Micro mobility improvement in proxy mobile IPv6 domain

Ahmed Kamaleldin Elsayed Baioumy

Thesis to obtain the Master of Science Degree in

Telecommunications and Informatics Engineering

Supervisors: Prof. Fernando Henrique Côrte-Real Mira da Silva
Prof. Rui Manuel Rodrigues Rocha

Examination committee

Chairperson: Prof. Paulo Jorge Pires Ferreira
Supervisor: Prof. Fernando Henrique Côrte-Real Mira da Silva
Member of the committee: Prof. Paulo Rogério Barreiros D' Almeida Pereira

November 2014

Anyone who has never made a mistake has never tried anything new.

Albert Einstein

Acknowledgments

I am indeed grateful to my supervisor Prof. Fernando Mira da Silva for his supervision, his best advice, kind supervision, useful discussions, and encouragement during the progress of this work.

Acknowledgments are also due to Prof. Rui Rocha for his valuable comments and suggestions at various stages of the work.

Deep thanks to my friends; Shady Alaa and Henrique Rocha for assisting me during the work and their encouragements all the time.

Also, I would like to thank all my family that always supports me in all my decisions in life.

Last but not least my wife and sons, my life is you.

Ahmed Baioumy

October 2014

Abstract

Micro mobility is one of the most important topics that had and still has a great interest in wireless networks. The growing need for mobility inside the network without losing the connection or any data transferred has motivated the researchers to work on this topic. The IETF has standardized a group of protocols that provide a seamless mobility across the wireless networks. There are two types of mobility management, the host based mobility management and the network based mobility management.

In the host based mobility management protocols operation, the mobile node is involved in the signaling process within the mobility domain.This in fact increases the complexity of the network stack and consumes the limited power sources available on the mobile nodes.

In the other hand, the network in network based mobility management protocol takes the responsibility of performing the required network's signaling messages exchange on behalf of the mobile node.

The Proxy Mobile Internet Protocol version 6 (PMIPv6), which is a network based mobility management protocol, aims to reduce the complexity of the network stack and improve the mobility of the mobile node in wireless networks. In spite of the fact that the protocol presents a very smart solution to improve the mobility and overcome the need of mobile node involvement in signaling exchange but it still has some limitations. These limitations due to the handover time delay, the packet loss during the handover process and the handover overhead that is caused by signaling message exchange.

This Thesis presents an implementation of a test bed for the PMIPv6 protocol, an evaluation of this protocol and some proposed solutions that attempt to overcome the protocol's limitations.

Keywords

Proxy Mobile IPv6, MPLS, handover, delay, packet loss.

Resumo

A micro mobilidade é um dos tópicos mais relevantes e ainda de grande interesse em redes sem fios. A necessidade crescente de mobilidade sem perda de conectividade ou de perda de pacotes motivou muitos investigadores a considerarem a transferência do protocolo IP para o protocolo IP móvel (*Mobile IP*). O IETF normalizou um grupo de protocolos com o objectivo de proporcionarem uma mobilidade suave e transparente entre redes móveis. A primeira categoria de protocolos é baseado na gestão de protocolos em cada nó. Neste grupo de protocolos, o nó móvel está envolvido no processo de sinalização dentro do domínio abrangido. Esta solução aumenta a complexidade da pilha de protocolos e consome uma fracção significativa da potência disponível nos nós móveis, reduzindo a sua autonomia.

Considerando estas limitações, o IETF normalizou um protocolo de gestão de mobiilidade baseado na rede. Nesta classe de protocolos, a rede realiza toda a sinalização necessária ao nó móvel. Um dos protocolos desta classe o protocolo IPv6 móvel baseado em proxy (PMIPv6). PMIPv6 tem como objectivo reduzir a complexidade da pilha de protocolos e e melhorar a mobilidade em redes sem fios. Apesar deste protocolo apresentar uma solução elegante para melhorar a mobilidade sem alterações do nó envolvido, apresenta ainda algumas limitações. Estas limitações

referem-se sobretudo nos atrasos de transferência entre pontos de acesso (*handover delay*), perda de pacotes e no tempo adicional de transferência (*handover*). Esta tese apresenta uma montagem de um ambiente de teste do protocolo (PMIPv6), uma avaliação do protocolo, e propõe algumas possíveis alterações para melhorar o seu desempenho.

Palavras Chave

Proxy Mobile IPv6, MPLS, handover, delay, packet loss.

Contents

List of Figures

List of Tables

Abbreviations

List of Acronyms

AAA Authentication, Authorization, and Accounting

AP Access Point

ATM Asynchronous Transfer Mode

BU Binding Update

Cellular IP Cellular Internet Protocol

CN Correspondent Node

FBU Fast Binding Update

FEC Forwarding Equivalence Class

FMIPv6 Fast Handover for Mobile Internet Protocol v6

FPMIPv6 Fast Hand over for Proxy Mobile Internet Protocol v6

FRep Forward Reply

FR Frame Relay

FReq Forward Request

HAck Handover Acknowledgment

HI Handover Initiate

HMIPv6 Hierarchical Mobile Internet Protocol version 6

HNP Home Network Prefix

IEEE Institute of Electrical and Electronics Engineers

IETF Internet Engineering Task Force

IP Internet Protocol

IPv4 Internet Protocol version 4

IPv6 Internet Protocol version 6

LDP Label Distribution Protocol

LER Label Edge Router

LFIB Label Forwarding Instance Base

LIB Label Information Base

LSP Label Switch Path

LSR Label Switch Router

LMA Local Mobility Anchor

LMD Local Mobility Domain

MAC Media Access Control

MAG Mobility Access Gateway

MIP Mobile IP

MIPv6 Mobile IPv6

MN Mobile Node

MNID Mobile Node Identifier

MPLS (Multiprotocol Label Switching)

NDPv6 Neighbor Discovery for IP version 6

NMAG New MAG

PAR Previous Access Router

PBA Proxy Binding Acknowledgment

PBU Proxy Binding Update

PCOA Proxy Care Of Address

PMAG Previous MAG

PMIPv6 Proxy Mobile Internet Protocol version 6

RA Router Advertisement

RADIUS Remote Authentication Dial In User Service

RTT Round Trip Time

RSS Received Signal Strength

RSVP-TE Resource Reservation Protocol - Traffic Engineering

TCP Transmission Control Protocol

UDP User Datagram Protocol

UMIP USAGI-patched Mobile IPv6 for Linux

VOIP Voice Over IP

VP Virtual Pipe

1

Introduction

Contents

1.1 Motivation

The main purpose of this work is to achieve an improvement in micro mobility inside the PMIPv6 domain. The micro mobility is the movement of the mobile node through different points of attachment in the same domain. These points of attachment which are refereed here as APs can operate from different subnets but they belong to the same domain and the mobile node mobility between theses AP in this case called intra-domain mobility.

The MIP [1] is considered a solution that allows the mobile node to keep connected to the network while changing its point of attachment. The IETF has introduced some new entities like Home Agent and Foreign Agent to support mobility in mobile IPv4 [2]. This step was followed by mobility support in IPv6 [3]. The registration between these agents is necessary in order to keep tracking the changes of the mobile node's location and address. The mobile node should update its location and address every time connects to a new point of attachment.

The signaling messages exchange between the network entities in MIP protocol causes a huge overhead inside the network. For this reason there was a need for new versions that provide efficient solution for the increasing in handover mobility.

The proposed solutions from IETF were Cellular Internet Protocol (Cellular IP) [4] , Hawaii [5], HMIPv6 [6]. The main idea in these solutions was to create kind of Hierarchical router distribution that keeps the registration and signaling traffic in the nearest point to the mobile node instead of doing this through a long path.

Recently proposed the PMIPv6 as a network based management protocol. The main advantage of Proxy mobile PMIPv6 is the non involvement of the mobile node in the signaling messages exchange process and the network does all of these procedures on behalf of the mobile node.

There is no need for the mobile node to have the proxy mobile mobility stack to be served in the PMIPv6 domain. In addition the mobile node as battery dependent device can save a significant amount of power and this result from the non-involvement in the signaling exchange process.

The motivation behind this work is to achieve an improvement in the mobility inside PMIPv6 [7] and this improvement could be presented by reducing the limitations in the PMIPv6. These limitations are due to handover delay, packet loss and handover overhead.

The work is based on a test bed for the PMIPv6 beside a modification in some procedures of the protocol in order to achieve the main goal of the thesis work which is the improvement in the micro-mobility of the mobile node inside PMIPv6 domain.

1.2 Objectives

The main goal is to achieve an improvement of micro-mobility inside the PMIPv6 domain and this improvement can be done with improving three main factors which are the handover overhead, the hand over delay and the packet loss. To achieve this goal the analysis is built on real test bed that may help in understanding the real behavior of the protocol in a real scenario even in a small scale. The proposed solutions need to be tested, evaluated and optimized in order to achieve the goals.

1.3 Dissertation research topics

This work is developed based on the next research topics:

- the MIP, which is the basis for all the micro -mobility protocols;
- the PMIPv6, the main target of the research and its improvement is the goal of this thesis;
- the MPLS, as a solution for reducing the overhead in the proxy domain; and
- the packet loss mechanisms, in order to reduce the limitation in the protocol.

1.4 Contributions

This work aims to provide a solution to improve PMIPv6 protocol and make it much closer to the commercial use. The protocol as network based mobility management protocol forms an interest point for a lot of researchers in order to facilitate the usage of the protocol within the recent technology devices.

1.5 Dissertation layout

This dissertation is organized into six main chapters. Chapter 1 gives an introduction to this work, its motivation and goals and the most important research topics. Chapter 2 presents a survey of the related work in this area, which includes the proxy mobile IPv6 overview, Fast handover for proxy mobile IPv6, buffering mechanisms and finally MPLS. Chapter 3 presents a detailed view of the proposed architecture. Chapter4 goes over the solution's implementation details Chapter 5 presents the evaluation of the implemented solutions, which includes functional tests results. Finally, Chapter 6 draws the final conclusions and lays out foundation for future work in the studied area.

2

State of the art

Contents

2.1 Proxy mobile IPv6 overview

The Proxy Mobile Internet Protocol version 6 (PMIPv6) is considered one of the solutions that has been specified by IETF to overcome the need of the mobile node's involvement in the mobility-related signaling exchange. The network takes the responsibility of the mobility management on behalf of the mobile node in this domain. This feature makes the PMIPv6 a distinct solution that helps in reducing the signaling overhead on the mobile node.

This solution gives the network operator the facility to support the mobility without any need to implement additional mobility stack on the mobile node. As the localized mobility process is transparent and independent that can facilitate the implementation of any global mobility solution. This transparent feature reduces the signaling overhead every time the mobile is attached to a new access point comparing to the previous solutions namely, cellular IP [4] , Fast Handover for Mobile Internet Protocol v6 (FMIPv6) [8], Hierarchical Mobile Internet Protocol version 6 (HMIPv6) [6] which all are host based management mobility.

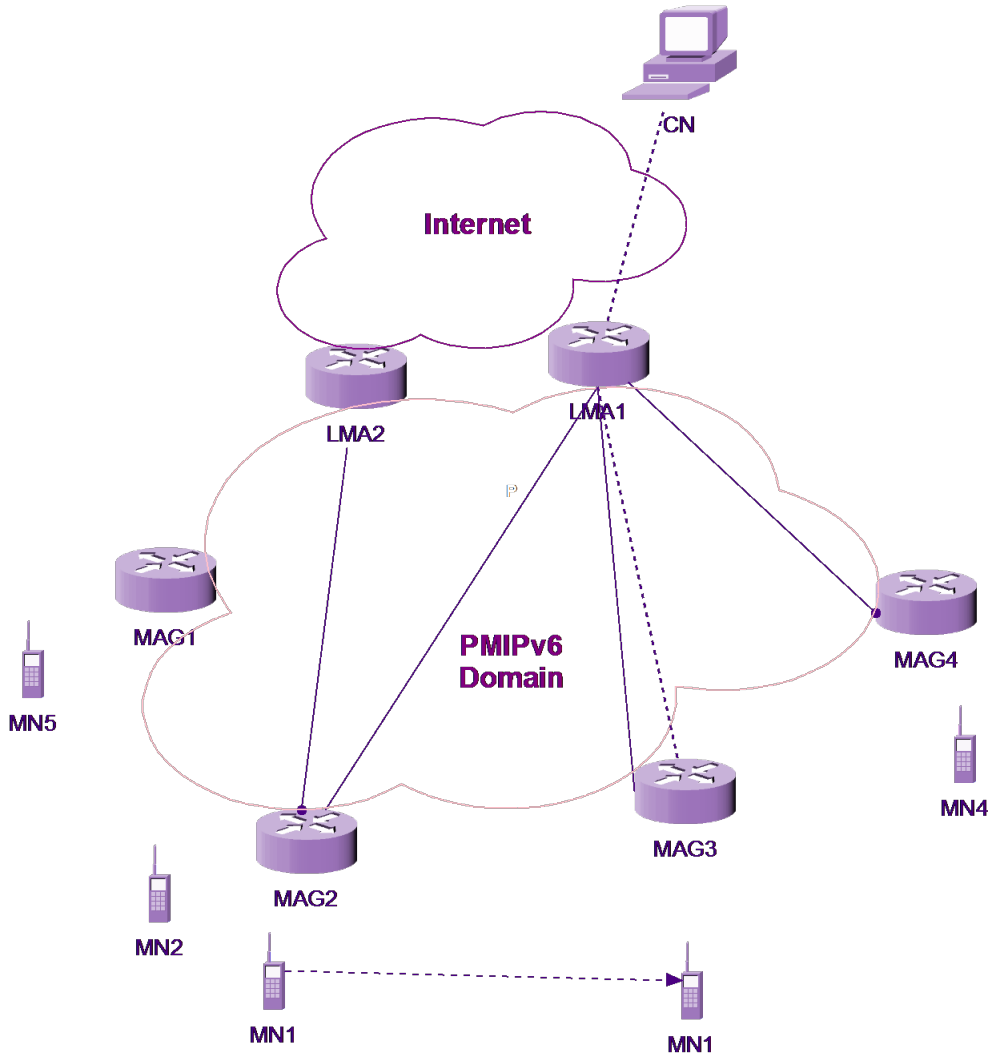

Figure 2.1: Proxy mobile IPv6 domain

The PMIPv6 provides mobility support within a localized area called the Local Mobility Domain

(LMD) or PMIPv6 domain. The mobile node keeps the same IP address within the movement in the domain and the network is in charge to keep tracking its location. There are two main functional entities inside PMIPv6 network as defined in [7],Local Mobility Anchor (LMA)and Mobility Access Gateway (MAG) as shown in figure 2.1.

The LMA is acting similarly to the home agent in Mobile IP (MIP) and is considered the topological anchor point for the mobile node inside the domain. Any traffic flows toward or from the mobile node passes through the LMA and the correspondent MAG tunnels. The main functionality for the LMA entity is clarified with more details in section 3.2.1

The MAGis the first steward for the mobile node that is attached to this MAG 's access links, also it performs the required signaling messages exchange on behalf of this mobile node. The MAG is considered the first hop router in the Localized Mobility Management infrastructure that tracks the movement of the mobile node in the LMD. The main functionality for the MAG entity is clarified with more details in section 3.2.1

As can be seen from figure 2.2, the Mobile Node (MN) once enters the PMIPv6 domain, the first MAG provides an access link and performs the identification process for this mobile node. The MAG after acquiring the MNID, sends a PBU message which includes this MNID and the MN's current location. This identifier can be the mobile node's MAC address or any other identifier. In this case the LMA allocates an address (es) prefix (es) to the mobile node and reply to the MAG with PBA that includes all the prefixes assigned for that particular mobile node.

The LMA then creates a binding cache entry and establishes a bidirectional tunnel with the serving MAG. The mobile node identifier inside the domain is associated with a policy profile. This profile identifies the mobile node's home network prefix(es), permitted address configuration modes, roaming policy, and other parameters that are important for the network-based mobility services. The authentication procedures are performed by the Authentication, Authorization, and Accounting (AAA) server by using either the RADIUS protocol [9] or DIAMETER protocol [10].

After the MAG receievs the PBA message, which contains the network prefix (es) assigned for this mobile node, it sends a router advertisement to the mobile node. The mobile node then auto- configures its interface(s) with (this/these) unique prefix(es). The mobile node configures these addresses in one of two ways either the stateless auto-configuration or stateful address auto-configuration.

The mobile node starts the handover process when it moves to a New MAG (NMAG). This NMAG subsequently updates the mobile node's location to the LMA and then advertises the same prefix to the mobile node. By this way the mobile node keeps the same configured address even it moves from point to point in this domain. The signaling flow of the handover process is shown in figure 2.3.

The MAG, to ensure that the mobile node never detects the changes in its default route configuration, assigns the same link local address to the mobile node during its movement in the LMD. A bi-directional tunnel is established between the LMA and the MAG. The LMA forwards the down-link packets (packets that are sent to the mobile node) through the tunnel to the serving MAG which in sequence sends these packets to the MN. The up-link packets(packets originated in mobile node), are sent firstly to the MAG and then similarly to LMA through the tunnel.

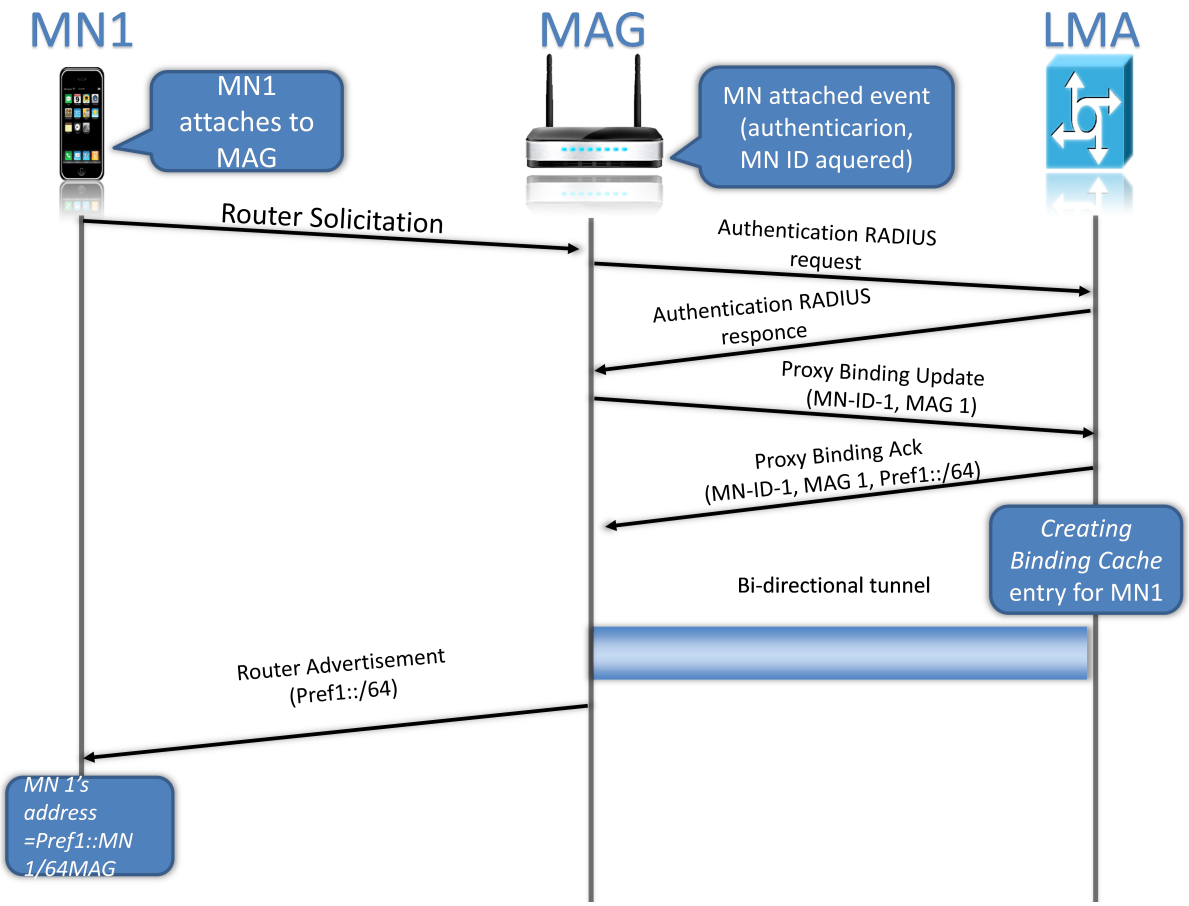

Figure 2.2: Mobile node attachment-Signaling Call Flow

The PBU message, as stated in [7], is considered an extension to the BU message of MIPv6 protocol. This message contains additional flag to indicate that it is a proxy binding updates message. This PBU message has a source address, similar to the egress interface address of the MAG, which is called the Proxy Care Of Address (PCOA)and is considered as the locator of this mobile node. There are additional information thet is included in the PBU message namely, the access link technology, the handover indicator, the life time for registration and other optional data.

The handover indicator [7] is a new option in PMIPv6 that gives some indication about the type of handover process, it is a 8 bit field has the values (0-255) and these values indicate specific situation [7] as follows:

[0]:→ Reserved

[1]:→ Attachment over a new interface

[2]:→ Handoff between two different interfaces of the mobile node

[3]:→ Handoff between mobile access gateways for the same interface

[4]:→ Handoff state unknown

[5]:→ Handoff state not changed (Re-registration)

The LMA performs some authentication procedures in order to determine if the mobile node is authorized for the proxy mobility services. Firstly, the LMA applies a policy checks to ensure that the connection with a trusted MAG which is authorized to send the message on behalf of that mobile

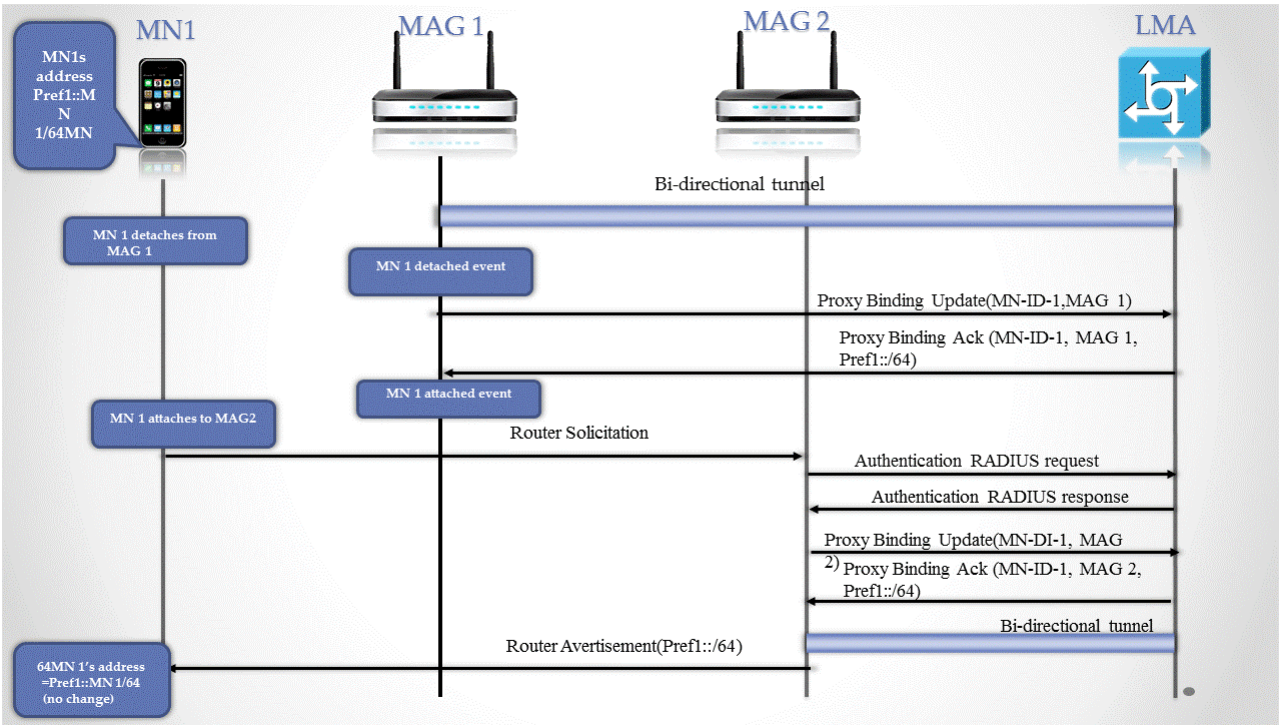

Figure 2.3: handover signaling flow in PMIPv6

node. Secondly, it identifies the mobile node's identification in the PBU message and if the mobile node is not authorized the LMA rejects the request. The LMA puts (missing MN identifier) inside the acknowledgement message and sends it back to the MAG.

2.2 Proxy mobile IPv6 limitations

2.2.1 Handover delay

In spite of the fact that PMIPv6 is a network management protocol and this in turn reduces the mobility- related signaling exchange overhead, that is associated with the previous mobility protocols, but the protocol still has some limitations regarding the hand over of the mobile node in the PMIPv6 domain.

One of these limitations is the time delay during the handover process of the mobile node. The is a verity in this time delay according to the used technology. This section explores the different types of time delay that affect the micro-mobility handover process and in turn has a big influence on the data delivery inside the PMIPv6 domain.

2.2.1.A Link layer handover delay

The link layer handover time delay, regarding that the used technology here is the 802.11 wireless communication, is resulted from performing three different phases:

1. The first phase is the scanning phase, the delay in this phase occurs when the mobile node moves inside the network and scans the wireless link searching for new access point. Once the mobile node senses the weakness of signal strength and the probability of losing the signal becomes high the handover process accordingly is required. The mobile node starts the scanning phase directly in one of two ways [11], the passive method and the active method. In the passive mode the MN listens the wireless medium for beacon frames. in active way the MN sends a Probe Request packet on each probed channel and waits for a Probe Response.

2. The authentication delay occurs when the MN accesses the domain and attempts to connect to the nearest access point to its link with sending an authentication request.

3. The re-association delay occurs after the success of authentication process and the MN exchanges re-association's messages with access point to complete the handover process.

2.2.1.B Network layer handover delay

The network handover time delay, starts when the MN moves inside the proxy domain between different (sub-nets). The exchange of signaling messages between MAG and LMA has a significant delay but this exchange is important to keep the updates of the location transparent for the mobile nodes. In addition this allows the LMA to forward the packets into or from the mobile node in the current location. This time delay consists of different component that can be summarized as the follows:

- the delay between the MN and the AP which is the time necessary for a packet to be sent between the MN and the AP through a wireless link,
- the delay between the AP and the MAG,

- the delay between the MAG and the mobility anchor point LMA,
- the delay between the LMA and the AAA server, and
- the delay between the LMA and the CN.

2.2.2 Packet loss

The PMIPv6 specification has not specified any buffering mechanism to eliminate the packet loss occurs in the handover period. This loss causes a loss in information which can be significant in some applications. In order to overcome this problem, there is a need to add a buffering mechanism to the PMIPv6protcol.

2.2.3 Handover overhead

The handover overhead can be measured by the number and weight of packets that are exchanged between the network entities, the packet weight can be measured by its length and the transmission mode. The mobility-related signaling messages consist of, MN's attachment messages, authentication messages, binding updates and router advertisement messages. The high handover overhead also results in operational overhead to process all these messages. So there is a need for fast forwarding technique that be able to reduce the handover overhead and in the same time costs less bits which in order results in less operational overhead.

2.3 Fast handover proxy mobile IPv6

2.3.1 FHPMIPv6 overview

The Fast Hand over for Proxy Mobile Internet Protocol v6 (FPMIPv6) protocol is one of the proposed solution from IETF to overcome the handover delay inside the PMIPv6. The main difference between this protocol and PMIPv6 is the additional mechanisms that allow the mobile node to send or receive data as soon as it detects a new subnet link as specified in [12].

In order to reduce the handover time delay, the IETF has specified a bi-directional tunnel between the PMAG and the NMAG. The Previous MAG (PMAG) is the last point of attachment for the MN before the starting of the handover process. The NMAG is the new point of attachment for the MN after the end of handover process.

There are two modes of operation in FPMIPv6, the predictive mode and reactive mode. In the predictive mode the tunnel between the PMAG and NMAGis established before the attachment of the mobile node to the NMAG. In the reactive mode this tunnel is established after the mobile node is attached to NMAG.

In order to work in predictive mode the mobile node should report its need to change the point of attachment. The PMAG receives this report and forwards a Handover Initiate (HI) message to the NMAG. The HI message format is specified in [12] as an extension to HI message in [13] and is shown in figure 2.4.

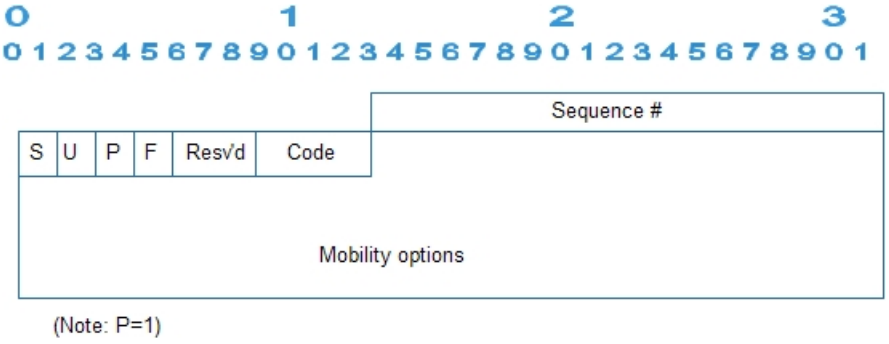

Figure 2.4: Handover Initiate (HI) message format

The detailed information of flags that is included in HI message which defined in [13] is as follows:

- the S flag, which is the assigned address configuration flag, is set to zero in fast handover FPMIPv6,
- the U flag, which called buffer flag, when is set so the buffer should start and if the code is set to zero then U flag is set to 1 and vice versa,
- code value, which is used by Previous Access Router (PAR), is set according to the source IP address and if the source of acsIP address is the PCOA so this value is set to 1 and vice versa,
- the P flag ,which is proxy flag, is an additional flag and it is set to mark the messages that belong to FPMIPv6 protocol, and

- the F flag, which is forwarding flag, is used to request the forwarding of the packets to the mobile node.

Figure 2.5 shows The steps of handover signaling inside the predictive FPMIPv6 and these steps can be summarized as the follows:

1. The mobile detects its need to perform the handover process and sends a report message which includes MNID associated with the new AP ID. This new AP is the most likely new point of attachment for mobile node after the handover process. The MN sends this report according to a trigger, this trigger can be a degradation in the signal strength value of the current AP connection comparable to the signal strength value of the new AP's connection.

2. The previous AP reports the handover of the MN to the PMAG. The PMAG recognizes the NMAG from the new AP ID previously sent in the mobile update message.

3. The PMAG sends the HI message to the NMAG, this message includes MNID, the Home Network Prefix (HNP)(s), and the current LMA address.

4. The NMAG replies with Handover Acknowledgment (HAck) message with (P) flag set.

5. A bi-directional tunnel is established and PMAG forwards the packets through this tunnel to the NMAG.

6. As soon the network is ready to do the handover, the PMAG sends a trigger to the MN to perform the handover to the new AP.

7. The mobile starts the physical-layer connection with the new AP which is followed by a connection with the NMAG that is connected to this AP.

It is clear from the last discussion that FPMIPv6 contains some additional mechanisms, buffering mechanism and usage of HI message. Although These mechanisms can help in reducing the handover latency and packet loss in PMIPv6 but in the same time it makes the mobile node be involved in some of the handover-related signaling. This in fact is not convenient for PMIPv6 protocol's operation as it is a network based management protocol. The mobile should not involved in any kind of mobility related , so there is a need for a new solutions that be able to fulfill this condition.

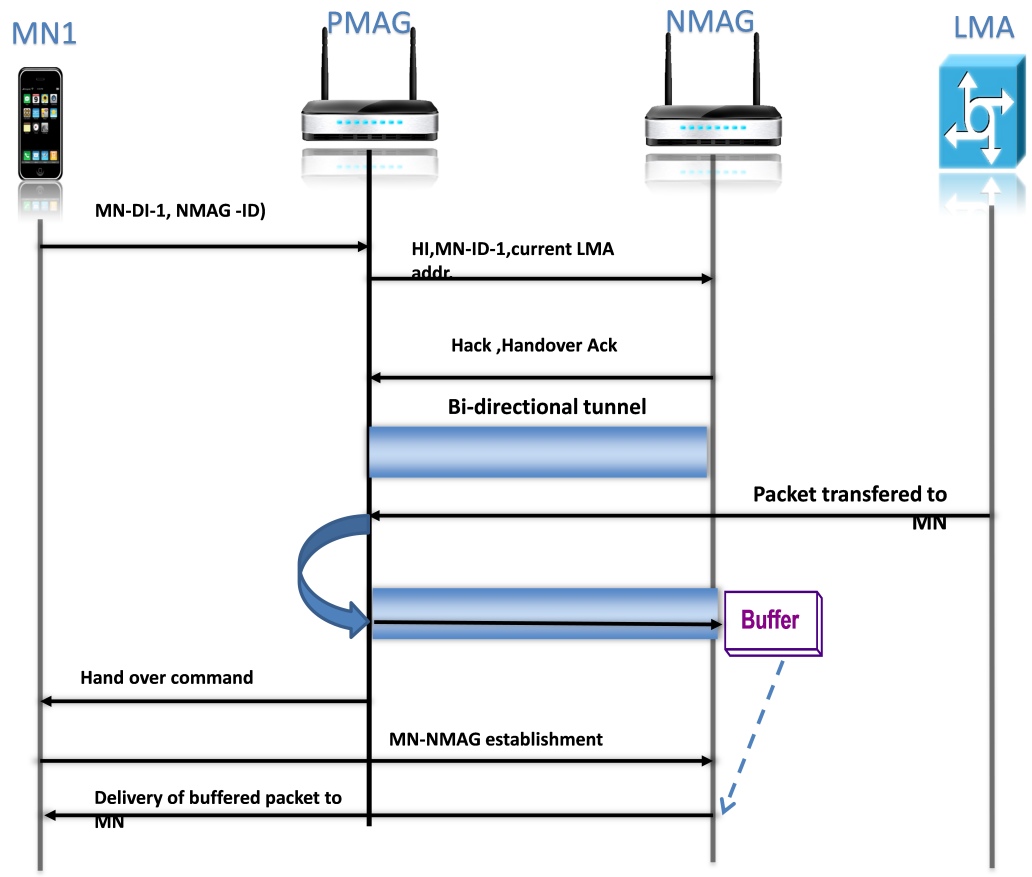

Figure 2.5: Predictive fast handover for PMIPv6

2.3.2 Related work to Fast handover for PMIPv6 solution

The most interesting approaches to this issue have been proposed by [12],[14]. The main goals of these approaches are to present a proactive fast handover scheme to minimize the handover delay. Also attempt to eliminate the packet loss by presenting a buffering mechanism that is not provided by PMIPv6's specification.

The draft in [14] proposes an enhancement to PMIPv6 protocol in order to improve layer 3 handover. The fast handover scheme operates in two modes, the predictive mode and reactive mode.

In predictive mode the PMAG sends context of the MN to the NMAG using HI message. In reactive mode the NMAG sends Fast Binding Update (FBU) to request context from PMAG. The proposal in [12] specifies a bidirectional tunnel betweenPMAG and NMAGto tunnel the packets into or from the mobile node.

The comparative handover performance analysis in [12] shows some evaluation of the fast handover extension FPMIPv6 and this can be summarized as follows:

- considering the Layer 2 information the predictive FPMIPv6 outperforms better than other mobility solutions and the reason for that is the proactive handover mechanism that results in reducing the handover blocking probability, and
- considering the packet loss, the FPMIPv6 also shows good performance's result due to the

buffering mechanism.

Although the analysis shows a better performance of the fast handover proposal in [12]and [14], still the fact that there is some difficulty to apply this approaches to PMIPv6 protocol. This difficulty comes from the dependence of the solution on the mobile to report its need to perform the handover process.

2.4 Buffering mechanisms for proxy mobile IPv6

The packet loss is considered one of the PMIPv6 protocol's limitations. This packet loss occurs during the handover period of the MN. There is a need for additional buffering mechanism to overcome this limitation. The buffering mechanism, that is presented by previous proposals, must be enhanced in order to be adaptive with the functionality of PMIPv6 protocol. The first step in this adaptation is the non involvement of the mobile node in any kind of mobility-related signaling exchange in the domain.

The considerations for creating a buffering mechanism, as mentioned in [12], can be summarized as follows:

- the buffer size and packets forwarding rate, are two important factors that must be taken into consideration when a buffering mechanism is provided,
- buffering requirement is different from an application to another, some applications transmit less data over a given period of time than others, for instance Voice Over IP (VOIP) application requires less buffer size than streaming video one, and
- the mobile node can face different bandwidth links with different signal condition during its movement in the domain.

The buffering mechanism that suits the PMIPv6 should provide the service without the involvement of the mobile node in any kind of signaling in the solution.

2.4.1 Related work for buffering mechanism

Recently, two proposals [15], [16] have proposed a buffering mechanism for PMIPv6. The proposal in [15] presents a buffering mechanism for PMIPv6 and the main idea of the proposal is to provide PMIPv6 with a buffering mechanism that is performed completely by the network entities. It is not required from the mobile node to give any reports about its need to perform the handover process.

The LMA entity is the entity responsible for this buffering mechanism. The packets that are sent to the mobile node is buffered in LMA until the time of the mobile node's attachment to the NMAG. The buffering mechanism starts to work after receiving a de-registration message from the PMAG which updates the disconnection of the mobile node from its access link.

The buffering mechanism operates in three stages, packet classification to determine the packet that should buffered, packet buffering and the packet forwarding. The purpose of the approach is to achieve a minimum packet loss with some adjustment for the packet forwarding rate. This proposal is discussed in more detail in the next chapters with an evaluation for the proposed buffering mechanism.

[16] presents a scheme to prevent a packet loss by a proactive buffering mechanism. The scheme provides a solution to eliminate redundant packets by reordering mechanism at the packet destination. The proactive way in this scheme is achieved by informing the serving MAG the exact time for the mobile node's handover and the target MAG after the handover process. The difference in this scheme from the fast handover scheme in [12] is that the prediction mechanism in this scheme is performed

from network side with the help of MAG discovery mechanism. The scheme presents the buffering mechanism in four phases: packet buffering, redundant packet elimination, PMAG discovery and packets reordering in a NMAG.

The packet buffering mechanism, as presented in [16], is performed in the PMAG entity. The PMAG starts the buffering mechanism when the Received Signal Strength (RSS) from the MNfalls below a pre-defined threshold value.

The packets buffering continues until the PMAG receives a forward request, then the PMAG forwards all the packets that are in the buffer. The buffering time is determined according to the maximum expected link layer handover delay which may be different from technology to another.

The approach in [16] presents a packet redundant elimination mechanism to prevent the re-transmission of the packets, that are successfully received at the mobile node and also stacked in the buffer, more than one time to the MN. This may happen because the exact disconnection time of the mobile node is unknown. The redundant packets can be known from the link layer re-transmission information, he packets that are received before the first re-transmission quitting event can be considered successfully received and can be dropped from the buffer. In addition, the packets with a maximum buffering time can be considered as redundant packets.

The approach in [16] introduces as well a MAG discovery mechanism. The NMAG attempts to discover the PMAG in order to retrieval the buffered packets. Two new messages are identified in [16] for MAG discovery scheme, Forward Request (FReq) and Forward Reply (FRep). The NMAG sends the acsFReq message which includes the MNID to all the MAGs and only the serving MAG replies with FRep. The FRep contains , number of buffered packets, average arrival packet rate and forwarding packet rate.

To perform the buffering mechanism, [16] also proposes a packet ordering mechanism to reorder the packets coming from the LMA and PMAG. The main idea here is to delay the packets that are coming from the LMA until all the packet be forwarded by the PMAG. The scheme in [16] has performed by simulation to test the effect of the smart buffering mechanism in reducing the packet loss.

Although the scheme presents a well-organized approach to eliminate the packet loss, but still does not present a solution in the case of high delay in the network. The PMAG discovery by the NMAG can increase significantly the hand over delay in PMIPv6.

2.5 MultiProtocol Label Switch protocol (MPLS)

2.5.1 MPLS overview

The ((MPLS) is a protocol that works with multiple network protocols like Internet Protocol (IP) ,Asynchronous Transfer Mode (ATM) and Frame Relay (FR) protocol. The MPLS 's techniques are applicable to any network layer protocol. The MPLS domain, is that domain which contains a set of nodes communicates between each other by using the MPLS routing and forwarding mechanisms.

The main entities inside MPLS domain as defined in [17]are the Label Edge Router (LER), the

Label Switch Router (LSR). The LER operates in the edges of MPLS domainand it may be ingress node (which handles traffic that enters the domain) or egress node (which handles traffic that leaves the domain) and it make the connection between the MPLS inside domain nodes with the others which are outside the domain and are not MPLS neighbors. The LSR on the other hand operates inside the domain and it is considered a LSR if only all its neighbors are routers operate in MPLS domain.

A new packet's header is added by the MPLS protocol , it is between the traditional data link layer's header and network layer's header, which belongs to layer 2.5. This layer is in between the network layer and data link layer. The MPLS protocol also extends its functionality from the ATM protocol with some expansion and modification for it. The main advantage of MPLS over the previous extension is the less operational overhead.

In IP routers, the forwarding decision for the IP packets is taken after looking up to destination IPaddress in the packet header and finding the best match in routing table. This inspection increases the complexity and adds some delay to the forwarding process.

In MPLS we have two plans, the data plan and the control plan. The data plan is the packet forwarding path through a router or a switch. The control plan is the set of protocols that helps in setting up the data plane.

The IP packet once enters the MPLS domain, a label is attached to this packet. This label is used as index in the forwarding table to indicate the next hop where a new label will be assigned. The intermediate LSR routers look up for this label and replace it with new label, which is assigned for the next hop. The MPLSheader format as specified in [17] is shown in figure 2.6.

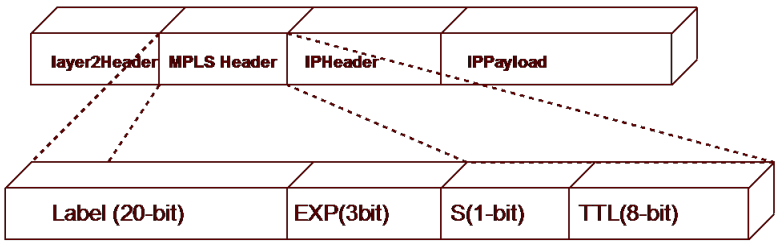

Figure 2.6: MPLS Header

(Label: 20 bit, EXP: Experimental, (QoS and ECN),S: Bottom-of-Stack and TTL: Time-to-Live)

In fact the packet does not carry only one single label but carries a group of labels. This group of labels is called a label stack which is defined in [17]. The label stack is organized by last-in first out mechanism and the processing is always based on the top label. Each LSR must perform label swapping to forward the packet.

A sequence of LSRs, that forward the labeled packet inside the MPLS domain, form the Label Switch Path (LSP). This path has ingress LSR which is the first point in the path and egress LSR which is the last point in that path. A group of forwarded packets that take the same path are called a Forwarding Equivalence Class (FEC). All the packets belong to the same FEC have the same label, but not all the packets have the same label must belong to the same FEC.

The Label Distribution Protocol (LDP) is one of the protocols responsible for organizing the label exchange between Label switch peer which are in this case the LSRs. There are some other protocols that can control the label distribution process like (MPLS-LDP), (MPLS-BGP),(MPLS-CR-LDP) and (RSVP-TE).

The LDP as defined in [18] is a set of procedures by which label switches routers establish the LSP through a network and map the network-layer routing information directly to data-link layer switched paths.

In the control plan in LDP protocol there are some tables that help in label distribution process. The LDP protocol starts with feeding the Label Information Base (LIB) table with label bindings then LIB feeds these label bindings to Label Forwarding Instance Base (LFIB) table. The LFIB table is that table forwards the labeled packets. Each LSR to perform its operation (swap, push, pop) must look at LFIB table. To exchange the label mapping messages all LSRs must establish a LDP session .

The LDP protocol associates the created LSP with the FEC, that specifies the shared path packets. In every LDP session both of the LDP peers exchange the label mapping in bidirectional way.

There are four types of LDP messages that can be exchanged between peers as defined in [18]:

- discovery messages which used for annunciation of existing in the network,
- session messages, used to establish, maintain, and terminate sessions between LDP peers,
- advertisement messages, used to create, change, and delete label mappings for FECs, and
- notification messages, used to provide advisory information and to signal error information.

The LDP protocol to have reliable connections uses Transmission Control Protocol (TCP) transport for session, advertisement and notification messages and uses User Datagram Protocol (UDP) session for discovery message, that is considered as a hello message.

In the case of having an error there are two types of messages, that the LDP uses:

1. Error Notifications, if this error is received by LSR, the later terminates the session and discarding all label mapping included in this session.
2. Advisory Notifications, which is used to identify the status of the session or the previous messages the peers had.

The MPLS architecture [17] specifies two ways of label distribution, on demand label distribution and unsolicited downstream label binding. In the on demand label distribution, the LSR requests a FEC label binding from anther LSR which upon this request distribute the FEC label binding. IN the unsolicited downstream label binding, the LSR distributes the label binding to anther LSR without any previous request. The LDP peers must be aware of the label distribution way that they are using between each other and this way must be the same under the same session.

The purpose of this overview is to explore the functionality of MPLS protocol. This functionality could help in improving the micro-mobility management inside the PMIPv6 domain by reducing the tunneling overhead. The next section discusses some of the related work for integration between the PMIPv6and MPLS in order to benefit from the MPLS low tunneling overhead in the PMIPv6 domain.

2.5.2 Related work for MPLS solution

The integration between the PMIPv6 and MPLS can be established by two ways as mentioned in [19], the integrated way and overlay way. In the overlay way the processes of the two protocol are separated without any merging. This in order can increase the complexity and overhead inside the domain. In integrated way the processes are shared between the two protocols, this can reduce the complexity and overhead results from the additional messages exchange to establish the communication between different processes.

The relationship between binding updates and LSPs setup is classified in [19]in two ways, the sequential way and the encapsulated way. In an encapsulated way the LSP setup is in the time before receiving the PBU message at the LMA and the time after sending the PBA message to the MAG. In the other hand the sequential way, the LSP setup is after the full binding update between the MAG and the LMA is completed.

The first approach regarding the integration between PMIPv6 and MPLS is in [20]. This draft proposes the replacement of (IP-in-IP) tunneling by MPLS tunneling in PMIPv6 domain.

The main idea is to convert the core entities in the PMIPv6 domain into LER as shown in figure 2.7. These entities perform the mobility-related signaling exchange in MPLS domain. The forwarding techniques in MPLS protocol is established by the label replacement and exchange between the LSRs as mentioned above.

The draft proposes the usage of two kinds of labels to allow the communication between MAGs and LMAs, a classical tunnel label and Virtual Pipe (VP) label. The VP labeling is used to differentiate the traffic coming to the LMA from different mobile nodes served by the same MAG.

In [20] MAG sends a Proxy Binding Update message to the LMA using the VP Label. The LMA assigns this VP label as the downstream label and put it in the binding cache Entry.

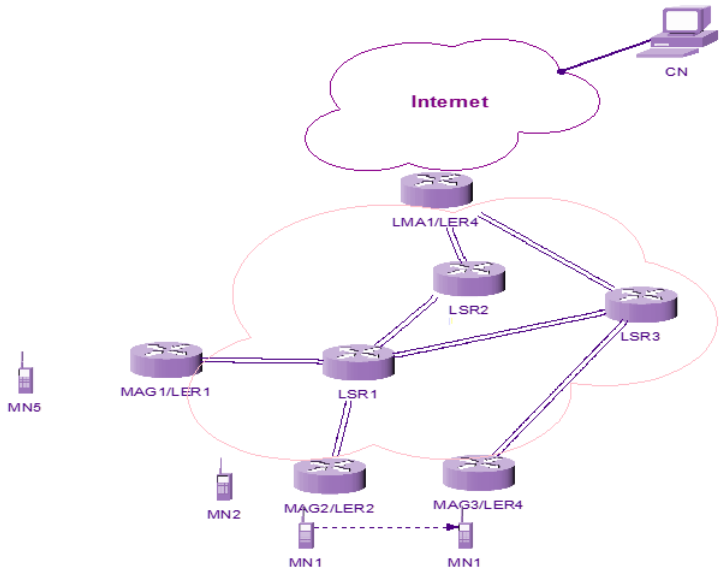

Figure 2.7: PMIPV6/MPLS domain

Once an IP packet, which sent to the MN, arrives at the LMA, it locates a binding update list entry based on MN IP address, fetches the downstream VP label, identifies the tunnel label based on its IP address ,encapsulates the packet with two layers label and sends it out according to [17].

The LMA then identifies the tunnel label based on the address of the serving MAG, which in sequence, pops the tunnel label ,strips the VP label and forwards the packets to the MN.

There approaches in [21],[22] have discussed the integration between the PMIPv6 and MPLS. In [21] the approach presents a study of the integration in wireless mesh network. The LSP is set up by RSVP-TE protocol with exchanges of PATH/RESV messages.

In [21] the technology used for wireless link is IEEE 802.11 access network. In this approach integration established with overlay way and the LSPs setup in sequential way. The approach also assigns two ways to set up the LSPs, the pre-established or dynamically assigned way.

In [21]the mobile node only IPv6 but the transport network can be both acsIPv4 and IPv6. The penultimate hop popping is used to avoid double processing in the last hop. An optimized sequential way is used in this approach for LSP's setup to achieve good performance in the case of the increasing in the number of hops.

The MPLS functionality of forwarding the packets can reduce significantly the handover overload. Using the labels to forward the packet can give a great result with the existence of a huge number of mobile nodes in the domain. These mobile nodes are served in the same the time and this causes a huge number of mobility-signaling exchange inside the domain. Also increasing the number of intermediate points in the core of the network can result in increasing the handover overhead but with using MPLS it is expected in this case that the overhead can be manageable regarding the usage of label forwarding. Also the fast forwarding techniques of the MPLS protocol can help in reducing the handover time delay in the PMIPv6 domain.

3

Architecture

Contents

3.1 Introduction

This chapter introduces the architecture of, PMIPv6 protocol, the authentication procedures modification and the buffering mechanism optimization. The chapter starts with general architecture overview of the PMIPv6 protocol followed by exploring the detailed architecture for the proposed enhancement for this protocol.

3.2 Proxy mobile IPv6 architecture

3.2.1 PMIPv6 Hardware architecture

The PMIPv6 domain contains two types of entities, core functional entities and users functional entities. The core functional entities are the LMA and the MAG, these entities are serving inside the domain and considered the main responsible for all mobility-related signaling performed in the PMIPv6 domain. The user entities are presented in MN and Correspondent Node (CN), which are not involved in any kind of mobility-related signaling in the domain and their main responsibility is sending or receiving data. As shown in figure 3.1 a general architecture for PMIPv6 system which consists of centralized LMA, serving MAGs, MN and CN.

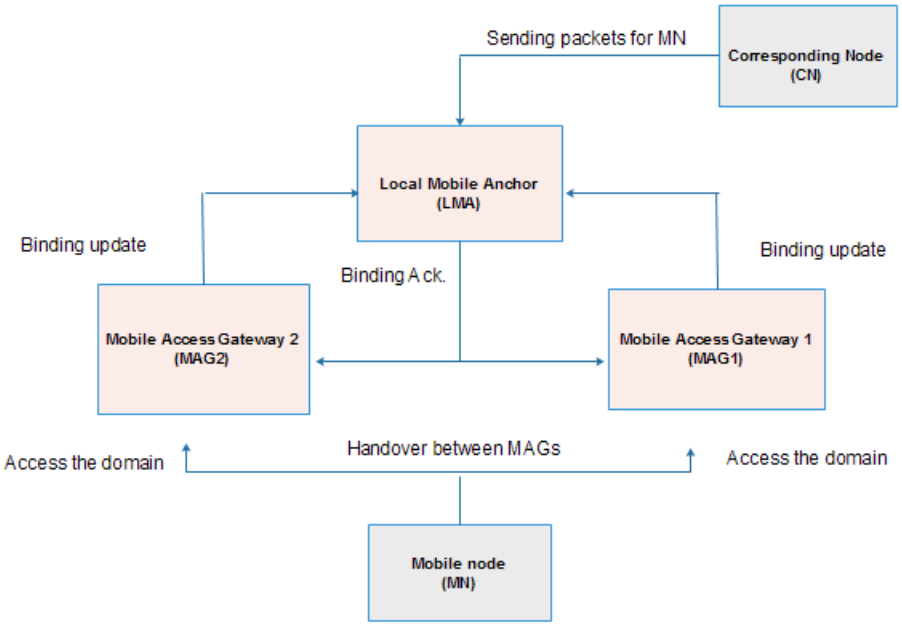

Figure 3.1: PMIPV6 architecture

The centralized LMA acts as local anchor point for the MN, it is equivalent to home agent in MIPv6, and its main functions are shown in figure 3.2. The functions of LMA entity begin with receiving the binding updates of the MN from the serving MAG. This update is presented in PBU message, then the LMA checks the polices for the mobile node and if it is authorized to use the proxy services in the domain. The LMA then creates cache entry for this MN contains, the MNID and the address of serving MAG. this message is important for the LMA in order to be aware of the MN location during the

movement in the domain. The LMA also sends a PBA message with the network prefix(es)assigned uniquely for this MN. Finally the LMA routes the traffic goes into or from the mobile node, this traffic can be internal traffic or external one. the internal traffic comes from mobile node connected to MAG inside the PMIPv6 domain or external traffic comes from outside the PMIPv6 domain.

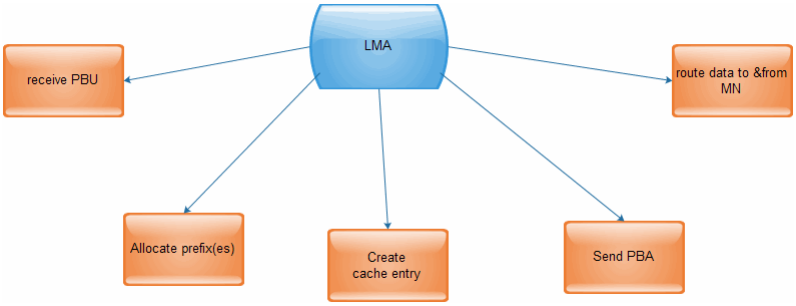

Figure 3.2: LMA functionalities

The MAG entity acts as a media access gateway, this is a new entity, has been added to PMIPv6, responsible for exchange the signaling on behalf of the mobile node within its movement inside the domain. the functions for MAG entity as shown in figure 3.3 can be summarized in, receives MN's solicitation, interacts to MN's policy profile, sends PBU, receives PBA, updates b-cache, creates a shared tunnel with LMA, manages a temporary b-cache and sends router advertisement to the MN.

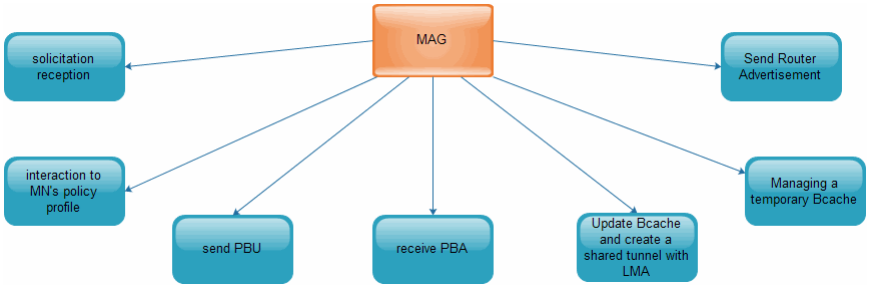

Figure 3.3: MAG functionalities

The MN in PMIPv6 is not involved in any kind of mobility -related signaling exchange and its functions is shown in figure 3.4. The MN, sends router solicitation to the nearest point of attachment, receives router advertisement and auto-configures its IPv6 address according to the network prefix(es)sent from the LMA entity.

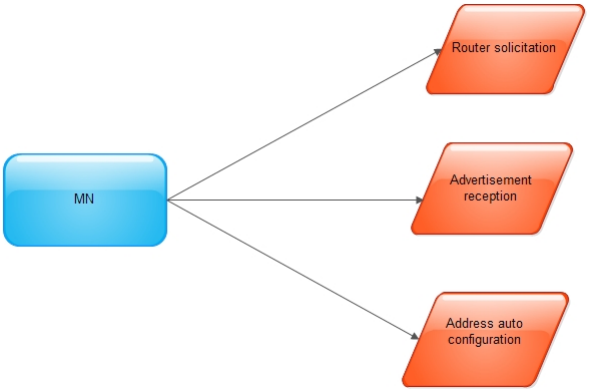

Figure 3.4: MN functionalities

3.2.2 PMIPv6 Software architecture

As shown in figure 3.5 the PMIPv6 implementation [23] is based on the USAGI-patched Mobile IPv6 for Linux (UMIP), which is an open source implementation for MIPv6 developed by the cooperation of GOCORE at Helsinki University of Technology and the USAGI/WIDE group [24]. The UMIP software architecture is divided into two different spaces the kernel space and user land space.

The main libraries that have been used from UMIP implementation are Tunnel ctl for handling the IP-in-IP tunneling , routing filter with INETLINK to deal with routing tables in IP stacks, task queue, mobility header and NDPv6.

Some additional libraries have been added to make the MIPv6 works according to proxy mobile IPv6 specification such as finite state machine, handler, PMIPv6 cache and messages.

These four libraries work in user space, the finite state machine considered the heart of this space and it controls all the other elements to provide a correct predefined protocol behavior. All the information about the MN is stored in PMIPv6 cache. It keeps all the updates about the location, the connected access point and the serving MAG address. The handler handles all the messages and event inside the domain, all the messages are parsed and provides as an input for the finite state machine, which makes appropriate decision for each different situation.

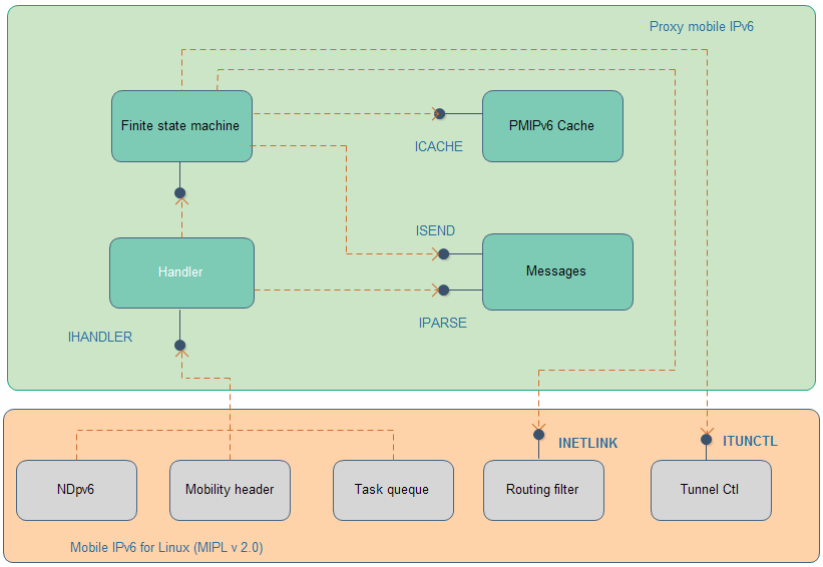

Figure 3.5: PMIPv6 software architecture

3.3 The proposed enhancement architecture

3.3.1 The authentication procedure modification

One the component of handover time delay is the authentication delay, the mobile node once enters the domain, the first MAG performs the authentication procedures.

These procedures are necessary to check the authorization of the MN for network-based mobility service. The MAG sends an authentication request to AAA server, which in order checks its cache entry for the mobile node policy.

The mobile node identifier in this case, is the mobile node's MAC address. After the AAA server finishes the authentication check, it sends either acceptance response or rejection response. In acceptance case the MAG starts directly the binding update step. The protocol that is used to perform the authentication procedures is the RADIUS protocol.

The authentication time delay is repeated every time the MN moves to a new MAG in the domain. The proposed modification attempts to reduce this delay by shortening the authentication's procedure to occur only in the entry of the MN to the PMIPv6domain.

As shown in figure 3.6 the MN once connects to the MAG, the normal procedures are performed by sending the authentication request and waiting for a response from the LMA.

The LMA sends a unicast response to the serving MAG and in sequence sends a copy of that response to all the MAGs that are serving in the domain. This message contains, MNID, the MN authorization response.

All MAGs after receiving this response from the LMA, cache this information in a specific entry for this mobile node. The next time the mobile node attempts to connect to any NMAG after the handover process. This NMAG does not send a new authentication request directly, instead it searches in its cache for this MN. if the MN exist in local cache, the MAG sends binding update directly to the LMA.

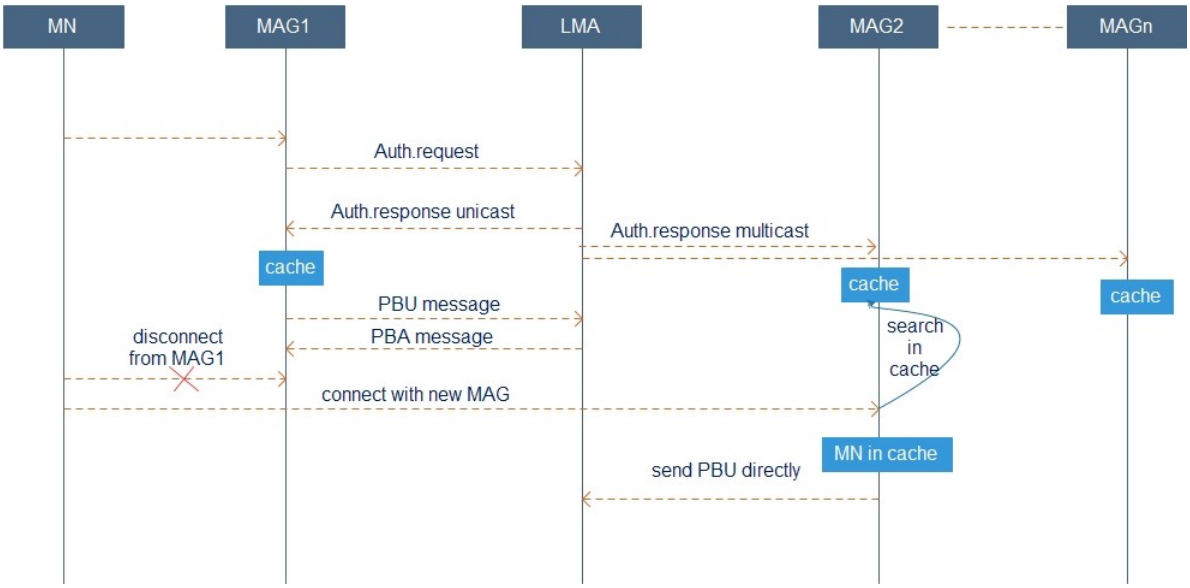

Figure 3.6: First solution signaling flow

3.4 The buffering mechanism optimization

The specification for PMIPv6 has not specified any buffering mechanism for the protocol to eliminate the packet loss during the handover process. The proposals in [15], [16], present a buffering mechanism to be applied in the PMIPv6 protocol.

The implementation in [25] is based on the open source implementation in [23] for PMIPv6 protocol. There are some additional libraries to apply the buffering mechanism, that have been added in [25]. The LMA is the entity that contains the buffer and performs the buffering mechanism in PMIPv6 domain.

The buffering mechanism as described in [15] has functionality in two plans, the kernel plan and user plan. In the kernel space the packets are hooked and then are passed to user space. The desired packets are referred by the netfilter libraries [26]. Firstly the packets are hooked at routing hook point in the netfilter then the packet are passed to the user space by IP6 queue module. The packet are sent to the user space and they are stored in the buffer with the Libipq library. The IP tables tool performs the packets pushing and popping to or into the buffer respectively. This pushing and popping happens by using the Listening thread and a (re-inject Thread).

The buffering mechanism software architecture is shown in figure 3.7. This mechsnism is based on the proposal in [15].

The packet buffering mechanism in [15] is implemented only in LMA entity. The results that are reported in [15] indicate the improvement of packet loss elimination in the PMIPv6. The solution in[15] has not presented a solution for the increase of the number of mobile nodes connected with the same LMA entity. Also the case with a high network latency or disconnection in the path between MAG and LMA or any changing in the (de-registration) message's path that can causes a loss of a big amount of packets at the MAG side. These packets can be dropped if there is no buffer at MAG entity.

The buffering mechanism optimization, that is proposed by this thesis work, focuses on the case

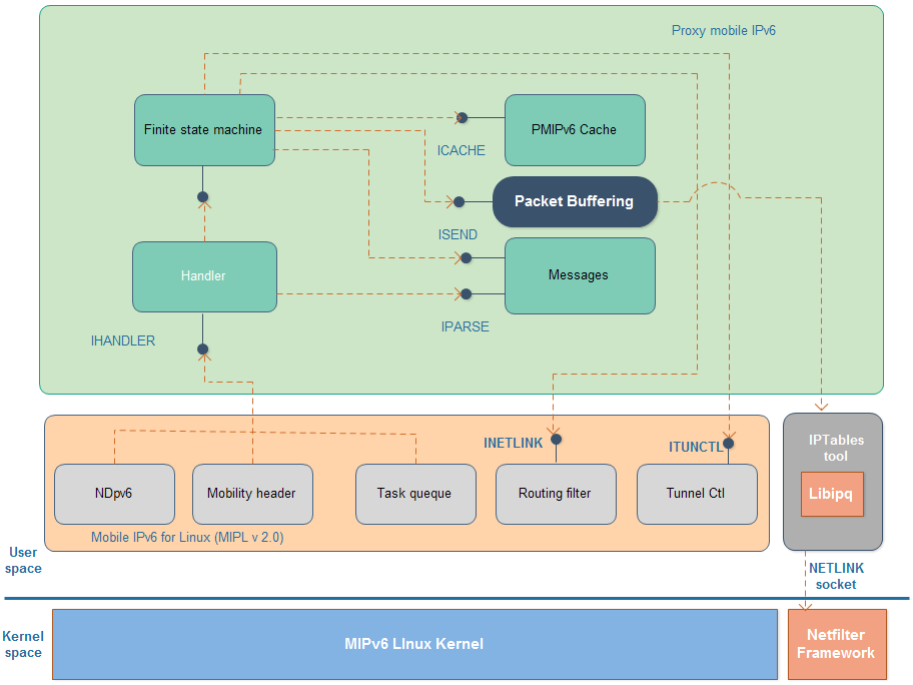

Figure 3.7: Buffering mechanism software architecture

when there is high latency in the network and presents a modification to the proposal in[15]. this optimization attempts to eliminate the packet loss in the case of high binding latency. Also it attempts to make some balance in the network by distributing the buffering mechanism between the serving MAGs instead of centralizing the buffering mechanism in only LMA entity.

The buffering mechanism optimization measures the number of packets that arrive at the MAG in the time between the mobile node is already disconnected and the LMA is not able to receive the (de-registration) message to start the packet buffering mechanism.

The mechanism operation as shown in figure3.7 starts with receiving a sequence of packets that pass through the LMA entity in its way to the MN. The MAG starts the buffering mechanism directly after receiving the disconnection event message from the mobile node.

The MAG updates the (de-registration) of the MN to the LMA. The tunnel between the PMAG and LMA in this case is not deleted by LMA as in the usual case of PMIPv6 operation, as previously mentioned. The LMA keeps the tunnel until it receives a new registration message from the NMAG. At this step the LMA sends a FReq message to the PMAG to forward the packet that in this MAG's buffer and changes the route of the packets to the NMAG. The PMAG forwards the packet and sends a FRep message to the LMA. The NMAG recives the new packets from the LMA and the old packets from the PMAG. The NMAG then reorders the packets with sorting function and forwards the all packets to the MN. The evaluation of this optimization and the results are covered in chapter 5.

4

Implementation

Contents

4.1 Introduction

This chapter presents the implementation of the test bed of the PMIPv6 and the proposed modification for the improvement in the protocol. The chapter focuses on the implementation and configuration of the main protocol entities. It starts with the implementation of the PMIPv6 as it is considered the basis for the whole work and follows by the implementation of the authentication procedures modification and finally the implementation of buffering mechanism optimization.

4.2 Proxy mobile IPv6 implementation

4.2.1 Network installation

The implementation of the PMIPv6 test bed is based on open air group Implementation [23] for PMIPv6. The system consist of five entities as shown in figure 4.1 LMA, MAG1, MAG2, CN and MN.

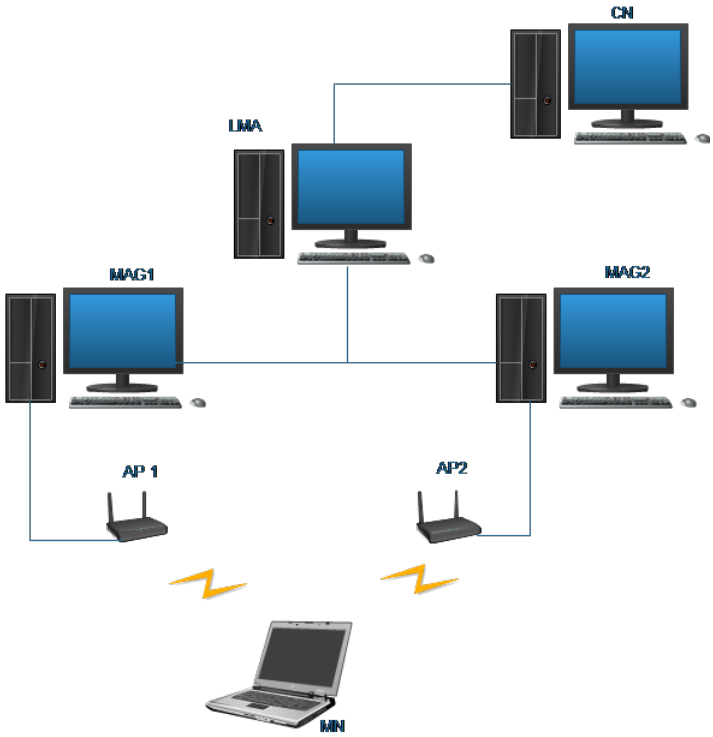

Figure 4.1: PMIPv6 testbed

4.2.1.A The configuration for the network entities

The configuration for each entity is explored separately in order to give more details about the requirements for each entity and how generally the system works. Most of the details here are taken from the documentation file in [23] which is the guide for PMIPv6 implementation.

The LMA as a centralized anchor for the mobile node it should contain special configuration and the configuration steps can be summarized as following:

1. Kernel Compilation, this step is necessary for the kernel preparation to be able to operate with mobility functions and all the kernel recompilation steps are shown in table A.1
2. Installation of FreeRADIUS server, which is an open source project [27], and is used as AAA authentication server. This server helps in testing the authentication of the mobile node in PMIPv6 domain.
3. The configuration files, there are three important configuration files need to be modified in order to make the server work in a right way, users file ,radiusd.conf file and clients.conf file.
4. Installation of FreeRadius Client, the free Radius client is installed on LMA machine.

The steps required for configuring the MAG machine are shown on table A.1 and can be summarized as following:

1. Kernel completion, which is similar to the kernel completion for LMA machine.
2. Syslog Server installation, to detect the attachment of the mobile node there is need to have syslog server /client installation between the MAG and the access point connected together in the same link. The access point contains syslog client which updates the log events for the mobile node with a message contains the MNID. The MAG parses the MNID and starts the authentication procedure after this parsing.
3. FreeRadius client installation, the same installation as acsLMA machine.
4. PMIPv6 Compilation, the same installation as LMA machine.

The installation procedures PMIPv6 is installed on the Ubuntu system and ready to be tested and evaluated. The evaluation of the system is covered in chapter 5

4.3 Authentication procedures modification implementation

The first modification concerns with reducing the hand over delay in the attachment event of the mobile node. The idea here is to eliminate the time consumed in the authentication process every time the mobile node changes its point of attachment.

The authentication procedures can be summarized as following:

1. The FreeRADIUS client which in this case is the MAG, after parsing the MNID sends a Radius request to the RADIUS server to check the authentication condition for that mobile node.
2. When this request arrives at the server, the server first checks if the MAG is an authorized client or not by searching in Client.conf file and if the client exist it moves to the next stage.
3. The next stage starts with searching in users file and if the mobile node exists the radius server responds with RADIUS accept.

These procedures take place every time the mobile node moves from a point of attachment to another and if the network contains delay this can resulting in a dramatic increase in the mobile node handover time delay. The proposed solution attempts to overcome the authentication overhead during the handover process by distributing the authentication response to all MAG nodes within the network. Each MAG stores this response in its local cache so that on the incidence of mobile node changing the point of attachment, the new point of attachment already has the authentication information. In such a case the new point of attachment skips the authentication procedure thus getting rid of the authentication overhead.

In order to achieve this, the following changes must be added to both LMA and MAG nodes:

- the LMA should send the authentication response to all MAG nodes within the network not only the current point of attachment, and
- each MAG nodes should wait all the time for authentication responses from the LMA regarding the mobile nodes that have not yet handled, and add this response to its local cache.

The following section shows the pseudo code for the implementation of the first solution and the changes that are made to the LMA and the MAG entities in order to apply the solution are shown in algorithm 1, algorithm 2.

4.3.1 Changes to LMA

The Changes here are implemented in the FreeRADIUS server in order to send the authentication response to all the serving MAGs that are connected to the PMIPv6 domain. The pseudo code is shown in algorithm 1.

Algorithm 1 Changes to the LMA

```
function HANDLINGNEWMN(MN)
    Response ← AUTHENICATEMN(MN)
    SENDTO(MN.AP, Response)          ▷ Sends the authentication response to the mobile node attachment point
    MAGs ← GETALLCONNECTEDMAGS(config)          ▷ Get all the MAG nodes within the network
    MAG.LP ← GETMAGLISTENINGPORT(config)
    for all MAG in MAGs do
        if MAG ≠ MN.AP then
            SENDTO(MAG, Response, MAG.LP)
        end if
    end for
end function
```

4.3.2 Changes to MAG

The changes here are made to the MAG client in order to make the MAGs entities ready to receive the authentication response and add content of this response in the local cache. The pseudo code is shown in algorithm 2.

Algorithm 2 Changes to the MAG

```
function INIT                          ▷ code that is executed when the MAG node is initiated
    STARTNEWTHREAD(AuthRespListener)          ▷ fork a new thread for the listener that will be receiving authentication responses
    AUTHRESPLISTENER                          ▷ listener function forked in a single thread
    MAG.LP ← GETMAGLISTENINGPORT(config)
    socket ← OPENSOCKET(MAG.LP)
    while True do
        msg ← RECEIVEDATA(socket)
        HANDLERESPONSE(msg)
    end while
end function
function HANDLERESPONSE(msg)
    data ← PARSE(msg)
    MN ← data.MN
    resp ← data.resp
    INSERTINTOCACHE(MN, resp)
end function
function INSERTINTOCACHE(MN, resp)
    if MN not in cache then
        CACHE.CREATEENTRY(MN, resp)
    else
        CACHEUPDATEENTRY(MN, resp)
    end if
end function
```

4.4 Buffering mechanism optimization implementation

The second enhancement in this thesis 's work is implemented to reduce the packet loss during the handover delay time. In the handover time period the mobile node is disconnected from the serving MAG and tries to connect to anther MAG within the new location. The serving MAG detects this disconnection of the mobile node with an event message coming from the connected Access AP.

The network latency between the PMIPv6 domain entities can cause a significant amount of packet loss especially with the increase in the handover time delay. The increasing number of mobile node can cause overload in the LMA buffer so it may present a point of failure in the domain.

For all these considerations there is a need for buffering mechanism at the MAG entity. This buffering mechanism should start in that critical time and store all the received packets belong to the mobile node till the end of the handover process. The LMA after the handover process is finished receives the binding updates from the NMAG contains the new location of the mobile node. The LMA then gives the order to the PMAG to forward all the packets stored in the buffer. This solution attempts to make balance in the network and moves the buffering function from the LMA to MAGs in the domain.

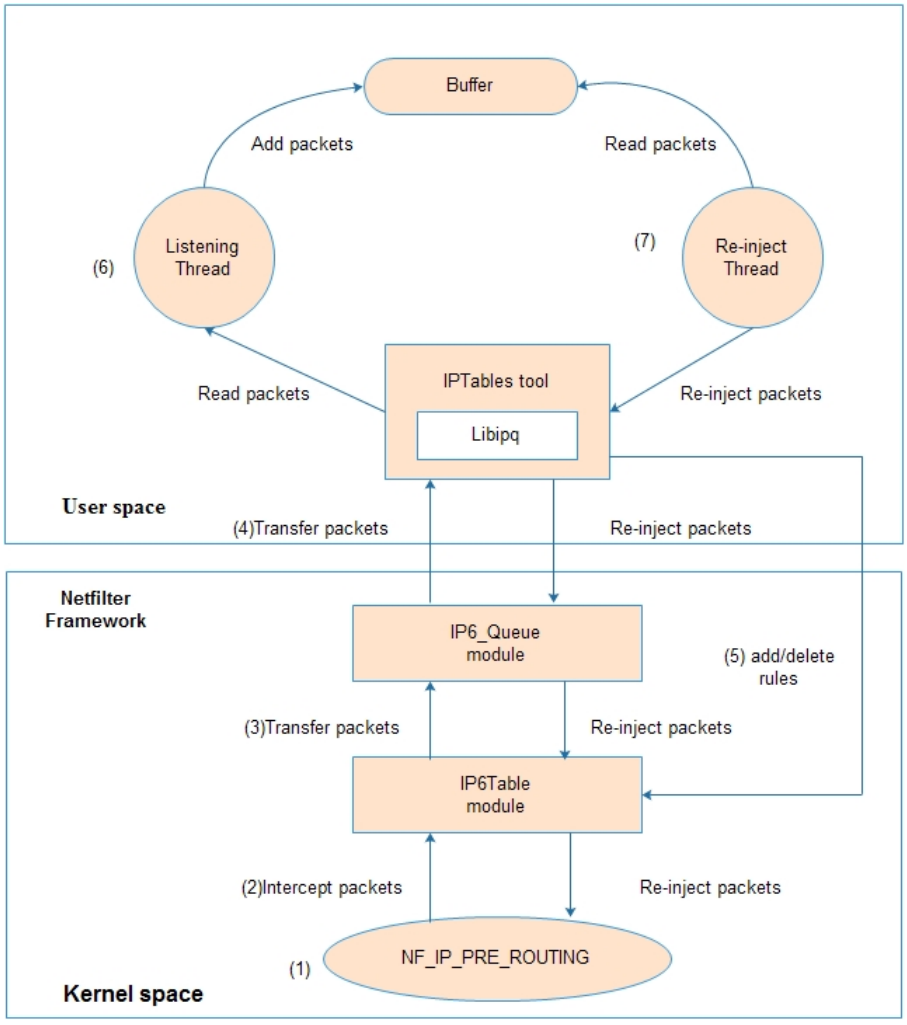

Figure 4.2: Buffering mechanism data flow

The implementation for the additional functions has the following steps:

1. The implementation starts with creating a buffer at MAG entity, the buffer should related with two factors, the handover time delay and the expected packet number in this period. The buffer size is limited with specific period of time which is the maximum handover time delay in the domain.
2. The second step is the modification in LMA entity to send the forwarding message contains the NMAG address.
3. The third step is the reordering function at MAG2 to arrange the packets coming from the LMA and the PMAG.

Figure 4.3 shows The sequence flow of signaling.

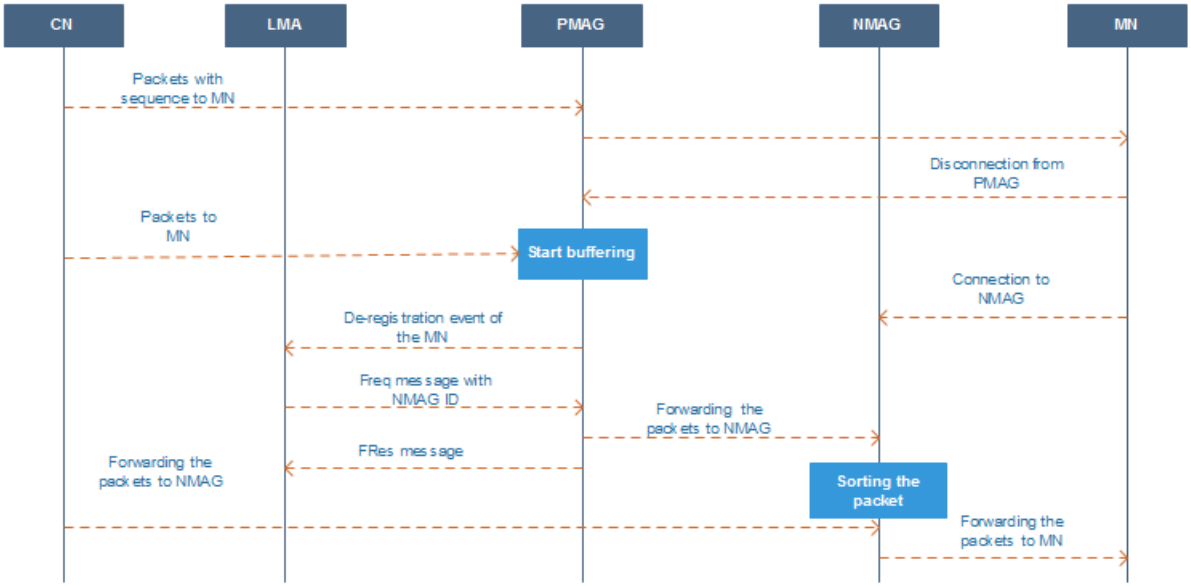

Figure 4.3: Second solution sequence flow

4.4.1 Changes to LMA

The changes here are implemented in order to modify the function of the LMA. The LMA should create sequence number for each MN and the serving MAG in this time. The LMA once receives a new registration message sends a forward message for the PMAG to forward the packets it buffers for that mobile node. The pseudo code for this modification is shown in algorithm 3.

Algorithm 3 Changes to the LMA

```
function RECEIVEPACKETATLMA(packet)
    mnAddr ← packet.dest
    servingMAG ← ROUTINGTABLE.FIND(mnAddr)
    packet.sqNumber ← GENERATOR.NEXTNUMBER(mnAddr)  ▷ generates sequential numbers for
each MN
    SENDTO(servingMAG, packet)
end function
function RECEIVECONNECTIONATLMA(mnAddr)
    currentMAG ← ROUTINGTABLE.FIND(mnAddr)
    SENDNEWLOCATION(currentMAG, newAddrMAG)
end function
```

4.4.2 Changes to current MAG

The changes here are implemented in order to make the current MAG, which is in this case the (PMAG), entity be able to perform the buffering optimization. The MAG in this case once receives an detachment event message from the MN, it initializes the buffer to store the packets until it receives the forward message from the LMA. The PMAG then forwards the packets in the buffer to the NMAG address. The pseudo code is shown in algorithm 4.

Algorithm 4 Changes to the current MAG

```
function RECEIVEPACKETATMAG(packet)
    SENDCONNECTONTOLMA(addrLMA, mnAddr)
    mnAddr ← packet.dest

    if mnAddr is connected then
        SENDTO(mnAddr, packet)

    else
        BUFFERMAG.INSERT(packet)

    end if
end function
function RECEIVENEWLOCATIONATMAG(newAddrMAG)

    while bufferMAG is not Empty do
        packet ←BUFFERMAG.POP
        SENDTO(newAddrMAG, packet)

    end while
end function
```

4.4.3 Changes to new MAG

The changes here are implemented in order to make the NMAG entity perform the second solution. The NMAG in this case sends the registration for the MN to the LMA entity. The pseudo code for this modification is shown in algorithm 5.

Algorithm 5 Changes to the new MAG

```
function RECEIVECONNECTIONATMAG(mnAddr)
    SENDCONNECTONTOLMA(addrLMA, mnAddr)
end function
```

5

Evaluation tests

Contents

5.1 Introduction

This chapter explores all the tests that have been done during the thesis work, starting from the implementation of PMIPv6 and ending with the evaluation of the proposed enhancements that are added to the PMIPv6 implementation.

5.1.1 Evaluation objectives

The main goals from the tests that have been done during the work, are the analysis and the evaluation of the PMIPv6's behavior in real scenarios. This evaluation aims to give a good understanding of the limitations that are in the PMIPv6 protocol namely, the handover delay, packet loss during the handover process and the handover overhead.

The evaluation tests have been performed in two main steps. The first step is the evaluation of the PMIPv6 protocol without any modification. The second step is the evaluation of the proposed enhancement to check the ability of these modifications to transcend the limitations of the PMIPv6 protocol.

5.1.2 Evaluation environment

The PMIPv6 test-bed setup is based on open air group implementation [23] for PMIPv6. The test set up consists of five entities as shown in figure 5.1 LMA, MAG1, MAG2, CN and MN.

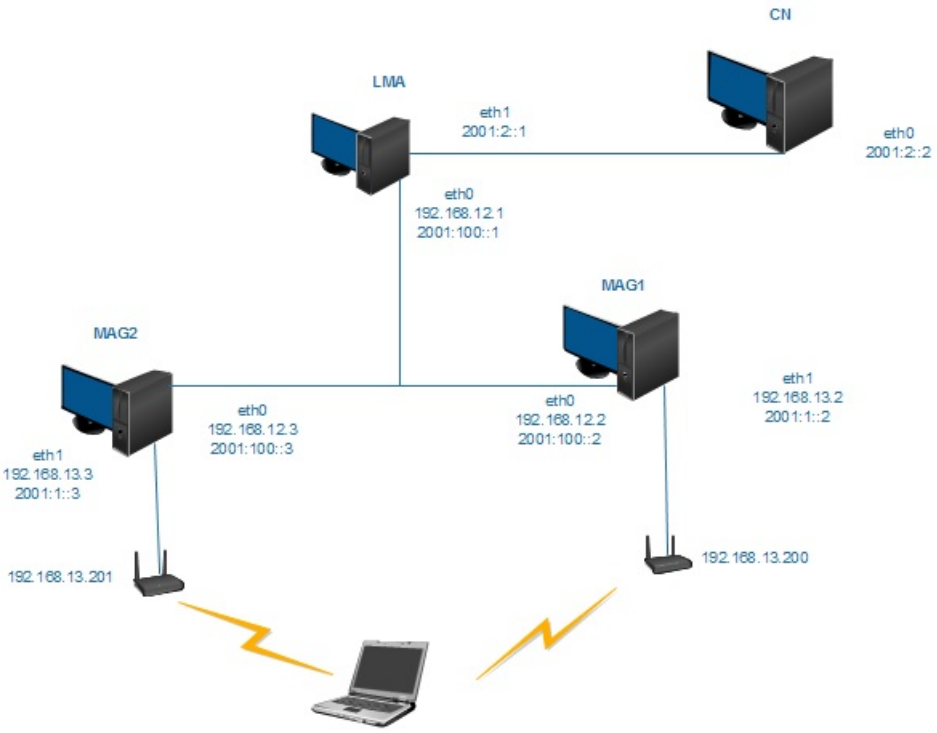

Figure 5.1: PMIPv6 network

The network consists of, LMA, MAG1 and MAG2 which present the core functional entities in the PMIPv6domain. Each one of these entities has, two network interfaces, eth0 and eth1. The

three entities are connected together by a switch in the middle point. This connection is through the interface eth0 in each machine. The network prefix for this network is 2001:100::/64.

The other interface in each machine connects to anther network as follows:

- the LMA connects to the CN with direct connection in a network with prefix 2001:2::/64,
- the MAG1 connects to the AP1 with a direct connection with interface (eth1) using IPv4 address (192.168.13.0), and
- the MAG2 connects to AP2 with a direct connection with interface eth1 using IPv4 address (192.168.13.0).

Ubuntu system version 10.04 with kernel 2.26.35 as recommended in[23], is used on all the network entities and the features of the test-bed's machines are shown on table 5.1.

Component	CPU	RAM	OS	SW	AP
LMA	Pentium 2.8GHz	1GB	Linux Kernel 2.6.32	FreeRadius Server FreeRadius Client PMIP6D configuration	
MAG1 MAG2	Pentium 2.8GHz	1GB	Linux Kernel 2.6.32	FreeRadius Client PMIP6D configuration	Microtech 4 Ports
MN	Core i5 2.4GHz	4GB	Linux Kernel 2.6.32		
CN	Pentium 2.8GHz	1GB	Linux Kernel 2.6.32		

Table 5.1: Description of the test bed nodes

5.2 Evaluation tests

5.2.1 Proxy mobile IPv6 evaluation test

5.2.1.A Access time delay evaluation tests

The handover delay in PMIPv6 can be divided into four different components. The first component is the layer 2 time delay, which occurs at the entry of the mobile node to the domain. This component of delay as in [11], consists of three phases, the scanning phase, the authentication phase and the association phase.

The second component consists of the authentication procedures time delay, that are performed by the network entities. The MAG after the detection of the MN, sends an authentication request to AAA server to check the authorization of the mobile node to be served inside the PMIPv6 domain. The protocol that is used in this procedure is RADIUS protocol. The time delay in this case is calculated by the time period between the sending time of the authentication request to the receiving time of authentication reply. This reply could be an acceptance or a rejection message. figure 5.2 shows the captured packets for the RADIUS protocol, the request is sent by MAG2 with address (2001:100::3)to the LMA entity with address (2001:100::1).

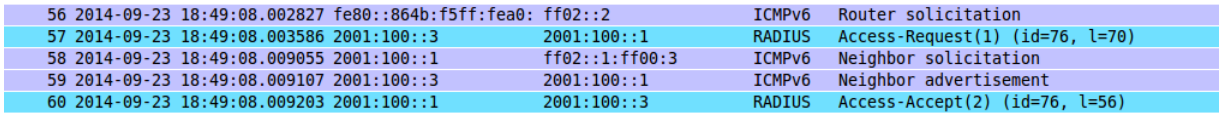

Figure 5.2: Radius Authentication

The third component is the binding time delay, during this time the serving MAG sends a periodically proxy binding update message to the LMA. This message is necessary for the LMA to determine the current location of the mobile node in order to route the data into or from this mobile node in its location. The time delay calculated between the time the MAG sends the PBU message and the time it receives the PBA message. This time delay depends on the RTT between the MAG and the LMA. Figure 5.3 shows the captured packets for binding updates that are sent periodically from the serving MAG to LMA.

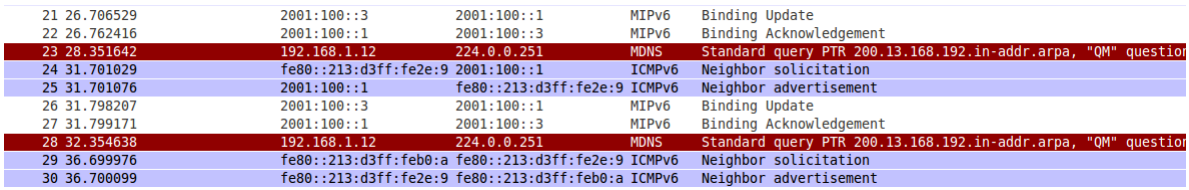

Figure 5.3: Binding Updates

The fourth and last component is the time taken to set up the tunnel, sending the router advertisement and the address (auto-configuration) for the mobile node. This tunnel is used to pass the traffic into or from the mobile node, it is a bidirectional tunnel installed between MAG and LMA. The time delay of the address (auto-configuration) for the mobile node occurs once when the mobile attached to the PMIPv6 domain.

The mobile node keeps this address during the movement and changing the point of attachment inside the domain. The time in this case can be calculated by adding these three periods, the time for tunnel set up, the time for sending the router advertisement, the address (auto-configuration) time delay.

The evaluation tests were run 10 times to obtain average results under some specific steps. The first step is to calculate the delay in PMIPv6domain within the first entry of the mobile node. The time delay is divided into the following components:

1. T_{L2} ,which is the layer 2 time delay and consists of three components, T_{wlan} , T_{ap-mag} and T_{ra}. T_{wlan} is the layer 2 Wireless LAN technology delay which consists of three phases, the scanning phase, the authentication phase and the association phase.

   T_{MN-MAG} is the time for packet transmission between the MN and the MAG entity.

   T_{ra} is the router advertisement time delay, which is sent by the MAG to the MN. The layer 2 time delay can be calculated as shown in equation5.1.

$$T_{L2} = T_{wlan} + T_{MN-MAG} + T_{ra} \tag{5.1}$$

2. T_{AAA} time delay of access authentication, this is a major step to determine if the mobile node is authorized to be in proxy mobility services or not. This time delay consists of two components $T_{Auth-request}$ and $T_{Auth-response}$. It can be calculated as shown in5.2.

$$T_{AAA} = T_{AuthRequest} + T_{AuthResponse} \tag{5.2}$$

3. $T_{Binding}$ is the time delay to send and receive the binding updates and binding acknowledgment between MAG and LMA. This time delay consists of T_{PBU} and T_{PBA}.

$$T_{Binding} = T_{PBU} + T_{PBA} \tag{5.3}$$

4. $T_{address}$ is the time to $(auto-configure)$ the IPv6 address for the mobile node. This time starts at the time of receiving the router advertisement message from the serving MAG and ends at the time when the MN can establish a communication with CN by using the new configured address.

5. T_{core} is the time between receiving the syslog message at MAG and the time of sending the router advertisement to the mobile node. This time consists of T_{AAA} ,$T_{Binding}$ and time of exchange core message.

$$T_{Total-delay} = T_{core} + T_{L2} + T_{address} \tag{5.4}$$

Figure 5.4 shows the total delay from the time of MN's access to the domain to the time when the MN is able to send packets to CN using the configured IPv6 address. The total access delay is about 3.70 s.

Test sequence \ Time (ms)	T_{MN-MAG}	$T_{address}$	T_{core}
1	1.832	2208.400	1421.001
2	1.303	2210.000	1459.847
3	1.480	2350.900	1299.100
4	1.335	2001.884	1389.770
5	1.320	2109.875	1489.235
6	1.640	2211.023	1311.000
7	1.258	2218.000	1375.210
8	1.359	2217.687	1572.874
9	1.685	2198.654	1487.745
10	1.2549	2097.521	1438.698
avarage	1.446	2173.813	1421.238

Table 5.2: Access time delay

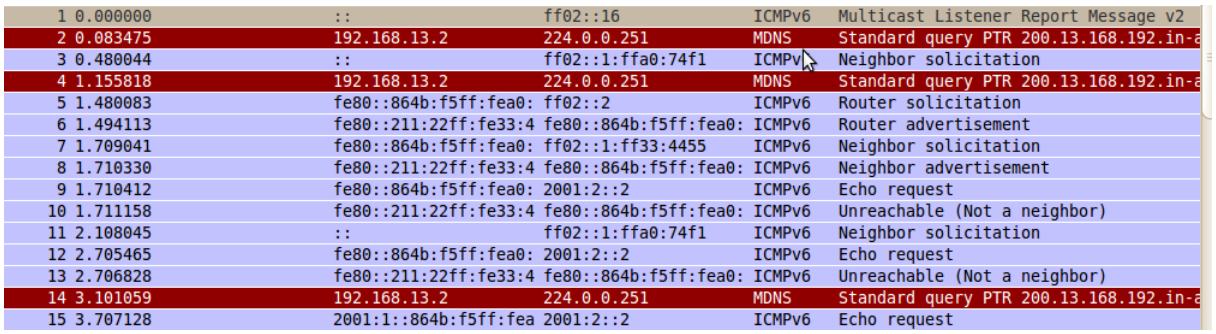

Figure 5.4: Mobile node access delay

The average value for the total delay is calculated as in equation 5.4 $T_{Total-delay}$ = 1421.238 + 1.446 + 2173.813 = 3596.497 (ms). The results state that the average value for the mobile node access delay is nearly 3.596 s

5.2.1.B Handover delay evaluation tests in proxy mobile IPv6

The test has been done by using ping6 command to send and receive packets between the MN and CN. This test is setup to measure the delay and packet loss in handover period. The MN in this scenario firstly, connects to MAG1 and then starts to send a specific number of packets to CN. The MN then disconnects from MAG1's access link and connects to MAG2's access link while keep sending the packets to CN. The detachment of the mobile node occurs as follows:

1. The previous point of attachment, the AP associated with MAG1, sends a syslog message with a disconnect event.

2. The MAG1 starts a (de-registration) process for the mobile node by sending a PBU message to LMA. This message contains the detachment event of the mobile node and can be considered in this case a (de-registration) request.

3. The LMA receives the message and recognizes that the mobile node is disconnected. The LMA waits for a specific period of time for a new registration message regarding this MN. If this period

goes more the pre-defined period then it deletes the cache entry for this MN.

4. If the LMA receives the PBU message from the NMAG, it keeps the cache entry and reply with the PBA message includes the network prefix of the mobile node.

5. The mobile node connects to the new MAG and continues to send the packets to CN.

The handover time delayis calculated as equation 5.4.

The test was run 10 times to get an average value for both the time delay and packet loss. Table 5.3 shows all the results in the 10 times.

Time Delay	3.840	3.980	3.792	3.690	3.670	3.780	3.570	3.993	3.527	3.534	Average 3.894
Packet loss %	13	14	15	14	13	12	15	16	11	13	Average 14

Table 5.3: handover time delay and the packet loss

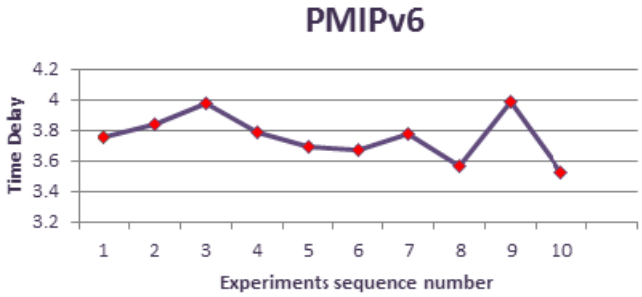

Figure 5.5: Handover time delay

The purpose of these calculations is not just measure the total time delay during the handover process but also the packet loss occurs during this period as shown in figure 5.6. The packet loss test was setup by using ping6 command in order to measure the percentage of the loss during the handover time delay.

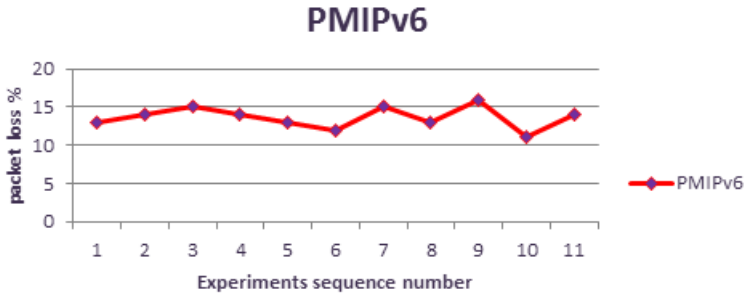

Figure 5.6: Packet loss in PMIPv6

5.3 Authentication procedures modification evaluation

The first proposed enhancement provides a mechanism to reduce the authentication procedures in proxy mobile IPv6 protocol. The first step after the mobile node access the PMIPv6domain is the authentication procedures which are performed by the core functional entities of the domain. These procedures are repeated every time the mobile node changes its point of attachment to perform the handover process.

This modification attempts to reduce these procedures inside the domain in order to reduce the total time delay during the handover process. The mobile node once moves to a new point of attachment, which is NMAG in this case, there is not any need to do the same authentication procedures as before. The mobile node with this modification moves between different points of attachment without more authentication procedures once it occurs in the entry phase.

This test is setup to measure the effect of the modification on the time delay during the handover process. In PMIPv6 normally the mobile node sends a request to access the domain. The access point then sends the syslog message to the MAG that is connected to it. The MAG sends the authentication request to the RADIUS server which then replies with the acceptance or the rejection response.

With applying the proposed modification , these procedures are changed, the server sends a unicast message with the authentication response to PMAG associated with a multicast message to the rest of MAGs in the domain. This multi-cast message is a copy of the uni-cast one but the destinations are different. The destination MAGs receive the message, parse the content and cache the included information in a specific entry fo this MN. This information includes the MNID and the authentication response for this MN.

This test is setup to measure the total delay in handover process within the proposed modification and compare it with the previous result of the PMIPv6 without any modifications.

The time has been measured with all the phases of the handover process as follows:

1. The first phase has been calculated as mentioned in section 5.2 when the mobile node accesses the PMIPv6 domain.

2. The second phase starts when the MAG sends the RADIUS request message to the RADIUS server. The time has been calculated from the time to send the request to the time to receive the response message.

3. The third phase starts when the MAG entity sends the binding message. The time has been calculated from the time of sending the binding update to the time of receiving binding acknowledgment.

4. The fourth phase starts when the the MAG receives the binding acknowledgment. In this phase the time delay has been measured from the time MAG sends the RA to the mobile node to the time the mobile node can establish a connection with the new configured address.

In PMIPv6 the mobile node moves to a NMAG, this NMAG starts the attachment procedures by sending the RADIUS request to the AAA server and after receiving the response with acceptance it starts the binding phase.

With applying the modification in the authentication procedures the NMAG does not send the request, instead it checks the entry for the mobile node and if it exists it starts the binding phase directly. The main idea of the solution is to replace the time consumed by sending the authentication request through the network by the processing time for just checking the entry. The processing time depends on the computational capabilities of the MAG entity and with recent technology it is expected that the processing time is less than sending the data through the network.

This modification has an effect in two cases, the first case when the mobile node moves between a significant numbers of MAGs inside the PMIPv6 and the second case when the network has a high delay in data transfer. The test has been done in two scenarios.

5.3.1 First scenario

In this scenario the test was done with the network in normal case to compare between the handover time delay without solution and the handover time delay with the solution. $T_{handover1}$ presents the handover time delay without the enhancement solution and $T_{handover2}$ presents the handover time delay with the enhancement solution. The$T_{handover1}$ and $T_{handover2}$ are calculated as equation5.4

The test has been repeated 10 times to get an average value in each case and the results are shown in table 5.4.

1	0.000000	::	ff02::16	ICMPv6	Multicast Listener Repo
2	0.027995	::	ff02::1:ffa0:74f1	ICMPv6	Neighbor solicitation
3	1.027977	fe80::864b:f5ff:fea0:	ff02::2	ICMPv6	Router solicitation
4	5.027994	fe80::864b:f5ff:fea0:	ff02::2	ICMPv6	Router solicitation
5	5.964006	fe80::864b:f5ff:fea0:	ff02::16	ICMPv6	Multicast Listener Repo
6	6.050602	fe80::211:22ff:fe33:4	fe80::864b:f5ff:fea0:	ICMPv6	Router advertisement
7	6.555971	::	ff02::1:ffa0:74f1	ICMPv6	Neighbor solicitation
8	7.429921	192.168.13.2	224.0.0.251	MDNS	Standard query PTR 200
9	8.453417	192.168.13.2	224.0.0.251	MDNS	Standard query PTR 200
10	8.516979	2001:1::864b:f5ff:fea	ff02::1:ff33:4455	ICMPv6	Neighbor solicitation

Figure 5.7: Handover delay with solution in the first scenario

Test sequence	1	2	3	4	5	6	7	8	9	10
$T_{handover1}$ (s)	3.78	3.59	3.89	3.78	3.99	4.00	3.64	3.76	3.25	4.00
$T_{handover2}$ (s)	3.06	3.15	3.51	3.65	3.84	3.59	3.43	3.33	3.01	3.80

Table 5.4: Handover delay with and without enhancement

The results show that the first solution has slightly better performance than the normal solution but with no big difference in normal network case. It is expected that the difference increases with the increase in the number of MAG in the domain.

5.3.2 second scenario

The delay has been increased within the implemented software to test the effect of the solution in the case of big authentication delay, the delay has been increased gradually from 1 to 5 second and the result are shown in table 5.5.

62	32.471930	::	ff02::16	ICMPv6	Multicast Listener Report Message v2
63	32.553930	192.168.13.3	224.0.0.251	MDNS	Standard query PTR 201.13.168.192.in-a
64	32.639936	::	ff02::1:ffa0:74f1	ICMPv6	Neighbor solicitation
65	33.589219	192.168.13.3	224.0.0.251	MDNS	Standard query PTR 201.13.168.192.in-a
66	33.639941	fe80::864b:f5ff:fea0:	ff02::2	ICMPv6	Router solicitation
67	33.701468	fe80::211:22ff:fe33:4	fe80::864b:f5ff:fea0:	ICMPv6	Router advertisement
68	34.363928	::	ff02::1:ffa0:74f1	ICMPv6	Neighbor solicitation
69	34.584926	fe80::864b:f5ff:fea0:	ff02::1:ff33:4455	ICMPv6	Neighbor solicitation
70	34.586021	fe80::211:22ff:fe33:4	fe80::864b:f5ff:fea0:	ICMPv6	Neighbor advertisement
71	34.586040	fe80::864b:f5ff:fea0:	2001:2::2	ICMPv6	Echo request
72	34.587091	fe80::211:22ff:fe33:4	fe80::864b:f5ff:fea0:	ICMPv6	Unreachable (Not a neighbor)
73	34.643932	fe80::864b:f5ff:fea0:	ff02::16	ICMPv6	Multicast Listener Report Message v2
74	35.583150	2001:1::864b:f5ff:fea	2001:2::2	ICMPv6	Echo request

Figure 5.8: Handover time delay in second scenario

Time delay (s)	1	2	3	4	5
$T_{handover1}$ (s)	3.70	5.20	5.90	7.54	8.51
$T_{handover2}$ (s)	3.26	3.48	3.39	3.11	3.50

Table 5.5: Handover delay with and without solution in second scenario

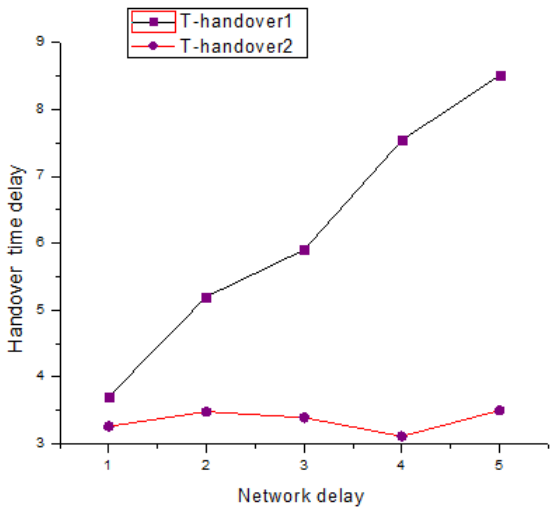

Figure 5.9: Performance of the solution with high latency

During the test it was not possible to increase the number of MAGs to test the solution but the total delay for one MAG was multiplied with the specific number of MAGs to calculate the total delay that can happen in this case as follows: $T_{delay_20access}$ = ($T_{Totaldelay}$ * 20 = (8.51-3.5)* 20 =125 (s).

Figure 5.9 shows the effect of applying the modification in the case of big latency in the network. For the access delay while the solution is not applied the access delay increased proportionally with increasing the delay. In the handover case the result shows the effect of the first solution in reducing the delay against network latency. The results of this test show that reducing the authentication procedure such that it only occurs at the entry of the mobile node to the domain has a better performance regarding the handover latency in PMIPv6 domain.

5.4 Buffering optimization evaluation test

This evaluation test is setup to demonstrate the effect of applying the proposed optimization on the elimination of packet loss in PMIPv6 domain.

The test has been done with client /server application implemented in java. The purpose of the test is to measure the packet loss during the handover period.

The setup of the test has the following scenario, the client which is the CN sends a sequence of packets to the server which is the MN. The mobile node moves to perform the handover from MAG1 to MAG2. The number of the received packet is counted to measure the packet loss percentage. There are three tests, the first test has evaluated the packet loss in different handover periods, the second test has evaluated the influence of increasing the sending rate on the packet loss and without the proposed solution and the third test has evaluated the packet loss percentage in the case of high binding latency.

5.4.1 First test

This test is setup to measure the packet loss with different values for the handover time delay in three cases. The first case is the PMIPv6 without buffering mechanism. The second case is the PMIPv6 with buffering only in LMA as in [15]. The third case presents the second proposed solution with additional buffering mechanism at the MAG entity. The packets has been sent with a rate of 512 kbps and total packet amount of 5Mbps. The handover latency has been increased with 0.5 second every time.

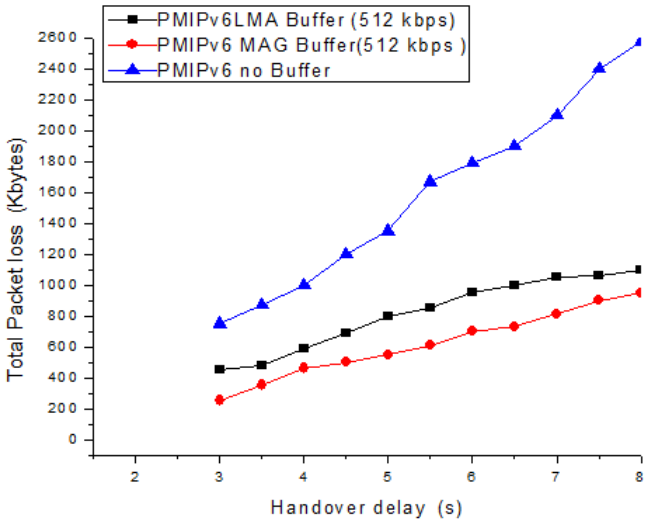

Figure 5.10: Buffering system performance

Figure5.10 shows the results for the first test. The relation in this diagram is between the amount of packet lost and the handover time delay period. The results indicate that the number of lost packets in the handover period is increased proportionally with the increase of handover time delay. The PMIPv6 implementation without the buffering has the maximum packet loss with increasing the handover period.

The second case which presents buffering mechanism implemented in LMA entity, presents better performance regarding the packet loss. The total amount of the lost packets is decreased comparing to the system without the buffering mechanism. With increasing the handover time delay the amount of lost packet increase but with smaller rate than the system without buffering mechanism.

In the third case which presents the proposed optimization with implementing the buffering mechanism in MAG entity, the results shows the best performance regarding the last two cases. These better performance in the case of increasing the handover delay due to the initialization of buffering mechanism by MAG entity directly once it receives the disconnection of the mobile node. This helps in reducing the number of packets that are lost in the period between sending the binding updates to the LMA and finishing the initialization of the buffering mechanism by LMA. During this time a packet loss is increased if the buffering mechanism implemented only in LMA entity.

5.4.2 Second test

This test is setup to measure the influence of increasing the packet rate on the percentage of packet loss. This packet loss is tested with considerable handover time delay and the results are shown in figure 5.11

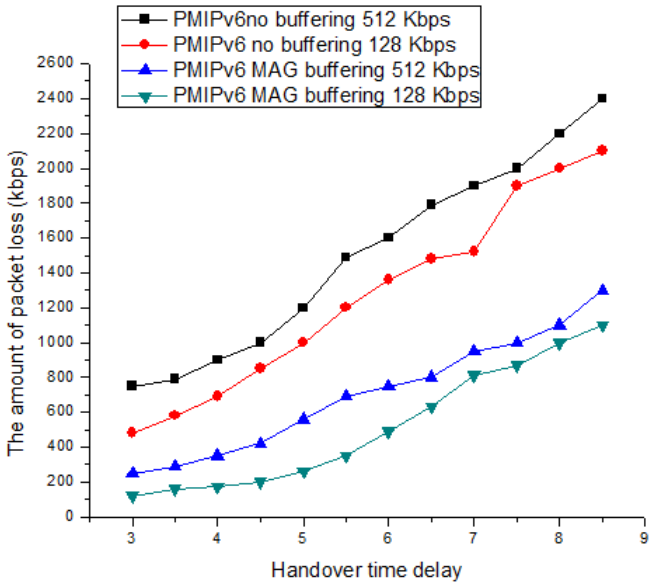

Figure 5.11: Packet rate effect

The relation in figure 5.11 is between the total amount of packet loss in Kbps and the handover time delay in second. The curves present four cases, the first case presents the PMIPv6 with no buffering mechanism and the sending rate is 128 kbps. The second case presents the PMIPv6 with buffering mechanism in MAGand the sending rate in this case is 128 kbps. The third case presents the PMIPv6 with no buffering mechanics and the sending rate is 512 kbps. The fourth and last case presents the PMIPv6 with buffering in MAG and the sending rate is 512(Kbps).

The results demonstrate that the second and fourth cases have better performance especially with increasing the handover time delay. The results also indicates that the increasing of the packet loss due to the increasing of the sending rate. The reason for that is that, the buffer during the handover period contains specific amount of packets and with increasing of the sending rate the rest of the packets lost at this period.

5.4.3 Third test

The purpose of this evaluation is to test the performance of the solution regarding the packet loss in the domain with increasing the delay between MAG and LMA entities. The time for binding updates is increased to test the packet loss in this period with and without the buffer at MAG entity.

In this test the CN sends the packet to MN in sequence. The mobile node disconnected from the MAG link and the binding time is increased to prevent the LMA from receiving the detachment event of the mobile node. The LMA keeps sending the packets to the MN which is disconnected at this period.

A comparison between PMIPv6 with LMA the buffering mechanism and the PMIPv6 with MAG buffering to see the influence of the solution on the packet loss in this period. The results are shown in figure5.12

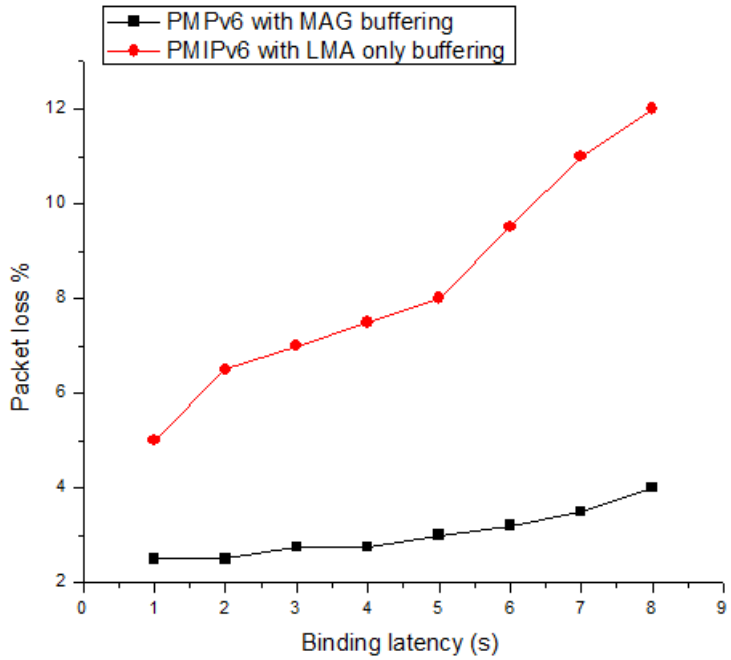

Figure 5.12: Packet loss with high binding latency

The results in figure 5.12 show that the buffer added to MAG entity has a great effect in reducing the packet loss percentage at the disconnection time of the mobile node which associated with increase in the latency of the binding updates from the MAG entity. The buffering mechanism initialization is related with the receiving of the detachment event and in this case the buffering mechanism is initialized only at MAGside.

5.4.4 Conclusion of the results and discussion for the proposed optimization solution

The results for the first test show a better performance in the case of increasing of the handover delay within the domain for applying a buffering mechanism in MAG entity. In the case of increasing the delay, the buffering mechanism performs better than the system without any supporting buffering mechanism.

The second test shows the influence of increasing the packet rate on the number of lost packets. The number of lost packets increased with the increase of the data rate during the long handover time delay.

The third test shows the performance of the system in the case with high latency between MAG and LMA, this latency prevents the LMA from receiving the PBU message to internalize the buffering mechanism and in this case the existence of buffer at MAG side prevents the packet loss occurs during the handover period.

6

Conclusions and Future Work

Contents

6.1 Conclusions

This project proposes two modification techniques to overcome the limitations that exist in the proxy mobile IPv6 protocol.

The work starts with the implementation of PMIPv6 in a real test bed in order to evaluate the performance of the protocol in a real scenario. The implementation is based on the open source implementation in [23] which follows the PMIPv6 specification as in [7].

After the implementation of the PMIPv6 test bed the work has continued with the implementation of the proposed enhancements. The first enhancement attempts to reduce the handover time delay within the movement of the mobile node in the domain by reducing the authentication procedures. This procedures occurs only one time with the entry of the mobile node to PMIPv6 domain. When the mobile node moves to new point of attachment within the domain, it is not required to repeat the same procedures again and the PBU message is sent directly once the detection of the mobile node occurs. The results show a good performance of the solution especially in the case associated with a big latency in the PMIPv6 domain.

The second enhancement provides a modification to the buffering mechanism proposed in [15] in order to reduce the packet loss percentage during the handover period. In the handover time the mobile node is disconnected from the serving MAG and tries to connect to anther MAG within the new location. The serving MAG detects this disconnection of the mobile node with an event message received from the connected AP.

The network latency between the PMIPv6 domain entities can cause a significant amount of packet loss especially with the increase in the handover time delay. The increasing in the number of the mobile nodes in the domain can cause overload in the LMA buffer so it can present a point of failure in the domain. The test for the evaluation of the second enhancement has setup in three steps as follows:

The results for the first test show a better performance in the case of increasing of the handover in the domain for the second solution. In the case increasing the delay the buffering mechanism performs better than the system without any buffering mechanism.

The second test shows the influence of increasing the packet rate on the number of lost packets. The number of lost packets increased with the increase of the data rate.

The third test shows the performance of the system in the case of high latency between MAG and LMA prevents the LMA from receiving the PBU message to internalize the buffering mechanism and in this time the existence of buffer at MAG side prevents the packet loss occurs during the handover period.

6.2 Future work

The future work will focus on the improvement in the protocol to overcome the limitations presented in the protocol. Some limitations of the test system are due to restrictions on the available equipment, since it was not possible to fully test the performance of the proposed solutions with a larger number of mobile nodes. The packet reordering needs some improvement in order to rearrange the packets that are coming from two sources, the LMA and previous MAG.

Future work should focus on the move of the localization anchor from a centralized function to distributed function. The distribution of the mobility 's functions between the PMIPv6 entities has a great effect in balancing the network load. To have more than one LMA that are severing the same mobile node can help to move the mobility-related signaling exchange to the nearest point to the mobile node. This in fact can reduce the signaling message overhead in the domain and improve the quality of service provided by the protocol.

Bibliography

[1] C. E. Perkins and A. Myles, “Mobile IP,” *Proceedings of International Telecommunications Symposium*, pp. 415–419, 1994.

[2] C. E. Perkins, “IP mobility support for IPv4,” Internet Requests for Comment, RFC Editor, Fremont, CA, USA, RFC 3344, Aug. 2002.

[3] D. B. Johnson, C. E. Perkins, and J. Arkko, “Mobility support in IPv6,” Internet Requests for Comment, RFC Editor, Fremont, CA, USA, RFC 6275, Jul. 2011.

[4] A. G. Valkó, “Cellular IP: a new approach to Internet host mobility,” *SIGCOMM Comput. Commun. Rev.*, vol. 29, no. 1, pp. 50–65, Jan. 1999.

[5] R. Ramjee, T. F. La Porta, S. R. Thuel, K. Varadhan, and L. Salgarelli, “IP micro-mobility support using HAWAII,” Working Draft, IETF Secretariat, Fremont, CA, USA, Internet-Draft draft-ietf-mobileip-hawaii-01.txt, Jul. 2000.

[6] H. Soliman, C. Castelluccia, K. El Malki, and L. Bellier, “Hierarchical mobile IPv6 mobility management (HMIPv6),” Internet Requests for Comment, RFC Editor, Fremont, CA, USA, RFC 4140, Aug. 2005.

[7] S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury, and B. Patil, “Proxy mobile IPv6,” Internet Requests for Comment, RFC Editor, Fremont, CA, USA, RFC 5213, Aug. 2008.

[8] R. Koodli, “Mobile IPv6 fast handovers,” Internet Requests for Comment, RFC Editor, Fremont, CA, USA, RFC 5268, Jun. 2008.

[9] B. Sarikaya, F. Xia, D. Damic, and S. Gundavelli, “Radius support for proxy mobile ipv6,” Internet Requests for Comment, RFC 6572, Jun. 2012.

[10] P. Calhoun, J. Loughney, J. Arkko, E. Guttman, and G. Zorn, “Diameter base protcol,” Internet Requests for Comment, RFC 3588, 2003.

[11] H. Velayos and G. Karlsson, “Techniques to reduce the IEEE 802.11b handoff time,” in *2004 IEEE International Conference on Communications (IEEE Cat. No.04CH37577)*, vol. 7. IEEE, 2004, pp. 3844–3848.

[12] H. Yokota, K. Chowdhury, J. Arkko, R. Koodli, B. Patil, and F. Xia, “Fast handovers for proxy mobile ipv6,” Internet Requests for Comment, RFC 5949, 2010.

[13] R. Koodli, “Mobile IPv6 fast handovers,” Internet Requests for Comment, RFC Editor, Fremont, CA, USA, RFC 5568, Jul. 2009.

[14] B. Sarikaya and F. Xia, “Mobile node agnostic fast handovers for proxy mobile ipv6,” Working Draft, IETF Secretariat, Internet-Draft draft-xia-netlmm-fmip-mnagno-02, Nov. 2007.

[15] C. Park, N. Kwon, H. Woo, and H. Choo, “Buffering in proxy mobile ipv6:implementationand analysis,” *The Journal of Supercomputing June 2014, Volume 68, Issue 3, pp 1503-1520*, 2014.

[16] H.-Y. Choi, K.-R. Kim, H.-B. Lee, S.-G. Min1, and Y.-H. Han, “Smart buffering for seamless handover in proxy mobile ipv6,” *Wirel Commun Mob Comput 11(4):491-499*, 2011.

[17] R. Callon and E. Rosen, “Multiprotocol label switching architecture,” Internet Requests for Comment, RFC 3031, Jan. 2001.

[18] L. Andersson, P. Doolan, N. Feldman, A. Fredett, and B. Thomas, “Ldp specification,” Internet Requests for Comment, RFC 3036, Jan. 2001.

[19] V. Vassiliou, “Design considerations for introducing micromobility in MPLS,” in *Proceedings of the 11th IEEE Symposium on Computers and Communications (ISCC 2006), 26-29 June 2006, Cagliari, Sardinia, Italy*, 2006, pp. 870–877.

[20] B. Sarikaya and F. Xia, “Mpls tunnel support for proxy mobile ipv6,” Working Draft, IETF Secretariat, Internet-Draft draft-xia-netlmm-mpls-tunnel-00.txt, Oct. 2008.

[21] R. G. Garroppo, S. Giordano, and L. Tavanti, “Network-based micro-mobility in wireless mesh networks: Is MPLS convenient?” in *Proceedings of the Global Communications Conference, 2009. GLOBECOM2009, Honolulu, Hawaii, USA, 30 November - 4 December 2009*, 2009, pp. 1–5.

[22] C. A. Astudillo, O. J. Calderón, and J. H. Ortiz, “Pm^{2}pls: Integrating proxy mobile ipv6 and MPLS in wireless access networks,” in *4th IFIP International Conference on New Technologies, Mobility and Security, NTMS 2011, Paris, France, February 7-10, 2011*, 2011, pp. 1–5.

[23] “Eurecom openairinterface proxy mobile ipv6,” http://www.opnairinterface.org, retrieved October 2014.

[24] “Umip: Usagi-patched mobile ipv6 for linux,” http://umip.linux-ipv6.org, retrieved October 2014.

[25] “Open source board,” http://monet.skku.ac.kr/, retrieved October 2014.

[26] “netfilter firwalling, nat, packet mangling for linux,” http://www.netfilter.org/, retrieved October 2014.

[27] “Freeradius wiki,” http://freeradius.org/, retrieved October 2014.

A

Title of AppendixA

A.0.1 Kernel Recompilation

the steps to recompile the linux system for IPv6 mobility as following: On the linux terminal write:

- apt-get update
- apt-get install linux-source
- cd /usr/src/
- tar xjf linux-source-XX.XX.XX (with XX.XX.XX depends on your system version)
- ln -s /usr/src/linux-source-XX.XX.XX /usr/src/linux
- apt-get install qt3-apps-dev g++
- cd /usr/src/linux-source-XX.XX.XX
- make xconfig (Qt-based) (recommended)

After enabling the feature the kernel should be recompiled from command line as following
$cd/usr/src/linux - source - XX.XX.XX$
$mkinitramfs - o/boot/initrd.img - XX.XX.XXXX.XX.XX$
$update - grub$
$reboot$

A.0.2 FreeRadius Installation

The FreeRadius v 2.1.10 is used in this testbed and the installation from the command line as following:

- wget ftp://ftp.freeradius.org/pub freeradius/freeradius-server-2.1.10.tar.bz2
- tar xjf freeradius-server-2.1.10.tar.bz2
- cd freeradius-server-2.1.10
- ./configure
- make
- make install

A.0.3 Syslog Installation

The syslog server installation can be done from command line as following:

- apt-get install socklog sysklogd
- Create a file called $pmip_s yslog.log$

- touch /var/log/$pmip_syslog.log$
- Make changes in syslog server configuration file
- gedit /etc/$syslog.conf$
- The line containing local7.info and change it to have this $\rightarrow$ "local7.info /var/log/ $pmip_syslog.log$"
- gedit /etc/defa $\rightarrow$ /etc/init.d/sysklogd
- restart

Option	Place in kernel
CONFIG_EXPERIMENTAL	GENERAL SETUP→ PROMPT FOR DEV AND OR INCOMPLETE DRIVERS)
CONFIG_SYSVIPC	(GENERAL SETUP → SYSTEM V IPC)
CONFIG_PROC_FS	GENERAL SETUP → SYSTEM V IPC)
CONFIG_INET	NETWORKING SUPPORT → NETWORKING OPTIONS → TCP/IP NETWORKING
CONFIG_IPV6	NETWORKING SUPPORT → NETWORKING OPTIONS → TCP/IP NETWORKING
CONFIG_IPV6_MIP6	NETWORKING SUPPORT → NETWORKING OPTIONS→ IPV6 PROTOCOL
CONFIG_XFRM_USER	NETWORKING SUPPORT → NETWORKING OPTIONS → TRANSFORMATION USER CONFIGURATION INTERFACE
CONFIG_XFRM_SUB_POLICY	NETWORKING SUPPORT → NETWORKING OPTIONS → TRANSFORMATION SUB POLICY SUPPORT
CONFIG_INET6_XFRM_MODE_ROUTEOPTIMIZATION	NETWORKING SUPPORT → NETWORKING OPTIONS → IPV6 PROTOCOL → IPV6: MIPV6 ROUTE OPTIMISATION MODE
CONFIG_IPV6_TUNNEL	NETWORKING SUPPORT → NETWORKING OPTIONS → IPV6 PROTOCOL → IPV6: IPV6 IN IPV6 TUNNEL
CONFIG_IP_ADVANCED_ROUTER	NETWORKING SUPPORT → NETWORKING OPTIONS→IP: ADVANCED ROUTER
CONFIG_IPV6_MULTIPLE_TABLES	NETWORKING SUPPORT → NETWORKING OPTIONS →IP: ADVANCED ROUTER
CONFIG_IPV6_SUBTREES	NETWORKING SUPPORT → NETWORKING OPTIONS →IP: ADVANCED ROUTER
CONFIG_ARPD	NETWORKING SUPPORT → NETWORKING OPTIONS → IP: ARP DAEMON SUPPORT
CONFIG_INET6_ESP	NETWORKING SUPPORT→ NETWORKING OPTIONS →IPV6 PROTOCOL → IPV6 ESP TRANSFORMATION
CONFIG_NET_KEY	NETWORKING SUPPORT → NETWORKING OPTIONS→ PF_KEY SOCKETS
CONFIG_NET_KEY_MIGRATE	NETWORKING SUPPORT→ NETWORKING OPTIONS→ PF_KEY SOCKETS → PF_KEY MIGRATE

Table A.1: Kernel recompilation