between the MN and ARs. Other adversary nodes must not be able to derive the handover keys.
- Integrity: Any malicious node must not be able to alter the contents of the HKReq, HKResp and FBU.

#### 5.6.1.2 HLPSL Specification

HLPSL is a role-based language, which means the actions of each participant must be specified in a module. The protocol steps are modelled as transitions in a role by HLPSL. After that, the desired security properties of the protocol are modelled. In this section, various important elements of the proposed model are highlighted.

For the specification of the scheme, the details of the implemented model (i.e. HOKEY to secure FBU and UNA messages) have been abstracted as shown in Figure 5.9.

In the HLPSL specification, each role is enacted by participants/agents. The numbers of concurrent sessions of the protocol that must run are also specified by HLPSL. The following goals of HOKEY have been specified:

- Confidentiality/secrecy of HIK, HK, and HK' between the MN, paR and nAR respectively
- Authentication and Integrity protection must be provided to the messages between the MN and ARs (i.e. HKReq, HKResp, FBU and UNA).

**Msg1.** ***MN->pAR: HKReq[MN_HKS_MAC.{MSG$_{ID}$.PRF, CoA, N$_{MN}$}_HIK]***

***%where MN_HKS_MAC = H( MSG$_{ID}$.PRF, CoA, N$_{MN}$)***

**Msg2.** ***pAR->MN:HKResp[MN_AR_MAC{MSG$_{ID}$.PRF, CoA, N$_{pAR}$}_HK]***

***%where MN_AR_MAC = H(*** **MSG$_{ID}$.PRF, CoA, N$_{pAR}$)**

**Msg3.** ***MN->nAR: HKReq[MN_HKS_MAC.{MSG$_{ID}$. PRF. CoA. N'$_{MN}$}_HIK]***

***%where MN_HKS_MAC = H( MSG$_{ID}$.PRF, CoA. N'$_{MN}$)***

**Msg4.** ***nAR->MN:HKResp[MN_AR_MAC.{MSG$_{ID}$.PRF. CoA. N$_{nAR}$. MN_HKS_MAC.{}_HK']***

***%where MN_AR_MAC = H( MSG$_{ID}$.PRF, CoA.N$_{nAR}$)***

**Msg5:** ***MN->pAR: FBU, FBU_MAC***

***%where FBU_MAC = PRF(HK, NCoA, N$_{pAR}$)***

**Msg6:** ***MN->pAR: UNA, FBU_MAC***

***%where UNA_MAC = PRF(HK', NCoA, N$_{nAR}$)***

Figure 5.9: HLPSL specification of the secured FMIPv6

For secrecy, the specified goals indicate which values should be kept secret between participants. The HLPSL specification of the goals is shown in Figure 5.10.

```
goal

% the HIK(sec_hik_mn and sec_hik_ar) is secret

% between the MN and the pAR/nAR

secrecy_of sec_hik_MN, sec_hik_ar

% the HK(sec_hk_mn and sec_hk_ar) is secret

% between the MN and the pAR

secrecy_of sec_hk_MN, sec_hk_ar

% the HK'(sec_hk_mn and sec_hk_ar) is secret

% between the MN and the nAR

secrecy_of sec_hk_MN, sec_hk_ar

% authentication and integrity of the MN_HKS_MAC1

authentication_on pAR

% authentication and integrity of the MN_HKS_MAC2

authentication_on nAR

% authentication and integrity of the MN_AR_MAC

authentication_on mn

end goal
```

Figure 5.10: Goals for the HLPSL specification

The second goal of the security analysis is to make sure that the HK (i.e. sec_hk_mn and sec_hk_par) is kept as a shared secret between the MN and pAR.

The third goal of the security analysis is to make sure that the HK' (i.e. sec_hk_mn and sec_hk_nar) is kept as a shared secret between the MN and nAR.

The remaining goals are to authenticate and check for integrity protection of MN_HKS_MAC, MN_AR_MAC by checking a participant correctly believes that its intended peer belongs in the current session, has reached a particular state, and agrees on a value, which is typically fresh.

### 5.6.1.3 Verification of Results

As mentioned earlier, OFMC and CL-AtSe have been used as the two back-ends for the implemented HLPSL specification. For a comprehensive automated analysis, OFMC builds an infinite tree in a driven manner which is defined by the protocol analysis problem [125]. It implements efficient protocol falsification and also employs session verification without bounding the messages the intruder can generate [125]. CL-AtSe provides translated sets of constraints and states from the HLPSL specification to find attacks on the protocols [125]. Both these tools (i.e. OFMC and CL-AtSe) utilize the Dolve-Yao intruder model.

The results of the OFMC and CL-AtSe are shown in Figure 5.11 and Figure 5.12 respectively. The results illustrate that protocol is safe, which means that no attack was successful in breaking security requirements and goals set by the protocol specification.

```
% OFMC
        % Version of 2006/02/13
SUMMARY
        SAFE
DETAILS
        BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
        /home/avispa/web-interface-computation/./tempdir/hokey_fmipv6.if
GOAL
        as_specified
BACKEND
        OFMC
COMMENTS
STATISTICS
        parseTime: 0.00s
        searchTime: 0.26s
        visitedNodes: 8 nodes
        depth: 3 plies
```

Figure 5.11: OFMC Result

```
SUMMARY

        SAFE

DETAILS

        BOUNDED_NUMBER_OF_SESSIONS

TYPED_MODEL

PROTOCOL

        /home/avispa/web-interface-computation/./tempdir/hokey_fmipv6.if

GOAL

        As Specified

BACKEND

        CL-AtSe

 STATISTICS

        Analysed: 16 states

        Reachable: 4 states

        Translation: 0.03 seconds

        Computation: 0.00 seconds
```

Figure 5.12: CL-AtSe Result

## 5.6.2 Implemented Software Modules

This thesis has undertaken the software implementation of a system prototype of the functional components of FMIPv6 (fully compliant with RFC4068) integrated with the GSABA architecture. The goals of this system prototype are to provide the network integration validation and verification of the handover latency of the FMIPv6 in a GSABA service environment. Figure 5.13 shows the software reference architecture along with the required modules and interfaces.

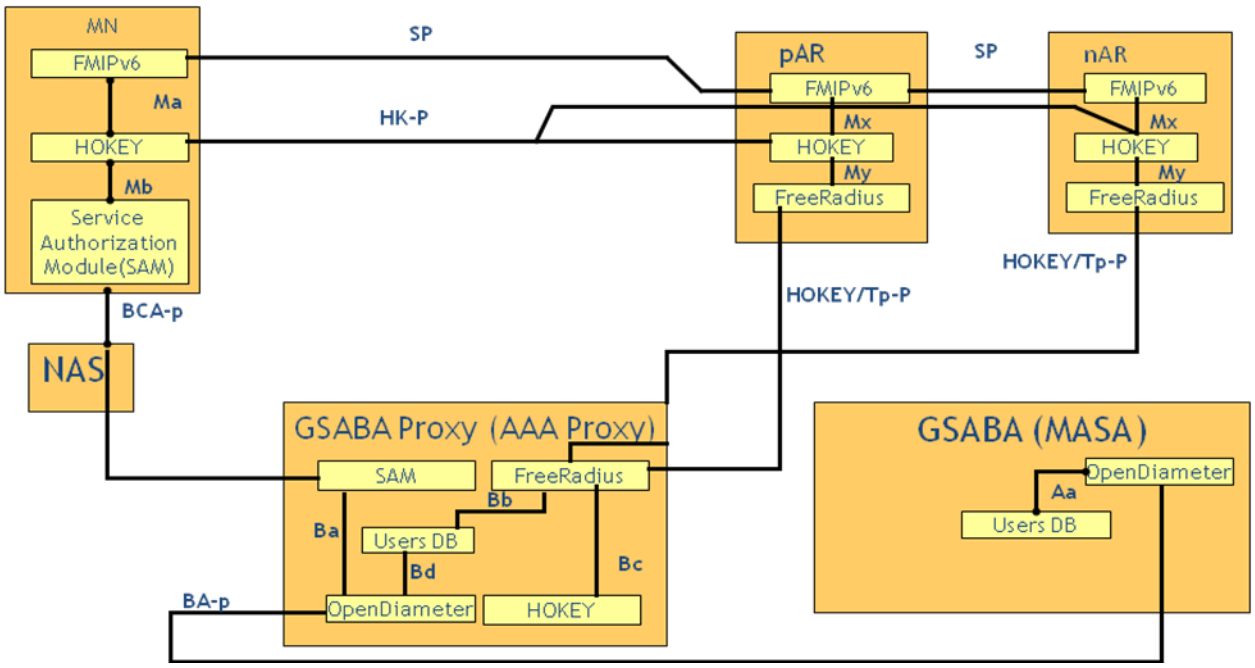


Figure 5.13: Modules and interfaces for FMIPv6 integrated with GSABA

The software architecture of the FMIPv6 / GSABA prototype contains the following components:-

- PAR
- NAR
- MN
- HA
- CN

The rectangles represent the software modules, namely FMIPv6, HOKEY, SAM, and FreeRadius. Meanwhile the main interfaces are represented with black connectors. For simplicity reasons the GSABA server and GSABA proxy have been co-located in the testbed development. Both software modules and interfaces are described in the following subsections.

### 5.6.2.1 MN

5.6.2.1.1 Service Authorization Module (SAM)

The SAM software module has been implemented using C programming language in Linux 'Ubuntu' distribution with kernel version 2.6.1. The result of implementing the SAM module at the MN side leads to the following interface:

***BCA-p***

The BCA-p interface is used for the communication between a MN and a GSABA proxy. This interface is intended to serve two purposes. Firstly, the configuration parameters needed for a specific service can be requested from the MN. Secondly, the authorization decision taken by the network is conveyed to the MN.

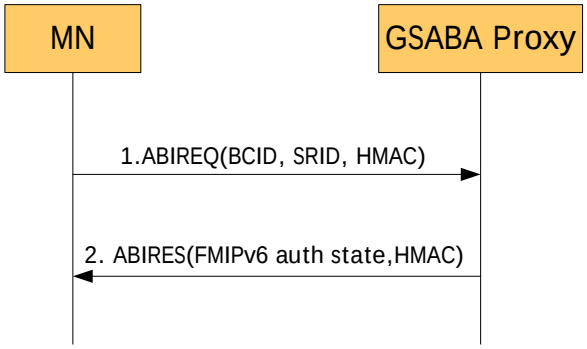


Figure 5.14: Message flows for FMIPv6 service Authorisation

After the GSABA key has been established, the MN and the GSABA proxy can exchange service configuration and authorisation information carried out by the ABIREQ and ABIRES messages via the BCA-p interface.

**HTTP/TLS** has been used to realise the functionality of the BCA interface. For this purpose **Openssl-0.9.8e** is installed and configured at both the MN side and the GSABA Proxy side. Apache-2.2.4 server is installed and configured at GSABA Proxy side.

***Mb***

Mb is an internal interface between the SAM and the FMIPv6 module. The SAM module uses the Mb interface to pass authorization values (i.e. success/failure) to the FMIPv6 module.

5.6.2.1.2 HOKEY (MN)

The HOKEY software module at has been implemented using **C programming language** in **Linux 'Ubuntu'** distribution with **kernel version 2.6.23-rc3**. This software module is in complete compliance with the [38]. The result of HOKEY module implementation is the creation

of the HK-p interface and Ma internal interface. Given below is the description of each of these interfaces.

***HK-p***

The HK-p is an external/network interface between the MN and AR. The HK-p is bidirectional in nature and through this interface the MN can retrieve the Handover Key (HK/HK') to protect the handover messages between the MN and the AR. With respect to the FMIPv6 application, the HK-p interface includes two aspects: one is the interface between the MN and pAR. The other is the interface between the MN and nAR.

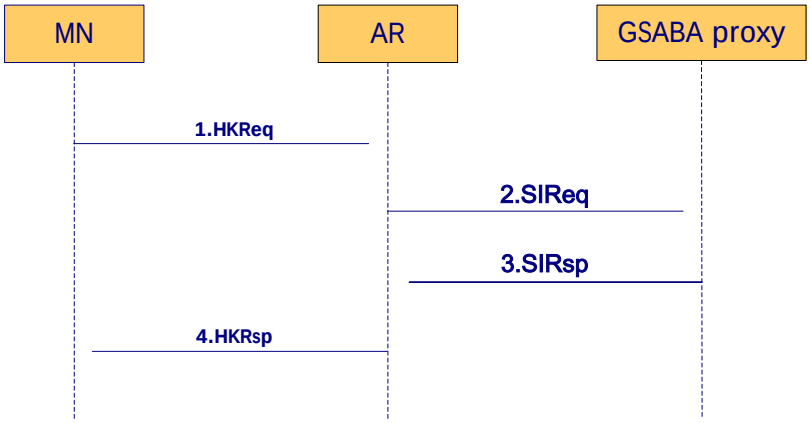


Figure 5.15: Message Flow for HOKEY

After bootstrapping and service authorization, the MN sends the Handover Key Request (HKReq) message to the serving access router (pAR). The HKReq message is created by the MN which contains the CoA, Network Access Identifier, message ID and the desired PRF algorithm. The HKReq also contains a MAC composed from the message fields which is included in a MN-AAA MAC Mobility sub-option. A timestamp mobility option should be included in the HKReq message for replay protection. Upon successful delivery of the HKReq, the HOKEY module waits for the HKResp message from the pAR.

On receiving a successful HKResp message, the MN checks to ensure that the MN-AR MAC mobility option exists [38]. The message will be silently discarded if it does not contain the MN-AR MAC mobility option [38]. If there is a mismatch between Message ID with that of the corresponding HKReq, the MN must also discard the packet [38]. Using the keying material existing in the HKResp message, the MN computes the handover key. The AUTH Value in the MN-AR MAC mobility option must be verified using the derived HK [38]. The HKResp

contains a MAC algorithm in the MN-AR mobility sub-option which must be supported by the MN, or else it must discard the message [38]. In the event of an AUTH Value verification failure, the MN will discard the message [38].

Once the HKResp has been successfully processed and a valid HK is derived, the MN stores the SPI and the associated key lifetime received from HKResp message [38]. Figure 5.16 and 5.17 illustrates the format of the HKReq and HKResp respectively.

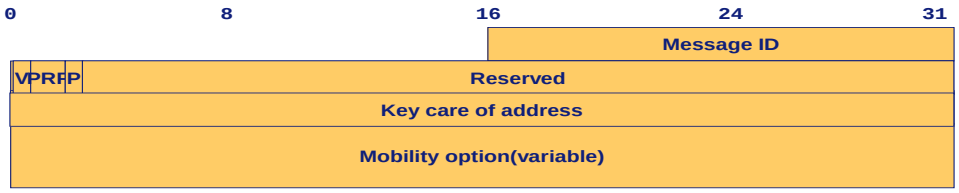


Figure 5.16: HKReq mobility header

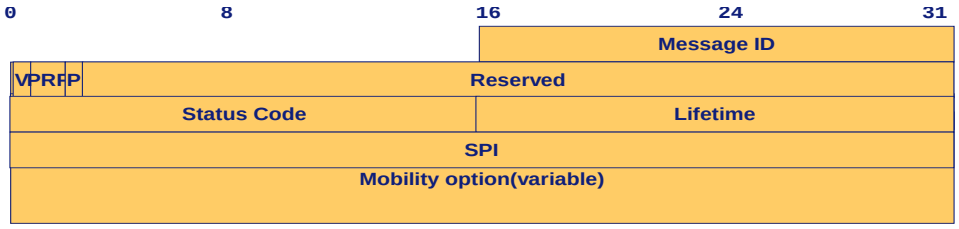


Figure 5.17: HKResp mobility header

***Ma***

After the HK processing with pAR, the MN will store the HK (between MN and pAR) and the related parameters (such as SPI and lifetime).

After the MN finishes the scanning, and before handover processing starts, the MN will do the HK' processing with the recommend nAR and store the HK' (between the MN and nAR) and the related parameters (such as SPI and lifetime).

So, at least 2 sets of HK parameters exist sometimes in the MN. For this purpose a structure to store the HK related parameters has been defined. The structure is:

```
struct hk_para{
uint16_t liftime;
uint32_t spi;
uint8_t  hk[12];            /*96 bits*/
struct in6_addr *ar_addr;  /*to distinguish which AR the HK belong to*/
};
```

Then a global variable is defined: ***struct hk_para* ar_hk_para;**

After the MN handles the received successful HKResp message from the pAR, the MN will store the HK parameters in the ar_hk_para structure.

After the MN handles the received successful HKResp message from the nAR, the MN will store the HK parameters in the ar_hk_para structure.

There are 2 other global variables defined:

```
struct hk_para mn_par_hk_para;
struct hk_para mn_nar_hk_para;
```

While the MN does the scanning procedure, the ar_hk_para variable is copied to mn_par_hk_para and during the MN handover procedure the ar_hk_para is copied to the mn_nar_hk_para.

Now the FMIPv6 module can get the HK (between the MN and the pAR) from the mn_par_hk_para variable to protect the FBU/FBack message, and can get the HK' (between the MN and the nAR) from the mn_nar_hk_para variable to protect the UNA message.

**Note:** the code for more than one nAR is for future work.

5.6.2.1.3 FMIPv6 (MN)

The FMIPv6 module in the MN uses the open source code developed by [52]. Brunel University has modified the source code in a **Linux 'Ubuntu'** distribution under the **2.6.23-rc3 kernel** version. The FMIPv6 at the MN is used for all the FMIPv6 signalling which is compliant with [7]. The modifications/extensions made by Brunel contribute to the creation of the SP interface.

***SP***

The SP interface is service specific and is the interface between the MN and ARs. The protocol used to implement this interface is [7] which is available as open source and distributed under the GNU General Public License.

It is very important to note here that source code in the MN needs to be modified to have a new mobility authentication option. This allows the Fast Binding Update (FBU) to be securely sent (i.e. in terms of integrity of the message, and authentication) from the MN to the pAR. The Fast Binding Acknowledgement (FBack) sent by the pAR in response to the FBU needs to be secured in the same way. Also, the UNA sent by the MN to the nAR needs to be secured using the mobility authentication option as well.

The new mobility authentication option should be in the form of a Message Authentication Code (MAC) and is described in [104]. A MAC is a "short piece of information used to authenticate a message. A MAC algorithm accepts as input a secret key and an arbitrary-length message to be authenticated, and outputs a MAC (sometimes known as a tag). The MAC value protects both a message's integrity as well as its authenticity, by allowing verifiers (who also possess the secret key) to detect any changes to the message content" [126].

The format of the MN-pAR and MN-nAR (i.e.FBU, FBack and UNA) mobility message authentication option is illustrated in Figure 5.18. The FBU and FBack messages are authenticated using the MN-pAR message authentication option [104]. In a similar manner, the UNA message is authenticated using the MN-nAR mobility option. There is an existing SA which consists of a key, authentication algorithm, mobility SPI and a replay protection process, between the MN and the pAR/nAR based on shared-key principles [104]. The key has an arbitrary length of 16 octets, and HMAC_SHA1 is used as the authentication algorithm [104]. As specified in [104] a sequence number or a Timestamp option may be used for providing a replay protection mechanism. The last option in the FBU and FBack message is the mobility message authentication option.

The encryption algorithms for HMAC available in **Linux (Ubuntu distribution, kernel 2.6.23-rc3)** are available in a package called **libdigest-hmac-perl (1.01-1)**. The encryption algorithms included in the package are MD5 and SH1.

The shared secret key (in this case, the HK key) is derived from the Handover Master Key (HMK).

The details of the format of the MN-pAR and MN-nAR mobility message authentication option are presented in [104].


Figure 5.18 MAC mobility option

### 5.6.2.2 ARs (pAR & nAR)

The ARs also use the open source code developed by [7]. Brunel University has modified the source code in [7] in a Linux 'Ubuntu' distribution under the 2.6.23-rc3 kernel version. The FMIPv6 at the AR is used for all the FMIPv6 signalling which is compliant with [7]. With the GSABA architecture requiring secure FMIPv6 handover, the following interfaces were created:

#### 5.6.2.2.1 Free Radius

The Free Radius software module at the AR is implemented in Linux 'Ubuntu' distribution with kernel version 2.6.23-rc3. The result for implementing Free Radius module at the MN side leads to the following interface:

***Hokey/Tp-p***

The Tp interface is used for communication between the AR and the GSABA Proxy/Server. Free Radius module functionality is implemented using [27] which is the premier open source RADIUS server (released under the GNU General Public License). SIREQ and SIRES messages are exchanged on this interface to transport the handover keys (i.e. HK and HK') from the GSABA Proxy to the ARs (i.e. pAR and nAR). The SIREQ message contains CoA, MN ID, message ID, life time and SPI. There are no existing AVPs for sending all the parameters. So,

two different protocols for this purpose have been used. The MN ID is sent via standard radius protocol and the remaining parameters are sent via standard SQL query which directly updates the user Database. SQL updates are only allowed from specified IP addresses of ARs on the database server to prevent un-authorized access. The RADIUS packet format is shown in Figure 5.19.

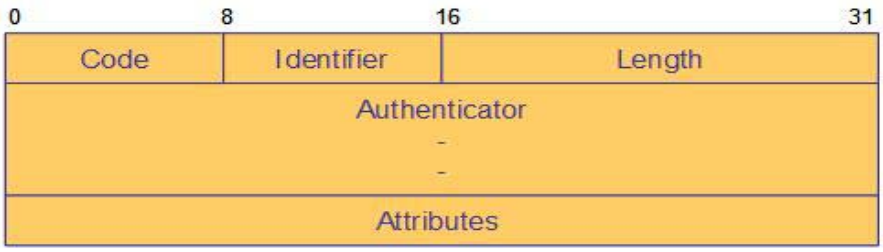


Figure 5.19: Tp Interface Message format

- Code: specifies type of RADIUS packet
- Identifier: specifies the RADIUS response with the correct outstanding request
- Length: specifies the length of the packet
- Authenticator: sixteen octets long and contains the information that the RADIUS client and server use to authenticate each other
- Attributes: is a section where an arbitrary number of attributes are stored.

The attribute section of the packet is used to send the MN ID to GSABA server, if it is verified correctly the GSABA would reply with an AAA-Nonce, GSABA time-stamp and handover keys.

***My***

My is the internal interface through which the Free Radius Module passes the handover keys (HK and HK') to the HOKEY module of the ARs. This interface has been implemented using C Programming language.

***Mx***

Upon receipt of a successful AAA response (i.e. SIREQ) from the GSABA Proxy, the AR must store the received handover key along with the CoA and MN ID [38].

The HKResp message sent by the AR to MN must contain parameters received in the RADIUS message which are the SPI, lifetime and AAA nonce [38]. The HKResp also contains a MAC of

the message created using the HK which is received in the MN-AR MAC Mobility Sub-Option [38].

When the AR sends the HKResp message to the MN, it should use the handover keys (HK/HK') to calculate the MAC to protect the HKResp message; and during the handover procedure, the AR should use the HK to protect the FBack message.

So the Mx interface functionality is how the HOKEY module gets the HK for calculating the MAC to protect the HKResp message. Also, the Mx module is used by the HOKEY module to the pass the handover keys (HK and HK') to the FMIPv6 module for protecting the FBack and UNA messages.

So a global structure variable is defined to store the received handover keys (HK/HK') from the GSABA at the AR side. The structure is:

```
struct hokey_para{
 uint32_t spi;
 uint8_t  hk[12];              /*96 bits*/
 struct in6_addr *coa;
struct in6_addr *mn_id;
uint16_t status_code,
uint16_t lifetime,
uint8_t ho_nonce[16]
uint8_t timestamp[8]
};
```

Then a global variable is defined**:** ***struct hokey_para mn_ar_hokey_para***

After receiving a successful AAA response (SIResp), the AR stores the HK/HK' parameters to the mn_ar_hokey_para global variable, and when the HK/HK' are needed at the AR side, it is from this variable that they are constructed. The following parameters:

***uint16_t status_code,***

***uint16_t lifetime,***

***uint32_t spi,***

***uint8_t ho_nonce[16]***

***uint8_t timestamp[8]***

will be sent to the MN using the hokey_ar_send_hkrsp( ) function. They can be read from the global structure variable: mn_ar_hokey_para.

5.6.2.2.2 HOKEY (AR)

The HOKEY software module at the AR has been implemented using **C programming language** in **Linux 'Ubuntu'** distribution with **kernel version 2.6.23-rc3**. This software module is in complete compliance with [38]. The HOKEY module at the AR leads to the following interfaces:

***The HK-p***

As mentioned earlier in 5.6.1.2 and 5.6.2.2, the HOKEY modules at the MN and the ARs are connected through the HK-p interface. The HK-p interface is bidirectional in nature and the AR side of it is used to transmit parameters through which the handover keys (i.e. HK and HK') at the MN could be retrieved. On receiving a successful HKReq message, the AR checks to ensure whether or not any pending request exists with same Message ID [38]. If there is a match, and an AAA response corresponding to the Message ID is present, then AR retransmits the HKResp [38]. For further information on retransmissions, replay protection and message uniqueness validation, please refer to [38].

As mentioned earlier in this chapter, on receipt of a successful AAA response from the GSABA Proxy, the AR stores the received handover key along with other parameters such as CoA and

MN ID. The HKResp must contain a MAC of the message created using the HK/HK' which is received in the MN-AR MAC Mobility Sub-Option [38].

5.6.2.2.3 FMIPv6 (AR)

The FMIPv6 module in the pAR and nAR uses the open source code of [52]. Like the FMIPv6 module at the MN, the FMIPv6 in the ARs (both the pAR and nAR) has been modified/extended by Brunel University. The FMIPv6 protocol at the pAR is responsible for sending the FBack upon receipt of the FBU from the MN. The following interfaces are created and used by the FMIPv6 module at ARs (i.e. pAR and NAR).

***SP***

The pAR and nAR will use the SP interface to securely send the FBACK to the MN. Also, the UNA message is sent securely from the MN to the nAR via the SP interface. For this reason, the 'fmipv6.org' source code [52] in the ARs has been modified to have a new mobility authentication option as described in section 5.6.2.1.3 of this thesis.

The new authentication option should be in the form of a MAC described in [104]. The MAC for the FBack is calculated using the shared secret between the MN and the pAR (i.e. HK) and the MAC for the UNA is calculated using the shared secret between the MN and the nAR (i.e. HK').

### 5.6.2.3 GSABA Server

Apache-2.2.4 server is installed and configured at the GSABA Proxy side to run in a Linux 'Ubuntu' distribution environment with kernel version 2.6.1. The Apache server (i.e. GSABA Proxy) hosts the Free Radius and the User DB modules. Free Radius module functionality at the GSABA Proxy is implemented using [27].

***Bb/Aa***

Bb/Aa is an internal interface of the GSABA server which is used between the user database and FreeRadius. FreeRadius supports different database servers including MySQL which is used in this case. Simple SQL queries are run over this interface.

### 5.6.3 The Test-bed

The software components for the FMIPv6 integrated with the GSABA architecture is illustrated in Figure 5.13. The actual layout of the FMIPv6 integrated with the GSABA architectural components is shown in Figure 5.20.

#### 5.6.3.1 Requirements

In this section, the hardware and software requirements for the test-bed are outlined.

##### 5.6.3.1.1 ARs (pAR & nAR):

The hardware and software requirements for the ARs are:

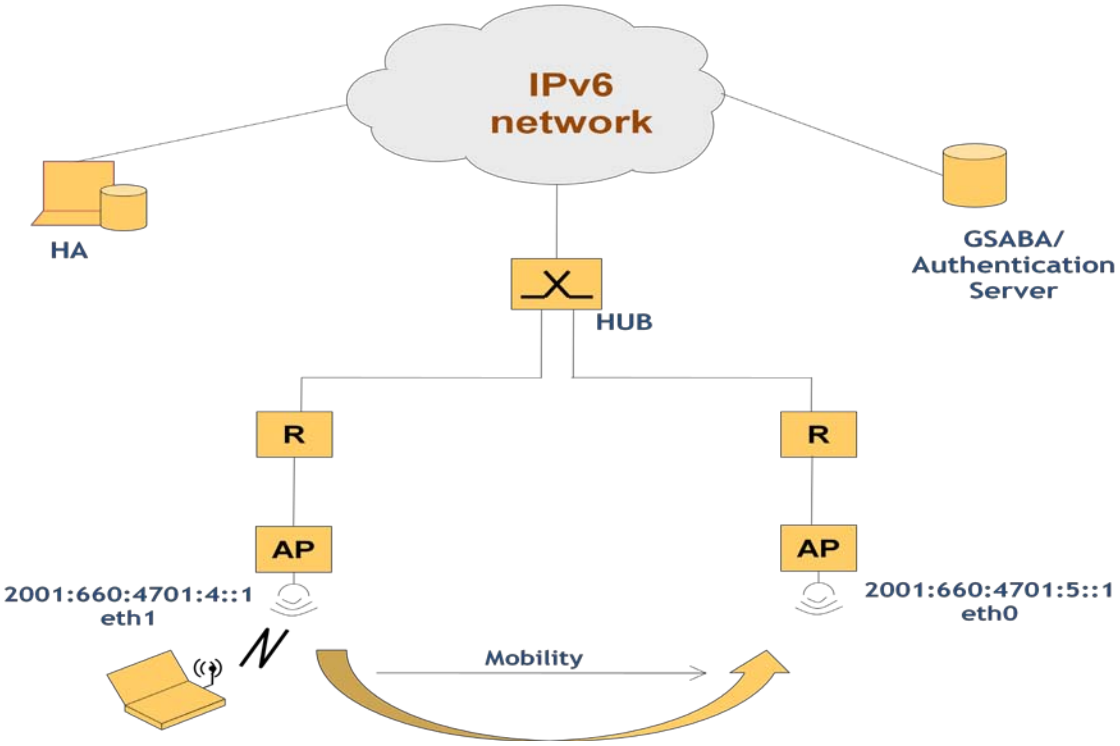


Figure 5.20: Layout of the Test-bed

**Hardware Requirements:**

- The ARs are optimized Linux boxes (i.e. PCs).
- Wireless cards based on an Atheros chipset with a Madwifi driver were used to provide

router functionalities.

**Software Requirements:**

- The operating system (OS) system used was Linux (Ubuntu distribution).
- Universal Mobile IP (UMIP) package was used for Mobile IPv6.
- The Quagga Routing Suite was used for providing routing functionality. RIPv3 was the routing protocol used.
- The ARs hosted the fmip-ar daemon implementation which is originally developed by fmipv6.org [52], but later modified and extended by Brunel University (UK) and Huawei Technologies (China).
- For router advertisement (RAs), Radvd was used.

#### 5.6.3.1.2 MN:

The hardware and software requirements for the MN are:

**Hardware Requirements:**

- The MN was a linux based machine (i.e. PC) with a wireless card based on an Atheros chipset.

**Software Requirements:**

- Again, the operating system (OS) system used was Linux (Ubuntu distribution).
- The MN was also running UMIP and with a modified implementation of the fmip-mn daemon (original source code from fmipv6.org).

#### 5.6.3.1.3 HA:

The hardware and software requirements for the HA are:

**Hardware Requirements:**

- The HA used was linux based box with an Ethernet card.

**Software Requirements:**

- As with other nodes in the testbed, Linux kernel version 2.6.23-rc3 with UMIP was used as

the OS core.

- Radvd was used for routing advertisements.
- The Quagga Routing Suite was used for providing routing functionality. RIPv3 was the routing protocol used.

#### 5.6.3.1.4 GSABA Proxy/Server (AAA Server):

The hardware and software requirements for the GSABA Server/Proxy are:

**Hardware Requirements:**

- The GSABA Proxy/Server server was a Linux machine (Ubuntu Distribution) with kernel version 2.6.23-rc3.

**Software Requirements:**

The GSABA Proxy/Server hosted an Apache (web server) with SSL support, modified FreeRadius server and Quagga routing daemon.

### 5.6.3.2 Test-Scenarios

For the purpose of a complete and consistent evaluation, three distinct scenarios were evaluated. The first scenario is the Predictive FMIPv6 operation over the GSABA architecture. The Second Scenario highlights the Reactive handover, and the third scenario illustrates the handover of a plain MIPv6 process. In all three scenarios, the MN undergoes an IPv6 handover by moving between AP1 and AP2 which are respectively connected to AR1 and AR2 belonging to different IP subnets. All the scenarios have been executed with a series of tests in which the MN receives a video stream from the CN using VLC player [54]. In the Video stream, data is sent as Real-time Transport Protocol (RTP) packets [55]. RTP packets have an average approximate length of 1336 bytes and are sent every 30ms.

#### 5.6.3.2.1 Performance Evaluation

In this section the results obtained from the test-bed are analyzed in detail and benchmarked with other similar well known and validated test models/cases.

**Predictive Handover**

The results presented in this section are obtained, by running the Wireshark tool [56] on the MN, CN and ARs, as well as using the timestamps displayed on the console of the MN, provided by the FMIPv6 suite when executed in a debug mode. Figures 5.21 and 5.22 present the predictive handover case. Figure 5.21 shows that the MN does not loose a single packet during handover. At 60.12 seconds after the entire process is started, the MN sends a HKReq to the pAR, and receives an HKResp after roughly 86ms. At 60.14 seconds, the MN senses that its signal from the currently attached AP has dropped below a certain threshold. Such a situation occurs because the signal strength of the AP that the MN was attached to was manually degraded by reducing the Tx power of the pAR, thus forcing it move to the nAR's link. Before the MN moves to the nAR's link, it has sufficient time to send the HKReq to the nAR and get an HKResp back with a RTT of 94ms. The L2 handover period, which is also the service interruption period (i.e. no packets being sent or received by the MN), is approximately 19ms. However, such a short handover period was only possible with the exclusion of the scanning time from the overall L2 handover time.

During the tests it was observed that the scanning process takes about 1.2-3.5 seconds depending on the type of wireless card used. On average, the Atheros based chipset card capable of 802.11b/g had a scanning time of about 1.9 seconds. However, the scanning time is largely dependent on the test environment (e.g. number of surrounding APs to be scanned). Such findings support the empirical studies in [57]. Due to the long scanning delays, a dual wireless interface was used; one for scanning purposes only, and the other for the actual FMIPv6 communication. As mentioned earlier, the MN in shown in Figure 5.21 incurs zero packet loss. This is possible only due to the tunnel established between the pAR and nAR. The tunnel was active for 150 ms which means the MN had sufficient time to move the nAR's link and send the UNA message to receive the buffered packets.

The results in Figure 5.21, support the findings in [93] and [94], where under similar conditions, FMIPv6 practical test-beds were deployed in an effort to study the effects of handover latencies. The connection loss times (i.e. handover delay) in [93] and [94] are around 10.5 ms which is 8.5ms more than the loss times shown in Figure 5.21. The small difference in handover latency can be attributed to the L2 trigger event delivery mechanism that exists in Linux based Operating

Systems. The conditions, under which these triggers are sent via RTNETLINK sockets, are specific to driver behaviour. Even though there is intensive work undergoing on standardising them, they are not currently standardised as yet [93].

As mentioned earlier, the handover latency depicted in Figure 5.21 shows the handover latency where the scanning time is not included in the L2 handover. This is the reason why the overall handover latency is minimal (i.e. 19ms).

In Figure 5.22, another case of predictive handover is shown. This time, only one wireless interface is used, and as result, the scanning time is imposed on the overall handover. The service disruption period (i.e. L2 handover) takes roughly 1.3 to 2 seconds, which is a drastic increase, when compared with the handover latency in Figure 5.21. Also, notice that due to the long handover latency, the packets at the nAR's buffer arriving from the tunnel are dropped due to the long queue at the nAR's buffer. As a result, 65 packets are dropped/lost causing substantial service interruption.

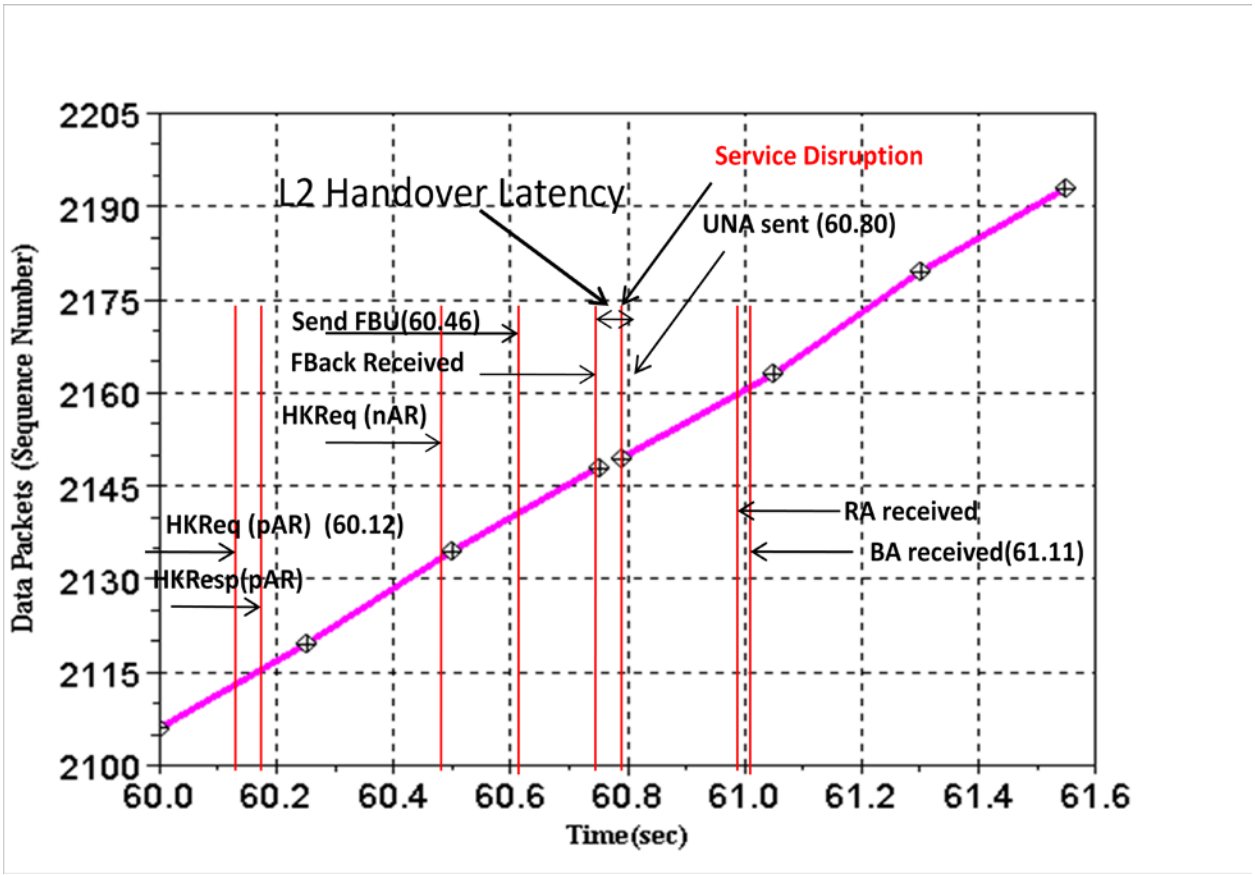


Figure 5.21: Predictive Handover (a)

The increase in the overall handover times presented in Figure 5.22 is quite drastic compared to the results shown in Figure 5.21 and the results of [93] and [94]. The low handover latencies reported in [93] and [94] are achieved by modifying the wireless drivers and also by using a secondary wireless interface for scanning purposes only. Such modifications are quite unrealistic since it cannot be expected that MNs will have a secondary interface just to reduce the L2 scanning time. The results in Figure 5.22 support the results of the mathematical analysis of [117], where the overall handover latency increases as the L2 switching delay (i.e. handover) increases. Due to the increase in the total handover delay, the buffer length at the nAR increases (as shown in equation (31) of chapter 4), which leads to packets being dropped and results in re-transmissions of FMIPv6 signalling, and hence the overall handover latency increases.

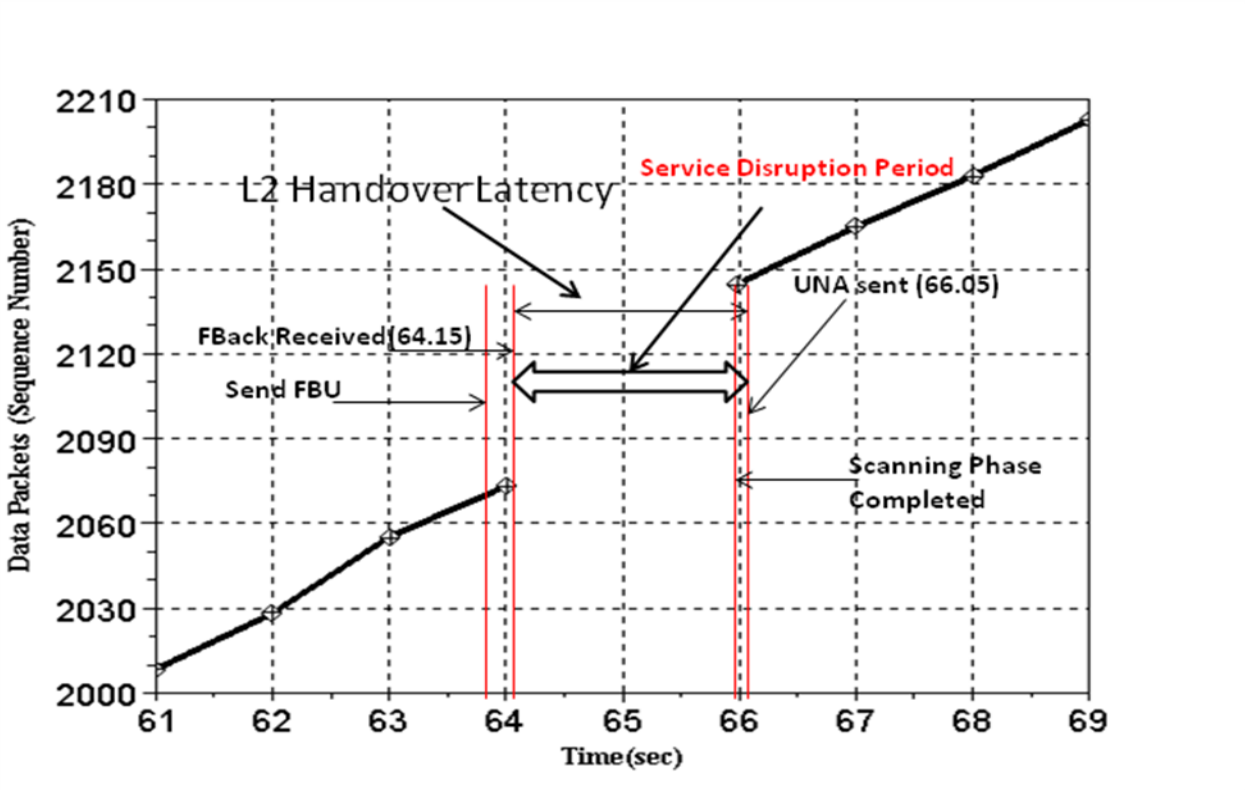


Figure 5.22: Predictive Handover (b)

**Reactive Handover**

When a handover cannot be predicted because of a sudden drop or loss in signal from its attached pAR (i.e. link loss before the FBU is sent or the FBack received), the MN performs a

Reactive handover. Prolonged service interruption is expected, since the MN would first execute a scanning process, and on completion would attach to an AP. Depending on the available channels and APs, it takes about 1.3-2 seconds for the entire scanning process to complete. During the testing of the reactive handover, the MN was forced to change its PoA by manually closing down the wireless interfaces of the pAR.

The MADWiFi driver detects the link failure through missing beacons. During the testing the driver uses the default value of 7 beacons. Upon completion of a scan, the FMIPv6 software module will try to connect to the AR with the greatest signal strength. In the event of no scanning being performed before the link is broken, the FMIPv6 software module would execute a scanning process to make a list of candidate ARs. On establishing L2 connectivity, the MN sends a UNA message to the nAR followed by a FBU to the pAR. As shown in Figure 5.23, it takes roughly 1.89 seconds to complete a reactive handover. Moreover, since there has been no buffering or tunnelling (the pAR would tunnel packets for the MN only after receiving the FBU from the MN), a substantial loss of 50 packets was incurred.

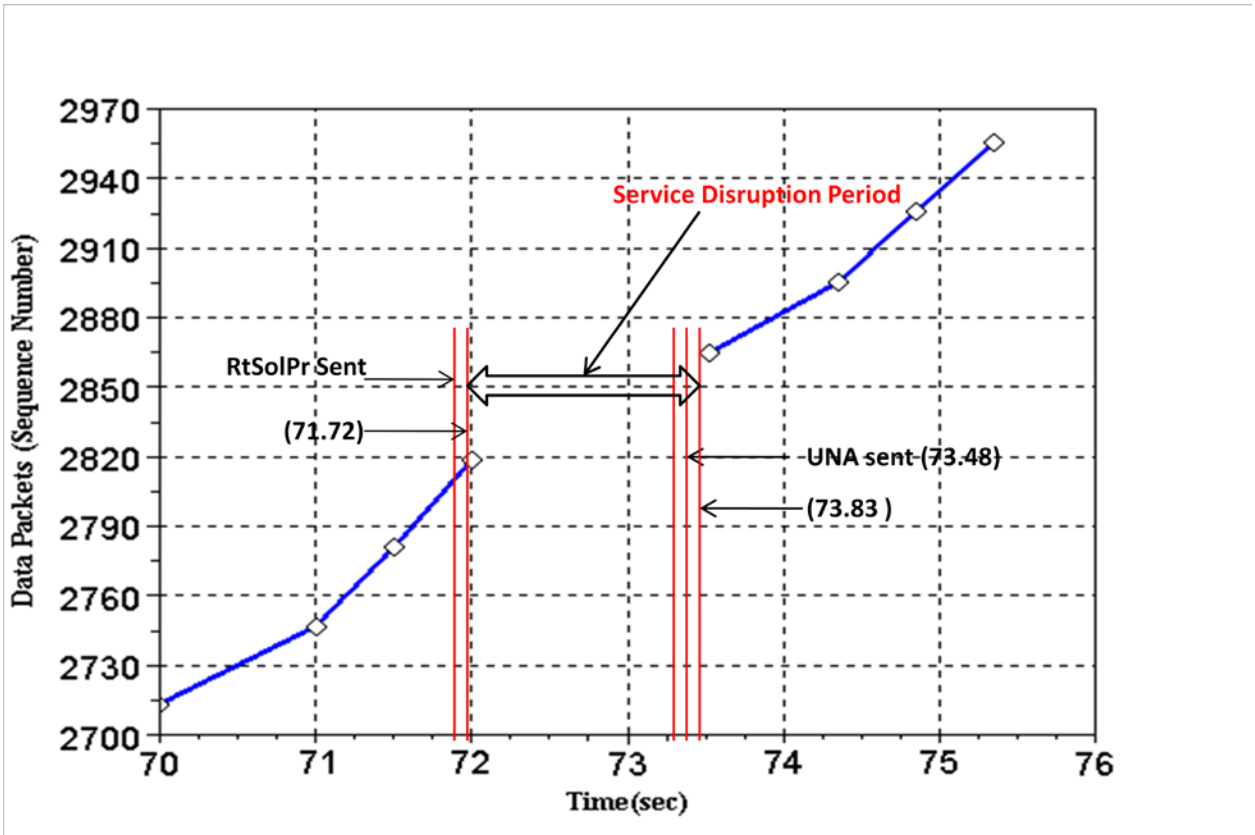


Figure 5.23: Reactive Handover

The results illustrated in Figure 5.23 correspond to the in results [73] where an optimized solution is proposed which considers the available timing and accurate criteria of L2 triggers. The average reactive handover time in [73] is around 100 ms more than the results presented in Figure 5.23, which could be due to the different hardware used (i.e. wireless cards), which has an impact on the scanning time, or even due to varying channel and link conditions (low SNR, low throughput, queuing delays). Since in the reactive handover, the MN does not accurately provide L2 triggers (i.e. the MN moves to the new PoA without anticipating a handover), the overall handover latency drastically increases.

**Plain FMIPv6**

The results for the plain FMIPv6 (with a single wireless interface) are presented in Table 5.1. Average handover latency is calculated from five consecutive experimental runs.

The handover for the proposed mechanism is the same as that of plain FMIPv6 handover. This is expected since the proposed mechanism (i.e. secured FMIPv6 over GSABA) performs all the required signalling pro-actively (i.e. before the handover occurs). However, the signalling overhead of the proposed mechanism would be much higher compared to the plain FMIPv6 process. Also, the computation overhead (due to secured signalling) for processing the packets at the MN and the ARs would be slightly higher compared to plain FMIPv6. Such overheads are negligible and have no significant effect on the overall handover process.

As mentioned earlier, the results in Table 5.1 drastically differ from the findings of [93] and [94] due to the inclusion of the scanning time in the overall handover latency.

| | ***Run 1*** | ***Run 2*** | ***Run 3*** | ***Run 4*** | ***Run 5*** | ***Average*** |
|---|---|---|---|---|---|---|
| ***Handover Latency*** | 1.98sec | 1.90sec | 2.0sec | 1.93sec | 1.87sec | 1.94sec |

Table 5.1 Plain FMIPv6 handover latency (single wireless interface)

**MIPv6 Handover**

The MIPv6 handover is very similar to that of the reactive case for FMIPv6. The MIPv6 protocol takes no advantage of any kind of L2 triggers to anticipate a handover. As result, the MN in

Figure 5.24 was forced to wait until it detected a link failure only after it moved to the new AR's link. The MN detects the link failure through beacon messages sent from the AP. The default value set for the MIPv6 test case is 7 beacon frames. Unlike the FMIPv6 handover process, MIPv6 incurs a L3 handover latency, which simply means that the MN is unable send or receive any IP packets until the movement detection and BU process are complete. The movement detection process involves receiving a RA and the BU process involves formulating a CoA and sending it to the HA. In Figure 5.24, L2 handover takes 1.3 seconds (with a single wireless interface). The RA is received 50ms after the termination of the L2 handover. The BU process takes 610 ms which includes the DAD time. As a result, the overall MIPv6 handover latency is approximately 2 seconds. The pattern of the results found in Figure 5.24 is similar to that of [73]. However, there are some differences. For example, CoA address configuration takes almost 790 ms longer in [73] compared to results in Figure 5.24. Such an increase in the CoA configuration time could be due to differences in RA intervals which seem to be a lot higher than the MIPv6 test case presented in this chapter, which is set to 70ms. Also, it could be due to the fact that the result in [73] is possibly based on a lower transmission rate of IEEE802.11 beacons compared to the results of Figure 5.24.

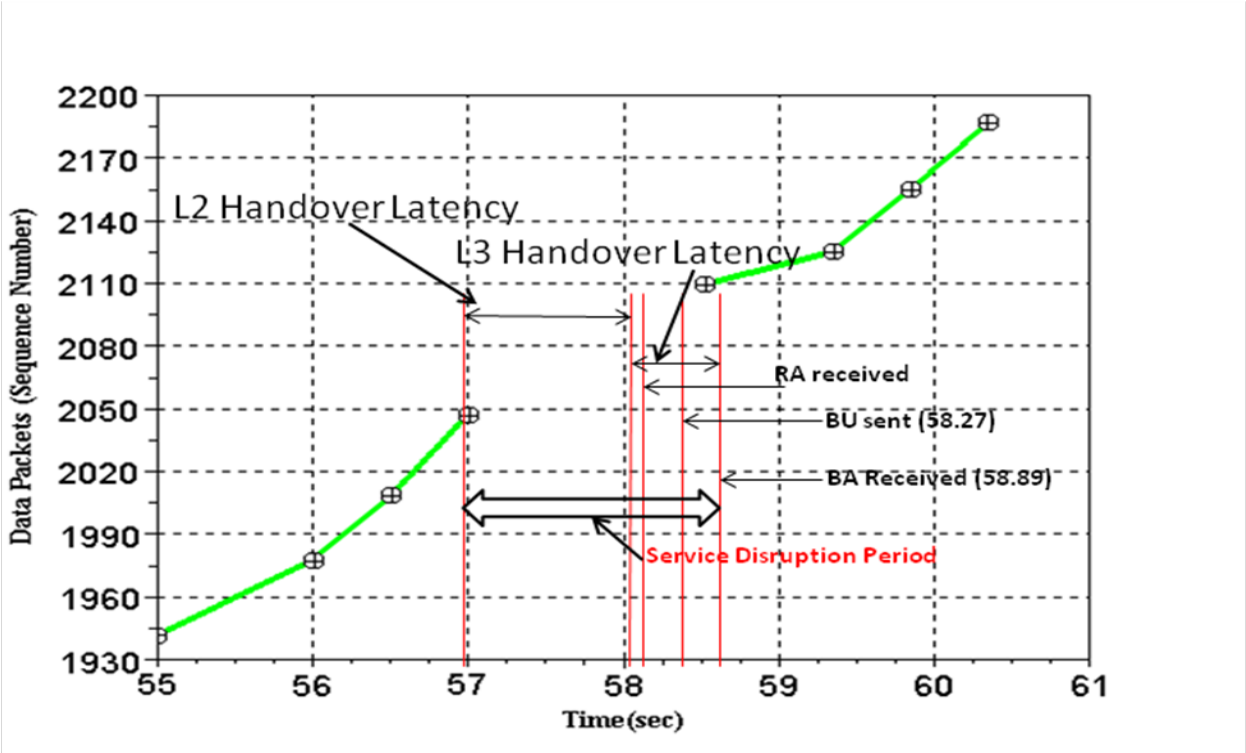


Figure 5.24: MIPv6 handover

## 5.7 Summary

In this chapter, a novel FMIPv6 bootstrapping and authorization architecture is presented in order to provide the MN with necessary configuration parameters and distributed keying materials to secure FMIPv6 messages in terms of authentication and authorization. The experimental results suggest that the proposed mechanism can provide seamless mobility with almost no packet loss. However, this is only the case when a secondary primary interface is used for the L2 scanning phase. The handover latency for all three solutions drastically increases when only one wireless interface is used. Still the results suggest the proposed mechanism has no adverse effect on the overall handover latency due to the additional signalling and computational overhead it brings compared to plain FMIPv6. As expected the proposed mechanism drastically outperforms plain MIPv6.

Also, a security analysis of the secured FMIPv6 along with the newly defined protocol/interfaces of the GSABA architecture has been done using a formal tool (i.e. AVISPA). The results suggest that the proposed mechanism is secure (i.e. safe) from the potential security threats it introduces.

# CHAPTER 6- IEEE802.21 Assisted Fast Re-authentication Scheme over GSABA

## 6.1 Introduction

One of the key characteristics of NGNs is the diversity of access technologies (e.g. 802.11a/b/g, 802.16e, UMTS etc.) that are available to end-users, and the ability to roam across these networks. With such a proliferation of heterogeneous access networks, it is only natural that mobility would also increase, creating demands for ubiquitous connectivity and pervasive services. However, roaming often implies a temporary service disruption due to handover from one PoA to another. Such a disruption is unacceptable for QoS stringent applications, such as VoIP, video conferencing, streaming media, etc. As discussed in previous chapters of this thesis, various mechanisms, namely, MIPv6 and FMIPv6 have been specified by the IETF as mobility standards to tackle the issues associated with handover latencies at the IP (i.e. L3) layer. Similarly, there are media specific mechanisms intended to improve the L2 handover, such as, the handover optimization in 802.16e and the fast BS transition in 802.11r [71]. Also, the IEEE802.21 WG has developed a standard for cross-layer interactions to enable handover and interoperability between heterogeneous network types including both 802 and non 802 networks [13].

Wireless handover between PoAs (APs, BSs) is typically an intrinsic process that involves several layers of protocol execution [119], which results in long latencies causing undesirable service disruptions. It must be noted that additional latencies are incurred for networks, or a mesh of integrated networks (e.g. NGNs as described in previous chapters), due to AAA services. EAP based solutions will play a fundamental role in NGNs by providing a generic authentication framework. However, such solutions are responsible for contributing significantly to the overall handover latency. This is due to the fact that, existing EAP implementations run a full EAP method (a very time-consuming process) when a MN encounters a new authenticator (i.e. PoA), irrespective of whether it has been authenticated to the network domain recently and has unexpired keying material [119]. Additionally, the home domain is contacted each time the MN is authenticated and this may introduce long delays when the home domain is far way (e.g. inter-continental). The home domain is expected to send keys to the access devices (e.g. APs, ARs) within the visited domain for establishing security associations.

Within the IETF, several alternatives have been proposed to reduce the handover delay when EAP authentication is required. The PANA WG has proposed mechanisms to pre-authenticate users to a new domain while connected to their current PoA in [53]. On the other hand, the HOKEY WG has been responsible for developing solutions [60], [61], [62], and [63] for providing fast re-authentication mechanisms without re-executing a full EAP method and re-using EAP derived keying material for handovers. However, such solutions either method specific or method independent, suffer from issues such as high signalling overheads and require major changes to the EAP protocol.

Recently, the IEEE802.21 WG has formed a task group (TG), known as IEEE802.21a to investigate the potential of applying MIH services to reduce latency caused by authentication and key establishment during handovers between heterogeneous access networks [121]. However, IEEE802.21a is in its infancy at the moment and there is a lack of clearly defined solutions to the question of how to use existing 802.21 MIH services to aid in the optimized re-authentication process.

Concurrently, the 802.21a TG has also undertaken the responsibility to provide solutions for confidentiality, data integrity, data origin authentication and replay protection for the IEEE 802.21 MIH protocol exchanges and allow for MIH services to be authorised [121]. At the moment, no such solution has been specified by the 802.21a TG. As a result there is great need to define mechanisms for 802.21 service authorization, and also for SAs to be established, so that IEEE802.21 MIH protocol messages are securely exchanged between end-points.

In this chapter, a novel IEEE802.21 assisted EAP based Re-Authentication scheme over a service authorization and bootstrapping framework (i.e. GSABA) is presented. The purpose of the proposed scheme is to reduce the signalling latency during the EAP re-authentication process, and as a result reduce the overall handover delay. Moreover, the proposed scheme would enable 802.21 service authorization and allow for SAs to be established between the MN and IS for securely provisioning MIIS. It will be shown through analysis of the signalling process that the overall handover latency for mobility protocols will be reduced by the proposed scheme.

## 6.2 Problem Statement

The issues associated with fast re-authentication are:

### 6.2.1 Further optimization required for existing solutions

There are many solutions that have been defined by the IETF to provide re-authentication solutions based on EAP. As mentioned earlier, the solutions either provide method specific or method independent re-authentication mechanisms. For instance [46] and [64] provide examples of method specific re-authentication mechanisms which are not suitable for NGNs. This is due to the fact that NGNs will comprise of heterogeneous access networks and will require re-authentication support for any (not just a few) EAP method. On the other hand, the IETF has proposed a few method independent EAP re-authentication mechanisms such as those presented in [60], [61], and [63]. However, such solutions (i.e. [60], [61], [63]) have issues, such as high signalling (i.e. RTTs) overhead or require major changes to EAP state machines and message flows. Moreover, EAP is originally based on a 2-party trust model between the peer and the authentication server. This imposes certain issues described later in this subsection and also in [65]. As a result, there is great need to clearly specify a 3-party re-authentication infrastructure. Even though the solution proposed in [64] is essentially motivated by the 3-party approach, it is still a rough “straw man”.

### 6.2.2 Need for a 3-party EAP re-authentication model

Existing EAP methods perform authentication using a two-party approach, where only two parties perform the EAP authentication, namely the EAP peer and the EAP server. However, from a key distribution standpoint, three parties are involved and the two-party model proposed for EAP is not valid for a secure key distribution. In the fast re-authentication scenarios, a key must be sent from a server to the EAP authenticator (i.e. target PoA) which the EAP peer (i.e. MN) has recently attached to (or will attach to) in order to establish a SA between the EAP peer and the EAP authenticator through a *security association protocol*. In other words, the authenticator is another party involved in the key distribution process since it receives a key from a trusted server.

The issues with using a two-party trust model have been noted in [65] and are generally referred to as a problem with "Channel Binding" [65]. Basically the MN infers the identity of the authenticator but it has no clear indication about the identity of the authenticator to which the

keying material was provided by the authentication server [65]. In other words, in event of the undesirable situation occurring where a NAS is impersonating another NAS, the peer and the authentication server will not have the same view of the NAS identity [65].

As a result a 3-party model seems the right approach for key distribution in mobile scenarios to provide channel binding procedures in order to avoid a situation where the trust with an intermediate authenticator is compromised and but it still continues to provide unverified and conflicting service information to both the EAP server and peers [119].

### 6.2.3 Need for IEEE802.21 MIH services to assist re-authentication

As mentioned earlier, recently, the IEEE802.21 WG established a TG (802.21a) to investigate ways to use the IEEE802.21 MIH services, namely the MIIS, to optimize authentication/re-authentication and key establishment mechanisms during handovers. Additionally, 802.21a will define solutions for securely exchanging MIH protocol messages by providing data integrity, replay protection, confidentiality and data origin authentication for IEEE 802.21 MIH services.

The 802.21a TG has liaised with IETF HOKEY WG to define solutions that utilize the MIIS to discover candidate PoAs with which the MN intends to start the fast re-authentication process with. Discovering only the candidate PoAs that offer the re-authentication capabilities will reduce the overall signalling overheads; i.e. target PoAs that do not support re-authentication will not be considered and contacted for handovers. However, at the moment there is a lack of clearly defined mechanisms that specify how the IEEE802.21 MIH Services (i.e. MIIS) could be integrated and deployed in an EAP based infrastructure. Moreover, the IEs that will be provided by the IS to discover the target/candidate PoAs and their capabilities need to be defined.

### 6.2.4 Integration of IEEE802.21 MIH Services with an AAA based Service bootstrapping and Authorization Framework

It was mentioned in chapter 5 that NGNs will be highly service oriented, and as such, a GSABA architecture (EAP/AAA based) to efficiently authorize and bootstrap services has been presented. On the other hand, in chapter 4 it has been shown that IEEE802.21 MIH can be used to drastically reduce the overall handover latency in heterogeneous access networks. Like any promising solution that can contribute significantly to the revenue stream, the IEEE802.21 functionalities will be considered as a "*payable*" service, since they will be used to assist in

optimizing the overall handover process, which includes the authentication procedure. As a result, users need be authorized to be granted access to the 802.21 MIH services. Therefore, it is essential, to integrate the components of the IEEE802.21 MIH entities and services with GSABA, for the purpose of efficient service authorization and bootstrapping.

It was mentioned earlier in section 6.2 of this chapter, that the IEEE802.21 MIH protocol messages must be securely exchanged between end-points. The 802.21 MIHF infrastructure is vulnerable to many security threats. For example, information sent by the IS to the MN can be tampered with in transit by an attacker which could result in malformed unreliable information being received, which could possibly lead to denial of service or the MN being redirected to a wrong network (e.g. where price of accessing the network is more expensive).

A detailed description of all the known security threats to 802.21 MIH services is provided in [72]. To date, there has been no solution defined by the IEEE802.21a TG which allows IEEE802.21 MIH messages to be securely transmitted. However, the integration of IEEE802.21 with the GSABA will allow for dynamic SAs (i.e. keys derived) to be established between the MNs and the IS. It will be shown later in section 6.4.3, how the derived keys can be used to secure the MIIS signalling.

## 6.3 Architectural Overview

An architectural overview of the proposed mechanism is illustrated in Figure 6.1. Before delving into the specifics of the proposed mechanism, it is important to understand the impact of integrating IEEE 802.21 with the GSABA framework. Specifically, for the MIIS provisioning, it is essential to investigate the IS deployment strategies and scenarios.

### 6.3.1 Deploying an Information Server for MIIS Provisioning

The IS is the main logical network entity that provides MIIS as defined in the 802.21 specification. However, the 802.21 formal specification does not provide an explicit definition of the IS nor the mechanism for maintaining and accessing it. As a result, the IEEE 802.21 specification provides flexibility in real IS deployments and implementations, with respect to

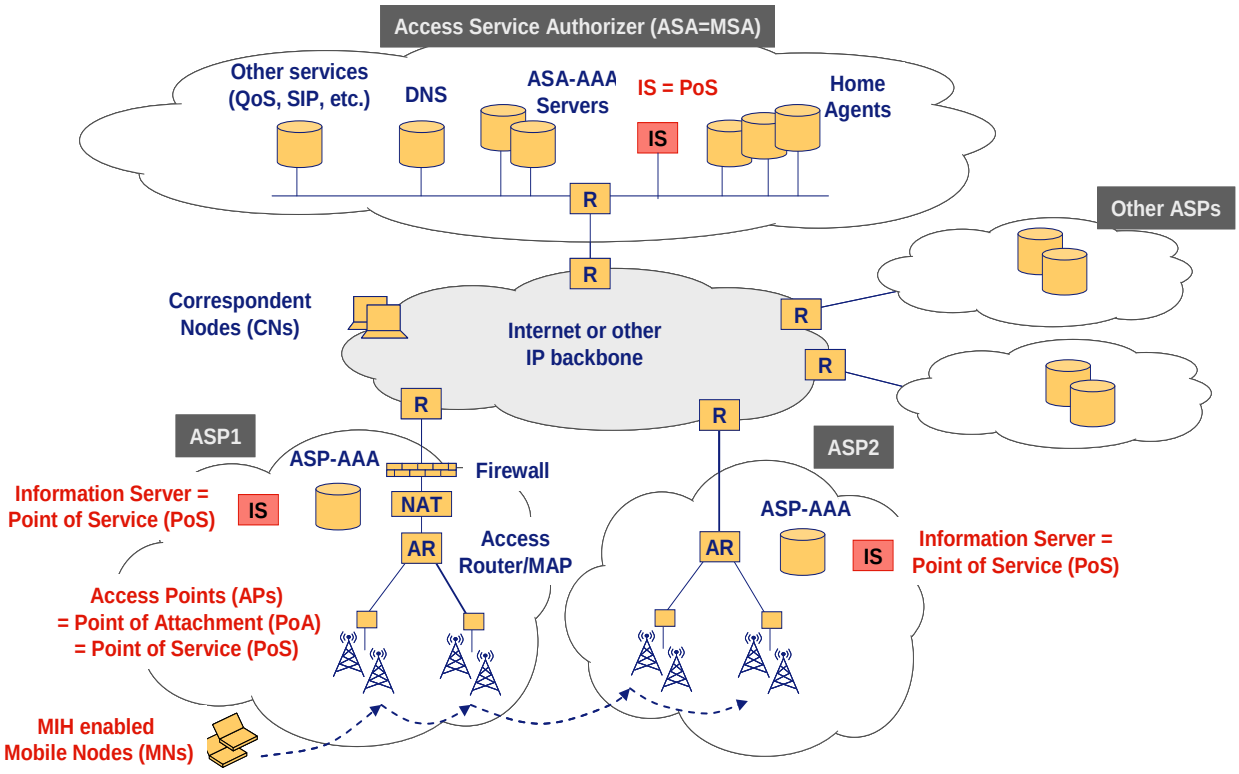


Figure 6.1: Overview of the proposed architecture

how to store, collect and provide the information from the neighbouring access networks. The information at the IS could be stored in the following ways:

- Pre-configured and stored locally in the MN.
- Stored in a distributed fashion across the network by multiple network nodes, which provide the information to the MN.
- The information is stored, and provided by a separate network entity, i.e. the IS.

Although the first option (i.e. pre-configure the information on the MN) is the easiest to implement, it is definitely the least flexible, since the information to be provided will be static in nature and composed of only a small subset of the all required network information for an optimized handover. For example, only fixed IEs such as Network Operators ID, geographic locations of the PoAs etc. could be included, whilst other useful information for handovers such as pricing/billing schemes and network capabilities, which may be dynamic in nature, cannot be included [130].

On the other hand, storing the information in a distributed manner will lead to significant transmission overhead and complicated discovery and maintenance mechanisms. Also, information synchronization will become an issue. It is therefore preferable to store all the desired information in a centralized manner (i.e. IS) or hierarchically by connecting individual ISs.

### 6.3.2 Relationships between Business Entities and the IS

Since the IS will be a new network entity that will be introduced into the NGN architectural models (e.g. GSABA), it is only natural to ask: who is going to deploy this entity and how it is going to fit in with existing business models for NGNs (see chapter 2, section 2.2). The relationship that the IS will form with business entities such as the ASA, ASP, MSA and MSP needs to be analyzed. As explained earlier, the IS will be the entity storing the information of neighbouring access networks within a geographic area inside a local domain (i.e. an operator's domain). It is thus reasonable to consider the IS as a part of the ASP network rather than the mobility infrastructure even though theoretically a third party MSP could also deploy ISs. Considering the sensitive nature of the information (e.g. billing/pricing, PoA capabilities, etc.) that could be involved, it is highly unlikely that the ASPs or MSPs belonging to different administrative domains (i.e. different operators) would wish to share much information (even if roaming agreements are in place).

Therefore, in answer to the question raised at the beginning of this sub-section: It is ideal for the IS to be deployed by the ASP [130]. The deployment of the IS and, furthermore, the maintenance of all the 802.21 MIH services will be the responsibility of the ASPs of an administrative domain. Even though, the introduction of 802.21 MIH services will bring new business opportunities, it doesn’t necessarily require any change to the established business relationships between the ASP, ASP, MSP, and MSA as shown in Figure 6.1.

### 6.3.3 Considered Network Scenarios

There are two possible network scenarios which arise from integrating IEEE 802.21 to assist in optimizing handover (i.e. re-authentication in this case):

- **S1:** (Intra-domain, intra-technology) handover between the same type of access network provided by ASPs and authorized by the same administrative domain.

• **S2:** (Intra-domain, inter-technology) handover between different types of access networks provided by ASPs and authorized by the same ASA-AAA (i.e. same administrative domains).

Of these two scenarios, S2 is a realistic option since re-authentication in NGNs will comprise of inter-technology handovers. Technology specific solutions for handovers and re-authentication (as in S1) already exist, such as those presented [66] and [67]. An emphasis is placed on the scenario S2 in using ISs for handling inter-technology (vertical) handovers, particularly, when a MN is roaming in a visitor/foreign network within the domain. It must be noted that inter-domain (i.e. between different operators) handover scenarios are not considered because, as explained earlier, the IS is part of the local access network (ASP). It will be unlikely that the ISs deployed in the home domain of a particular operator can provide any useful information to a MN about the access networks in a visited domain, belonging to a different operator. In that situation, the MN should try to access the local ISs provided by the ASP in the visited domain. Figure 6.1 provides a reference architecture (IEEE802.21 integrated with GSABA) where there are ISs in the ASPs and another IS in the ASA network.

### 6.3.4 IS Deployment strategy

In this section, an IS deployment scheme is investigated and analyzed. In the scheme shown in Figure 6.2, the IS is deployed outside the MN's subnet, serving several subnets. It is possible to deploy only one IS within a single domain that will serve all the access networks, or a hierarchy/chain of ISs could be deployed to provide information to different blocks (home/visiting) of the administrative domain. The latter approach has the advantage of tackling redundancy issues (in case one of the IS fails, other ISs could still provide information). The MN will discover the IS through DHCPv6 as mentioned in [13] and access it directly through a L3 transport protocol. In must be noted that other deployment schemes can be derived, such as:

i) An IS is deployed in each subnet and co-located with the AR/NAS.
ii) IS or IS-Proxies are deployed in each subnet (co-located with the AR/NAS) and connected in a hierarchical manner.

However, such schemes suffer from scalability problems. To deploy and maintain an IS or an IS-proxy at each subnet in an access network requires a significant amount of work and effort by the ASPs since the AR needs to be heavily modified. Operators are likely to favour a solution that

involves minimal changes to the network infrastructure to support 802.21 MIH (MIIS in this case) services. The deployment scheme presented in Figure 6.2 is potentially the most appealing one to deploy because of its simplicity. Only one new network element will be introduced to the existing network [130]. Also only a single interface needs to be introduced to the MN at the IP layer. There is no need to modify each subnet in the access network [130].

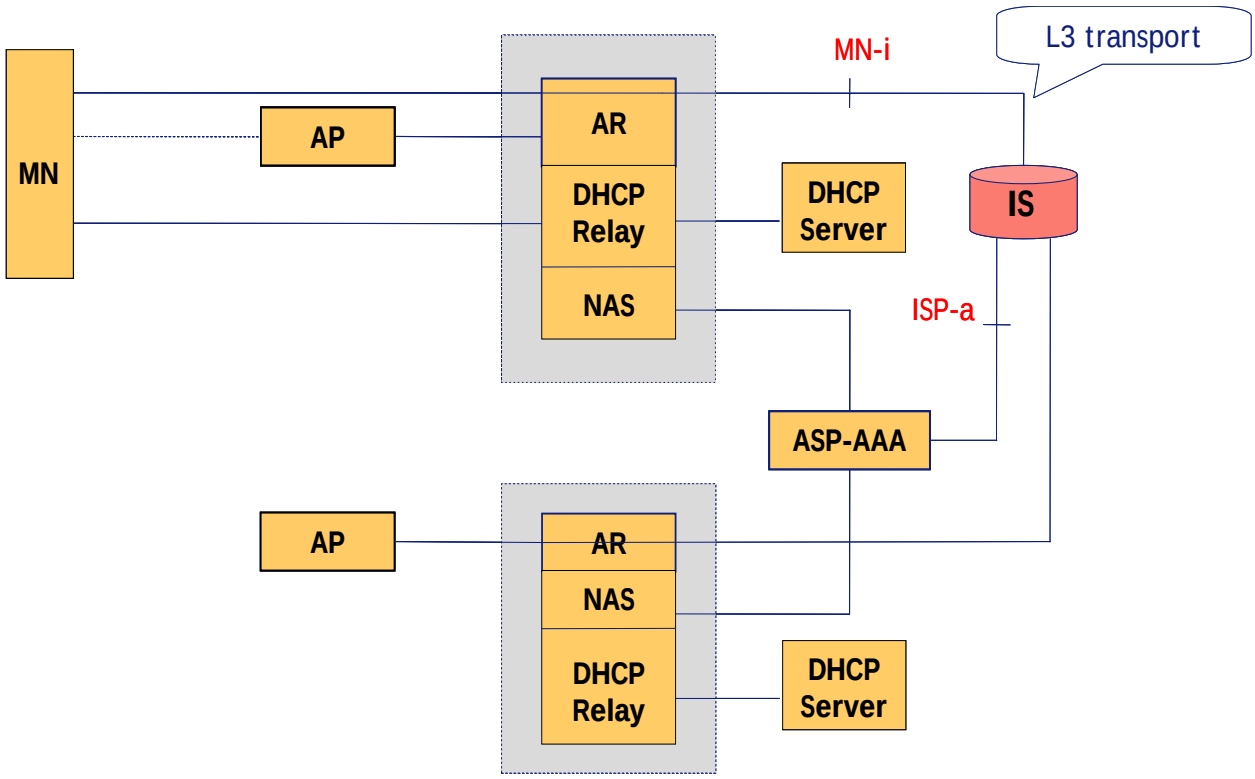


Figure 6.2: IS deployment in the ASP

## 6.4 An Overview of the IEEE802.21 assisted EAP based Re-Authentication Mechanism over GSABA

As mentioned earlier, authentication in wireless networks (e.g. 802.11a/b/g, 802.16e etc.) is usually based on EAP; this could be a problem when the MN moves to a new PoA (i.e. authenticator), since it runs a full EAP method, regardless of the fact that the MN may have been recently authenticated by the domain and have unexpired keying material. The process of a full EAP authentication requires several roundtrips between the EAP client (MN) and the EAP server and takes significant time to complete (even in the minimal case where four EAP messages are

needed). The delay depends on the distance between the EAP server and the MN. As a result, it can take a significant time to perform re-authentication increasing the overall handover latency.

In the subsequent sections, an EAP re-authentication mechanism is defined which is integrated with the IEEE802.21 infrastructure over GSABA to reduce the handover latency due to re-authentication.

### 6.4.1 The 3-party approach

The HOKEY WG is working to specify a solution to reduce the latency introduced by EAP authentication during handover. The issues that have been described in section 6.2 present some drawbacks which triggered the investigation of a new solution based on the extension to EAP Re-Authentication Protocol (ERP) [68] defined by the IETF HOKEY WG. The ERP provides a fast re-authentication process between the MN and the server in a single roundtrip at the cost of modifications to existing EAP deployments. The basic idea consists of securely distributing specific keys between the MN and the PoA from a trusted server without incurring the delays associated with lengthy full EAP authentications. The distributed keying material will eventually serve for the establishment of SAs between the MN and the PoA.

However, the ERP follows the traditional EAP two-party model for key distribution. As explained in section 6.2 of this chapter, this solution has inherited the EAP model for key distribution, that is, a two-party model which is inefficient and open to wider problems such as those related to the key distribution between the three parties involved in mobile handover.

Taking this into account, a 3-Party approach solution described in [123] is extended to utilize the IEEE 802.21 MIH services (namely MIIS) over GSABA. The goal is to provide fast handover and smooth transition by reducing the impact (i.e. minimizing the number of roundtrips) of the EAP based re-authentication process when the MN changes authenticator. At the same time, the key distribution mechanism of the presented solution provides proper channel binding of the key to the parties that will use it. Taking into account the problem of handover keying, the proposed solution must meet the requirements listed below:

- Confidentiality - disclosure of the keying materials to passive and active attackers must not be possible. [65]
- Integrity protection – alteration of a network access credential must be detected.

- Validation of credential source – Once network access credentials are received, the recipients must validate the source of the credentials .[120]
- Verification of identity - The three parties involved must confirm the identities of each other. [65][120]
- Agreement by all parties – All three parties must agree on the disclosed keying material and the identity of the entities to which the keying material will be disclosed to [120].
- Peer consent –Without the clear consent of the client the credentials must not be distributed [120].
- Replay protection - The key distribution protocol must not be affected by replay attacks [120].
- Transport independent - The 3-party protocol must be independent of the transport protocol used for carrying the 3-party protocol messages.

#### 6.4.1.1 Keying Hierarchy to be used

The proposed mechanism of the 3-party model for re-authentication over GSABA utilizes the EAP keying hierarchy described in [47] and [69]. On completion of the EAP authentication method, the EAP server produces the EAP EMSK as defined by the executed EAP method. From the EMSK, a Usage Specific Root Key (USRK) and further keys may then be derived for various purposes, including, handover keys, encryption, integrity protection, entity authentication/re-authentication. The keys to establish SAs between the MN and IS to secure the MIIS signalling will be derived from the USRK key. As mentioned earlier in chapter 4, the USRK key is referred as the GSABA key. The GSABA key could also be called the Root Master Key (RMK). Specification of the generation of USRKs is in progress [69] but it is expected that since the EAP layer does not export the EMSK, the GSABA Proxy server needs to request derivation of the GSABA Key (i.e. the RMK) from the EAP server after authorization has been provided. The EMSK root key hierarchy used to derive keys for efficient EAP re-authentication and IS SA establishment is shown in [69].

### 6.4.2 Detailed Explanation of the Proposed Mechanism

To start with, there is an assumption that there exists a SA between the MN and GSABA server. The GSABA Proxy and GSABA Server have another SA. Also, another assumption is that the

EAP peer (i.e. the MN) has already completed a successful full EAP authentication with the EAP (i.e. GSABA Server) server through the currently attached EAP authenticator (i.e. the PoA). This allows the MN and the GSABA server to share a fresh EMSK. From the EMSK, a key hierarchy is derived for supporting the proposed 3-party re-authentication mechanism. This step is only performed once while the EMSK lifetime is still valid.

When the MN senses (e.g. through L2 triggers) that it is losing connectivity with the currently attached PoA as a result of signal degradation, it immediately sends a MIH message that carries the '*MIH_Get_ Information*' request TLV as its payload to the IS. The IS can be discovered by using DHCP (please refer to chapter 4, section 4.4.3 for more details). The purpose of sending the *MIH_Get_ Information*' request message is to discover neighbouring candidate PoAs/authenticators that support the proposed EAP re-authentication mechanism. Such security related information is crucial to make a handover decision and to prepare a fast handover using fast authentication options (e.g. pre-authentication, re-authentication, etc) supported by the network which the candidate PoA is associated with.

As explained earlier, there is a substantial delay due to re-transmissions of EAP-Initiate/Re-auth messages before the MN realizes that a particular candidate PoA does not support EAP re-authentication. As a result, there will be significant signalling overhead and resource wastage if there are many candidate PoAs that need to be contacted before the actual handover. Moreover, using the information provided by the IS (e.g. the HNI container described in chapter 4), the L2 scanning phase will be eliminated. This will drastically reduce the overall handover delay, as shown by analysis and simulation in chapter 4.

On receiving the '*MIH_Get_ Information*' request, the IS responds with a '*MIH_Get_ Information*' reply message which contains the requested information as an Information Element (IE) container. A container named '*SEC_CONTAINER*' has been defined for this purpose. The '*SEC_CONTAINER*' will include information about the PoA MAC address, the PoA IPv4/6 address, the supported EAP methods, and EAP re-authentication support etc.

The contents of the '*SEC_CONTAINER*' are presented in Figure 6.3.

| Type = TYPE_IE_HNI_REPORT | Length = Variable |
|---|---|
| *SEC_CONTAINER #1* | |
| Open Authentication Support IE | |
| Password Support IE | |
| Certificate Authority IE | |
| Authentication Protocol Type IE | |
| Supported EAP Methods IE | |
| Re-authentication Support IE | |
| Pre-authentication Support IE | |
| Roaming Partners IE | |
| PoA MAC address | |
| PoA IPv4/6 address | |
| SEC_CONTAINER #2 | |
| ... ... ... | |

Figure 6.3: SEC_CONTAINER

However, it must be noted that prior to the '*MIH_Get_ Information*' request/reply message exchange, the IS and the MN must establish SAs to secure the MIIS signalling. In the following subsection, the SA establishment with the IS is explained.

### 6.4.2.1 SA Establishment between the MN and the IS

After the MN has been successfully authenticated for initial network access, the GSABA Server delivers the GSABA key to the GSABA proxy. Details of *when* and *how* the GSABA key is delivered to the GSABA Proxy are provided in chapter 5 (see section 5.5.3). Since the

IEEE802.21 functionalities will be considered as *premium* services, which would enable optimized handovers across heterogeneous networks, it is essential to authorize and bootstrap the offered 802.21 MIH services. As a result, the MN sends an ABIRES message to the GSABA Proxy. Like the solution provided in chapter 5 (refer to section 5.5), it also assumed here that the MN profile (i.e. statement that gives the authorization for services for the MN) is delivered in advance to the GSABA Proxy during the initial EAP full-authentication phase. This is an enhanced case, since the GSABA Proxy will be free to generate authorization decisions locally instead of having to contact the home AAA server (i.e. GSABA server) every time a service is requested.

The MN secures the ABIREQ message with the BCA key which is derived from the GSABA Key. The minimum set of parameters in the ABIREQ message is the BCID, SRID (i.e. the ID of the IEEE802.21 service in this case), and the corresponding identifier intended to be used on the SP interface. In response, the GSABA Proxy sends an ABIRES message containing the needed parameters. All the parameters and message flows for the ABIREQ /ABIRES messages are provided in chapter 5 (see section 5.5.3). The BCA key protects the ABIREQ/ABIRES message by providing data confidentiality and integrity.

Immediately after the initial network authentication and service authorization, the MN will use the HOKEY protocol (please refer to chapter 5, section 5.5.4.1) to create SAs (i.e. keys) to protect the MIIS signalling between the MN and the MIIS. The HOKEY protocol assumes that the MN shares a key, called the Information Master Key (IMK), with the GSABA Server. The IMK can be thought of as a GSABA key or a USRK which is derived from the EMSK.

A Message Integrity Key (MIK) is derived from IMK at the MN and the GSABA proxy. The MIK is used to provide data integrity for messages exchanged between the MN and the GSABA Proxy and can be referred as the BCA Key. The Information Key (IK), which is used to protect the signalling exchange between the MN and IS is also derived from the IMK as shown in Figure 6.4.

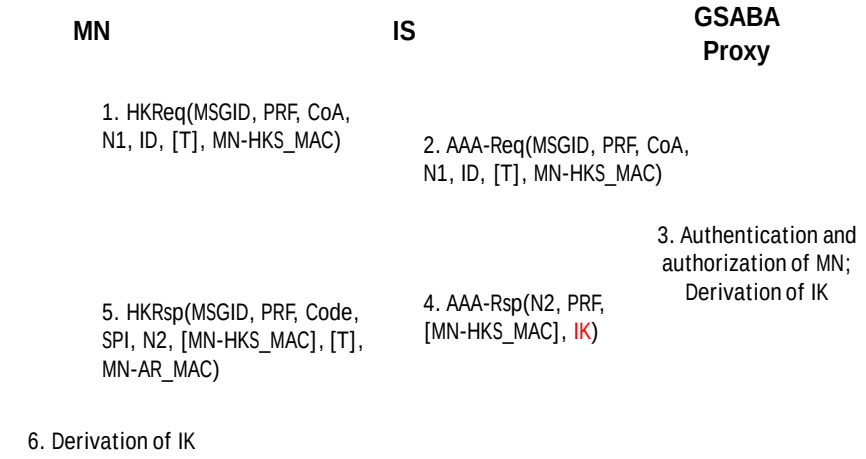


Figure 6.4: SA Establishment between the MN and IS

Prior to sending the '*MIH_Get_ Information*' request, the MN sends an HKReq message to the IS in order to start the HOKEY process. The integrity of the HKReq message is protected by the use of a MIK. The IS forwards the content of the HKReq message via an SIREQ message to the GSABA Proxy, as only the GSABA Proxy can verify the message and generate a new IK. The GSABA Proxy Server authenticates the MN and checks whether the MN is authorized for IEEE802.21 MIH Services (namely MIIS). If so, the GSABA Proxy derives the IK. The process of deriving the IK is shown in chapter 5, section 5.5.4.1. The GSABA Proxy delivers the Information Key (IK) and the AAA nonce N2 as well as the IK lifetime and the chosen PRF. Thereby; it is assumed that the IS and the HKS share a security association protecting the AAA messages. On receiving the SIRES, the IS sends an HKResp message to the MN, containing, beside other parameters, N2 and MN-AR_MAC, which is protected using theIK. Using the contents of the HKResp, the MN is able to derive the IK. As a result, a SA is established between the MN and the IS, which enables MIIS signalling (i.e. '*MIH_Get_ Information*' request/reply) to be protected.

### 6.4.2.2 Details of the proposed Re-authentication process during Handover

The re-authentication during the handover phase is presented in Figure 6.5. As mentioned earlier, this chapter presents an EAP Re-authentication based on a 3-party approach over GSABA as described in [123].Using an EAP based model is the ideal option due to the fact that many devices implement EAP. Extension of the EAP messages *EAP Response Id* and *EAP Success* is required. However such extensions have minimal impact on the *EAP state machine,* compared to others solutions such as [68].

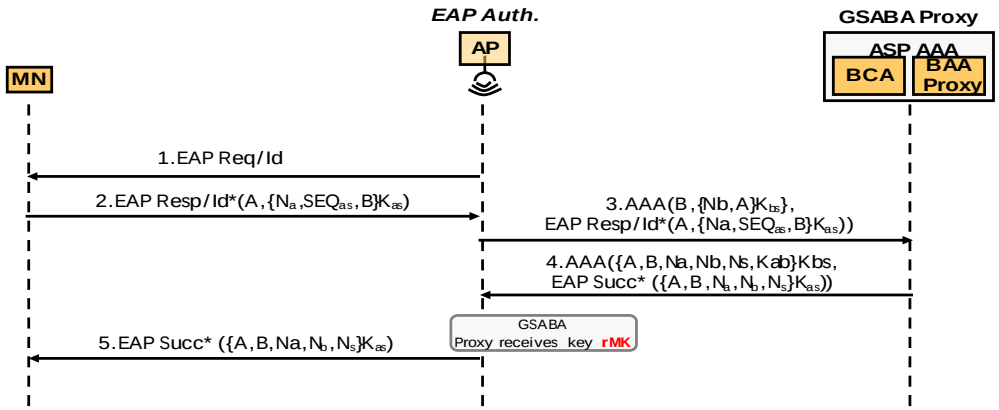


Figure 6.5: Message flow for the proposed 3-party Re-authentication process

In this phase the goal is to achieve the installation of a key in the new authenticator. It must be noted that if the MN needs to be authorized by the ASP as part of the proposed re-authentication process, then there needs to be an ABIREQ/ABIRES message exchange between the MN and the GSABA Proxy. The process of obtaining such authorization from the GSABA is identical to the process described in section 6.4.2.1 of this chapter.

The message flow depicted in Figure 6.5 shows the movement of the MN when it wants to attach to another authenticator. The new authenticator sends an EAP Request Identity message in order

to authenticate the MN (step 1) [68]. The EAP Request Identity message is integrity protected using the rIK [68]. The rIK is derived from the GSABA key. As has been explained earlier, the GSABA Key is derived from either the EMSK or a DSRK. For the purpose of GSABA key derivation, this thesis specifies the derivation of a USRK or a Domain-Specific USRK (DSUSRK) in accordance with [47] for re-authentication. The USRK designated for re-authentication is the re-authentication root key (the GSABA Key). Next, the MN responds with an EAP Response Identity message and this message is modified to allow the insertion of the additional information needed to perform the proposed 3-Party Protocol (step 2).

The proposed model provides a protected facility to carry channel binding (CB) information to tackle the issues describe in section 6.2 and in [65]. The TLV type range of 128-191 is reserved to carry CB information in the EAP-Response Id [65] [68]. Examples of CB information such as Called-Station-Id will be included in the EAP-Response Id message sent to the authenticator, as shown in Figure 6.5.

The EAP Response Identity message sent by the MN to the authenticator is forwarded by the authenticator to the GSABA Proxy, where the authenticator adds additional information (i.e. a NAS-Identifier as CB information) in the AAA message in order to be authenticated by the GSABA Proxy (step 3). At this point, both parties are authenticated by the GSABA Proxy and the key that it is going to be installed in the authenticator is derived by the GSABA Proxy. This key is known as the rMK and is derived from the GSABA key. A message which is a modified EAP Success message and the rMK is sent to the authenticator (step 4). The authenticator installs the key sent by the GSABA Proxy. With this key the authenticator and the MN establish a SA. Then, the authenticator sends a modified EAP Success message to transport the necessary information to derive the same key that was installed in the authenticator (step 5). Finally to finish, the MN receives the modified EAP Success message. The MN is now authenticated by the network and derives the same rMk that was derived by the authenticator in order to establish a SA for the re-authentication mechanism.

## 6.5 Performance Evaluation

In this section, the overall latency due to the security signalling of the proposed EAP based re-authentication scheme is analyzed, and compared to the un-optimized (i.e. full) EAP re-authentication mechanism. The performance of the two schemes is evaluated using the

authentication signalling and the EAP method latency metrics. The authentication signalling latency $D_{SA}$ is defined as the time elapsed between the sending of the first authentication message (i.e. L2 SA such as the 4-way handshake in 802.11) until the Acknowledgment of the last authentication message is received by the MN. On the other hand, the EAP method latency, $D_{EAP}$, is defined as the time elapsed between the sending of the first EAP message and the reception of either an EAP SUCCESS or EAP FAILURE message. The notation used to express the parameters and variables of the authentication signalling latency is provided in Table 6.1.

| | |
|---|---|
| $S_{EAP}$ | Total number of signalling messages required for the successful execution of an EAP method. It must be noted that this parameter does not include the EAP Start message |
| $S_{Auth}$ | Total number of messages required for the execution of the authentication signalling of the lower layers (e.g. 4-way handshake in 802.11i). This parameter does not include the EAP message exchanges. |
| $d_{MC}$ | Average propagation delay between the MN and the currently attached PoA. |
| $d_{MT}$ | Average propagation delay between the MN and the target PoA. |
| $d_{ST}$ | Average propagation delay between the EAP Server (i.e. GSABA Proxy) and the target PoA. |
| $C_{FA}$ | Time required for the involved parties to perform all the cryptographic operations, including key derivations, for a full EAP authentication. |
| $C_{RA}$ | Time required for the involved parties to perform all the cryptographic operations, including key derivations, needed by the proposed re-authentication mechanism. |

Table 6.1: Notation used in expressing the security latencies

### 6.5.1 Full Authentication

The latency incurred by a full EAP method authentication exchange is expressed as:

$$D_{EAP} = 2d_{MT} + ( d_{MT} + d_{ST} ). S_{EAP} + d_{ST} + C_{FA} \quad (1)$$

where, $2d_{MT}$ is the delay caused by the initial two EAP messages. It is the delay incurred at the very beginning, when the authenticator sends an EAP-Request message, which contains a Type

field, requesting a MN's Identity. In response to a valid request, the MN sends its identity in a Response message. Here, $(d_{MT} + d_{ST}). S_{EAP}$ is the time taken to complete a full authentication. The delay introduced by the key distribution procedure is represented by $d_{ST}$.

After a successful EAP authentication, media dependent SA protocol exchanges take place. For example, in 802.11 the MN undergoes a 4-way handshake to establish unicast and multicast SAs for protecting the signalling between the MN and the PoA (i.e. the authenticator). The delay introduced by the media dependent SA protocol exchange is shown in (2).

$$D_{SA} = d_{MT} \times S_{Auth} \quad (2)$$

where, $D_{SA}$ is the latency incurred by exchanging media specific authentication messages. The total latency for the overall authentication phase is expressed as:

$$D_{Total} = D_{EAP} + D_{SA} \quad (3)$$

### 6.5.2 Proposed Re-authentication Scheme

The EAP latency for the proposed re-authentication mechanism is expressed in (4) below.

$$D_{Pr\text{-}reauth} = 2d_{MT} + D_{Re\text{-}auth} + C_{RA} \quad (4)$$

where

$$D_{Re\text{-}auth} = 3d_{MT} + 2d_{ST} \quad (5)$$

In (5), the EAP re-authentication method exchange is composed of a total of five messages. Three of the messages, including the EAP Success/Failure message, are between the MN and the target PoA, and two of them are between the target PoA and the EAP Server (i.e., the GSABA Proxy) as shown in Figure 6.5.

Here,

$$C_{RA} < C_{FA}$$

since most of the cryptographic operations will be eliminated and key derivation is much more lightweight and simpler. The overall authentication latency for the proposed scheme is, therefore, expressed as:

$$D_{Total} = D_{Pr\text{-}reauth} + D_{SA} \quad (6)$$

where

$$D_{Pr\text{-}reauth} < D_{EAP}$$

### 6.5.3 System Modelling

With reference to the system model in [70] the GSABA Proxy in the proposed mechanism presented in section 6.4 of this chapter can manage a number of ARs in its management domain. The GSABA Server is in the home domain and other layers containing the GSABA Proxy disperse from it. It is assumed that the distance from a GSABA Server to a GSABA Proxy follows a Poisson distribution with a parameter value of $\mu$. It is also assumed that a MN needs to move its PoA $m$ times until it leaves the domain of the GSABA Proxy, which means that there are $m\text{-}1$ intra-domain authentications and the $m^{th}$ one is the inter-domain (i.e. inter GSABA Proxy) authentication. The probability that a MN moves out of a PoA's coverage area (i.e. intra domain) is:

(7)

Where $N$ is the number cells visited by the MN in a given domain.

The probability of a MN moving out of the GSABA Proxy's domain is provided in [70] and expressed as:

(8)

where and $K$ is the radius of a GSABA Proxy's domain.

Based on (7) and (8), the total authentication cost $C_{total}$ can be derived as:

$$C_{total} = \qquad (9)$$

where $T$ is the total time, and are the cost of inter (i.e. mobility from a GSABA server to a GSABA Proxy) and intra domain (mobility within a GSABA Proxy's domain) authentication respectively.

The total cost of the full EAP based authentication solution $C_{org}$ (i.e. $C_{total}$ for the full authentication) is:

$$C_{org} = \text{———————————} \quad (10)$$

Where,

$$C_{first} = D_{EAP} + D_{SA} \quad (11)$$

$C_{first}$ is the authentication cost incurred when the MN moves to the GSABA's Proxy's domain for the first time. $C_{each}$ is the authentication cost every single time the MN moves to a new authenticator's (i.e. PoA) link. In the case of the un-optimized EAP mechanism (i.e. $C_{org}$), $C_j$ would be equal to $C_{first}$, since the home domain (i.e. GSABA server) will be contacted every time the MN moves to a new GSABA Proxy's domain. In essence, $C_{first}$ is a case of an inter-domain authentication (i.e. $C_j = C_{first}$). In equation (10), $C_{each}$ can be considered as the cost of the intra-domain authentication ($C_i$), since the MN moves within the boundary of a GSABA proxy. However, the total authentication cost for the full EAP authentication, $C_{org}$ in equation (10) can be derived as:-

$$C_{org} =$$

$$\text{——} \quad \text{——} \quad \text{——} \quad \text{———————————} \quad (12)$$

where

$$C_{each} = C_{first} \quad (13)$$

Based on equation (9), the total cost of the proposed scheme, $C_{pr}$ can be derived as:

$$C_{pr} = \text{———————————} \quad (14)$$

where

$$C_{other} = D_{Pr\text{-}reauth} + D_{SA} \quad (15)$$

$C_{other}$ is the cost of the re-authentication mechanism. As mentioned earlier, it can be inferred that :

$$C_{pr} < C_{org}$$

since

$$C_{other} < C_{each}$$

The cost of the proposed re-authentication scheme (i.e. $C_{total}$ ) is expressed as:

$$C_{pr} =$$

(16)

In equation (16), $C_i$ is equal to $C_{other}$ due to the fact that $C_{other}$ is the cost for an intra-domain handover (i.e. $C_i$).

### 6.5.4 Results Analysis

The results presented in this sub-section have been derived using parameters provided in [70] and from the simulation and experimental results presented in chapters 4 and 5. From the analytical results presented in Figures 6.6 and 6.7, it is clear that the proposed IEEE802.21 assisted re-authentication scheme outperforms the original (i.e. full EAP authentication) solution in terms of the reducing the overall handover latency for both FMIPv6 and MIPv6. The results suggest that the overall handover latency can be reduced by roughly 70% by using the proposed mechanism. This is due to the fact that the proposed mechanism reduces the total EAP authentication signalling (i.e. $D_{Pr\text{-}reauth}$) and the required cryptographic operations (i.e. $C_{RA} < C_{FA}$). Also, by using the IEEE802.21 MIIS, the scanning phase of the L2 handover is eliminated which drastically reduces the overall handover latency.

The results of Figures 6.6 and 6.7 support the findings in [70] where the total cost (i.e. handover and authentication latency) increases as the Average Residence Time (AVR) decreases. The AVR is defined as the average time a MN stays within the coverage of a PoA. Even though the results in Figure 6.6 compare the overall handover latency with the EAP authentication delays as opposed to the total cost versus AVR in [70], the results in [70] still support the concepts of the

proposed scheme presented in section 6.4 of this chapter and the results shown in Figure 6.6. For instance, a decrease in the AVR means that the MN stays within an authentication server's domain for a shorter period of time, which will lead to an increase in the rate of handover and authentication signalling. An increase in the total authentication signalling leads to an increase in the authentication cost. Since authentication is a fundamental component of a NGN handover, an increase in the authentication signalling/cost will lead an increase in the handover latency.

The results in Figure 6.6 which take into account the total cost (i.e. Authentication signalling cost) presented in equations (12) and (16) of this chapter are a testament to the fact that an increase in the total cost due to an increase in the authentication signalling will result in an incremental increase in the overall handover latency.

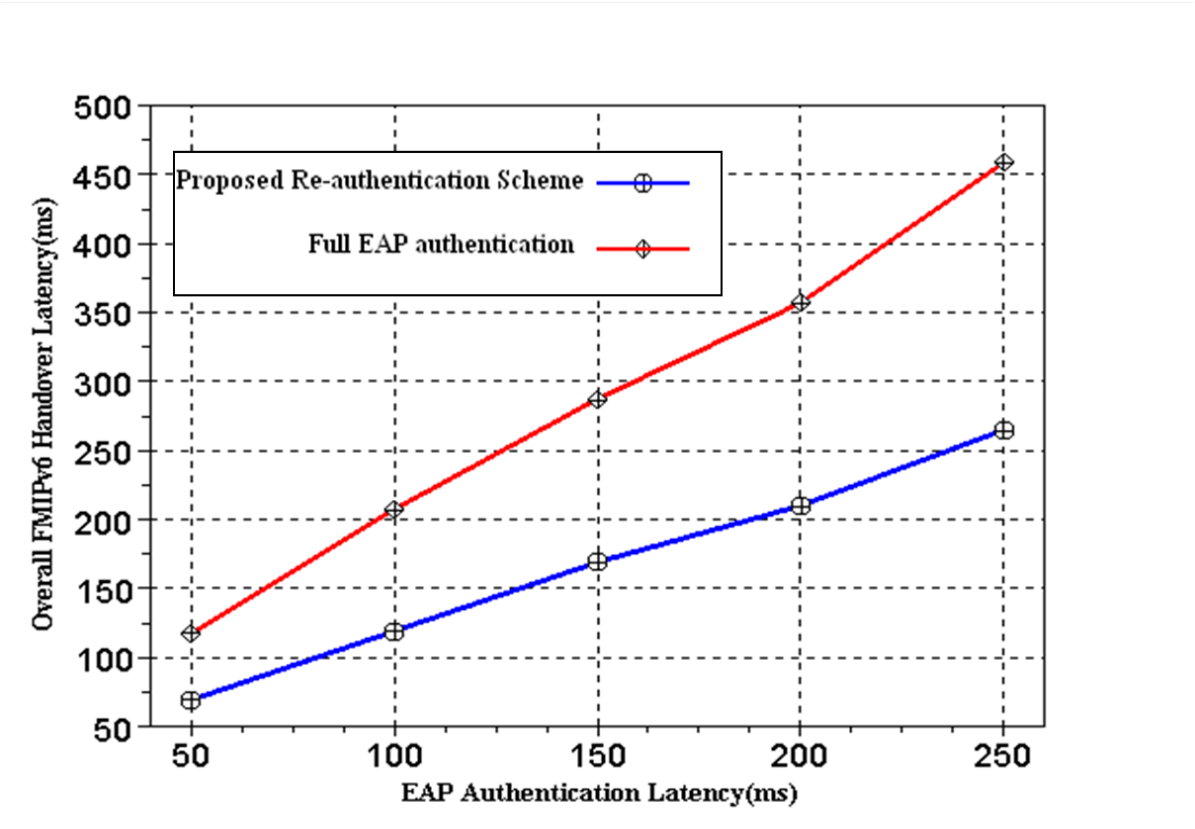


Figure 6.6: Overall Handover Delay for FMIPv6

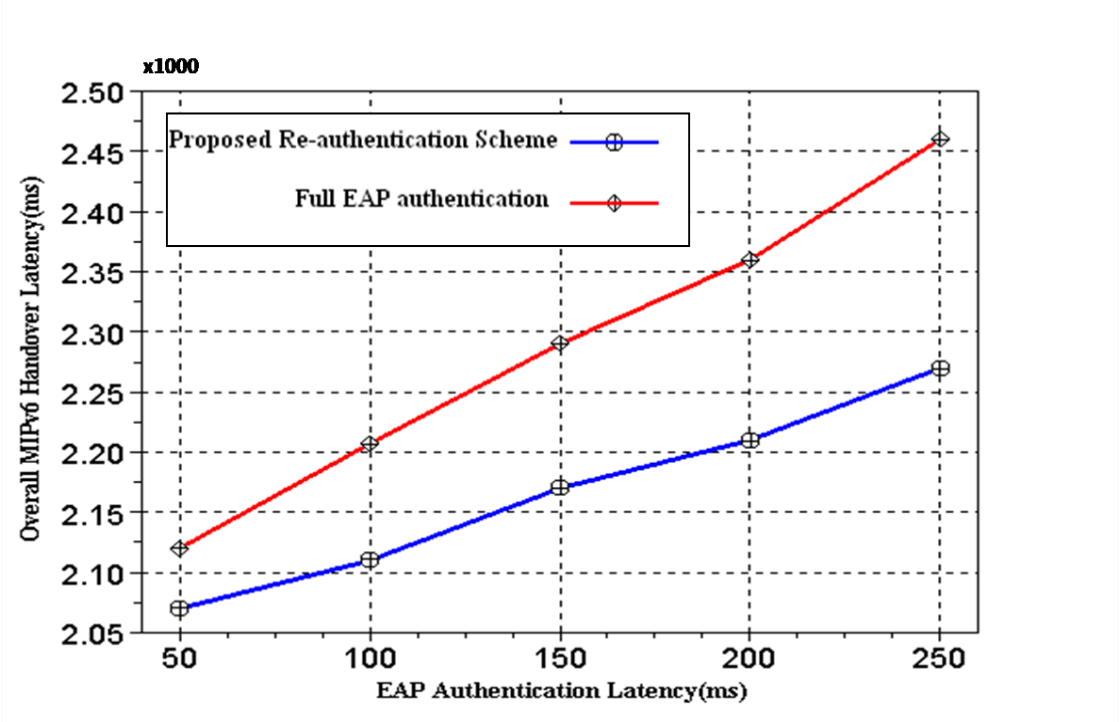


Figure 6.7: Overall Handover Delay for MIPv6

The impact of the distance between the MN and the EAP server (the GSABA Proxy/Server in this case) on the overall handover latency is illustrated in Figure 6.8. In Figure 6.8, the distance is directly proportional to the end-to-end delay between the MN and the GSABA Proxy/Server. Unsurprisingly, the overall handover latency increases with the end-to-end (i.e. distance) delay between the MN and the GSABA server. If the GSABA Proxy is far away from the MN, then the packet transmission cost for the EAP authentication signalling is also increased.

The results in Figure 6.8 support the findings in [70] where an increase in the distance between the MN and the AAA server (i.e. GSABA and GSABA Proxy) would result in an increase in the overall handover latency. The findings hold true to the conventional wisdom for end-to-end latency which depends on many factors such as processing delays at intermediate routers due to queuing, the number of hops between the MN and the EAP server, transmission delays, bottlenecks at public exchanges, etc, as explained in chapter 4 (see section 4.5.6).

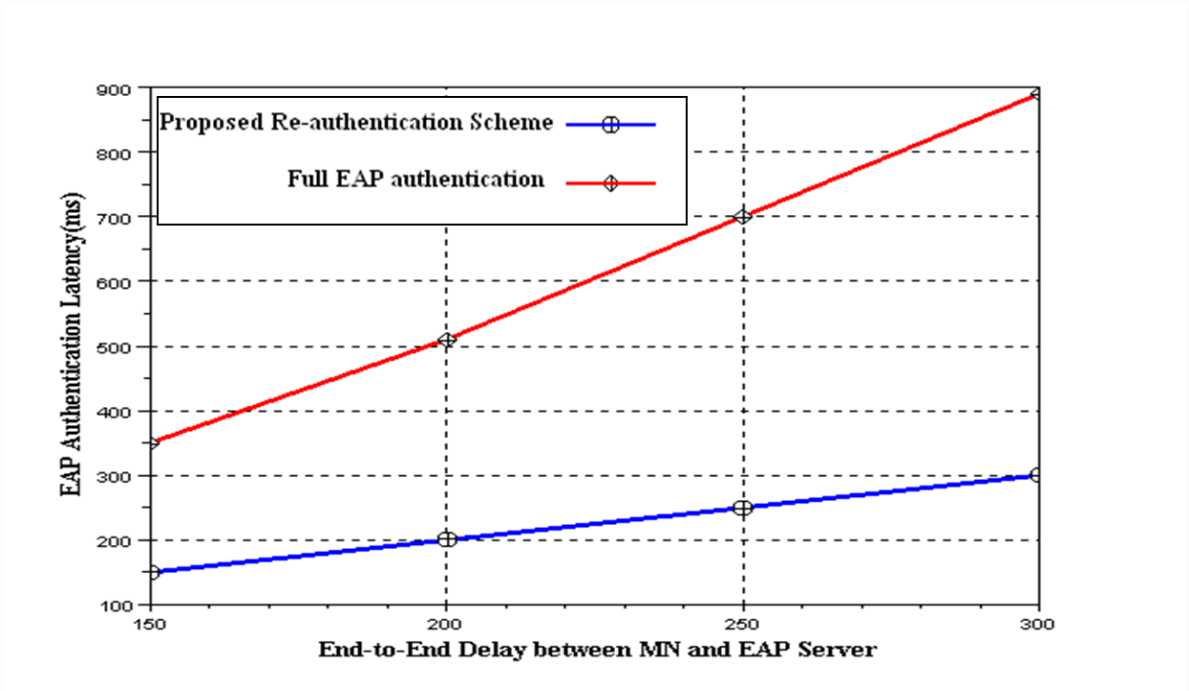


Figure 6.8: Impact on EAP Latency of end-to-end delay

## 6.6 Summary

In this chapter, a mechanism has been proposed which optimizes the EAP re-authentication procedure with the assistance of IEEE802.21 MIH services over a GSABA infrastructure. To do this, the MIIS has been exploited to provide information about discovered target PoAs in neighbouring networks that support the re-authentication mechanism. A new Information Container, the '*SEC_CONTAINER*', has been defined for this purpose. Also, using the MIIS eliminates the need to perform a L2 scanning process which dramatically reduces the overall handover delays. Moreover, the proposed scheme enables 802.21 service authorization and allows for dynamic SAs to be established between the MN and the IS to secure the MIIS signalling. It is shown analytically that when the proposed mechanism is applied, it drastically reduces the overall EAP re-authentication latency, and as a result, also reduces the overall handover latency for both MIPv6 and FMIPv6.

# CHAPTER 7 – CONCLUSIONS AND FUTURE WORK

## 7.1 Conclusions

The research conducted throughout this thesis provides mechanisms to facilitate optimized and intelligent handovers across converged IP-based heterogeneous access networks. The results gained from the experimental evaluations and analysis will provide valuable insight to the relevant research and standards community at a time when mobility management for NGNSs using cross-layer techniques is an extremely “hot” topic of discussion. Already, mobile phone manufactures (e.g. Apple Inc's iPhone, Nokia, Huawei) [102], chip makers (e.g. Intel) [103] and telecoms operators, such as BT are investing huge amounts of finance geared towards research efforts for the commercial product developments of IEEE802.21 MIH Services.

### 7.1.1 Summary of the Thesis

In this sub-section, a summary of the research work undertaken and accomplished by this thesis is presented. Also, a subsection is devoted to a discussion of future work.

In chapter 1, the thesis starts with a brief overview of IP based Next-Generation Networks (i.e. 4G) and then discusses the current research issues in the area of the mobility management across NGNs. The overall contribution that the thesis has made towards the relevant research community is also discussed.

Chapter 2 provides *background information* relevant to the thesis, such as supported services in NGNS, business models, mobility scenarios, types of handovers, mobility protocols (e.g. MIPv6, NEMO, and FMIPv6), IEEE802.21 MIH Infrastructure, Service Authorization and Bootstrapping, etc. The chapter discusses *the motivation* (in terms of the tackling the current issues of mobility management across heterogeneous access networks) for pursuing the chosen area of research.

In chapter 3, a comprehensive survey of the related research work in the area of mobility management across heterogeneous IP based networks is provided. The survey details the issues with existing mobility management solutions across NGNs and highlights (i.e. justifies) the need for the extensive research this thesis has undertaken.

In chapter 4, FMIPv6 integrated with IEEE802.21 Media Independent Handover (MIH) services is used to optimize the handover procedure of the FMIPv6 protocol in vehicular

environments. With the aid of the lower three layers' information of the MN/MR, the neighbouring access networks, the radio access discovery, and candidate AR discovery issues of FMIPv6 are tackled. Through detailed analysis, it is shown that the anticipation time in FMIPv6 is reduced, thus increasing the probability of the predictive mode of operation. A cross-layer mechanism is proposed for making intelligent handover decisions (i.e. appropriate network selection) by using a Policy Engine (PE). It is shown through analysis and simulations of the signalling process that the overall expected handover latency in FMIPv6 is reduced drastically by the proposed mechanism by the eliminating the L2 scanning phase. Also, the signalling overhead and packet loss for the proposed mechanism is improved by 50% and 79% respectively.

In chapter 5, a novel FMIPv6 authorization and bootstrapping architecture is presented in order to provide the MN with necessary configuration parameters and distributed keying materials to secure FMIPv6 messages in terms of authentication and authorization. In this respect, a practical Linux operating system based FMIPv6 authorization and bootstrapping test-bed has been implemented to provide experimental analysis. The experiments presented the handover performance of the secured FMIPv6 over the GSABA architecture compared to plain FMIPv6 and MIPv6 by providing quantitative measurements and results on the quality of experience perceived by the users of IPv6 multimedia applications. The results showed the inclusion of the additional signalling of GSABA architecture, for the purpose of authorization and bootstrapping (i.e. key distribution using HOKEY), has no adverse effect on the overall handover process. In fact, the handover for the proposed mechanism is the same as that of plain FMIPv6 handover. As expected, the plain MIPv6 takes drastically longer compared to the proposed secured FMIPv6 over GSABA. Also, a security analysis of the secured FMIPv6 along with the newly defined protocol/interfaces of the GSABA architecture has been done, using a formal (i.e. AVISPA) analysis tool. The results suggest that the proposed mechanism is secure (i.e. safe) from the imposed security threats.

In chapter 6, a novel IEEE802.21 assisted EAP based Re-Authentication scheme over a service authorization and bootstrapping framework (i.e. GSABA) is presented. Moreover, the proposed scheme enables 802.21 service authorization and SAs to be established between the MN and IS for securely provisioning MIIS. It is shown through mathematical analysis of the signalling process that the overall handover latency for mobility protocols will be reduced significantly by the proposed scheme.

In conclusion, the thesis shows that the transparent migration of data flows between two PoAs belonging to independent heterogeneous technologies using cross-layer techniques (i.e.IEEE802.21 MIH Services) is achievable. This is justified as follows:

The thesis defines mechanisms for the integration IEEE802.21 with a mobility protocol (namely FMIPv6) that enables vertical handovers between the disparate access technologies. This convergence poses challenging research issues such as the two topics that this thesis tackled: (a) how to minimize mobility disruptions (i.e. handover latency) when roaming and (b) how to provide efficient mobility service authorization and bootstrapping. To address the former, FMIPv6 has been integrated with IEEE802.21 to make intelligent handover decisions to reduce the overall handover latency (both L2 and L3). Moreover, the thesis shows that reducing the mobility protocol latencies is not enough to optimize the overall handover process. Therefore, a fast re-authentication scheme has been defined to reduce the EAP authentication latency in order to optimize the overall handover process across heterogeneous access networks. To address the latter, a GNU Linux based test-bed has been developed to provide generic service authorization and bootstrapping solutions. As shown from the results in the earlier chapters (4, 5 and 6), the performance of the proposed mechanisms that this thesis contributes to, are very promising. Therefore, using the solutions that have been presented and evaluated in this thesis, it is practical to deploy a suitable architecture that supports seamless mobility in forthcoming 4G systems.

Some overall observations can be derived from the outcome of the research this thesis has undertaken:

i) Through thorough theoretical analysis, simulation, and deployment of practical test-beds, this thesis proves and reinforces the fact that mobility protocols such as MIPv6, FMIPv6, alone are not capable of efficiently handling mobility across heterogeneous access networks. The overall handover procedure across integrated IP-based access networks is a very complicated process, which occurs almost at every layer of the protocol stack. Therefore, in order to perform an intelligent and optimized handover, it is essential to exchange and utilize cross-layer information between different layers of the protocol stack.

ii) In order to clearly define a sophisticated, yet practical solution, i.e., in terms of the deployment of large heterogeneous IP based converged networks this thesis has successfully

proposed an optimized handover mechanism (namely for FMIPv6) using cross-layers techniques with the assistance of the IEEE802.21 MIH services. The proposed solution (see chapter 4) has been applied in simulated vehicular environments in order to optimize the NEMO handover process. The proposed solution successfully tackles the issues related with vertical handovers in NGNs, such as network discovery, PoA/PoS discovery, Network Selection, seamless (i.e. with no service disruption) mobility. In particular, the MIIS plays a vital role in optimizing the Network/PoA discovery and selection to drastically reduce the overall handover. On the other hand, if cross-layers mechanisms (e.g. IEEE802.21) are not used then network discovery and selection becomes a real issue which causes undesirable service disruptions. Such behaviour is shown in chapter 5, where the L2 scanning phase is reported as taking between 1-3.5 seconds to complete, and as a result causes long handover delays. The findings provide extremely useful insight into the actual issues in real-world deployments and how they can be mitigated and solved.

iii) This thesis takes into consideration the business architecture/components of NGNs and presents a generic service authorization and bootstrapping architecture (see chapter 5). The thesis shows that a highly scalable and efficient service authorization and bootstrapping (in particular for mobility services) framework can be developed using existing technologies and infrastructure, such as AAA using EAP and Radius. As a proof of concept, a GSABA framework has been developed and deployed for mobility services (i.e.FMIPv6). The HOKEY protocol, which is a topic of great interest in the research community, along with the other protocols/interfaces have been developed and deployed. Such a test-bed is believed to be "*first of its kind*" and through its novelty will significantly contribute to the relevant research and standards organization.

iv) This thesis provides the novel concept of considering IEEE802.21 MIH as a profitable service and shows how to authorize and bootstrap the IEEE802.21 MIH supported services. As a result, a mechanism to securely exchange MIH service messages has also been defined. To the best of knowledge such work has not been done before and will contribute effectively to the relevant research communities, such as the IETF and the IEEE802.21 WG. Also, this thesis draws attention to a much neglected, but a very important issue; i.e., re-authentication delays during handovers in NGNs. In this respect, a novel optimized fast re-authentication scheme utilizing IEEE802.21 has been presented to reduce the overall handover delay. Such work paves way for an area of much needed research and can contribute to existing research groups, such as the IEEE802.21a WG (the security new task group within IEEE802.21).

## 7.2 Future Work

This thesis has raised various issues that have yet to be addressed. Several of the most interesting problems are discussed below, as well as potential avenues for further research are discussed.

- The proposed mechanism presented in chapters 4 and 6 are heavily dependent on the IS. How the IS collects information about its neighbouring access networks is beyond the scope of the IEEE802.21 WG and the IETF. As a result, this is an open issue which will require active research.
- The intelligent network selection scheme presented in chapter 4, section 4.4.7 is a very simple one. A much more sophisticated and intrinsic scheme is required which would take into account a wider array of parameters to make a more intelligent and optimized network selection.
- The solution presented in chapter 4 is meant for vehicular environments. The performance of the proposed mechanism is evaluated through NS2 simulations. However, there are limitations to the simulations and the results are not necessarily as accurate and realistic as would be necessary for real world roll out of the solution. As a result, it would be ideal to develop experiments for a field trial to evaluate real-world deployments.
- In chapter 6, a mathematical model has been presented to evaluate the performance of the IEEE802.21 fast EAP re-authentication mechanism. Due to the lack of security tools available in NS2 a simulation has not been possible. In order to provide a more detailed analysis, simulation results are required.
- Lastly, this thesis has considered most of the existing access technologies (both IEEE and non-IEEE, such as UMTS). However, it does not consider the upcoming uni-directional broadcast technologies, such as DVB-H [105]. Very recently, the IEEE802.21b TG has taken the initiative to define mechanisms to support optimized handovers between these technologies and other technologies already supported by IEEE 802.21. Currently, there is no standard which specifies such handovers. Therefore, much research is required in this field.

# References


[1] M. Roberts (2008-07-07), *Mobile Traffic boom to revive base station market* [Online], Available:http://www.lloydsmiu.com/itmgcontent/icoms/s/sectors/networksinfrastructure/20017550026.html

[2] (2009-03-07), *GSA Information Paper - HSPA evolution for the mobile handset always on experience* [Online], Available: http://www.gsacom.com/gsm_3g/info_papers.php4

[3] (2003-02-11), *MIPv6 diagram* [Online], Available: http://www. http://4ellene.net/tt/thumbnail/1/1200416370.w500-h308.jpg

[4] J. Rosenberg, et al., "SIP: Session Initiation Protocol", RFC 3261, IETF, June 2002

[5] R. Moskowitz, et al., "Host Identity Protocol", RFC5201, IETF, April 2008

[6] D. Johnson, et al., "Mobility Support in Ipv6", RFC 3775, IETF, June 2004

[7] R. Koodli, et al., "Fast Handovers for Mobile IPv6", RFC 4068, IETF, July 2005

[8] S. Gundavelli, et al., "Proxy Mobile IPv6", RFC 5213, IETF, August 2008

[9] H.Soliman, et al.,"Hierarchical Mobile IPv6 Mobility Management (HMIPv6)", RFC 4140, IETF, August 2005

[10] (2009-03-15) *Nemo diagram* [Online],

Available: http://www. http://www.cisco.com/web/about/ac123/ac147/images/ipj/ipj_10-2/102_nemo_fig1_lg.jpg

[11] T. Melia, et al., "Mobility Services Transport: Problem Statement", RFC 5164, IETF, March 2008

[12] S. Sreemanthula, et al., "Requirement For Handover Information Services", Internet Draft (work in progress), IETF, March 2006

[13] IEEE802.21 Standard and Metropolitan Area Networks: Media Independent Handover Services, Draft IEEE standards, Draft P802.21/D00.05, March 2006

[14] CALM –Medium and Long Range, High Speed, Air Interfaces parameters and protocols for broadcast, point to point, vehicle to vehicle, and vehicle to point communication in the ITS sector – Networking Protocol – Complementary Element, ISO draft ISO/WD 2121 (works in progress), ISO, Technical committee 204, WG16, December 2005

[15] V. Devarapali, et al., "Network Mobility (NEMO) Basic Support Protocol", RFC 3963, IETF, January 2005

[16] S. Deering et al, "Internet Protocolv6 Specification", RFC 791, IETF, December 1998

[17] M.Rey, "Internet Protocol Specification", RFC 2460, IETF, September 1981

[18] T. Socolofsky, C. Kale, "TCP/IP tutorial", RFC 1180, IETF, January 1991

[19] J. Bound, et al., "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, IETF, July2003.

[20] A. Patel and G. Giaretta, "Problem Statement for Bootstrapping Mobile IPv6 (MIPv6)", RFC 4640, September 2006

[21] J. Geier (2009, 01, 15**),** *Understanding 802.11 Frame Types* [Online**],** Available: http://www.wi fiplanet.com/tutorials/article.php/1447501

[22] R. Rouil, N. Golmie, “ADAPTIVE CHANNEL SCANNING FOR IEEE 802.16e”, In *Proceedings of Military Communications Conference*, MILCOM 2006

[23] S. Sreemanthula, et al., “Requirement for Handover Information Services”, Internet Draft (work in progress), IETF, March 2006

[24] G. Bajko, “Locating IEEE 802.21 Mobility Servers using DNS”, RFC 5679, IETF, December, 2009

[25] (2009-03-07), *NIST Project- Seamless and Secure Mobility tool suits* [Online], Available: http://www.antd.nist.gov/seamlessandsecure/doc.html

[26] (2009-03-07), *Nemo Simulation Toolkit* [Online], Available: http://www.w3.whu.edu.cn/en/

[27] C. Rigney, et al., “Remote Authentication Dial In User Service (RADIUS)”, RFC3971, IETF, June 2000

[28] V. Devarapalli, et al., “Mobile IPv6 Bootstrapping for the Authentication Option Protocol”, Internet Draft (work in progress), IETF March 2007

[29] G. Giaretta, et al., "MIPv6 Authorization and Configuration based on EAP", Internet Draft (work in progress), IETF, October2006

[30] K. Chowdhury and A. Yegin “MIP6-bootstrapping via DHCPv6 for the Integrated Scenario”, Internet Draft (work in progress), IETF April 2008

[31] A.Patel et al. ,"Problem Statement for bootstrapping Mobile IPv6", RFC4640, September 2006, IETF May 2005

[32] G. Giaretta, et al., “Mobile IPv6 bootstrapping in split scenario,” IETF, RFC 5026, IETF October 2007

[33] T. Hannes, et al., “Enriching Bootstrapping with Authorization Information”, Internet Draft (work in progress), IETF October 22, 2005

[34] B. Aboba, et al., “Extensible Authentication Protocol (EAP)”, RFC 3748, IETF, June 2004

[35] (2010-03-15), Generic Authentication Architecture (GAA); Generic bootstrapping architecture [Online], Available: http://www.3gpp.org/ftp/Specs/html-info/33220.html

[36] The Avispa Project [Online], Availaible: http://avispa-project.org/, Dec 10, 2008

[37] J. Kempf, et al.,“SEcure Neighbor Discovery (SEND)”, RFC3971, IETF, March 2005

[38] V. Narayanan, et al., “Establishing Handover Keys using Shared Keys”, Internet Draft (work in progress), IETF, March 6,2007

[39] C. Finseth, “An Access Control Protocol, Sometimes Called TACACS”, RFC 1492, IETF, July 1993

[40] P. Calhoun, “Diameter Base Protocol, RFC 3588, IETF, April 2010

[41] (2009-06-15), *EAP-MD5-Challenge Authentication Protocol*[Online], Available: http://www.juniper.net/techpubs/software/aaa_802/sbrc/sbrc70/sw-sbrc-admin/html/EAP-029.html

[42] D. Simon, et al., “The EAP-TLS Authentication Protocol”, RFC5216, IETF, March 2008

[43] P. Funk and S. Blake-Wilson,"Extensible Authentication Protocol Tunneled Transport Layer Security Authentication Protocol Version 0(EAP-TTLSv0)", RFC5281, IETF, August 2008

[44] A. Palekar, et al., "Protected EAP Protocol(PEAP) Version 2", Internet Draft (work in progress), IETF, October 15, 2007

**[**45**]** H. Tschofenig, et al., "The Extensible Authentication Protocol-Internet Key Exchange Protocol version 2 (EAP-IKEv2) Method**",** RFC 5281, IETF, August 2008

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

[47] B. Aboba, et al., "Extensible Authentication Protocol (EAP) Key Management Framework**"**, RFC 5247, IETF, August 2008

[48] P. Jayaraman, et al., "Protocol for Carrying Authentication for Network Access (PANA) Framework", RFC 5193, IETF, May 2008

[49] Requirements, scenarios and initial architecture, Project IST_ENABLE Deliverable D1.1, December 2006

[50] Definition of a general framework for service authorization and control, Project IST_ENABLE Deliverable D4.1, December 2006

[51] J. Salowey, et al., "Specification for the Derivation of Root Keys from an Extended Master Session Key (EMSK)", RFC 5295, IETF, June 23, 2008

[52] (2009-06-15), *fmipv6.org – Source code for FMIPv6* [Online], Available: www.fmipv6.org, March 30, 2007

[53] A.Izguierdo, et al., "Using the EAP framework for fast media independent handover authentication" In *Proceedings of the 4th Annual international Conference on Wireless internet*, Maui, Hawaii, 2008, pp.1-8.

[54] *VLC Media Player* [Online], Available: http://www.videolan.org/vlc/, May 30, 2007

[55] H. Schulzrinne, et al., "RTP: A Transport Protocol for Real-Time Applications", RFC3550, IETF, July 2003

[56] (2009-04-10), *Wireshark* [Online]: http://www.videolan.org/vlc/, July 15, 2007

[57] Mishra, et al., "An empirical analysis of the IEEE 802.11 MAC layer handoff process", *SIGCOMM Comput. Commun, Rev.* 33, 2, April, 2003

[58] S. Sreemanthula, et al., "Problem Statements and requirements for Event and Command Services in Media Independent Handovers", Internet Draft (work in progress), IETF, March 2006

[59] A. Rahman, et al.,"Transport of Media Independent Handover Messages over IP", Internet Draft (work in progress), IETF, January 1 2008

[60] M. Nakhjiri, “Keying and signaling for wireless access and handover using EAP (EAP-HR)”, Internet Draft (work in progress), IETF, April 5, 2007

[61] Y. Ohba, et al., “An EAP Method for EAP Extension”, Internet Draft (work in progress) July 2007

[62] J. Arkko and H. Haverinen, “Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)”, RFC 4182, IETF, January 2008

[63] V. Narayanan, L. Dondeti, “EAP Extensions for Efficient Re-authentication”, Internet Draft (work in progress), IETF, January 2007

[64] T. Clancy and H. Tschofenig, “EAP Generalized Pre-Shared Key”, RFC 5433, IETF, November 19, 2008

[65] D. Harkins, et al., “Problem Statement and Requirements on a 3-Party Distribution Protocol for Handover Keying”, Internet Draft (work in progress), IETF, March, 2007

[66] Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications - Amendment 2: Fast BSS Transition″, IEEE Standard 802.11r, January 2008 Transition, IEEE Standard 802.11r, January 2008

[67] IEEE Standard and Metropolitan Area Networks: Part16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems, IEEE Standard 802.16e, December 7 2005

[68] V. Narayanan and L. Dondeti, “EAP Extensions for Reauthentication Protocol”, RFC 5296, IETF, March 29, 2008

[69] V. Narayanan and G. Giaretta, “EAP-Based Keying for IP Mobility Protocols”, Internet Draft (work in progress), IETF, November 16, 2007

[70] W. Li, et al., “An efficient hierarchical authentication scheme in mobile IPv6 networks”, *ScienceDirect, 15(suppl*), pp 9-13, September 2008

[71] Jeff Goldman (2008-10-7), *Introducing IEEE802.11r* [Online], Available: http://www.wi-fiplanet.com/news/article.php/3776351, October 7, 2008

[72] S. Saha (2010-05-2009), *PLA-MIH: A secure MIH transport signaling scheme* [Online], – Submitted to IEEE802.21a WGAvailable: https:// sumanta679.wordpress.com/research/

[73] Y. Kim, et al., 2007. “Seamless handover support over heterogeneous networks using FMIPv6 with definitive L2 triggers”, *Wirel. Pers. Commu*, 43, 3, pp 919-932, November. 2007

[74] J. Lee and T. Chung, “Experimental Performance Evaluation of Mobile IPv6” Handovers over Wireless LAN, In *Proceedings of the international Conference on Systems and Networks Communication*, Washington, DC, 2006

[75] Y. Chu, et al., “Performance Evaluation of Mobile IPv6 Wireless Test-Bed in Micro-mobility Environment with Hierarchical Design and Multicast Buffering” *Technologies for Advanced Heterogeneous Network*s, Vol 3836, November 24, 2005, pp-57-67

[76] S. Kuppussami and L. Ganesam, “Parametric Analysis of Mobile IPv6 Using Ns2” *Journal of Mobile Communication 1*, 2007, pp-6-12

[77] A. Busaranun, et al., ( 2009-01-25), *Handover Performance of Mobile IPv6 on Linux Testbed* [Online], Availaible: http://wiki.nectec.or.th/ngiwiki/pub/Project/MobileIPv6/AdisakBusaranunECTI2006final.pdf

[78] X. Costa. P. and Hannes Hartenstein, “A simulation study on the performance of mobile IPv6 in a WLAN-based cellular network” *Comput. Netw*. 40, 1, pp 191-204 September, 2002

[79] X. Costa, et al, “A performance comparison of Mobile IPv6, Hierarchical Mobile IPv6, fast handovers for Mobile IPv6 and their combination”, *SIGMOBILE Mob. Comput. Commun. Rev.* 7, 4, pp5-19, October. 2003

[80] S. Haseeb and A. Ismail, “Handoff latency analysis of mobile IPv6 protocol variations”, *Comput. Commun.* 30, 4, pp 849-855, February 2007

[81] S. Nam, et al., “Fast Macro Handover in Hierarchical Mobile IPv6”, In *Proceedings of the Eighth IEEE international Symposium on Network Computing and Application,* Washington, DC, Volume 00, 2009, pp-323-326

[82] P. Kim, and Y. Kim, "Hierarchical Mobile IPv6 Based Fast Vertical Handover using IEEE 802.21 Media Independent Handover Function", *JCIT: Journal of Convergence Information Technology*, Vol.2 No.4, 2007, pp.41-45

[83] C. Gu, et al., "An Intelligent Seamless Handover Mechanism Based on IEEE 802.21," In *Proceedings of the International Conference on MultiMedia and Information Technology,* 2008, pp.558-561

[84] S. Hyeon, et al., “Empirical performance evaluation of IETF mobile IPv6 and proxy mobile IPv6”, In *Proceedings of the International Conference on Mobile Technology, Applications, and Systems*, Yilan, Taiwan, September 2008

[85] J. Jang, et al., “An Efficient Handoff Mechanism with Reduced Latency in Hierarchical Mobile IPv6”, *Springer Berlin/Heidelberg*, revised selected papers, 2004, 184-194

[86] I. Kim, et al., “Low Latency Proactive Handover Scheme for Proxy MIPv6 with MIH, Challenges for Next Generation Operations and Service Management”, Springer Berlin/Heidelberg, Vol.5297/2008

[87] J. Montavont, et al., “Deploying NEMO: A Practical Approach”, In Proceedings 6th International Conference on ITS Telecommunications, 2006

[88] H. Petander, et al., “Measuring and Improving the performance of Network Mobility Management in IPv6 Networks”- *IEEE Journal on selected areas in communications*, 2006

[89] H. Kang, et al, “Route optimization for mobile network by using bi-directional between home agent and top level mobile router”, Internet Draft (work in progress), IETF, June. 2003

[90] H. Ohnishi, et al., “HMIP based route optimization method in a mobile network”, Internet Draft (work in progress), IETF, Oct. 2003

[91] R. Wakikawa, et al., “ORC: Optimized route cache management protocol for network mobility,” in *Proceeding of 10th Int.Conf. Telecomm. (Protocol for Network Mobility)*, Papeete, Tahiti, French Polynesia, Feb. 2003.

[92] K. Bae, et al., "Access Router Information Protocol for Efficient Operation of Fast Handovers for Mobile IPv6", Proceedings of KISS Fall Conference, pp.7-9, 2004.

[93] E. Ivov and T. Noel, “An Experimental Performance Evaluation of the IETF FMIPv6 Protocol over IEEE 802.11 WLANS,” In *Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC’06)*, vol. 1, April 2006, pp. 568–574.

[94] E. Ivov, et al., “Thorough Empirical Analysis of the IETF FMIPv6 protocol over IEEE 802.11 networks” *Wireless Communications, IEEE* In Wireless Communications, IEEE, Vol. 15, No. 2. (2008), pp. 65-72.

[95] H. Jung, et al., “A Scheme for Supporting Fast Handover in Hierarchical Mobile IPv6”, *ETRI Journal*, Volume 27, Number 6, December 2006

[96] H. Yoo, et al., “ES-FHMIPv6: An Efficient Scheme for Fast Handover over HMIPv6” International Journal of Future Generation Communication and Networking**,** Vol. 2, No. 2, June, 2009

[97] G. Barjko, “Locating IEEE802.21 Mobility Servers using DNS”, Internet Draft (work in progress), IETF, July 12 2009

[98] S. Trong, et al., “Enhanced Vertical Handovers in Mobile IPv6 with Media Independent Handover Services and Advance Duplicate Address Detection”, In *Proceedings of I KNOM*, conference, 2008

[99] IEEE Standard for Information technology: Telecommunications and information exchange between systems Local and metropolitan area networks. Specific requirements, ANSI/IEEE Std 802.2, 1998

[100] High-speed Physical Layer in the 5 GHz band, ISO/IEC 8802-11:1999/Amd 1:2000, ISO Standard, 2005

[101] M. Liebsch, et.al, “Candidate Access Router Discovery (CARD)”, RFC 4066, IETF, 2005.

[102] R. Goodwins (2005-09-23), Intel senses united wireless future in 802.21 [Online], Available: http://news.zdnet.co.uk/communications/0,1000000085,39214636,00.htm

[103] (2009-07-17), *AT&T using 802.21 for iPhone 3G-Wifi handoffs?*, Available: http://www.9to5mac.com/ATT-802.21-protocol-wifi-3G-apple-iphone

[104] A. Patel, et al., “Authentication Protocol for Mobile IPv6”, RFC 4285, IETF, January 2006

[105] ETSI *standard* EN 302 304, ETSI Standard, November 2004

[106] S.Ryu, et al.,”Performance Analysis for FMIPv6 considering Probability of Predictive Mode Failure”, In *Proceedings of International Conference on Computational Science and Its Application*, Jeju, Korea, 2009

[107] C.Bettstetter, et al.,"Stochastic Properties of the Random Waypoint Mobility Model," In *Proceedings ACM Mobicom Workshop MSWIM*, 2002.

[108] N.Dutta, "Performance Studies of Layered MIPv6 based Network Architecture for better QoS: a Mathematical Approach", *International Journal of Computer Science and Network Security*, VOL.10, January 2010.

[109] W.B. Diab, et al., "End-to-End Security and Seamless Handover Solution for Real-Time Communication over 3G Networks", In *Proceedings of International Workshop on Modelling Analysis and Simulation of Wireless and Mobile Systems Proceeding of the 5th Symposium on QoS and Security for Wireless and mobile Networks,* conference, 2009

[110] N.Dutta,et al., "Cost Analysis of Three Layered MIPv6 (TLMIPv6) Mobility Model and HMIPv6, "- *International Journal on Computer Science*, 2010

[111] K.Ayyappan, et al., "RSS Measurement for Vertical Handoff in heterogeneous Network", -*Journal of Theoretical and Applied Information Technology*, 2008

[112] N.Dutta, "Performance Studies of Layered MIPv6 based Network Architecture for better QoS: a Mathematical Approach"- *International Journal of Computer Science and Network Security*, 2010

[113] V.Solouk, "Layer-2 Protocol Adaption Method to Improve Fast Handoff for Mobile IPv6 Vertical Handoffs", *Journal of Communication*, 2009

[114] M.R.Souryal, et al., "Link Assessment in an Indoor 802.11 Network", In *Proceedings of WCNC,* conference, 2006

[115] G.Gordon, System Simulation, 2nd Edition, PHI, 2002 pg.147.

[116] D.P. Agarwal et.al., Introduction to Wireless and Mobile Communication Systems, 2nd Edition, Thomson, 2004 pg.109

[117] B.Park, et al., "A Study on Optimal Fast Handover Scheme in Fast Handover for Mobile IPv6 (FMIPv6) Networks", In *Proceedings of ICUCT 2006, LNCS 4412*, pp. 120–129, 2007.

[118] Project Presentation, Project IST_ENABLE Deliverable D7.1, March 2006.

[119] T. Clancy, et al., "Handover Key Management and Re-Authentication Problem", RFC 5169, IETF, March 2008.

[120] R. Martin, et al., "3 Party Approach for Fast Handover in EAP Based Wireless Networks", SpringerLink, Lecture Notes in Computer Science Vol.4804/2007, 2007.

[121] Y. Ohba (2010-07-07), *IEEE802.21a Status Report* [Online], Available: http://www.ietf.org/proceedings/78/slides/hokey-2.pdf

[122] F.Kohlmayer, et al., "GSABA: A Generic Service Authorization Architecture", In *Proceedings of the ACM/IEEE International Workshop on Mobility in the Evolving Internet Architecture(MobiArch'06),* December 2006

[123] Service Authorization and control for fast/smart handover, Project IST_ENABLE Deliverable D4.3, December 2007

[124] P.Hankes., et al., “Formalizing and Analyzing Sender Invariance”, Lecture Notes in Computer Science, 2007, Volume 4691/2007

[125] S.Hee, et al., “FMIPv6 based Secure Binding Update Authentication in Wireless Vehicular Networks”, In *Proceedings of Wireless Pervasive Computing 2009, ISWPC*, February 2009.

[126] (2009-07-07), *Message Authentication Code* [Online], Available: http://www.answers.com/topic/message-authentication-code

[127] G.Y Jay., “Advances in mobile access networks”, Artech House Inc, Norwood, MA, 2004.

[128] (2009-02-07), *IPv6 Network Mobility* [Online], Available: http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_10-2/102_ipv6.html.

[129] J.Kempf, et al., “Distributing a Symmetric Fast Mobile IPv6(FMIPv6) Handover Key using SEcure Neighbour Discovery (SEND)”, RFC 5269, IETF, June 2008.

[130] Final Evaluation of state of art Mobile IPv6 alternatives, analysis of architectural impacts and description of possible deployment strategies, Project IST_ENABLE Deliverable D5.2, December 2006

## *GLOSSARY*

**Third Generation (3G):** A family of standards for mobile communications that fulfil specifications of the International Telecommunication Union (ITU), which includes UMTS, and CDMA2000. Compared to its precursors, 3G offers simultaneous use of speech and data services and higher data rates (at least 200kbits/s peak bit rate).

**3rd Generation Partnership Project (3GPP):** The scope of 3GPP is to make a globally applicable third generation (3G) mobile phone system specification within the scope of the ITU's IMT-2000 project. 3GPP specifications are based on evolved GSM specifications, generally known as the UMTS system.

**Fourth Generation (4G):** 4G is also known as “beyond 3G” or “fourth-generation” wireless technology. It offers an improvement over 3G networks and may stand as a successor thereof. A 4G system is expected to provide a comprehensive and secure all-IP based solution where services such as VoIP, high speed Internet access, streamed multimedia, gaming services etc may be provided to users. According to ITU requirements, 4G networks must have target peak data rates of up to approximately 100Mbit/s for high mobility and up to approximately 1Gbit/s for low mobility such as nomadic/local wireless access. 4G comprises different standards such as LTE Advanced and WiMAX (e.g.IEEE802.16m).

**Authentication, Authorization and Accounting (AAA):** AAA refers to the process of providing network security through Authentication, Authorization and Accounting mechanisms.

**Access Point (AP):** A wireless access point, identified by a Medium Access Control address, providing service to the wired network for wireless nodes.

**Access Router (AR):** The entity interconnecting the access network to the Internet or other IP-based networks; The AR provides connectivity between hosts on the access network at different customer premises. It is also used to provide security filtering, policing, and accounting of customer traffic.

**Access Service Authorizer (ASA):** A network operator that authenticates a mobile node and establishes the mobile node's authorization to receive Internet service.

**Access Service Provider (ASP):** A network operator that provides direct IP packet

forwarding to and from the end host.

**Asymmetric Digital Subscriber Line (ADSL):** A type of broadband communication technology where the data is sent over existing copper telephone lines, when compared to traditional modem lines. ADSL offers more downlink speed (24 Mbit/s) compared to its uplink speed (3.5Mbit/s)

**Bootstrapping Authorization Agent (BAA):** The BAA is a functional component that is responsible for asserting authorization statements which are conveyed to the mobile nodes.

**Bootstrapping Configuration Agent (BCA):** The BCA is a functional component that is responsible for providing necessary bootstrapping information to the mobile node (e.g. Home Agent address, the security association and the Home address).

**Bootstrapping Target (BT):** Entity that is part of the service providing server and is responsible for obtaining the service and Mobile Node related information from the BAA and BCA, and converting the obtained information into service target function understandable format.

**Binding Update (BU):** During the MIPv6 handover process, the BU is the message sent by the MN to inform the Home Agent of the new IPv6 address of the MN. The Home Agent uses the new IPv6 address to tunnel packets destined to the MN in the foreign link.

**Base Station (BS):** A wireless station, providing services to the wired network for wireless nodes.

**Care-of Address (CoA):** A unicast routable address associated with a mobile node while visiting a foreign link; the subnet prefix of this IP address is a foreign subnet prefix. Among the multiple care-of addresses that a mobile node may have at any given time (e.g., with different subnet prefixes), the one registered with the mobile node's home agent for a given home address is called its "primary" care-of address.

**Correspondent Node (CN):** A node on either a foreign network or the home network or other network with which the MN communicates

**Denial-of-service attack (DoS):** A malicious attempt to make computer resources (e.g. web site) unavailable to users. A common method of attack is by bombarding the target machine with packets requesting services, such that it cannot respond to

legitimate traffic since all the resources are consumed by the ill-intended requests.

**Digital Video Broadcasting – Handheld (DVB-H):** A standard that defines the digital transmissions of video and audio signals via antenna to mobile devices such as mobile phones, smart phones, PDAs, etc.

**Digital Subscriber Line (DSL):** A family of technologies that provide transmission of data over the local telephone network. The data throughput typically ranges from 384 KB/s to 20 MB/s in the direction of the customer.

**Extensible Authentication Protocol (EAP):** EAP is an authentication framework which is frequently used in wireless networks and point-to-point connections to provide authentication services.

**General Packet Radio Service (GPRS)**: The GPRS is an overlay network on top of the Global System for Mobile Communications (GSM) infrastructure. GPRS is a mobile data service available to users of GSM mobile phones

**Global System for Mobile Communications (GSM):** GSM is the international digital radio standard created by the European Telecommunications Standards Institute. GSM allows users to roam freely among GSM networks.

**High Speed Packet Access (HSPA):** HSPA is a collection of two cellular telephony protocols; High Speed Downlink Packet Access (HSDPA) and High Speed Uplink Packet Access (HSUPA). HSPA improves the peak data rates up to 14 Mbits/s and doubles the capacity for the uplink.

**High-Speed Downlink Packet Access (HSPDA):** HSDPA is an evolution of the W-CDMA standard, designed to increase the available data rate by a factor of 5 or more.

**High Speed Uplink Packet Access (HSUPA)**: It is an upgrade of the uplink introduced by HSPA.

**Host Identity Protocol (HIP):** A mechanism to separate the end-point identifier and locater roles of IP addresses. It introduces a new Host Identity (HI) name space which is based on public keys which are typically self-generated by the Host.

**Home Address (HoA):** A unicast routable address assigned to a mobile node, used as the permanent address of the mobile node. This address is within the mobile node's home link. Standard IP routing mechanisms will deliver packets destined for a mobile node's home address to its home link. Mobile nodes can have multiple home addresses, for

instance when there are multiple home prefixes on the home link.

**Home Agent (HA):** A router on a mobile node's home link with which the mobile node has registered its current care-of address. While the mobile node is away from home, the home agent intercepts packets on the home link destined to the mobile node's home address, encapsulates them, and tunnels them to the mobile node's registered care-of address.

**International Telecommunication Union (ITU):** A United Nations agency which is responsible for regulating information and communication technology issues.

**Internet Engineering Task Force (IETF):** The IETF develops and promotes Internet standards for the TCP/IP and Internet Protocol suite, by cooperating with other standards bodies such as the World Wide Web Consortium (W3C) and International Organization for Standardization (ISO)

**Internet Service Provider (ISP):** A company that offers Internet access to its customers using technologies such dial-up, Digital Subscriber Line, cable modem etc.

**Information Societies Technologies (IST):** The priorities set out for the European Union Framework Programmes for research, technological development and demonstration in the area of Information Technologies.

**Internet Protocol (IP):** A protocol used to identify an end-device in the Internet and used for communicating data and routing packets across a packet-switched internetwork.

**Internet Protocol Security (IPSec):** A protocol suite for securing IP communications by providing authentication and encryption of each IP packet of a data stream. IPSec also includes protocols for mutual authentication and negotiation of cryptographic keys to be used during a communication session.

**Local Area Network (LAN):** A network of end-devices (typically computers and servers) for data transmission, which covers a small physical area like a home, office, or small groups of buildings, such as a school, or an airport. Ethernet (i.e.IEEE802.3) and twisted pair cabling are the two most common LAN technologies currently in use.

**Medium Access Control (MAC):** The MAC layer is a sub-layer of the Data Link Layer of the TCP/IP protocol suite. It provides addressing and channel access control mechanisms that allow for multi-point network communication.

**Mobile Node (MN):** A node that can change its point of attachment from one link to

another, while still being reachable via its home address.

**Mobility Service Authorizer (MSA):** A service provider that authorizes Mobile IPv6 service.

**Mobility Service Provider (MSP):** A service provider that provides Mobile IPv6 service. In order to obtain such service, the mobile node must be authenticated and be authorized to obtain the service.

**Mobile-Stream Control Transmission Protocol (MSCTP):** A transport layer protocol which is similar to TCP and UDP. It provides message-oriented services like UDP and ensures reliable transport with congestion control like TCP. MSCTP is defined as providing the capability of dynamic address reconfiguration to aid IP handover.

**Network Access Server (NAS):** A server that provides access to a network.

**Portable Digital Assistant (PDA):** Generally, a PDA is a small portable device that works as an organizer.

**Point-of-Attachment (PoA):** The PoA is a device with which a mobile device has wireless connectivity such as an Access Point or Base Station.

**Point-of-Service (PoS):** Any network entity with which a mobile device exchanges Media Independent Handover Information (MIH) messages is referred as the PoS in this thesis.

**Received Signal Strength (RSS):** The RSS is the power (in mW) of a received signal in a wireless environment.

**Real-time Transport Protocol (RTP):** A standard for packet format and delivery of audio and video data over the Internet.

**Roaming Broker (RB):** An entity that provides (global) services for Home Entities and Hotspot Operators by operating as an intermediary and trading broadband access between them at a fixed or transactional price (buying and re-selling roaming airtime usage), and performs clearing and settlement services. Brokers may provide centralized authentication services in order to compute and validate the broadband traffic.

**Round-trip delay time (RTT):** Is the time taken for a segment to be sent and the time it takes to receive an acknowledgment of that segment.

**Session Initiation Protocol (SIP):** An IETF defined signalling protocol used for controlling communications for voice and video calls over IP. The protocol can create, modify and terminate two-party (unicast) or multiparty (multicast) sessions consisting of one or several media streams.

**Level 3 Multihoming for Shim Protocol for IPv6 (SHIM6):** The shim6 protocol specifies a layer 3 shim approach and protocol for providing locator agility below the transport protocols, so that multihoming can be delivered for IPv6 for load sharing and failover.

**Stream Control Transmission Protocol (SCTP):** A transport layer protocol which is similar to TCP and UDP. It provides message-oriented services like UDP and ensures reliable transport with congestion control like TCP.

**Universal Mobile Telecommunications System (UMTS):** UMTS is a next generation network for mobile communication. UMTS is a 3G network (3rd generation) and is the successor of the 2nd generation GSM.

**Ultra Wide Band (UWB):** UWB is a technology for transmitting information spread over a large bandwidth that should, in theory and under the right circumstances, be able to share spectrum with other users.

**Voice over Internet Protocol (VoIP):** Is a general term for an umbrella of transmission technologies for transmitting voice data over the Internet. VoIP systems employ session control protocols to control the set-up and termination of calls as well as audio codecs which encode the voice data.

**Wireless Local Area Network (WLAN):** A network where devices are linked via a wireless method (typically spread spectrum or OFDM) which usually provides shared access connectivity with an Access Point to the wider Internet. The WLAN is synonymous with the IEEE802.11 family of standards, which is the most mature and widely used set of Wireless LAN standards.

**(Wi-Fi):** A Wi-Fi is usually referred as a trademark of the Wi-Fi Alliance that manufacturers use to brand certified products that belong to a class of wireless devices which provides Internet access over a Wireless Local Area Network through the use of a router connected to an Internet service provider.

**Wireless Code Division Multiple Access (W-CDMA):** An air interface standard for the 3G specification. It is the most commonly used member of the Universal Mobile Telecommunications System (UMTS) family.

**Quality of Service (QoS):** Quality of Service refers to resource reservation control mechanisms rather than the achieved service quality. Examples of QoS metrics are delay, jitter, packet dropping probability, etc.