SMART SELECTION HIERARCHICAL MOBILE INTERNET PROTOCOL
VERSION 6 WITH LOAD BALANCING AND MOBILITY
ANCHOR POINTS QUEUE MANAGEMENT

MA’EN TAYSEER EKRAYRM AL-RASHDAN

THESIS SUBMITTED IN FULFILLMENT FOR THE DEGREE OF DOCTOR OF PHILOSOPHY

FACULTY OF ENGINEERING AND BUILT ENVIRONMENT
UNIVERSITI KEBANGSAAN MALAYSIA
BANGI

2011
DECLARATION

I hereby declare that the thesis is based on my original work except for quotations and citations which have been duly acknowledged.

Date

MA’EN TAYSEER ALRASHDAN
P31452
ACKNOWLEDGMENT

In the name of Allah, the Almighty Lord, the Most Gracious and Merciful.
Praise be to Allah who has given me the strength, inspiration and prudence to bring this study to close. Peace be upon His messenger Muhammad and his honorable family.
Throughout this academic quest, the following people have generously granted their precious guidance and never-ending assistance for which I am eternally grateful.
First of all, I would like to express my deepest gratitude to my supervisor, Professor Dr Mahamod Ismail and my co-supervisor Professor Dr Kasmiran Jumari, for their immeasurable wisdom, endless patience and ever constructive comments.
I am also indebted to my beloved parents, wife and brothers. A big thank you may not be enough for their encouragement, understanding, tolerance and prayers that acts as a giant support for my success.
My thanks also go to all the staff at the Department of Electrical, Electronic and Systems Engineering, (Universiti Kebangsaan Malaysia) for their cooperation and helpfulness in academic matters.
Last but not least in recollection of my much kindness, continuous encouragement for perseverance and patience, my grateful thanks to all my friends and colleagues wherever they may be. Thank you.
ABSTRACT

The increasing demands of Internet applications with mobility support give a great challenge in providing an efficient mechanism for mobile wireless access. The Internet Engineering Task Force (IETF) standardized the Mobile Internet Protocol (MIP) and MIP version 6 (MIPv6) to make the communication for the wireless access more efficient. However, the service quality of the MIPv6 is degraded because of extra signaling and long transmission due to latency resulted from excessive address translation. Hierarchical MIPv6 (HMIPv6) was introduced to achieve the best scalable solution for global mobility by dividing the world into domains. HMIPv6 regional registration adopted a Mobility Anchor Point (MAP) to control the visited Mobile Nodes (MN) in the domain to reduce the number of Location Updates (LU) in the home network. The MAP in the Foreign Agent (FA) area intercepts all the packets addressed to the MN and then tunnels them to the On-link Care of Address (LCoA) of the MN in the FA area. Nevertheless, HMIPv6 still unable to resolve the problem of scalability besides its high location updates cost, high packet delivery delay and large number of lost packets particularly when huge number of MNs visits the domain. The main objective of this thesis is to propose, analyze and evaluate an enhanced HMIPv6 called Smart Selection Hierarchical Mobile IPv6 (SSHMIPv6) to encounter those problems. SSMIPv6 has a domain consisting of multiple MAPs using the same Regional Care of Address (RCoA) and each MAP in the domain is attached to an Access Router (AR). SSMIPv6 environment have been simulated and used to evaluate the performance of SSMIPv6 over HMIPv6 and to analyze the effect of adding multiple MAPs to serve each region using the Join Shortest Queue (JSQ) selection scheme. Then a load balancing strategy was introduced by ascendingly sorting the multiple MAPs having the same RCoA and attached with the same Access Routers in the SSMIPv6 domains which adopt the HMIPv6 protocols. Simulation shows that SSMIPv6 outperforms HMIPv6 in term of packet delay, lost packets, Goodput, and location update cost. In terms of the average packet transfer delay the average percentage reduction between using one MAP and two MAPs is 51 %. Taking into consideration the lost packet ratio, an average percentage reduction of 20 % was observed between when using one MAP and two MAPs. Finally, an application of SSMIPv6, a concept of incorporated domains is simulated that allows adjacent domains to be incorporated together while keeping their MAPs sharing the same RCoA. It is found out that about 30% to 60% reduction in the location update cost was achieved. From the results above, we can conclude that SSMIPv6 can solve the scalability problem because more mobile nodes are able to be handled and better served in the foreign domain.
PEMILIHAN PINTAR PROTOKOL INTERNET VERSI 6 BERGERAK HIRAKI DENGAN PENGIMBANGAN BEBAN DAN PENGURUSAN GILIRAN TITIK SAUH BOLEHGERAK

ABSTRAK
Permintaan aplikasi Internet yang disokong dengan kebolehgerakan memberikan cabaran yang besar dalam menyediakan mekanisme bagi capaian tanpa wayar bergerak yang cekap. Pasukan Petugas Kejuruteraan Internet (IETF) telah mempapai Protokol Internet Bergerak (MIP) dan MIP versi 6 (MIPv6) untuk membolehkan komunikasi bagi capaian tanpa wayar lebih cepat. Sungguhpun demikian, kualiti perkhidmatan MIPv6 menurun kerana pengisyaratan yang berlebihan dan penghantaran yang lama akibat lengah yang terhasil daripada terjepihan alamat yang melampau. Oleh itu, MIPv6 Berhiraki (HMIPv6) telah diperkenalkan untuk mencapai penyelesaian bolehskala yang terbaik bagi kebolehgerakan sejagat dengan membagahikan dunia kepada domain-domain. Pendaftaran kawasan HMIPv6 menggunakan Titik Sauh Kebolehgerakan (MAP) bagi mengawal Nod Bergerak (MN) Pelawat dalam domain untuk mengurangkan Kemaskini Lokasi (LU) dalam rangkaian perumah. MAP dalam kawasan Agen Pelawat (FA) akan memintas semua paket yang dialamatkan ke MN dan kemudian melorot paket tersebut ke Alamat Bertanggungjawab Atas-Pautan (LCoA) bagi MN dalam kawasan FA. Walau bagaimanapun, HMIPv6 masih tidak berupaya untuk menyelesaikan masalah kebolehskalaan di samping mempunyai kos kemaskini dan lengah penghantaran paket yang tinggi dan bilangan kehilangan paket yang besar khususnya apabila bilangan MN yang melawat domain sangat besar. Objektif utama tesis ini adalah untuk mencadang, menganalisis dan menilai HMIPv6 yang ditambahbaik iaitu Pemilihan Pintar IPv6 Bergerak Berhiraki (SSHMIPv6) bagi mengatasi masalah-masalah tersebut. SSHMIPv6 mempunyai satu domain yang mengandungi berbilang MAP dengan menggunakan Alamat Bertanggungjawab Kawasan (RCoA) yang sama dan setiap MAP dalam domain disambung kepada Perout Capaian (AR). Persekitaran SSHMIPv6 telah disimulasi dan digunakan bagi menilai prestasi SSHMIPv6 terhadap HMIPv6 dan menganalisis kesan penambahan berbilang MAP untuk melayan setiap kawasan menggunakan skema pemilihan Giliran Bersambung Terpendek (JSQ). Seterusnya strategi pengimbangan beban telah diperkenalkan dengan menyusun secara menurun berbilang MAP yang mempunyai RCoA yang sama dan disambungkan kepada AR yang sama dalam domain SSHMIPv6 yang menggunakan protokol HMIPv6. Simulasi menunjukkan bahawa SSHMIPv6 mengatasi HMIPv6 dari segi lengah paket, kehilangan paket, kadar data berkesan dan kos kemaskini lokasi. Dari segi lengah penghantaran paket purata, pengurangan peratusan purata antara satu dan dua MAP ialah 51%. Dengan mempertimbangkan nisbah kehilangan paket, pengurangan peratusan purata sebanyak 20% diperolehi apabila satu dan dua MAP digunakan. Akhirnya, suatu aplikasi SSHMIPv6 iaitu suatu konsep domain bersebelahan telah disimulasi yang membolehkan domain bersebelahan turut bergabung dengan mengekalkan MAP berkongsi RCoA yang sama. Daripada simulasi di atas didapati bahawa pengurangan lebih kurang 30% hingga 60% kos kemaskini lokasi tercapai. Daripada semua keputusan di atas, adalah dapat disimpulkan bahawa SSHMIPv6 boleh menyelesaikan masalah kebolehskalaan kerana lebih banyak nod bergerak berupaya dikelolakan dan dilayan dengan baik dalam domain pelawat.
# CONTENTS

**DECLARATION**  

**ACKNOWLEDGMENT**  

**ABSTRACT**  

**ABSTRAK**  

**CONTENTS**  

**LIST OF FIGURES**  

**LIST OF TABLES**  

**LIST OF ABBREVIATIONS**  

<table>
<thead>
<tr>
<th>CHAPTER I</th>
<th>INTRODUCTION</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>Introduction</td>
<td>1</td>
</tr>
<tr>
<td>1.2</td>
<td>Internet of things</td>
<td>4</td>
</tr>
<tr>
<td>1.2.1</td>
<td>Consumer Electronic Gadgets</td>
<td>5</td>
</tr>
<tr>
<td>1.2.2</td>
<td>Micro-Computers</td>
<td>5</td>
</tr>
<tr>
<td>1.2.3</td>
<td>Scalability</td>
<td>6</td>
</tr>
<tr>
<td>1.3</td>
<td>Problem statement</td>
<td>7</td>
</tr>
<tr>
<td>1.4</td>
<td>Research objectives and scope</td>
<td>8</td>
</tr>
<tr>
<td>1.5</td>
<td>Research contribution</td>
<td>9</td>
</tr>
<tr>
<td>1.6</td>
<td>Thesis organization</td>
<td>9</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CHAPTER II</th>
<th>LITERATURE REVIEW</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>Introduction</td>
<td>11</td>
</tr>
<tr>
<td>2.2</td>
<td>Internet Protocol version 4</td>
<td>13</td>
</tr>
<tr>
<td>2.2.1</td>
<td>IPv4 addressing (Spaces and Formats)</td>
<td>14</td>
</tr>
<tr>
<td>2.3</td>
<td>Mobile IP</td>
<td>15</td>
</tr>
<tr>
<td>2.3.1</td>
<td>Movement detection</td>
<td>15</td>
</tr>
<tr>
<td>2.3.2</td>
<td>Location registration</td>
<td>15</td>
</tr>
<tr>
<td>2.3.3</td>
<td>Handoff management</td>
<td>17</td>
</tr>
</tbody>
</table>
2.3.4 Limitations of Mobile IP

2.4 IP version six
2.4.1 Neighbor discovery
2.4.2 Address autoconfiguration
2.4.3 Tunneling

2.5 Mobile IPv6
2.5.1 Mobile IP components
2.5.2 Mobility over IPv6

2.6 Security

2.7 IPv6 versus IPv4
2.7.1 IPv6 design considerations
2.7.2 Inadequacies of IPv4
2.7.3 IPv6 characteristic outlines
2.7.4 Mobile IPv6
2.7.5 Fast Handover MIPv6

2.8 HMIPv6
2.8.1 MN operation
2.8.2 MAP operations
2.8.3 Regional Registrations MIPv6 (RRMIPv6)

2.9 IPv6 researches over NS-2

2.10 Related studies
2.10.1 Dynamic efficient MAP selection (DEMAPS)
2.10.2 MAP selection based on moving direction pattern
2.10.3 Effects of network topology on MAPs selection
2.10.4 Adaptive Route Optimization (ARO)
2.10.5 Cooperative diversity in PHMIPv6
2.10.6 Hybrid Location-Update scheme for mobile networks

2.11 Summary

CHAPTER III METHODOLOGY

3.1 Introduction
3.2 Selection scheme In HMIPv6
3.3 Smart Selection Hierarchical Mobile IPv6 (SSHMIPv6)
3.3.1 MAP reassignment in SSHMIPv6 68
3.4 Simulation environment 70
3.5 Simulation model 74
3.5.1 Program initialization 74
3.5.2 Packet generation 75
3.5.3 Packet delivery 77
3.5.4 Performance metrics 79
3.6 SSHMIPv6 simulation using Network Simulator NS-2 85
3.6.1 the simulation tools: NS-2 85
3.6.2 Simulation model topology 86
3.7 Summary 87

CHAPTER IV RESULTS AND ANALYSIS 89
4.1 Introduction 89
4.2 Results and discussions 89
4.3 Lost packets performance analysis through NS-2 104
4.4 Summary 107

CHAPTER V INCORPORATED DOMAINS 108
5.1 Introduction 108
5.2 Incorporated domains in HMIPv6 108
5.3 Concept and characteristics of incorporated domains 110
5.4 Mathematical model analysis 111
5.5 Simulation 112
5.5.1 Cost due to changing the AR 112
5.5.2 Cost due to changing the MAP 113
5.5.3 The simulation GUI 113
5.6 Performance of location update in incorporated domains 117
5.7 Summary 122

CHAPTER VI CONCLUSION 123
6.1 Introduction 123
6.1 Conclusion 124
6.2 Future work 125

REFERENCES 126
APPENDIX A 134
APPENDIX B 138
APPENDIX C 141
APPENDIX D 144
# LIST OF FIGURES

<table>
<thead>
<tr>
<th>Figure No.</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>Mobile IP architecture</td>
<td>2</td>
</tr>
<tr>
<td>1.2</td>
<td>HMIPv6 Domain</td>
<td>4</td>
</tr>
<tr>
<td>2.1</td>
<td>Mobile IPv4 architecture</td>
<td>15</td>
</tr>
<tr>
<td>2.2</td>
<td>Mobile IP location registration</td>
<td>16</td>
</tr>
<tr>
<td>2.3</td>
<td>Mobile IP handoff with binding from FA to another FA</td>
<td>17</td>
</tr>
<tr>
<td>2.4</td>
<td>Mobile IP handoff without binding from FA to another FA</td>
<td>18</td>
</tr>
<tr>
<td>2.5</td>
<td>Encapsulated and normal packet</td>
<td>26</td>
</tr>
<tr>
<td>2.6</td>
<td>Data Flow for Mobile IPv6</td>
<td>30</td>
</tr>
<tr>
<td>2.7</td>
<td>ICMPv6 HA Discovery Request</td>
<td>32</td>
</tr>
<tr>
<td>2.8</td>
<td>ICMPv6 HA Discovery Reply</td>
<td>33</td>
</tr>
<tr>
<td>2.9</td>
<td>Binding Update</td>
<td>33</td>
</tr>
<tr>
<td>2.10</td>
<td>Binding Acknowledge</td>
<td>34</td>
</tr>
<tr>
<td>2.11</td>
<td>Binding Request</td>
<td>34</td>
</tr>
<tr>
<td>2.12</td>
<td>IPv4 problems</td>
<td>37</td>
</tr>
<tr>
<td>2.13</td>
<td>IPv6 address scopes</td>
<td>39</td>
</tr>
<tr>
<td>2.14</td>
<td>MIPv6 handover</td>
<td>43</td>
</tr>
<tr>
<td>2.15</td>
<td>HMIPv6 Domain</td>
<td>48</td>
</tr>
<tr>
<td>2.16</td>
<td>HMIPv6 routing scheme</td>
<td>49</td>
</tr>
<tr>
<td>2.17</td>
<td>Packet flow in RRMIIPv6 for MN in the Domain</td>
<td>55</td>
</tr>
<tr>
<td>3.1</td>
<td>Packets flow to the MAP in HMIPv6</td>
<td>65</td>
</tr>
<tr>
<td>3.2</td>
<td>Methodology Block Diagram</td>
<td>66</td>
</tr>
<tr>
<td>3.3</td>
<td>Smart Selection Hierarchical Mobile IPv6 architecture</td>
<td>67</td>
</tr>
<tr>
<td>3.4</td>
<td>Packets flow in SSHMIPv6</td>
<td>68</td>
</tr>
<tr>
<td>3.5</td>
<td>SSHMIPv6 routing scheme</td>
<td>70</td>
</tr>
<tr>
<td>3.6</td>
<td>(a) Hypothetical HMIPv6 Internet consists of five domains, (b)</td>
<td>71</td>
</tr>
<tr>
<td></td>
<td>Hypothetical SSHMIPv6 Internet consists of five domains</td>
<td></td>
</tr>
<tr>
<td>3.7</td>
<td>The MAP Queue</td>
<td>73</td>
</tr>
<tr>
<td>3.8</td>
<td>Sample Program Screen-Shot</td>
<td>75</td>
</tr>
<tr>
<td>3.9</td>
<td>The empty MAP Queue</td>
<td>78</td>
</tr>
</tbody>
</table>
3.10 The packet occupation in the MAP Queue
3.11 The MAP Queue full of Packets
3.12 The simulation results display
3.13 Network topology of the simulation carried out in NS-2
4.1 Average Packet Delay versus Number of MAPs at each Area
4.2 Number of lost Packets versus number of MAPs at each Area
4.3 Lost Packets Ratio versus Number of MAPs at each Area
4.4 Average Packet Delay versus Number of Maps at each Area
4.5 Number of lost packet versus number of MAPs at each area
4.6 Lost Packets Ratios versus Number of MAPs at each Area
4.7 Goodput versus Number of MAPs at each Area
4.8 Average packet delay versus number of MAPs
4.9 Number of lost packets versus number of MAPs
4.10 Lost Packets Ratio versus number of MAPs
4.11 Goodput versus number of MAPs
4.12 Average packet delay versus number of MAPs
4.13 Number of lost packets versus number of MAPs
4.14 Lost Packets Ratio versus number of MAPs
4.15 Goodput versus number of MAPs
4.16 No. of lost packet for data flow of 1200 packets under HMIPv6
4.17 No. of lost packet for data flow of 300 packets under SSHMIPv6
4.18 No. of lost packet for data flow of 400 packets under SSHMIPv6
4.19 No. of lost packet for data flow of 500 packets under SSHMIPv6
4.20 Comparison between SSHMIPv6 and HMIPv6
5.1 Incorporated domain HMIPv6 architecture
5.2 Possible configuration in the simulation software for incorporated domains
5.3 Entering the traveling path of the Mobile Node
5.4 Cost calculation
5.5 Location Update Cost
5.6 Total Cost Versus Number of Mobile Nodes
5.7 Improvement Percentage versus Number of Mobile Nodes
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8</td>
<td>Number of domains inside each incorporated domain versus Cost reduction</td>
<td>119</td>
</tr>
<tr>
<td>5.9</td>
<td>Percentage of Cost Reduction versus Number of Domains inside each incorporated domains</td>
<td>120</td>
</tr>
<tr>
<td>5.10</td>
<td>Worst Case Scenario for MN path</td>
<td>121</td>
</tr>
<tr>
<td>5.11</td>
<td>Best case scenario</td>
<td>121</td>
</tr>
</tbody>
</table>
## LIST OF TABLES

<table>
<thead>
<tr>
<th>Table No.</th>
<th>Table Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>Comparisons between IPv4 and IPv6</td>
<td>45</td>
</tr>
<tr>
<td>3.1</td>
<td>Load balance table</td>
<td>69</td>
</tr>
<tr>
<td>3.2</td>
<td>Parameters specification applied in simulation</td>
<td>72</td>
</tr>
<tr>
<td>3.3</td>
<td>Links Defined For NS-2 Simulation Model</td>
<td>87</td>
</tr>
<tr>
<td>4.1</td>
<td>Improvement of using three MAPs in SSHMIPv6</td>
<td>107</td>
</tr>
</tbody>
</table>
# LIST OF ABBREVIATIONS

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARO</td>
<td>Adaptive Route Optimization</td>
</tr>
<tr>
<td>ARP</td>
<td>Address Resolution Protocol</td>
</tr>
<tr>
<td>BAck</td>
<td>Binding Acknowledgement</td>
</tr>
<tr>
<td>BOOTP</td>
<td>Bootstrap Protocol</td>
</tr>
<tr>
<td>BU</td>
<td>Binding Update</td>
</tr>
<tr>
<td>CIDR</td>
<td>Classless Inter-Domain Routing</td>
</tr>
<tr>
<td>CN</td>
<td>Correspondent Node</td>
</tr>
<tr>
<td>CoA</td>
<td>Care of Address</td>
</tr>
<tr>
<td>CSA-PHMIPv6</td>
<td>Connection Stability Aware PHMIPv6</td>
</tr>
<tr>
<td>DAD</td>
<td>Duplicate Address Detection</td>
</tr>
<tr>
<td>DEMAPS</td>
<td>Dynamic Efficient MAP Selection</td>
</tr>
<tr>
<td>DHCP</td>
<td>Dynamic Node Configuration Protocol</td>
</tr>
<tr>
<td>EUI–64</td>
<td>64-bit extended unique identifier</td>
</tr>
<tr>
<td>FA</td>
<td>Foreign Agent</td>
</tr>
<tr>
<td>FBACK</td>
<td>Fast Binding Acknowledgment</td>
</tr>
<tr>
<td>FBU</td>
<td>Fast Binding Update</td>
</tr>
<tr>
<td>FHMIPv6</td>
<td>fast handover</td>
</tr>
<tr>
<td>FIFO</td>
<td>First In, First Out</td>
</tr>
<tr>
<td>FNA</td>
<td>Fast Neighbor Advertisement</td>
</tr>
<tr>
<td>GPS</td>
<td>Global Positioning System</td>
</tr>
<tr>
<td>GFA</td>
<td>General Foreign Agent</td>
</tr>
<tr>
<td>HA</td>
<td>Home Agent</td>
</tr>
<tr>
<td>HACK</td>
<td>Handover Acknowledge</td>
</tr>
<tr>
<td>HI</td>
<td>Handover Initiate</td>
</tr>
<tr>
<td>HMIPv6</td>
<td>Hierarchical Mobile IPv6</td>
</tr>
<tr>
<td>IANA</td>
<td>Internet Assigned Numbers Authority</td>
</tr>
<tr>
<td>ICANN</td>
<td>Internet Corporation for Assigned Names and Numbers</td>
</tr>
<tr>
<td>ICMPv6</td>
<td>Internet Control Message Protocol Version 6</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>RCoA</td>
<td>Regional Care of Address</td>
</tr>
<tr>
<td>RRMIPv6</td>
<td>Regional Registrations MIPv6</td>
</tr>
<tr>
<td>RS</td>
<td>Router Solicitation</td>
</tr>
<tr>
<td>RtSolPr</td>
<td>Router Solicitation for a Proxy</td>
</tr>
<tr>
<td>SHMIP</td>
<td>Stealth-time HMIP</td>
</tr>
<tr>
<td>SLA</td>
<td>Site Level Aggregators</td>
</tr>
<tr>
<td>SMIP</td>
<td>Simple Mobile IP</td>
</tr>
<tr>
<td>SMR</td>
<td>session-to-mobility ratio</td>
</tr>
<tr>
<td>SPI</td>
<td>security parameter index</td>
</tr>
<tr>
<td>SSHMIPv6</td>
<td>Smart Selection HMIPv6</td>
</tr>
<tr>
<td>TCP</td>
<td>Transport Control Protocol</td>
</tr>
<tr>
<td>TLA</td>
<td>Top Level Aggregators</td>
</tr>
<tr>
<td>TTL</td>
<td>Time To Live</td>
</tr>
<tr>
<td>UDP</td>
<td>User Datagram Protocol</td>
</tr>
<tr>
<td>VOIP</td>
<td>Voice Over IP</td>
</tr>
<tr>
<td>WLAN</td>
<td>Wireless LAN</td>
</tr>
</tbody>
</table>
CHAPTER I

INTRODUCTION

1.1 INTRODUCTION

In 1994, the IETF (The Internet Engineering Task Force) designed IPv6 (Bradner & Mankin 1995) which is also named IP-Next-Generation (IPng), to enhance the Queue management performance of the current version Internet Protocol, IP Version 4 (Deering & Hindin 1998). IPv4 is used for the past decades; begin to have problems mostly due to its growing lack of addresses, which are needed by all devices connected to the Internet. IPng eventually will replace IPv4 (Deering & Hindin 1995) to fix its problems, such as addresses, routing and network auto-configurations, and also to run high performance networks as well as maintaining its efficiency for low bandwidth networks.

Millions of network devices such as computers and web servers are part of the global network of networks. Also the protocols that control the communications between these devices are a part of the Internet, which formally called Internet standards (Johnson & Perkins 1996). Internet standards guide to standard work of the Internet components. Internet technology consists of the Internet services and its protocols such as the Transport Control Protocol/Internet Protocol (TCP/IP) technology. Many strength and advantages of the Internet Protocol (IP) make it the most successful network layer protocol in computer networks services, but it also has some limitations. Simultaneously with the development of IP of computers that moved infrequently (Fritsche & Heissenhuber 2000) there are also millions of mobile devices and mobile computers need to connect via wireless network connections. Hence, it is important to support the best IP facilities for these mobile devices.
For supporting the wireless networking to keep the mobile devices connected to Internet, IP Mobility Support was introduced (Jonsson et al. 1999). In Mobile IP as shown in Figure 1.1, the communication and network activities should not be disrupted while the Mobile Node changes its attachment point to the Internet. In another word, the Mobile Node’s IP address must be updated as it travels from one network to another, which supported by Mobile IP which standard released 1993 (Calhoun & Perkins 2000).

![Figure 1.1 Mobile IP architecture](image)

Internet Protocols passed a lot of stages before reaching Internet Protocol Version 6 (IPv6) which is the last version number now applied for routing and addressing (Leiner et al. 2003); starting from testing the possibility of packet switching network and initiating an early version of Network Control Protocol (NCP) in 1969, going through proposing the new functionality of Transfer Control Protocol (TCP) introduced in 1974 (Cerf & Kahn 1974), IP-Internet Protocol was introduced and added to TCP in 1978, taking over the routing of messages in 1981, TCP/IPv4 was standardized, and by 1983, TCP/IP had replaced NCP within the original ARPAnet (Comer & Stevens 2000).

In the Mobile IPv6 operation (Deering & Hindin 1998; Montavont & Noël 2002), when a Mobile Node (MN) is connected to the Internet, it needs to check if it is currently connected to its home network or a foreign network. If MN detects it is under a foreign network, it will obtain a Care of Address (CoA) at the foreign network. Then it will notify its HA about its CoA. This procedure is called Binding...
Update (BU). The MN also reports its CoA to the Correspondent Nodes (CNs). The BU with the CN is known as the Route Optimization. The Route optimization is used to improve the performance of the IPv6 MN which takes place when the correspondent node knows the MN’s new CoA, then it will be able to send further packets directly to the MN’s CoA, without going through the triangle route via MN’s Home Agent (HA).

The Hierarchical MIPv6 (Soliman et al. 2001) separates mobility management into micro-mobility and macro-mobility. The essential element of this structure is the Mobility Anchor Point (MAP). It is a router that maintains a binding with MNs presently visiting its domain. It is usually located at the boundaries of a network, on top of the Access Routers (AR), to receive packets from the MNs attached to that network.

The MAP acts as the local HA for the MN. It intercepts all packets addressed to the out-of-towners mobile node, hands it out and tunnels them to the corresponding on-Link Care of Address (LCoA) of the mobile node. If the mobile node travels to another address within a MAP domain, it only needs to register the new on-link address with the MAP since the universal CoA does not change. If a mobile node travels into a new MAP Area, it needs to get a Regional Care of Address (RCoA) and an on-Link Care of Address. The mobile node then uses the new MAP’s address as the RCoA, while the LCoA address can be produced as stated in (Soliman et al. 2001). Subsequent to forming these addresses, the mobile node sends an ordinary MIPv6 BU to the MAP, which will bind the mobile node’s RCoA to its LCoA as seen in Figure 1.2. Then the MAP will return a binding acknowledgement (BAck) to the mobile node indicating a successful registration. The mobile node must also register its new RCoA with its home agent by sending another BU that indicates the binding between its home address and the RCoA. Finally, it may send a similar BU to its current corresponding nodes, specifying the binding between its home address and the RCoA.
1.2 INTERNET OF THINGS

In today’s fast based technological growth the traditional computer networks are no longer capable of handling the increasing demands with the best Quality of Service (QoS) which depend on the type of service that network device provide (O'neil 2002). This is not totally a result of an increasing number of computers in its common sense (Welbourne et. al 2009). Instead, the introduction of new devices that need to be connected to the Internet is another contributing factor.

Quality of Service (QoS) is a term used for a series of service requirements by which the network shall respond to during the transferring processes of the data and which can also be represented by parameters such as of delay and/or loss rate -which are adapted in this study-. QoS is necessary in order to control and provide a data delivery service that is consistent and predictable besides responding to various application requirements. QoS therefore undertakes various levels of packets to be received by various levels of services (Wenjiang et al. 2003)

These devices can be generally categorized under two main categories: the consumer electronics (gadgets) and the micro-computers which are present in most of
today’s activities. This section will briefly discuss examples of each of these categories and attempt to analyze the effects they introduce to the issue of scalability which is the main objective of this thesis.

1.2.1 Consumer Electronic Gadgets

This category includes consumer electronics such as mobiles, MP3/MP4 players, tablet PCs such as iPad, digital cameras, printers and e-books’ readers.

Most of mobiles are capable of browsing the World Wide Web and even publish contents on the web. MP3/MP4 players connect to Internet to enable the user to download music tracks and lyrics. And the recent introduction by Apple for its iPad opened the way for a whole new range of handheld tablet devices that provides the user with Internet connectivity on the comfort of their couch. Furthermore, the popularity of e-books’ readers such as Amazon’s Kindle which allows the users to buy, read and take notes on any book they choose to read from a wide selection of books.

1.2.2 Micro-Computers

Micro-computers are now available in the least places that one would expect. For instance, many cars, washing machines, fridges, traffic lights and surveillance cameras have micro-computers that logs into the Internet to provide extra functionality. The Global Positioning System GPS installed in modern cars for example allows the driver to search the Internet for nearby restaurants and further fetches the critics’ and users’ reviews of these restaurants before guiding the driver to its position. Similarly, air-conditioners now connect to the Internet and allow its owner to turn it on or off remotely. Furthermore, traffic lights are now connected to a network that allows the traffic department to control its operation from a remote control room depending on the traffic conditions in the neighboring areas. Not only that, but even surveillance cameras now have wireless access routers that allows access to the Internet for the house owner to watch and see his/her house even from the opposite side of the globe.
For all these devices to be connected to the Internet networks that was initially designed to cater for normal computers the issue of scalability arises as a concern of wither further improvements need to be implemented to cater for this increase in the number of mobile nodes.

1.2.3 Scalability

Increasing number of mobile nodes causes several issues in the implementation of computer networks. These issues include performance of the network components, bottleneck in some network components that decreases the overall network performance especially the Mobility Anchor Points (MAP) which is the main gate of transferring the date and the finite nature of networks address.

The Queue Management approach allows network operators to manage throughput and average delay with respect of queue length and the level of congestion (Floyd et al. 2001). It is the synthesized term of buffer management and packet scheduling, is one of the key mechanisms of QoS provision (Wenjiang et. al, 2003). A packet that is placed in a queue will be sent according to the same order in which they have arrived hence it is called as first in first out (FIFO) queue (Fiat et al. 2007).

QoS has been receiving a strong demand in modern internet day. Besides the sources, links also play an essential role in avoidance and congestion control. In order to control queue lengths, Random Early Discard (RED) was initially proposed. RED enabled dropping packets before overflow of buffer. Another pattern of congestion notification which has been initially explained due to advent of RED, is ECN that is Explicit Congestion Notification. The core reason why ECN has been proposed was for each link to be able to participate in congestion control through notifying users if an onset of congestion is detected. In such case the mark is reacted by the user as it there is a packet loss. Hence the link may avoid dropping the packet (which at the same time enhances the goodput) and still takes control of delivering congestion information to the user.
Active Queue Management (AQM) schemes are algorithms which are employed by routers in order to deliver this type of information. The policy of the router determines whether the AQM scheme mark or drop packets. When congestion based on the queue lengths are detected by most of the initially proposed AQM schemes at the link, some AQM schemes such as virtual queue-based schemes however detect congestion based on packets’ arrival rate at the link. Some of the schemes also use a combination of both such as PI. Most of the AQM schemes take part in adapting the probability of marking in any possible way.

1.3 PROBLEM STATEMENT

In HMIPv6, the MAP acts as the local HA for the MN if the Mobile Node out of its Home Network as mentioned before. It is only the gate which intercepts all packets addressed to the out-of-towners Mobile Node, hands out and tunnels them to the corresponding LCoA of the mobile node. This study concentrates on handling many Mobile Nodes in the domain due to;

i. The problem of scalability has not been resolved using multi MAPs, with the same regional CoA, handling the Mobile Nodes in the domain in HMIPv6. For instance, recent research introduce by Chen et al. (2007) who proposed a cross-layer partner-based HMIPv6 called PHMIPv6 which improve the performance of HMIPv6 by predicting the new CoA of the new access router did not solve the problem of scalability that this thesis intends on solving.

ii. To the author knowledge from the literature, no other researcher has used the join shortest queue as a queue management technique to solve the problem of high delay, lost packet and lost packet ratio in HMIPv6 if the domain carries too many MNs. For instance, research conducted by Lai and Chiu (2005) which introduced Stealth-time HMIP (SHMIP) tackled the problem from the angle of DAD time reduction but did not approach the scalability issue that we are focusing on.

iii. Also, the problem of reducing location update cost in HMIPv6 domains has not been solved properly by other researchers in term of incorporated domains (Taleb
et al. 2009) which will be discussed in Chapter 5. In order to reduce and balance the cost of location update, some researchers have made use of Gateway Location Register (GLR) which is made of three database structure levels by designing a dynamic location management method that is movement area based. The GLR method can be used in optimizing the size of the movement area based on the speed which leads to reduction in the location management (Chen et al. 2010).

1.4 RESEARCH OBJECTIVES AND SCOPE

Given the aforementioned in the introduction and problems discussed in the problem statement, the study aims to propose, evaluate a novel protocol and further enhancement SSHMIPv6 using load balance management scheme.

The objectives of this study are:

i. To propose an enhanced HMIPv6 conceptual model referred to as Smart-Selection HMIPv6 (SSHMIPv6) and to evaluate and compare their performance using simulation.

ii. To implement load balance among the MAPs using Join-Shortest-Queue (JSQ) selection method for MAPs queue management in SSHMIPv6

iii. To minimize location update signaling cost of SSHMIPv6 by proposing an incorporated domains.

The research focus on the scalability enhancement of HMIPv6 while handling large amounts of mobile nodes through the introduction of multi-MAPs in a domain. The performance measure is totally based on the simulating the proposed mathematical models. However, the handover scheme, data compression, security issues and retransmission delay of lost packets will not been considered at this early stage of development of the new proposed system. Furthermore, the implementation of proposed scheme on the real test-bed is out of scope of the study.
1.5 RESEARCH CONTRIBUTION

The research contribution can be identified and summarized as follows:

i. A new architecture for HMIPv6 called SSHMIPv6 is developed to solve the scalability problem as well as the effect of intermittence or cut-off especially in the situation whereby the domain carries too many Mobile Nodes.

ii. A simplified mathematical model for evaluating the location update cost was derived by deducting the HA and CNs from the model when the Mobile Node moves within an incorporated-domain in HMIPv6.

iii. Extra features of SSHMIPv6 architecture have been added to be able to create a load-balanced between the MAPs by sharing the traffic in an incorporated domains either during light or heavy traffic conditions thereby making this system more efficient by utilizing all the MAPs in the domain hence the effect of intermittence or cut-off will be almost insignificant or negligible due to the decrease in lost packets and packet delay at the entrance of the data or packet transferred.

iv. A new scheme for incorporated domains which plays a role in the reduction of location-update packets which in turn reduces the cost is implemented.

1.6 THESIS ORGANIZATION

This thesis is organized in 6 chapters; Chapter 1 gives a brief introduction about this thesis including general overview about IPv6 history, problem statement, research objectives, and research contributions.

Chapter 2 reviews the literature written about networks and the IPv4. It commences with a short history of the development of the IP standard. The chapter further presents an introduction into the Internet Protocol version 6. It starts with a short history of the improvement of the IPv6 standard and goes on to define and explain the format of the IPv6 address. The chapter is concluding with an outline of transition mechanism from IPv4 to IPv6. Special attention is paid to related studies and IPv6 researches using Network Simulator NS-2.
Chapter 3 deals with the methodology and the proposed scheme, which is also based on the HMIPv6, Smart Hierarchical Mobile IPv6 (SSHMIPv6). The main contribution of this work explained together with the introduction of our model. It also shows how the model fulfills the requirements proposed in the previous chapter.

In Chapter 4, the simulation results and analysis are discussed. The hypothetical network is benchmarked, and simulation is carried out to ensure that the objectives are fulfilled. “Incorporated domains” which is an application of SSHMIPv6 is presented in Chapter 5. Location update cost cutting is taken out from the “incorporated domains”. Lastly, this research is concluded in Chapter 6, where a summary of the findings is presented along with points of future works.
CHAPTER II

LITERATURE REVIEW

2.1 INTRODUCTION

The expression of Internet was modified from “interworking” which means the interconnection of many different networks that is based on multiple technologies (like Ethernet, token ring and satellite links) to a single large network (Salkintzis 2004).

From a technological point, it is difficult to design a single technology that mandate the global network because of the unfair compromises and the difficult decisions that should be taken. Beside the technology, the political obstacles would be formidable. By taking third generation 3G wireless systems as an analogy, the single unified global 3G systems failed to emerge despite the efforts of the International Telecommunication Union (ITU).

Therefore, to maintain the multiple network technologies and interconnect the separate networks into a single network, the Internetworking concept arouse as an alternative. Thus, the advantages of a single large network will be achieved without requiring the usage of an underlying single one, like the connectivity between two computers in the network. Therefore, it is alive example of convergence, where Internetworking will be the glue that gathered the disparate networks into a single converged network.

The Internet infrastructure (Perlman 1999) could include routers (machines that forward packets between other machines) and gateways (machines situated on the
boundary of two or more disparate networks, allowing communications to pass between the networks).

We distinguish the Internet from the technology that makes this possible, called Internet technology. Internet technology includes all the services and protocols used in the Internet.

Transport Control Protocol/Internet Protocol (TCP/IP) technology is a main part in Internet technology, because of its high performance and the large products number is handled by it for a lot of vendors, beside to the local Internet (Intranet) handling with huge number of nodes. Indeed, the Internet Protocols IP is the common understanding that control computers communication, interpret packet headers make the Internet standards formal and route packets.

The routed IP packets to all destinations are represented by IP address is called destination IP address. The majority of IP address are unique, specific will be booked for private use, like those will be used for Intranet. These specified addresses are hidden to the global Internet. For the IPv6, 128-bit addresses are used, different of the former IPv4, which is using 32-bit addressing.

For the classical address categorization method, n may get the values of 8, 16 or 24 for the following classes correspondingly: A, B and C. Obviously, in class A addresses, the node address ration will be the most room, this room has 16,777,216 (2^24) special node addresses, but another room just for 65,536 and 256 different addresses per class B and class C network prefix, correspondingly (Roberts & Challinor 2000).

Formally, by addressing classification: in the network address, the class will be determined by the first few bits. Classless is no more been used for addressing, the network address is written in the way w.x.y.z/v regarding to it. Suppose that the network address is 192.46.0.0/16 which means the first 16 bits are the network portion of the address, whereas 192.46.0.0/20 means that the first 20 bits are the network
portion of the address. In both cases, the network address starts the same way (Daniel 2005).

A private address, at least officially, is an address in one of the 3 designated blocks for private addresses. These are:
- 10.0.0.0 To 10.255.255.255;
- 172.16.0.0 To 172.31.255.255;
- 192.168.0.0 To 192.168.255.255

2.2 INTERNET PROTOCOL VERSION 4

Internet Protocol Version four is the stable one after the Internet Protocol got different revisions. IPv4 is now ubiquitous where IPv6 is fit for certain quarters. Across all network types to deliver data IP is the universal protocol into datagram the data will be packed, theses datagram comprise the Source destination payload data to be delivered and some control information.

Since datagram sends its own and has its own route through the network it is called connectionless. There is a difference between a packet and datagram, we call any protocol message at the network or transport layer Packet, where any connectionless protocol message is datagram at any protocol layer (Postel 1980). Therefore, in IPv4 we may use Packet and Datagram interchangeably since it is connectionless protocol.

To identify the sender and recipient, an IP datagram should be informational controlled, this control information will be classified in a header at the beginning of datagram to be accessed easily by the computer without searching through the entire datagram.

The headers of all the datagram should be formatted by the same manner so processing the datagram by the computer will access the needed information quickly.
2.2.1 IPv4 Addressing (Spaces and Formats)

In an IP network each node assigns one or more IP addresses (Richard 1994). Within the context of the network these addresses are unique and allowing the source and packets destinations identifying clearly. Nodes in the network are told by the destination addresses on packets where the packets are headed and it enables nodes forwarding the packets to their destinations.

The length for all IPv4 address is 4-byte, so their length is not enough to hold common data-link layers addresses, which are usually six bytes been assigned from different address space. In dotted decimal notation the four bytes of addresses are represented, so it is easy for a human operator to read and remember.

Certain structure will be applied to IPv4 addresses where the bits of the address are all important, but the most important is carried by the leftmost bit especially if the addresses were a number. Through local registries, IP addresses are assigned, the responsibility for a subset of all the available addresses will be delegated by the body overseeing, the Internet Corporation for Assigned Names and Numbers (ICANN).

The IP address is an enough efficient unique identifier to determine perfectly a single node. Single node can get a unique or multiple addresses, for those to be unique just in limited networks. Like a node having an IP address so it is known through the Internet, where it uses another one within its local network.

The address space 0.0.0.0 to 255.255.255.255 is divided to classes of addresses. The clue is to assign a random network that is belonging to a certain class is chosen by the numbers of the nodes in the network. Then an address range will allocate the network by using the class and to manage the nodes addresses administratively.
2.3 MOBILE IP

Mobile IP is more reliable application of IP for mobility. IP address stops shorting the particular of each procedure start the essential part of the protocol. This technique will strengthen the protocol use, it gives the deploying flexibility.

2.3.1 Movement Detection

In Mobile IP (see Figure 2.1), by moving among foreign agents mobile nodes should be updated. Different algorithms will be specified by the Mobile IP address, lazy, eager cell switching and prefix matching (Cheshire & Aboba 2002). To decide foreign agent change, the new one should send a router advertisement to be heard by the mobile node. Layer-2 information will be used by handovers (a draft standard, low-latency) to update the mobile node about its new foreign agent, it is possible to use the help of the new and/or old foreign agent (Pandey & Jamadagni 2002).

![Figure 2.1 Mobile IPv4 architecture](image)

2.3.2 Location registration

Every MN should obtain HA when it visits a far network. Tracking the used IP address by MN needs its registration with its home agent. Each MN will have two IP addresses, the first one to locate and the other one to identify. Regarding to standard
terminology, by visiting a foreign link, MN will be related to a new IP address by its care of address (CoA).

MN’s home address is joined to the current CoA via a mobility binding, thus it is possible to route packets that were received by MN, and this routing will be done with the CoA whatever the Internet MN point of attachment. While the MN’s registration process determination, a specific lifetime amount will be for every binding, after a while this registration is deleted. MN registration within this time is to ensure its service continuity with CoA.

The attachment way will decide sending MN’s location registration messages immediately to the related HA (Figure 2.2), or via a sender FA for registration toward the HA. In a different case, registration demand is exchanged by the MN with registration reply messages that is depending on IPv4. Registration demand message is used to register the MN with the related HA (Perkins & Johnson 1999). MN’s mobility binding with a new lifetime is created by the HA. Registration reply messages have been returned by the suitable mobile agent. Since the necessary codes to update the mobile node about its request status are possessed by the reply message to give the lifetime with HA guaranty.
2.3.3 Handoff management

Within IPv4 (Gustafsson et al. 2004), routing optimization schemes at the time being allows the previous foreign agent to fix a binding for the related formers mobile visitors and explaining a current CoA for everyone.

After that, packets had been sent to the first CoA, the related pervious foreign agents shall send the current MN’s CoA as shown in Figure 2.3.

Accordingly, during the packets’ updating to the home agent and the related nodes with new CoA on the link, packets will be accepted by their MN at its previous CoA.

![Figure 2.3 Mobile IP handoff with binding from FA to another FA](image)

In the case that there is no new binding for the former FA, packets will be sent by FA to the MN’s home agent that is forwarding from the MN’s end place registration these packets to the CoA as shown in Figure 2.4. This may implicitly make unneeded traffic if the HA’s binding keep referring to the previous FA. On the other hand, the previous FA can ask utilizing of specific tunnels that send the packets, and more than it explain the necessity of specific handling at the HA.
By using specific tunnels, packets that had been forwarded to the HA will be encapsulated with the FA’s address like the source IP address. By receiving the new encapsulated packets, a comparison will be carried out by HA between the IP address source and the most new CoA of the MN.

Therefore, by matching the two addresses, packets never been circled to the FA back. Though, if match of addresses does not occur, the packets will be decapsulated and sent by HA to the current CoA of the MN as shown in Figure 2.5 (Perkins & Johnson 1999).

The procedure to route MN’s datagrams via the related HA generally results utilization paths longer than the optimal definitely. Mobile IP routing optimization techniques is using tunnels. Like the specific tunnels mentioned for the smooth handoff to reduce using insufficient path. Like, as datagram is tunneled toward CoA by the HA, the home address of the MN is protected well from interchanging routers between its home network and current location.

Recovering and delivering the original datagram by the MN will happen at the moment the agent is reached by the datagram. At the current time, to route optimization and compose tunnel, two protocols are used: route optimization in mobile IP (Perkins & Johnson 1999) and the tunnel establishment protocol (Calhoun & Perkins 2000).
The simple clue for routing optimization is to set extensions to basic mobile IP protocols that allow better routing, in order that datagrams movement is possible from correspondent node to a mobile node with no need to go to the home agent firstly (Perkins 1996).

The mentioned extensions are giving paths for the nodes to cache an MN binding, after that to tunnel datagrams immediately to the CoA correspondent to that binding, via passing the home agent of the MN. Furthermore, extensions allow the immediate forwarding toward the MN’s new CoA for situations as forwarding datagrams as an MN is travelling and datagram that are forwarded regarding to the out-of-data binding.

In establishing the tunnel protocol, Mobile IP improvement was considered to act among nodes roughly (Calhoun & Perkins 2000). Regarding tunnel establishment, the transmission of PDUs by the encapsulated agent (HA) toward the tunnel endpoint (FA) will be according to parameters set. On other words, establishing a tunnel is the process to create or update the parameters of a tunnel.

In general, MN’s network address is included by parameters establishment. Using tunnel establishment in PDUs transition needs a fine selection the MN’s tunnel point (FA) by the home agent.

This will be possible by creating a table with MN’s IP address indexes it. Every entry in it has the address of the suitable tunnel endpoint, in addition to any different needed tunnel parameters. As the packets are received, after that the foreign agent prefers any transmission manner to transmit the decapsulated PDUs to get the MN receiving it. If at this specific particular FA was resided by the MN, there is no need for any other network operations.

Different issues will be experienced by Fourth Generation 4G IP networks like the security. Regarding to the PLMN, to authenticate a mobile is very difficult, since the connection between the address of the mobile and a permanent access point will be
lost. That allows a better chance for applying an MN to receive services (Yabusaki et al. 2005).

The second issue is simultaneous binding. Since getting different CoAs by the MN at the same time, the HA should be developed enough to tunnel packets to different endpoints. Therefore, the HA is controlled to forward the duplicate encapsulated datagrams to every CoA. As MN receives the packets from the CoAs, a process to remove the duplication will be started. It is possible to keep the duplicated packets for signal reconstruction assistance.

Registration options must be taken in considerations. At the time being, three major principles were identified as possible principles to limit location update and to register cost.

First, a scheme necessity is to manage the MN’s available local connectivity and datagrams buffering to be delivered. By this, the network will be able to make use from the smooth handoffs without applying route optimization processes. Second, there is a necessity for the foreign agent’s multicast group to permit the usage of a multicast IP address by the MN as its CoA. Third, foreign agent’s Hierarchy will be used in agent advertisement for localizing the registrations to the minimum public CoA’s FA at the two attaching points.

To get this method alive, a decision by the MN should be taken to select the three-height needed for MN new registration message, after that arranging this message transmission to get each level of the Hierarchy among itself and the minimum public ancestor of MN’s new and former CoA (Perkins 1996).

Another principle, SMIP that stands for Simple Mobile IP (Perkins & Johnson 1999), this approach seems to be enough simple to assist the users mobility, by compare it with asymmetric triangular approach that was introduced by IPv6. SMIP applies a lot of symmetric and distributed solutions regarding the local management depending on MN connections for the fixed network routers which added many mobility functions.
Regarding wireless ATM, (Wang et al. 2007) mobility management does deal with transitioning from ATM cell depends on transporting on widely possible resources over wire line toward cell transport depends on the limited and relativity undependable resources over the wireless channel.

2.3.4 Limitations of Mobile IP

The main issue with Mobile IP is that it is inapplicable widely because of Internet’s heterogeneous nature. Though, even when it is applicable, a lot of limitations in operating and performing will be excited.

As previously discussed, within a wireless cellular system, Mobile IP is considered as macromobility and not high-velocity micromobility, to serve a continuous IP connectivity through handoff. Just below are some issues and offered solutions. Refer to (Dutta et al. 2002) and references therein for details.

(1) Tunneling Delay

A little delay will be added by the tunnel. From a Quality of Service (QoS) point of view, the strong and weak connection can be considered regarding to this element. Different solutions are introduces for this element, like using co-located IP address, allowing a direct communication between MN and CN, supposing no other hindrances are there. This is the route optimization (Dutta et al. 2002) and causes HA to send mobility binding updates to CN.

(2) Discontinuities in Communications

Regional registration: it is proposed as an alternative solution for this issue in reference, in this a bigger domain has a Hierarchy of FAs. All FAs are possible to be tunneled. On the other hand, possible tunneling occurs by GFA, the gateway FA.
Though, when FA is maximum or minimum in the Hierarchy, MN is registering. So, by the presence of the HM in a bigger domain, no registration from among FA will occur. More solutions, as mentioned in (Dutta et al. 2002) contain the usage of layer information to update possible movement’s mobile host before it happens and the mobile identifies it. The previous two mechanisms are possible since layer-2 detects mobility before layer-3. Tunneling delay will be handled properly by IPv6.

(3) Firewall

Currently the private networks are firewalled. By MN movement to a foreign network that is forbidden by CN domain. The domain will block them. To troubleshoot this issue, reverse tunneling will be used (Braun & Danzeisen 2001), where all data among MN and CN will pass through HA. A tunneling delay will be added because of this. But, it is still useful to keep the higher protocol binding (e.g. TCP/UDP sockets).

(4) Security

The protocol needs the help of mobility societies, which is applied between two nodes which are carrying authentication’s information, like encryption algorithm, any related keys and mechanism rerun detection and protection. The mobility security society is indexed by security parameter index (SPI) specifically and node’s IP address (Perkins & Johnson 1997), which will introduce a security context usage and should be restricted in the range (0-255), which is difficult condition set and clear obstacle to international application of mobile IP.

(5) Intra-domain Mobility

Mobile IP is not proper for micromobility. Inside a specific domain, if the MN traverses between link connections, it requires a handoff process to deal with several link layers. There are two possible choices for the new link layer, like WLAN or 3G cellular access network connection with a new base station. Mobile IP is not projected for this type of mobility, and it will be addressed independently.
2.4 IP VERSION SIX

Internet engineers have commenced their work on the replacement of the current Internet protocol (IPv4) with a new IP version 6 at the early to mid-1990s. This had been done due to address space exhaustion, inextensible option support, and other limitations of the old version of the Protocol (Postel 1981). IPv6, as it is now called, has reflected various technical and policy oriented improvements over the old version protocol. The main objectives behind embarking on such improvements were to increase address space, reduce complexity at routers, as well as to improve extensibility. Thus, IPv6’s provides a huge address space of 128 bits as compared to IPv4’s 32 bits (Huitema 1998). This had also been accompanied by certain policy changes. In cases where the address space would become exhausted, an important policy change grants the Internet Assigned Numbers Authority (IANA), the central address delegation authority *inter alia*, the ability to repossess address space from designees. Comparatively, IPv4 options were only fixed at standardization due to the fact that any new option needed to be supported by every IPv4 node regardless of whether it had utilized that option. Hence, in IPv6, it may or may not be mandatory to have support of a particular option. As a replacement for including options inside the IPv4 packet header, and to result in a fixed size IPv6 header, options are daisy-chained using the Next Header field of the packet header. This fixed packet size, as well as the ability to target options to a particular audience, such as for routers or for the destination only, eases the routing task. Added to this are other protocol features that also simplify routers.

2.4.1 Neighbor Discovery

The method, through which end nodes realize routers and other nodes as well as identify alterations in connectivity in IPv6, is called Neighbor Discovery (Narten & Draves 2001). The functionality of neighbor and router discovery that is present in the markedly different IPv4 protocols are incorporated in Neighbor Discovery, for instance: ARP and Router Advertisements.
Router Solicitations and Router Advertisements which primarily emerged in IPv4 (Deering 1991) are greatly enhanced in IPv6. Such router Solicitations and Advertisements bear prefix data as well as the network ID. Thus, no additional method or system is required to establish the prefix netmask. Significantly, these routers offer a way for nodes to auto-configure their selves on the link. Routers are able to place two bits in Router Advertisements, lead nodes to configure their selves either in a stateful method, for instance: with Dynamic Host Configuration Protocol (DHCP), or a stateless method through utilizing Stateless Address Autoconfiguration. The Mobile IPv6 design indicates particular support for Mobile IPv6 (Johnson 2002).

Some of the researchers identify the Neighbor Discovery as a protocol for IP Version 6. Therefore Neighbor Discovery is used in order for the IPv6 nodes on the same link to discover their existence, to find out their link layer addresses, to determine routers and to ensure a seamless flow of information. Thereof it avoids various threats such as those particularly for wireless networks to local link address resolution as the link between them is the access point (Kempf & Koodli 2008).

2.4.2 Address Autoconfiguration

Nodes autoconfigure their selves by having assistance from IPv6 Router Advertisements. That can be done either by a stateful or a stateless method. In the stateful method, end nodes are required to utilize an external protocol such as DHCP (Droms 1997) in order to configure their selves.

The alteration of wireless units can only operate in wireless connections. In addition, perceiving media alterations necessitates the support of the operating system, such support is not provided by all main operating systems. IPv4 Router Advertisements are not usually sent by IPv4 routers; special configuration is needed for these routers for that to be done.

In cases where IPv6 routers state the stateless method, the nodes would autoconfigure their selves by utilizing Stateless Address Autoconfiguration (Thomson
A node that utilizes Stateless Address Autoconfiguration would affix the network prefix broadcast that is found in the Router Advertisement with a node ID that is automatically and statelessly produced by the node. Any algorithm can be used for that purpose. Nevertheless, two algorithms have acquired general recognition, and these are: the EUI–64 and temporary address generation algorithms (Narten & Draves 2001). EUI–64 node IDs which are recommended for the IEEE 802.x interfaces are produced by acquiring the interface’s 6-byte hardware address and putting in the 16-bit hexadecimal number FFFE to link the third and fourth byte. The periodical alteration in temporary addresses requires that they be utilized only for a short period of time and in unidentified sessions (Wells et al. 2001).

In case the end node does not receive a reply from another node within a specific time limit (by default following the termination of one transmission) the address would quite definitely be available for use. IPv6’s being viewed as a pioneer, link layer addresses have been recommended to be utilized in IPv4 (Cheshire & Aboba 2002).

### 2.4.3 Tunneling

Packets normally pass through a source node to a destination node by the most efficient transitional routers in accord with routing algorithms. Nevertheless, a node may infrequently desire its packets to be routed by way of one or more intermediary routers prior to their reaching the required destinations. Otherwise, similar to the case where packets are designed to a mobile node under Mobile IP, a node could desire to transmit packets to a different destination.

Some protocols, particularly IPsec (Kent & Atkinson 1998), depend on the packet continuing without being altered while in transit. Hence, within a tunnel, packets stream from a single endpoint to another, while remaining unaltered through the process of transit. In order to ensure that packets do stream from a single endpoint to another, packets are encapsulated with a new IP header that is named the outer IP header. The latter is placed between the link-layer header and the original IP header.
With the source and destination addresses being determined with the two endpoints, the original IP header is duplicated in the outer header. The resulting encapsulated packet is next dispatched to the other endpoint. The encapsulated packet is then decapsulated or deprived of its outer header once it reaches the other endpoint. Consequently, the original packet is regained and launched to its original destination. The said procedure is exemplified in Figure 2.5, where a node A dispatches a packet to a node B, and packets pass through a channel between R1 and R2 in transit, the packets will tag along the loose route, and \( \Rightarrow \) represents an encapsulated packet and \( \rightarrow \) a normal packet. Tunneling only requires that packets become regained in a somewhat intact condition at the remote endpoint. The most commonly used three tunneling protocols on the Internet are: IP-in-IP encapsulation (Gustafsson et al. 2004), Generic Routing Encapsulation (McCloghrie et al. 2000), and minimal encapsulation (Johnson et al. 2004).

\[
A \rightarrow R1 \Rightarrow R2 \rightarrow B
\]

Figure 2.5 Encapsulated and normal packet

2.5 MOBILE IPv6

There is a space indicating extension headers in the base header pertaining to IPv6 packet. Similarly, every extension header has a space indicating other headers. It is also possible that numerous extension headers materialize in one IPv6 packet. Such headers constitute a header sequence in an IPv6 packet.

There are three kinds of IPv6 addresses as stated by IPv6 Addressing Architecture (Conta & Deering 1995), these are: unicast, multicast and anycast address. A packet that has a unicast address is transmitted to the node which contains the unicast address allocated for its interface. Yet, a packet that has a multicast address is transmitted to all nodes which are associated with the group that is recognized by the multicast address. An anycast packet, nevertheless, is transmitted to any of numerous probable nodes that are recognised by the address. That is usually the node nearest to the dispatcher of the packet.
2.5.1 Mobile IP components

A mobile node's home network, as far as mobile node is concerned, is the network that contains a network prefix corresponding to this mobile node's home address. Every other network is regarded as this mobile node's foreign network.

Mobile IPv6 has three essential constituents as perkins & Johnson (2001), these are: the mobile node, home agent and correspondent node.

(1) Mobile Node (MN)

As illustrated in Figure 2.3, a mobile node traveling the Internet can be a wired tool or a wireless point of connection. A number of link layer connections may exist in these kinds of nodes to link with the Internet. Just a single connection operates as the principal connection for Mobile IP at any given time. The Internet connection of a node is determined by the principal connection. Every sent and received control message, like binding messages, crosses the principal connection. The tunneled IP packets would remain to be sent to the principal connection until the connection expires.

(2) Home Agent (HA)

A home agent that remains in the home network pertaining to a mobile node controls the mobile node's place as well as other data. Numerous nodes could possibly be working concurrently as home agents in a network. Every one of these home agents can determine in advance the mobile nodes which it is meant to control or offer service to. Another possibility is that a mobile node would not be pre-assigned to a home agent. The home agent of a mobile node may dynamically be determined by the latter. When such a situation occurs, the development of a method is needed in order to coordinate the operation among the home agents. Only a single home agent operates for a mobile node at any given time.
(3) Correspondent Node (CN)

A correspondent node that can be found in any location in the Internet dispatches IP packets to a mobile node. Packets which are dispatched by the correspondent node, being uninformed of the mobile node's care-of address, are sent to the borne network pertaining to the mobile node. In cases where the mobile node is not in its home network, the packets would be intercepted and channeled towards the mobile node's care-of address through the mobile node's home agent.

2.5.2 Mobility over IPv6

The mobile node connects or transfers to a new network as far as the network to which the mobile node connects is concerned (Perkins & Johnson 2001). In cases where the resulting network prefix is compatible with the earlier network prefix, the Router Advertisement message could be utilized for the purpose of updating the router data which is stocked up in the mobile node, like the checking time of the router. On occasions, a number of routers can be found in a single network. Hence, the data for every router may need to be stored by the mobile node.

In cases where no pre-assigned home agent is available for a mobile nod, it would be necessary for the latter to discover the home agent that exists in its home network at the time when the mobile node firstly joins the network. The home agent can be discovered by the mobile node through making a Home Agent Discovery Request. The destination address of the latter is an anycast address having a home network prefix. A home agent within the home network pertaining to this mobile node would return an ICMPv6 Home Agent Discovery Reply message for the purpose of notifying the mobile node about the matching data. The data pertaining to every home agent, that is able to operate as a home agent for this mobile node, would be incorporated in the message.

Once a Binding Update message is delivered to a home agent, the home agent would determine whether it should permit the mobile node to register. The affirmation
would then be required to be returned to the mobile node through a Binding Acknowledge message.

In the event that the mobile node takes delivery of the Binding Acknowledge message, and the said message signifies that the home agent accepts its binding registration, it would be necessary for the mobile node to dispatch a Binding Update message to matching nodes in order to notify them of its recent position.

The IPv6 packets which have been dispatched by correspondent nodes, being uninformed of the care-of address pertaining to the mobile node, would be routed to the mobile node's home network the mobile node's home address. The home agent would then tunnel them by means of IPv6 Encapsulation to the care-of address pertaining to the mobile node. In the event that a correspondent node recognizes the mobile node's care-of address, the IPv6 packets which have been dispatched by this correspondent node would be directly dispatched to the mobile node by means of an IPv6 Routing header. The said header would then specify the mobile node's care-of address as being a halfway destination. Reversely, packets that have been dispatched by a mobile node would be directly channeled to their destination by having the mobile node's care-of address or home address being utilized as the source address within the packet.

Subsequent to a mobile node's return to its home network, the mobile node uses a Binding Update message in order to de-register from its home agent as well as to inform other correspondent nodes by means of Binding Update messages.

The flow of information and messages between the mobile node, home agent, correspondent node and router are illustrated in Figure 2.6.
Figure 2.6 Data Flow for Mobile IPv6

Amongst the messages dispatched between Mobile IPv6 constituents, Router Advertisement and Solicitation messages; Home Agent Discovery Request as well as Reply messages are dispatched using ICMPv6. The IPv6 Destination headers carry the Binding update, the Binding Acknowledge, and Binding Request. Presently, no new IPv6 protocols or programs that utilize the IPv6 Destination header exist to transmit data. Given that binding control messages are dispatched in IPv6 Destination headers, the messages can be found in any IPv6 packets with further payload. In order for Mobile IP to be supported, a Mobile IP node (mobile node, home agent, and correspondent node) would have to verify all the IPv6 packets and interrupt those which contain binding messages in IPv6 destination header.
(1) Achieving Care of Address

Care-of address of a mobile node can be formed or obtained in a number of ways. As far as a mobile node is concerned, these include the stateful, stateless, and static ways. A number of link layer interfaces, in certain mobile nodes, may connect to diverse networks simultaneously. Each interface may have a distinctive care-of address. Yet, only a single care-of address operates as the main care-of address for the mobile node at all times.

(i) Stateful

Once a mobile node discovers that it is connected to a foreign network, it becomes capable of obtaining a new care-of address by means of DHCP through the DHCP Server that exists in the new network. Yet, when this address is no longer needed by the mobile node, the address would either be returned by the mobile node to the DHCP server or left to expire.

(ii) Stateless

The location of a mobile node is discovered by it through a Router Advertisement message that exists in the network to which it is attached. The network Prefix Information Option is included in the Router Advertisement message. This information as well as the matching amount of the connection interface through which it links to this network can be utilized by the mobile node to create a new care-of address. An instance is that the matching amount of this link can be Ethernet address pertaining to the interface designed for a PC or laptop.

(iii) Static

On several occasions, a mobile node may be allocated an IPv6 address that should be utilized only when the mobile node connects to a foreign network. Through Mobile IPv6, the mobile node is capable of utilizing this previously allocated IPv6 address
instead of creating a new care-of address. If such an event occurs, the mobile node's home network, as well as the foreign network to which the mobile node connects, is required to sustain particular node routing in relation to that care-of address.

(2) Home Agent Discovery

A home agent address may be obtained by a mobile node in two ways: pre-assigned or dynamic discovery. A new method may be developed by the combination of these two ways.

ICMPv6 Home Agent Discovery messages are of two types: ICMPv6 Home Agent Discovery Request as well as ICMPv6 Home Agent Discovery Reply. ICMPv6 Home Agent Discovery Request would be anycasted to home network to which it relates from a mobile node. ICMPv6 Home Agent Discovery Reply is dispatched to the mobile node from the mobile node's home network. It could be dispatched through a home agent or a node that manages the home agents that are found within the mobile node's home network. This message format is illustrated in Figure 2.7 and Figure 2.8.

<table>
<thead>
<tr>
<th>Type</th>
<th>Code=0</th>
<th>Checksum</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Identifier</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Reserved</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Home Address</td>
</tr>
</tbody>
</table>

Figure 2.7 ICMPv6 HA Discovery Request

The Home Agent Address field, in the Home Agent Discovery Reply message, consists of a directory of addresses of home agents as a part of the home link pertaining to the mobile node. The residual length of the IPv6 packet which carries the Home Agent Address Discovery Reply message indicates the quantity of addresses found in the directory.
(3) Binding operation

Binding messages would be dispatched connecting a mobile node with its home agent or correspondent node(s). The messages would be dispatched in IPv6 destination headers together with every other message found in an IP packet. Binding messages are of three types: Binding Update, Binding Acknowledge, and Binding Request.

Binding Update would be dispatched to its home agent as well as correspondent nodes from a mobile node. This message format is illustrated in Figure 2.9.

An Acknowledge bit would be placed in order to demand a Binding Acknowledgment to be sent back once the Binding Update is received. A Home Registration bit would be placed in order to demand the receiving node to operate as the node's home agent. In addition, when a router bit is placed, it signifies that the mobile node happens to be a router.
As an affirmation of Binding Update, a Binding Acknowledge would be dispatched. It is usually dispatched from a home agent toward a mobile node. It would only be dispatched by means of the Binding Update recipient at the time the first bit is placed within the Binding Update message. The message format is illustrated in Figure 2.10.

<table>
<thead>
<tr>
<th>Next Hdr</th>
<th>Hdr Len</th>
<th>Reserved</th>
<th>Option type = 7</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Length</td>
<td>Status</td>
<td>Sequence Number</td>
<td></td>
</tr>
</tbody>
</table>

Life Time

Refresh

Sub-options ...

Figure 2.10 Binding Acknowledge

A Binding Request would also be dispatched to a mobile node from a home agent or correspondent node for the purpose of requesting a mobile node's binding by the mobile node. It is usually dispatched at the time the binding information within the sender is about to expire. As a response to the Binding Request message, a mobile node dispatches a Binding update message. The message format is illustrated in Figure 2.11. No extra sub-option information is asked for in a Binding Request message.

<table>
<thead>
<tr>
<th>Next Hdr</th>
<th>Hdr Len</th>
<th>Reserved</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Type = 8</td>
<td>Option Length</td>
<td>Sub-options ...</td>
</tr>
</tbody>
</table>

Figure 2.11 Binding Request

(4) Traffic operating

For dispatching IP packets, a mobile node can utilize its home address or care-of addresses to perform as the source address, when it is outside its home network. There is no stringent rule related to this issue in Mobile IPv6. Given that the home address' network prefix is not equivalent to the network prefix pertaining to the foreign network with which the mobile node would be attaching, the packets having the mobile node's home address as being the source address would not be able to go by the routers with a number of control filters within the foreign network.
Once a packet reaches a mobile node, the mobile node would prepare the packet prior to the packet moving toward the IP stack. Whether or not the packet exists in IPv6 encapsulation would be checked by the mobile node. In the event that it does exist, the packet would be de-encapsulated.

### 2.6 SECURITY

A constant concern related to Internet communication is Security. Security has various constituents which are: confidentiality, authentication, integrity checking, and non-repudiation. Confidentiality refers to the decoding of information by authorized persons only. Authentication refers to the validation or invalidation of the individual who claims the identity. The process of guaranteeing that information would not be modified or altered without such alteration being capable of detection is referred to as integrity checking. Moreover, the process of verifying the source of certain information, even if the dispatcher denies that fact, is referred to as non-repudiation (Atkinson 1995). Due to the fact that Security is not a topic of main consideration in this research, there has not been an in-dept study on it.

### 2.7 IPv6 VERSUS IPv4

The essential protocols related to IPv6 have been stipulated since 1998. Thus, a central query in telecommunications is: when will IPv6 be executed? Notwithstanding the varying demands stated previously, it seems troublesome to shift from an operational system without having an easy and convincing motive to act as a means for transformation. As far as IPv6 is concerned, such motive is the used up IPv4 address space. As a result of address depletion IPv4 would soon be impractical. The termination of IPv4 is predicted to occur between 2008 and 2015 (Brown et al. 2002). Yet, the incorporation of IPv6 has, until this moment, been very slow.
2.7.1 IPv6 Design Considerations

Specific demands have appeared or have become important (or predicted to be as such). For instance, QoS support has become more significant due to the increase in streaming multimedia as well as different traffic which have diverse QoS requirements. Excellent protection has become ever more essential as a result of the increasing commercial utilization of the Internet as well as the development of wireless IP. IP mobility support has also become more essential due to the development of wireless IP (Johnson & Perkins 2001).

2.7.2 Inadequacies of IPv4

The most severe practical dilemma related to IPv4 is possibly the restrictions pertaining to its 32-bit address space. Given that a few of the $2^{32}$ addresses are specific broadcast or multicast addresses, not every one of them is available for utilization like normal addresses for unicast (Cheshire & Aboba 2002).

Address management had been assisted by employing procedures such as introducing CIDR as well as expanding the recognition of NATs. However, as illustrated in Figure 2.12, such impermanent resolutions lessen the indicators; yet, they do not resolve the original dilemma. In general, systems that operate on the basis of IPv4 would be configured by hand through individual network managers. The automation of various address configuration tasks is assisted by protocols such as the boot protocol (BOOTP) and DHCP, a derivative of BOOTP (Hankins 2009). Nevertheless, DHCP is not accessible all over, and it needs a DHCP server. Additionally, in particular circumstances, there is no access to the services offered by a DHCP server.
The method of processing IPv4 headers causes some other defects, such as: At every node between an IPv4 origin and destination, fragmentation and reassembly processing could occur, which adds to the processing exertion of the IP routers. Furthermore, Header checksum is inspected at each node; which also adds to the processing exertion of the IP routers.

2.7.3 IPv6 characteristic outlines

The IPv6 features include the following:

As an alternative to the 32-bit addresses utilized by IPv4, IPv6 utilizes 128-bit addresses (Hinden & Deering 2003).

Compared to IPv4, IPv6 includes stronger and more adaptable autoconfiguration facilities. A few of such functions (such as the autoconfiguration pertaining to a link-local address) are relevant to nodes as well as routers. Others, however, are only relevant to nodes. IPv6 furnishes improved support to mobility compared to IPv4. IPv6 includes supporting functions such as autoconfiguration. IPv6 furnishes improved QoS support compared to IPv4. An additional function in IPv6 is the Flow Label field found in the IPv6 header.
(1) Scalability

A number of aspects pertaining to scalability are included in the IPv6 design. First, the availability of the huge number of addresses is in itself a scalability aspect even though it is argued that a massive address space adds to the requirement of scalability (Narten & Draves 2001).

(2) Hierarchical Routing

There are various theoretical analyses performed by researchers, especially in presenting its benefits through high level simulations. Hierarchical routing is defined by Ivanichki & Steen (2009) as promising approach for point to point routing with a routing state that is very small.

Since the emergence of IPv4, hierarchical routing design has been a source with relation to scalability (Cheshire & Aboba 2002). Nevertheless, previously, IP addresses' blocks had not well spread and classless addressing had started only when a shortage of addresses had already taken place. There are advantageous exercises related to conveying bulky adjacent blocks to ISPs and demanding websites which necessitate that IP addresses reach them in the form of sub-blocks originating from ISPs. Such exercises enable the reduction of the size pertaining to routing tables found in the Internet core as well as cause hierarchical routing to be more effective.

Hierarchical routing, in IPv6, becomes effective due to the more efficient aggregation of the blocks of addresses. Hence, the advantageous exercises related to address assignment must be adopted upfront. Blocks of IP addresses would be designated to ISPs as follows: the prevalent ISPs, similar to level 1 ISPs pertaining to the IPv4 are allocated as Top Level Aggregators (TLAs) and all are allotted a huge block of addresses.
(3) Addressing

IPv6 presents an addressing a more affluent model compared to IPv4 for the purpose of supporting a few of its new functions (Thomson & Narten 1998). Therefore, IPv6 presents Scope which is related to the scope of applicability of an address, and Anycast addresses:

Site-local addresses are local to websites which contain multiple LANs, e.g. university or corporate networks. Global addresses are similar to the standard IPv4 addresses, i.e. possessing global scope as appeared in Figure 2.13.

![Figure 2.13 IPv6 address scopes](image)

The utilization of link-local addresses as well as site-local addresses in IPv6 is corresponding to the utilization of private addresses pertaining to IPv4.

A large group of multicast addresses is specified in IPv6. Every unicast or anycast address contains a corresponding solicited-node multicast address, created through supplementing the recognized 104-bit solicited-node multicast address prefix which has the 24 lowest-order bits related to a unicast or anycast address. Given that interfaces related to multiple nodes could theoretically share the same 24 lowest-order
bits, multiple unicast addresses corresponds to every solicited-node multicast address (Doyle 2003).

(4) IPv4 and IPv6 Coexistence

Essential methods for the interworking as well as the coexistence of IPv4 and IPv6 are as follows.

IPv6 packets' tunneling within IPv4 networks; i.e. IPv6 packets would be encapsulated inside IPv4 packets within IPv4 networks. A method for doing tunneling is the configuration of point-to-point tunnels for the purpose of transporting IPv6 packets around IPv4 networks. Nevertheless, another possibility for tunneling IPv6 packets automatically around IPv4 networks is when IPv4 compatible IPv6 addresses are utilized (Johnson & Perkins 2004).

Utilization of particular NATs involving IPv4 and IPv6 networks. The NATs, in such cases, would deal with the required address versions. Secluded IPv6 nodes not linked to an IPv6 router; yet, if connected to an appropriate IPv4 network, may utilize the IPv4 network to play the role of a virtual Ethernet, multicasting IPv6 packets to and from different secluded IPv6 nodes (Carpenter & Moor 1999).

2.7.4 Mobile IPv6

There is great similarity between mobile IPv6 (MIPv6) and MIPv4 with the exception that the former operates by using IPv6 in lieu of IPv4 (Johnson et al. 2003). The essential function of MIPv6 is to make it possible for a roaming mobile node to keep on receiving packets emanating from functions within correspondent nodes which dispatch the packets toward the permanent IP address pertaining to the mobile node. Compared to IPv4, IPv6 is more responsive to mobile nodes due to the concern toward mobility support in the design of IPv6. Specific functionality that sustains MIPv6 is fixed in IPv6. Hence, mobility support would be included in IPv6. Thus, there are advantages pertaining to MIPv6 compared to MIPv4. These include:
i. IPv6 contains greater address autoconfiguration facilities. Consequently, every MN must be capable of obtaining a worldwide routable address within a distant network, hence lessening the requirement for FAs. On many occasions, MN in IPv4 would not be able to obtain an address within a distant network except by means of FA. That is except in cases where, for example, DHCP is utilized or where it is making connection via GPRS.

ii. Route optimization is a regular element in MIPv6, while it constituted an optional feature of MIPv4 and not generally provided. Every IPv6 node needs to recognize requisite updates compared to an IPv4 node. Yet, a MN need not dispatch binding updates to every CN.

iii. Once a CN directly dispatches packets to the COA pertaining to a MN, it would not be required to encapsulate the said packets, and it would consequently not sustain encapsulation overhead. As an alternative in IPv6, a fresh routing header for the purpose of source routing would be specified for this function.

iv. Instead of utilizing particular messages, binding updates would be attached to normal IP packets by means of utilizing new mobility headers in the form of IPv6 extension headers. This means that normal IP packets would be dispatched while the mobility header would be supplemented to such packets in order to transmit MIPv6 data.

MIPv6 operates in the following manner: After an MN reaches a distant network it would autoconfigure an address in the said network. Such an address would be appropriate for utilization as the MIPv6 CoA. Subsequently, the MN would be recorded in its HA through dispatching a binding update toward the HA, which would send back a binding acknowledgement.

The first way is where an MN does not notify the CN with regard to its present CoA. Packets dispatched from the CN would set off to the HA, the HA within MIPv6
being a modified IPv6 router inside the home network. Subsequently, as in IPv4, the packets would be tunneled toward the foreign network. Nonetheless, as far as the return path is concerned, packets would be tunneled backwards toward the HA in lieu of moving straight toward the CN. That would be done through utilizing the CoA as being the external source address as well as the MN’s home address as being the source address within the encapsulated packet. The packets would subsequently be dispatched from the home network toward the CN. The said process would resolve several dilemmas concerning firewall ingress filtering and egress filtering, at the expense of quadrilateral routing in lieu of triangular routing.

The second way through which an MN and a CN would communicate, as expected, is the utilization of route optimization (Johnson et al. 2003). The MN would dispatch binding updates toward the CNs every time it travels toward a foreign network.

A query that first comes into mind is the method for reserving a network prefix with relation to a node link. A usual process within IPv6 advocates the non-subnetting of IPv6 networks further than a /64. An instance is where stateless address autoconfiguration presumes that the last 64 bits are required to be allocated in the capacity of the node ID (Thomson & Narten 1998). In addition, as far as a /64 network is concerned, nodes which statelessly autoconfigure their selves are able to select an address on any location in the 64–bit node ID space provided that they utilize the EUI-64 address generation method for the purpose of Ethernet interfaces. Nevertheless, the link router is capable of reserving a little space in a /64 network, perhaps the upper half. Every standard node which would autoconfigure itself by means of an address in the said upper have is required to utilize Duplicate Address Detection for the purpose of detecting whether the said address is being utilized.

Any mobile router which connects to the domain would determine the said substitute home agent and would demand the allocation of a prefix to it. It would maintain the prefix provided that it would continue to be within the routing domain. Using this technique, routing would remain to be optimal inside the domain, external network access routers would not be required to keep extra address space designed for
mobile routers. In addition, mobile routers would not be required to continually dispatch care-of address updates. Nevertheless, the technique could be expensive for the domains which support very mobile or huge quantities of mobile networks. Localized Mobility Management (LMM) protocols, including Hierarchical Mobile IPv6 (Soliman et al. 2003), basically carry out the task of a substitute home agent. Hence, they could be the answer to the said techniques.

### 2.7.5 Fast Handover MIPv6

Handover is the procedure wherein a mobile terminal alters the serving cell pertaining to it. As far as mobile communications systems are concerned, several IP addresses could be allocated to a mobile terminal and it could consequently be handled as a mobile node. By means of every support station operating in the capacity of a radio access router (AR), the support stations would develop into the attachment points to the Internet. Mobile IP permits a mobile node to sustain the connection to the Internet throughout its handover between access routers (refer to Figure 2.14). All through the handover procedure, a period of time exists wherein the mobile node would not be capable of dispatching or taking delivery of IP packets as a result of link exchange delay as well as IP protocol processes.

![Figure 2.14 MIPv6 handover](image)

On many occasions the handover latency that occur from ordinary mobile IPv6 handover processes could over-adequate for the purpose of supporting concurrent or
delay-sensitive interchange. For the purpose of lessening handover latency, a fast handover protocol had been included in mobile IPv6 (Koodli & Perkins 2001). The said protocol permits a mobile node to dispatch packets once a new link is detected, as well as to convey packets toward a mobile node once there is detection of the existence of the mobile node via the new access router. Researchers have reviewed the concept of quality based settings for handover process by which they have come to conclude that the quality can be either by aggregated pilot strength that is distributed by various connected pilots and/or by the pilot that is strongest out of other pilots of preference (Huang et al. 2008).

The features, components, addressing spaces and format, handoff management, packet routing management of IPv4 and IPv6 have been discussed in details initially. Table 2.1 summarizes the differences between IPv4 and IPv6 with respect to number of bits used, number of possible addresses available, address allocations, address types, fragmentation and routing management.
Table 2.1 Comparisons between IPv4 and IPv6

<table>
<thead>
<tr>
<th>Aspect</th>
<th>IPv4</th>
<th>IPv6</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Address</strong></td>
<td>It uses 32 bits</td>
<td>It uses 128 bits</td>
</tr>
<tr>
<td><strong>Address Space</strong></td>
<td>It has over $10^9$; possible addresses</td>
<td>It has over $10^{38}$; possible addresses</td>
</tr>
<tr>
<td><strong>Special Fields in Header</strong></td>
<td>It has many types, often not supported by vendors due to impact on performance</td>
<td>They are eliminated for efficiency or replaced by other features</td>
</tr>
<tr>
<td><strong>Address Allocation</strong></td>
<td>Its allocation uses network classes A, B, C (large, medium, small nets). It has CIDR (stopgap measure to deal with address space exhaustion, router table overgrowth). Its local use limited to link only</td>
<td>It has IPv4 compatibility and it is hierarchical by registry, provider, subscriber, and subnet. It is hierarchical by geographic region and its local use is by link or site</td>
</tr>
<tr>
<td><strong>Address Types</strong></td>
<td>Its address is point-to-point. Its local broadcast depending physical link features have limited multicast. It uses experimental anycast (not globally available)</td>
<td>Its address is either Multicast (sends to many interfaces at once) or anycast (reaches one of a group of interfaces)</td>
</tr>
<tr>
<td><strong>Fragmentation</strong></td>
<td>Multiple step fragmentation, done by routers, impacting routing performance is possible</td>
<td>Fragmentation can be done at most once, by host (not router)</td>
</tr>
<tr>
<td><strong>Routing Management</strong></td>
<td>It uses TCP-high overhead, designed for 32-bit addresses, uses single address family and full tables use large amounts of its storage</td>
<td>Its IP datagram-based - low overhead, it accommodates 128-bit addresses, it has multiple address types, its aggregated tables economize storage</td>
</tr>
</tbody>
</table>

2.8 HMIPv6

Mobile IP is very suitable to be utilized in roaming communications in which a point of connection would not be continuously moving. Nonetheless, in support of mobile communications, another development pertaining to mobile IP is required for the
purpose of supporting micro-mobility, the latter indicating the motion amid sectors and cells and within a radio access network.

Nodes are permitted by mobile IPv6 to travel inside the Internet topology and maintain attainability and current links among the mobile and the correspondent nodes. In order for that to take place, a mobile node would, while traveling, dispatch binding updates toward its home agent as well as every correspondent node communicating with it. Nevertheless, authenticating binding updates would necessitate around 1.5 round-trip times linking the mobile node with every correspondent node. Furthermore, a single round-trip time would be required for the purpose of updating the home agent. That could be done at the same time as updating correspondent nodes is done.

Regular handovers could exist between radio accesses routers related to IP-based mobile points of connection within a mobile communications system. The mobile terminal would dispatch as well as take delivery of a huge amount of signaling messages on the space interface intended for every correspondent node and the home agent. In order to develop the performance pertaining to mobile IPv6 in similar situations, as well as to restrict the quantity of mobile IPv6 signaling exterior to the local domain, a new local node, namely the mobility anchor point (MAP), would be initiated in mobile IP, consequently bringing about the hierarchical MIPv6 (HMIPv6) (Soliman et al. 2003).

Basically, a MAP happens to be a local home agent which could be situated at a point within a routers’ hierarchical network such as the radio access router. It also combines the leaving traffic pertaining to mobile nodes. Through the MAP initiation, the mobile node would dispatch binding updates toward the local MAP instead of the correspondent node and home agent, being usually at a greater distance, consequently lessening the signaling traffic within the mobile network. In addition, without connection to the number of correspondent nodes communicating with the mobile node, simply a single binding update message would require to be conveyed via the mobile node prior to the routing of the traffic coming from the home agent as well as every correspondent node toward its new radio access router.
A MAP happens to be a router that is situated within a network which the mobile node visits, and a number of MAPs may exist. Due to the hierarchical formation, two care-of addresses would be created in HMIPv6. The regional care-of address (RCoA) constitutes an address that is found on the MAP’s subnet, and it would be acquired through the mobile node which visits the network. Furthermore, it is auto-configured by means of the mobile node after the MAP preference is delivered. The local care-of address (LCoA), however, constitutes the on-link care-of address configured that is found on the mobile node’s interface established upon the subnet prefix that is promoted via its default radio access router. The local binding update constitutes the update which is dispatched by the mobile node toward the MAP for the purpose of establishing a binding common to the RCoA and the LCoA.

The mobile node arriving at a MAP domain would take delivery of router advertisements that include data related to various local MAPs. The mobile node would be able to bind the current on-link CoA pertaining to it through a RCoA address that exists on the MAP’s subnet. The MAP, in the capacity of a local home agent, would take delivery of every packet in the name of the mobile node which it serves. It would also encapsulate as well as forward them immediately toward the mobile node’s current address. In the event that the mobile node alters its current address inside a local MAP domain (LCoA), it would only be required to register the new address in the MAP. Consequently, barely the regional CoA (RCoA) would be required to be recorded in correspondent nodes as well as the home agent. Alteration would not be made to the RCoA provided that the mobile node travels inside a MAP domain. The MAP domain’s boundaries would be specified via the access routers which would promote the MAP data to the added mobile nodes.

It must be kept in mind that the HMIPv6 idea basically constitutes an addition pertaining to the mobile IPv6 protocol. A mobile node that is attentive of HMIPv6 amid the execution of Mobile IPv6 would merely select to utilize the MAP at the time of finding out a similar facility within a visited network. Still, the mobile node could, on several occasions, give priority to the utilization of the standard mobile IPv6 implementation. An example is where the mobile node could be situated within a
visited network in the home site pertaining to it. If so, the home agent would be situated close to the visited network and may be utilized in lieu of a MAP. In such a situation, the mobile node merely would update the home agent every time it is in motion.

An instance of the utilization of the MAP within a visited network is reflected by the network design illustrated in Figure 2.15. The mobile node would find out the global address pertaining to the MAP after reaching a visited network. The said address would be collected inside the access routers and would then be communicated in the direction of the mobile node by means of router advertisements (RAs).

![Figure 2.15 HMIPv6 Domain](image)

The above process is required for the purpose of notifying the mobile nodes regarding the existence of the MAP. During the stage of detection, the mobile node too would be notified about the space separating the mobile node from the MAP. For instance, the MAP utility might be executed in the method illustrated in Figure 2.15 and simultaneously in AR1 as well as AR2. If such an event occurs, the mobile node would be able to select the initial hop MAP or any other hop that is more distant
within the routers’ hierarchy. The MAP detection procedure would carry on while the mobile node travels from a single subnet to another. When the mobile node roams inside a MAP domain, it would take delivery of a message from the access routers regarding the very MAP address or addresses. In the event that an alteration pertaining to the promoted MAP’s address is taken in, the mobile node would react to the alteration through undertaking motion detection and dispatching the required binding updates toward its home agent as well as the correspondent nodes as shown in Figure 2.16.

Figure 2.16 HMIPv6 routing scheme

In the event that the mobile node is not attentive of HMIPv6, no MAP detection would be undertaken. This would result in the mobile node utilizing the mobile IPv6 protocol for the purpose of the mobility management pertaining to it. Alternatively, in the event that the mobile node is attentive of HMIPv6, then the mobile node would initially be required to register in MAP through dispatching a binding update that includes its home address as well as on-link care-of address (LCoA). This information would be collected by MAP within its binding cache for the purpose of forwarding packets toward their last destination once they are accepted from the various home agents or correspondent nodes.
The mobile node is required to determine the first sender of every received packet in order to determine whether route optimization would be necessary. Such information could be utilized by the mobile node as the MAP would not adjust the substance pertaining to the original packet. Standard handing pertaining to the received packets would supply the mobile node with the required data.

In order to utilize the network bandwidth in an effective way, the mobile node would choose to concurrently register with various MAPs as well as utilize every MAP address in favor of a particular set of correspondent nodes. For instance, as illustrated in Figure 2.16, in the event that the correspondent node exists on the very link as that of the mobile node, then it is deemed to be further effective to utilize the initial hop MAP (assuming it is AR1) for the purpose of communications among them. The said process would circumvent the dispatching of every packet using the main MAP within the hierarchy, and consequently cause an effective utilization of network bandwidth.

2.8.1 MN Operation

Two addresses pertaining to the mobile node exist in HMIPv6. These are an RCoA that is found on the MAP’s subnet as well as an on-link CoA (LCoA). The said RCoA is created through the combination of the mobile node’s interface detector with the subnet prefix that is acquired in the MAP preference. The protocol necessitates exceptional handling only through the mobile nodes. The home agent would remain unaltered. The MAP would carry out the task pertaining to a local home agent with the intention of binding the mobile node’s RCoA with an LCoA.

Once a mobile node goes inside a new MAP domain, it would be required to construct two CoAs, i.e. an RCoA resting on the MAP’s subnet as well as an on-link CoA (LCoA). Following the formation of the RCoA on the basis of the prefix acquired within the MAP preference, the mobile node would dispatch a local binding update toward the MAP. The mobile node’s RCoA within the home address preference would be specified by the local binding update. The LCoA would be utilized in the capacity of the source address pertaining to the binding update. The said
binding update would bind the abovementioned mobile node’s RCoA with its LCoA. Once registered with the MAP, the mobile node would register the new RCoA related to it with its home agent through the dispatching of a binding update that identifies the binding linking the RCoA with the home address. A similar binding update would be dispatched by the mobile node toward the mobile node’s existing correspondent nodes.

For the purpose of speeding up the local home agent handover among MAPs, the mobile node could dispatch a local binding update toward its previous MAP that includes a specification of its new LCoA. Traveling packets which arrive at the previous MAP would be conveyed toward the new LCoA. Packets which are addressed en route for the mobile node’s RCoA, whether coming from the home agent or from the correspondent nodes, would be obtained by the MAP. Then, packets would be tunneled toward the mobile node’s LCoA from the MAP. Consequently, the mobile node would decapsulate the said packets and would handle them in the usual way.

At the time the mobile node travels in the vicinity (i.e., the MAP pertaining to it does not differ), it would only Register the new LCoA related to it with its MAP. When this occurs, the RCoA would remain unaltered. However, it must be kept in mind that a mobile node could dispatch a binding update that includes its LCoA toward correspondent nodes that are attached to its link. Following that, packets would be transmitted promptly without having to go through the MAP.

2.8.2 MAP Operations

The MAP operates as a home agent. It would intercept every packet addressed to every registered mobile node and would tunnel them toward the corresponding LCoAs. The MAP would not have information about home address pertaining to the mobile node. A local binding update would be dispatched by the mobile node toward the MAP in order to notify the MAP about the creation of an RCoA by the mobile node through utilizing the RCoA as being the home address existing within the
binding update. In the event the process succeeds, the MAP would be required to send back a binding acknowledgment toward the mobile node to signify the successfulness of the registration. If not, the MAP would be required to send back a binding acknowledgment together with a suitable error code. MAP would be capable of accepting packets that are tunneled as of the mobile node, having the mobile node as the tunnel access spot and the MAP as the tunnel departure spot. Following that the MAP would operate in the capacity of a home agent in support of the RCoA. Also, packets which addressed to the RCoA would be cut off via the MAP, encapsulated, and would then be routed toward the mobile node’s LCoA. Nevertheless, it must be kept in mind that the sustenance of HMIPv6 would totally be apparent to the function of the home agent. The home agent would convey packets, which are addressed to the mobile node’s home address, toward its RCoA.

HMIPv6 offers an adaptable system designed for restricted mobility management in any visited network. MAP could be present at every level within a hierarchy, such as the access router. Numerous MAPs could separately be situated in a hierarchy. Furthermore, coinciding MAP domains would also be recommended and permitted. Static as well as dynamic hierarchies are equally sustained. (Soliman et al. 2005) advocated that a mobile node found within a hierarchical mobile IP network must be “eager” to carry out new bindings and “lazy” when it comes to discharging existing bindings. What is meant is that a mobile node would be required to register through every “new” MAP that is promoted via the AR (eager). Present bindings must not be discharged by the mobile node until the MAP preference is not received by it anymore or until the duration of its present binding ends (lazy). Such an eager-lazy methodology is practical in terms of offering a reserve system in the event that a MAP router fails. This is because it would decrease the duration needed by a mobile node to notify its correspondent nodes as well as its home agent regarding its new CoA.

2.8.3 Regional Registrations MIPv6 (RRMIPv6)

Under this sub-topic a description is made of the Mobile IPv6 Regional Registrations protocol as outlined by (Malinen & Perkins 2001). Mobile IPv6 Regional Registrations protocol lessens the handoff latency via the localization of the binding
updates toward the foreign domain as well as the signaling load. That would be done through utilizing regional-aware routers for the purpose of completing the handoff intended for a mobile node which travels inside the foreign domain.

Access routers within the foreign domain would promote their ability to support regional registrations through dispatching customized router advertisements plus a recently specified advertisement flag. As soon as a mobile node goes through a new foreign domain, it would carry out instant detection and would take delivery of a router advertisement message as of the accessible access router. Moreover, the mobile node would carry out the access router detection procedure. The mobile node would acquire the regional care of address (RCoA) designed for the recently visited foreign domain through utilizing a directory of Regional CoA annexes that are connected to the router advertisement. The mobile node would utilize the said RCoA to operate as primary care of address for the purpose of dispatching key Mobile IPv6 binding updates (BUs) beyond the foreign domain. An on-link care of address (LCoA) would also be configured by the mobile node for the purpose of obtaining an address within the foreign domain.

Subsequent to obtaining the RCoA as well as the LCoA, the mobile node would carry out a home registration together with the first regional binding update. The regional binding update is basically a customized Mobile IPv6 binding update that transmits upwards, hop-by-hop, via a regional-aware routers hierarchy, until an intersection router is arrived at. As a new development in regional registration, Gateway router would operate as a crossover router. The regional aware router is basically a special router designed for the purpose of supporting regional registrations. In addition, a crossover router is basically a router wherein the previous course that leads to the mobile node as of the gateway, as well as the latest course, would intersect one another.

As far as a regional binding update's IP header is concerned, the destination address would be a "visited domain routers" anycast address. A regional-aware access router would be the first to take delivery of the local binding update message. Next, the message would be propagated toward the following higher regional-aware router
subsequent to encapsulation. The higher regional-aware router would then decapsulate the message for handling and would re-encapsulate it for the purpose of dispatching it to the following-higher regional-aware router. Every regional-aware router on the way between the mobile node and the crossover router, at the same time as handling the regional binding update, would generate or even update their regional binding cache record intended for the mobile node. The said cache would include mapping involving the home address pertaining to the mobile node as well as the source address pertaining to the regional binding update message. Thus, the crossover choice would dynamically be made dependant on the network, while the mobile node would be independent in terms of dispatching the packets as of the network router's addresses. Once a regional binding update is received, the crossover router would dispatch a key Mobile IPv6 binding acknowledgment. Such a message would be sent back to the mobile node via the up hierarchy.

Following the success of the regional registration procedure, the mobile node would carry out a regional registration for the purpose of completing the handoff with relation to all handoffs found in the very same foreign domain. It would not dispatch a binding update beyond the domain toward a home agent or toward correspondent nodes because the regional care of address pertaining to it would not have been altered. The mobile node could dispatch regional binding updates for the period of home binding in order to maintain the regional binding cache. Furthermore, it could dispatch normal binding updates toward the home agent as well as the correspondent nodes in order to maintain the validity of the mapping in their caches. The binding cache records would be erased once a de-registration message is taken delivery of or when the duration of the cache ends.

The signaling message course, pertaining to mobile node micro mobility case as well as macro mobility case within RRMIPv6, is illustrated in Figure 2.17.
Within the local domain, regional registrations would influence the routing of the packets which are conveyed for mobile nodes, and they would be sent via a regional-aware information routing. Since the mobile node utilizes regional care of address within bindings in connection with home agent as well as correspondent nodes, every packet sent toward the mobile node would reach the gateway router that exists within the foreign domain. The regional binding cache would be utilized for regional-aware information routing with relation to the forwarding of the encapsulated, or source routed information packets, pertaining to the mobile node. The tunneled packets would be de-capsulated by the gateway router. The home address pertaining to the mobile node is the destination of encapsulated packets. The gateway router would check a record related to the home address within its binding cache, and would discover the lower care of address. It would re-encapsulate the concerned packets to a lower regional-aware routers corresponding care of address. The said procedure would go on until the packets arrive at the mobile node. The packets dispatched by means of the mobile node would not be affected by regional registrations; and such packets could follow the default IPv6 route.
2.9 IPv6 RESEARCHES OVER NS-2

The enhanced HMIPv6 is called Robust Hierarchical Mobile IPv6 (RH-MIPv6) (You et. al. 2003). The key ideas are to allow multiple registrations via primary and secondary regional CoAs by the MN and to change the serving MAP from the primary RCoA to the secondary RCoA in the case of the MAP failures which provide the ability of the system to reduce the failure detection time and the failure recovery time. In the performance analysis, RH-MIPv6 shows a shorter recovery time than HMIPv6. Simulation results by NS-2 simulator are presented confirm the analytical evaluations under different environments.

For the simulation, Hierarchical Mobile IP (HMIP) Implementation is used, which was implemented in Columbia IP Micro-mobility Software (CIMS). It supports micromobility protocols such as Hawaii, Cellular IP, and HMIP extension for the NS-2 network simulator based on version 2.1b6. The MAP functionality is added to provide regional registration with the existing CIMS implementations and the multiple registrations are implemented, which register simultaneously P-RCoA and S-RCoA to CNs.

NS-2 based on the standard NS-2 distribution NS-allinone2.1b6 is used to evaluate the proposed scheme of Fast Mobile IPv6 with reordering algorithm for handovers (Park & Latchman 2008). The analysis of the impact of handovers between ARs for out of sequence packets under Mobile IPv6 in a fast handover environment was designed on the top of INRIA/MotorolaMIPv6 code for NS-2. Due to the ability of NS-2 to extend the code with two main modules; a recording algorithm for data and a recording algorithm for ACK using a modified snoop protocol, some modifications have been done to original release to show that EF-MIPv6 can improve TCP performance and prevent the out-of-sequence packet problem in existing Mobile IPv6 network. The simulation results showed that EF-MIPv6 has better performance than existing Mobile IPv6 protocols, and it works well in fast handover environments.

A scheme to perform fast handovers for hierarchical mobile IPv6 networks in the macro-mobility and micro-mobility management is proposed (Habaebi 2003). Fast
handover performance is achieved by forwarding the multicast packets from the mobility anchor point to every adjacent access router. They have simulated the performance in NS-2 network simulator which allows the MN to receive packets faster than the HMIPv6 scheme. NS-2 version 2.1b is used to implement the proposed multicast schemes for macro/micro-mobility management extensions into the HMIPv6. NS-2 is used due to its allowance to the user to configure the parameters of the topology that is already supported by NS-2 flexibly.

A study via NS-2 network simulator is conducted to implement Neighbor Discovery, HMIPv6, FMIPv6 and the proposed combination of HMIPv6 and FMIPv6 (Moreno et al. 2003). A ‘stress test’ of the protocols was performed to study the effect of the number of MNs on handoff latency, packet loss rate, obtained bandwidth and fast handoff process success probability of IPv6. The signaling load costs associated to the different proposals compared to the performance of obtained improvements have a significant influence over the performance metrics.

The simulation code used for the experiments was designed on top of INRIA/Motorola MIPv6 code for NS-2 implementation. The code has been extended with four main modules: Neighbor Discovery, Hierarchical Mobile IPv6, Fast Handovers for Mobile IPv6 and their combination.

A novel QMS scheme in M-HMIPv6 networks is proposed (Lei & Zeng 2007). Analysis of the handover process theoretically and derive a lemma to estimate AHD was done, which is the key design of QMS scheme. Then, they verify the analysis by comparing the numerical results with the statistics from NS-2 simulations. The proposed scheme can be applied for handover optimization for multimedia services in M-HMIPv6 networks. The simulation runs with NS-2.1b6a installed in Redhat Linux 9.0.

A cross-layer partner-assisted handoff protocol, called PHMIPv6 protocol, is proposed (Chen & Wo 2009). The PHMIPv6 protocol is a cross-layer approach among layer 2 and layer 3. A new station, called PS, is adopted in PHMIPv6 protocol. The scheme basics are to scan the neighbor BSs and PSs with association in the
802.16e handoff procedure, the MS can request the PS to pre-perform the DAD procedure to obtain the unique LCoA and RCoA in advance. PHMIPv6 protocol significantly reduces handoff delay time and packet losses. In the mathematical analysis, we verify that our PHMIPv6 protocol offers better handoff latency than MIPv6 and HMIPv6 protocols.

Two NS-2 modules, NIST Wimax module and Mobiwan are adopted to simulate and compare HMIPv6 protocol and PHMIPv6 protocol with the successful and unsuccessful cases.

2.10 RELATED STUDIES

Based on HMIPv6 and its management routing schemes, a lot of researches are done in the recent years which some of them will be introduced.

2.10.1 Dynamic Efficient MAP Selection (DEMAPS)

A recently introduced scheme of Dynamic Efficient MAP Selection (DEMAPS) proposed by Taleb et al. (2009) is one of the recent developments attempting to solve the issue of scalability in HMIPv6 through the introduction of the concept of dynamic selection of MAPs in cases of higher number of MNs.

The concept behind this scheme was inspired by networks operators who are forced to introduce several MAPs to cater for a single domain due to the fact that assigning one MAP to a large domain can create packet delays due to the distance between the MN and the MAP as the MN moves away from the MAP. When more than one MAP is introduced for one large domain the issue of load balancing among theses MAPs arises and MAPs are usually either overloaded or underutilized (Taleb et al. 2009).

The DEMAPS scheme attempts to solve this issue by introducing a dynamic scheme that behaves just like traditional HMIPv6 when the loads are within a certain limits and behaves differently when the loads start to soar.
This is accomplished by assigning a predefined threshold and storing it in a MAPs selection system that stores a list of all the MAPs with loads not exceeding these thresholds. For normal situations, the furthest MAP among this list is selected first as an implementation of the traditional distance-based selection scheme for HMIPv6. However, in cases where all the MAPs have loads which exceed the threshold then the MAPs selection scheme follows an exponential moving average EMA method. This means that the first priority will be given to the furthest MAP which has higher tendency for its load to decrease. This decision is made after calculating the exponential moving average for each of the available MAPs.

This DEMAPS scheme was tested through computerized simulations and it is claimed by (Taleb et al. 2009) that the scheme reduces the number of packet drops, guarantees shorter service delays, makes better utilization of the network resources, and maintains a fair efficient distribution of the network load.

Nevertheless, one of the disadvantages of this proposed system is that the MAP selection is done in the MN level which can result in increased energy consumption and thus a shorter battery life of the MN (Taleb et al. 2009). It is therefore the opinion of the author of this thesis that performing the task of load balancing of MAPs selection in a higher level can bring an advantage of lower energy consumption and less computational power in the MN. This can be accomplished by applying the SSHMIPv6 proposed by this thesis.

2.10.2 MAP selection based on moving direction pattern

Another MAP selection method for areas served by multiple coexisting mobility anchor points (MAPs) is one that takes into account the movement direction pattern of the mobile node MN. This investigation into the best MAP selection model in terms of performance is important due the fact that it is a challenging issue for an arriving mobile node to choose the most appropriate MAP to bind. This task must be carried out by considering the issues of load balancing, binding update and packet delivery cost minimization (Baek et al. 2010).
This selection scheme proposed by (Baek et al. 2010) was tested and found to be providing considerable performance improvement over the earlier adaptive selection approach due to its consideration of the movement direction of the mobile node since it can make a more informed decision based on the probability of future possible location updates since a MN is more likely to change to a MAP located in the direction its heading towards.

2.10.3 Effects of Network Topology on MAPs Selection

The literature produced a lot of research on the best MAPs selection scheme that yields the best results. For instance, (Taleb et al. 2009) and (Baek et al. 2010). Yet the topology of the network and its effects on the performance of these selection methods where not investigated before (Vilhar et al. 2010) where the previously assumed tree topology is examined and compared with other candidate topologies.

It was shown that the improvement of MAP selection algorithms used in tree topologies is limited, due to the fact that the distance from the MAP and the frequency of MAP changes cannot be lowered simultaneously.

2.10.4 Adaptive Route Optimization (ARO)

The introduction of MAPs enabled HMIPv6 to produce better performance through taking care of assigning a RCoA that enables seamless movement between domains and provides lower handoff latencies. Nevertheless, in cases where mobile nodes MNs have high volume of session activities with relatively little mobility (or even stationary MNs) the tunneling taking place through the MAP provides an unnecessary delay in the packet delivery due to the additional packet tunneling through the MAP.

The Adaptive Route Optimization ARO scheme introduced by (Pack et al. 2007) attempts to solve this issue by suggesting to measure the session activity of the MN and to compare it to the relative mobility of the same MN. The resulting ratio is called the session-to-mobility ratio (SMR) which is then used to determine wither the
packets need to be tunneled through the MAP or if the packets should be redirected directly to the MN thus saving the overhead resulting from tunneling the packets through the MAP.

As (Pack et al. 2007) put it, depending on the measured session-to-mobility ratio SMR, ARO chooses one of the two different route optimization algorithms adaptively. Specifically, an MN informs a correspondent node CN of its on-link care-of address LCoA if the CN’s SMR is greater than a predefined threshold. If the SMR is equal to or lower than the threshold, the CN is informed with the MN’s regional CoA RCoA.

This adaptive mechanism allows the network to get the best of both worlds. When there is a need for the MAP tunneling due to the high probability of the MN to move from one domain to another then the CN is informed by the mobile node of its RCoA. However, in cases where the MN is relatively stationary, the CN is informed by the MN of its LCoA thus saving the packets delays resulting from the unnecessary MAP tunneling. Furthermore, if the MN mobility is low but also the session activity is low then the MAP tunneling would not make a significant difference and it is thus determined by the adaptive system following this scheme to keep the MAP tunneling since the benefits of mobility oversights the negligible decrease in performance.

However, one of the disadvantages of this system is that the session-to-mobility ratio SMR needs to be calculated by the MN which needs to also determine withers to inform the CN with its RCoA or its LCoA. This adds extra computing power and computational overhead on the MNs and might decrease the performance and battery life in ways that overweigh the expected improvement in packets delay thus more research should investigate wither this computation consists a burden on the MNs.

Applications of this ARO scheme include its implementation in network mobility NEMO where a group of MNs are moving together in vehicular area networks (Pack et al. 2009). This is accomplished by an adaptive NEMO support protocol based on Hierarchical Mobile IPv6. The proposed protocol jointly optimizes
binding update (BU) traffic and tunneling overhead by employing the adaptive BU strategy, depending on the session-to-mobility ratio (SMR).

### 2.10.5 Cooperative Diversity in PHMIPv6

Cooperative diversity was proposed by (Letaief & Taleb 2010) as a scheme that provides faster handover through communicating with a partner MN before entering to the new domain in what is known as Partner-based Hierarchical Mobile IPv6 (PHMIPv6). Traditionally, this was accomplished by selection of a partner MN according to its single strength. But this method produces some errors especially since the connection with the partner MN does not last long enough as the MN enters to the new domain. Another issue of concern is the security vulnerability that arises from these MNs communicating among each other.

To solve these issues a new scheme called Connection Stability Aware PHMIPv6 (CSA-PHMIPv6) was proposed by (Letaief & Taleb 2010) which ensures that the connections which has the tendency to remain active for a longer time are given priority. This is accomplished by employing the Link Expiration Time (LET) parameter. To tackle the security issues, a simple two distinct authentication keys were used to provide an extra layer of security.

### 2.10.6 Hybrid Location-Update Scheme for Mobile Networks

Traditionally, location updates LU in mobile networks were carried out either following a time- or movement based approach. Each of which had its own advantages and disadvantages. The Hybrid Location-Update Scheme introduced by (Goo et al. 2009) combines both approaches into one hybrid approach.

This is accomplished by the following proposed by (Goo 2009), a mobile user updates its location after the following two events have occurred: First, the mobile crossed $n$ cell boundaries, and then, a time interval $T$ elapsed. We also examine the inverse scheme, where an update is performed after the $n$ boundary crossings occur subsequent to the time interval $T$. 
The proposed system was tested and found that the hybrid scheme (i.e., $T > 0$, $n > 0$) outperforms each of the two approaches, namely, the time- and movement-based location-update schemes, when these schemes are individually applied.

2.11 SUMMARY

In this chapter we took a glance at the development of the Internet Protocol IP starting from its earlier version IPv4 and the mobility support in IP and its latest version IPv6 which was the beginning of a new revolution in the Internet in terms of the number of possible number of addresses and the improved quality of service. The operation of IPv4, IPv6 and their extensions such as Fast Handover Mobile IPv6 and Hierarchical Mobile IPv6 were discussed in this chapter. Furthermore, the usage of MAP was explained which act as an MN’s HA in the visited domain. Research introduced in the recent years were elaborated and discussed in the end of this chapter.
CHAPTER III

METHODOLOGY

3.1 INTRODUCTION

In order to solve the scalability issue of current implementations of HMIPv6 a new enhanced scheme of HMIPv6 called Smart-Selection Hierarchical Mobile Internet Protocol Version 6 will be introduced. This newly proposed scheme is further tested using newly developed simulation software to test the validity of the introduced conceptual model. For the choice of programming languages, Network Simulator (NS-2) was chosen and preferred over other programming languages due to its conformity to the real network and its general-purposes nature which allows the implementation of the mathematical model in order for us to evaluate the validity and soundness of the proposed conceptual model. Also the choice of (NS-2) was mainly due to the familiarity of the programming language. This proposed concept and the methodology followed will be detailed in this introduction section and further explained in the rest of this chapter.

3.2 SELECTION SCHEME IN HMIPv6

In Hierarchical Mobile IPv6, MAPs are responsible in the foreign domains of the registration of the Mobile Nodes (MNs) and tunneling the data to MNs when it is unreachable through its Home Agent (HA) IP address. However recent research shows that the traffic bottleneck could be formed at a MAP when it experiences high intensity of the tunneled traffic and the MN registration information. In other words when the number of served MNs increases to a large extent, the packets will queue up at a MAP as shown in Figure 3.1; this queuing will cause long delays of data traffic and registration process. Under certain traffic conditions; like providing multimedia
functions for many MNs in Mobile IPv6 networks, the interchange bottleneck can be produced at the MAP by the tunneled data interchange oriented to the MN. The bottleneck can produce large delay, losing data packets of the traffic and may cause the MAP offline.

A Smart Selection Hierarchical Mobile IPv6 that is proposed takes account information of the MN registration and the tunneled data traffic to release effectively and prevent the formation of the traffic bottleneck at the MAP. The SSHMIPv6 proposed mechanism can be implemented in Hierarchical Mobile IPv6 without changing the protocols of the communication between MAPs and MNs in IETF MIPv6 draft.

The proposed solution is focusing on the traffic load troubles including packets delay and number of lost packets at the MAP stage by organizing multiple MAPs using the same RCoA in the domain, so that the traffic can be shared between the MAPs. Load balancing methods are designed so that MAPs are animatedly allocated and suspended according to the traffic at each MAP. The Joining Shortest Queue (JSQ) was implemented in this study.

Figure 3.1 Packets flow to the MAP in HMIPv6
Deployment of MAPs will work on the tunnel traffic information and the registration information at each HA to reduce and prevent traffic overload. The number of MAPs in the domain depends on the number of MNs in the domain and the transferred packets among the MNs in the domain and their Home Agents and their Correspondent Nodes.

This chapter specifies in details the proposed Smart Selection Hierarchical Mobile IPv6 which adapts the Hierarchical Mobile IPv6 general management scheme and the research methodology. The overall methodology will be as shown in the block diagram Figure 3.2. The process starts by the development of theoretical, conceptual, mathematical and structural model for the enhanced SSHMIPv6 followed by a simulation for the theoretical and structural system. Performance evaluation is then carried out to check the validity of the proposed model through model validation and performance comparison.

Figure 3.2 Methodology Block Diagram
3.3 SMART SELECTION HIERARCHICAL MOBILE IPv6 (SSHMIPv6)

This proposed model will introduce an alternative architecture for the conventional HMIPv6 architecture which will further detailed in the rest of this section. Furthermore, a MAPs reassignment mechanism was introduced to specify how the distribution and load-balancing is handled.

Smart Selection Hierarchical Mobile IPv6 adapts a new operation using Multi Mobility Anchor Point (MAP) having the same RCoA, some mobile node expansion and access router processes as shown in Figure 3.3. The operations of the correspondent nodes and home agents are not involved in the change of location update since the entire cluster of MAPs has the same RCoA.

In SSHMIPv6, the domain is composed of multiple Mobility Anchor Points; each MAP in the domain is attached with an Access Router (AR) and the procedure shares the traffic packets among the MAPs in the domain to select the most suitable MAP to serve the MN as shown in Figure 3.4. The SSHMIPv6 conscious mobile node discovers the address of MAP and the distance from it. It configures two care of
addresses: Regional Care of Address (RCoA) on the MAP(s) link - the MAPs at the domain give the same RCoA- and On-Link Care of Address (LCoA). These two addresses are created in a stateless way as in HMIPv6.

![Figure 3.4 Packets flow in SSHMIPv6](image)

This chapter will further evaluate the performance of the proposed model by introducing and investigating the topology and architecture.

### 3.3.1 MAP Reassignment in SSHMIPv6

Sharing the traffic mechanism among multi MAPs in the domain is the main concept of SSHMIPv6 to decide about MAP Reassignment. An ascending order of the current MAP queue load is recorded to give an indication about the traffic load level of all MAPs in the domain.

The MAP should check its queue load and the registered MN number as shown in Table 3.1. Each MAP from time to time broadcasts its traffic load advertisement to all other MAPs in the domain.
Table 3.1 Load balance table

<table>
<thead>
<tr>
<th>MAP Number</th>
<th>MAP Queue Load</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAP 3</td>
<td>6</td>
</tr>
<tr>
<td>MAP 2</td>
<td>7</td>
</tr>
<tr>
<td>MAP 1</td>
<td>12</td>
</tr>
</tbody>
</table>

In the proposed SSHMIPv6 mechanism, the queue size field is used to make decision for MAP reassignment to free the traffic burden. This will prevent overloading a single MAP and thus provide a more balanced queue load.

The main concern is the effect of adding more than one MAP to serve each domain using the Join Shortest Queue (JSQ) selection scheme as shown in Figure 3.5 SSHMIPv6 routing scheme. The SSHMIPv6 mechanism shares the traffic information among the MAPs in the domain to make a decision about MAP reassignment. The load balancing strategy was also achieved among the multiple MAPs having the same RCoA and attached with the same Access Routers in the SSHMIPv6 domains which adopt the HMIPv6 protocols. When the Mobile Node (MN) moves to a new domain a new access router will updated through Binding Update (BU) which in turn will perform BU with the new MAP which will check for Duplication Address Detection (DAD) check to make sure that this MN is a new arrival to the domain. Subsequently, binding update acknowledgment will be returned to the AR and tunneled to the MN. And then another BU will be initiated to start receiving the packets tunneled through the MAP.
3.4 SIMULATION ENVIRONMENT

The situation studied was considered to execute experiments which are close enough to a real atmosphere and to offer sensible results. Chosen scenario is a hypothetical Internet was considered while simulating using a hypothetical IP address format considering of an integer number. Each hypothetical Internet network is assumed to consist of five domains and each domain is assumed to be composed of 100,000 nodes. Some of these are mobile nodes (1 to 5000). There are two copies of this hypothetical Internet, in one copy only one MAP is used in each region as shown in Figure 3.6 (a) while in the other copy more than one MAP is used in each region as shown in Figure 3.6 (b)
Figure 3.6 (a) Hypothetical HMIPv6 Internet consists of five domains (b) Hypothetical SSHMIPv6 Internet consists of five domains

The two Internets are identical in everything including events and packets generated. But only differs in the number of mobility anchor points in each region. It has been considered that all of the networks in the Internet are identical as well as all
mobility anchor points are identical. The time it takes to process a packet is the same for all of the mobility anchor points and for all types of packets.

To guarantee a reasonable foundation for the comparison, only the entrance of packets to the new domain (MAP part only) was examined, in the case where the MN is away from its HA.

A code tool was developed to simulate HMIPv6 as well as the proposed SSHMIPv6 which was used to verify the numerical results over the hypothetical Internet.

During the simulation the packet were generated of each clock tick using an assumed natural logarithm distribution equation because it is mathematically simple to use, the generated packets can be normalized simply and the correlation structure can be evaluated directly from the original value (Schneider & Gert 1982). The natural logarithm of the total number of mobile nodes is taken then it is multiplied by a small random number factor between 0 and 0.4 that indicates the assumed maximum number of active MN.

Each generated packet is assigned a random source IP and a destination IP. These hypothetical packets are generated randomly in the networks while time passes, consisting of a packet size field, time of reaction field and source and destination addresses are considered. The parameters that have been applied in simulation are summarized in Table 3.2.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packet Length</td>
<td>64 bits</td>
</tr>
<tr>
<td>Packet Process Time</td>
<td>8 ms</td>
</tr>
<tr>
<td>MAP Queue Size</td>
<td>16 packets</td>
</tr>
<tr>
<td>No. of Nodes in each area</td>
<td>1-100000 N</td>
</tr>
<tr>
<td>No. of MN in each area</td>
<td>1-5000 MN</td>
</tr>
<tr>
<td>No. of MAPs in each area</td>
<td>1-10 MAPs</td>
</tr>
<tr>
<td>No. of Areas</td>
<td>5 Areas</td>
</tr>
<tr>
<td>No. of Available Addresses in each area</td>
<td>100000 Addresses</td>
</tr>
</tbody>
</table>
Then the new packets trying to enter the domain are added to the packet queue of the region that has its destination address as shown in Figure 3.6. If the MAP queue is full, the packet is considered to be lost and so is added to the number of lost packets.

![Figure 3.6 The MAP Queue](image)

A packet that is placed in a queue will be sent according to the same order in which they have arrived hence it is called as first in first out (FIFO) queue (Fiat et al. 2007). The packet has to wait in the queue until it is picked up by the mobility anchor point in the region following FIFO mechanism which processes the packet arrived first. The time that the packet spends in the queue waiting for the mobility anchor point to process is considered the packet delay and it is later used to compute the average packet delay.

A logical clock was used and structures were constructed for events and packets. Each event was stored with its time of occurrence. First, addresses to all nodes on the networks such as IP addresses and CoAs were assigned and all simulation variables were set up and then clock was initialized.
A series of simulation experiments was performed to examine the delay of transmitted packets, lost packets, and Goodput for HMIPv6 and SSHMIPv6 architectures.

The domain is not divided into part domains, because if the part domain with only one MAP handles many MNs, we will face again the same scalability problem which causes a big delay and a lot of lost packets. Moreover, if other part domain serves a slight number of MNs, it will be waste cost.

Since security issues in mobile IP did not play a direct role in our analysis, and since we did not want to do injustice to an issue which would be a whole research topic in itself, we did not concern ourselves with the security considerations in our simulation.

At the beginning we defined the types of the used elements starting from packet size and then we store the packet information; packet size, packet source IP address, packet destination IP address and the sent time for the packet. After that the MN IP address and CoA was stored as well as the time for processing the received packet in the MAP. The information for the MAP as its IP addresses, number of packets, number of nodes and MAP queue size also were stored. The number and the list of MAPs in the area, the list of Mobile Nodes in the area, number of Mobile Nodes, the available addresses for the local nodes and Mobile Nodes in the area were stored as well.

3.5 SIMULATION MODEL

The main processes in the simulation is as follow:

3.5.1 Program Initialization

Initialize all program variables and parameters such as giving each node an IP address and each Mobile Node a care of address and distributing the nodes all over the areas
on the networks and initializing mobility anchor points and their variables as shown in Figure 3.7.

![Sample Program Screen-Shot](image)

**Figure 3.7 Sample Program Screen-Shot**

### 3.5.2 Packet Generation

The process of packet generation is to generate a random number of packets all over the Internet and send them to their destination queues. While keeping track of the total number of the generated packets on the Internet during the simulation time and also counting all the lost packets when a new generated packet has to be sent to an area which has a full destination queue.

The generated packets were chosen to have a UDP packet specifications because a simpler message-based connectionless protocol is used. In this study there is no concept of acknowledgment, retransmission and timeout. Furthermore if two
packets have been sent to the same destination, the order in which they reach cannot be predicted (Postel 1980).

Three traffic models have been used to generate packets during the simulation:

(i) Generating packets using the natural logarithm model:

To generate the packets in this model (Schneider & Gert 1982), two matters are considered; the first is that 40% of the Mobile Nodes are active and transferring Packet at the moment. The other is the generation of random number for the natural logarithm of the Mobile Nodes.

\[
P_G = 0.4 \times R \times \ln(MNs)
\]

(3.1)

\[
P_{TG} = \sum P_G
\]

(3.2)

where

- \(P_{TG}\) is the total number of generated packets.
- \(P_G\) is the number of generated packet at each microsecond.
- \(R\) is the random number between 0 to 1
- \(MNs\) is the total number of Mobile Nodes.

(ii) Generating packets using the specific model:

In this model we assumed that each Mobile Node generates a packet at each step of the simulation. The following equations show the total number of generated packets in terms of total number of mobile nodes and the summation of number of packets generated each microsecond.

\[
P_G = MNs
\]

(3.3)

\[
P_{TG} = \sum P_G
\]

(3.4)

where

- \(P_{TG}\) is the total number of generated packets.
- \(P_G\) is the number of generated packet at each microsecond.
- \(MNs\) is the total number of Mobile Nodes.
(iii) Generating packets using the random model

In this model we assumed that random number for the Mobile Nodes generate a packet at each step of the simulation (Murdoch & Lewis 2005). The following two calculate the total number of generated packets and the number of generated packets at each microsecond taking into account the generation of a random number.

\[ P_G = R \times MNs \]  
\[ P_{TG} = \sum P_G \]  

where

- \( P_{TG} \) is the total number of generated packets.
- \( P_G \) is the number of generated packet at each microsecond.
- \( R \) is the random number between 0 to 1
- \( MNs \) is the total number of Mobile Nodes.

### 3.5.3 Packet delivery

Deliver packets in the queues to their destination nodes through the mobility anchor point if there is only one map or through any available MAP if there are multiple MAPs in the area. Keeps track of the total packets delay during simulation

Once the packet arrives to the queue it will check if there is an empty location to occupy or not. If there is a location to occupy, the MAPs will be scanned whether it is busy or free. If \( Q_{in} = Q_{out} \), then the MAP is free now as shown in Figure 3.8. But if \( Q_{in} \neq Q_{out} \), then the MAP is busy with processing other packets. Then the packet takes place in the queue waiting its order to have the process from the MAP as shown in Figure 3.6.
Figure 3.8 The empty MAP Queue

\[ Q_{\text{nin}} = (Q_{\text{pin}} + 1) \mod (Q_s) \]  \hspace{1cm} (3.7)

where

- \( Q_{\text{nin}} \) is the first available location in the queue for the new coming packet to occupy.
- \( Q_{\text{pin}} \) is the location where the last packet is occupied.
- \( Q_s \) is the queue size.

If there is any free location in the queue to pick up new packets as shown in Figure 3.9, the packets will occupy \( Q_{\text{nin}} \) which is \((Q_{\text{pin}} + 1)\) until they reach the end of the queue then they will continue to take places starting from the first place in the queue which will be illustrated in the Figure 3.9.
Figure 3.9 The packet occupation in the MAP Queue

### 3.5.4 Performance Metrics

The analyses concentrate in Packet Delay, Lost Packets, Lost Packet Ratio and Goodput.

i. Packet delay

Network delay is often a key performance parameter in the communication that denotes the performance of the network services upon Internet Service Provider (ISP) users (Huston 1998). When packets are sent over a network towards a destination node, some of them might be delayed. The delayed packet may come late or may not come at all, in case it is lost. So delay also occurs when packets of data take more time than expected to reach their destination (Demichelis & Chimento 2002).

The packet has to wait in the queue until it is picked up by the Mobility Anchor Point in the region. The time that the packet spends in the queue waiting for the Mobility Anchor Point to process is the considered packet delay and it is later used to compute the average packet delay.

Average packet delay is identified as the ratio of the accumulated delay of the packets delivered to the destinations together with the total number of the packets delivered. Hence delay of an individual packet is the time in between the entry of the
packet into the queue and the time of its delivery to the receiver (Chuah & Zhang 2006).

For 1 MAP using HMIPv6, the packets delay can be calculated by subtracting the packet generated time from the current process time or by multiplying the number of packets in the queue with the packet process time as can be seen in the following equation (Demichelis & Chimento 2002).

\[ D_p = T_{CP} - T_{PG} = P_{NQ} \times T_{PP} \]  \hspace{1cm} (3.8)

where

- \( D_p \) is the packet delay.
- \( T_{CP} \) is the current process time.
- \( T_{PG} \) is the packet generated time.
- \( P_{NQ} \) is the number of packets in the queue.
- \( T_{PP} \) is the packet process time.

For \( M \) packets, subsequently, to calculate the average packet delay in the MAP is applied by summing up the delay in all the packets. This can be seen in the following equation.

\[ D_{TP} = D_{P1} + D_{P2} + D_{P3} + \ldots + D_{P(M-2)} + D_{P(M-1)} + D_{PM} \]  \hspace{1cm} (3.9)

\[ D_{TP} = \sum D_p \]  \hspace{1cm} (3.10)

where

- \( D_{TP} \) is the average packet delay in the MAP.
- \( D_p \) is the packet delay.

For \( N \) MAPs using SSMIPv6, the average packets delay for all MAPs in the SSMIPv6 is calculated by summing up the accumulated average Packet Delay in each of the MAP in the system as shown in the following equation.

\[ D_{STP} = D_{TP1} + D_{TP2} + \ldots + D_{TP(N-1)} + D_{TPN} \]  \hspace{1cm} (3.11)

\[ D_{STP} = \sum D_{TP} \]  \hspace{1cm} (3.12)

where

- \( D_{STP} \) is the average Packet Delay for all MAPs in the SSMIPv6.
$D_{TP}$ is the average Packet Delay in the MAP.

ii. Lost packets

Packet loss describes an error condition in which data packets appear to be transmitted correctly at one end of a connection, but never arrive at the other (Bolot 1993). This might be either because the network conditions are poor and the packet became damaged in transit or because the packet was deliberately dropped at a router because of Internet congestion.

Packet loss means the total number of packets aside from the number of packets received by the receiver. Thereby the term Packet Loss is used as a measure of the overall number of packets which are not delivered to the destination and/or to the receiver (Jacquet & Cho 2005).

If there is a packet in the header of the queue $Q_{out}$ and also there is a packet in the tail of the queue $Q_{in}$, the MAP queue is full as shown in Figure 3.10. If the region queue is full, the new packet has no location to occupy then it is considered to be lost and so it is added to the number of lost packets, $P_L$, which could be presented as:

$$P_{Q_{out}} = (P_{Q_{in}} + 1)\mod(Q_s) \quad (3.13)$$

Where

$P_{Q_{out}}$ is the location of the packet in the header of the queue.

$P_{Q_{in}}$ is the location of the packet in the tail of the queue.

$Q_s$ is the queue size.
Figure 3.10 The MAP Queue full of Packets

For $M$ Lost Packets, the total lost packets is the summation of all the lost packets. This can be seen in the following equation.

$$P_{TL} = P_{L1} + P_{L2} + P_{L3} + \ldots + P_{L(M-2)} + P_{L(M-1)} + P_{LM}$$  \hspace{1cm} (3.14)

$$P_{TL} = \sum P_L$$  \hspace{1cm} (3.15)

where

$P_{TL}$ is the total number of lost packets for one MAP.

$P_L$ is the number of lost packet.

For $N$ MAPs in the case of SSHMIPv6

$$P_{STL} = P_{TL1} + P_{TL2} + \ldots + P_{TL(N-1)} + P_{TLN}$$  \hspace{1cm} (3.16)

$$P_{STL} = \sum P_{TL}$$  \hspace{1cm} (3.17)

where

$P_{STL}$ is the total number of lost packets for all MAPs in the SSHMIPv6.

$P_{TL}$ is total number of lost packets for one MAP.

iii. Packet Lost Ratio

The Lost Packets Ratio is the percentage ratio for the lost packets with respect to the Generated Packets (Oshida & Ihara 2006).

$$RP_{TL} = \frac{P_{TL}}{P_G} \times 100\%$$  \hspace{1cm} (3.18)

where
\( R_P_{TL} \) is the lost packets ratio.
\( P_{TL} \) is the total number of lost packets.
\( P_G \) is the number of generated packets.

iv. Throughput

Throughput is defined as the number of data bits correctly transferred per unit of time (Green 2006). The number of information bits per second which are received completely by the data users served is also referred to as data throughput. Average data throughput therefore is defined as the ratio of the number of information bits which are received at a simulation run and simulation time by the receivers. In general, the greater the bandwidth of a given path, the higher the Throughput and is calculated by dividing the total generated packets by the simulation time in microseconds as seen in the following equation (Chuah & Zhang 2006).

\[
\text{Throughput} = \frac{P_G}{T_S \times 10^{-6}} \times \frac{S_P \times 8}{1024 \times 1024} \tag{3.19}
\]

where

\( Throughput \) (Mbps).
\( P_G \) is the number of generated packets.
\( T_S \) is the simulation time (\( \mu s \)).
\( S_P \) is the packet size (byte)

It is known that: 1 byte = 8 bits, 1 Mega byte = \( 2^{20} \) bytes, 1 \( \mu s \) = \( 10^{-6} \) s.

v. Goodput

Goodput is referred to as the number of useful bits per unit of time forwarded by the network from a certain source address to a certain destination, excluding protocol overhead, and excluding retransmitted data packets. For instance, when a file is transferred, the goodput that the user experiences corresponds to the file size in bits divided by the file transfer time (Henssonow et al. 2010). Goodput is also defined as the number of successful transmissions per second (Kochut et. al 2004). The goodput is usually expressed in bits, characters, blocks, or frames per second. The goodput may be averaged over a period of seconds, minutes, or hours. In this study the goodput is expressed as bits per second.
The total delivered packets is calculated by subtracting the total lost packets delivered from the generated packets as can be seen in the following equation.

\[ P_{TD} = P_G - P_{TL} \]  \hspace{1cm} (3.20)

where

- \( P_{TD} \) is the total number of delivered packets.
- \( P_G \) is the number of generated packets.
- \( P_{TL} \) is total number of lost packets.

The goodput is calculated by dividing the total delivered packets by the simulation time in microseconds as seen in the following equation (Nakanishi et al. 1994).

\[ \text{goodput} = \frac{P_{TD}}{T_s \times 10^{-6} \times \frac{S_P \times 8}{1024 \times 1024}} \]  \hspace{1cm} (3.21)

where

- \( \text{goodput} \) \text{ (Mbps)}
- \( P_{TD} \) is the total number of delivered packets.
- \( T_s \) is the time of simulation (\( \mu \text{s} \)).
- \( S_P \) is the packet size (\text{byte}).

1) Simulation main routine

The simulation main routine calls other routines and controls the program execution as the following:

- a. Determine the starting point
- b. Determine the end time
- c. Initialize random numbers
- d. Prepare the progress bar
- e. Moving the clock step by step (the end of simulation clock equal to the end time)
- f. Display the results as shown in Figure 3.11.
3.6 SSHMIPv6 SIMULATION USING NETWORK SIMULATOR (NS-2)

NS-2 is widely used in network simulation due to the facts that it is free, open source, flexible and scalable. Although NS-2 has been a good support for Mobile IPv4 simulation, it is still considered to be weak for Mobile IPv6. Therefore the Mobiwan was formed in order to fulfill NS-2 by adding MIPv6 features for NS-2. Mobiwan was developed by MOTOROLA Labs Paris in collaboration with INRIA PLANETE Team in aim of simulating wide area mobility protocols such as Mobile IPv6 and Hierarchical Mobile IPv6 (Saldatos & Karestos 2003).

3.6.1 The Simulation Tool: NS-2

This section verifies the performance improvement of SSHMIPv6 by performing a simulation. The simulation was carried out using Network Simulator (NS-2). NS-2 is widely used network simulation tool extensively developed by the worldwide
academic community. Its wide usage is contributed to it being free, open sources, flexible and supports scalability. NS-2 has a good support for Mobile IPv6 through the Mobiwan extension which was created to improve NS-2 by adding Mobile IPv6 simulation features for NS-2 (Thoppe & Ganesan 2007). Its results are referenced in academic researches, journal papers and textbooks and it has a wide acceptance in the academic community.

According to the documentation of NS-2, NS-2 is a discrete event simulator targeted at networking research. NS-2 provides substantial support for simulation of TCP, routing, and multicast protocols over wired and wireless (local and satellite) networks. NS-2 provides a library of network models and components that can ease the process of designing the network topology to be used in the simulation. For instance, ready made components such as routers, mobile nodes, packets and MAPs are available and programmed to be configurable according to the specific needs of the current simulation model.

### 3.6.2 Simulation Model Topology

For the purpose of our simulation the following topology was constructed to simulate the standard HMIPv6 using the following assumptions. Three Mobile Nodes (MNs) were introduced and configured to send packets to Correspondent Nodes (CNs) in another domain. Hence, a Mobility Anchor Point (MAP) was introduced to act as the tunnel connection the two Access Routers (ARs) illustrated in Figure 3.12.

Each network component was named with a node ID starting from zero as shown in Figure 3.12. The links were defined in the simulation models according to the details presented in Table
Finally, to compare between the performances of SSHMIPv6 in contrast with that of HMIPv6, a model was constructed assuming that SSMHIPv6 through its queue management algorithm has successfully distributed the 1200 packets with a size of 1460 bytes each which needs to be sent on three MAPs thus reducing the congestion occurring on the single MAP in the HMIPv6 model. It will be assumed that this distribution resulted in 300 packets being redirected to one MAP, another 400 packets to the second MAP and finally the remaining 500 packets to the third MAP. The total of 1200 packets sent is finally compared to that of the standard HMIPv6 case.

### 3.7 SUMMARY

In this chapter the methodology was outlined by introducing the proposed implementation of the Smart Selection Hierarchical Mobile IPv6 (SSHMIPv6) by
preventing the formation of a traffic bottleneck at the MAP level. This was achieved by focusing on the traffic load troubles including packets delay and number of lost packets at the MAP stage by organizing multiple MAPs using the same RCoA in the domain. For the implementation of the queuing handling algorithm this chapter suggested the usage of a Join Shortest Queue (JSQ) mechanism that should provide better queues handling. The need for simulation software was discussed and the mathematical models and equations used in this simulation software were introduced and explained in this chapter.
CHAPTER IV

RESULTS AND ANALYSIS

4.1 INTRODUCTION

This chapter will present and analyze the results obtained by the simulation software. These results are calculated based on number of packets generated using natural algorithms mathematical model. The results show and analyze the improvement achieved by the implementation of SSHMIPv6 in terms of packets delay and lost packets ratio. Two parameters are varied in the generation of the previous results namely the number of Mobile Nodes and the number of MAPs in each domain. Furthermore, the processing time of each packet by the MAPs is taken into account to analyze its effect on the performance of the MAP in terms of packets processing time.

Moreover, the mathematical model used for the generation of packets is changed to experiment on the effects of applying different packets generation models such as the Random Model and a model that is based on the number of mobile nodes.

4.2 RESULTS AND DISCUSSIONS

The first aim of the simulation is to analyze the effect of adding more than one MAP to serve each region on the performance of Mobile IPv6 in terms of packet delay and lost packets, and the second aim is to show the study validation by serving different number of generated packet, using several MAP processing time and testing different traffic modules.

Figure 4.1 to Figure 4.3 show the performance of SSHMIPv6 and HMIPv6 in terms of average packet delay, number of lost packets and the lost packet ratio in the MAP for various numbers of transferred packets respectively.
Figure 4.1 shows that if more MAPs are used, the average delay will be reduced. Taking the results at 1688680 packets transferred, it was noticed that in the case of HMIPv6 that uses just an MAP, the average packet delay is around 221 ms but if we increases the number of MAPs to two, the average packet delay will go down to 108 ms. However if we use three MAPs at each area, it will absolutely enhance the performance of the Internet by making the average packet delay less and it will reach 69 ms, whereas 4 MAPs are simultaneously serving the MNs in the domain but the reasonable result is not obtained as in the case of using five MAPs which gives a result that tends to a 21 ms average-packet delay. These results show reductions in average packets delivery delay of 51.5% when using two MAPs and reaching up to 92% reduction when using four MAPs. This reduction in the average-packet delay is really significant since it means that users will experience higher speeds. It can be seen here that although only few megabytes of data transmission are considered, yet a significant improvement was achieved as seen in the previous results. Therefore, very significant improvements can be achieved when dealing with higher data transmission sizes in application such as video transmission and VOIP protocol.
From Figure 4.2; it can be observed that we will get a better performance for the number of lost packets when using more MAPs. Taking the results for 1625000 packets transferred, we can conclude that in the case of HMIPv6 that uses just one MAP the number of lost packets is around 1294540. If we increase the number of MAPs to two, the number of lost packets will be slightly reduced to 961240 packets. But in case of using three MAPs at each area, the performance of the Internet gets better by making the Number of packet-lost smaller to about 629780 packets, whereas if there are 4 MAPs running at the same time and handling the MNs in the domain, a better result will be obtained but it still not as good as using five MAPs which gives a very good result. Subsequently, reduction percentage in the number of lost packets were calculated to be 24.4% when using two MAPs and can reach up to 73.3% reduction when four MAPs are used in each domain. This improvement is significant due to the fact that the reduced number of lost packets will result in a better performance in terms of reducing intermittence.
As is known the lost-packet ratio is defined as the number of lost packet divided by the total number of transferred packets. However, it follows the same behavior of the lost-packet number as shown in Figure 4.3. It is also noticeable from the figure above that there is an inverse relationship between the number of MAPs and the lost packet ratio. If we study the (1599300 transferred packets) line, we can see the descending order of lost-packet ratio starting from 80% as in the case of using one MAP in HMIPv6 ending with only 2% as in the case of 5-MAPs. This is due to fact that the 5 MAPs were sufficient to cater for all the packets. Thus, almost no packets dropped and as a result the lost-packet ratio reduced significantly when 5 MAPs were used.

Figure 4.2 Number of lost Packets versus number of MAPs at each Area
The numbers from 1242020 to 1698440 in the legend of Figure 4.1 to Figure 4.3 which are randomly generated, represent the total number of the transferred packets within the simulation, that indicate the most suitable number of MAPs needed to be used for each area. For instance the graph indicates that three MAPs are enough to handle all of the MNs and process all transferred-packets if the number of transferred packets is 1242020 packets, with a good performance. Hence one can conclude that more than 3-MAPs are useless and costly since increasing the number of MAPs will not provide further significant improvement.

On the other hand, when the MAPs handle more packets, such as handling 1599300 transferred packets as shown in the Figure 4.3, we can notice that more than 3-MAPs are needed to get the best performance.

Furthermore, Figure 4.4 to Figure 4.7 show the performance of SSHMIPv6 and HMIPv6 in terms of average packet delay, number of lost packets, the ratio of lost packets Goodput for various packet process time.
From Figure 4.4, we can see that if more MAPs are used, the average delay will be reduced. As if we take the 12 ms packet-process time line, we can notice that in case of HMIPv6 that consists of one MAP the average packet delay is around 176 ms but if the number of MAPs is increased to two, the average packet delay will descend to 85 ms. while if we use three MAPs at each area, the performance of the network is enhanced by decreasing the average packet delay to 53 ms, whereas 4 MAPs are simultaneously serving the MNs in the domain, some improvement can be seen but using five MAPs still yields the best results since it gives an almost zero average-packet delay.

Similarly, once we look into the Figure 4.5; it is observed that we will get better performance in terms of number of lost packets when using more MAPs. For instance, in the 20 ms packet-process time line, we can conclude that in case of HMIPv6 that uses just one MAP the number of lost packets are around 1448220 packets. Where else if we increase the number of MAPs to two, the number of lost packets will slightly decrease to 1198240 packets. However, in the case of using three MAPs at each area, the performance of the network gets better by decreasing the
number of packets-lost to 952820 packets, whereas if there are 4 MAPs running simultaneously and handling the MNs in the domain, the result will see some improvement but not to the optimal level of using five MAPs.

Figure 4.5 Number of lost packet versus number of MAPs at each area

Similarly, it follows the same trend of the lost-packet number as shown in the Figure 4.6. It is also noticeable from the figure above that there is an inverse relationship between the number of MAPs and the lost packet ratio. If we study the (24 ms packet-process time) line, we can see the descending trend of the lost-packet ratio starting from 88% at the case of using one MAP in HMIPv6 to about 4% for the case of using 8-MAPs.
Figure 4.6 Lost Packets Ratio versus Number of MAPs at each Area

Figure 4.7 shows that if more MAPs are used, the Goodput will be increased. As if we take the 12 ms packet-process-time line, we can notice that in case of HMIPv6 which uses only one MAP the Goodput is about 203 Mbps. However, if we increase the number of MAPs to two, the Goodput will be increasing to 407 Mbps. while if we use three MAPs at each area, the Goodput increases up to 610 Mbps, whereas 4 MAPs are simultaneously serving the MNs in the domain. This reveals that although some improvement was achieved, the optimal number of MAPs in this case is five.
The series numbers from 8 ms to 32 ms in the legends of Figure 4.4 to Figure 4.7 represent the assumed time needed by the MAPs to process a packet which indicates the maximum number of MAPs needed for each area. For instance, the graph indicates that three MAPs are enough to handle all of the MNs and process all transferred packets if the process time for each packet is 8 ms, with a good performance. Hence one can conclude that the optimal number of MAPs is three since adding any more MAPs will not improve the results.

Furthermore, if the AR takes longer time to process the data as in the line with the 16 ms process-time shown in Figure 4.4 to Figure 4.7 it can be noted that more than 3-MAPs are needed to get the best performance, since the packet-process times have been changed from 8 ms up to 16 ms.

As we have mentioned, to validate the study, the simulation has compared the analysis elements between HMIPv6 as in the case of using one MAP serving the domain and SSHMIPv6. Also, the study has used different number of MAPs serving...
one domain to make sure that the model is valid. Another step to test the validity of the study was to use different traffic sizes and different MAP process times as shown above.

The previous results shown in Figure 4.1 to Figure 4.7 are obtained from the natural logarithm generated packet module. Moreover to ensure the validity of the model, another two traffic modules were tested; the first is the specific module and the other is the random module.

In the case of assuming the number of packets to be equal to the number of Mobile Nodes MN which means that each MN is assumed to be sending only one packet, Figure 4.8 to Figure 4.11 show the performance of SSHMIPv6 and HMIPv6 in terms of average packet delay, number of lost packets and the ratio of lost packets in the MAP.

Looking into Figure 4.8, we can see that the same indication as using natural logarithm traffic generation model could obtained; if more MAPs are used, the average delay will be reduced. We can notice that in case of HMIPv6 that uses just one MAP the average packet delay is around 14 ms but if we increases the number of MAPs to two, the average packet delay will decreases to 6.5 ms while if we use three MAPs at each area, the performance of the network in enhanced by decreasing the average packet delay to reach the 4 ms, whereas 4 MAPs are simultaneously serving the MNs in the domain, some improvement can be noted but the case of using five MAPs still yields better performance.
From Figure 4., it can be observed that we will get a better performance for the number of lost packets when using more MAPs. We can conclude that in the case of HMIPv6 that uses just one MAP the number of lost packets is around 35998600 packets. If we increase the number of MAPs to two, the number of lost packets will be slightly reduced to 29998700 packets. But in case of using five MAPs at each area, the performance of the Internet gets better by making the number of packet-lost smaller to about 14998800 packets.
The Lost Packets Ratio follows the same trend of the lost-packet number as shown in Figure 4. It is also noticeable from the figure that there is an inverse relationship between the number of MAPs and the lost packet ratio. It is seen that the descending order of lost-packet ratio starting from 83% as in the case of using one MAP in HMIPv6 ending with only 36% as in the case of 5-MAPs.
If we have a look towards Figure 4., we can see that if more MAPs are used, the Goodput will be increased. It is noticed that in case of HMIPv6 that uses just a MAP the Goodput is around 2441 Mbps but if we increases the number of MAPs to be two, the Goodput will be increased to 4883 Mbps. while if we use three MAPs at each area, this will enhance the performance of the network by increasing the Goodput up to 7324 Mbps.

Furthermore, Figure 4.12 to Figure 4.15 show the performance of SSHMIPv6 and HMIPv6 in the case of using a random traffic generation model in terms of average packet delay, number of lost packets, the ratio of lost packets and Goodput.

As can be seen in Figure 4.12, it is noted that if more MAPs are used, the average delay will be reduced. we can notice that in case of HMIPv6 which uses just one MAP the average packet delay is near to 15 ms but if we increases the number of MAPs to two, the average packet delay decreases to 6 ms while if we use three or more MAPs at each area, the performance of the whole network improves correspondingly.
It can be noted from Figure 4.13 and Figure 4.12 that the optimal performance for the number of lost packets and the lost packets ratio can be obtained when using more MAPs. Whereas if there are 5 MAPs running at the same time and handling the MNs in the domain, this results to an increase in savings reaching to 70%.
Looking at Figure 4.15, we can see that if more MAPs are used, the Goodput is almost identical to the case of using natural logarithm and specific traffic models.
4.3 LOST PACKETS PERFORMANCE ANALYSIS THROUGH NS-2

The results obtained from testing the standard HMIPv6 under a flow of 1200 packets can be seen in Figure 4.16. It can be noted from the figure that HMIPv6 performs adequately in the beginning of the sending interval. However, as the sending time progresses and the number of packets queued on the MAP increase the number of packets lost increases significantly to reach a value of above 30 KByte of lost data.

![Figure 4.16 No. of lost packets for Data Flow of 1200 packets under HMIPv6](image)

The simulation results for the first MAP under the SSHMIPv6 model can be seen in Figure 4.17 which illustrates that the data lost throughout the sending interval was merely 3.3 Kbytes. Subsequently, the second MAP which handled a data flow of 400 packets showed the results represented in Figure 4.18. It can be seen that data loss of only 8.1 Kbytes were experienced. Finally, the third MAP which was assigned with 500 packets of the data sent showed a data loss of about 12.1 Kbytes.
Figure 4.17 No. of lost packets for Data Flow of 300 packets under SSHMIPv6

Figure 4.18 No. of lost packets for Data Flow of 400 packets under SSHMIPv6
Figure 4.19 No. of lost packets for Data Flow of 500 packets under SSHMIPv6

Figure 4.20 shows the comparison of results obtained from sending 1200 packets of data through Standard HMIPv6 in contrast with sending the same amount of data through the proposed SSHMIPv6. It can be seen that while HMIPv6 suffered from significant data loss of 35 Kbytes, the distributed nature of SSHMIPv6 though its queue management algorithm resulted in a combined data loss of 23.5 Kbytes which is significant improvement over the current standard HMIPv6 model. The improvements which could be gained through using three MAPs in SSHMIPv6 instead of one in HMIPv6 show approximately 33 % decrease in lost packets as illustrated in Table 4.1.
<table>
<thead>
<tr>
<th>No. of Transferred Packet</th>
<th>Transferred Data Size</th>
<th>Lost Packets</th>
<th>Lost Packets for 1200 Transferred Packets</th>
<th>Improvement of using 3 MAPs</th>
</tr>
</thead>
<tbody>
<tr>
<td>300</td>
<td>438 Kbyte</td>
<td>3.3 Kbyte</td>
<td>23.5 Kbyte</td>
<td>33 %</td>
</tr>
<tr>
<td>400</td>
<td>584 Kbyte</td>
<td>8.1 Kbyte</td>
<td>(SSHMIPv6)</td>
<td></td>
</tr>
<tr>
<td>500</td>
<td>730 Kbyte</td>
<td>12.1 Kbyte</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1200</td>
<td>1752 Kbyte</td>
<td>35 Kbyte</td>
<td>35 Kbyte (HMIPv6)</td>
<td></td>
</tr>
</tbody>
</table>

### 4.4 SUMMARY

As a conclusion for this chapter, after performing the simulation over SSHMIPv6 it has been shown that using more MAPs leads to a reduction in packet transmission delay, less number of lost packets and less lost packet ratio. This is supported by the concrete findings stated in Chapter 5 including a reduction in average packets delivery delay of 51.5% when using two MAPs and reaching up to 92% reduction when using four MAPs. Moreover, reduction percentage in the number of lost packets were calculated to be 24.4% when using two MAPs and can reach up to 73.3% reduction when four MAPs are used in each domain. NS-2 network simulation tool was used to verify these results and it was shown that SSHMIPv6 provided improvement over the standard HMIPv6.
CHAPTER V

INCORPORATED DOMAINS

5.1 INTRODUCTION

In the previous chapter it was already seen that an improvement was achieved by assigning neighboring Mobility Anchor Points (MAPs) in a domain sharing the same Regional Care of Address (RCoA). Furthermore, if we combine more than one domain together using the same RCoA even better performance can be achieved since the frequency of location updates on the MAP level will be minimized thus resulting in a lower cost of location update.

The objective of this chapter is to introduce the concept of incorporated domains as an application of SSHMIPv6. This is done by introducing the concept, developing the conceptual and mathematical model and analyzing the improvement in terms of cost reduction through simulation.

The scope will be limited to the brief description and simulation of the newly proposed concept of incorporated domains through the development of a computer application that will be used to test and simulate the improvement in term of reduction of cost of location updates in the system. The effect of hand-off latency is beyond the scope of this thesis. However, further research can experiment on its effects on the cost reduction shown in this thesis.

5.2 INCORPORATED DOMAINS IN HMIPv6

In HMIPv6, When a Mobile Node moves between different Access Routers under the same domain in Micro-Mobility movement, only the LCoA changes while the RCoA
remains the same and only the corresponding MAP will be informed about the change. However, when the movement occurs between ARs which are located under different Mobility Anchor Points MAPs both the LCoA and the RCoA need to be changed thus more cost will incurred since both the HA and all the CNs need to be informed of the new location address.

To study the performance of location updates it is assumed that the number of location updates between Access Routers follows Poisson distribution which is described by the following mathematical models according to Dutta & Misra (2007) who study the Location Update performance in HMIPv6 with assumption of the subnet-crossing rate of all the mobile nodes is independent of each other and based on the probabilistic function and obey Poisson distribution. This model is an improvement of the mathematical model first proposed by (Peng et al. 2003).

\[
P_{AR} = \frac{(\mu t)^k e^{-\mu t}}{k!}
\]

(5.1)

Where

- \(P_{AR}\) is the frequency of location update due to change of AR.
- \(\mu\) is the sub-net crossing rate.
- \(k\) is the number of changes of AR in t second.

Then, the mathematical model of the location updates between MAPs

\[
P_{MAP} = \frac{(\mu l t)^k e^{-\mu l t}}{k!}
\]

(5.2)

Where

- \(P_{MAP}\) is the frequency of location update due to change of MAP.
- \(l\) is the MAP level.
- \(\mu\) is the sub-net crossing rate.
- \(k\) is the number of changes of MAP in t second.
5.3 CONCEPT AND CHARACTERISTICS OF INCORPORATED DOMAINS

SSHIMIPv6 cater the issue of scalability through clustering more than one MAP, besides reducing the delay encountered by packets in the previous implementations of HMIPv6.

The domains which share a high number of traffic among them, for example, the domain that covers a university campus and a domain that covers the hostel of that camps share a huge number of Mobile Nodes moving between the two domains on daily basis as shown in Figure 5.1. The same concept can be applied to a domain covering a business district and the condominiums that accommodate those who work in this district are likely to have a high number of Mobile Nodes moving from one domain to the other.

Figure 5.1 Incorporate domain HMIPv6 architecture
If such relationships can be established, then combining these domains that share large numbers of Mobile Nodes moving between them under one SSHMIPv6 incorporated domain can provide huge savings in terms of cost of location update reduction and performance improvement since the movement between domains under the same incorporated domain involve cost of location updates only due to change of Access Routers (ARs) and not due to change of Mobility Anchor Points (MAPs).

Moreover, if such a relationship cannot be identified easily then merely combining several adjacent domains under one incorporated domain can achieve the same effect stated above since mobile nodes are more likely to move to adjacent domains instead of moving to distant far away domain. This concept of incorporated domains if implemented can provide cost of location update reduction and improve the performance since the load on the Home Agent (HA) and Mobility Anchor Points (MAPs) will be significantly reduced thus allowing faster processing of the remaining location update requests in the queue.

5.4 MATHEMATICAL MODEL ANALYSIS

When the concept of incorporated domains is applied to the previously stated mathematical model devised by Dutta & Misra (2007) in Equation 5.2 which will be affected as follows:

The mathematical model describing the number of location update due to change of MAPs shown in Equation 5.2 will be modified due to the change in the Sub-net crossing rate (µ) which can be calculated using the following equation derived by Wu (2003):

\[ \mu = \frac{\pi V}{4R_m} \]  

(5.3)

where \( R_m \) is the radius of the MAP domain and \( V \) is the average speed of MN. The radius will be increasing as a result of combining several domains together. Subsequently, the sub-net crossing rate (µ) will decrease resulting in a decrease in the frequency of location updates due to change of MAPs.
Nevertheless, the frequency of location update due to change of AR will remain the same and Equation 5.1 will not be affected. However, this will not affect the reduction in total cost since the number of location updates due to change of MAP will reduce significantly.

The above analysis based on mathematical models showed that the implementation of the concept of incorporated domains will result in an increase in the number of location updates due to change of Access Routers (AR) and a decrease in location updates due to a change of MAP. This supports the proposed concept of incorporated domains since it has a positive change compared with the original HMIPv6 mathematical model. This improvement will be further verified using a computer based simulation to test the validity of the mathematical analysis.

5.5 SIMULATION

This section verifies the performance improvement by performing a simulation supporting theoretical incorporated domains scenarios. The simulation program will allow the end-user to specify the number of domains out of possible 25 domains. Any number of these domains can be combined under incorporated domains. It is assumed that every Mobile Node (MN) belongs to a single Access Router (AR) and a single MAP inside each domain. Theses domains, MAPs, ARs and MN are assumed to be identical in terms of packet processing time, quality of service and serving area for the purpose of this simulation.

For the purpose of this simulation the cost will be calculated using the following formulas outlined by Dutta & Misra (2007).

5.5.1 Cost due to changing the AR

The cost of AR location update can be estimated as follows by multiplying the number of mobile nodes by the cost of packet processing in the queue and the summation of
the cost of packet processing in the queue, the cost per distance and cost of MAP update. This cost will be measured in Bytes.

\[ C_{AR-U} = m \times P_{AR} \times [Q_d + d_{LA} \times E(z) + C_{MAP-U}] \]  

(5.4)

Where

\( m \) is the number of mobile nodes.
\( P_{AR} \) is the frequency of location update due to a change in AR as defined in 5.4.
\( Q_d \) is the cost of packet processing in the queue.
\( d_{LA} \) is the distance in terms of number of hops from AR to MAP.
\( E(z) \) is the unit cost per distance.
\( C_{MAP-U} \) is the cost of MAP update.

5.5.2 Cost due to changing the MAP

The cost of MAP location update can be estimated as follows,

\[ C_{MAP-U} = C_{AR-U} + m \times P_{MAP} \times [Q_d + (d_i \times E(z)) + C_{MAP-U}] + d_{HG} \times E(w) \]  

(5.5)

Where

\( C_{AR-U} \) is the cost due to change of an AR as defined in 5.5.1.
\( m \) is the number of mobile nodes.
\( P_{MAP} \) is the frequency of location update due to a change in MAP.
\( Q_d \) is the cost of packet processing in the queue.
\( d_i \) is the distance in terms of number of hops from MAP to MAP.
\( E(z) \) is the unit cost per distance.
\( C_{MAP-U} \) is the cost of MAP update.
\( d_{HG} \) is the distance between HA and MAP.
\( E(w) \) is the unit cost.

5.5.3 The Simulation GUI

The software was designed in a way that allows the test to be carried out on different situations by allowing changes in any of the variables used in the mathematical model. The simulation also tests several configurations that might benefit from the implementation of the concept of incorporated domains. Figure 5.2 shows one of the
possible configurations for combining more than one domain under one MAP. The next parameter that should be entered to the simulation software is the path that the mobile node will follow. A proposed traveling path is shown in Figure 5.3 below.

The path and domains distribution shown below are of the ideal case where the majority of location updates are due to a change in ARs. However, the software was designed to test all types of configurations including the worst case scenario when every move in the path requires the location update to occur in the MAP level. Nevertheless, the real situations are not represented by these two extremes and thus we will consider cases where a mixture of both scenarios is applied.

![Figure 5.2 Possible configuration in the simulation software for incorporated domains](image-url)
The user is then prompted by the program to enter the costs which will be used in the calculations. These costs can be calculated based on the formulas stated in sections 5.5.1 and 5.5.2. The required variables and its assumed values are shown in Figure 5.4.

Figure 5.3 Entering the traveling path of the Mobile Node
These values shown in the cost variables are default assumptions which can be changed if required. Since the cost is measured in Bytes, the cost per distance was chosen to be 0.125 to represent one bit (1/8 of the byte) of cost. In Figure 5.5 the cost of location update due to change of AR is titled $C(\text{AR-U})$, the cost of location update due to change of MAP $C(\text{MAP-U})$ and the cost of location update due to updating the RCoA for the MN (HA $C(\text{LU})$) are calculated and used in later calculations. After the calculate button is pressed the cost fields are evaluated and the total cost is calculated for both the normal HMIPv6 as well as the new proposed incorporated domains application for HMIPv6 as shown in Figure 5.5. The figure shows a significant improvement in terms of cost reduction. For the path shown in Figure 5.3 the total cost for the current implementation is 1284 units while the incorporated domains...
The implementation of HMIPv6 is calculated to be 728 units which show a reduction of 43.3%.

![Location Update Cost](image)

Figure 5.5 Location Update Cost

### 5.6 PERFORMANCE OF LOCATION UPDATE IN INCORPORATED DOMAINS

To test that the improvement is persistent over a wider range of scenarios starting by varying the number of mobile nodes since an increase of the number of mobile nodes can lead to an increase in the cost which might affect the improvement percentage of the proposed system. The results showed that the percentage of improvement did not decrease in terms of the percentage of improvement when the number of mobile nodes increased. This is to be expected since the concept of incorporated domains is one of the possible applications of SSHMIPv6 which was designed in the first place to deal with the issue of scalability of the HMIPv6. The improvement trend can be noticed in the total costs shown in Figure 5.6. Furthermore, the improvement percentage and its relationship with the number of mobile nodes can be seen in Figure 5.7. This results show that the system showed significant cost reductions even with the increase of number of mobile nodes.
When the analysis is geared towards the relationship between the number of domains inside each incorporated domain and the location update cost reduction as a result of implementing incorporated domains as an application of SSHMIPv6, the results showed that a higher number of domains inside each incorporated domain is preferred and yields better results in terms of cost reduction. For instance, when the number of mobile nodes increased from 50 to 100 in Figure 5.6 and Figure 5.7 the
percentage of improvement decreased slightly from 44% to 43% and the total cost increased from 800 to 1200 bytes.

Figure 5.8 shows the relationship between the number of domains inside each incorporated domain and the total cost incurred as a result of location updates. It can be seen that the total cost starts to increase as the number of domains inside each incorporated domain decreases. This is to be expected since reducing the number of domains inside each incorporated domain increases the probability of the location update to be due to a change in the MAPs.

![Figure 5.8 Number of domains inside each incorporated domain versus Cost reduction](image)

The same is illustrated in Figure 5.9 in terms of percentage of cost reduction in location updates. It can be noticed that better cost reductions were achieved at higher numbers of domains per each incorporated domain.
In the worst case scenario of a path that moves from one incorporated domain to the next in every step of the movement path an example of which is provided in Figure 5.10, the incorporated domain implementation will provide no improvement in terms of cost reduction. However, this scenario is highly unlikely since the concept of incorporated domains revolves around assigning domains that statistically have showed rapid movement among themselves and assigning one incorporated domain to cater for theses domains. Nevertheless, even in this worst case scenario the cost performance of the incorporated domain implementation did not show any degradation in the cost incurred by the location update.
However, another possible scenario is one where the path is entirely inside one incorporated domain; in this case the savings encored as a result of the implementation of incorporated domains are much lesser than the normal HMIPv6. The case can be seen in Figure 5.11. A huge cost reduction of 65.91% was achieved be using the incorporated domains implementation of HMIPv6.
The actual scenario however, is not one of these two extremes previously mentioned but instead it is a combination of both. One where some of the steps involve movement of the Mobile Node between domains under different incorporated domains while others involve movement among domains under the same incorporated domain. In this case the improvement can be somewhere in between the improvement of the two extremes and is expected to be in the range of 30% to 66%.

5.7 SUMMARY

In this chapter we have introduced the concept of incorporated domains, which is an application of SSHMIPv6 that provides reductions in the cost of location update and provide better performance for the overall system. The mathematical model was referenced and the effects of implementing the proposed conceptual model on the mathematical model were analyzed. The cost reductions were measured by the development of new simulation software that relied on the mathematical models for the calculation of cost of location updates incurred by the system before and after the implementation of the concept of incorporated domains. The collected data were further analyzed and the relationship was established between the different parameters like number of Mobile Nodes and the nature of the path that the mobile node is following. When the number of mobile nodes increase the packets are distributed among the MAPs through the Join Shortest Queue (JSQ) algorithm as mentioned in SSHMIPv6. It is also worth mentioning that the topology of the network and the size of the domains are neglected in this study.

As mentioned earlier, other researchers have experimented with predicting the next movement of the MN in order to prevent connection loss during the hand-over from one domain to the next. However, this proposed concept of incorporated domains attempts to solve the issue from a different perspective by reducing the need for frequent Binding Updates (BU) since movement between the incorporated domains will be treated as if the movement was inside only one domain.
CHAPTER VI

CONCLUSION

6.1 INTRODUCTION

This thesis introduced the concept of Smart Selection Hierarchical Mobile Internet Protocol Version 6 (SSHMIPv6) to improve the HMIPv6 by using a cluster of MAPs using the same RCoA to allow for scalability and improved performance in terms of decreasing packets delivery delay, lost packets and lost packet ratio.

Incorporated domains were proposed in this thesis as an application of SSHMIPv6. Cost reductions in the cost of location update were shown and supported by performance improvement. Under this concept, adjacent domains are incorporated together while maintaining the same RCoA in their MAPs. Therefore, reduction was shown in LU signals if the MNs tend to move to adjacent domains most of the time.

The methodology followed by this thesis focused on the development of simulation software to test the validity of the conceptual model introduced by this thesis and to measure the improvement attained by applying mathematical models to the conceptual model developed.

It can be concluded that the proposed SSHMIPv6 was successfully able to solve the problem of scalability especially in cases whereby the domain carries excess mobile nodes or it carries more mobile nodes than its capacity. This was implemented through the successful implementation of the Join Shortest Queue (JSQ) selection algorithm. From the results, the developed simulator codes used to simulate HMIPv6 showed a better performance with the results of the SSHMIPv6 than with the HMIPv6 in terms of packet delay, lost packets and Goodput.
6.2 CONCLUSION

Using more MAPs leads to a reduction in packet transmission delay, less number of lost packets and less lost packet ratio. This is supported by the concrete findings stated in Chapter 5 including a reduction in average packets delivery delay of reduced almost by half when using two MAPs and reduced even more when using four MAPs. Moreover, reduction percentage in the number of lost packets was seen to reduce when using two MAPs and reduce even more when more MAPs were used in each domain.

If the average packet transmission delay is close to zero or if there is a slight different in the average packet transmission delay between the number of MAPs used then there is no need to increase the number of MAPs used in the domain. Furthermore, The SSHMIPv6 is suitable for any MAP quality and therefore the number of MAPs is dependent on the MAP process time, in the other words with less MAP process time the needed MAPs will be less. Similarly, by comparing HMIPv6 with SSHMIPv6 it was found that for several number of transferred packets will result in less packet transmission delay, less number of lost packets, less lost packet ratio and more Goodput.

Incorporated HMIPv6 is an application of SSHMIPv6 and therefore if the mobile node moves within the incorporated domains, there is no need to notify the HA and CNs about its new location because it keeps the same RCoA. It can therefore be concluded that the location update cost will be less as shown in the results. The results found by our simulation found that implementing incorporated domains can result in noticeable improvement. In the best scenario however, a substantial improvement was achieved by using the incorporated domains implementation of HMIPv6 in the case when every move of the MNs was inside one incorporated domain.

6.3 FUTURE WORK

This work did not consider the effect of hand-over latency on the performance improvement achieved by implementing SSHMIPv6. Future research could
experiment on the effects of implementing schemes such as the Fast Hand-Over Mobile Internet Protocol Version 6 (FHMIPv6) in a way that combines it with SSHMIPv6 and allows Mobility Anchor Points (MAPs) to predict the incoming Mobile Nodes (MN) and prepare for the location updates beforehand and study whether it will be beneficial to the entire system.

This thesis introduced the theoretical concept of SSHMIPv6 and tested its effectiveness and efficiency in improving the performance in terms of decreasing the packets latency using simulation software that was built based upon mathematical and conceptual models applied using hypothetical Internet networks. Future work could test the actual system in real situations by applying the concepts of SSHMIPv6 in real-world telecommunication infrastructures. Such a test could help in improving upon the achievements of this thesis.

This thesis established the theoretical and conceptual model of SSHMIPv6. After this conceptual model is tested in real-world scenarios the system could be further analyzed to determine the optimal number of clustered MAPs that could cater for the actual needs of real-world situations in terms of number of serviced MN and other realistic parameters. This needs to be done while keeping in mind that the cost of maintaining the cluster of MAPs should be kept minimal by finding the optimal number of MAPs needed to achieve the best performance.
REFERENCES


Fritsche, W. and Heissenhuber Florian, 2000, mobility support for the next generation Internet, white paper, IABG.


APPENDIX A

SIMULATION PROGRAM FLOW CHART
Display results

Data Rate = \( \frac{\text{numOfPkts} + \text{Area}(i).\text{LostPkts}}{\text{clock} / 1000000} \times \frac{64 \times 8 / 1024}{1024} \)

\[
\text{EDataRate} = \frac{\text{numOfPkts}}{\text{clock} / 1000000} \times \frac{64 \times 8 / 1024}{1024}
\]

\[
\text{TextMatrix}(1, i) = \text{Int}(\frac{\text{EDataRate} \times 1000}{1000})
\]

\[
\text{TextMatrix}(2, i) = \text{Int}(\frac{\text{DataRate} \times 1000}{1000})
\]

\[
\text{TextMatrix}(3, i) = \text{Int}(\frac{\text{DataRate} - \text{EDataRate} \times 1000000}{\text{DataRate} \times 1000000} \times 100\%)
\]

\[
\text{TextMatrix}(4, i) = \text{Round}(\frac{\text{numOfPkts} + \text{Area}(i).\text{LostPkts}}{\text{clock} / 1000000})
\]

\[
\text{TextMatrix}(5, i) = \text{Int}(\frac{\text{Area}(i).\text{Pktsdelay}}{\text{numOfPkts} \times 10000} \times 100\%)
\]

\[
\text{TextMatrix}(6, i) = \text{Round}(\frac{\text{Area}(i).\text{Pktsdelay} \times \text{numOfPkts}}{\text{clock} / 1000000})
\]

\[
\text{TextMatrix}(7, i) = \text{Int}(\frac{\text{Area}(i).\text{LostPkts} \times \text{numOfPkts}}{\text{numOfPkts} \times 10000} \times 100\%)
\]
APPENDIX B

DERIVATION FOR POISSON DISTRIBUTION

According to Bob Deserio’s Lab handout, a way of describing $\lambda$ is as a probability per unit time that an event will occur. That is

$$dP = \lambda dt \quad (B.1)$$

where $dP$ is the differential probability that an event will occur in the infinitesimal time interval $dt$. Of course, some care must be taken when translating a rate to a probability per unit time. For example, if $\lambda = 10/s$, it is obviously not true that the probability is 10 that an event will occur in any particular second. However, if that same rate is expressed $\lambda = 0.01/ms$ it is roughly true that the probability is 0.01 that an event will happen in any particular millisecond. Eq. B.1 only becomes exact in the limit of infinitesimal $dt$. It is approximately correct for any finite $\Delta t$.

$$\Delta P = \lambda \Delta t \quad (B.2)$$

to the extent that $\Delta P \ll 1$.

There are several possible derivations of the Poisson probability distribution. It is often derived as a limiting case of the binomial probability distribution. The derivation to follow relies on Eq. B.1 and begins by determining the probability $P(0; t)$ that there will be no events in some finite interval $t$. The first step is to break the interval from 0 to $t$ into $N$ intervals of equal length $\Delta t = t/N$. (The limit as $N \to \infty$ will be performed at the end.) The probability of an event in a small enough but finite interval $\Delta t$ will be given by Eq. B.2 and thus the probability of no event in this same interval is given by $1 - \lambda \Delta t$ For the full interval from 0 to $t$ to have no events, each and every one of the $N$ subintervals must have no events. Consequently, the probability of no events in a time $t$ is the product of the $N$ probabilities for no events in the subintervals.

$$P(0; t) = (1 - \lambda \Delta t)^N \quad (B.3)$$

Substituting $\Delta t = t/N$

$$P(0; t) = (1 - \lambda t/N)^N \quad (B.4)$$

Taking the limit $N \to \infty$ and recognizing that
\[ \lim_{N \to \infty} \left( 1 - \frac{x}{N} \right)^N = e^{-x} \quad (B.5) \]

gives
\[ P(0; t) = e^{-\lambda t} \quad (B.6) \]

Next, a relation is derived for the probability, denoted \( P(n + 1; t) \), for there to be \( n + 1 \) events in a time \( t \). It will be a recursion relation because it will be based on the probability \( P(n; t) \) of one less event. For there to be \( n + 1 \) events in \( t \), three independent events must happen in the following order (their probabilities given in parentheses).

- There must be \( n \) events up to some point \( t' \) in the interval from 0 to \( t \) (\( P(n, t') \) by definition)

- An event must occur in the infinitesimal interval from \( t' \) to \( t' + dt' \) (\( \lambda dt' \) by Eq. B.1).

- There must be no events in the interval from \( t' \) to \( t \) (\( P(0, t - t') \) by definition).

The probability of \( n + 1 \) events in the interval from 0 to \( t \) would be the product of the three probabilities above integrated over all \( t' \) from 0 to \( t \) to take into account that the last event may occur at any time in the interval. That is,
\[ P(n + 1; t) = \int_0^t P(n; t') \lambda dt' P(0; t - t') \quad (B.7) \]

From Eq. B.6 we already have \( P(0; t - t') = e^{-\lambda(t - t')} \) and with the following definition
\[ P(n; t) = e^{-\lambda t} \overline{P}(n; t) \quad (B.8) \]

substituted, Eq. 9 becomes (after canceling \( e^{\lambda t} \) from both sides):
\[ \overline{P}(n + 1; t) = \lambda \int_0^t \overline{P}(n; t') dt' \quad (B.9) \]

From Eqs. B.6 and 10, \( \overline{P}(0; t) = 1 \) and then \( \overline{P}(1; t) \) can be found from an application of Eq. B.9
\[ \overline{P}(1, t) = \lambda \int_0^t \overline{P}(0, t) dt = \lambda t \quad (B.10) \]

Applying Eq. B.9 for the next few terms … the pattern clearly emerges that
\[ \bar{P}(n; t) = \frac{(\lambda t)^n}{n!} \quad (B.11) \]

Thus with Eq. B.8, the Poisson probabilities result

\[ P(n; t) = e^{-\lambda t} \frac{(\lambda t)^n}{n!} \quad (B.12) \]

BobC - truncating and shortening BobD Using \( \mu = \lambda t \) as the “expected” number of events

\[ P(n) = e^{-\mu} \frac{\mu^n}{n!} \quad (B.13) \]

BobD also derives that

\[ \langle n \rangle = \sum_{n=0}^{\infty} nP(n) = \mu \quad (B.14) \]

And

\[ \langle n^2 \rangle = \sum_{n=0}^{\infty} n^2P(n) = \mu^2 + \mu \quad (B.15) \]

Leading to

\[ \sigma^2 = \left( \langle n - \mu \rangle^2 \right) = \left( \langle n^2 \rangle - \mu^2 \right) = \mu \quad (B.16) \]
APPENDIX C

RESULTS DATA

Table C.1 shows the Average Delay for diff. Number of transferred Packets for diff. Number of MAPs at each Area

<table>
<thead>
<tr>
<th>No. of trans. Pack</th>
<th>1242020</th>
<th>1380960</th>
<th>1461880</th>
<th>1519820</th>
<th>1557260</th>
<th>1599300</th>
<th>1625000</th>
<th>1663160</th>
<th>1688680</th>
<th>1698440</th>
</tr>
</thead>
<tbody>
<tr>
<td>No. of MAPs</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>219.9</td>
<td>220.3</td>
<td>220.5</td>
<td>220.6</td>
<td>220.67</td>
<td>220.8</td>
<td>220.9</td>
<td>220.9</td>
<td>220.9</td>
<td>221</td>
</tr>
<tr>
<td>2</td>
<td>106.6</td>
<td>107.3</td>
<td>107</td>
<td>107.6</td>
<td>107.5</td>
<td>107.4</td>
<td>107.9</td>
<td>108.2</td>
<td>108</td>
<td>108.4</td>
</tr>
<tr>
<td>3</td>
<td>63.7</td>
<td>66.8</td>
<td>67.6</td>
<td>68.9</td>
<td>69.2</td>
<td>69</td>
<td>68.6</td>
<td>69</td>
<td>69.2</td>
<td>69.5</td>
</tr>
<tr>
<td>4</td>
<td>15.7</td>
<td>31.5</td>
<td>39</td>
<td>42.76</td>
<td>44.4</td>
<td>46.2</td>
<td>46.6</td>
<td>47.5</td>
<td>47.9</td>
<td>47.9</td>
</tr>
<tr>
<td>5</td>
<td>2.3</td>
<td>4.6</td>
<td>7.3</td>
<td>10.1</td>
<td>12.7</td>
<td>15.3</td>
<td>17.7</td>
<td>20</td>
<td>21.7</td>
<td>23.1</td>
</tr>
</tbody>
</table>

Table C.2 shows the Number of Lost Packets for diff. Number of transferred Packets for diff. Number of MAPs at each Area

<table>
<thead>
<tr>
<th>No. of trans. Pack</th>
<th>1242020</th>
<th>1380960</th>
<th>1461880</th>
<th>1519820</th>
<th>1557260</th>
<th>1599300</th>
<th>1625000</th>
<th>1663160</th>
<th>1688680</th>
<th>1698440</th>
</tr>
</thead>
<tbody>
<tr>
<td>No. of MAPs</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>907880</td>
<td>1052680</td>
<td>1121860</td>
<td>1182940</td>
<td>1233160</td>
<td>1269520</td>
<td>1294540</td>
<td>1333360</td>
<td>1337380</td>
<td>1363600</td>
</tr>
<tr>
<td>2</td>
<td>574600</td>
<td>719360</td>
<td>788580</td>
<td>849620</td>
<td>899860</td>
<td>936220</td>
<td>961240</td>
<td>1000080</td>
<td>1004060</td>
<td>1030320</td>
</tr>
<tr>
<td>3</td>
<td>240880</td>
<td>379720</td>
<td>463000</td>
<td>519340</td>
<td>564900</td>
<td>597200</td>
<td>629780</td>
<td>651800</td>
<td>669320</td>
<td>697280</td>
</tr>
<tr>
<td>4</td>
<td>9940</td>
<td>64800</td>
<td>132980</td>
<td>176360</td>
<td>233020</td>
<td>266800</td>
<td>299280</td>
<td>320160</td>
<td>348240</td>
<td>364200</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>180</td>
<td>1820</td>
<td>8200</td>
<td>12640</td>
<td>20380</td>
<td>35600</td>
<td>42000</td>
<td>55060</td>
<td>61160</td>
</tr>
</tbody>
</table>

Table C.3 shows the Ratio of Lost Packets for diff. Number of transferred Packets for diff. Number of MAPs at each Area

<table>
<thead>
<tr>
<th>No. of trans. Pack</th>
<th>1242020</th>
<th>1380960</th>
<th>1461880</th>
<th>1519820</th>
<th>1557260</th>
<th>1599300</th>
<th>1625000</th>
<th>1663160</th>
<th>1688680</th>
<th>1698440</th>
</tr>
</thead>
<tbody>
<tr>
<td>No. of MAPs</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>73.1</td>
<td>75.9</td>
<td>77</td>
<td>77.9</td>
<td>78.6</td>
<td>79.1</td>
<td>79.5</td>
<td>79.9</td>
<td>80</td>
<td>80.3</td>
</tr>
<tr>
<td>2</td>
<td>46.2</td>
<td>51.8</td>
<td>54.1</td>
<td>56</td>
<td>57.4</td>
<td>58.4</td>
<td>59</td>
<td>60</td>
<td>60</td>
<td>60.7</td>
</tr>
<tr>
<td>3</td>
<td>19.4</td>
<td>27.5</td>
<td>31.6</td>
<td>34.2</td>
<td>36.1</td>
<td>37.4</td>
<td>38.6</td>
<td>39.4</td>
<td>40.1</td>
<td>41</td>
</tr>
<tr>
<td>4</td>
<td>0.8</td>
<td>4.7</td>
<td>9.1</td>
<td>11.7</td>
<td>14.9</td>
<td>16.8</td>
<td>18.3</td>
<td>19.3</td>
<td>20.7</td>
<td>21.4</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>0</td>
<td>0.1</td>
<td>0.5</td>
<td>0.8</td>
<td>1.3</td>
<td>2.2</td>
<td>2.5</td>
<td>3.3</td>
<td>3.6</td>
</tr>
</tbody>
</table>
Table C.4 shows the Average Packet Delay for different Packet processing Time for different Number of Maps at each Area

<table>
<thead>
<tr>
<th>Pack. Process time</th>
<th>12 ms</th>
<th>16 ms</th>
<th>20 ms</th>
<th>24 ms</th>
<th>28 ms</th>
<th>32 ms</th>
</tr>
</thead>
<tbody>
<tr>
<td>No. of MAPs</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>176.17</td>
<td>235.93</td>
<td>295.61</td>
<td>355.11</td>
<td>414.58</td>
<td>474.02</td>
</tr>
<tr>
<td>2</td>
<td>85.44</td>
<td>115.67</td>
<td>145.71</td>
<td>175.62</td>
<td>205.11</td>
<td>235.33</td>
</tr>
<tr>
<td>3</td>
<td>53.35</td>
<td>74.84</td>
<td>94.96</td>
<td>114.69</td>
<td>134.83</td>
<td>155.19</td>
</tr>
<tr>
<td>4</td>
<td>23.69</td>
<td>52.60</td>
<td>69.37</td>
<td>84.34</td>
<td>98.90</td>
<td>114.68</td>
</tr>
<tr>
<td>5</td>
<td>3.47</td>
<td>32.62</td>
<td>52.41</td>
<td>65.53</td>
<td>78.25</td>
<td>89.74</td>
</tr>
<tr>
<td>6</td>
<td>0.90</td>
<td>8.27</td>
<td>37.59</td>
<td>52.14</td>
<td>63.52</td>
<td>73.79</td>
</tr>
<tr>
<td>7</td>
<td>0.00</td>
<td>2.02</td>
<td>15.74</td>
<td>40.14</td>
<td>51.64</td>
<td>61.43</td>
</tr>
<tr>
<td>8</td>
<td>0.00</td>
<td>0.70</td>
<td>4.36</td>
<td>22.73</td>
<td>41.92</td>
<td>51.79</td>
</tr>
<tr>
<td>9</td>
<td>0.00</td>
<td>0.00</td>
<td>1.45</td>
<td>7.89</td>
<td>28.05</td>
<td>43.06</td>
</tr>
<tr>
<td>10</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>2.51</td>
<td>12.58</td>
<td>31.99</td>
</tr>
</tbody>
</table>

Table C.5 shows the Average Packet Delay for different Packet processing Time for different Number of Maps at each Area

<table>
<thead>
<tr>
<th>Pack. Process time</th>
<th>12 ms</th>
<th>16 ms</th>
<th>20 ms</th>
<th>24 ms</th>
<th>28 ms</th>
<th>32 ms</th>
</tr>
</thead>
<tbody>
<tr>
<td>No. of MAPs</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>1282840</td>
<td>1385620</td>
<td>1448220</td>
<td>1487940</td>
<td>1526000</td>
<td>1543860</td>
</tr>
<tr>
<td>2</td>
<td>866220</td>
<td>1073140</td>
<td>1198240</td>
<td>1279600</td>
<td>1347400</td>
<td>1387580</td>
</tr>
<tr>
<td>3</td>
<td>456620</td>
<td>761200</td>
<td>952820</td>
<td>1075220</td>
<td>1164580</td>
<td>1237200</td>
</tr>
<tr>
<td>4</td>
<td>396220</td>
<td>451220</td>
<td>695000</td>
<td>872600</td>
<td>988340</td>
<td>1078320</td>
</tr>
<tr>
<td>5</td>
<td>280</td>
<td>449260</td>
<td>447620</td>
<td>653420</td>
<td>809900</td>
<td>922740</td>
</tr>
<tr>
<td>6</td>
<td>0</td>
<td>4580</td>
<td>206400</td>
<td>445020</td>
<td>630880</td>
<td>765720</td>
</tr>
<tr>
<td>7</td>
<td>0</td>
<td>100</td>
<td>29040</td>
<td>238560</td>
<td>452920</td>
<td>613740</td>
</tr>
<tr>
<td>8</td>
<td>0</td>
<td>0</td>
<td>20</td>
<td>5900</td>
<td>107980</td>
<td>294340</td>
</tr>
<tr>
<td>9</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>120</td>
<td>20120</td>
<td>148180</td>
</tr>
<tr>
<td>10</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Table C.6 shows the Ratio of Lost Packets for different Packet processing Time for different Number of Maps at each Area

<table>
<thead>
<tr>
<th>Pack. Process time</th>
<th>12 ms</th>
<th>16 ms</th>
<th>20 ms</th>
<th>24 ms</th>
<th>28 ms</th>
<th>32 ms</th>
</tr>
</thead>
<tbody>
<tr>
<td>No. of MAPs</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>75.42</td>
<td>81.53</td>
<td>85.20</td>
<td>87.64</td>
<td>89.44</td>
<td>90.73</td>
</tr>
<tr>
<td>2</td>
<td>50.92</td>
<td>63.14</td>
<td>70.50</td>
<td>75.37</td>
<td>78.98</td>
<td>81.54</td>
</tr>
<tr>
<td>3</td>
<td>26.74</td>
<td>44.77</td>
<td>55.91</td>
<td>63.18</td>
<td>68.43</td>
<td>72.45</td>
</tr>
<tr>
<td>4</td>
<td>4.10</td>
<td>26.30</td>
<td>40.97</td>
<td>51.11</td>
<td>57.94</td>
<td>63.25</td>
</tr>
<tr>
<td>5</td>
<td>0.02</td>
<td>8.75</td>
<td>26.35</td>
<td>38.52</td>
<td>47.52</td>
<td>54.10</td>
</tr>
<tr>
<td>6</td>
<td>0.00</td>
<td>0.27</td>
<td>12.10</td>
<td>26.24</td>
<td>37.03</td>
<td>44.91</td>
</tr>
<tr>
<td>7</td>
<td>0.00</td>
<td>0.01</td>
<td>1.70</td>
<td>14.06</td>
<td>26.58</td>
<td>35.91</td>
</tr>
<tr>
<td>8</td>
<td>0.00</td>
<td>0.00</td>
<td>0.06</td>
<td>3.88</td>
<td>16.08</td>
<td>26.42</td>
</tr>
<tr>
<td>9</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.35</td>
<td>6.35</td>
<td>17.30</td>
</tr>
<tr>
<td>10</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.01</td>
<td>1.18</td>
<td>8.70</td>
</tr>
<tr>
<td>Pack. Process time</td>
<td>12 ms</td>
<td>16 ms</td>
<td>20 ms</td>
<td>24 ms</td>
<td>28 ms</td>
<td>32 ms</td>
</tr>
<tr>
<td>-------------------</td>
<td>-------</td>
<td>-------</td>
<td>-------</td>
<td>-------</td>
<td>-------</td>
<td>-------</td>
</tr>
<tr>
<td><strong>No. of MAPs</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>203.46</td>
<td>152.59</td>
<td>122.07</td>
<td>101.75</td>
<td>87.21</td>
<td>76.32</td>
</tr>
<tr>
<td>2</td>
<td>406.90</td>
<td>305.17</td>
<td>244.14</td>
<td>203.49</td>
<td>174.41</td>
<td>152.64</td>
</tr>
<tr>
<td>3</td>
<td>610.34</td>
<td>457.76</td>
<td>366.21</td>
<td>305.23</td>
<td>261.62</td>
<td>228.96</td>
</tr>
<tr>
<td>4</td>
<td>798.92</td>
<td>610.33</td>
<td>488.28</td>
<td>406.98</td>
<td>348.83</td>
<td>305.27</td>
</tr>
<tr>
<td>5</td>
<td>829.98</td>
<td>759.45</td>
<td>610.32</td>
<td>508.65</td>
<td>436.00</td>
<td>381.59</td>
</tr>
<tr>
<td>6</td>
<td>831.22</td>
<td>827.38</td>
<td>731.46</td>
<td>610.38</td>
<td>523.20</td>
<td>457.87</td>
</tr>
<tr>
<td>7</td>
<td>0.00</td>
<td>831.64</td>
<td>817.90</td>
<td>711.42</td>
<td>610.37</td>
<td>534.17</td>
</tr>
<tr>
<td>8</td>
<td>0.00</td>
<td>832.00</td>
<td>829.18</td>
<td>799.48</td>
<td>697.12</td>
<td>610.38</td>
</tr>
<tr>
<td>9</td>
<td>0.00</td>
<td>0.00</td>
<td>829.97</td>
<td>830.17</td>
<td>777.21</td>
<td>686.55</td>
</tr>
<tr>
<td>10</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>832.00</td>
<td>824.27</td>
<td>758.86</td>
</tr>
</tbody>
</table>
APPENDIX D

LIST OF PUBLICATIONS


Ma’en T. Alrashdan, Mahamoud Ismael, Kasmiran Jumari, “Location Update Cost Improvement over Incorporated Domains in Hierarchical Mobile IPv6”, ICSRS, Accepted.