

An Efficient Duplicate Address Detection Scheme for Micro-Mobility Handovers in Hierarchical Mobile IPv6 Networks

T07314



Developed by:

Muhammad Wasim
Registration# 358-FBAS/MSCS/F07

Supervised by:

Mr. Mata Ur Rehman

**Department of Computer Science, Faculty of Basic and
Applied Sciences, International Islamic University, Islamabad**

2010



بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

**In the name of ALMIGHTY ALLAH,
The most Beneficent and the most
Merciful.**

**Department of Computer Science
International Islamic University Islamabad**

Dated: 11 /12/2010


Final Approval

It is certified that we have examined the thesis report submitted by **Mr. Muhammad Wasim, Reg No: 358-FBAS/MSCS/F07**, and it is our judgment that this research project is of sufficient standard to warrant its acceptance by the International Islamic University, Islamabad for the Degree of Master of Science in Computer Science.

Committee:

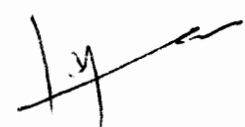
External Examiner

Dr. Abdus Sattar
Former D.G,
Pakistan Computer Bureau,
House No 143, Street No 60, I-8/3,
Islamabad.



Internal Examiner

Mr. Syed Muhammad Saqlain
Assistant Professor
Department of Computer Science,
International Islamic University,
Islamabad.



Supervisor

Mr. Mata Ur Rehman
Assistant Professor
Department of Computer Science,
International Islamic University,
Islamabad.



Dedication

Dedicated to Almighty Allah and my Family who has supported me in all aspects throughout my life.

A dissertation submitted to the **Department of Computer Science, International Islamic University, Islamabad** in partial fulfillment of the requirements for the degree of **MS Computer Science**

International Islamic University, Islamabad
2010

Declaration

We hereby declare that this research project, neither as a whole nor as a part thereof has been copied out from any source. It is further declared that the implementation has been carried out entirely on the basis of our personal efforts under the sincere guidance of our teachers. No portion of the work presented in this report has been submitted in support of any application for any other degree or qualification of this or any other university or institute of learning.

Muhammad Wasim
358-FBAS/MSCS/F07

ACKNOWLEDGMENT

I would like to thank Almighty ALLAH for providing me the strength, courage and patience during my MS studies.

I would like to pay thanks to my supervisor Mata Ur Rehman, and acknowledge the help and support of Dr Muhammad Sher, Dr Naveed Ikram and Qaiser Javed whose valuable advices and guidance made this dissertation a reality. My gratitude also goes to Dr Farrukh Aslam Khan for his time and help.

I would like to thank my parents for their unconditional love, encouragement, advices and all their support.

Last but not least, I would like to pay thanks to all my friends, Israr Ullah, Muhammad Shoaib, Kamran Ullah, Muhammad Salman, Shuja Ud Din Bakhshali (Late), Afshan Ahmed, Aslam Khan, Ashfaq Muhammad, Tahir Hussain, Iftikhar Muhammad, Amad Ali Khan and everyone who was involved in my work and who offered their friendship and support.

Muhammad Wasim

Reg # 358-FBAS/MSCS/F07

Project In Brief

Project Title:	An efficient Duplicate Address Detection Scheme for Micro-Mobility handovers in Hierarchical Mobile IPv6 Networks
Undertaken By:	Muhammad Wasim
Supervised By:	Assistant Professor Mata Ur Rehman
Start Date:	01-09-2009
Completion Date:	20-05-2010
Tools & Technologies	NS 2.31 as Simulation Tool
Documentation Tools	Microsoft Word XP EDraw Network Diagrammer 3.0 Microsoft Excel 2003
Operating System:	Windows XP Professional Redhat Linux 9
System Used:	Pentium 4 2.4GHz Intel Dual Core 1.8 GHz

Abstract

The Hierarchical Mobile IPv6 protocol has been proposed as an improved technology of MIPv6 to solve the problem of handover management mechanism between macro-mobility and micro-mobility, by introducing a new entity called Mobility Anchor Point (MAP). Whenever a Mobile Node (MN) roams into a new MAP domain, it needs to configure two Care-Of-Addresses (CoAs): A Regional Care-Of-Address (RCoA) on the MAP link and an On-link Local Care-Of-Address (LCoA). Each time when a MN visit a New Access Router (nAR) in a MAP domain a Duplicate Address Check (DAD) is performed on LCoA to verify the uniqueness of this address. For a fast moving MN within a MAP domain, the MN may undergo frequent handovers; therefore a majority of handover latency is occupied by DAD check of LCoA, by which handover efficiency has been affected badly. Longer handover latencies results in high packet loss which is almost unacceptable for real time applications.

For such local movements within a particular MAP domain (Micro Mobility handovers), in this thesis we proposed a Less-Frequent Duplicate Address Detection (LF-DAD) scheme that reduces the frequency of DAD check while visiting different Access Routers (AR) in a MAP domain. We have evaluated the performance of the proposed scheme through extensive NS-2 simulation.

TABLE OF CONTENTS

Chapter No	Contents	Page No
1.	Introduction	1
	1.1 Introduction	1
	1.2 Mobile IP Protocols	1
	1.2.1. Mobile IPv4 (MIPv4)	2
	1.2.2. Mobile IPv6 (MIPv6)	4
	1.2.3. Hierarchical Mobile IPv6 (HMIPv6)	6
	1.3 Mobile IP Handovers	8
	1.3.1 Macro and Micro mobility	8
	1.3.2 Handovers in HMIPv6 networks	10
	1.3.3 HMIPv6 Micro mobility handover	12
	1.4 Motivation	13
	1.5 Problem Domain	13
	1.6 Proposed Approach	14
	1.7 Thesis Structure	14
2.	Related Work	15
	2.1 Introduction	15
	2.2 Related Research	16
	2.2.1 Literature Survey	16
	2.2.2 A comparative study of existing DAD schemes	22
	2.3 Concept Matrix	26
	2.4 DAD Schemes proposed by different Researchers	28
	2.5 Factors Affecting performance of HMIPv6 handover process	28

Chapter No	Contents	Page No
	2.6 limitations	29
	2.7 Summary	30
3.	Requirement Analysis	31
	3.1 Problem Domain	31
	3.2 Handover Delay	32
	3.3 Problem Statement	33
	3.4 Proposed Solution	34
	3.4.1 Binding Update Message	35
	3.4.2 Less Frequent Duplicate Address Detection Scheme	36
	3.5 Contribution	38
	3.6 Summary	39
4.	Simulation Design	40
	4.1 Introduction	40
	4.2 Simulation Tool	40
	4.2.1 Why NS2?	41
	4.2.2 IP Mobility Support in NS2	41
	4.3 Simulation Goals	42
	4.4 Simulation Model	44
	4.5 Simulation Scenario	46
	4.6 Research Methodology	47
	4.6.1 Experimental Setup	49
	4.6.1.1 Experimental Setup for Increasing Handovers	49
	4.6.1.2 Experiment for Investigating Impact of Link-Delay	49
	4.6.1.3 Experiment for probing the impact of DAD Time	50
	4.6.1.4 Experiment for varying Mobile Node Speed	51
	4.7 Summary	51

Chapter No	Contents	Page No
5.	Performance Evaluation	52
	5.1 Introduction	52
	5.2 Performance metrics	52
	5.3 Simulation Results	54
	5.3.1 Increasing number of handovers	54
	5.3.2 Investigating the impact of link delays	56
	5.3.3 Changing DAD Time	59
	5.3.4 Changing Node Speed	61
	5.4 Major Conclusions about the impact of handover process	64
	5.5 Summary	65
6.	Conclusion and Future work	66
	6.1 Achievements	66
	6.2 Conclusion	67
	6.3 Future work	67
	6.4 Summary	68
	References	69
	Table of Acronym	

List of Figures

Figure	Page No
Figure 1.1 Mobile IP version 4 (MIPv4)	3
Figure 1.2 Mobile IP version 6 (MIPv6)	5
Figure 1.3 Hierarchical Mobile IP version 6 (HMIPv6)	7
Figure 1.4 Macro/Micro Mobility	9
Figure 1.5 HMIPv6 Macro Mobility Handover	10
Figure 1.6 HMIPv6 Micro Mobility Handover	12
Figure 2.1 Components of HMIPv6 Handover process	16
Figure 2.2 Duplicate Address Detection Schemes	17
Figure 3.1 HMIPv6 Micro-Mobility Domain	32
Figure 3.3 Binding Update Message Format	35
Figure 3.4 Proposed Binding Update Message	36
Figure 3.5 Less Frequent DAD (LF-DAD) Scheme	37
Figure 4.1 NS2 IP Mobility Modules	42
Figure 4.2 Implementation of Simulation	43
Figure 4.3 Scheduled Events for moving MN	45
Figure 4.4 Simulation Scenario	46
Figure 5.1 Handover Latency	55
Figure 5.2 Packet Loss on each handover	55
Figure 5.3 Handover Latency for varying Link Delays	57
Figure 5.4 Packet Loss Ratio for changing Link Delays	58
Figure 5.5 Throughput Ratio with changing Link Delays	59
Figure 5.6 Handover Latency for changing DAD Time	59

Figure 5.7 Packet Loss Ratio for changing DAD Time	60
Figure 5.8 Throughput Ratio for changing DAD Time	61
Figure 5.9 Handover Latency for changing MN Speed	62
Figure 5.10 Packet Loss Ratio for changing MN Speed	62
Figure 5.11 Throughput Ratio for changing MN Speed	63

List of Tables

Table	Page No
Table 2.1 Concept Matrix	27
Table 2.2 Features of existing DAD Strategies	29
Table 4.1 Simulation Parameters	48
Table 4.2 Parameters for Experiment No. 1	49
Table 4.3 Parameters for Experiment No. 2	50
Table 4.4 Parameters for Experiment No. 3	50
Table 4.5 Parameters for Experiment No. 4	51

1

Introduction

1.1 Introduction

In current era, there has been an increasing demand for Mobile Communication where users are moving fast, changing their point of attachment to different communication networks. In such circumstances the main goal is to provide such users a seamless connectivity, with possibly minimum delay, while visiting various mobile networks.

There is an increasing demand for real time communication through internet. Real time applications are increasing day to day like video/audio conferencing, voice over IP (VoIP), online games, Radio/TV on internet etc. Such applications normally require high speed links. In wired scenarios such demands can be met but current wireless technologies are unable to meet such kind of requirements.

Combining these two issues, the big challenge to next generation networks is to provide seamless connectivity, while visiting different networks, with minimum delay.

1.2 Mobile IP Protocols

TCP/IP stack was originally developed for the management of fixed networks, but later on it was modified to support mobility [23]. Internet Protocol IP [19][24] is a connectionless and unreliable routing protocol, which supports source to destination packet delivery. This is done through IP addressing. An IPv4 address is a 32-bit address which uniquely identifies a host on internet. Similarly an IPv6 address is 128-bit address, where some part is reserved for current IPv4 address and some part is reserved for link

local address, which is an address that allows nodes to communicate directly to each other on same link without need of routers. The nodes on the same link know about each other through neighbor discovery protocol. The neighbor discovery protocol for IPv6 is based on improved version of two IPv4's protocols named, ICMP router discovery protocol and Address Resolution Protocol (ARP) [20][10].

The key features of Internet Protocol version 6 (IPv6) are summarized as:

- IPv6 uses Hierarchical addresses which results in reducing the size of routing tables.
- It supports the dynamic assignment of addresses.
- The header is simple which reduces the processing overhead on routers thus making the routing process fast.
- The security is enhanced in IPv6 by allowing authentication and encryption.

The following section describes how mobility has been incorporated in Internet Protocol.

1.2.1. Mobile IPv4

IP Version 4 uniquely identifies a host's current point of attachment to internet. When a host changes its point of attachment to internet it may be unable to receive datagram destined to it. To support host mobility IETF has proposed a solution "IP Mobility Support" [16], also called Mobile IP.

Mobile IPv4 (MIPv4) allows mobile nodes (MN) to change their current point of attachment to internet without losing their ongoing sessions with their corresponding nodes (CN). This is done by allowing a MN to keep two addresses. One address remains permanent and does not change on movement while the other address is temporary and gets changed each time a node visits a new foreign network. The permanent address is called the home address and is assigned by MN's home network, while the temporary is called Care-of-Address (CoA). The CoA is an address assigned to a MN by a router on foreign network called foreign agent [16].

Mobile nodes (MN) visits different foreign networks while its movement and attaches to different foreign agents (FA) through router discovery. The foreign agent discovery is accomplished through ICMP Router Discovery [20][16]. Foreign agents continuously

send out ICMP Router Advertisement (RA) messages in their coverage area. These RA messages contain all necessary mobility options. Another method of FA discovery is through Router Solicitation (RS) Messages. When a mobile node detects that it has moved to new network and is not getting the RA messages, it sends an RS message to FA in a visiting network. This message is a request message to a particular FA in order to solicit the information about that FA. When FA receives RS messages it sends Router Advertisement to the requesting mobile node, if permissible by administrative constraints applied to that particular network.

When a MN detects that it has moved to a new network, it needs to be registered on that network. Registration process is done through exchange of Registration Request and Registration Reply messages [16].

During registration process an MN gets a new CoA. This CoA is either advertised by FA in Router Advertisement Message or may be assigned through some other mechanism like DHCP [17]. The home agent is informed about MN's new CoA. Both the MN's home agent and FA maintain an association, Home address: Care-of-Address, in their cache. A temporary tunnel is created between MN's home agent and the Foreign Agent which is used for delivery of packets destined for that MN, as shown in the following figure.

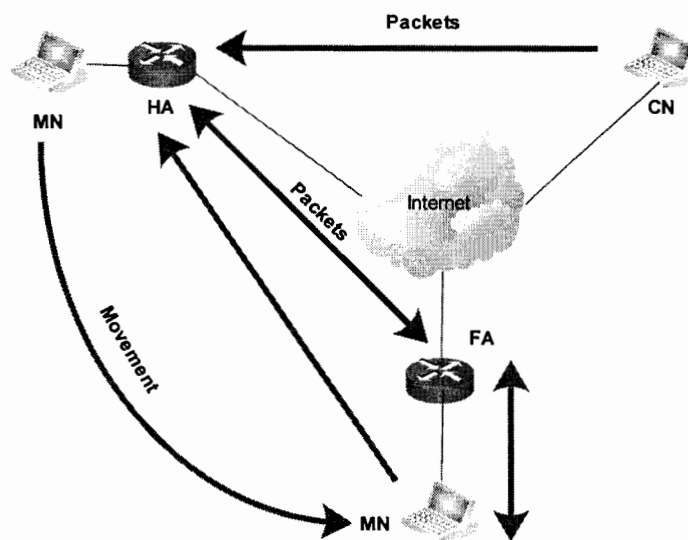


Figure 1.1: Mobile IPv4 (MIPv4)

The corresponding host sends packets to mobile node using MN's home address. When the home agent receives packets destined for MN, it checks in its cache whether MN is at home or at some other location. If at home, HA will simply forward packets to MN. When Home agent finds an association in its cache it means that MN is away from home, then the Home Agent encapsulates the packet and forwards it to MN's foreign agent. The FA receives the packets, decapsulates the packet and forwards it to the MN [16].

Mobile IPv4 imposes some limitations on communication. First, the communication between CN and HA is done through the home agent, i.e. CN and MN can't communicate to each other directly. Second, Home agent intercepts packets on behalf of MN, decapsulates the packet to see FA's address, again encapsulates the packet and forwards it to the corresponding FA. On the other hand FA receives the packet decapsulates it and forwards it to MN. So multi-tunneling is used. Third, if the CN lies in the same Foreign Network as MN, then it leads to triangular routing problem [25].

1.2.2. Mobile IPv6

The Mobile IPv6 (**MIPv6**) [10] has been standardized by IETF in order to provide node mobility in IPv6 networks. The mobility in this case is completely transparent to all mobile nodes in the sense that, during movement, a node visits different access networks without necessarily changing its IPv6 address. Each Mobile Node has been assigned a home address, which is an IPv6 address, in its home network by its home agent. When a MN moves away from its home network it is always addressable by this home address, i.e. the packets destined to this particular node are routed to its home address. This makes the movement of MNs completely transparent to higher level protocols.

MIPv6 protocol architecture is almost similar as MIPv4, with some modifications in registration process, authentication, security, address configuration and agent discovery. When a MN moves from one foreign network to another foreign network, it configures a CoA in a stateless manner called "Stateless Address Auto Configuration" [10][21]. Address can also be assigned to MN in a stateful manner like DHCP, but it is highly

recommended to use stateless method. When MN configures its new CoA it must inform its home agent about the new CoA through binding update message. The MN's CoA is associated with the home address stored in the binding cache of IPv6 nodes and the HA. The HA intercepts the packets destined for MN, searches its binding cache and tunnels the packets to MN's CoA using IPv6 encapsulation.

MIPv6 allows Mobile Nodes to communicate directly to their Corresponding Node through a procedure called Route Optimization [3]. MIPv6 route optimization is almost similar as MIPv4's. According to this method the MN informs its CN about its CoA, each time it configures a new CoA, through binding update messages. The CN also maintains a binding cache. When CN receives a BU message it updates its binding cache with MN's new CoA. The CN then forwards the packets directly to MN's CoA rather than Home Agent [3].

MIPv6 route optimization method solves the problem of triangular routing that exists in MIPv4, reducing the delays in packet delivery process to a large extent. Further, due to direct communication between MN and CN, there is minimal encapsulation as exist in the presence of Home Agent [10].

Following figure shows the Mobile IPv6 operation.

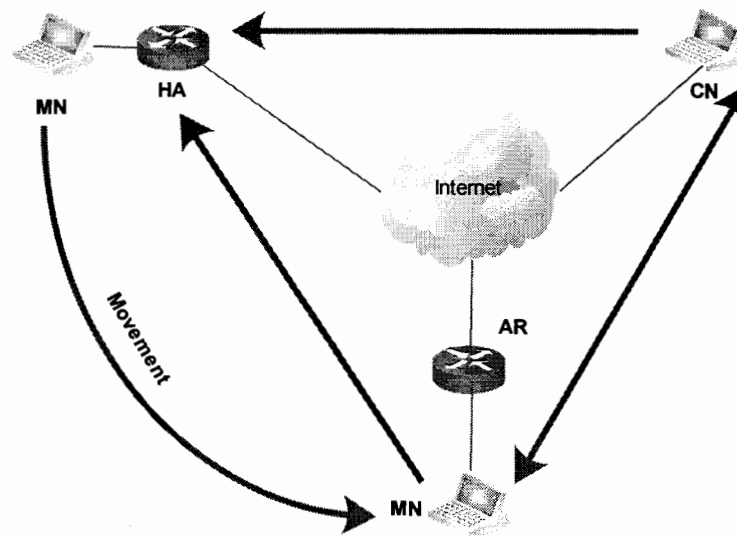


Figure 1.2: Mobile IPv6

MIPv6 requires authentication to be implemented on all IPv6 node, so that a MN may send only authentic binding update messages, which is a dominant security feature.

MIPv6 results in more overhead than MIPv4 because of extra signaling with the CN. It sends Binding Notifications not only to its HA but to its CN as well, which results in longer delays. MIPv6 only supports Macro Mobility and is extremely poor for local movements within a domain.

1.2.3. Hierarchical Mobile IPv6

Hierarchical Mobile IPv6 (HMIPv6) [7] has been standardized by Internet Engineering Task Force (IETF), which is an enhancement to MIPv6 that has greatly improved the handover speed for mobile node and has reduced the amount of signaling in the network by localizing the mobility.

A new node called Mobility Anchor Point (MAP) has been introduced in HMIPv6 which acts as a local home agent for MNs to help in handover procedure. Any router in the hierarchy can serve as MAP which implements this function and can be located anywhere in the network. The introduction of MAP decreases handover latency greatly because of this mobility localization, i.e. a local MAP can be more quickly updated than a home agent [7].

A MN entering in a MAP domain receives Router Advertisement messages (RA), which contain information about one or more MAPs. In HMIPv6 an MN configures two addresses, a Regional Care-of-Address (RCoA) and a Local Care-of-Address (LCoA). The MN normally binds its LCoA, current location of MN, with RCoA, which an address configured by MN on the MAP's link. Serving as a local HA, the MAP receives all the packets destined to MN, encapsulates them and then forwards these packets to MN's LCoA. If the current address, LCoA, of mobile node changes within the MAP domain, the MN must register this address with the MAP. If the Regional CoA (RCoA) of the MN changes, i.e. MN moves from one MAP to another MAP domain, it must be registered with correspondent nodes (CN) and the Home Agent (HA). The RCoA of MN does not

change while visiting different ARs within a MAP domain. This makes the movement of mobile nodes completely transparent to all the CNs an MN is communicating with [7]. Following figure shows the HMIPv6 operation.

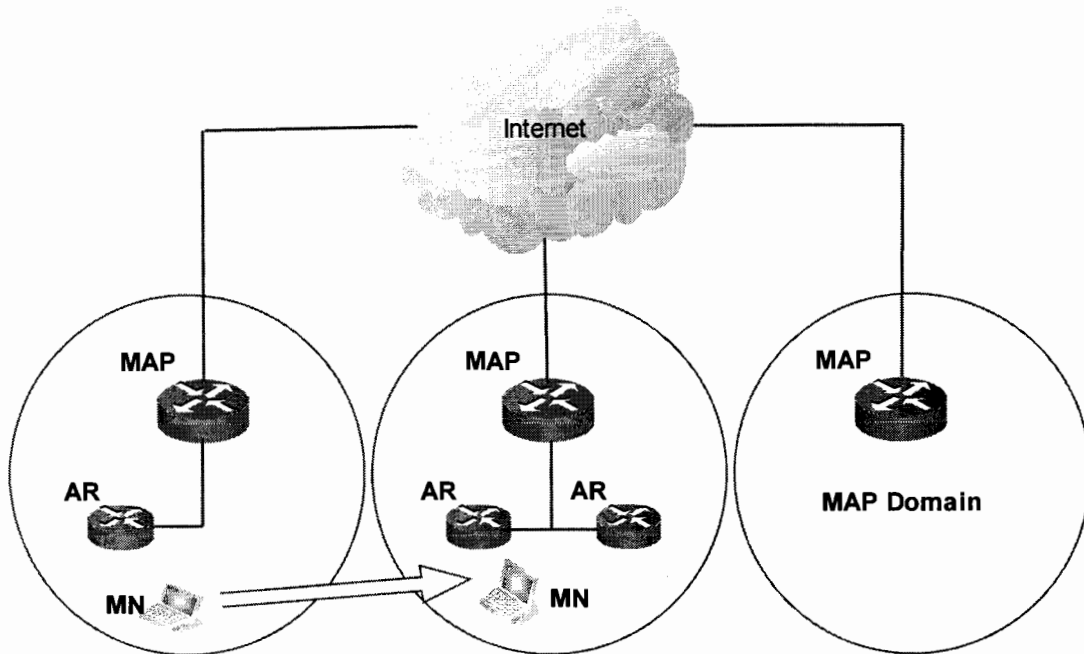


Figure 1.3: Hierarchical Mobile IPv6

HMIPv6 does localize the mobility management and reduces the signaling overhead incurred in MIPv6 but it is insufficient to support real-time IP services, which is the same as MIPv6, because each time when a MN visits a nAR in a particular MAP domain, it configures a new LCoA and DAD check is performed on it. For a fast moving MN node that visits different ARs frequently in a MAP domain this check is performed as many times as the number of ARs that the MN visits. Therefore, due to long address resolution time, of the DAD procedure to verify the uniqueness of the new CoA, results in long handover delays.

MIPv6 is capable of managing global mobility and does not provide support for managing local mobility. MIPv6 uses the same procedure in both cases. This results in an inefficient use of resources in the case of local mobility. In HMIPv6, global mobility is managed by the MIPv6 protocols, while local handoffs are managed locally.

1.3 Mobile IP Handovers

A mobile node using MIP performs several tasks, while moving from one access network to another, by exchanging information and signaling with his home agent and corresponding node. The main tasks that a MN needs to carry out, as it visits a new foreign network, are movement detection, address configuration and binding completion. Collectively, these tasks are called a handover process. On successful completion of this process a mobile node then resumes its ongoing session with its corresponding nodes [44]. In brief the major components involved in a Mobile IP handover are

- Movement Detection
- Router Discovery
- Address acquisition/configuration
- Address Registration
- Binding Update Completion

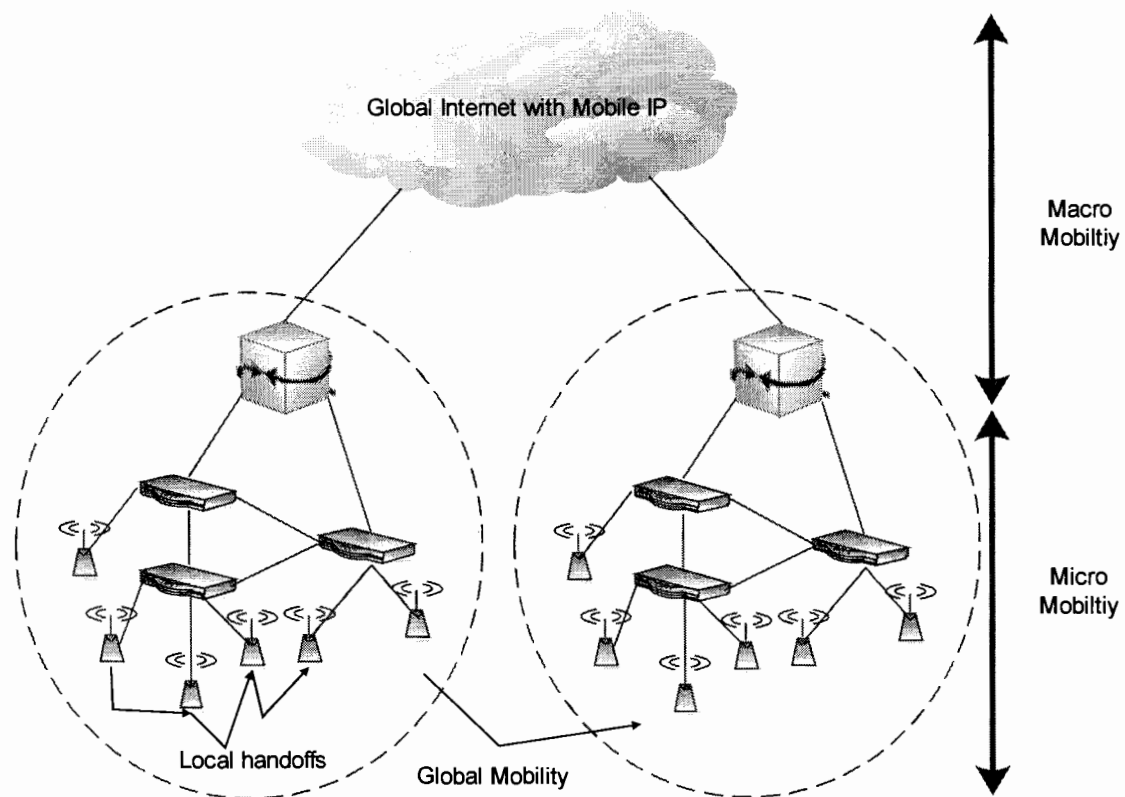
These points shall be explained in the proceeding chapters.

1.3.1 Macro and Micro Mobility

Normally, the fixed nodes remain connected to internet all the time even they do not have anything to communicate. This allows a node to be always reachable to internet resources. Mobile nodes connected to internet through some wireless network also demand the same service. To ensure such service for a Mobile host, a MN must frequently maintain its location information, which normally requires excessive location updates, resulting in consumption of bandwidth and power. To overcome this problem, Micro mobility protocols like HMIP [7] and CIP [26] implements a technique called paging. With this technique a MN operates in a certain paging area, in this case an idle MN need not send his location updates signaling as long it remains in that particular paging area. This limits

the amount of signaling overhead and the amount of location update messages in the network.

Following figure provides a clear understanding of Macro and Micro mobility, where nodes are kept in a Hierarchical order in mobile IP based networks, i.e. whether Mobile IPv4 or Mobile IPv6 network.



“Figure 1.4: Macro/Micro Mobility”

The movement from one access domain to another domain across the internet is referred to as Macro Mobility while the movements within a single domain are termed as Micro Mobility. This Hierarchical mobility localizes the mobility by handling local movements locally. In this case, the home agent need not be informed about MN’s local movements. Incase of local movements, MN attaches to a gateway node on the top level of hierarchy.

This gateway serves as a local home agent for that MN as long as MN remains in this domain. MN visits different access points or access routers attached to this gateway, configures an address on each visit and registers its address with the gateway rather than its home agent. The gateway keeps MN's local binding information and receives packets on behalf of MN, decapsulates them and forwards them to the intended MN.

This reduces the longer latencies incurred due to frequent exchange of location update messages with the home agent and corresponding nodes.

1.3.2 Handovers in Hierarchical Mobile IPv6 networks

HMIPv6 is a Micro Mobility protocol that localizes the mobility by introducing a Mobility Anchor Point (MAP) [7]. It divides the mobility into Macro Mobility and Micro Mobility. Following figure shows the HMIPv6 handover process.

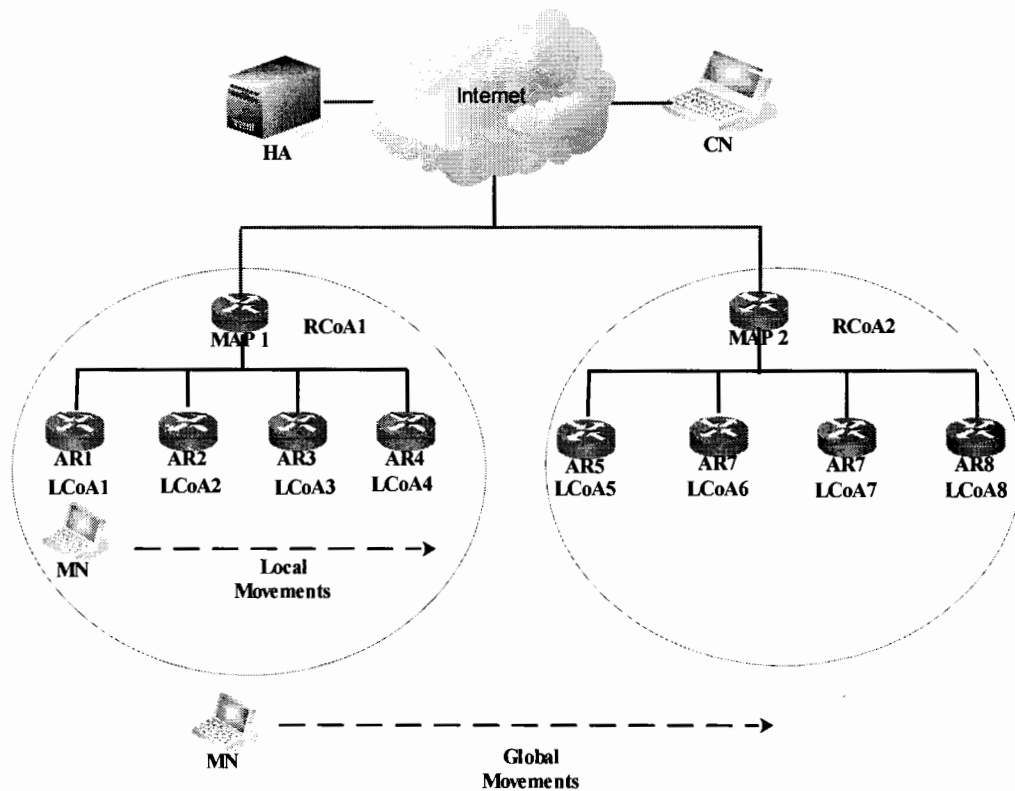


Figure 1.5: HMIPv6 Macro Mobility Handover

MN is currently attached to MAP1 and is receiving its destined packets through RCoA1. MN performs local handovers (Micro/Intra domain handover) as long it moves inside MAP1's domain, visiting AR1 - AR4. In local movements MN registers its LCoA with MAP, without informing its Home Agent or Corresponding Node.

Now during movement when the MN moves from MAP1 to MAP2 domain, i.e. performing an inter-domain or macro mobility handover, it needs to configure a new RCoA2. The handover process given the scenario is as:

MN is attached to MAP1 having RCoA1 and LCoA4. Now if MN moves from MAP1 domain to MAP2 domain:

- First of all MN needs to configure two addresses, an RCoA2 on MAP2 link and an LCoA5 on AR5 link.
- MN sends a BU message to MAP2 via AR5.
- MAP2 receives BU message and performs Duplicate Address Detection Check on newly configured addresses to verify its uniqueness.
- MAP2 then sends a Binding Acknowledgement (BA) message to MN. This indicates that MN has been successfully registered with MAP2.
- MN then sends a BU to its HA and/or CN in order to inform them about its new location.
- HA/CN stores MN's new RCoA2, i.e. change address from RCoA1 to RCoA2, in their binding caches and start forwarding packets to MN on its new RCoA2.
- MAP2 receives packets on behalf of MN and tunnels them to MN via AR5.

MN receives the packets and de-capsulates them and processes them in normal manner.

1.3.3 Hierarchical Mobile IPv6 Micro Mobility handover

Following figure shows HMIPv6 micro mobility handover process.

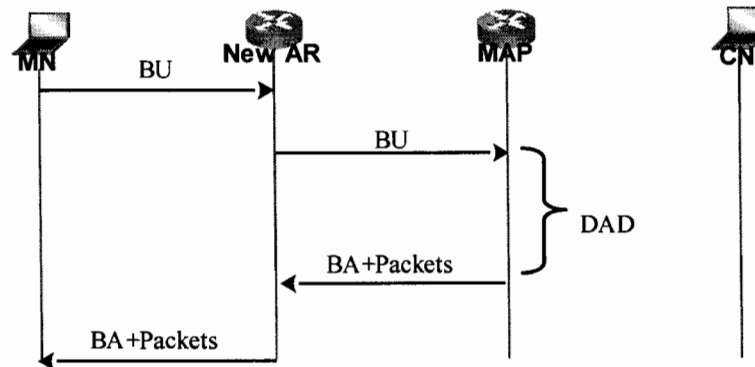


Figure 1.6: HMIPv6 Micro Mobility Handover

- MN receives Router Advertisements (RA) from new AR in current MAP domain.
- MN configures a new LCoA and sends BU to MAP via new AR (nAR).
- MAP receives BU and performs Duplicate Address Detection Check (DAD) on this LCoA. MN is unable to send or receive packets until successful completion of DAD check.
- After successful completion of DAD checks MAP sends BA and packets, destined for MN, to MN via nAR.

The RCoA does not change on local movements, only LCoA changes and gets registered with MAP. The HA and CN need not be informed about MN's location while moving within a MAP domain.

This approach avoids unnecessary location update messages to HA and CN, thus localizing the mobility using a MAP agent. Here the MAP acts a local Home Agent for MN and is responsible for all mobility related management for MN.

1.4 Motivation

Since the last decade there has been an increasing demand for real time applications like video/audio conferencing, Voice-Over-IP, TV on internet and many other multimedia applications. Mobile IP is a technology that provides a seamless connectivity while keeping a mobile host's ongoing sessions intact during movement from one network to other, and is an active research area from last decade. Due to increasing mobility where users continuously change their point of attachment to different communication networks, such real time services face severe performance degradation due to higher delays in the registration process. Different areas of Mobile IP, as research topics, have been targeted by researchers. One of the challenging areas is MIP handover process because this process results in longer delays, which badly affect the performance of MIP protocol. A lot of solutions have been proposed to overcome this problem but still there exists some factors that need to be considered. So, there is a need to uncover the unidentified factors that result in longer delays in handover process and give a solution that increases the performance of handover process.

1.5 Problem Domain

A key factor involved in HMIPv6 handover process is Duplicate Address Detection Check. On visiting new networks an MN configures a new address in a stateless manner, so DAD check is mechanism that verifies the uniqueness of this address. DAD process takes considerable amount of time in the handover process, and until successful completion of this check MN is unable to communicate. For local movements within a MAP domain when MN frequently moves between different ARs, this DAD-check is repeated proportionally as the number of visits made by MN, i.e., on each movement MN configures a new LCoA and performs DAD on it. Thus for a frequently moving MN in a MAP domain it reduces the efficiency of HMIPv6 handover process badly. So, enhancement is needed.

1.6 Proposed Approach

In our proposed approach, we have first identified the necessary components involved in a handover process. We have modified the existing DAD scheme and proposed a Less Frequent DAD scheme that reduces the impact of DAD process on handover delay, for local handover within a MAP domain. We have analyzed the performance of our proposed scheme with current approach used by HMIPv6, through simulation.

1.7 Thesis Structure

The rest of this thesis is organized as follows. In chapter 2 we have presented, the related work; In chapter 3 problem domain and proposed solution; and in chapter 4 the simulation designs has been presented. Chapter 5 deals with performance metrics, simulation and analysis results. Chapter 6 is about conclusions and future work.

2

Related Work

2.1 Introduction

This chapter presents a thorough and enough rich literature on Mobile IP and its extensions. This literature survey has been organized concept wise, starting from very basic to advance concepts in a bottom up manner. This survey mainly focuses on delays and latencies associated with handover process in Hierarchical Mobile IPv6 networks. In the early research, a lot of solutions have been proposed and efforts have been undertaken to minimize this latency. Researchers identified the missing or undiscovered factors that result in bad performance of handover process and tried to fix them but still there are some deficiencies that need to be figured out and should be considered to maximize the performance of Hierarchical Mobile IPv6 protocol. The literature focuses on the impact of Duplicate Address Detection (DAD) check, which is indeed an important part of handover process but comprises significant delays in a handover process. This chapter documents almost all measurements that have been undertaken by various researchers, in order minimize this delay. The investigation is undertaken for Micro mobility handovers within a single access domain, where a Mobile Host visits different access routers connected to some Gateway node on the top level of hierarchy.

2.2 Related Research

The following papers, surveys and technical reports have been considered for related work on Hierarchical Mobile IPv6 handover optimization and approaches used for Duplicate Address Detection scheme.

2.2.1 Literature Survey

Hierarchical Mobile IPv6 [7], is a proposed standard that localizes the mobility to a single network domain, by introducing a MAP agent which acts as a local HA for a MN within its domain. This localization has reduced the longer handover delays that mostly stems from exchange of location update messages between MN, HA and CN. A handover process in HMIPv6 network mainly consists of five major components, which corresponds to total handover delay. These are: Movement Detection, Router Discovery, Address Configuration, Duplicate Address Detection and Binding Update completion [7].

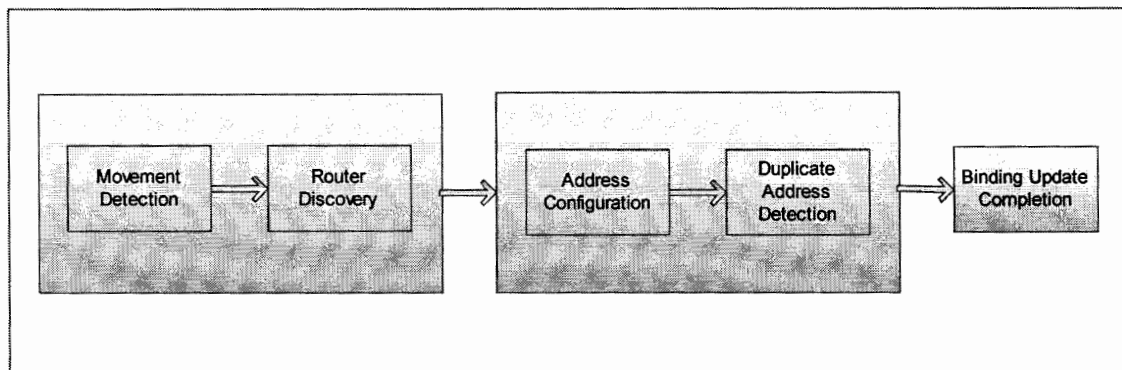
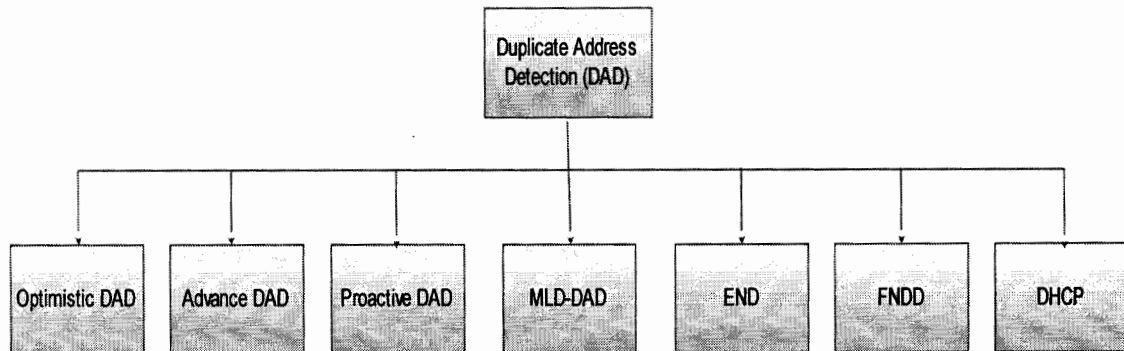


Figure 2.1: Components of HMIPv6 Handover process

Each of these steps corresponds to some amount of delay in overall handover process. Duplicate Address Detection process affects performance of HMIPv6 micro mobility handovers badly.

A detailed study about different Duplicate Address Detection Schemes is presented by Panita Pongpaibool in [56]. Following are some of the most famous approaches that have been proposed for DAD.



“Figure 2.2 Duplicate Address Detection Schemes”

(1) Optimistic Duplicate Address Detection [29], ensures the uniqueness of newly configured CoA, referred to as optimistic address. This technique restricts nodes to advertise their physical address along with the optimistic address by setting the “Override” field in the neighbor advertisement message to 0, which is a modification to IPv6 Neighbor Discovery [19] and IPv6 Stateless Address Auto-configuration [21]. This is done so that the nodes in the network do not store this untested address in their cache, in case of duplication. Further it also imposes that optimistic address must not be used for Neighbor Solicitation and Router Solicitation messages for two reasons: First, a node is unable to contact any router until it is ensured that the address is unique, i.e DAD process completes. Second, the node is unable to resume a session with a neighbor that is not present in its cache. All the communication flows through the default router, which then generates an ICMP redirect message containing the MAC address of destined neighbor. In this way the node updates its cache and starts communication with its neighbor directly.

(2) Advance Duplicate Address Detection (A-DAD) [12] [30], is another scheme that minimizes the DAD time by performing the DAD process prior to assigning an address to a mobile node. According to this technique, each access router in the network maintains a pool of ipv6 addresses. Addresses are generated randomly and after the generation DAD

is performed on that address. After verifying the uniqueness of an address, the address is then kept in cache called passive proxy cache, which is actually an AR that acts as a proxy for such tested addresses. If the AR, serving as passive proxy, detects that another node is performing DAD check on an address which is already in its cache it removes that address from its cache, in order to let other node use this address. Now when a MN detects that it has moved to a new network it sends a request message for obtaining a new Care-Of-Address. The passive proxy selects one of the addresses from its cache and sends it to MN in a reply message. A-DAD also works with Fast Mobile IPv6 (FMIPv6) [8]. FMIPv6 was designed for fast handover in MIPv6 networks, based of layer 2 triggers and pre-binding approach. The working of A-DAD with FMIPv6 had been described in [30].

(3) Proactive Duplicate Address Detection (P-DAD) [31], verifies the uniqueness of an address prior to movement of a mobile node to a new network. This scheme allows a MN to configure an address in a stateless manner and then verify its uniqueness. This scheme introduces some new entities. It assumes that there is central storage server called Regional Information Point (RIP). This Regional Information Point server maintains a table called Mobile Node Attachment Point Table or MAP table. This table contains all the information about access points and their Basic Services Set ID (BSSID) and the prefixes of all the Access Routers. All the access routers in the network know the address of RIP server. When a Mobile Node predicts that it is about to move to a new network it obtains the prefix of the visiting AR from Mobile node Attachment Point table. When it receives the desired prefix it then configures a Care-of-Address. After the address has been configured the MN perform DAD on it by exchange of Pre-allocate Request and reply messages, while it has not moved to new network yet. When the MN moves to the new network and attaches to that particular AR it then activates the CoA which was configured and DAD was performed on it. This is done through the exchange of CoA-Activation Request and CoA-Activation Reply messages.

(4) Multicast Listener Discovery based Duplicate Address Detection (MLD-DAD): MLD [32][33] is a protocol that is used by routers in an IPv6 network in order to know which nodes in the network wants or willing to receive multicast packets on their directly connected links. Taking advantage of this property, this scheme finishes the DAD process earlier by imposing some checks. Before performing DAD a node must first joins a multicast address with the newly configured address [21]. At this point, the visiting router checks whether the requesting node is the first node joining the multicast group, by looking at the configured address [34]. If it is the first one then it means that there are no more addresses in group and this address is unique. When a MN configures a new address it sends an MLD Report message to an MLD-Querier router. This router is responsible for all MLD related signaling. Soon after sending MLD-Report MN also initiates DAD check. The MLD-report message shows the MN presence on the link and asks whether it is the first node that visits this domain. If so, MLD-Querier router sends an MLD-Response message to MN showing that this address is unique. If another address is present in the multicast group then it means that there is atleast one member that is getting served on this particular link. In this case, the Standard DAD is carried out on the newly configured address rather than sending MLD-Response message back to MN. In this case the MN waits until the DAD process is complete and it is properly informed about the uniqueness of CoA or else the retransmission timer gets expired. In both cases it is assumed that the CoA configured by MN is unique and is not duplicated.

(5) Enhanced Neighbor Discovery (END) is more like MLD-DAD. This scheme introduces some new entities and messages. It introduces a new entity called Neighbor Discovery Rely Agent (NDRA) [35]. The NDRA is a function that is implemented on some router in the network. The purpose of this agent is to maintain a cache of all nodes IPv6 addresses. Each node that configures a new address, it encapsulates that address in an MLD Join message and sends NDRA. In this way the cache is maintained and updated of all addresses used in the network. To finish DAD early, the END protocol sends an acknowledge message to MN. This acknowledge message is a modified RA message containing a field called Available Address Option field; this field carries an address that

represents the availability of an address for a visiting node, which means that the address is unique. If duplication is found then the Standard DAD process is carried out on the address by initiating an NS-DAD message to the owner of the address.

(6) Fast Neighbor Discovery and Duplicate Address Detection (FNDD) minimizes the DAD time by using the neighbor cache lookup process [36]. In this scheme it is assumed that each Access Router in a visiting network contains all addresses nodes connecting to its link in its neighbor cache. When a new node arrives it configures a new address and sends it to AR in a RS message. AR receives this message and checks its neighbor cache to verify the uniqueness of that address. If it is found unique the AR sends an acknowledgement to MN. If a collision is found, then AR also contains a list of pre-configured addresses that have been properly tested. In this case it picks one of those addresses and allocates it to the visiting node.

(7) Dynamic Host Control Protocol (DHCP) [17], is a stateful method for address configuration. According to this scheme, a MN on visiting a new network contacts a DHCP server to solicit a CoA. The DHCP server contains a pool of addresses that are unique and respond to a solicitation message by assigning one of the available address to the requesting node. In this scenario DHCP server is responsible for maintaining all information about address assignment and other related information like NAT etc.

In [2] the authors have presented an MLD-Based scheme to improve the handover performance of FHMIPv6 affected due to DAD check. According to this scheme the visiting node first of all set up a multicast group for itself to MAP. The MAP then asks all neighbors to join the group. After a new address has been configured by a node and arrives at MAP for verification, the MAP either respond by replying the requesting node representing the uniqueness of address or initiate a Standard DAD process incase of collision. The performance of the scheme has been shown through simulation. This scheme is designed to work in parallel with the Standard DAD process.

In [1] a Pre-DAD check scheme has been presented. It is shown that whenever a MN detects that it is about to move to a new network, it sends some information to MAP. MAP forwards this information to all ARs connected to its link. Based on this information each and every AR configures a CoA on behalf of MN and performs DAD on it. When the MN connects to any of the AR it shows its presence and the corresponding AR start forwarding packets on the address that was configured and tested for MN.

[37] Presents another scheme for detecting duplicate addresses. This scheme uses passive duplicate address detection (PDAD) [38][5], to report duplication of addresses. According to this technique the incoming routing protocol traffic is examined by a node to estimate the possibility of address conflict. The chance of address duplication is estimated in a probabilistic manner where a table is maintained by each node that records the probability of an address's conflict. If the probability reaches to some threshold value then it is assumed that the address is duplicated, and conflict resolution procedure is initiated.

A new scheme V-DAD has been proposed in [39]. This scheme uses the concept of a visual domain that changes the operation of traditional DAD process. According to this scheme a visual domain server is an entity that comprises a large area usually a MAP and its adjacent MAP i.e. neighbor MAP (N-MAP). This area is known as a visual domain. With in a visual domain the MAPs exchange information about its topology. With this scheme the handover delay is reduced by pre-performing the DAD process. After DAD is successful, each MAP maintains a Node Information Table listing some extra parameters, regarding each visiting node, to avoid duplication in a visual domain.

A Fast-Robust DAD (FR-DAD) scheme has been presented in [41]. This scheme is almost similar as A-DAD, where a P-Server keeps a list of addresses and are assigned to

visiting nodes on request. These addresses are pre-configured and are passed through standard DAD process. An address that successfully undergoes DAD process is then kept in a list maintained by P-Server. This scheme introduces some new message types, a modified Option and an additional storage entity (P-Server).

2.2.2 A comparative study of existing DAD schemes

Duplicate Address Detection is a key component of Mobile IP handover process. The degradation of handover performance that come due to DAD process has been studied by various researches and alternative solutions has also been proposed in order to minimize the impact of DAD procedure on handover process to a minimum possible level. This section documents the shortcomings of each of the existing schemes that have been proposed for Duplicate Address Detection.

Optimistic DAD [29], is based on the use of random addresses and assumes that the address conflict is very rare. This may be true for small networks but if the network size grows at large, it become very hard or almost impossible to distribute and configure random addresses in large network, so collision is possible. If an address conflict does arises then this schemes becomes more time consuming and normally takes more time in recovery process than the existing DAD process. Further, this scheme makes use of the newly configured untested address in some communication messages while DAD is in progress; this mainly minimizes the communication disruption rather than handover latency.

Unlike optimistic approach A-DAD assumes that the address conflict is sure to happen, so it prevents it from happening. With this approach the handover performance improves significantly but this approach puts an extra burden on ARs. Each AR need to maintain and manage a pool of addresses. Further, mobile nodes are not able to configure their own addresses, i.e, address configuration is no longer stateless, which goes against the

standard. A-DAD allows a limited number of MNs as the number of addresses in the proxy cache. In case of large number of mobile nodes this approach doesn't seem to be working effectively.

Proactive DAD (P-DAD) [31] assumes that the MN is able to predict its movement in advance. To achieve this some efficient and interoperable movement prediction algorithms needs to be developed. An amazing feature of P-DAD is that it allows the stateless configuration of address which is the most desirable feature of Mobile IPv6, but this scheme requires some additional entities like RIP server. Further, the configuration and maintenance of MAP-Tables, in RIP servers, and Registration Caches puts extra management overhead. As compared to A-DAD the DAD check is performed by AR rather than MN itself. Without movement detection the delay is comparable to that of A-DAD.

The MLD-DAD minimizes DAD time only to a single roundtrip time if there is no address conflict. If a conflict is found then it takes as much time as standard DAD. This scheme requires that MLD must be properly configured on all nodes across the networks. This requirement may not be met in some scenarios and node may be unaware of MLD. Further, this scheme puts some extra overhead on routers for monitoring all multicast groups regularly and responds to all MLD-Report even if it is not necessary or required.

With Enhanced Neighbor Discovery (END) scheme, if an address is found available for use, i.e. address is found unique, the delay is almost same as MLD-DAD. But if a collision occurs then this scheme takes more time than MLD-DAD because it involves cache lookup time, which is always carried out before the Standard DAD initiates.

FNDD combines the features of both MLD-DAD and END by maintaining a list of all address in use to check for duplicate addresses. This scheme checks the uniqueness of an address only on the link to which the MN is trying to connect. If an AR contains multiple

interfaces connecting multiple links, then this scheme fails to work. The delay is comparable to MLD and END schemes and the neighbor cache lookup time, which is approximately $5.3 \mu\text{sec}$ [36]. This scheme avoids the standard process if a collision is found but it imposes that each router must contain a list of pre-configured and tested addresses which makes the scheme stateful.

DHCP ensures the uniqueness of an address by maintaining a pool of unique address but still DAD is unavoidable with this scheme because address assignment through DHCP require unique identifiers to identify the client and server. In this case Link local address is used as DHCP unique identifier, which must be passed through standard DAD to ensure its uniqueness.

MLD-Based DAD check scheme for FHMIPv6 allows nodes to configure address in a stateless manner. This scheme is suitable if the multicast group contains minimum number of nodes. In case of large number of nodes sharing the same multicast group, it is highly possible that collision may occur. In case of conflict, this scheme switches to standard DAD process which then takes longer than usual.

Pre-DAD scheme does reduce the handover latency by pre-address configuration and pre-DAD check but this scheme does not reduce the frequency of DAD check. This procedure needs to be carried out each time a MN wishes to move into a new AR. In case of fast moving MNs, and if the number of MNs increases at large, this scheme puts significant processing overhead on MAP and ARs, as MAP will tunnel each MN's packet stream to all ARs and ARs will need to configure a LCoA for each MN and perform DAD-check on it. Further, MN will connect to only one AR but MAP tunnels packets to each and every AR in its domain and all ARs buffer these packets for MN. This leads to wastage of bandwidth and poor utilization of resources.

PDAD based algorithm requires each node to maintain a table, calculate conflict probability and monitor this table constantly each time a new address is configured. It also requires monitoring each incoming routing protocol's traffic, on the basis of which identification of the duplicate addresses is carried out. This scheme produces extra processing overhead on nodes while DAD is still carried out if a conflict does occur.

V-DAD scheme requires MAP to keep information of each node that enters in its domain and shares it with other neighbors. This puts extra processing, monitoring and management overhead on nodes. Further it also increases the responsibilities of MAP to act a visual domain server. It also require the development of some efficient table search algorithms in size Node Information Table (NIT) increases at large, otherwise this scheme will take as longer as the number of entries increases in NI-Table in cache. Further, this scheme works fine for Macro mobility handovers while in case of local handovers this scheme is unsuitable.

FR-DAD doesn't allow nodes to configure addresses in a stateless manner. Due to this stateful behavior most of the researches does not recommend such kind of schemes for address assignment.

2.3 Concept Matrix

The following Table summarizes the investigation of different Duplicate Address Detection schemes.

Paper/Draft/RFC	Concept	Findings/Results/Conclusions
Optimistic Duplicate Address Detection for IPv6	<p>Random number generator is used to avoid address conflicts.</p> <p>Optimistic addresses are used for communication while DAD is in progress.</p> <p>New communication strategy has been introduced.</p>	<p>Optimistic DAD performance depends on the size of network. The performance varies as the network size grows.</p> <p>Management and configuration of random addresses is hard or almost impossible in large networks. So due to this infeasibility, address duplication is possible. If a conflict arises, the time required in the recovery process becomes more than the existing DAD process. So this scheme is not suitable for large networks.</p>
Advance Duplicate Address Detection (A-DAD)	<p>A new entity Passive Proxy Cache has been introduced that keeps a list of unique addresses. Addresses are assigned to nodes in a stateful manner.</p> <p>A pessimistic approach that prevents potential duplication of addresses.</p>	<p>Allows a constant number of MNs. As the address assignment is stateful, MNs cannot configure their own addresses which is a desired feature in most scenarios. Due to these problems this approach suffers from severe scalability issue. It also put extra burden on intermediate ARs. So this scheme fails in scenarios where MNS increases by large number.</p>
Proactive-DAD A Fast Address-Acquisition Strategy for Mobile IPv6 Networks	<p>A P-DAD scheme that performs DAD before moving to new network.</p> <p>RIP server maintains MAP-Tables.</p> <p>MAP-Tables contain prefix information of all ARs.</p>	<p>Preserves stateless property of Address configuration.</p> <p>DAD is performed by AR on request sent by MN and not by MN itself.</p> <p>Improves handover performance but puts extra burden on network, like RIP server management, MAP-Table configuration, Registration cache maintenance etc. Further, it also require development of movement prediction algorithms.</p>
Duplicate Address Detection Optimization using IPv6 Multicast Listener Discovery	<p>An MLD-DAD scheme.</p> <p>Verifies address uniqueness by checking where the multicast group by querying the group status. i.e; empty or not.</p> <p>Works in parallel with standard DAD.</p>	<p>New entity MLD-Querier router introduces that serves new messages like MLD-Report and MLD-Response messages. Shorten DAD time if multicast group is found empty else it increases the DAD time more than the standard DAD time.</p>
Duplicate Address Detection Optimization Using Enhanced Neighbor Discovery	<p>Proposes an END scheme for DAD.</p> <p>A protocol that verifies the uniqueness of an address by maintaining a cache of all neighbors address.</p>	<p>This scheme takes advantage of MLD-Join messages for building an address cache. It means that all nodes must be aware of both END and MLD protocol. So this requirement may not be fulfilled in some scenarios.</p> <p>Also in the worst case this scheme takes longer than MLD-DAD to check uniqueness of an address.</p>

A Fast Neighbor Discovery and DAD Scheme for Fast Handover in Mobile IPv6 Networks	A hybrid scheme for address configuration. If an address that has been configured in a stateless manner is found duplicate, another pre-configured tested address is assigned to MN.	MN can configure an address in a stateless manner. ARs keep a list of tested addresses to be assigned to MN if newly configured address was found duplicated. Reduces DAD time as no standard DAD is initiated in case of duplication. This scheme is applicable to a single link and fails to work an AR have multiple interfaces sharing same prefix.
Dynamic Host Control Protocol for IPv6 (DHCPv6)	A DHCP server contains a pool of unique addresses to be assigned to nodes visiting a particular network.	DAD is still performed on Link local address. Address assignment is stateful. Nodes can't configure their own addresses. Due to these reasons this scheme is not recommended for reduction of delay associated with DAD process.
An Improved DAD check Scheme MLD-Based in FHMIPv6	MN prior to moving to a new network setup for itself a multicast group on that link. All other neighbors on that link join this group. MAP either reply to MN showing that the address is unique or starts standard process.	MAP will establish and maintain a multicast group for each MN that wish to join its link. This is not usually possible if the arrival rate of MN to a network is high. So this scheme fails to work when the large number of nodes frequently visits some particular network or domain.
Fast Handover Solution using Multi-tunnel in HMIPv6	A Pre-DAD check scheme has been proposed where each AR connecting to the visiting MAP configures and tests a CoA for MN.	For a single visit a separate tunnel is created to each of the connected AR. Every AR configures and performs DAD on CoA, for a single MN. This scheme is inappropriate particularly if the number of AR connected to a MAP is large or the number of MN visits a MAP domain. This scheme results in high wastage of resources and processing overhead.
An efficient DAD scheme for Hierarchical Mobile IPv6 Handoff	A probability table is maintained by nodes that shows the chance of an address conflict. Duplication is identified by examining incoming routing protocol traffic based on a Passive DAD algorithm.	Separate tables are maintained for each address. Traffic monitoring is carried out. Puts unnecessary processing overhead on nodes. Requires extra bandwidth and storage.
Research on Handover in Hierarchical Mobile IPv6 based on Fast DAD mechanism in Visual Domain	A MAP and its neighbor MAPs forms a visual domain. MAP exchange information with each other and no DAD is performed if a MN enters another MAP domain within a visual domain.	MAP stores extra information about MN and share it with MAPs in visual domain. MAP also act as a visual server and perform extra activities that produces unnecessary overhead on routers.
Fast and Robust Duplicate Address Detection Scheme for Mobile IPv6	An FR-DAD scheme is presented where a P-Server contain a list of properly tested unique addresses. FR-DAD is a stateful address assignment scheme.	Introduces new message formats and central storage devices like P-Server. Nature of address assignment is statful, which is not recommended by most of the researchers.

Table 2.1: Concept Matrix

2.4 DAD schemes proposed by different Researchers

To sum up the literature survey it is clear that different researches have proposed the following DAD schemes to improve HMIPv6 handover performance. The schemes presented later on are mostly based on the following techniques.

- Optimistic DAD (O-DAD)
- Advance DAD (A-DAD)
- Proactive DAD (P-DAD)
- MLD-DAD
- END
- FNDD
- DHCPv6
- V-DAD
- FR-DAD

2.5 Factors Affecting performance of HMIPv6 handover process

As discussed previously, the following factors affect the performance of HMIPv6 handover

- Arrival Rate of MNs entering a domain
- Speed of MN
- Number of ARs within a MAP domain
- Movement Detection
- Address configuration
- DAD time
- Binding Update completion time
- Handover Frequency
- Link Delays

2.6 Limitations

From the literature survey it is clear that different researches proposed different DAD schemes to minimize DAD time. These schemes in a broader sense fall into two main categories. Stateful Address assignment and Stateless Address configuration. Stateful address assignment schemes like A-DAD, DHCPv6 and FR-DAD etc are strongly discouraged by most of the researchers. The reason is that, in stateful address assignment the address is assigned by some central storage entity or server, i.e. the nodes can't configure their own addresses, this is unacceptable in situations where address configuration involves some cryptography key algorithms [36]. The stateless address assignment schemes involve the use of some other protocols like Neighbor Discovery or Multicast listener Discovery protocols. This imposes a constraint that each and every node in the network must have properly implemented and configured with these protocols. Further, these schemes mostly use positive acknowledgement to end the DAD process early otherwise the standard DAD process is carried out on the new address. Thus in local handovers if a node moves frequently between different ARs the DAD process will be carried out each time a new address is configured on visiting an AR. This result in repetition of DAD process, which affects the handover performance badly, particularly in local handovers.

Following table includes some dominant characteristics of existing DAD schemes.

Characteristics	DAD Schemes
Stateful Address Assignment	A-DAD, DHCPv6, FNDD, FR-DAD
Need Central Storage Device	MLD-DAD, END, A-DAD, DHCP, FR-DAD, FNDD
Use positive acknowledgement	MLD-DAD, END, FNDD
Rely on Multicast listener Discovery	MLD-DAD, END
Introduces new message types	P-DAD, MLD-DAD, FR-DAD
Modification to existing messages	O-DAD, P-DAD, FNDD, END, FR-DAD, MLD-DAD
Suitable for wireless environment	A-DAD, P-DAD, O-DAD

Table 2.2: Features of existing DAD Strategies

2.7 Summary

In this chapter we have given a description of related work. Different researchers have presented different schemes with different characteristics and tried to improve the DAD time in order to optimize the handover performance. Though existing schemes work fine in some scenarios, still some more efficient schemes need to be developed. We have highlighted the limitations of some of the existing schemes and illustrated the requirement for a scheme to control the frequency of DAD process.

3

Requirement Analysis

3.1 Problem Domain

Due to the high user mobility, providing a seamless connectivity to the mobile devices has been a hot research area over the last decade. This requirement led to the proposal and standardization of Mobile IP protocol. Researches have so far focused different aspects of Mobile IP to enhance the performance of this protocol. The most demanding issue has been to improve handoff performance. A lot of extensions and scheme were proposed to optimize handover performance. Hierarchical Mobile IPv6 is one of those proposals which is developed in order to localize the mobility, with the introduction of a MAP, dividing mobility into Macro and Micro Mobility. Macro mobility handovers are still managed in the manner as MIPv6 does but handover performance has been significantly improved in Micro Mobility handovers. In Micro mobility handovers the MN performs local movements within a particular MAP domain by visiting different ARs connected to that MAP. MAP in this case act as local HA for MN, performs mobility management completely seamless to MN's HA and CN. Though, HMIPv6 greatly minimizes handover latency, still researchers are focusing some key issues in order to make the handover performance, in Micro Mobility, even more optimized. Some of the reasons that results in handover delay are described in next section. Following figure shows a HMIPv6 Micro-Mobility domain.

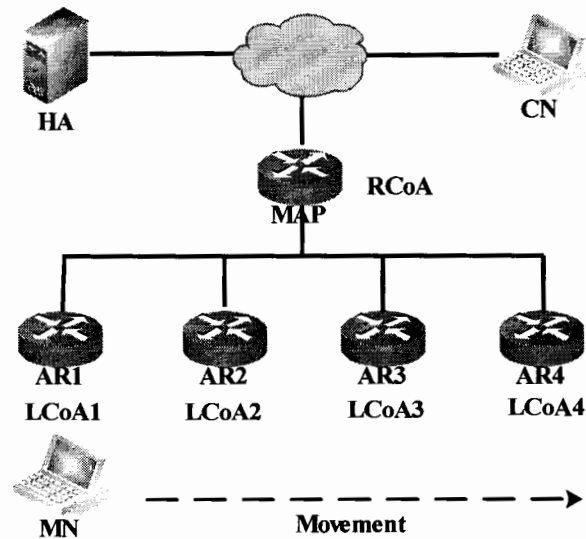


Figure 3.1: “HMIPv6 Micro-Mobility Domain”

3.2 Handover Delay

A MN while accessing different ARs in a visited domain performs different tasks while attaching to an AR. A handover process in HMIPv6 network mainly consists of five major components, which corresponds to total handover delay. These are: Movement Detection, Router Discovery, Address Configuration, Duplicate Address Detection and Binding Update completion

- Movement Detection
- Router Discovery
- Address Configuration
- Duplicate Address Detection
- Binding Update Completion

Movement Detection corresponds to check, how MN has been disconnected or moved to a new network. This is accomplished through Router Solicitation and Router Advertisement Messages as described in [7]

After an MN detects that it has moved to a new network it must be attached to some router in a foreign network. The decision as to which router in a foreign network an MN is going to be attached is carried out through ICMP router discovery procedure described in [7][28][42]

Once an MN chooses a router to attach with, it then configures a CoA on that link. This address is configured in a stateless manner as described in [21].

Duplicate Address Detection check is performed on this newly configured CoA in order to verify the uniqueness of this address on the link through DAD process [10].

Finally, after an address has been verified and found unique, the HA and CN of MN are notified about MN's new CoA through Binding Update messages.

Each of these steps takes some amount of time; collectively the sum of delays of each of these steps corresponds to the total handover delay.

3.3 Problem Statement

Based on the limitation and drawbacks of the existing work presented in chapter 2 we have developed our problem statement as follows.

Duplicate Address Check (DAD) check plays a vital role in MIPv6 handovers. When an MN detects that it has moved to a new subnet, the MN configures a new LCoA and performs Duplicate Address Detection (DAD) to verify the uniqueness of its link-local address on the new link as specified in MIPv6 [10]. Similarly in HMIPv6 the same

procedure is undertaken when a MN moves to new MAP's domain or visit a new AR in a particular MAP domain. During this time the MN must wait until successful completion of DAD process. This DAD check takes 1000ms to 1500ms (in worst case) [1], [2].

For local movements within a MAP domain if the MN frequently moves between different ARs, this DAD-check is repeated proportionally as the number of visits made by MN, i.e., on each movement MN configures a new LCoA and performs DAD on it. Thus for a frequently moving MN in a MAP domain it reduces the efficiency of HMIPv6 handover process badly.

Further, the MN is not able to send or receive packets until successful completion of handover process. As DAD take considerable amount of time in handover process, this result in higher packets loss for an MN's ongoing session and also the network suffers from unnecessary signaling and message exchange.

To enhance the efficiency of handover process in HMIPv6 the repetition of DAD check must be reduced, thus enhancement is needed.

3.4 Proposed Solution

From the problem statement it is understood that key idea is to reduce the frequency of DAD check; i.e. it must not be carried out at every individual handover. For this purpose we are going to propose a *Less-Frequent Duplicate Address Detection Scheme (LF-DAD)* for Micro Mobility handovers in HMIPv6 networks.

To achieve our goal we have modified the actual binding update message by adding an extra bit that is necessary for this scheme. First of all, we will explain the binding update message and then the LF-DAD scheme.

3.4.1 Binding Update Message

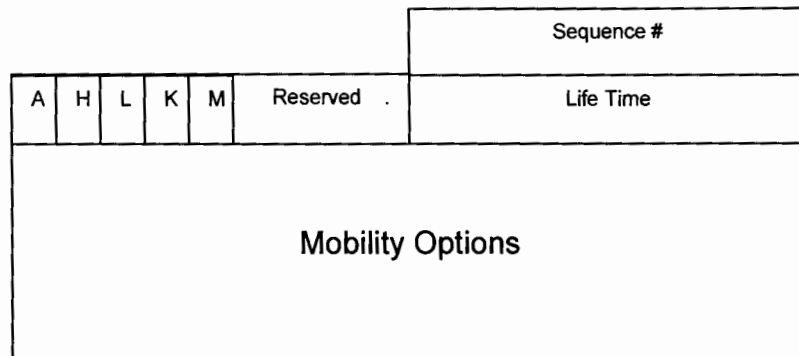


Figure 3.3: Binding Update Message Format

Sequence Number: 16-bit unsigned integer.

Acknowledgment (A): Indicates MN's request for acknowledgment from MAP. If set means MN wait until receives ack from MAP. :

Home Registration (H): If set by MN it means that the receiving node should act as HA for MN.

Link local Address Compatibility (L): if set it means that the Home address has same interface identifier as MN's link local address.

Key Management Mobility Compatibility (K): Indicates IPsec security association between MN and HA.

MAP Registration (M): If set to 1 it shows MAP registration.

Reserved: Total field length is 16-bits, 5 bits have been used and 11 are still available for future research.

Life Time: 16-bit unsigned integer. Represent Binding life time.

Mobility Options: Variable length field, each an integer multiple of 8 octet long.

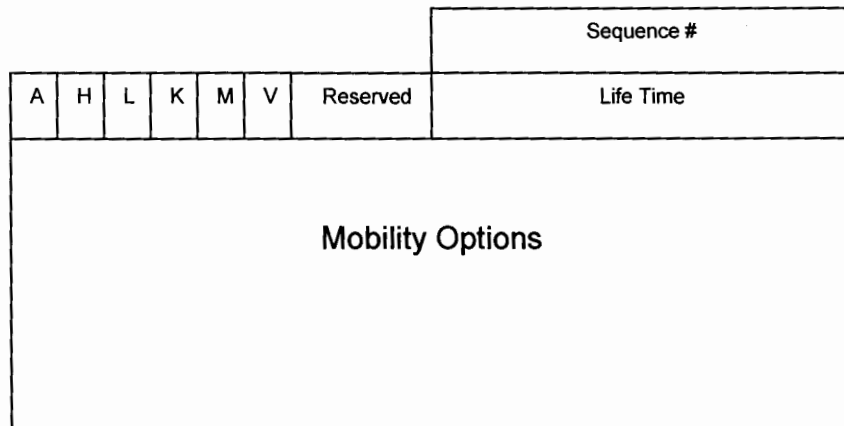
Proposed Binding Update Message:

Figure 3.4: Proposed BU Message Format

V: Shows whether a MN has already been verified by MAP or not. If this bit is set to 1, then it means that MN is already verified itself with the MAP; if not set, then MAP assumes that the MN is trying to connect on its link for the first time.

3.4.2 Less Frequent Duplicate Address Detection (LF-DAD) Scheme**Mobile Node Considerations:**

When a MN visits a new domain it receives AR's prefix information via RA or RS messages. MN then configures an LCoA and will encapsulate this address and its interface identifier in a binding update (BU) message and sends it to MAP. Note this time the V bit in BU message must be 0, i.e.; MN is performing his first handoff on a MAP's link.

MAP Considerations:

MAP receives the BU message, de-capsulate it and checks that the V bit is 0. Now the MAP performs DAD check on CoA sent by MN to verify its uniqueness. On successful completion of DAD check, MAP stores this address and MN's Interface ID in its binding cache and starts forwarding packets destined for MN.

If MAP finds that the V bit in BU message is set to 1, then it means that MN has already been verified and MAP has already stored its Int ID in its binding cache. In this case, the MAP only updates its binding cache with newly configured LCoA without performing DAD. Following figure explains the whole idea.

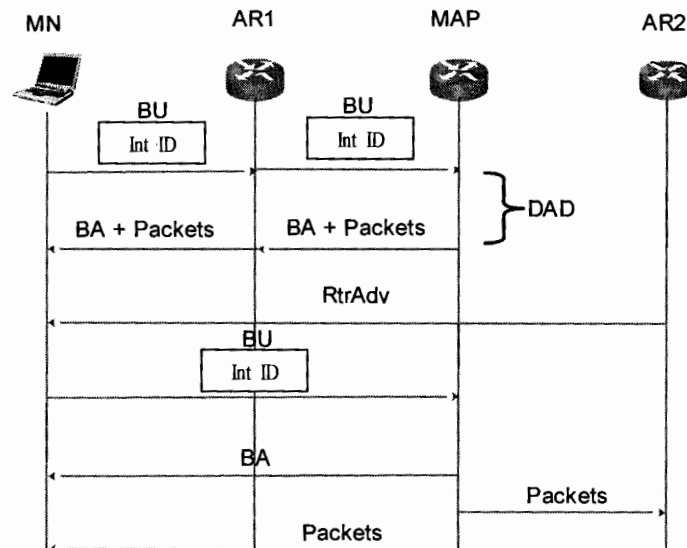


Figure 3.5: Less Frequent DAD (LF-DAD) Scheme

- MN sends LCoA and its Interface Identifier in BU message to MAP.
- MAP perform DAD on this LCoA, if successful, MAP updates its binding cache by associating MN's LCoA and its interface identifier against its RCoA, as RCoA:Int_ID:LCoA.
- MAP then sends Binding Acknowledgement (BAck) and the packets destined for MN on its new CoA.
- While MN enters the overlapping area of AR2 , it receives Router Advertisement messages (RtAdv) message containg AR2 subnet prefix.
- MN configures a new LCoA and sends BU and its Interface_ID to MAP, setting V bit to 1.
- MAP see the V bit set to 1 and scans its cache and checks for association MN's RCoA: Interfacd_ID, if matched, MAP will update its cache with new LCoA *without performing DAD*. As shown in fig, AR2.
- After updating its cache MAP sends BAck to MN and will start forwarding packets to MN's new LCoA. i.e. to MN via AR2.

3.5 Contribution

The main contributions of this thesis can be summarized as follows.

- A detailed understanding of Mobile IP, Mobile IPv6 and Hierarchical Mobile IPv6.
- Macro and Micro Mobility management in Hierarchical Mobile IPv6 networks.
- Micro Mobility handover procedure and its associated issues that results in bad performance.
- Modified handover scheme enhancing the actual handover procedure.
- Used different metrics to analyze the influence of proposed handover scheme on the conventional HMIPv6 scheme.

3.6 Summary

A detail study about the problem domain, our problem statement and proposed solution is presented in this chapter. Improving MIP handoff performance has been an active area of research. It is obvious from the problem statement that the DAD procedure affects the performance of handover process badly as DAD is repeated on each handover within a single domain. Our proposed solution is based on the idea of minimizing this repetition, making fast handovers within a MAP domain.

4

The Simulation Design

4.1 Introduction

Simulation is a technique or method that is undertaken when real world test are either too expensive, complex, time consuming or almost impossible due to any reason. The network topologies we come up in our daily life are mostly wired or wireless but there are situations, like MIP networks, where we need a hybrid topology for our simulation. The challenging issue in such an environment is to provide connectivity between wired and wireless domains. The MIP model in NS2 introduces a base station node which consists of a wired and a wireless interface capable of providing connectivity between two wired and wireless domains. This chapter explains our proposed simulation tool, simulation goals, simulation model, reference scenario and finally experimental setup for different tests.

4.2 Simulation Tool

The simulation tool we used for our simulation is the Network Simulator (NS 2.31) [43][52] [53]. The NS is a discrete event simulator which was developed by VINT project and is maintained under the supervision of Information Science Institute

(ISI). NS is an open source simulator particularly designed for networking research. It is the most widely used simulator by researches related to networking field.

4.2.1 Why NS2?

Network Simulator (NS 2) is a discrete event object-oriented simulator. NS is written as a front-end in an object oriented language C++ and OTCL. Support of C++ in NS2 allows detailed simulations of protocols and provides means for efficient manipulation of packet headers, bytes, and implementing algorithms particularly designed to run over larger data sets. Due to these facts the more desiring feature is the run time speed which is provided by C++. The turn around time in this case is less important. OTCL provides means for varying different simulation configurations and parameters, or exploring configuration setups for various scenarios [52][53].

NS2 provides a built-in support for a lot of transport, routing and multicast protocols and covers a wide range of network types, applications and traffic models. Beside that NS2 also provides an easy way for simulating different wireless and wired-cum-wireless scenarios.

4.2.2 IP Mobility Support in NS2

Currently, NS2 provides support only for the base Mobile IP protocol. All other extensions to Mobile IP protocols are mostly external contributions by different researches or communities. These extensions are available for the sake of research purpose with open licenses. Most of the contributed codes and modules were designed for some particular versions of NS2 and were later updated to most recent versions of NS. Following figure shows the NS2 support for IP mobility and the contributed code and modules.

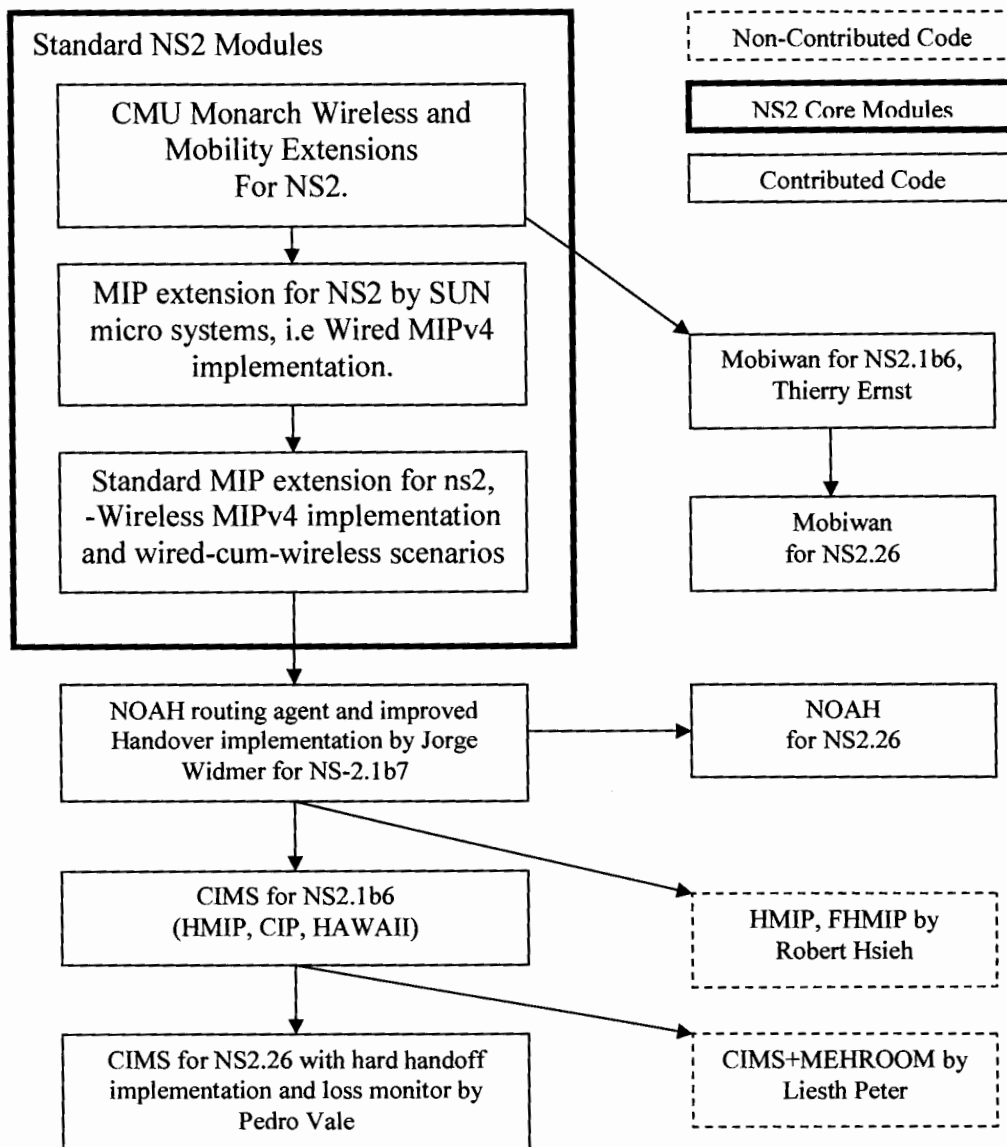


Figure 4.1: NS2 IP Mobility Modules

4.3 Simulation Goals

The simulation is carried out in the following steps:

- First of all, selection of a simulation model for Hierarchical Mobile IPv6 networks.

- Implementation and configuration of the model in NS2.
- Running simulation in order to obtain the required metrics.
- Finally, analyzing the results to show the performance optimization of the protocol in the network.

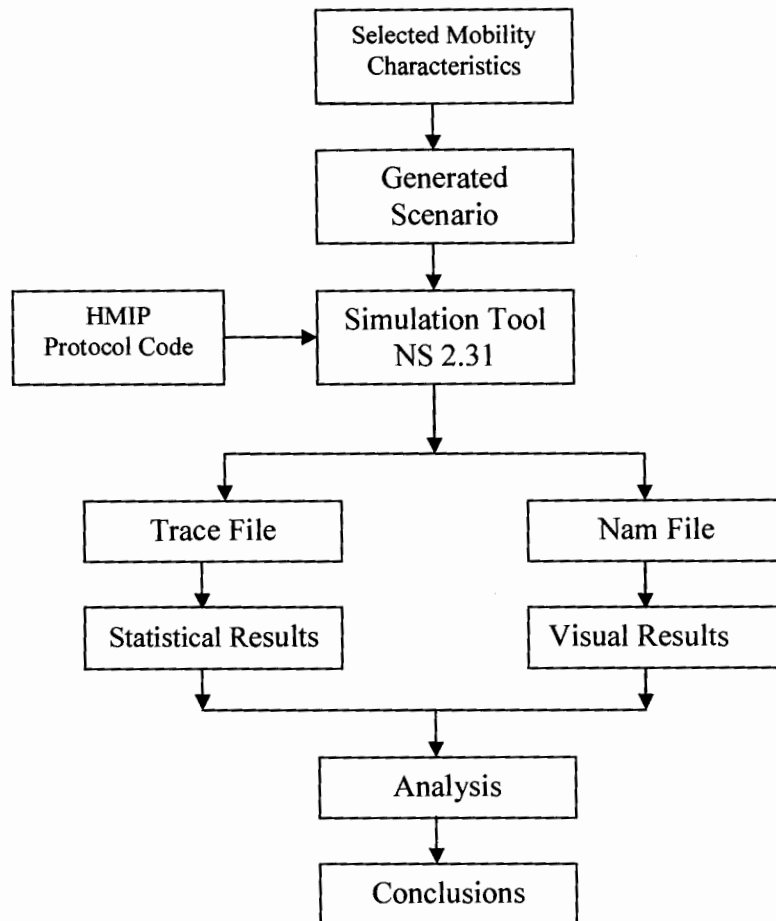


Figure 4.2 Implementation of Simulation

The main goal of this simulation is to analyze the reduction in HMIPv6 Micro Mobility handovers. We will study the effect of our proposed handover scheme on Local handovers within a particular domain and will compare it with the current

implementation of HMIPv6 protocol. We will analyze our proposed scheme under different simulation setups.

4.4 Simulation Model

The simulation study is carried out using Columbia Micro Mobility Software (CIMS) [49][50][54]. This software was first designed for ns version 2.1b6, later it was upgraded for ns 2.26 and currently it is made available for ns 2.31. CIMS provides a common framework for all simulation studies.

The Hierarchical Mobile IP simulation model presents two levels of the protocol; first is the Mobility Anchor Point (MAP) and on the lower level are Access Routers (ARS). ARs are actually the Base Station nodes that contain a wired and a wireless interface. The MNs are purely wireless and move within a wireless domain. The ARs provides connectivity and traffic forwarding facilities to these wireless MNs in a hybrid scenarios. Our simulation uses a hybrid wired-cum-wireless topology. Following are the main entities of the proposed simulation model.

Gateway (GW)

CIMS was designed for simulation of various micro mobility protocols, The GW node in case of HMIP simulation acts as MAP in the simulated scenario. This node acts as a local home agent for the mobile node and is responsible for keeping track of MN's movement, maintaining binding cache for MN and other mobility management.

Access Routers (ARS)

ARs are base station nodes that transmit beacons in some particular range. ARs consist of two different interfaces where one interface is connected to a wired link and the other interface is connected to a wireless link. AR plays a key role in MIP networks because these networks mostly consist of a hybrid topology.

Access Network Gateways (ANG)

These nodes are responsible for simulating the inter-domain behavior of the protocol, which are not used in our simulation because the scope of our study is limited only to intra-domain or micro mobility handovers.

Corresponding Nodes (CN)

CN is the source of the traffic. CN generates the traffic for MN and is responsible for encapsulating and tunneling the packets destined for MN to MAP.

Mobile Node (MN)

MN is the receiver of the traffic. MN is a wireless node which moves and connects to different ARs during the simulation.

In order to compare the performance of current handover scheme and our proposed scheme all the simulations are done using the same common framework. The flow of events during the simulation is given in the following figure.

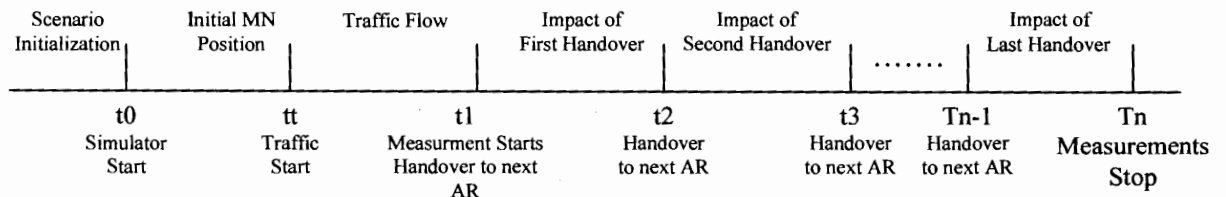


Figure 4.3: “Scheduled Events for moving MN”

The simulation begins with initializing the reference scenario by loading the HMIP library at the simulator starts. The MN is placed in its initial position and after sometime the traffic starts. MN movement is scheduled as directed and starts performing handovers to different ARs during its movement. On each individual handover a series of parameters is calculated and at the end of simulation the trace files are closed. Based on calculated parameters during simulation the final results are calculated and the results are stored in an output file.

4.5 Simulation Scenario

The following figure shows the scenario for our simulation. This scenario presents a true picture of real world network. In the enterprise network there could be different configurations of the nodes in the network, for instance there may be the nodes which have no support for mobility i.e. mobility unaware nodes. This scenario consists of a mixture of mobility aware and mobility unaware nodes which reflect a closer look of the real world network topology.

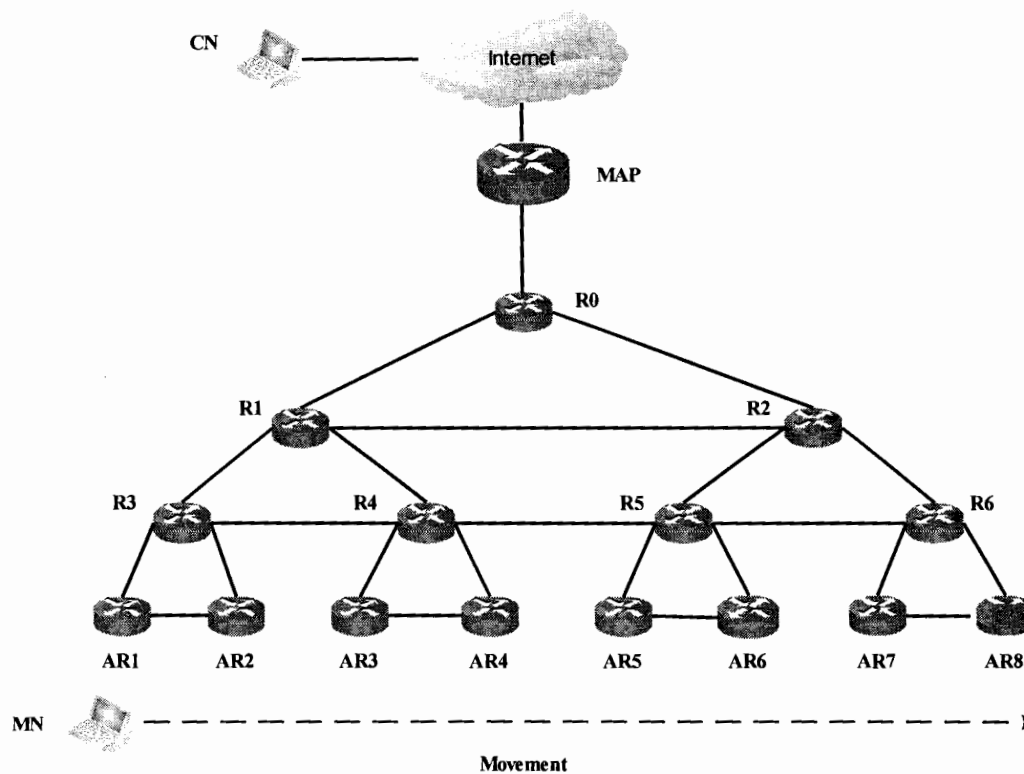


Figure 4.4: Simulation Scenario

Scenario Details

The above scenario consist of two parts; First, the wired part and, second, the wireless part, forming a wired-cum-wireless (hybrid) topology. The wired part consists of nodes arranged in a hierarchical order, connected via Ethernet links between them, reflecting a

mesh structure. Outside the domain is the CN which is the traffic generator source during the simulation.

At the last level of topology there are 8 Access Routers which are actually the BS nodes with wired and a wireless interface. MN moves in the network, connecting to these ARs using IEEE 802.11 wireless links. Each AR covers a 1 Mbps IEEE 802.11 cell independently. All ARs are connected to MAP through a series of routers. These routers are connected via point-to-point links of 10 Mbps, with a constant 5ms link delay.

The MN in the topology is the receiver of the traffic generated by CN and will move inside the domain. At the start of simulation the MN initial location will be at AR1. After it starts movement it will visit ARs one-by-one in a sequential order, from AR1 ... AR8, and will perform handoff.

The CN is the source of the traffic. It will generate UDP traffic of the type Constant-bit-rate (CBR). The packet size is kept 1000bytes with a rate of 100 packets per second.

The simulation finishes with calculating the required metrics and sending the results to an output file.

4.6 Research Methodology

A detailed setup for our simulations has been described in this section. Four experiments were conducted for each handover scheme. In the first experiment we analyzed the impact of the number of increasing handovers, in second we analyzed the impact of varying link delays, in third we analyzed the impact of varying DAD time and finally the impact of varying MN's speed. In each experiment we have analyzed the effect of handover latency, packet loss ratio, One-way delay and throughput ratio. Based on these performance metrics we'll present our conclusions about each handover scheme and their effects. All simulation has been carried out in an open source network simulator NS 2.31

[43][52][53], Redhat Linux 9 operating system, Dual Core processor 1.8 GHz and 1 GB RAM. We have used omni directional antenna with 250m transmission range. UDP is used as transmission protocol with a packet size of 1000 bytes at 100 packet/sec. Table 4.1 shows the general parameters for the whole simulation.

Table 4.1 Simulation Parameters

Variables	Values
Simulation tool	NS2.31
Propagation model	TwoRayGround
Antenna Type	Omni directional
MAC Type	802.11 MAC
Interface Queue	Wireless Physical
Topology size	1360m x 1360m
Transport protocol	UDP
Packet size	1000 bytes
Traffic Type	CBR
Queue Type	Drop Tail
Wired link Type	Ethernet
Wired links Speed	10Mbps
Wireless link Type	IEEE 802.11
Wireless link Speed	1 Mbps
Protocol Agent	HFA (HMIP protocol)
Number of MN	1
Number of CN	1
Simulation time	33 sec

4.6.1 Experimental Setup

The details of complete experimental setup are given as follows.

4.6.1.1 Experiment for increasing number of handovers

Besides the above general parameters in table 4.1 each handover scheme is tested for some additional parameters. In this experiment we will analyze the impact on handover latency, packet loss, One-way delay and the throughput, as we increase the number of handovers. This experiment is conducted for both handover schemes. The details of this experiment are given in table 4.2, where we shall only vary the number of handovers while keeping all other parameters constant for all tests.

Table 4.2 Parameters for Experiment No. 1

Variables	Values
Experiment	Impact of Increasing Number of Handovers.
Number of handovers	1,2,3,4,5,6,7
Link Delay	10 ms
MN Speed (Handovers/minute)	15
DAD Time	MAX (1500 ms)
Number of tests	7 tests. One test for each handover scheme

4.6.1.2 Experiment for investigating the impact of Link delays

In this experiment we will investigate the impact of link delays in our simulation. The experiment is conducted for both schemes. The details of this experiment are given in table 4.3, where we will vary the link delays and performs a test to obtain results for both handover schemes. Here we will vary the link delay from 5ms-50ms while keeping all other parameters constant for each test. The results for both schemes on each test will be

then compared in order to check the performance optimization of our proposed handover scheme again the current HMIPv6 handover scheme.

Table 4.3 Parameters for Experiment No. 2

Variables	Values
Experiment	Impact of Varying Link Delays
Number of handovers	7
Link Delay	5,10,15,20,25,30,35,40,45,50 ms
MN Speed (Handovers/minute)	15
DAD Time	MAX (1500 ms)
Number of tests	10 tests. One test for each handover scheme

4.6.1.3 Experiment for probing the impact of DAD time

Duplicate Address Detection (DAD) normally takes 1000-1500 ms in the overall handover process. In this experiment we will analyze the impact of DAD time on handover latency, packet loss, One-way-Delay and throughput. The details are given in table 4.4, where we vary the DAD time and a test is carried out each time DAD time changes. The DAD time 0 means the test is conducted for the proposed scheme where the DAD check has been ignored. All other parameters for each test will remain constant.

Table 4.4 Parameters for Experiment No. 3

Variables	Values
Experiment	Impact of DAD time
Number of handovers	7
Link Delay	10 ms
MN Speed (Handovers/minute)	15
DAD Time	1000, 1100, 1200, 1300, 1400, 1500, 0 ms
Number of tests	7 tests

4.6.1.4 Experiment for varying Mobile Node (MN) Speed

In this experiment we will investigate the impact of MN's speed on our performance metrics. The details of the experiment are given in table 4.5, where we will vary the speed on MN while keeping all other parameters constant. The MN will be varied from 3-15ms as given in the table and on each change an individual test will be carried out for both handover schemes and will be compared to know about the performance optimization of our proposed handover scheme.

Table 4.5 Parameters for Experiment No. 4

Variables	Values
Experiment	Impact of Varying MN Speed
Number of handovers	7
Link Delay	10 ms
MN Speed (Handovers/minute)	3, 6, 9, 12, 15
DAD Time	1500 ms
Number of tests	5 tests-One for each handover scheme

4.7 Summary

In this chapter we described our simulation goals, the simulation model and simulation scenario for our simulation and the flow of events in our simulation process. Also we have presented a detailed study about the required entities and their characteristics required for our simulation. Further more, we have presented a detailed study about the simulation and experimental setup for the assessment of performance optimization of our proposed scheme.

5

Performance Evaluation

5.1 Introduction

In this chapter we analyze the results obtained from our simulation. Here we present the performance of the current HMIPv6 handover procedure and our proposed scheme. We shall compare our proposed scheme against current handover scheme through calculation of some performance metrics. Based on our experimental design we have presented our required results in graphical form with sufficient explanation. Four experiments are performed and in each experiment the results for the following metrics have been collected, Handover latency, Packet Loss Ratio, One-Way-Delay and throughput ratio. Each experiment is undertaken for both handover schemes under same environment and same conditions. Each experiment consists of one or more tests. Each test is conducted for both schemes and results have been collected. The next section describes how different metrics have been calculated and then we will show our results and finally the summary of our work is given.

5.2 Performance metrics

The performance metrics that we have chosen for our simulation are; Handover Latency, Packet Loss Ratio, Average One-Way-Delay and Throughput Ratio. For each individual

test in each experiment the results have been collected for these four metrics. These metrics are calculated as:

Handover Latency

Handover latency is the time difference between the first packet through new AR and last packet received through old AR.

T_n = Reception Time Stamp of first packet received via new AR

T_o = Reception Time Stamp of last packet received via Old AR

N = Number of handovers

$$\text{Handover Latency} = \sum_{n=1}^N \left(\frac{T_n - T_o}{N} \right) ms$$

Packet Lost Ratio

It is defined as the ratio of total number of packet lost to total number of packet transmitted and is calculated as

P_d = Number of not received packets

P_t = Total number of transmitted packets

$$\text{Packet loss Ratio (\%)} = \frac{P_d}{P_t} * 100$$

One-Way-Delay

The time taken by a packet to reach its destination including route acquisition time and is calculated as.

T_r = Reception Time Stamp

T_s = Sender Time Stamp

N_p = Number of received Packets

$$\text{Average Delay} = \sum \frac{(T_r - T_s)}{N_p} \text{ms}$$

Throughput Ratio:

It is calculated as:

B_r = Number of bytes accepted/received

B_s = Maximum number of bytes sent

$$\text{Throughput Ratio (\%)} = \frac{B_r}{B_s} * 100$$

5.3 Simulation Results

The simulation results of the mobility models is given as follows.

5.3.1 Simulation results for Increasing number of handovers

Handover Latency

Figure 5.1 shows the handover latencies associated with both schemes. It is clear from the figure that the handover latency is greatly improved by our proposed scheme. Increasing the number of handover between cross-over routers places a very minor, i.e. the variation in handover delay seems almost constant, impact on handover delay but the contribution of our proposed scheme is very significant and predictable.

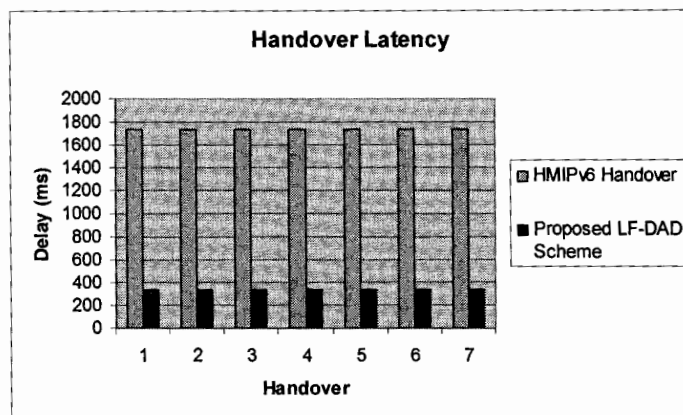


Figure 5.1: Handover Latency

Packet Loss

Figure 5.2 shows the number of lost packets during each individual handover. We can observe that the packet loss in the HMIPv6 is much higher and our proposed scheme has reduced this loss to greater extent. Packets loss occurs on each handover as the MN registration process is in progress; hence by reducing the delay in handover time results in lower packet loss. The average Packet Loss ratio found in HMIPv6 handover was 46.31 %, which was reduced to 8.6 % by our proposed scheme.

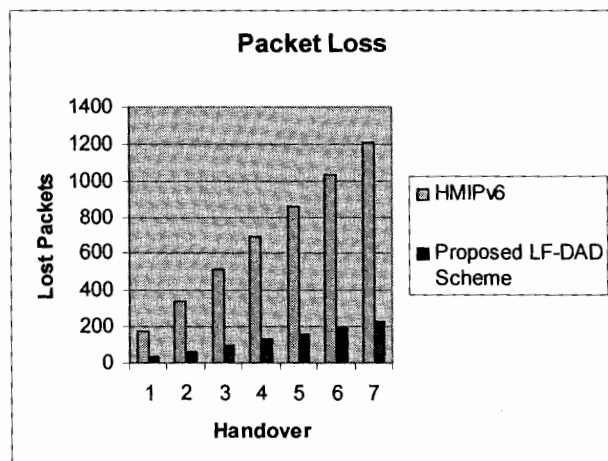


Figure 5.2: Packet loss on each handover

Average One-Way-Delay (O.W.D)

A very slight variation is seen in the average One-Way-Delay in the both schemes. The handover latency has nothing to do with the One-Way-Delay because this delay does not involve the delays associated with handovers but rather it is the summation of difference of reception time stamp and sender time stamp divided by number of received packets. So the One-Way-Delay calculated for each scheme is given as

O.W.D for HMIPv6 = 241.69 ms

O.W.D for LF-DAD = 241.70 ms

Throughput Ratio

Our proposed scheme has improved the throughput significantly. By reducing the handover latency the network throughput has been increased because the MN receives more packets than it does in current HMIPv6 scheme. The throughput ratios calculated for both schemes are given as

Throughput Ratio (HMIPv6) = 53.69 %

Throughput Ratio (LF-DAD) = 91.38 %

5.3.2 Simulation results for investigating the impact of Link delays

Handover Latency

Figure 5.3 shows the handover latencies are getting higher as the delay in link increases. A comparison of both the schemes is presented and it is very clear from the results that our proposed solution is performing much better than the actual handover scheme in situations where the links suffers different delays in the network.

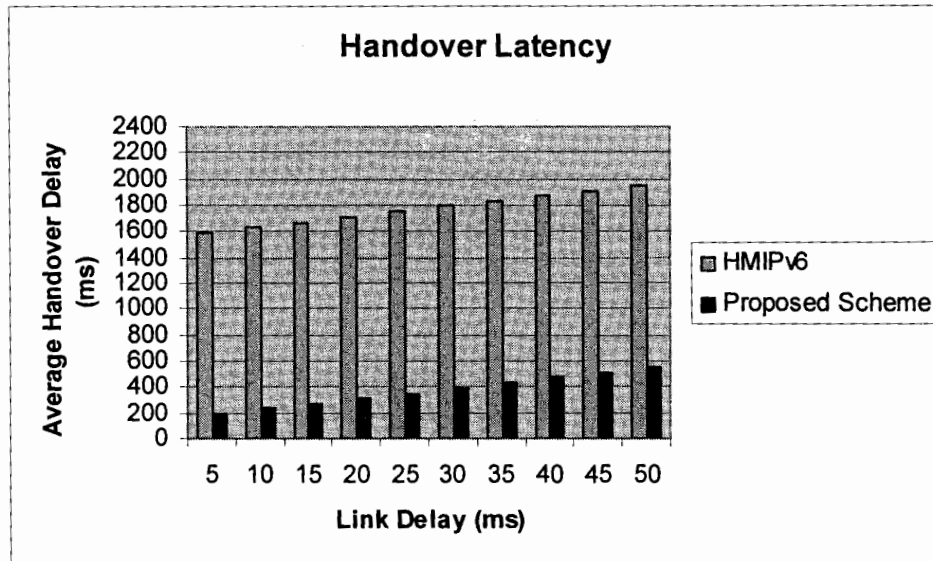


Figure 5.3: Handover Latency for varying Link Delays

Packet Loss Ratio

The packet loss ratios for both schemes are given in figure 5.4. The loss ratio increases as the delay in link increases. The comparison of both the schemes is shown and we can clearly observe that our proposed scheme reduces the packet loss to greater extent as compared to current HMIP handover scheme. The minimum loss ratios for HMIP and our proposed scheme are 42.5 % and 4.8 % respectively, and the maximum values for these are 52.3% and 14.7% respectively. These results shows that, in the network system where links encounters different link delays, our proposed scheme will work more efficiently than current HMIPv6 scheme.

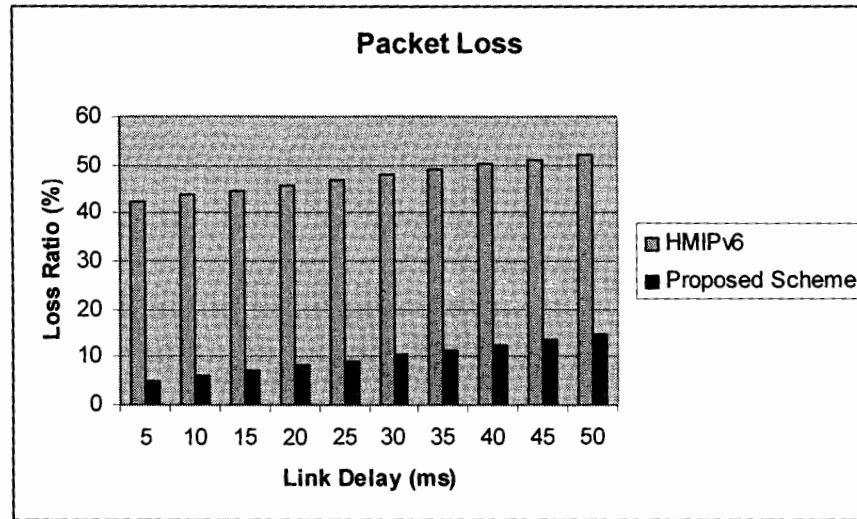


Figure 5.4: Packet Loss Ratio with changing Link Delays

Average One-Way-Delay (O.W.D)

A very slight variation is seen in the average One-Way-Delay in the both schemes. The one-way-delay increases with the increasing the link delays but in case of comparison simulation test is carried out for both schemes under same varying conditions. Hence for each link delay value the of O.W.D for each scheme comes out almost similar. If represented in graph it will show a constant behavior.

Average O.W.D for HMIPv6 = 246.2 ms

Average O.W.D for LF-DAD = 246.7 ms

Throughput Ratio

The throughput ratios for the schemes are given in figure 5.5. We notice that the throughput ratio decreases when delay in link increases. However it is clear from the results that our proposed scheme is performing more efficiently as compared to current handover scheme. At each point our proposed scheme gives much higher throughput ratio than HMIPv6.

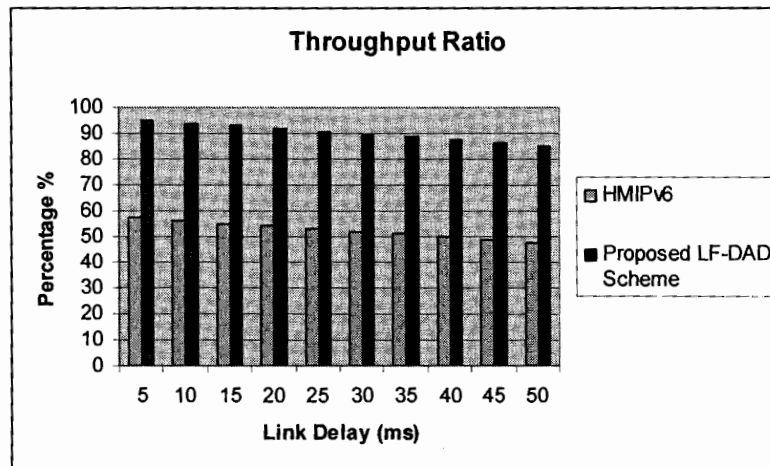


Figure 5.5: Throughput Ratio with changing Link Delays

5.3.3 Simulation results for changing DAD time

Handover Latency

Figure 5.6 shows the impact of DAD time on the handover process. DAD time takes 1000 to 1500ms (in the worst case) to complete. We have shown that how DAD time affects the handover latency. The point 0ms on x-axis of the graph shows the handover latency when the DAD time was avoided by our proposed scheme

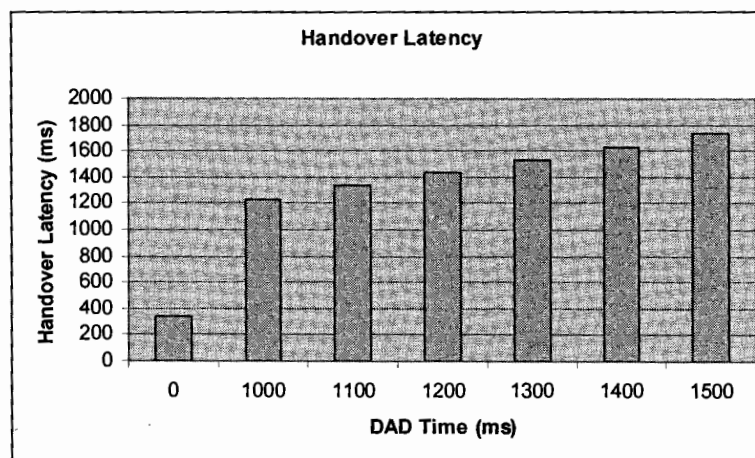


Figure 5.6: Handover Latency for changing DAD Time

Packet Loss Ratio

The packet loss ratios for varying DAD time are given in figure 5.7. Here we can notice that packet loss ratio increases as long as DAD takes time to complete. The value 0 on x-axis shows the results of our proposed scheme. Even if DAD completes in its best case, i.e. 1000ms, the loss ratio is almost 33% while our proposed scheme reduced this ratio to 9.5%.

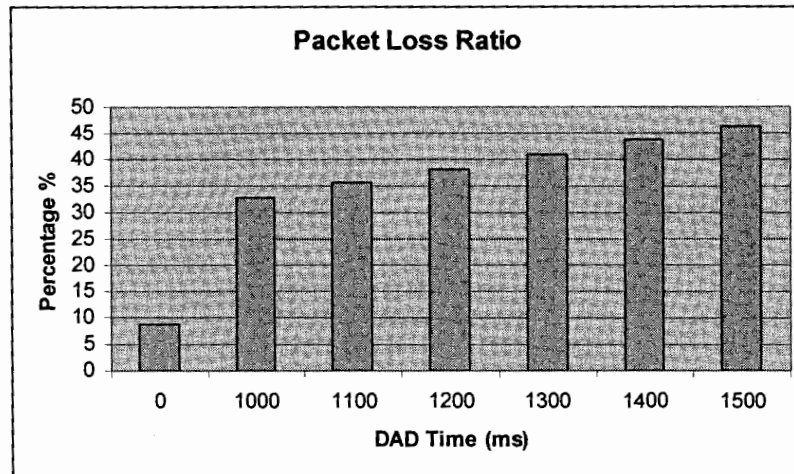


Figure 5.7: Packet Loss Ratio for changing DAD Time

Average One-Way-Delay (O.W.D)

The result of one-way-delay for both schemes is almost similar and shows a constant behavior each time. It means that DAD time has no impact on one-way-delay.

Average O.W.D for HMIPv6 = 241.69 ms

Average O.W.D for LF-DAD = 241.84 ms

Throughput Ratio

Figure 5.8 shows the impact of DAD time on throughput ratio. Longer the DAD takes to complete will minimize the throughput ratio. The maximum highest throughput ratio we can obtain in the presence of DAD is approximately 67%, in the case where DAD ends in

its best case i.e. 1000ms. On the other hand our proposed scheme provides a throughput upto 91.5% approximately.

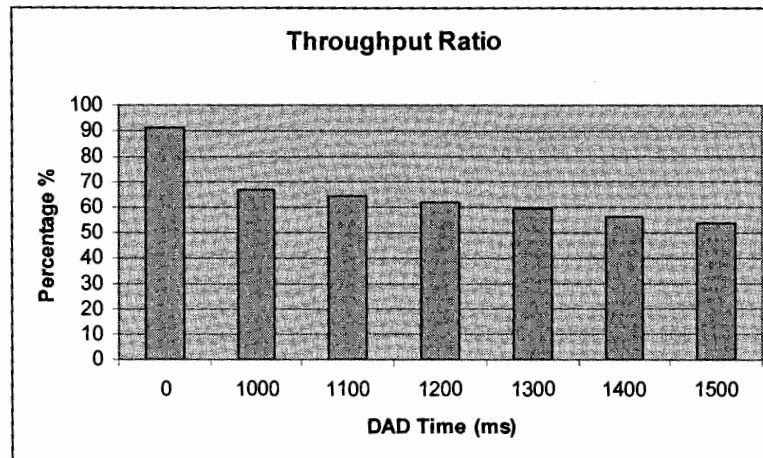


Figure 5.8: Throughput Ratio for changing DAD Time

5.3.4 Simulations results for changing Node Speed

Handover Latency

Figure 5.9 shows the impact of MN speed on the handover process. The results for both schemes have been compared and it is understood that our proposed scheme is performing well as compared to HMIPv6 handover scheme. In both cases the graphs shows a constant behavior which means that the speed of MN has a very low impact on handover latency as there is a very slight variation seen in the results for each scheme. However the performance improvement of our proposed scheme is very clear from the results.

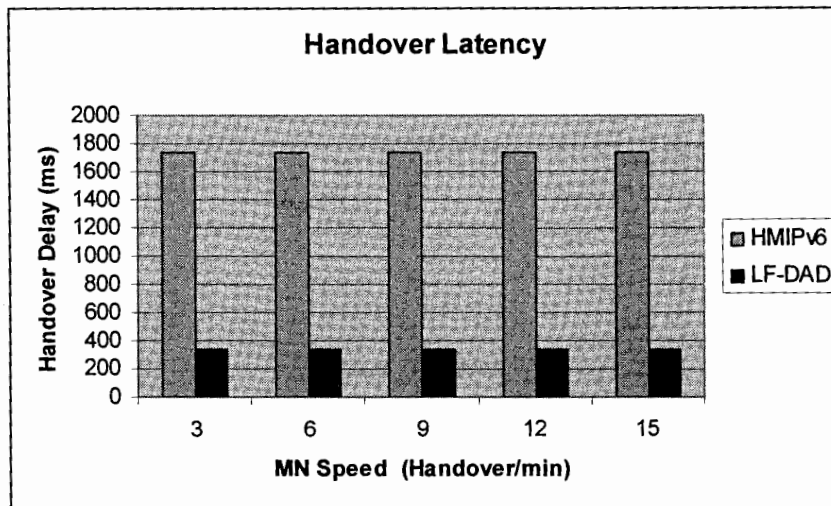


Figure 5.9: Handover Latency for changing MN Speed

Packet Loss Ratio

The impact of MN speed on the packet loss ratio is in figure 5.10. Here we can notice that for both schemes the packet loss ratio increases as the MN speed increases. This is because when the MN speed increases it remains attached to an AR for a shorter time. The comparison of both schemes under varying speed shows that our proposed scheme has reduced the packet loss to greater extent than HMIPv6.

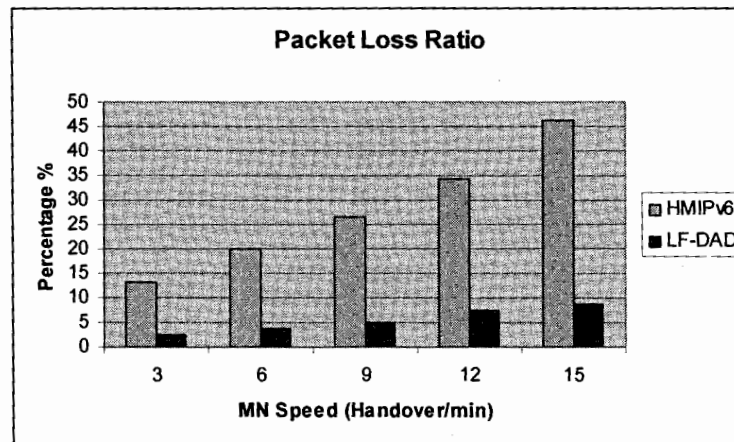


Figure 5.10: Packet Loss Ratio for changing MN Speed

Average One-Way-Delay (O.W.D)

The result of one-way-delay for both schemes is almost similar and shows a constant behavior each time. It means that speed of MN do not have any significant impact on One-Way-Delay.

Average O.W.D for HMIPv6 = 241.7 ms

Average O.W.D for LF-DAD = 241.66 ms

Throughput Ratio

Figure 5.11 shows the impact of MN speed on the throughput ratio. In both schemes the throughput ratio decreases as the speed of MN increases. Results show that our proposed scheme is giving high throughput ratio as compared to HMIPv6. If we observe closely we will find that the on changing the MN speed the throughput ratio for HMIPv6 scheme is decreasing in the range 90 to 50, while that for our proposed scheme is decreasing within the range 90 to 100. This shows that our proposed scheme gives higher throughput ratio in varying MN speeds.

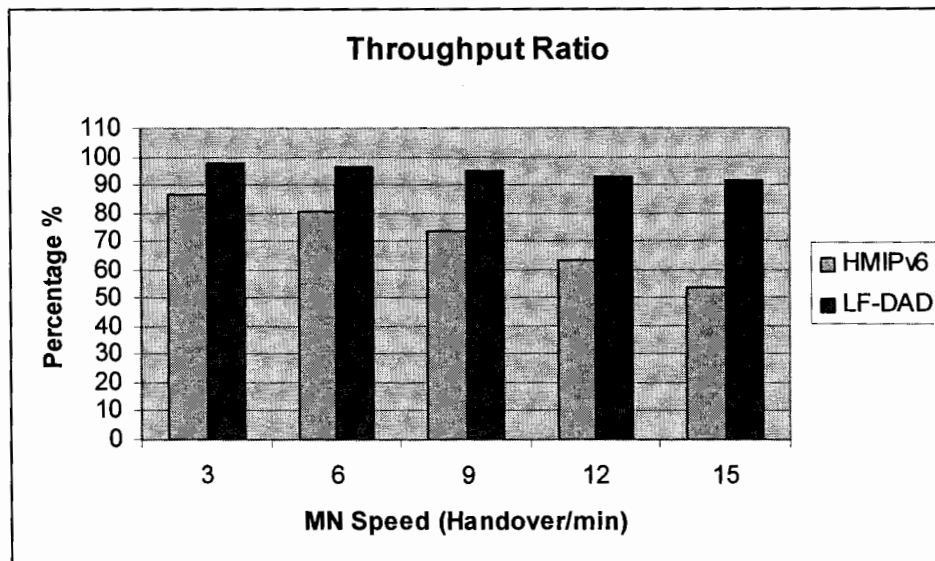


Figure 5.11: Throughput Ratio for changing MN Speed

5.4 Major Conclusions about the impact on handover process

The performance of the handovers is greatly affected by a number of reasons including address configuration and address verification processes in HMIPv6 networks. Besides these reasons there are other reasons which may affect the handover process in certain ways. Some of these are those that were targeted in this thesis like MN speed, DAD time, Handover frequency and link delays. Collectively, these are all the factors that impact the handover process and must be considered for performance evaluation. Following subsection shows a comparative study of both the schemes in a summarized form.

Comparative analysis of HMIPv6 and proposed LF-DAD scheme

Both the schemes are tested in some varying conditions and experiments were conducted in order to present the performance of our proposed scheme. Four major experiments were conducted for Handover frequency, Link delay, DAD time and MN speed. In each experiment several tests are carried out and results were obtained for four metrics, namely, handover latency, packet loss ratio, one-way-delay and throughput ratio. From the results it is clear that the link delays and DAD time affect the handover latency to a large extent while handover frequency and MN speed has a low impact on handover delay as the graphs shows very slight variation for these factors. However, in all four experiments our proposed scheme gives extremely better performance as compared to current HMIPv6 handover scheme. Results for packet loss show that all these factors have significant impact on packet loss. Packet loss increases as any of these factor increases. In all cases our proposed scheme has reduced the packets loss to greater extent. The results for one-way-delay showed almost constant delay in all experiments. It means that these factors have no or extremely low effect on one-way-delay. Throughput is badly affected by HMIPv6 handover scheme because of longer handover latencies. Our proposed scheme shortened the handover latency and thus in all experiments our proposed solution have improved throughput as compared to current HMIPv6 scheme.

5.5 Summary

This chapter details about the performances metrics and the simulations results have been presented. We have chosen handover latency, packet loss ratio, One-Way-Delay and Throughput ratio as performance metrics. Each scheme is tested for varying handover frequency, link delay, DAD time and MN speed and then we have presented our results and conclusions.

6

Conclusion and Future work

In this chapter we will summarize our conclusions about the thesis and will present the future dimensions of this work.

6.1 Achievements

The main achievements of this project can be summarized as follows.

- The main contribution of this research project is the reduction of handover latencies in Hierarchical Mobile IPv6 networks.
- We achieved our goal by presenting a more efficient handover scheme, which reduced the handover latency noticed in HMIPv6 micro mobility handoff process.
- We have modified the actual handover process of HMIP handover process and have given a scheme which reduces the frequency of Duplicate Address Detection (DAD), during local handovers in a MAP domain, called LF-DAD scheme.
- We have analyzed the performance optimization of HMIPv6 protocol by comparing both schemes.
- We have calculated some performance metrics for both the schemes and have come up with some useful and meaningful results.

- The results we have gotten during our simulation process are both statistical (numerical values) and visual, i.e. results can be viewed in the Network Animator (NAM).

6.2 Conclusion

We have analyzed the HMIPv6 handover process in a micro mobility domain and realized that the base HMIPv6 protocol is performing poor for local handovers within a particular domain. We have identified the reasons for this bad performance and proposed another scheme for micro mobility handovers called Less-Frequent DAD scheme. We performed several tests using NS2 simulation in order to present the performance optimization of our proposed scheme against the current scheme. Several experiments were performed to obtain results based on the four main metrics handover latency, packet loss, delay and throughput. These experiments are conducted under several changing environments like effect of handovers, effect of node speed, effect of DAD time and effect of link delay. The experiments were conducted for both schemes and the results of both the schemes were compared. From the simulation study and the calculated performance metrics it is obvious that our proposed scheme works more efficiently than current HMIPv6 handover process.

The only drawback of our proposed scheme is that the MAP cache will increase by a large amount when the number of MN increases in the networks. In case of large number of MNs in a MAP domain, even then the cache look up time takes less time than DAD check.

6.3 Future work

In mobile IP networks the MN visits different networks performing handover to different ARs. During this process the MN can neither send nor receives data until and unless it completes its registration process with the visiting router. It means that in MIP and all its extensions including HMIPv6 the handover delay needs to be kept as minimum as

possible to reduce packet loss and improve throughput. The most time consuming part in a HMIPv6 handover process is the address configuration and verification. Verification of address was done through DAD process which was targeted in this thesis. The Address configuration is still carried out on each visit and in HMIPv6 a MN configure two CoAs when moved from domain to another. So researchers should propose some efficient schemes based on context transfer methods where the MN no longer need address configuration and could be able to use a single address within a MAP domain without the need to change the address on each visit.

6.4 Summary

In this chapter we have concluded our work and the future dimensions of our work. The performance of handover procedure in MIP networks is greatly affected by the address configuration and verification time. So there is the need to develop some more efficient schemes or techniques like context transfer in order to avoid such kind of delays in handover process.

References

1. Dong-cheol Shin, Sung-gi Min, "Fast Handover Solution using Multi-tunnel in HMIPv6", 2008.
2. Sun Wei, Chen Lin, Song Jian, "An Improved DAD Check Scheme MLD-Based in HMIPv6", IEEE, 2007.
3. J. Arkko, C. Vogt, W. Haddad, "Enhanced Route Optimization for Mobile IPv6", RFC 4866, May 2007.
4. M.H. Habaebi, I. Vivaldi, B.M. Ali, V. Prakash, "Macro/Micro-Mobility Fast handover in Hierarchical Mobile IPv6", *Computer Communications, Volume 29, Issue 11, 26 July 2006*.
5. A. Forte, S. Shin, H. Schulzrinne, "Passive Duplicate Address Detection for Dynamic Host Configuration Protocol (DHCP)", September 2005.
6. May Siksik, Hussein Alnuweiri, Saif Zahir, "A Detailed Characterization Of The Handover process Using Mobile IPv6 In 802.11 Networks", 2005.
7. H. Soliman, C. Castelluccia, K. El Malki and L. Bellier, "Hierarchical Mobile IPv6 Mobility Management (HMIPv6)", IETF RFC 4140, Aug. 2005 *Work in progress*
8. R. Koodli, "Fast handovers for mobile IPv6", RFC 4068, July 2005.
9. Hee Young Jung, Hesham Soliman, Seok Joo Koh, "Fast Handover for Hierarchical MIPv6", Internet Draft, April 2005.
10. D. Johnson and C. Perkins, "Mobility Support in IPv6", IETF RFC 3775, 2004
11. J. Manner, Ed., M. Kijoj, Ed., "Mobility Related Terminologies", June 2004.

12. Y. Han, J. Choi and H. Jang, "Advance Duplicate Address Detection, "IETF Internet Draft, Dec 2003.
13. JinHyeock Choi, Greg Haley, "Router Advertisement Issues for Movement Detection/Detection of Network Attachment", Internet Draft, October 2003.
14. Vivaldi I., Habaebi M.H, Ali B.M, Prakesh V., "Fast handover algorithm for hierarchical mobile IPv6 macro-mobility management", September 2003.
15. Hee Young Jung, Seok Joo Koh, Dae Young Kim, "Address Pool Based Stateful NCoA configuration for FMIP v6", Internet Draft, August 2003.
16. C. Perkins. Ed., "IP Mobility Support for IPv4", RFC 3344, August 2002.
17. R. Droms, J. Bounds, Hewlett Packard, B. Volz, et, "Dynamic Host Configuration Protocol for IPv6", RFC 3315, July 2003.
18. M. Bagnulo, I. Soto, A. García, A. Azcorra, "Random generation of interface identifiers", <draft-soto-mobileip-random-iids-00.txt>, January 2002.
19. T. Narten, E. Nordmark, W. Simpson, "Neighbor Discovery for IP Version 6", RFC 2461, December 1998.
20. A. Conta, S. Deering, "Internet Control Message Protocol (ICMPv6) for Internet Protocol Version 6 (IPv6) Specification", RFC 2463, December 1998.
21. S. Thomson, T. Narten, "IPv6 Stateless Address Autoconfiguration", RFC 2462, Dec 1998.
22. S. Deering, R. Hinden, "Internet Protocol Version 6 Specification", IETF RFC 2461, 1998.
23. Behrouz A. Forouzan, "TCP/IP Protocol Suit", Second Edition.
24. Hyewon K. Lee, "Understanding IPv6".
- 25 Chaskar, H., Ed. "Requirments of a Quality of Service (QoS) Solution for Mobile IP", RFC 3585, September 2003.
- 26 Z. D. Shelby, D. Gatzounas, A. T. Campbell, C-Y. Wan, "Cellular IPv6", Internet draft, draft-shelby-seamoby-cellularipv6-00.txt, IETF Mobile IP Working Group Document, November 2000.
- 27 C. Perkins, "IP Mobility Support for IPv4", IETF RFC 2002, Oct 1996.

- 28 S. Soliman, C. Castelluccia, K. ElMalki, "Hierarchical Mobile IPv6 (HMIPv6) Mobility management", RFC 5380, Oct 2008"
- 29 N. Moore, "Optimistic Duplicate Address Detection (DAD) for IPv6", IETF RFC 4429, April 2006.
30. Y. H. Han, S. H. Hwang, "Care-of address provisioning for efficient IPv6 mobility support", 2006.
31. Chien-C. Tseng, Yung-C. Wong, Li-H. Yen, "Proactive DAD: A Fast Address-Acquisition Strategy for Mobile IPv6 Networks", Dec 2006.
- 32 S. Deering, W. Fenner, B. Haberman, "Multicast Listener Discovery for IPv6", IETF RFC 2710, October 1999.
- 33 R. Vida, L. Costa, "Multicast Listener Discovery Version 2 (MLDv2) for IPv6", IETF RFC 3810, June 2004.
- 34 Greg Daley, Richard Nelson, "Duplicate Address Detection Optimization using IPv6 Multicast Listener Discovery", Internet Draft, Expired Sep 2003
- 35 F. Xia, B. Sarikaya, "Duplicate Address Detection Optimization Using Enhanced Neighbor Discovery", Internet Draft, Expired June 2007
- 36 B. Park, S. Lee, H. Latchman, "A Fast Neighbor Discovery and DAD Scheme for Fast Handover in Mobile IPv6 Network", 2006
- 37 P. Harini, O. B. V. Ramanaiah, "An Efficient DAD Scheme for Hierarchical Mobile IPv6 Handoff", International Journal of Computer Science and Network Security, VoL.8, August 2008.
- 38 Kilian Weniger, "Passive duplicate address detection in mobile ad hoc networks", 2004.
- 39 Zheming Li, Ling Li, Y. Huang, "Research on Handover in Hierarchical Mobile IPv6 based on Fast DAD mechanism in Visual Domain", 2008.
- 40 Khalid E. Aldalaty, "Mobile IP Handover Reduction Using Seamless Handover Architecture", Blekinge Institute of Technology, August 2009.
- 41 P. Sotthivirat, P. Pongpaibool, S. Kistisin, Chavalit S. , "Fast and Robust Duplicate Address Detection for Mobile IPv6", 2008
- 42 S. Deering, "ICMP Router Discovery Message", IETF RFC 1256, Sep 1991
- 43 "The Network Simulator – ns (version 2) Website", <http://www.isi.edu/nsnam/ns>

- 44 Reza Malekian, "The Study of Handover in Mobile IP Network", Third International Conference on Broadband Communication, IT and Biomedical Applications, 2008.
- 45 S. Lee, E. Kim, T. Lim, S. Jeong, J. Park, "Micromobility Management Enhancement for Fast Handover in HMIPv6 Based Real-Time Applications", 2007.
- 46 Andrew T. Campbell, J. Gomez, S. Kim, "Comparison of IP Micro-Mobility Protocols", 2005.
- 47 Bagnulo, Soto. I, Garcia, Martneza, Azcorra, A., "Random Generation of Interface Identifier", Internet Draft, 2002.
- 48 Hsieh, R., Zhou, Z.-G., and Seneviratne, "A. S-MIP: A Seamless Handoff Architecture for Mobile IP", In *Proceedings of INFOCOM*, San Francisco, 2003
- 49 "The Columbia IP micro mobility Suite for Network Simulator NS2", home page, S Source Code Distribution for Cellular IP, Hawaii and Hierarchical Mobile IP, April 2007
- 50 CIMS for NS2.31 upgrads, <http://tagus.inesc-id.pt/~pestrela/ns2/ist-cims.html>
- 51 OPNET, OPNET Technologies, Inc, Home page, <http://www.opnet.com/>
- 52 "The NS Manual", <http://www.isi.edu/nsnam/ns/ns-documentation.html>
- 53 "Tutorial for the Network Simulator ns", <http://www.isi.edu/nsnam/ns/tutorial/>
- 54 Padro V Estrela, "NS2 IP Mobility", <http://tagus.inescid.pt/~pestrela/ns2/mobility.htm>
- 55 "NS2 help and support", <http://mailman.isi.edu/mailman/listinfo/ns-users>
- 56 Panita Pongpaibool, P. Sotthivirat, Sukumal I. Kitisin, C. Srisathapornphat, "Fast Duplicate Address Detection for Mobile IPv6", 2007.

Table of Acronym

MIPv6	Mobile Internet Protocol Version 6
FMIPv6	Fast Mobile Internet Protocol Version 6
HMIPv6	Hierarchical Mobile Internet Protocol Version 6
MN	Mobile Node
CN	Corresponding Node
HA	Home Agent
MAP	Mobility Anchor Point
AR	Access Router
nAR	New Access Router
pAR	Previous Access Router
RA	Router Advertisement
RtrSol	Router Solicitation
RtrAdv	Router Advertisement
BU	Binding Update
BAck	Binding Acknowledgement
DAD	Duplicate Address Detection
FNA	Fast Neighbor Advertisement
NAAK	Neighbor Advertisement Acknowledgement
CoA	Care of Address
RCoA	Regional Care of Address
LCoA	Local Care of Address
nCoA	New Care of Address
pCoA	Previous Care of Address