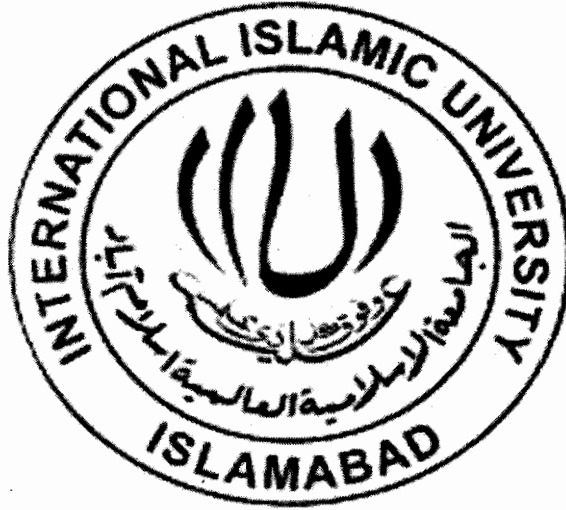


# Improved Authentication Scheme of Proxy Mobile IPv6 Handover Process

TO 8147



*Developed By*

**Tahir Hussain**

**379-FBAS/MSCS/F07**

*Supervised By*

**Muhammad Mata ur Rahman**

**Department of Computer Science**

**Faculty of Basic and Applied Sciences**

**International Islamic University Islamabad**

**2011**



**Department of Computer Science**

**International Islamic University Islamabad, Pakistan**

Dated: 17-08-2011

**Final Approval**

This is to certify that we have read and evaluated the thesis entitled **Improved Authentication Scheme of Proxy Mobile IPv6 Handover Process** submitted by **Tahir Hussain** under **Reg.No. 379/FBAS/MSCS/F07**. In our views it is completed in scope and quality for the degree of **Master of Science in Computer Science**.

**Project Evaluation Committee**

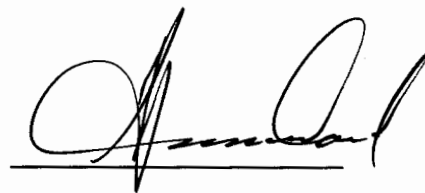
**External Examiner:**

**Prof. Dr. Muhammad Younus Javed,**

Associate Dean (Academic & Evaluation),

College of Electrical and Mechanical Engineering,

National University of Science and Technology (NUST) Rawalpindi.



**Internal Examiner:**

**Dr. Muhammad Zubair,**

Assistant Professor,

Department of Computer Science & Software Engineering,

International Islamic University Islamabad.



**Supervisor:**

**Mr. Muhammad Mata ur Rahman,**

Assistant Professor,

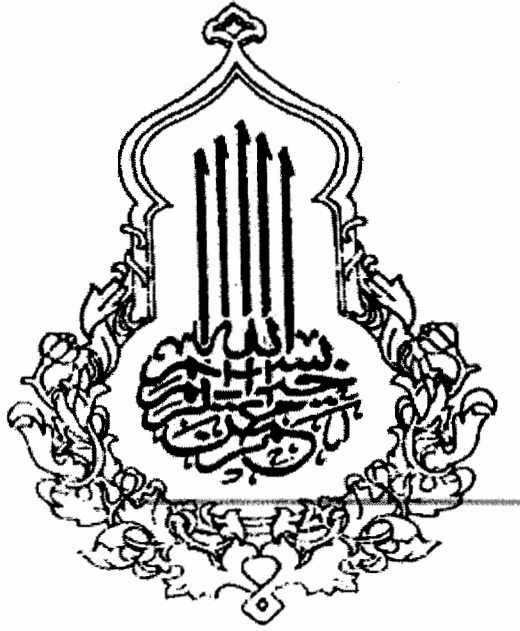
Department of Computer Science & Software Engineering,

International Islamic University Islamabad.



## **Dedication**

**I dedicate this research project to my friends**



*In the Name of*

**ALLAH,**

*The most merciful and compassionate, the most gracious and beneficent Whose help and  
guidance we always solicit at every step and every moment.*

## **ABSTRACT**

Mobile IP is used to provide continuity of traffic for users while moving within the same network or moving from one network to another. Two versions of Mobile IP i.e Mobile IPv6 and Mobile IPv4 have been proposed to support mobile connections. MIPv6 is an updated version of the Mobile IP standardized by IETF (Internet Engineering Task Force) that performs the authentication of mobile nodes using IPv6 addressing mechanism.

In traditional routing protocols, IP address is the representation of the network topology. In these protocols routing mechanisms is depended on the idea that each network node will always use the same point of attachment to connect to the Internet, and that the IP address of each node shows the link where it is connected to the network. In these routing mechanisms, if you want to disconnect your device from the current network and connect to a different network for using Internet then your device will have to use a new IP address which breaks the session continuity.

With the help of MIPv6 a mobile node can transparently maintain its connection to the Internet while moving from one subnet to another. In MIPv6 each device is given a permanent home address and a temporary care of address. When connected to foreign network, a mobile device sends its location information to a home agent, which intercepts packets, intended for the device and tunnels them to the current location.

MIPv6 provides host based mobility management in which mobile node performs the mobility updating signaling by itself. We have another protocol i.e Proxy Mobile Ipv6 which provides network based mobility management in which the underlying network executes all the mobility related signaling for the mobile node. In order to provide a connection to the mobile node, the network performs the authentication of mobile nodes and other related components which introduces delay in the handover process.

We have analyzed the existing mobile node handover mechanisms and their cost metrics and proposed mechanism which perform the authentication of the components before the actual handover process. Our result shows that the proposed mechanism reduces the handover delay during handover of the mobile node in the Proxy Mobile Ipv6 network.

## **ACKNOWLEDGMENT**

**With the name of Allah, Most Gracious, Most Merciful**

Thanks to the creator of this universe for giving me the courage and patience to complete this work. I am very thankful to International Islamic University for providing me such a good research environment.

I wish to thank my supervisor Mr. Muhammad Mata ur Rahman for his continuous advise, support and encouragement throughout this work. He has instilled in me a state of confidence, with which I now feel that I can do research of any new topic following his research guidelines. I am grateful to department of computer science IIU Islamabad and faculty members for providing healthy environment for research.

I would be failing in my duties if I would not remember to thank my fellow graduate students, especially Mr. Iftikhar Muhammad, Mr. Kamran Ullah, Mr. Muhammad Wasim, Mr. Muhammad Asif for their continuous motivation and support. I am looking forward to a continue collaboration with them in the future.

I would also like to thank my dear friends Mr. Hamdullah Lecturer Cantt. Garrison College Rawalpindi, Mr. Muhammad Ishaq Lecturer Govt. Degree College Mardan, Mr. Farhan Khan Lecturer Govt. Degree College Takht Bhai Mardan Mr. Ikram Ullah BISE Mardan, who have been a continuous motivation behind my success.

Finally I am eternally grateful to my parents and whole family. Their endless support encouragement and stimulation have been a true source of strength and inspiration for me.

## Table of Contents

<u>Chapter Number</u>		<u>Page Number</u>
<b>1.</b>	<b>Introduction</b>	<b>1</b>
	1.1 Introduction	1
	1.2 Mobility management.	1
	1.2.1 Host Based Mobility Management	1
	1.2.2 Network Based Mobility Management	3
	1.3 Difference between Host based and network based mobility management.	4
	1.4 Proxy Mobile IP handover.	5
	1.5 Motivation	7
	1.6 Summary	8
<b>2</b>	<b>Related Work</b>	<b>9</b>
	2.1 Introduction	9
	2.2 Literature Survey	9
	2.2.1 Fast Proxy MIPv6	9

2.2.2 Fast Handover Scheme with Neighboring MAG Collaboration.	11
2.2.3 Context Transfer scheme for PMIPv6	13
2.2.3.1 Proactive Handoff scheme	13
2.2.3.2 Reactive Handoff Scheme	14
2.2.4 IEEE 802.21: Media-Independent Handover (MIH) based scheme	15
2.3 Summary	18
<b>3 Requirement Analysis</b>	<b>19</b>
3.1 Introduction	19
3.2 Problem Statement	19
3.3 Media independent handover.	20
3.3.1 The Need of IEEE 802.21Media Independent Handover (MIH)	21
3.3.2 Media Independent Handover Function (MIHF).	21
3.4 Improved Authentication Scheme of Proxy Mobile IPv6 (IASPMIPv6)	24
3.5 Summary.	28
<b>4 Simulation</b>	<b>30</b>
4.1 Introduction.	30
4.2 Simulation tool	30
4.3 Mobility support in NS2:	31
4.4 The AWK language	31



4.5 Simulation Goal	32
4.6 Model of simulation	33
4.7 Simulation Scenario	36
4.8 Research Methodology	38
4.8.1 Experiment for increasing handovers.	39
4.8.2 Experiment for testing the effect of Link Delays	40
4.8.3 Experiment for the MN speed	41
4.9 Summary	41
<b>5 Evaluating Performance</b>	<b>42</b>
5.1 Introduction	42
5.2 Elements of performance	42
5.3 Results	44
5.3.1 Calculating results for testing impact of handovers.	44
5.3.2 Calculating results for effect of link delays variation	47
5.3.3 Calculating results for MN speed variation	49
5.4 Summary	51
<b>6 Conclusion and Future work</b>	<b>52</b>
6.1 Conclusion	52
6.2 Future Work	52

## List of Figures

<b>Fig 1.1 Mobile IPv6 .....</b>	<b>2</b>
<b>Figure 1.2 Proxy Mobile IPv6 Domain .....</b>	<b>6</b>
<b>Figure 1.3 PMIPv6 signaling call flow.....</b>	<b>7</b>
<b>Figure 2.1 Fast Proxy MIPv6 .....</b>	<b>10</b>
<b>Figure 2.2 Handover neighbor MAGs.....</b>	<b>11</b>
<b>Figure 2.3 Handover neighbor MAGs signaling flow .....</b>	<b>12</b>
<b>Figure 2.4 Proactive handoff scheme .....</b>	<b>14</b>
<b>Figure 2.5 Reactive handoff scheme .....</b>	<b>15</b>
<b>Figure 2.6 802.21 MIH based scheme .....</b>	<b>17</b>
<b>Figure. 3.1 Location of MIH function .....</b>	<b>24</b>
<b>Figure 3.2 Proxy Mobile IPv6 Network .....</b>	<b>25</b>
<b>Figure 3.3 signaling call flow .....</b>	<b>27</b>
<b>Figure 3.4 Binding Update Message.....</b>	<b>27</b>
<b>Figure 3.5. Proxy Binding Acknowledgment Message.....</b>	<b>28</b>
<b>Figure 4.1 Implementation of Simulation.....</b>	<b>33</b>
<b>Figure 4.2 Sequence of events for MN.....</b>	<b>36</b>
<b>Figure 4.3 Proxy Mobile IPv6.....</b>	<b>37</b>
<b>Figure 5.1 Handover delay.....</b>	<b>45</b>
<b>Figure 5.2 Packet loss ratio.....</b>	<b>46</b>
<b>Figure 5.3 Handover delay.....</b>	<b>47</b>

**Figure 5.4 Packet loss.....48**

**Figure 5.5 Handover delay..... 49**

**Figure 5.6 Packet loss..... 50**

## **List of Tables**

<b>Table1.1 Comparison of the host and network based mobility management.....</b>	<b>4</b>
<b>Table 4.1 Parameters of simulation.....</b>	<b>38</b>
<b>Table 4.2 Parameters for experiment No.1.....</b>	<b>40</b>
<b>Table 4.3 Parameters for experiment No. 2.....</b>	<b>40</b>
<b>Table 4.4 Parameters for experiment No.3.....</b>	<b>41</b>

## List of Abbreviation Used

CoA	Care of address
DAD	Duplicate Address Detection
FMIPv6	Fast Mobile Internet Protocol v6
HA	Home Agent
HI	Handover Initiate
HMIPv6	Hierarchical Mobile Internet Protocol version 6
HoA	Home Address
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
LMA	Local Mobility Anchor
MAG	Mobility Access Gateway
MN	Mobile Node
CN	Correspondent Node
nMAG	New MAG
pMAG	Previous MAG
PBAck	Proxy Binding Acknowledgment
PBU	Proxy Binding Update

FPMPv6	Fast Proxy Mobile IPv6
AAA	Authentication, Authorization, and Accounting
MIH	Media Independent Handover
MIES	Media Independent Event Service
MICS	Media Independent Command Service
MIIS	Media Independent Information Service
NS2	Network Simulator 2

# Introduction

# 1

## 1.1 Introduction.

In this chapter we introduce the ideas of host and network based mobility management. This chapter gives a detail description of the protocols that provide these types of mobility management. This also provides a comparison of both with respect to performance. Finally this introduces the Proxy Mobile Internet Protocol version6 domain and mobile node handover process.

## 1.2 Mobility management.

Nowadays the demand for continuous network connectivity is a basic preference in our lives. Many current wireless technologies have realized this idea. However for providing a fast and seamless continuous network access many challenges and problems are still there that are to be solved. The focus is mainly on to realize mobile networks of IP (Internet Protocol) which will enable the users to combinely use the Internet and the telecommunication networks. One of the basic problems in this realization of IP mobile networks is how to handle mobile nodes mobility management. Mobility management includes location management and handover management.

Recently two types of mobility management have been proposed.

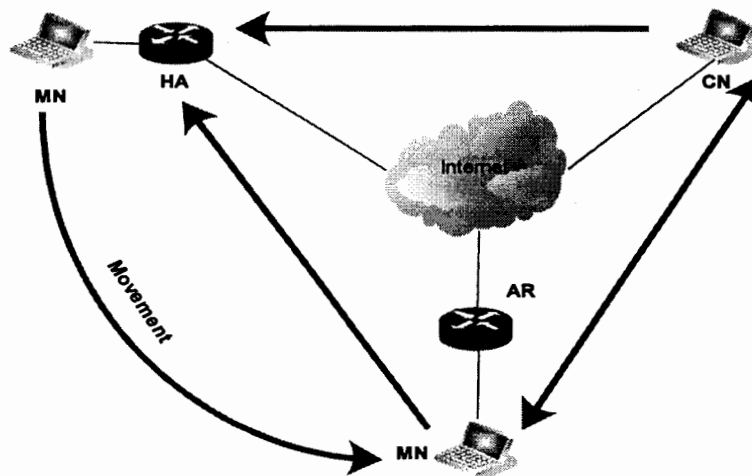
1.2.1 Host based mobility management

1.2.2 Network based mobility management

### 1.2.1 Host based mobility management.

Host based mobility management require changes in the protocol stack of mobile node (MN). It means that to provide mobility support both the network and the mobile node is to be modified, which makes it complex. Also in host based mobility the MN is involved in the exchange in the

mobility management signaling session updating. A well known protocol for providing mobility is Mobile Internet Protocol (MIP). It is widely accepted as a standard protocol for providing mobility. It combines two powerful technologies i.e. the Internet and mobile communication. Two standard versions of this protocol which provide host based mobility are Mobile Internet Protocol version 4(MIPv4) and Mobile Internet Protocol version 6(MIPv6). These protocols propose two types of IP addresses for the hosts while providing host based mobility. These two types of addresses are a home address (HoA) that shows the permanent address of the mobile node (MN) in the original network and a care of address (CoA) that changes while the mobile node moves. The main difference between the MIPv4 and MIPv6 is that MIPv6 uses access router in place the Foreign Agent (FA) of MIPv4. In addition there was no concept of route optimization in MIPv4. However this concept was standardized by MIPv6.



**Fig 1.1 Mobile IPv6**

Although It is true that host based mobility management protocols(MIPv4,MIPv6) handles many of the mobility management problems such as the route optimization or triangle route problem,



and limited IP address space but it still has many problems such as high handover delay, packet loss, frequent duplicate address detection, and signaling issues. In order to solve or minimize the effects of these problems many enhancement of MIPv6 were presented such as Hierarchical Mobile IP (HMIPv6), Fast handover Mobile IPv6 (FMIPv6). However MIPv6 and its all its enhancements provide host based mobility management and require a change at mobile node protocol stack which make it complex.

### **1.2.2 Network Based Mobility Management.**

In a network based mobility management the current network performs all the mobility management tasks for the MN. The MN does not take part in mobility related session updating signaling. Also there is no need for the modification of the MN protocol stack. It has also advantages in easy implementation as compared to the host based mobility management, therefore the Internet Engineering Task Force(IETF) has accepted a new protocol as standard protocol called Proxy Mobile IPv6 (PMIPv6) that provides network based mobility management for MN.

PMIPv6 provides local network based mobility without requiring the MN to participate in the mobility management signaling. The main functional components which provide mobility support in the PMIPv6 domain are the Local Mobility Anchor (LMA), Mobility access gateway, and the Authentication, Authorization, and Accounting (AAA) server. The function LMA is similar to that of the home agent (HA) in Mobile IPv6 network. It is responsible for keeping MN's reachability and binding state and all the traffic intended for the MN pass through it. The mobility access gateway (MAG) is the component to which the MN connects and it sends mobility management messages to the LMA on behalf of MN. The MAG is also responsible for detecting the MN's movements in PMIPv6 network for initiating binding registrations to the MN's LMA. The AAA server maintains the accounting, authorization and authentication information of the MN. The PMIPv6 domain components i.e MAGs and LMA access these information for providing session continuity and new connection to a given MN.

### 1.3 Difference between Host based and network based mobility management.

Table 1.1 shows the basic differences of host and network based mobility management. This comparison shows that the network based mobility management provide better network management and handles most of the problems of the host based mobility management such as MN protocol sack modification, and the duplicate address detection check which is performed each time when a MN changes its attachment, however it is performed only once in case of shared MN prefixes and not at all in case of per MN prefixes in network based mobility.

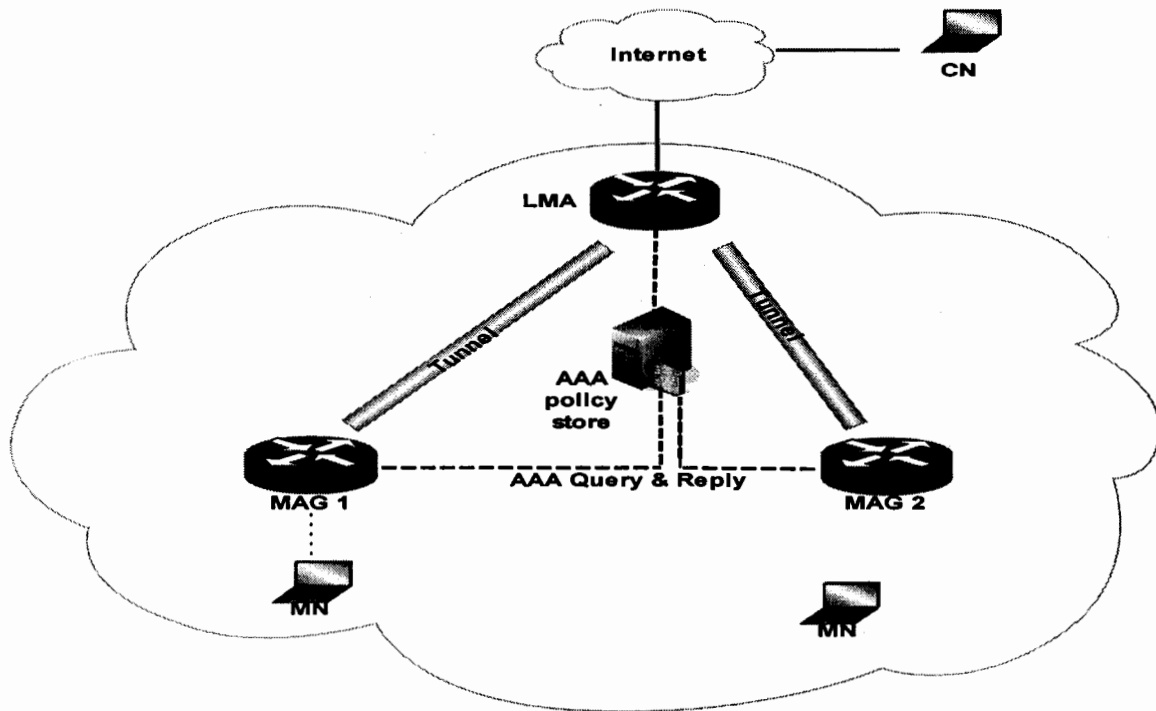
	<b>Host Based Mobility Management</b>	<b>Network Based Mobility Management</b>
Mobility Scope	Global	Local
Topological Entity	Access Router	Mobility Access Gateway
Functional Component	Home Agent	Local Mobility Anchor
Mobile Node Modification	Required	Not Required
Registration Message	Binding Update	Proxy Binding Update
Mobile Node Address	Home Address or Care of Address	Always Home Address
Router Advertisement	Broadcast	Unicast
Moment Detection	Performed by Router Solicitation/Router Advertisement	Performed by Layer 2

**Table1.1 Comparison of the host and network based mobility management**

#### 1.4 Proxy Mobile IP handover.

Whenever a MN enters into a PMIPv6 network and obtain an attachment to serving Mobile Access Gateway (MAG) the MN informs it by sending a router solicitation (RS) message to it. The router solicitation message presents the MN identifier. When MAG receives RS message, it obtains information about the MN and perform the access authentication using MN's identifier by sending a Query message to AAA server, which contain all network access information. If the MN is found to be authorized for accessing the network services, the MAG obtains the MN's AAA information, LMA address from the AAA server and then sends Proxy Binding Update (PBU) message containing the identifier of MN to LMA for the MN. When the LMA receives this PBU, it also performs the same operation. For this purpose the LMA also sends an AAA query message to the AAA server. The AAA server checks the identity of MAG and replies to the LMA. If the access authentication of the MAG is successful the LMA creates a binding cache in order to keep the binding state of the MN. After this it sends Proxy Binding Acknowledgment (PBA) message to the MN via MAG. These messages include the MN's home network prefix. The LMA also creates a tunnel with MAG. The MAG sends Router Advertisement (RA) messages to MN on the access link which advertises the MN's home network prefix, got from LMA. The MN then performs IP address configuration, and uses the tunnel between MAG and LMA to send or receive packets.

The above process is repeated each time the MN is handed over to new MAG within the PMIPv6 domain. Since the authentications steps are performed each time the MN moves this causes delay in the handover of the MN thereby increasing the packet loss. Following figure shows PMIPV6 handover process.



**Figure 1.2 Proxy Mobile IPv6 Domain.**

Figure 1.3 shows a detailed signaling call flow of the PMIPv6 domain. It is clear that the MN cannot receive traffic from the MAG until the authentication of the MN and MAG are completed. The MAG sends an AAA query message to the AAA policy store which then responds through an AAA query reply message. Similarly when the authentication of MN is performed by the MAG then LMA contacts with the AAA query and reply message to authenticate the MAG. When these steps are completed and the MN as well as the LMA is found authorized the packets are forwarded to the MN.

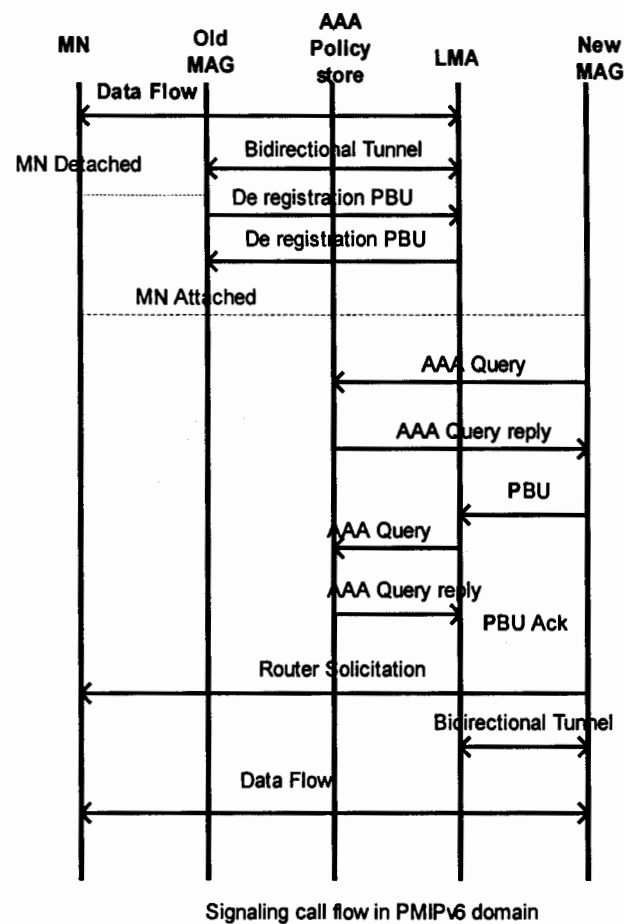


Figure 1.3 PMIPv6 signaling call flow

### 1.5 Motivation.

In a networked environment it is extremely important to check the identity of all users that are requesting for the network resources. It means that each time a user request for some services from the network it must be authenticated. However when MN moves from one location to another and obtains another connection such authentication causes delay in the handover process which affects the performance of network based mobility management. Therefore it is necessary to handle this problem.

**1.6 Summary.**

This chapter discussed host and network based mobility management for MNs. The chapter explained the merits and demerits of both with respect to different parameters. A detailed description of the proxy mobile IPv6 protocol was given which support network based mobility management. The different features and handover of mobile nodes within proxy mobile IP network were explained.

# Related Work

# 2

## 2.1 Introduction.

This chapter we perform a deep survey of the literature to gain knowledge about the Proxy Mobile IPv6 domain. We study current and important problems of the PMIPv6 environment. The chapter analyzes all the approaches that are carried out for improving the handover process in the network based mobility management of the PMIPv6.

## 2.2 Literature Survey.

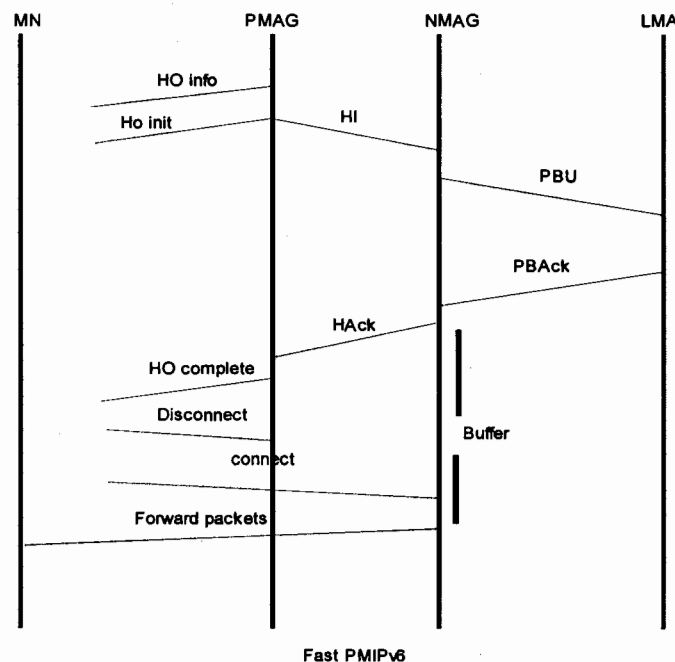
For many years researchers are actively working to improve the performance of network based mobility management using PMIPv6. This section include some protocols and mechanisms that are proposed for reducing the authentication delay in order to reduce the handover delay ,during handover of the MN between Mobile Access Gateways(MAGs) in the PMIPv6 domain.

### 2.2.1 Fast Proxy MIPv6.

Fast Proxy Mobile IPv6 (FPMIPv6) was proposed to reduce the handover delay by reducing MN node authentication delay and packet loss during handover. In this scheme the handover is predicted by receiving a notification from the MN. As a result of the prediction, the previous MAG (pMAG) sends a handover initiate message (HI) and policy profile to the new MAG (nMAG), which includes the MN identifier and a timestamp. The nMAG then creates a proxy binding update (PBU) message and forwards it to the LMA. The LMA then replies with proxy binding acknowledgement (PBUAck) message, create a new binding and forward the packets to the nMAG. Upon the receipt of PBUAck the nMAG sends HIack message to the pMAG, buffer

the traffic until the MN is connected. The downlink traffic arriving at the pMAG after a MN disconnects are buffered. A temporary tunnel between the pMAG and the nMAG is established and used to forward the traffic from pMAG to nMAG. [1]

Although FPMIPv6 is efficient scheme to reduce packet loss during handover, a critical issue in the operation of FPMIPv6 is the timely and correct prediction of a handover. Similarly if the distance between the LMA and the nMAG is less than the tunnel distance between LMA, pMAG and nMAG then the packets arriving at the nMAG may be out of order. In addition this scheme only reduces the MN authentication delay and does not consider the MAG authentication delay.



**Figure 2.1 Fast Proxy MIPv6**



### 2.2.2 Fast Handover Scheme with Neighboring MAG Collaboration.

This scheme is based on the concept of handover neighbor MAG that is the new MAG knows some information about the MN in advance. A neighboring MAG is one to which the MN can handover. This MAG is geographically adjacent to the MAG to which the MN is currently linked. Each MAG keeps a handover neighbor cache that contains all MNs attached to the neighbor MAGs. This cache is updated by control messages when the MNs move from one place to another.

Figure 2.2 gives detail description of the handover neighbor concept. When the MN is linked with the MAG1, it announces MN information to its adjacent MAGs i.e MAG2 and MAG4. When MN moves near to MAG2 it is linked with MAG2, it then announces MN information to MAG1, MAG3, and MAG4 and so on.

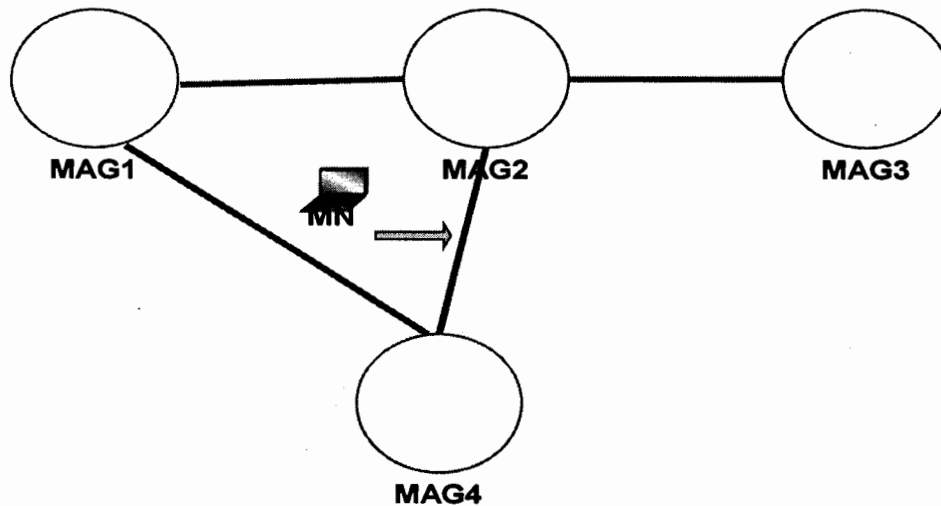
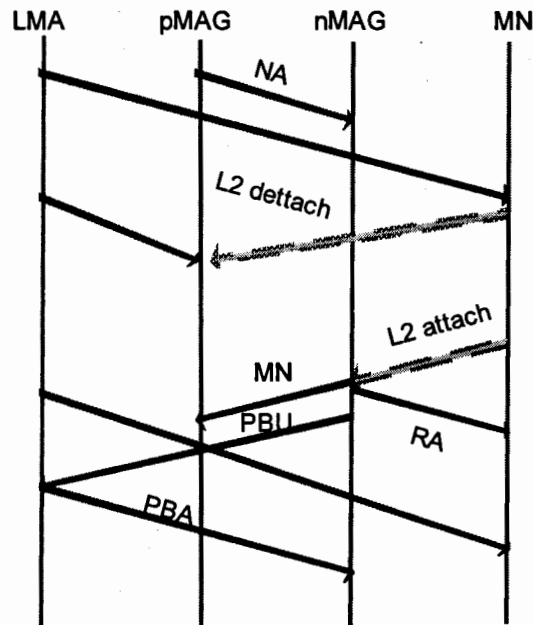


Figure 2.2 Handover neighbor MAGs

Using the idea of neighbor MAG collaboration the new MAG obtains information about MN before the actual handover. Therefore MN obtains fast router advertisement eliminating authentication and default router reconfiguration delay during the handover process. Upon the receipt of fast router advertisement the MN can communicate with LMA.



**Figure 2.3 Handover neighbor MAGs signaling flow**

Fast handover with neighbor MAGs is an efficient approach towards reducing handover delay. This scheme eliminates the MN authentication delay during the handover process. It also prevents the packet loss by using a tunnel between the new and previous MAGs.[2]

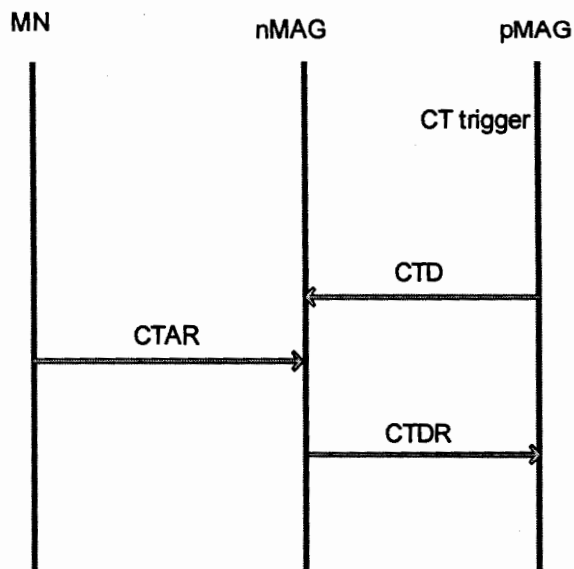
Like the Fast PMIPv6 scheme this scheme also does not consider the MAG authentication delay. In addition the traffic is forwarded to MAG before the binding registration (PBU, PBAck) are completed.

### 2.2.3 Context Transfer scheme for PMIPv6.

This scheme proposes a method to transfer the AAA context information about a MN from pMAG to the nMAG in advance. The AAA information includes authentication information (e.g. MN-identifier, shared secret key), authorization information (e.g. a list of authorized services by the network), and accounting information. (e.g. usage record of resources and services by MN). When MN attempts to handoff to a nMAG, the AAA context information stored in LMAs and MAGs are used to support the handoff without visiting the AAA server. This scheme proposes the following two methods for context transfer.

#### 2.2.3.1 Proactive Handoff scheme.

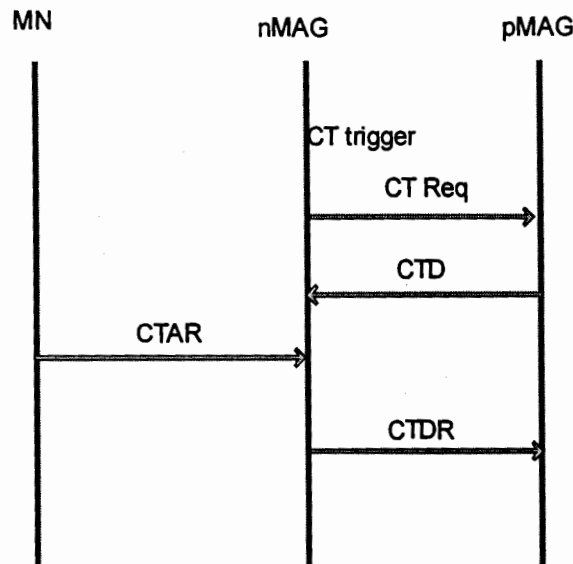
In the Proactive handoff/handover approach the pMAG forwards the context information about a MN to the nMAG before the MN attaches to the nMAG. The pMAG receives information about the nMAG through predictive handoff (link layer ) trigger. It is assumed that the MAGs that may exchange these information have preconfigured security associations. Figure 2.4 shows detailed signaling call flow of proactive handoff scheme. When the pMAG sends a context transfer data (CTD) message to the nMAG in response to context transfer(CT) trigger. This message contains the MN previous IP address and some other parameters. The MN sends a context transfer activate request (CTAR) message to the nMAG before the handover. The nMAG then response to the pMAG with context transfer data reply (CTDR) message to complete this process.



**Figure 2.4 Proactive handoff scheme**

### 2.2.3.2 Reactive Handoff Scheme.

This scheme uses slightly different approach than the proactive handoff scheme. In this scheme when MN gets attachment to the nMAG, the nMAG sends Proxy Binding Update(PBU) message to the LMA, the LMA replies with Proxy Binding Update Acknowledgment(PBUA) message which contains the IP address of the pMAG. The nMAG then sends a Context Transfer Request (CTReq) message to the pMAG. The CTReq message is generated by the nMAG when it receives a context transfer trigger. In the CTReq message, nMAG provides the MN's previous IP address, the sequence number from the CTAR, and the authorization token from the CTAR. The pMAG sends a Context Transfer Data (CTD) message as a response to the CTReq message. When the nMAG receives a CTD message, it sends CTD Reply (CTDR) message to confirm the reception of context transfer.



**Figure 2.5 Reactive handoff scheme**

Proactive scheme retrieves the context information before MN is handed over to the nMAG whereas the Reactive scheme retrieves such information after the handover is completed. Context transfer scheme is efficient in reducing the authentication delay by elimination the steps to visit the AAA policy store, However the Proactive scheme introduces delay since the MN will have to wait at nMAG even after attachment until the nMAG retrieves the context information from the pMAG. In addition like the fast handover scheme this scheme also does not consider the MAG authentication delay. [3]

#### 2.2.4 IEEE 802.21: Media-Independent Handover (MIH) based scheme.

This scheme uses link layer intelligence and related information to optimize MN's handover. This is achieved by introducing a media independent handover (MIH) function. The MIHF is

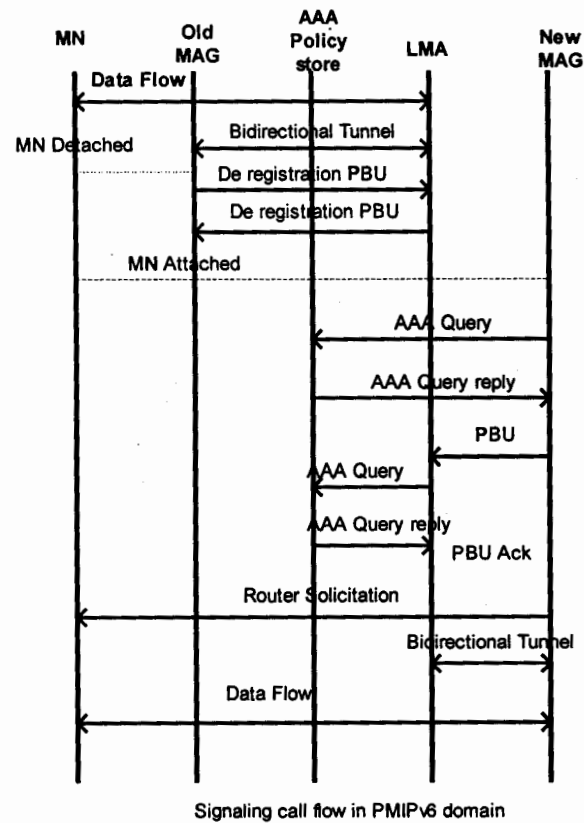
based on the following three functional components that enhance seamless handover across the heterogeneous as well as homogenous networks.

- i. Media Independent Event Service (MIES) continuously reports dynamic changes and events in the lower layer, such as, link up, link down, link state changes and predictive events to upper layers.
- ii. Media Independent Command Service (MICS) enables the MIH users to control and manage the behavior of the link for making connectivity decisions in case of handover and mobility.
- iii. Media Independent Information Service (MIIS) provides static and dynamic information about characteristics and services offered by current and neighboring networks.

The IEEE 802.21 MIH scheme use proactive signaling between the MAG, LMA and AAA server. Using these signaling the MAG authenticates the MN before the handover process. Using the Media Independent Information Element (MIIE) service the nMAG obtains information about other MAGs and MNs from the local MIIS information server.

A list of possible candidate MAGs where a roaming MN can attach based on its (MN) current location is also included in the MIIS server. network information are continuously updated in the information elements of the information server by the MIES service as the environment changes.

Because of the continuous exchange of MIH signaling and messages, any event occurring in the PMIPv6 domain is immediately reported at the MIIS information server [18]. Thus, when a MN is going to hand over from a pMAG to nMAG, the nMAG already have some information about the incoming MN. In fact, nMAG has already performed the access authentication of the MN from the policy store. The updating of the MIIS information is triggered by dynamic events such as MN attachment or detachment from the MAGs among other events. Hence, a new MAG is able to perform fast authentication of the MN with the help of MIH messages before the actual handover [4].



**Figure 2.6 802.21 MIH based scheme**

Although the MIH assisted scheme is efficient that proposes the network based mobility management using the media independent handover capabilities of the 802.21 MIH function but scheme also covers only a portion of the authentication process. That is this scheme also eliminates only the MN authentication delay, The MAG authentication delay is still in this process which further increases the packet loss. For an efficient handover process this authentication delay need to be eliminated.

**2.3 Summary.**

This chapter presented a detail analysis of all the approaches towards optimizing the MN handover between MAGs. We analyzed all the approaches with respect to authentication delay and overall handover process performance. We highlighted the features and limitations of different approaches.





# Requirement Analysis **3**

## 3.1 Introduction

In this chapter we perform an analysis of the Proxy Mobile IPv6 domain. The critical issues that affect the handover of MN/s between MAGs are highlighted. The different events that occur during the handover process of MN are pointed and compared against the performance of mobility management. To improve the performance we have explained our proposed solution.

## 3.2 Problem Statement.

In Mobility supported networks the authentication plays very important role to provide the identity of an entity that is requesting for some service. The main idea behind authenticating an entity is to verify that the user is actually who they say they are. In PMIPv6 authentication of the MN and MAG (mobile access gateway) is performed to make sure that they are the authorized components to use some service in the PMIPv6 domain.

When a MN enters into a PMIPv6 domain it presents its identifier to the MAG. This is the first step to access the network. On the basis of this identifier the MAG sends a AAA Query message to the AAA Policy store to check the authorization of the MN and retrieve other network related information for accessing the network. The MAG then creates and forwards a binding update(BU) message to the LMA which is the topological anchor point. When the LMA receives this message the it also sends a AAA (accounting, authorization, authentication) Query message to the AAA Policy store to ensure the identity of the MAG. This process is repeated each time the MN is handed over to another MAG in the PMIPv6 domain. Before the completions of these

authentications the MN cannot communicate with that particular MAG. Therefore the authentication causes delay during each handover within the PMIPv6 domain.

When a MN has to switch from from current MAG to a new MAG in PMIPv6 domain it has to face the following layer2 (L2) and layer3 (L3) handover tasks:

channel scanning ( $T_{scan}$ ), authentication( $T_{auth1}$ ), reassociation ( $T_{reas}$ ), proxy binding update( $T_{PBU}$ ),MAG authentication( $T_{auth2}$ ),proxy,duplicate address detection check( $T_{DAD}$ ) binding acknowledgement( $T_{PBA}$ ),Router advertisement( $T_{RA}$ ). Therefore the overall handover delay may be given as

$$T = T_{scan} + T_{MNauth} + T_{reas} + T_{PBU} + T_{MAGauth} + T_{PBA} + T_{RA}$$

Among these steps the duplicate address detection check is avoided because proxy mobile IPv6 uses a per mobile node prefix model. Per MN prefix model gives unique home network prefix to each mobile node. PMIPv6 also proposes shared MN prefix in which the duplicate address check is performed only one when the MN enters into the PMIPv6 domain. However among these steps the authentication causes significant amount of delay. It takes approximately 40 to 50ms to authenticate the MAG.To improve handover process in PMIPv6 network the,like the MN,the authentication of the MAG must also be performed before the actual handover process, thus enhancement is needed.

### 3.3 IEEE 802.21Media Independent Handover (MIH).

The IEEE 802.21 Standard working group was started in 2004, and the IEEE-SA Standard Board accepted its latest version as new standard in 2008,The IEEE 802.21 working group introduced the first standard for handling smooth handovers in both heterogeneous and homogeneous networks, called Media-Independent Handover (MIH).The standard allow mobile users to handover within the same network or between two networks smoothly. It

provides an architecture for efficiently discovering networks within the range of a mobile node and undergoing intelligent homogeneous and heterogeneous handovers, based on underlying network capabilities and current link conditions.

### **3.3.1 The Need of IEEE 802.21 Media Independent Handover (MIH).**

The scope of the IEEE 802.21 MIH standard is to provide a general architecture that provides link layer intelligence and other mobility related network information to upper layers of the protocol stack to optimize handovers of MNs between heterogeneous and homogeneous media. This contains links used by 3GPP, 3GPP2 and both wired and wireless media in the IEEE 802 family of specifications.

The IEEE 802.21 can support handovers for both mobile and stationary nodes/users. In case of mobile nodes/users handovers may occur due to a change in wireless link conditions i.e link down, up etc. Whereas for the stationary nodes/users handovers will occur when the surrounding conditions around them changes, in which one network is more feasible than the other. The node/user may select an application which requires handover to a higher data rate channel, for example to download a huge file of data. It is important that the handovers should not affect the MN session continuity, to minimize the interruption in service.

The IEEE 802.21 standard is based on the collective use of both mobile nodes and underlying network. Due to the use of IEEE 802.21 the mobile node is capable to collect information about the available networks, and the network is to store overall network information, such as neighborhood base station list and the location of mobile devices. In general, both the mobile nodes and the network point of attachments such as base stations or access points can be multimode, i.e. supporting different radio standards. And may be in some cases being capable of transmitting on more than one interface at the same time.

A network may contain two types of cells, micro cells (IEEE 802.11 or IEEE 802.15 coverage) and macro cells (3GPP, 3GPP2 or IEEE 802.16) and these will in general intersect. The

handover process of MN is typically based on the triggers received from the link layers on the terminal.

The IEEE 802.21 framework provides the network discovery and selection facility by exchanging network information that helps mobile nodes determine which networks are in their range. This information may include information about the link type, the link identifier, link availability and link quality, network services etc. of surrounding network links. This process of network discovery and selection enables a mobile node to connect to the most appropriate network that can fulfill its requirements. As the mobile node moves between different network Points of Attachment (PoA), proper security associations between the communicating end-points is necessary. These security associations can be obtained both via lower layer and higher layer mechanisms which are supported by IEEE 802.21.

### **3.3.2 Media Independent Handover Function (MIHF).**

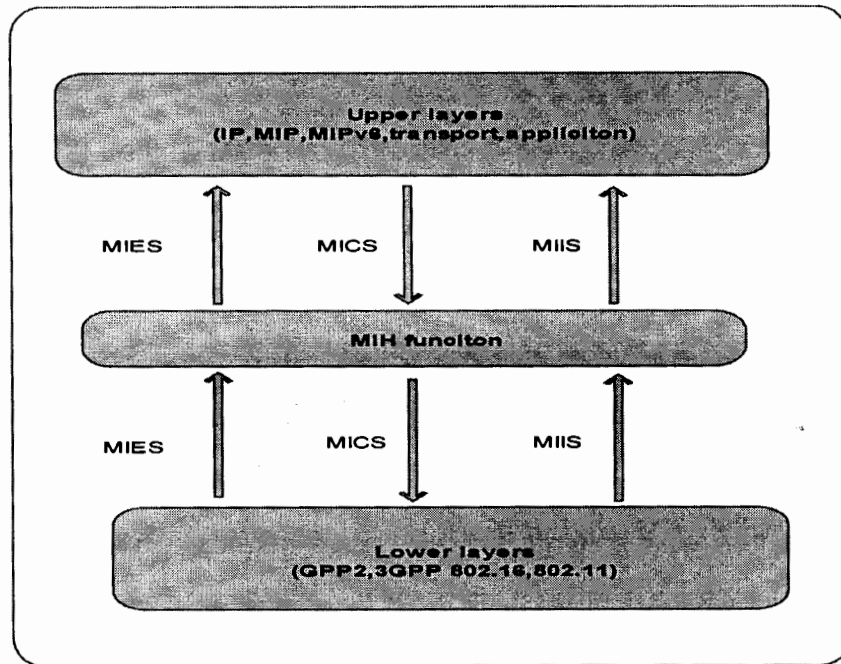
IEEE 802.21 provides support for both network and host based mobility management. This is provided by using a media independent handover function (MIH). The MIH function defines the tools that exchange information, events and commands to support the handover process of MN nodes. It forwards lower layer and other network information to the protocol stack upper layers to handle network and mobility management. These services are offered by Media independent handover function (MIH) which has the following three elements.

1. Media Independent Event Service (MIES)
2. Media Independent Command Service (MICS)
3. Media Independent Information Service (MIIS)

1. Media Independent Event Service: The MIES shows that events that cause changes in the link such as the status and quality of the dynamic link. MIES events are actually

changes in the state and behavior of the lower layers i.e physical, data link and logical link layer. These events may be divided into two groups i.e. link events and MIH events. Link events are generated by lower layers and forwarded to upper layers. Whereas the MIH events are generated by MIH function. Events notifications are forwarded to the MIH function or an entity may be located in the upper layers. The upper layers then register these events and react accordingly.

2. **Media Independent Command Service.** The main function of the MICS is to control the behaviour of linkr such as scanning and configuration. MICS contains those commands that controls the state of the link. These commands are called by MIH function or MIH users. The receiver of is located in the protocol stack that generated the command. Commands may be of two types i.e local or remote.local and remote commands are generated by local and remote entity respectively. Local commands are forwarded from MIH user to the MIH function and then from MIH function to the lower layers. Remote commands are forwarded through the messages of MIH protocol responsible for controlling link behavior such as scanning configuration etc.
  
3. **Media Independent Information Service.** MIIS provides a mechanism for the MIH elements to obtain information in order to make a decision for handover. The MIIS may be used by any component to obtain some specific information (network types, resources etc) about networks within a coverage area to perform a successful handover. In a situation where the information required is not available locally, the MIH protocol uses remote information sources. These information may be used in another network component knows as information server as in proxy PMIPv6. These informations are maintained in Accounting, Authorization, and Authentication (AAA) server.



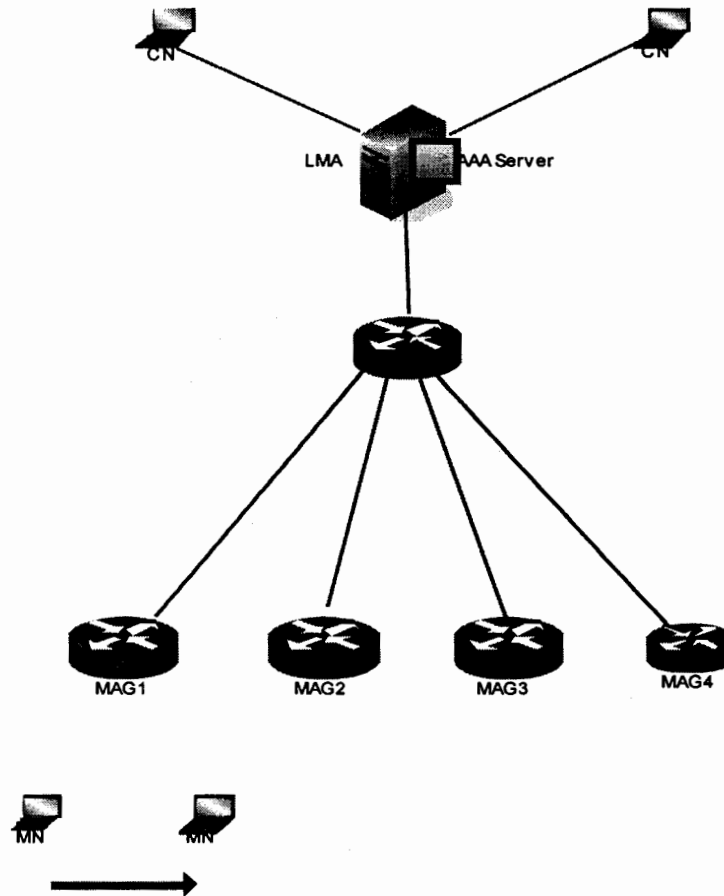
**Figure. 3.1 Location of MIH function**

Figure 3.1 gives a general architecture of the MIH function and its three components. The MIHF is a logical component which exists both on MN and on the underlying network. Triggers are generated to exchange information locally within node's protocol stack, whereas MIH specific messages are used to exchange information between a network entity and MN.

### **3.4 Improved Authentication Scheme of Proxy Mobile IPv6 (IASPMIPv6).**

Improved Authentication Scheme of Proxy Mobile IPv6 (IASPMIPv6) is based on the same Media Independent Handover Protocol. The basic idea behind the authentication of the MN and MAGs in the PMIPv6 domain is to provide the identity of the MNs to the MAGs and that of MAGs to the serving LMA. If the authentication is performed on each individual visit then the effect of authentication on the handover process is required to be reduced.

IASPMIPv6 is based on the same idea of forcing the MAG and LMA to perform authentication each time a MN visit another nMAG.



**Figure 3.2 Proxy Mobile IPv6 Network**

The IASPMIPv6 scheme uses the IEEE 802.21 media independent handover function services. This scheme actually performs the authentication of MAGs before the actual handover process therefore reduces the handover delay.

In the very beginning when a MN enters to the PMIPv6 network it is registered to the MAG through MIHF of the MN. After registration MN sends events notifications such as L2 triggers to the MAG. In addition MAG also collects information about other nearby MAGs to which the attached MNs is expected to handover in the near future. The serving MAG collect these



information by sending Media Independent Handover get information request (MIH\_Get\_Info\_Req) message to the Media Independent Information Server (MIIS) which replies with the Media Independent Handover get information response (MIH\_Get\_Info\_Res) message. When the status of the link between MN and serving MAG changes and the signal strength becomes weak, the MIES of MAG receives Media Independent Handover link going down request (MIH\_Link\_Going\_Down\_Req) trigger from the MN. The MAG performs a search of its cache to collect information about neighbor MAGs on which the MN will perform scanning. This information is passed to MN through the Media Independent Handover link action request (MIH\_Link\_Action\_Req) message. When the MN completes scanning, the current MAG starts to get information for the selection of target MAG. MAG sends Media Independent Handover node to node handover query resource request (MIH\_N2N\_HO\_Query\_Resource\_Req) message to the target MAG. The target MAG replies with MIH\_N2N\_HO\_Query\_Resource\_Res message. On the basis of these information obtained the current MAG decides handover of MN and selects a new MAG (nMAG).

When the handover decision is made, pMAG requests the handover to the nMAG by sending Media Independent Handover node to node handover commit (MIH\_N2N\_HO\_Commit) request. The nMAG replies to the request and obtains MN's profile information from the AAA policy(MIIS Server) store which is used as function of the LMA by the exchange of Media Independent Handover get information request (MIH\_Get\_Info\_Req) and MIH\_Get\_Info\_Res message with MIIS server. At the same time the nMAG send Handover Initiate (HI) to MIIS. The MIIS verifies the identity of the MAG and replies with Handover Acknowledge (HACK) indicating successful pre-registration. Since pre-registration is successful, nMAG may now include MN's HNP to the router advertisements sent on its link. When the nMAG receives the link up trigger it sends the proxy binding update message to the LMA on behalf of MN. The LMA updates binding cache entry establishes a tunnel and sends proxy binding acknowledgment (PBA) message to the MAG. The MAGs exchange messages with the LMA/MIIS server before the actual handover process, it is therefore already known to the LMA and no checking is required when it sends the BU message.

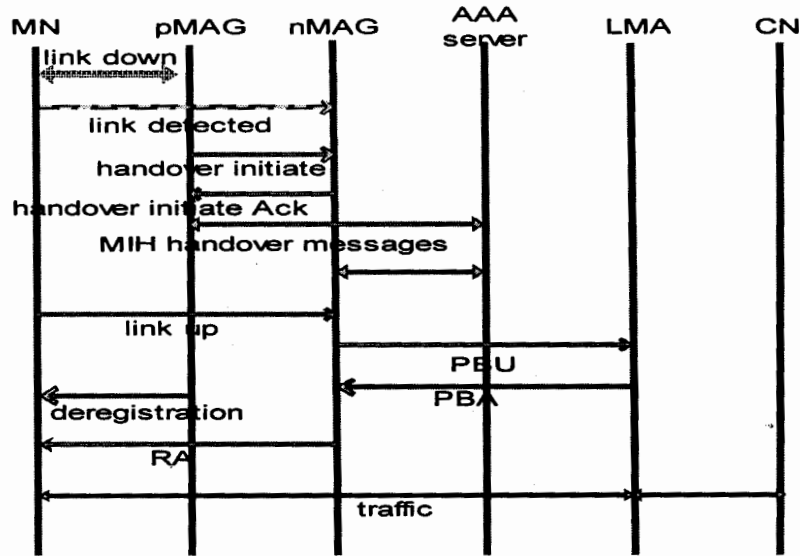


Figure 3.3 Signaling call flow

Upon the receipt of PBU the traffic is forwarded to the MN. The format of the Proxy Binding (PBU) Update message is as under.

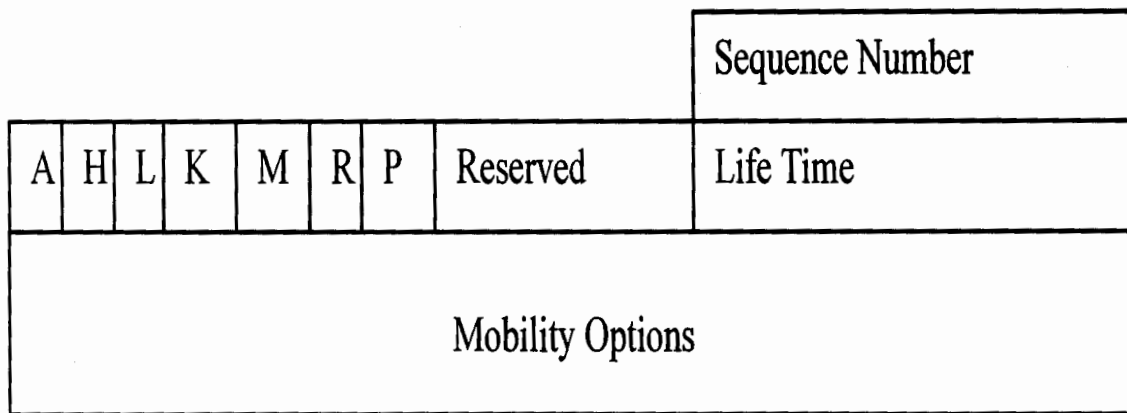
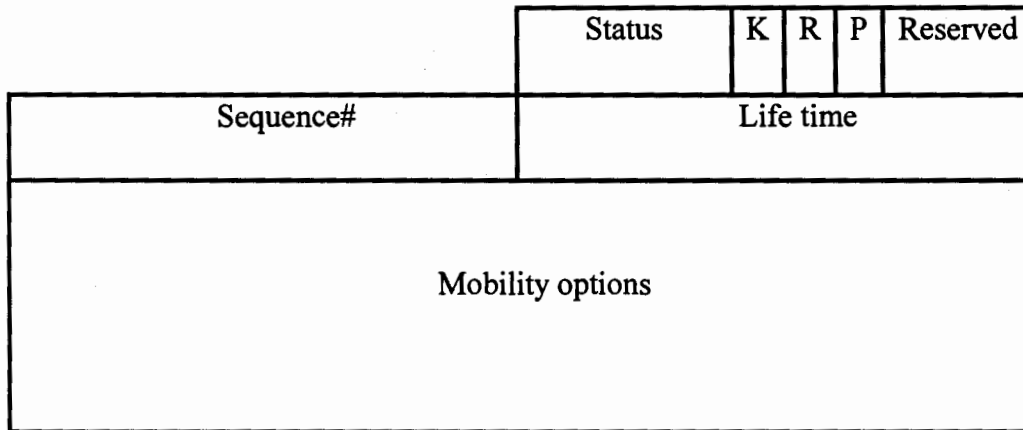


Figure 3.4 Binding Update Message.

A new flag (P) is included in the BU message to indicate to the LMA that the BU message is a proxy registration. This flag is set 1 for proxy registrations and to 0 for direct registration sent by a MN.

The format of the Proxy Binding Acknowledgment message is given as



**Figure 3.5. Proxy Binding Acknowledgment Message**

The LMA maintain a Binding Cache entry for each currently registered MN. That contain a flag to see that whether this Binding Cache entry is created due to a proxy registration, MN Identifier, The link-local address of the MAG on the point to point link shared with the MN, the access technology type, by which the MN is currently attached and the 64-bit timestamp value of the most recently accepted PBU message sent for this MN.

### 3.5 Summary.

In this chapter we studied the Proxy Mobile IPv6 handover process. The different events that occur in the MN handover process are discussed. The measured the affect of authentication delay

on the handover process. Finally we presented our proposed scheme for the elimination of MAG authentication delay in the handover process.

7/18/17

# Simulation

# 4

## 4.1 Introduction.

Simulation is the method of designing a model of a real world system for the purpose of understanding those events which will affect the present and future behavior of the system. Simulation is performed when the actual real world test of a system or process are costly, difficult, dangerous, time consuming or impossible due to some reason. The important issue in the design of real world network environment is providing connection between components in wired and wireless domains. We design such environment using the network simulator (NS2). This chapter provides information about our proposed simulation tool, goals of simulation, model of simulation, simulation scenario and finally simulation setup for different tests.

## 4.2 Simulation Tool.

We have used Network Simulator V2.29 (NS 2.29) for our simulation. NS is the most widely used simulation tool for performing simulation of network environment both wired and wireless.

Network Simulator (NS 2) is a discrete event object-oriented simulator. The development of NS2 started in 1989. Nowadays many version of this are available such as NS 2.27, NS 2.28, and NS 2.29.

The back end of NS 2 is designed in object oriented language C++, whereas the front end of this is modeled in object oriented Tcl. The network topology is designed by writing OTcl scripts, NS 2

then performs the simulation of that topology with the given parameters. NS 2 can be run on Linux, Solaris and even on Microsoft windows with the help of Cygwin Software.

The use of C++ in NS2 provides the facility for developers to perform detailed simulations of different routing protocols, effective use of packet headers, bytes, and algorithms particularly designed for larger data sets. Otcl enables the developers to use different simulation configurations and parameters, or exploring configuration setups for various scenarios.

### 4.3 Mobility support in NS2

The original NS2 provides mobility support only for the basic Mobile IP protocol. It is extended by different researchers or communities according to their works. These extensions are openly available for research purposes. In the beginning most of the contributed codes and modules were designed for a specific version of NS2 and later on updated for most recent versions of NS. Currently all versions of NS 2 provide the initial mobility support for MN. NS 2 provides two mechanisms to produce movement in MN. In the first case, initial position of the node and its destination point may be given. In the second case the node movement is updated by triggers whenever the position of the node at a given time is required to be known. The mobility components for a MN consist of link layer(LL), ARP module connected to LL, interface priority queue(IFq), mac layer(MAC), and a network interface(netIF). All of these are connected to the channel. Otcl is used to create and combine these components.

### 4.4 The AWK language

The term AWK is derived from the names of its authors; Aho, Kerninghan and Weinberger, it is a programming language used by many researchers for retrieving information from text and data files.

The main feature of AWK is that complex text processing tasks can be done in a very short period of time with few instructions. AWK programs mainly work on the idea of pattern matching. The program scans a document looking for a pattern match and when found it performs the action.

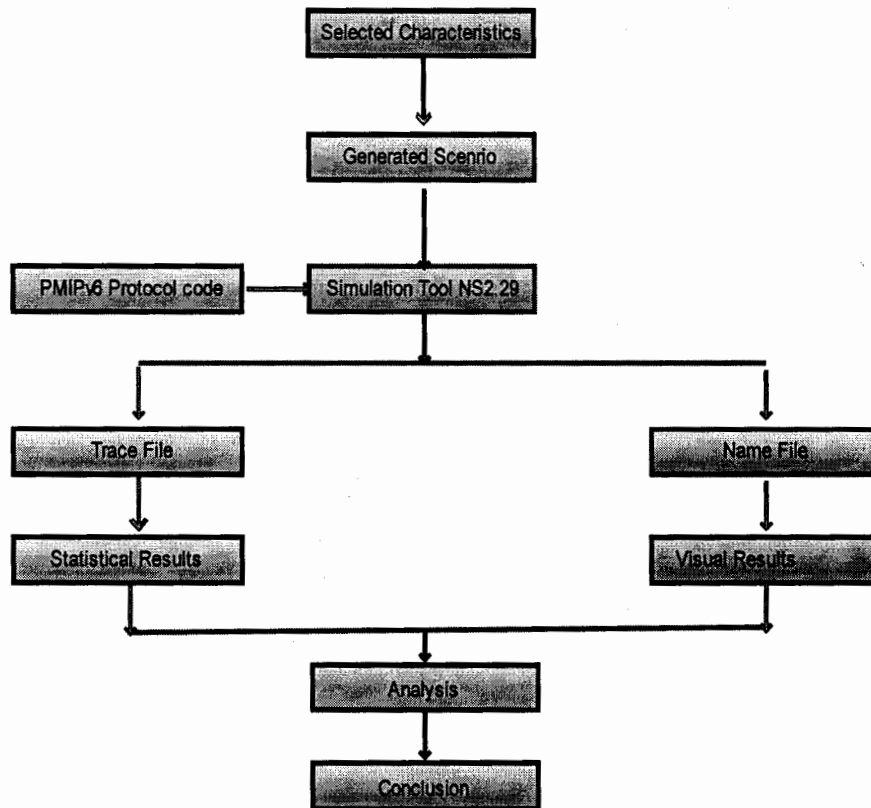
#### **4.5 Simulation Goal.**

Our proposed network based mobility management scheme performs the authentication of the MN and MAGs of the PMIPv6 domain before the actual handover from one MAG to another MAG takes place. Therefore this scheme improves the handover performance as compared to the host based approaches.

This scheme also improves the performance of the networked based mobility management with reference to the heavy packet loss. In the existing scheme no attention is given to minimizing the loss of packets during exchange of data as well as loss of packets during the handover process. The scheme significantly reduces the packet loss at all time during movement of a MN within a PMIPv6 domain; this increases the throughput and hence improves the performance.

The existing schemes proposed many signaling messages in media independent handover function for mobility management which overloaded the components of the network, the scheme also eliminates the use of such extra signaling messages and hence reduces the load on the network.

We have assessed the performance of our scheme by comparing the results of our scheme against the traditional PMIPv6 schemes, through NS-2 simulation using the following PMIPv6 scenario.



**Figure 4.1 Implementation of Simulation**

#### **4.6 Model of Simulation.**

The Proxy Mobile IPv6 (PMIPv6) software is used to study the simulation. This software is available for ns 2.29. The software provides a general architecture for studying network based mobility management.

PMIPv6 simulation model presents LMA and MAGs as its main components. The LMA is the central component of the PMIPv6 domain and also is the mobility anchor point for any MN.



At the lower level are the MAGs which are actually the base station nodes that handle signaling for the given MN. The MNs are wireless nodes and freely move within the PMIPv6 domain. A hybrid topology composed of wired and wireless nodes are used in our simulation. Following are the main components of PMIPv6 simulation model

### **Local Mobility Anchor (LMA)**

In PMIPv6 domain LMA performs the same function as that of the home agent used in the mobile IPv6 domain. It keeps the MN binding state. It has also the responsibility of keeping the MN global reach ability and routing state. The LMA creates a binding cache for each of the currently attached MN. This cache is updated by PBU, and PBUA messages when the MN executes a handover from one MAG to another. This binding cache contains information such as the identifier of the attached MN, the MN home network prefix, the flag indicating the proxy registration, and the identifier for the tunnel between LMA and MAG.

In general the Local Mobility Anchor (LMA) perform the following tasks:

**MN registration:** The LMA maintain information for the MN's in its cache.

**MAG registration:** When MAGs boot up Proxy Mobile IPv6 domain they register themselves with the LMA. The LMA should check if the MAG is part of its domain whenever it receives the Proxy Binding Update message for the the MN from the MAG.

**Binding update processing:** PBU request messages coming from MAGs should be checked and processed if valid.

**Acknowledgment generation:** In response to the PBU message, the LMA generate Proxy binding Update Acknowledgments (PBUA message) and sent.

**Forwarding MN traffic:** The LMA is the entity that is responsible for the MN's home address processing. All traffic for and towards the MN passes through this node.

**Mobility Access Gateway (MAG)**

MAG is used as function on the access router(AR) it manages the mobility related signaling for the MN. It is also responsible for the detection of MN movements in the PMIPv6 domain.

It performs the following major tasks:

**Registration to LMA:** When the MAG boots up it should register itself with the LMA.

**MN registrations:** MN register itself with the with the MAG for traffic forwarding.

**Sending Binding Update Requests:** Mobility updation message (PBU) for the MN.

**Handover coordination:** The MAG is responsible for handover coordination.

**Router**

The router is the device that delivers the traffic received from LMA to the appropriate MAG.

**Correspondent Node (CN)**

Correspondent node is the traffic source. It generates traffic which is transmitted to the MN through LMA and MAGs

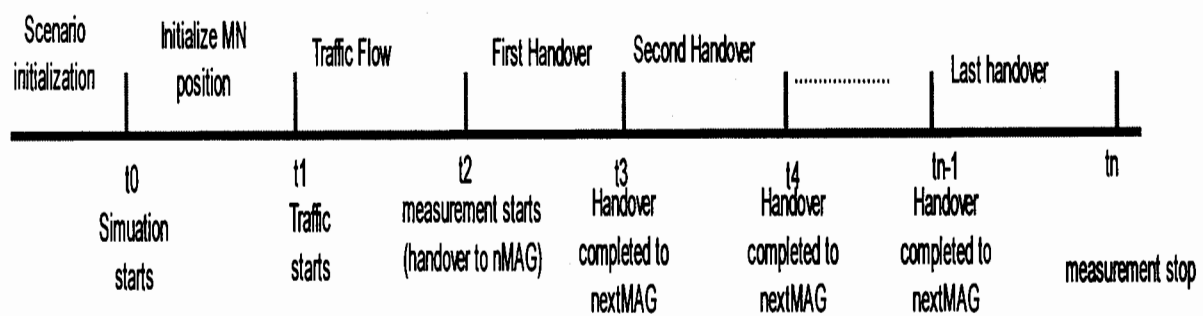
**Mobile Node (MN)**

It is host that that moves within the PMIPv6 domain and receives the traffic generated by CN. It is not involved in the mobility related signaling because the PMIPv6 network manages the mobility itself.

**AAA server**

The AAA server is implemented as function on the LMA. It contains information about all the entities in the PMIPv6 domain.

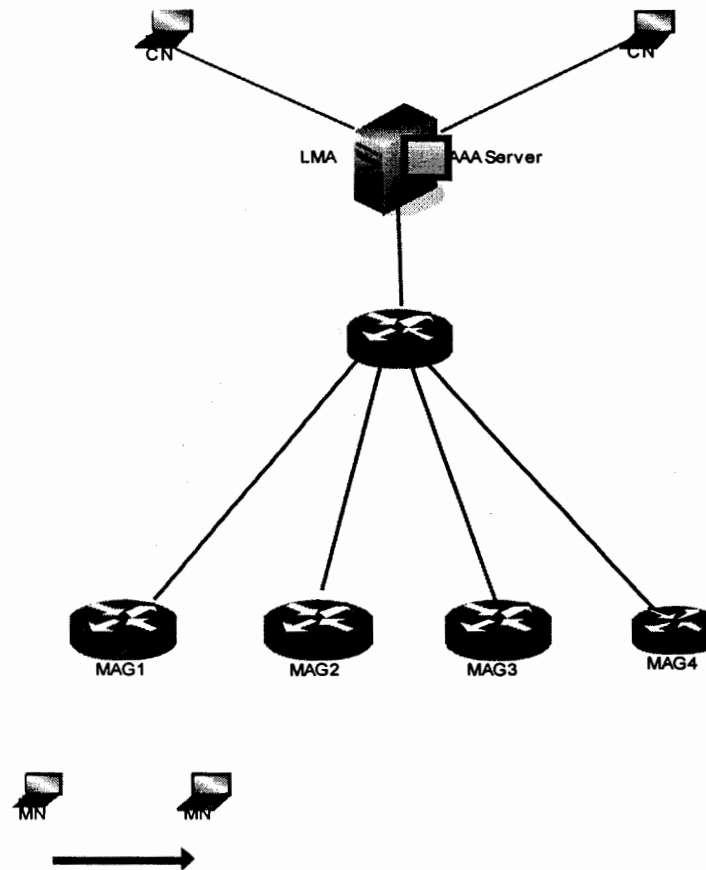
For comparing the proposed scheme with the existing schemes the simulation was carried out using the same platform. The flow of events may express as follows.



**Figure 4.2 Sequence of events for MN**

#### 4.7 Simulation Scenario.

The figure given below represents our simulation scenario. It shows a real world picture of the PMIPv6 network. There may be different configuration of this network, but all will work in the same manner as the following topology shows.



**Figure 4.3 Proxy Mobile IPv6**

**Detail of simulation scenario.**

There are two part of this topology the wired and wireless forming a hybrid topology. The wired portion of this topology connects the nodes in a hierarchal fashion. It connects the LMA router and MAGs in a top down manner. The correspondent node which is the traffic generator is outside of the PMIPv6 domain.

The MN moves in the PMIPv6 domain and obtains an access link from the MAGs. The simulation completes with recording all the information in an output file.

#### 4.8 Research Methodology

This section discusses the detailed setup of our simulation. Three different experiments were performed for each scheme. In the first experiment we studied the effect of increasing handover, the second experiment was conducted for studying the effect changing link delays and the third experiment was performed to study the effect of mobile node speed. In each of this experiment we measured, handover delay, packet loss, one way delay and the throughput ratio. The main tools used for simulation are, the network simulator 2(NS-2), AWK scripts, Red hat Linux, Intel processor 1Ghz, and 512Mb of RAM. The following table shows the parameters used in this simulation.

Variables	Values
Simulation Tool	NS 2.29
Propagation Model	Two Ray Ground
Antenna Type	Omni Directional
MAC Type	802.11 MAC
Interface Queue	Wireless Phy
Interface Queue Length	30
Topology Size	1600 X 1600
Transport Protocol	UDP

Packet Size	1000
Traffic Type	CBR
Queue Type	Drop Tail
Wired Link Type	Ethernet
Wired Link Speed	100Mbps
Wireless Link	IEEE 802.11
Wireless Link Speed	1Mbps
Routing Protocol	DSDV
Protocol Agent	PMIPv6
Number of MN	2
Number of CN	2
Simulation Time	36 Sec

**Table 4.1 Parameters of simulation**

#### **4.8.1 Experiment for increasing handovers.**

In this experiment we study the effect of increasing number of handovers on handover delay, packet loss, One-way delay and the throughput ratio. Table shows the detail where we shall keep the other entire parameters constant and increasing only the number of handovers.

Variable	Values
experiment	Increasing handover
Number of handovers	1,2,3,4
Link delay	10ms
MN speed	20m/s
Number of tests	4

**Table 4.2 Parameters**

#### 4.8.2 Experiment for testing the effect of Link Delays

This experiment was carried out to study the effect of changing links delays. The experiment was performed for both the existing schemes and proposed scheme. The detail of this experiment is given in the table below. The experiment was repeated for the values of 10-50 link delays, keeping all other parameters constant. The results were obtained for both the existing and proposed schemes and the performance was compared.

Variables	Values
Experiment	Effect of changing link delays
Link delay	1,5,10,15,20
Mobile Node Speed	50 m/s
Number of tests	5

**Table 4.3 Parameters**

### 4.8.3 Experiment for the Mobile Node speed

This experiment was performed for analyzing the MN speed variation on the performance of our proposed scheme. The speed of 30-70 meter per second was given to the mobile node in the PMIPv6 domain and its effect on the performance was recorded.

Variables	Values
Experiment	MN speed testing
Link Delays	10ms
MN speed	30,40,50,60,70 m/s
Authentication time	40ms
Number of tests	5

**Table 4.4 Parameters**

### 4.9 Summary

In this chapter we provided details about our simulation and experimentation, goals and model of simulation, scenario and the flow of events. Also we have discussed about the required entities and their characteristics for our simulation. Furthermore, we have given a detail study about the simulation setup for the assessment of performance optimization of our proposed scheme.



# Evaluating Performance

# 5

## 5.1 Introduction

In this section we perform an analysis of the results obtained from our simulation. We compare the performance of the existing PMIPv6 schemes and IASPMIPv6 scheme. We have shown our results in graphical form with explanation. Three experiments are performed and in each experiment the results for the handover delay, packet loss ratio, one way delay and throughput ratio have been calculated. The next section describes the details of all experiments.

## 5.2 Elements of performance.

In order to examine the performance of the proposed scheme three major elements were chosen in the simulation. These elements are handover delay, packet loss ratio, average one way delay, and throughput ratio. The results have been collected for these metrics and compared. The results are calculated using the following equations.

### Handover delay.

it is the interval between first packet received by MN through nMAG, and last packet by pMAG. It is calculated as follows

$$\sum T_{nmag} - T_{omag} / N$$

where

$T_{nMag}$  = is the time of first packet by nMG.

$T_{oMag}$  = is the time of last packet by pMAG.

$N$  = is the total number of handover in the PMIPv6 domain.

### Packet Loss Ratio

It is the percentage ratio of the total number of lost packets to the total number of transmitted packets. It is calculated as

$$\text{Packet loss Ratio} = \frac{\sum P_d}{\sum P_t} * 100$$

Where

$P_d$  = is the total number of lost packets

$P_t$  = is the total number of transmitted packets

### One Way Delay

It is the time required for a packet to travel from source to destination node. It can be calculated as

$$\text{Average One Way Delay} = \frac{\sum T_r - T_s}{N_p}$$

Where

$T_r$  = is the time stamp of receiver node

$T_s$  = is the time stamp of sender node

And  $N_p$  is total number of received packets

## Throughput

It is the percentage ratio of received bytes to the sent bytes. It can be calculated as

$$\text{Throughput} = \text{Br/Bs} * 100$$

Where

Br = total received bytes

Bs = total sent bytes

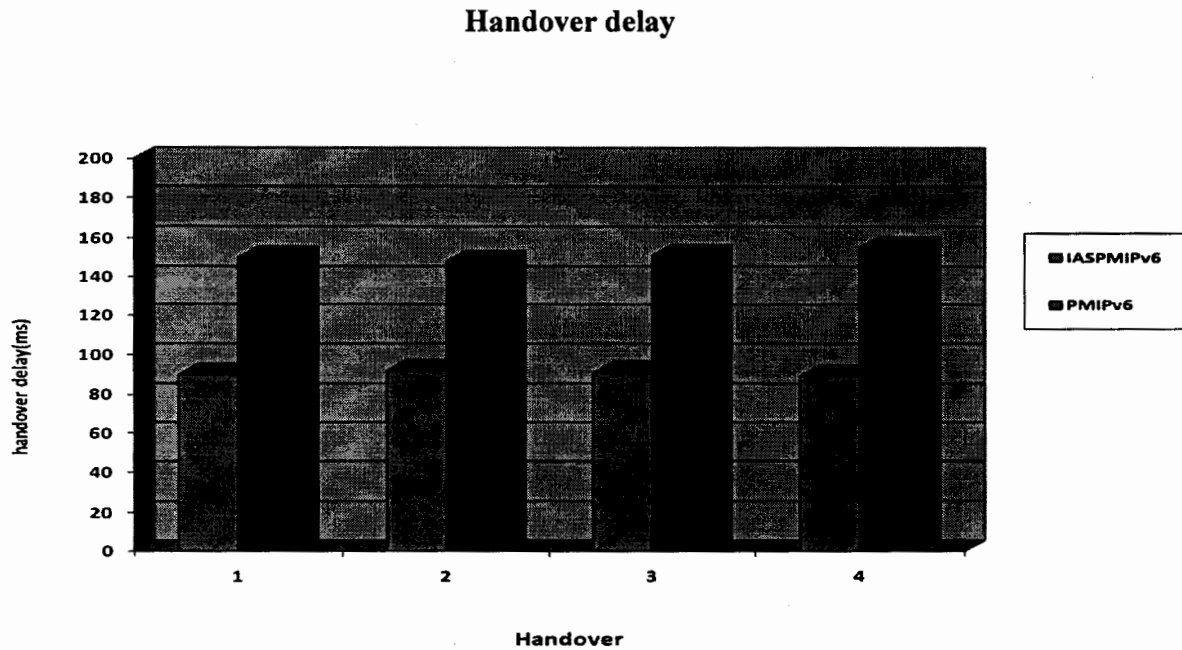
## 5.3 Results

The simulation results obtained for the existing and proposed scheme(IASPMIPv6) are given below.

### 5.3.1 Calculating results for testing impact of handovers.

#### 5.3.1.1 Handover delay

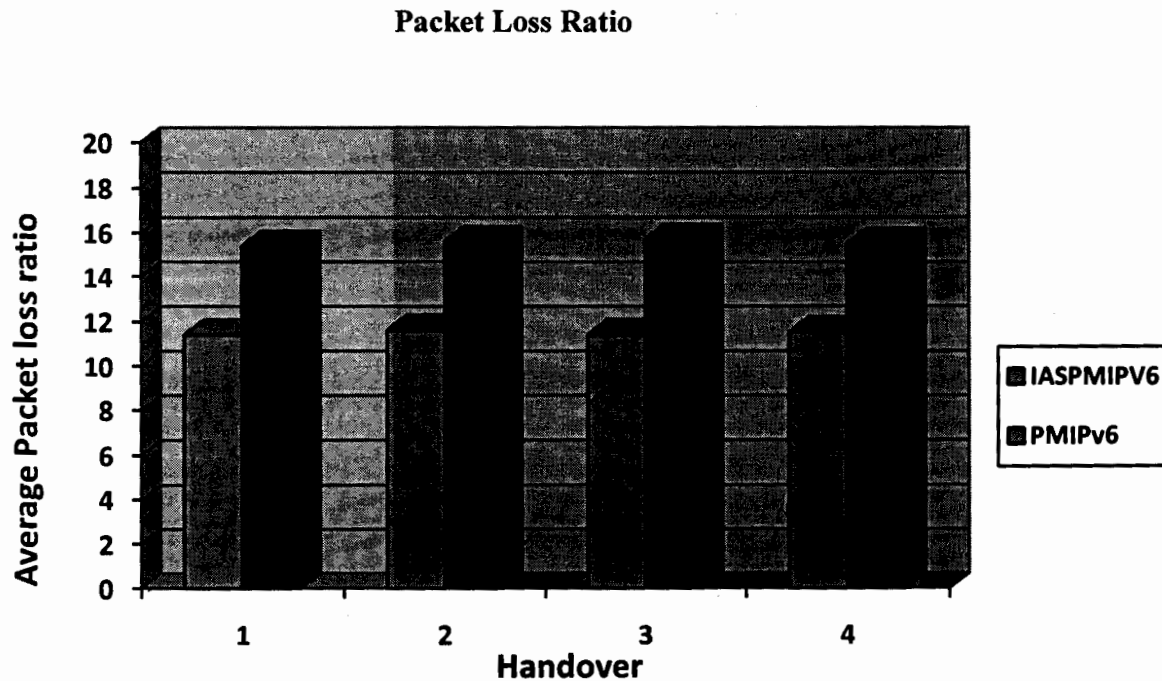
Figure 5.1 provides comparison of the handover delay in both schemes. It is clear from the figure that the handover delay is improved by Improved authentication scheme of Proxy Mobile IPv6(IASPMIPv6) handover process. Increasing handovers between the MAGs places a very minor affect on the performance of IASPMIPv6. In fact the variation in handover delay shows a constant behavior, but the performance of IASPMIPv6 is very significant and predictable.



**Figure 5.1 Handover Delay**

### 5.3.1.2 Packet loss

Figure 5.2 shows the percentage packet loss ratio during each individual handover of the MN. It is clear that the packet loss in the existing PMIPv6 scheme is higher and IASPMIPv6 has reduced this loss to greater extent. Packet loss occurs on each handover as the MN registration process is in progress; hence eliminating the authentication delay in handover time results in lower packet loss.



**Figure 5.2 Packet Loss Ratio**

### 5.3.1.3 One way delay of packets

One way delay of packets is the time taken by a packet to travel from source to the destination node. We checked the one way delay of packets in each of the individual handover. The results are collected under similar conditions. It is clear that both the existing and proposed schemes shows nearly the same behavior.

Average one way delay for PMIPv6= 12.4 ms

Average one way delay for Proposed Scheme= 12.1 ms

### 5.3.1.4 Throughput

The throughput ratio of both the existing and proposed schemes shows that the proposed scheme improves the throughput ratio by 8%. It is due to the fact that fewer packets are lost in the proposed scheme as compared to the existing scheme therefore the performance of IASPMIPv6 is better as compared to the existing schemes.

Throughput Ratio (PMIPv6) = 83.3%

Throughput Ratio (IASPMIPv6) = 88.9%

### 5.3.2 Calculating results for the effect of link delays variation.

#### 5.3.2.1 Handover Delay

The following figure graphically shows the effect of delaying link speed on both the existing scheme and proposed scheme. The handover delay increases as the link speed increases. Both schemes show nearly the same behavior on link speed variation. It is clear from figure that the proposed scheme shows better performance over the existing scheme.

Handover delay

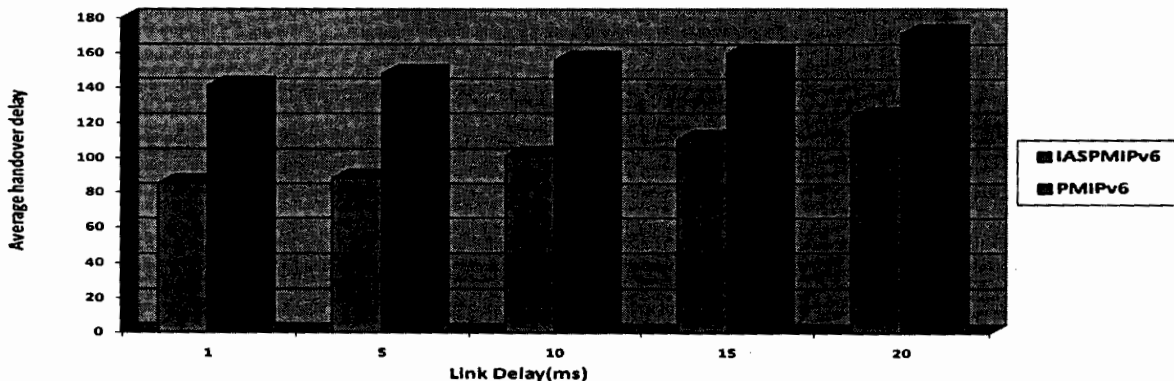


Figure 5.3 Handover Delay

### 5.3.2.2 Packet loss

Figure 5.2 shows a comparison of both the existing and proposed schemes. It is clear from the analysis of the graph that fewer packets are lost in the proposed scheme as compared to the existing scheme. Therefore the performance of proposed scheme is better than the existing schemes with respect to packet loss if the delays of links are changed.

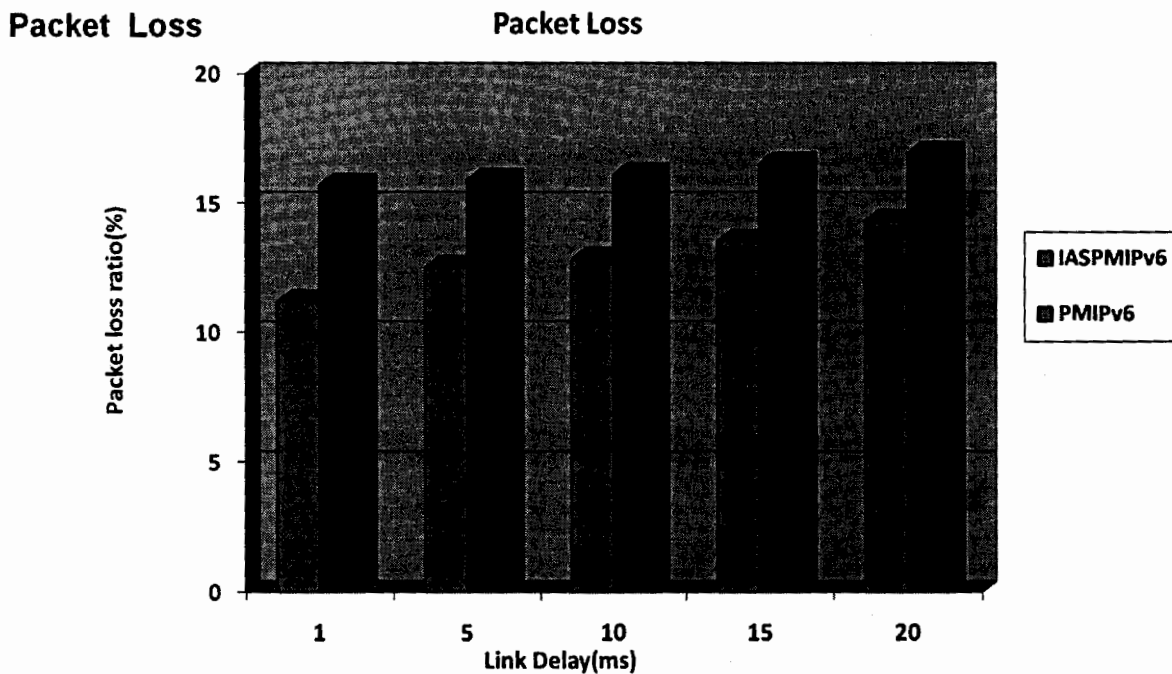


Figure 5.4 Packet Loss

### 5.3.2.3 One way delay of packets

One way delay of packets is the time for a packet to travel from sender to the receiver. If the link speed is reduced then the one way delay increases. When tests are carried out under the similar conditions both the existing and proposed schemes shows nearly the same behavior.

Average one way delay for PMIPv6= 12.4 ms

Average one way delay for Proposed Scheme= 12.1 ms

### 5.3.2.4 Throughput

The throughput ratio of both the existing and proposed schemes is given below. Since fewer packets are lost in the proposed scheme therefore the performance of proposed scheme is better as compared to the existing schemes.

Throughput Ratio (PMIPv6) = 80.1%

Throughput Ratio (Proposed Scheme) = 86.5%

### 5.3.3 Calculating results for MN speed variation.

#### 5.3.3.1 Handover delay

Figure 5.6 shows the effect on changing the MN speed on both schemes. It is clear that MN speed variation has nearly the same effect on both schemes. Both schemes show constant behavior on different MN speeds.

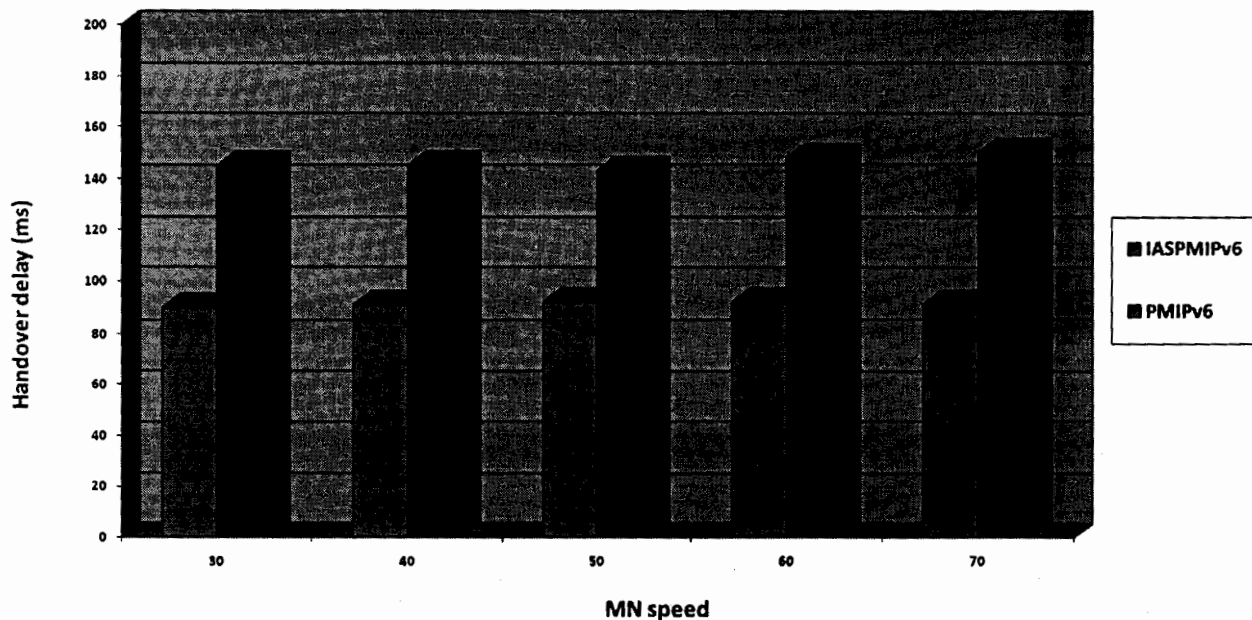
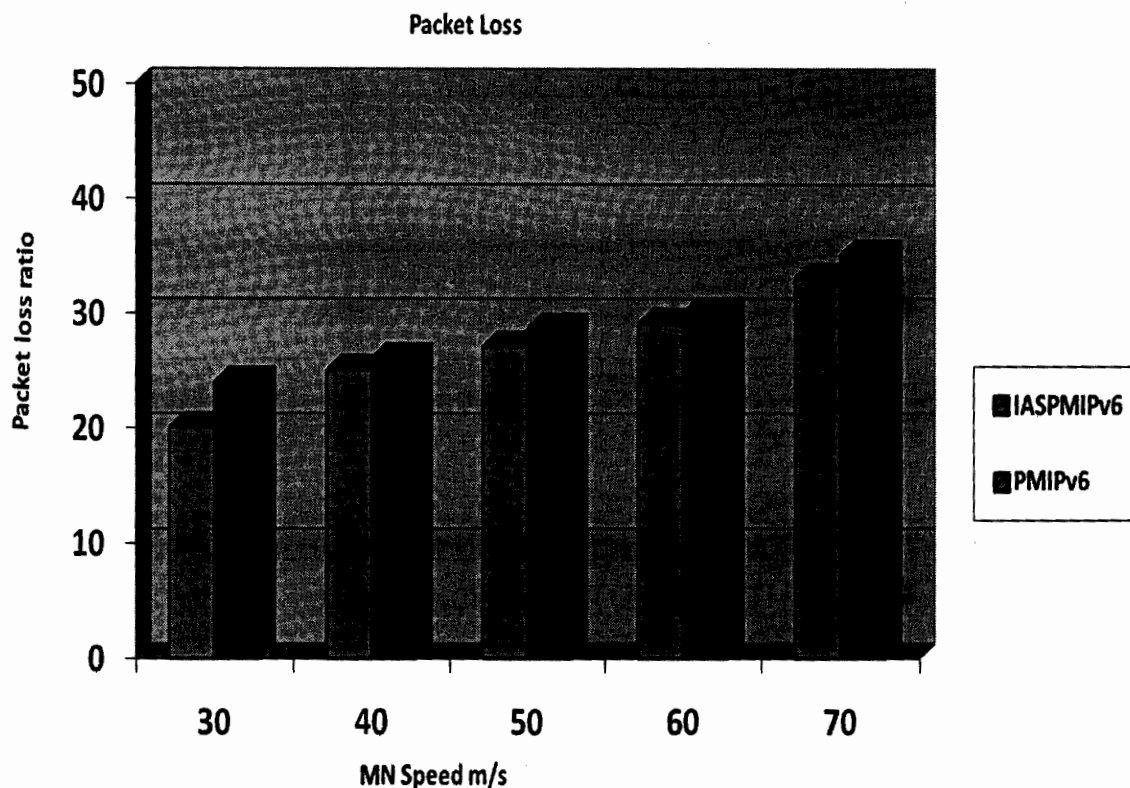


Figure 5.5 Handover Delay



**5.3.3.2 Packet Loss.** The variation of MN speed has nearly the same effect on both the schemes. Figure 5.6 graphically shows the effect of speed changes. It is clear that the effect is same in both cases.



**Figure 5.6 Packet Loss**

### 5.3.3.3 One way delay.

The one way delay of packet for proposed scheme changes in the same manner as the existing scheme when the MN speed varies.

One way delay for PMIPv6 = 12.9ms

One way delay for Proposed Scheme = 12.3ms

#### 5.3.3.4 Throughput

Figure shows the effect of MN speed variation on the throughput of both schemes. It is clear from the results that the proposed scheme gives high throughput for the given MN speeds. When the MN speed changes in the range of 30-40 the throughput ratio for both schemes decreases, however the proposed scheme still gives high throughput ration as compared to the existing scheme.

#### 5.4 Summary.

In this chapter we presented the detail of our simulation results. We have used handover delay, packet loss, one way delay of packets and the throughput as the parameters for testing performance of both the schemes. We have compared both schemes on the basis of these parameters.

# Conclusion 6

## 6.1 Conclusion.

We have proposed improved authentication scheme for the network based Proxy Mobile IPv6 handover process. The scheme uses the IEEE 802.21 media independent services to perform the authentication of MN and MAG before the actual handover process. Therefore it eliminate the delay that occur due to the authentication steps of MN and MAG during handover from one MAG to another in Proxy Mobile IPv6 domain The scheme also reduces the packet loss that occur during handover over. The scheme is limited to single Proxy Mobile IPv6 network administered by a single Local Mobility Anchor. We performed simulation of the scheme through NS2 and analyzed the results. Simulation results showed that the scheme performs better than the other schemes.

## 6.2 Future work.

In the future will We wish to remove the remaining packet loss in the scheme. We want to provide mechanisms between the adjacent MAGs that will forward the dropping packets during handover from pMAG to nMAG in a local Proxy Mobile IPv6 domain. Furthermore we hope to extend the scheme for two local Proxy Mobile Ipv6 domain administered by two different Local Mobility Anchors. We intend to eliminate the same issues between the adjacent local mobility anchors.

**References:**

- [1] Geert Heijenk<sup>1</sup>, Mortaza S. Bargh<sup>2</sup>, Julien Laganier<sup>3</sup>, and Anand R. Prasad “Reducing Handover Latency in Future IP-based Wireless Networks: Fast Proxy Mobile IPv6 ” IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks 2008.
- [2] Sungyeol Kim, Soonmok Kwon<sup>O</sup>, Cheeha Kim “A Fast Handover Scheme for Proxy MIPv6 using Neighboring MAG Collaboration” Institute for Information Technology Advancement (IITA-2008-C1090-0801- 0045) Ministry of Knowledge Economy, Korea.
- [3] JaeJong Baek, JooSeok Song “Adaptive Context Transfer Scheme for Fast Handoff in Proxy Mobile IPv6” The Second International Conference on Next Generation Mobile Applications, Services, and Technologies IEEE 978-0-7695-3333-9 /08/ 2008
- [4] Igor Kim, Young Chul Jung, and Young-Tak Kim “Low Latency Proactive Handover Scheme for Proxy MIPv6 with MIH” APNOMS '08 Proceedings of the 11th Asia-Pacific Symposium on Network Operations and Management: Challenges for Next Generation Network Operations and Service Management Springer-Verlag Berlin, Heidelberg ©2008.
- [5] Marc Emmelmann, Sven Wiethoelter, Andreas Koepsel, Cornelia Kappler, and Adam Wolisz “Moving towards Seamless Mobility—State of the Art and Emerging Aspects in Standardization Bodies” wireless personal communication, springer journal DOI10.1007/s11277-007-9255-6/ 2008.

- [7] S. Gundavelli , V. Devarapalli RFC 5213 Proxy Mobile IPv6 IETF network working group 2008.
- [8] Ki-Sik Kong and Wonjun Lee, "Mobility management for all IP Mobile Networks: Mobile IPv6 vs. Proxy Mobile IPv6" IEEE Wireless Communications, April 2008
- [9] HeeYoung Jung, Eun Ah Kim, Jong Wha Yi, and Hoeing Ho Lee "A Scheme for Supporting Fast Handover in Hierarchical Mobile IPv6 Networks" ETRI Journal, vol.27, no.6, Dec. 2005, pp.798-801.
- [10] HeeYoung Jung and Seok Joo Koh "Fast Handover Support in Hierarchical Mobile IPv6" Advanced Communication Technology, 2004. IEEE The 6th International Conference on Wireless Communications.
- [11] Xavier Pérez Costa, Ralf Schmitz, "A MIPv6, FMIPv6 and HMIPv6 handover latency study: analytical approach" IEEE GLOBECOM 2007' IEEE Global telecommunications Conference 2007.
- [12] Chakchai So-In "Mobile IP Survey"2006 available at <http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.104.487>
- [13] Zhigang KAN, Dongmei ZHANG, Runtong ZHANG, Jian MA "QoS in Mobile IPv6" ICC '02 Proceedings of the 15th international conference on Computer Communication 2002.
- [14] Mortaza S. Bargh, bobhulsebosch, Henk Eertink Geert Heijenk, "Reducing Handover Latency in Future IP-based Wireless Networks: Proxy Mobile IPv6

with Simultaneous Bindings” IEEE WOWMOM '08 Proceedings of the 2008 International Symposium on a World of Wireless, Mobile and Multimedia Networks.

- [15] Jong Hyouk Lee and Tai-Young Chung “A Traffic Analysis of Authentication Methods for Proxy Mobile IPv6” ISA '08 Proceedings of the International Conference on Information Security and Assurance 2008.
- [16] Jung Wook Song, Sun Young Han “One-time Key Authentication Protocol for PMIPv6” ICCIT '08 Proceedings of the 2008 Third International Conference on Convergence and Hybrid Information Technology - Volume 02, 2008.
- [17] Young Song Mun Miyoung Kim “Mutual Authentication Scheme in Proxy Mobile IP” Computational Sciences and Its Applications, ICCSA '08. 2008.
- [18] Jun Lei, Xiaoming Fu “Evaluating the Benefits of Introducing PMIPv6 for Localized Mobility Management” IEEE Wireless Communications and Mobile Computing Conference, 2008. IWCMC '08. International. 09/2008.
- [19] S. Gundavelli , V. Devarapalli ,Proxy Mobile IP Internet draft “ NETLEM working group 2008.
- [20] Joong Hee Lee, Jong Hyouk Lee, and Tai Myoung Chung “Ticket-based Authentication Mechanism for Proxy Mobile IPv6 Environment”, 3rd International Conference on Systems and Networks,2008
- [21] Huachun Zhou, Hongke Zhang “An Authentication Protocol for Proxy Mobile IPv6” The IEEE 4th International Conference on Mobile Ad-hoc and Sensor Networks, 2008
- [22] Hun-Jung Lim, Seon-Ho Park, Young-Ju Han and Tai-Myoung Chung “Hybrid Mobile

- Ad hoc Network support for Proxy Mobile IPv6”, Sixth International Conference on Networked Computing and Advanced Information Management NCM 2010.
- [23] Pyung Soo Kim<sup>1</sup> and Hyong Soon Kim<sup>2</sup>, “An Efficient Correspondent Registration to Reduce Signaling” IJCSNS International Journal of Computer Science and Network Security, VOL.7 No.9, September 2007.
- [24] Hyun Gon Kim, ByeongKyun Oh “Secure and Low Latency Handoff Scheme for Proxy Mobile IPv6” 08 Proceedings of the International Conference on Mobile Technology, Applications and Systems 2008.
- [26] Jae-Min Lee, Jong-Hyouk Lee, and Tai-Myoung Chung,” Performance Analysis of Route Optimization on Proxy Mobile IPv6.”, Systems and Networks Communications, ICSNC '08. 3<sup>rd</sup> International Conference 31 Oct. 2008.
- [27] Sangheon Pack “Relay-based Network Mobility Support in Proxy Mobile IPv6 Networks”, IEEE 5<sup>th</sup> Consumer Communications and Networking Conference, 2008.
- [28] Yang Li, Dong-Won Kum, and You-Ze Cho “Multihoming Support Scheme for Network Mobility Based on Proxy Mobile IPv6” Computing, Communication, Control, and Management, 2008. CCCM '08. ISECS International Colloquium Aug 2008.
- [29] Venkatesh Sarangan, “Comparative Study of Protocols for Dynamic Service Negotiation in the Next-Generation Internet” , IEEE Communications Magazine, March 2006.
- [30] Burkhard Stiller, “ Mobility in the Future Internet” , 26th Annual IEEE Conference on Local Computer Networks, 2001.

- [31] Nen Chung Wang and Yi-Jung Wu, "A Route Optimization Scheme for Mobile IP with IP Header Extension" ,IEEE international conference on Wireless communications and mobile computing 2006.
- [32] Andrew t. Campbell, Javier Gomez, "Comparison of IP Micro mobility Protocols", IEEE Wireless Communications February 2002.
- [33] Bonam Kim, Junmo Yang , "A Survey of NETLMM in All-IP-based Wireless Networks" , International Conference on Mobile Technology, Applications, and Systems 2008.
- [34] Huu Nghia Nguyen, Christian Bonnet, " Scalable Proxy Mobile IPv6 For Heterogeneous Wireless Networks", 8<sup>th</sup> Proceedings of the International Conference on Mobile Technology, Applications, and Systems 2008.
- [35] Ryuji Wakikawa , Sawako Kiriya , "The use of Virtual Interface for Inter-technology handoffs and Multihoming in Proxy Mobile IPv6" Wireless Communications & Mobile.2008.

