A Study on Mobile IP Handoff Management for Seamless Mobility

A thesis submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy

Basav Roy Choudhury
Regd. No. 005 of 2006

School of Engineering
Department of Computer Science & Engineering
Tezpur University

November, 2006

Abstract

This thesis discusses two schemes to enhance the usability of Mobile IPv6 (MIPv6) in an all-IP network scenario by reducing handover latency and binding update/registration traffic. While high handover latency affects the seamlessness in mobility, excessive binding update/registration traffic negatively influences MIPv6 scalability. The two schemes presented here are:

- *Mobile IPv6 with Mobile Agent Assisted Handover* (MAAH Scheme), and
- *Transparent Multihomed Mobile IPv6* (TMMIPv6 Scheme).

The MAAH Scheme uses mobile agents to speed up the registration process and reduce associated handover delay, when a mobile node travels from one network to a different one. The mobile agents in this scheme are envisaged to:

- proxy for the mobile node's home agent at the foreign networks,
- assist in registering the Care-of Addresses (CoAs),
- assist in return routability procedure to set up authorization key for correspondent binding to achieve route optimization,
- prevent packet drop during handover by redirecting the packets in transit to the new CoA, and
- collect information about network usage for billing, etc.

The use of the mobile agent in this scheme will result in the following benefits:

- reduced handover latency,
- reduced network traffic load in terms of number of packet hops, and
- increased robustness of the protocol due to reduced dependence on the home agent.

This thesis lays out the MAAH protocol details, with necessary modifications to the base protocol. In addition, simulation experiments have been performed to arrive at a coarse estimate of the handover latency reduction using the aforesaid scheme. The simulation experiments were performed on two topologies, considering various movement scenarios for the mobile node. The results of these experiments, though highly topology dependent, show an average reduction of up to 59% in time consumed for registration renewals in MAAH scheme, as compared to that for the base protocol.

In contrast to MAAH scheme – which considers single interfaced node, the TMMIPv6 proposes protocol enhancement to support node multihoming and bandwidth augmentation through simultaneous use of multiple node interfaces. This scheme envisages to:

- provide seamless mobility through horizontal and/or vertical handover, leading to ubiquitous Internet access,
- improve performance through bandwidth aggregation in scenarios where simultaneous use of multiple interfaces is possible,
- dynamically distribute traffic across the available interfaces in proportions commensurate to current network conditions,
- increase robustness of the base protocol by making it less dependent on a single home agent.

The above mentioned goals are proposed to be achieved transparently, without any change to the existing infrastructure, except at the communication endpoints by introducing a *Convergence Module* (*CM*) at layer 3 of the protocol stack. .

Another feature of the proposed TMMIPv6 scheme is the possibility for multiple Home Addresses (HoAs). To reap the full benefit of simultaneous use of multiple interfaces, the MN should be accessible through more than one HoA. However, in presence of several HoAs, these can no longer function as MN identifier at the home agent or at CN's binding cache. The concept of Primary HoA (PHoA) is therefore introduced, which being an IP address, is unique over the Internet. In the face of multiple HoAs, the TCP connection will now be maintained for the given flow with the help of this single static PHoA.

Simulation experiments were carried out using NS2 to study the TCP performance for mobile node equipped with two interfaces. These experiments indicate that the benefit due to multiple interfaces can be appreciable if the interfaces under consideration support distinct, rather than the same wireless access technologies. Simulations for multi-interfaced node, with two interfaces, showed up to 95% increase in throughput, as compared to the single interfaced node. While it is evident that a multi-interfaced node will have a higher throughput; the main advantage of these nodes, as borne out by the simulation experiments, was the absence of discontinuity in packet transfer during handovers, resulting in seamless mobility.

The performance improvement in micro-mobility protocols like HMIPv6, or in the proposed scheme TMMIPv6 scheme, when either is made to collaborate with MAAH scheme, is also discussed. Apart from performance improvement for HMIPv6 through this collaboration, the authentication of control messages can also be handled by mobile agents of MAAH scheme. In case of TMMIPv6, the performance enhancement resulting from this cooperation is attributed to an increased availability of mobile node interfaces.

This thesis furthermore presents the formats for new control messages that will be required to support the proposed alterations in the base protocol. In addition, it discusses the minor modifications required in the format and handling of some existing control messages.

TEZPUR UNIVERSITY

This is to certify that the thesis entitled **A Study on Mobile IP Handoff Management for Seamless Mobility** submitted to the Tezpur University in the Department of Computer Science & Engineering under the School of Engineering in partial fulfillment for the award of the degree of Doctor of Philosophy in Computer Science is a record of research work carried out by Mr. Basav Roy Choudhury under my personal supervision and guidance.

All helps received by him from various sources have been duly acknowledged.

No part of this thesis has been reproduced elsewhere for award of any other degree.

27th November, 2006
Tezpur

Professor Dilip K Saikia
Department of Computer Sc. & Engineering
School of Engineering

TEZPUR UNIVERSITY

This is to certify that the thesis entitled **A Study on Mobile IP Handoff Management for Seamless Mobility** submitted by Mr. Basav Roy Choudhury to Tezpur University in the Department of Computer Science & Engineering under the School of Engineering in partial fulfillment of the requirement for the award of the degree of Doctor of Philosophy in Computer Science has been examined by us on ________________ and found to be satisfactory.

The Committee recommends for the award of the degree of Doctor of Philosophy.

Signature of

Prof. Dilip K Saikia
Principal Supervisor

External Examiner

Date : _____________

Acknowledgement

I take this opportunity to convey my sincerest gratitude to my guide Professor Dilip K Saikia, Department of Computer Science and Engineering, Tezpur University, Tezpur. This thesis has seen the light of day due to his constant inspiration and guidance. In addition to the technical guidance, I would like to thank him for having patience with me when the going was tough, and for being there for me whenever I needed him.

In addition, I would like to express my gratitude to Prof. M. Dutta, Prof. R. K. Das, Prof. D. K. Bhattacharyya, Dr. S K Sinha and Shri N Sarma of the Department of Computer Science and Engineering for their thought provoking questions, their constructive criticisms and their valuable assistance at different stages of my work. I hereby put on record my thanks to other faculty members of the department for their important advice from time to time. I would also like to express my deep appreciation for Shri Ajay Sharma, who helped me with the laboratories whenever the need arose.

There have been worthwhile contributions from my wife Probidita Roychoudhury, who had lend her hand in many ways, including helping in debugging the codes for simulations presented in this thesis. I would like to earnestly thank her for all that.

I would also like to put on record the help that I had received from Ms Jonalee Sarma and Shri Anjan Das for enrolling myself in this program.

Thanks are due to my colleagues at the Department of Computer Science, St. Anthony's College, Shillong for their encouragement and for sharing my load when I had to be away from Shillong for my research work. Their generosity is deeply appreciated.

Last, but not the least, I would like to thank all others who have helped me in this venture.

Basav Roy Choudhury

Contents

Chapter 1

Chapter 2

Chapter 3

Chapter 4

Chapter 5

Chapter 6

Chapter 7

Glossary

List of Figures

List of Abbreviations

3G	Third Generation
4G	Fourth Generation
AR	Access Router
ATM	Asynchronous Transfer Mode
BID	Binding unique Identification
BU	Binding Update
CDMA	Code Division Multiple Access
CIP	Cellular Internet Protocol
CM	Convergence Module
CN	Correspondent Node
CoA	Care-of Address
cSCTP	Cellular Stream Control Transmission Protocol
FBU	Fast Binding Update
FNA	Fast Neighbour Advertisement
GGSN	General GPRS Support Node
GPRS	General Packet Radio Service
GTP	GPRS Tunneling Protocol
HA	Home Agent
HAWAII	Handoff Aware Wireless Access Internet Infrastructure
HMIPv6	Hierarchical Mobile Internet Protocol version 6
HoA	Home Address

IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
LAN	Local Area Network
LCoA	Local Care-of Address
LEO	Low Earth Orbit
MA	Mobile Agent
MAAH	Mobile Agent Assisted Handover
MAP	Mobility Anchor Point
MIP	Mobile Internet Protocol
MIPv4	Mobile Internet Protocol version 4
MIPv6	Mobile Internet Protocol version 6
MMI	Mobile IPv6 for Multiple Interfaces
MN	Mobile Node
monami6	Mobile Nodes and Multiple Interfaces in IPv6
MP	Mobile Agent Platform
m-SCTP	Mobile Stream Control Transmission Protocol
NCoA	New Care-of Address
NG	Next Generation
NGWS	Next Generation
NGWS	Next Generation Wireless System
PCoA	Primary Care-of Address
PCoA	Previous Care-of Address
PHoA	Primary Home Address
PLMN	Public Land Mobile Network

RCoA	Regional Care-of Address
RFC	Request For Comments
RRP	Return Routability Procedure
SCTP	Stream Control Transmission Protocol
SGSN	Serving GPRS Support Node
TCP	Transmission Control Protocol
TMMIPv6	Transparent Multihomed Mobile Internet Protocol version 6
TraSH	Transport layer Seamless Handover
UMTS	Universal Mobile Telecommunications System
VoIP	Voice Over Internet Protocol
WATM	Wireless Asynchronous Transfer Mode
WLAN	Wireless Local Area Network

Chapter 1

Introduction

1.1. Mobility

Advances in the fields of radio technologies and micro devices over the past couple of decades have led to a boom in wireless networking. This has resulted in dramatic changes in telecommunication. With every passing day, there is addition in the number of people accessing wireless networks. One very important factor behind this increasing popularity of wireless networks is mobility. Wireless technology allows physical movement of the user while remaining connected, ideally, without disruption in the communication. So much is the impact of mobility using wireless networks that these two terms – mobility and wireless networks – have become synonymous with each other. Cellular mobile telephone network is perhaps the most prominent examples of such wireless networks, even though Wireless LANs and Bluetooth are not lagging far behind. Over the past decade or so, mobile phones have moved from the position of luxury item to become an essential commodity. The wireless LANs are becoming commonly available in academic campuses as well as other organizations. Devices of wide variety are coming to the market enabled with Bluetooth technology.

At the same time, the Internet has seen a meteoric rise in popularity as a consequence of increasing interest in the World Wide Web [1] and the other Internet services. An increasing number of applications are being added over the Internet every passing day. These applications spread across wide spectrum – thereby transforming the Internet into a utility necessary for everyday life. This has brought in a newer requirement – the need to be connected to the Internet – anytime, anywhere.

This need for anytime anywhere connectivity has led researchers towards evolving a ubiquitous communication network. Ubiquitous computing aims to "enhance computer use by making many computers available throughout the physical environment, but making them effectively invisible to the user" [2]. While the idea of a globally omnipresent computing infrastructure may sound utopian, it is widely anticipated that future mobile users will have near ubiquitous access to high bandwidth wireless communications [3]. Development of protocol architectures supporting mobile terminals are, in a way, laying the foundation for such ubiquitous availability of modern communication services for personal computing devices. Presently, there exist various wireless technologies and networks that address the different needs and requirements of mobile users. For high-data-rate local-area-access, Wireless LANs (WLANs) are a satisfactory solution. For wide-area communications, traditional and next-generation (NG) cellular networks may provide voice and data services. For worldwide coverage, satellite networks have been used extensively in military and commercial applications. These different wireless networks are complementary to each other. While a particular locality might be covered under WLAN, connecting such localities may be possible through cellular network support, and connecting to remote areas may be possible only through satellite networks. Though there may be more than one network covering a given region, no single wireless access technology support may be available covering an entire region. Thus, the integration of various access technologies will be necessary to empower the mobile users to remain connected to the system from anywhere and using access networks that suit their needs the best [4].

The challenge in moving from a wireline network to a wireless network supporting mobile terminals is, of course, the mobility management [5]. This involves locating the mobile terminal and delivering the packets meant for the same. This also includes maintaining the connection as the mobile terminal moves from one location to another. This mobility management involves two components:

- *location management*, and
- *handoff management*.

Location management is the process by which the network keeps track of the mobile terminal. First step towards this is location registration (or update). By this the mobile terminal keeps the network informed about its current location from time to time. The other step is call delivery – that is, delivering a packet meant for the mobile terminal. At times, the exact location of the mobile terminal may not be precisely known. Due to this, the call delivery may involve querying the network for the current point of attachment of the mobile terminal and may also include paging a given area of the network for the same. This process involves messages to and from the mobile terminal, and may eat up valuable bandwidth of the wireless network. Moreover, these signaling may introduce delays and may adversely affect the user experience, especially if the network has to support a large number of mobile terminals.

The other component of mobility management is the handoff management. This involves the scheme of handling an on going connection as the mobile terminal changes its point of attachment to the network, which may be due to terminal mobility or may be to reduce load on a given network path. The process requires initiating the handover procedure either by the mobile terminal or by a mobility manager when a need for the same is recognized. For this the first step is the identification of a new point of attachment to the network for the mobile terminal. Then a new network path is set up between the mobile terminal and the correspondent node via the new point of attachment. The new path consumes a new set of resources of the network.. The on going communication is then handed over to the new network path and the resources used by the earlier path are released. The handoff can either be soft or hard. In the former case, the old resources are not released before the connection is setup using the newer resources. Thus, the mobile terminal, at a certain intermediate point in time, may actually be consuming the old as well as the new resources simultaneously. This is possible if the mobile terminal is connected to two base stations – new and old – at the same time. This ensures that the on going communication is not disrupted in the entire process. The other case is the hard handoff, in which the terminal subscribes to the service of at most one base station at a time. Thus the terminal releases the services of the old base station before (or just after) it connects to a new one. This may result in a disruption of the ongoing communication.

The mobility management scheme should ideally be such that it can provide seamless communication in spite of the mobility. Seamless communication requires the ability of the mobile equipment to successively or simultaneously attach to different access points in the network infrastructure in a way that makes the physical movement transparent and preserves application-level connectivity unaltered [6].

1.2. IP and its significance in node mobility

With Internet connectivity becoming important for day to day activities, anytime anywhere Internet connectivity is no longer a luxury, but is fast becoming a necessity. One of the motivations that is fuelling the rapid growth of mobile wireless networks is the Internet.

The Internet has come a long way from its early ARPANET days. ARPANET was started with four sites. Today, the Internet consists of thousands separate heterogeneous networks that are interconnected to provide interconnectivity to millions of nodes spread all over the globe. Data are transmitted in packets from a source system to a destination across a path that may typically involve many networks connected by routers. The operation is usually connectionless. A router accepts datagrams and relays them on toward the destination. The routers are responsible for determining the path to be followed by these datagrams [7]. The growth and the evolution of the Internet continue, and so does its heterogeneity in the access networks.

Whether wireless or wireline network, whether mobile or stationary hosts – the communication amongst the entities must be taken care of by certain protocols. The presence of various heterogeneous access networks implies the use of diverse protocols. The heterogeneity is not a passing phase. A variety of networks – and therefore their associated protocols – will always be around, even in the distant future [8]. The installed base of different networks is large involving enormous amount of investment, and hence cannot be replaced by a homogenous alternative. Diverse networks have very different technologies, and thereby necessitate separate protocols. While there are these diverse protocols at various sub-network layers, an interconnection of these networks is imperative for the Internet to be possible. The glue that holds this whole Internet together is the network layer protocol – Internet Protocol (IP). This is a protocol that was designed with the internetworking in mind from the very beginning. IP treats all networks equally – whether it is a local area network like an Ethernet, or a wide area network used as a backbone, or whether it's a point-to-point link between two computers [9].

Over the years, IP has become *the* protocol to unify the networks with heterogeneous access technologies. However, IP was developed with the consideration that the terminals are stationary. Its design did not factor in the possibility for terminal mobility.

In the terminal mobility front, the unparalleled success of cellular wireless network infrastructure has led to the omnipresence of mobile phones. However, with market saturation, the average revenue per user for current generation of cellular wireless services has been dropping rapidly [10]. The battle for the market share has resulted in the demand for higher levels of competitiveness. Reducing cost of operation and achieving higher efficiency in utilization of the resources are therefore imperative for today's cellular service providers.

With the advent of Voice over IP (VoIP), it has become possible to have voice communication over the Internet at lower costs. The IP is potentially more efficient in resource utilization [11] as it follows packet-switching in contrast to circuit-switching used in the current generation of cellular telecom networks. With IP, it is also possible to add new services quickly, and with little additional cost. In addition, IP allows adaptation of new access technologies easily and quickly, thereby providing a competitive edge. The Internet, therefore, has become a competitor for the telecom sector. The best way to beat the competition arising out of the Internet is to become a part of the Internet itself. While initial cellular telecom networks did not include IP, embracing IP to become a part of the Internet is now a compulsion in order to achieve and retain the necessary competitiveness.

The objective of the "all-IP"[12] network in the telecom domain is multi-pronged. On one hand, it allows convergence of voice and data resulting in considerable cost saving. Additionally, it allows integration of land-line and cellular telecom networks seamlessly [13]. Further, use of IP also makes the integration of the telecom networks with the Internet automatic [14].

The 3G [15] standardization effort is defining this "all-IP" multimedia subsystem as a separate extension to the existing networks [16], that is, the implementation of IP has been on the top of existing transport networks. The existing transport networks are still circuit switched, limiting the overall cost efficacy of packet switched IP. For example, in both CDMA2000 and UMTS networks, a data session is established to carry IP packets between the network access server and the mobile terminal [17]. Both networks use tunnels to support mobility. In CDMA2000, the tunnel is between the network access server and the base station controller, while in UMTS the tunnel from the network access server is routed through a tunnel switch.

A better option would be to adopt an integrated packet switched approach, instead of having IP function over the existing circuit switched networks. Apart from cost reduction due to packet switching, a native IP architecture will support all the functionality of IP throughout the network. Caching can be employed at any point within the network, but particularly within the access network where it can significantly reduce load and latency. Multicast can be used throughout the network to support multimedia services and conserve bandwidth [18] [19]. A tunneling solution for mobility hides the packet headers, and makes caching and IP multicast difficult to implement within the access network of CDMA2000 or anywhere within UMTS. Moreover, in a native IP architecture, routing to local resources is efficient. Packets do not have to travel to the core of the network and back again just to reach another mobile within the same cell, as required in UMTS. Integration with wireless LAN will be simple, because they use exactly the same architecture.

To sum up, an all-IP network architecture can result in the following benefits:

- seamless services through IP, regardless of underlying access technologies,
- efficient solutions for simultaneous multimedia services including voice, data and advanced real time services [20],
- cost saving due to efficient network resource utilization through packet switching.

This realization has resulted in a drive towards building IP into the transport network of the Next Generation of telecom networks. Future telecom infrastructures will therefore consist of a set of heterogeneous networks using IP as the common protocol [21][22]. Towards this, researchers are currently developing frameworks [23] for future fourth-generation (4G) networks. 4G networks are all-IP based heterogeneous networks that allow the use of any system – anytime and anywhere.

From the above discussion it is clear that IP is going to play an even bigger and unifying role in the entire arena of communication. While the importance and usefulness of IP is accepted for both wireline and wireless networks, the IP in its native form does not support node mobility. To fill this shortcoming, Mobile IP was proposed to take care of mobility management.

1.3. Mobile IP and its Limitations

There have been discussions as to which layer should take up the responsibility of mobility management. There has been arguments for and against in case of almost every layer. While link layer support is mandatory in any case [24], it can do very little to either preserve higher layer connections or provide location management when movement is across administrative domains. There may be several transport layer connections active at a node at any given instant. A mobility management scheme at this layer would therefore involve managing all these connections individually. Since the main focus behind mobility management is routing, it should be managed at network layer – the layer typically involved with the job of packet routing.

Internet uses IP as its long time trusted protocol at layer 3. However, as mentioned in the section above, neither IPv4 nor IPv6 natively supports host mobility. In the current scenario, the node mobility at layer 3 is managed by Mobile IP (MIP). With the dominance of mobile wireless networks, an efficient Mobile IP network is essential to support this node mobility, especially if IP has to be built into the core of the Next Generation telecommunication network.

In an all-IP mobile network architecture, the problem of mobility management must be solved at the IP layer – the layer responsible for routing packets. In contrast, the 3G mobile architecture solves the problem of mobility in layer 2 [22]. For example in UMTS [25], packets are forwarded from the core network to the mobile host by setting up GPRS Tunneling Protocol (GTP) from the Gateway GPRS Support Node (GGSN) to the mobile host. The Serving GPRS Support Node (SGSN) handles inter-radio network controller (RNC) mobility, and the GGSN manages inter-SGSN mobility. The changeovers take place in the sub-network layer (L2), and works fine until the mobile host leaves the UMTS network. The problem arises when the host has to move out into a new (CDMA2000, say) network [26].

Unlike the 3G architecture, if mobility is solved in the IP layer, routers will have access to the packet header. This would allow the routers to implement IP-based QoS algorithms. IP/ATM network has already shown the complexity that result from attempting to translate quality of service requirements from one network to another [22]. To put an additional argument in favor of mobility management at IP layer – the authors in [14] had considered both Mobile IP and Session Initiation Protocols to manage mobility for VoIP services in wireless networks. Their results show that disruption due to handoff in case of Mobile IP is smaller in most situations.

IP mobility has been defined for both IPv4 and IPv6 [27][28]. Both versions of mobility support have similar modes of operation. In this thesis, the focus is on the provision for mobility support in IPv6 [27]. Mobile IPv6 (MIPv6) provides connectivity as the mobile node (MN) moves from its home network to a foreign network, or from one foreign network into another. As long as the MN stays connected in its home network, it is reachable by usual IP mechanism. The MIPv6 protocol comes into picture when the mobile node moves away from its home network.

A TCP connection is identified by the tuple – source IP address, source port, destination IP address, and destination port. This tuple changes when MN's IP address changes, and thereby disrupts the TCP connection. To keep the TCP connection alive, there should be no change in the mentioned tuple. MIP achieves this by allowing the mobile node to have two IP addresses – one being its home address (HoA), which does not change even when the MN moves to a different network; and a topologically correct Care-of Address (CoA) which depends on the network to which the node connects from time to time. The CoA is transparent to the transport layer, and only the static HoA is used for the TCP connection.

Each time the MN connects to a foreign network, it obtains a temporary CoA which is valid only for the time the node stays connected to the given foreign network. As long as the MN stays away from its home network, it must use the service of a Home Agent (HA), which is a router at its home network. When the mobile node obtains the CoA, it has to register the same with an HA in its home network. Once registered, the IP packets addressed to the MN reaching its home network will be intercepted and redirected to the CoA by the HA. MIPv6 also provides for optimized communication route between the MN and the correspondent node (CN). Under this mode of operation, the MN can register its CoA also with the CN, allowing the latter to send the packets directly addressed to the CoA rather than the usual HoA.

However, the MN cannot receive packets immediately after getting into a new foreign network. It has to wait for the handover process to be completed. This handover process includes the prefix discovery at the newly visited subnet, establishment of new CoA, registering this CoA with the HA, setting up a session key with the CN, and notifying the CNs this new CoA [27]. The *handover latency* is the time required for completion of this handover process.

The handover latency, as discussed for Mobile IP, can be too pronounced, especially for real time multimedia applications. Many extensions to MIPv6 have therefore been proposed [29][30][31]– focusing at reduction in the handover latency, in the number of lost packets due to the handover process, and in the signaling load on the network during the process. These extensions to the Mobile IP protocol are particularly helpful in environments where mobile hosts change their point of attachment to the network so frequently that the base MIPv6 mechanism introduces significant overhead in terms of increased delay, packet loss and signaling [32]. However, many of these extensions bring with them the problem of security – that is, how to authenticate the communication among the various entities involved in the protocol. In fact, the predecessor of MIPv6 – Mobile IPv4 had the *Route Optimization* [28] extension, which required pre-configured security association among the entities. With mobile communication becoming the order of the day, having pre-configured security association among the various entities in a global scale would be next to impossible. MIPv6 had removed such a requirement by generating the key on the fly using a challenge-response mechanism. But many of these extensions to MIPv6 bring back similar requirements. Moreover, these micromobility protocols — as these extensions are called — take care of the mobility in a localized area, beyond which it is the MIPv6 once again.

The evolution towards an all-IP network infrastructure demands that IP – with necessary augmentation - be capable of managing mobility of nodes. MIP, as discussed above, is an existing solution allowing such mobility management at the network layer. However, its capability in terms of scalability and seamlessness of handover are yet to be proven. To make an all IP space a reality, these issues must be adequately addressed.

1.4. Improving Performance through Multihoming

With the expansion of wireless networks with diverse access technologies, overlaid networks of these assorted technologies such as Wi Fi, GPRS, Bluetooth, Wi Max etc. are now available. Along with the expansion of these wireless networks and consequent developments in the support for terminal mobility, the mobile terminals too have grown in sophistication. There is a trend for mobile devices to come equipped with more than one network interfaces, thereby providing the possibility for simultaneous connectivity of the terminal through multiple access technologies. The proposed *Always Best Connected* (ABC) concept allows a person connectivity to applications using the devices and access technologies that best suit his or her needs and within his/ her reach, thereby combining the features of diverse access technologies [33][34]. Same is the idea behind Next Generation Wireless Systems (NGWS) [35]. The integrated NGWS keeps the best features of the individual networks: the global coverage of satellite networks, the wide mobility support of 3G systems, and the high speed and low cost of WLANs. At the same time, it eliminates the weaknesses of the individual systems. For example, the low-data-rate limitation of 3G systems can be overcome by using WLAN for the access, whenever such coverage is available. When the user moves out of a WLAN coverage area, it can be handed over to the overlaid 3G system. Similarly, a satellite network can be used when neither a 3G system nor a WLAN is available. The basic idea is to use the best available network at any time.

In the parlance of *Internet Engineering Task Force* (IETF), the provision of multiple network interfaces with multiple network addresses is referred to as Multi-homing [36][37]. The possible benefits of multi-homing are many, including seamless connectivity, multi-streaming, load balancing, fault tolerance, preferential routing, etc. [38].

A host is called *multi-homed* if it has multiple network layer addresses – in case of IP networks this means that the host has multiple IP addresses. This does not necessarily mean that the host has multiple link layer interfaces – a single interface can also be connected to various access routers resulting in multiple IP addresses. However, given the trend of mobile nodes equipped with multiple interfaces to support varied access technologies, this discussion focuses on multi-homed hosts having multiple link layer interfaces.

The MIP in its present form, however, does not support multiple network interfaces. Considering the possible benefits of multi-homing, IETF has initiated work to provide support for multi-homing in MIP [39]. Due to the interest in this area and the possibilities it opens up for wireless mobile communication, a new IETF working group has been recently set up – Mobile Nodes And Multiple Interfaces in IPv6 (monami6) Working Group[40].

With the concept of multihoming gaining ground, extensions have been proposed to MIPv6 to support registration of multiple CoAs at the HA [41]. The MMI (Mobile IPv6 for Multiple Interfaces) extension [39] focuses on the MN's ability to use a backup interface for ongoing communications and also to spread flows across the mobile node's multiple interfaces. However, to extract the maximum benefit from the presence of multiple interfaces, extensions to MIP should be defined such that the traffic can be distributed across the interfaces, at a proportion dynamically derived from the prevailing network status at the available interfaces.

1.5. Work Done

Given the progress towards the "*all-IP*" scenario, improvement to MIPv6 in terms of reduced handover latency is extremely essential. The availability of multiple interfaces at the mobile devices, protocol enhancements for achieving maximum benefit from these interfaces is also imperative. Given this background, work was undertaken towards a solution to ease the problem of handover latency for terminals equipped with single as well as multiple interfaces:

- **Reducing Handover Latency through Mobile Agent Support:**

  As already mentioned, handoff is an essential element of mobile/wireless communication. A handoff mechanism is needed to maintain connectivity as a mobile terminal migrates, and minimize service interruption with in-progress transfers. The handoff scheme should exhibit low latency, incur little of no data loss, and provide efficient use of resources.

  In view of the adverse affect that the handover latency can have on the overall performance of the mobility protocol,. possibilities towards a reduction in this was explored. The number of people using mobile devices is increasing by leaps and bounds, thanks to availability and reduction in cost – a direct end product of stiff business competition among the service providers. A concern in this expansion story is the limitation in the available frequency spectrum. For various advantages including higher data throughput, greater frequency reuse, location information and finer granularity, and lower mobile transmit power requirements, the future networks will adopt micro/picocellular architectures. A consequence of using small cell sizes is the increased rate of handoffs as mobile terminals move between cells during the holding times of their calls/data transfers [20]. Thus, any improvement in the handover latency will go a long way towards usability of MIP in the next generation networks. A solution using mobile agents to minimize this latency is developed and is presented in this thesis.

- **Overcoming Handover Latency through Simultaneous use of Multiple MN Interfaces:**

  As discussed above, the modern mobile devices are equipped with multiple interfaces supporting distinct wireless access technologies. This allows the user to switch from one technology to another in the absence of a particular type of connectivity infrastructure at a given location. The wireless support infrastructure is developing in such a way that there is a considerable overlap of different types of access technology support. Thus, a given area may be supported, for example, by GPRS, WLAN as well as Bluetooth. To take full advantage of such a scenario, there should be possibility of simultaneous connectivity to multiple access networks. While multiple interfaces of the mobile terminal may make this possible, there is also a need for modifications in the existing protocols to support such possibility, and allow the TCP packets flow from the source to the destination through varied intermediate network infrastructures and different interfaces at the source/destination. A solution is explained in this thesis which introduces a *convergence module* in the MIP sub layer to take care of dynamic distribution of traffic flow across available interfaces. The convergence module makes the multiplicity of interfaces transparent to the higher layers and allows the extensively deployed TCP to function without any modifications.

There have been very many proposals towards improvement of mobility management protocols. While some are transparent to the underlying network, others required certain modifications in the intermediate infrastructure. This thesis proposes modifications to MIP to reduce handover latency and also to allow simultaneous usage of the available interfaces. While the handover reduction is done through the use of mobile agents necessitating modifications at the access routers to allow for the functioning of mobile agents, the simultaneous usage of multiple interfaces is achieved through minor modifications at the communication end points and without any change to the communication infrastructure. While either of the schemes can be independently used to improve performance, the two can also be combined to derive the benefit in case the support for the mobile agents at the access routers as well as multiple interfaces at the mobile nodes is available.

1.6. Organization of this Thesis

This thesis presents the above mentioned extensions to MIP in an attempt to reduce handover latency. It discusses the two schemes in detail and presents some experimental results in support of these schemes. The new/modified message formats that would be needed to support these schemes have also been formulated.

Related works by other researchers are discussed in Chapter 2. Chapter 3 elucidates a scheme to reduce handover latency through the use of mobile agents. This chapter also presents the experimental results in favor of the scheme. In Chapter 4, an extension to MIP to support simultaneous usage of multiple interfaces to make the handover process seamless is discussed. This chapter also describes as to how the traffic can be dynamically distributed among the available interfaces to take full advantage of overlapping network infrastructure. Experimental results are also presented to show the advantage of simultaneous use of multiple interfaces. Chapter 5 explicates the inter-working of the schemes amongst themselves, in addition to that of proposed mobile agent based scheme with existing HMIPv6. Chapter 6 details out the new message formats as well as modifications needed to existing message formats to manage the proposed extensions. Chapter 7 concludes this thesis.

Chapter 2

A Survey of Works on Mobility Management for IP Based Networks

Mobility of nodes is supported using different techniques, and these attempts to integrate the mobile system with the existing infrastructure of the wireline communication networks. Some of the alternative backbone networks supporting mobility of the terminals are Public Land Mobile Network (PLMN), Mobile Internet Protocol (Mobile IP) networks, Wireless Asynchronous Transfer Mode (WATM) networks, and Low Earth Orbit (LEO) satellite networks [42].

However, given the progression towards an *all-IP* network infrastructure, the thesis is oriented towards mobility management of IP nodes. This chapter enumerates the benefits of IPv6 over its popular older version, and goes on to present a brief overview of existing mobility management protocols and their extensions. Existing extensions to the base protocol for supporting node multihoming are also discussed.

2.1. IP version 6

Version 4 of the Internet Protocol (IPv4) provides the basic mechanism for communication among varied networks that makes up the Internet. This protocol has been around since 1970s. The technologies making up the communication subnets have undergone rapid changes over this period. In spite of this IPv4 survived, and this longevity shows the flexibility and capability of its design. However, it has a major limitation – the limitation of the address space [9].

IP version 6 (IPv6) [43] is the new version of the Internet Protocol designed to be the successor of IPv4 [44]. IPv6 retains many of the features that contributed to the success of IPv4 – so much so that conceptually IPv6 can actually be considered to be IPv4 with some modifications. However, while conceptually very similar to IPv4, IPv6 has changed many protocol details. The major changes brought forward by IPv6 are:

- Expanded Addressing Capabilities: IPv6 increases the IP address size from 32 bits to 128 bits to support more levels of addressing hierarchy, a much greater number of addressable nodes, and simpler configuration of addresses.
- Header Format Simplification: IPv6 uses an entirely new and incompatible datagram format. Some IPv4 header fields have been dropped or made optional to reduce the common case processing cost of packet handling. This limits the bandwidth cost of IPv6 header.
- Improved Support for Extensions and Options: Changes in the way IP header options are encoded allow for more efficient forwarding, less stringent limits on the length of options, and greater flexibility for introducing new options in the future.
- Flow Labeling Capability: A new capability is added to enable the labeling of packets belonging to particular traffic "flows" for which the sender requests special handling, such as non-default quality of service or "real-time" service.
- Authentication and Privacy Capabilities: Extensions to support authentication, data integrity, and (optional) data confidentiality are specified for IPv6.

Given the expanse of the installed base of IPv4, the shift from IPv4 to IPv6 has been an extremely slow process. Both these versions co-exist in today's communication subnet, and it might be quite a while before the last IPv4 node moves to IPv6. However, in spite of its slow progression, there will most possibly be a time (may be in distant future) when the Internet will be entirely supported by IPv6. The discussions from this point onwards therefore pre-suppose IPv6 as the layer 3 protocol.

2.2. Mobile IPv6

Though IP very well manages transportation of packets across heterogeneous networks, it does not support node mobility. When a node moves from one network into another, its network address, i.e. the IP address, changes. IP uses the topologically valid IP address to transport packets from the source to the destination. The transport protocol TCP at the immediate higher layer identifies the connections through the tuple – source IP address, source port, destination IP address and destination port. With a change in any of the aforesaid IP addresses, the TCP connection will get disrupted – and so will the communication.

Mobile IP (MIP) is a solution that allows mobility management at layer 3 of the protocol stack, ensuring at the same time that the node mobility is left transparent to the higher layers. MIP was first defined for IPv4 – MIPv4 [28]. With the advent of IPv6, MIP too graduated into its higher version – MIPv6 [27]. The following subsections present a brief overview of MIPv6.

2.2.1. Basic Operation

As in case of a stationary node, a *mobile node* (MN) is expected to have a permanent address. In MIPv6, a MN is expected to be always addressable at this *home address* (HoA), irrespective of whether it is currently attached to its home link or is away from home. The HoA is an IP address assigned to the MN within its home subnet prefix on its home link. While the MN is at its home link, packets addressed to its HoA are routed to it using conventional Internet routing mechanisms.

While visiting some foreign links away from its home network, the MN connects itself to an *Access Router* (*AR*) in the visited network. In such cases, it is also addressable at one or more *Care-of Addresses* (CoAs). A CoA is an IP address associated with a MN that has the subnet prefix of a particular foreign link. The MN can acquire its CoA through conventional IPv6 mechanisms. As long as the MN stays in this location, packets addressed to this CoA will be routed to the MN.

The association between a MN's HoA and CoA is known as *binding* for the MN. While away from home, a MN registers its *primary CoA* with a router on its home link, requesting this router to function as its *home agent* (HA). The MN performs this binding registration by sending a *Binding Update* message to the home agent. The HA responds to this message with a *Binding Acknowledgement* message.

The MN may have multiple CoAs at any given time, for example with different subnet prefixes. However, as per MIPv6, only one of them can be registered with the home agent (HA) for a given home address. This CoA is called its *primary* CoA.

Any node communicating with a MN is referred to as a *correspondent node* (CN) of the MN. MNs may keep their CNs informed about their current location. This happens through *correspondent registration*.

2.2.2. Modes of Operation

There are two possible modes of communication between the MN and its CN:

- Bidirectional Tunneling, and
- Route Optimization

Bidirectional Tunneling does not require MIPv6 support from the CN and is available even if the MN has not registered its current binding with the CN. Packets from the CN are sent to the MN's HoA. If the concerned MN is in its home link, the packets will be routed to its HoA. Conversely, if the MN is stationed at a foreign link, the HA at MN's home link will intercept this packet and tunnel the same to the former's CoA. The HA intercepts any IPv6 packets addressed to MN's HoA using *Proxy Neighbour Discovery*. From the MN's end, packets to the CN are tunneled to the HA (*reverse tunneled*) and then normally routed from the home network to the CN.

Route Optimization requires the MN to register its current CoA at the CN. Packets from the CN can then be routed directly to the CoA of the MN. Such direct routing of packets to the MN's CoA allows the shortest communication path to be used. It also helps in easing congestion at the HA. In addition, the impact of any possible failure of the HA or networks on the path to and from it is reduced.

Whenever the MN changes its point of attachment and configures a new CoA, it informs the same to it's HA through a binding update message. If route optimization is envisaged, it should also perform a correspondent registration to update the cached bindings at the CN. However, the binding updates (whether to HA or to CN) always needs to be authenticated before registering the new CoA to avoid attacks from malicious hosts.

2.2.3. Binding Update Security

The MN and the HA must use an IPSec security association to protect the integrity and authenticity of the binding updates and acknowledgements [45]. As with all IPSec security associations, manual configuration of security associations must be supported. The used shared secrets must be random and unique for different MNs, and must be distributed off-line to the MNs. Such manual configuration becomes possible since the MN and it's HA belongs to the same administrative domain.

The protection of binding updates sent to CNs does not require the configuration of security associations or existence of an authentication infrastructure between the MN and its CNs. The CNs may belong to varied administrative domains, and any requirement for manual security association configuration or authentication infrastructure will drastically limit the usability of the protocol. Instead, a method called the *return routability procedure* (RRP) is used to assure CN that the right MN is sending the messages.

The RRP enables the CN to obtain some reasonable assurance that the MN is in fact addressable at its claimed CoA as well as its HoA. This is done by testing whether packets addressed to the two claimed addresses are routed to the MN.

This process is initiated by the MN by sending two messages to the CN –

- *Home Test Init* (HoTI) message is reverse-tunneled to CN through the HA, and
- *Care-of Test Init* (CoTI) message is sent directly to the CN.

Both these messages contain a cookie each – the *home init cookie* and the *care-of init cookie* respectively.

On receipt of these messages, the CN responds with

- *Home Test* (HoT) message which is send to the HA and then tunneled to the MN's CoA, and

- *Care-of Test* (CoT) message which is send directly to the claimed CoA

These messages contain *home keygen token* and *care-of keygen token* respectively. They also include the *home init* and *care-of init cookies* respectively to reasonably convince the MN that its protocol messages are being processed by the desired CN.

When the MN has received both the HoT and CoT messages, the RRP is complete. As a result of this, the MN now has the data required to send the binding update message to the CN. The MN hashes the *home keygen and care-of keygen tokens* together to form a 20 octet binding key *kbu* which is used by the CN to authenticate the received binding update message. The CN does not create any state specific to the MN until it receives the binding update message from the MN authenticated by the *kbu*.

For the purpose of brevity, the details of the cookies, tokens and the *kbu* formats are omitted from this discussion. These details can be found in [27].

2.3. IP Micromobility Protocols

MIPv6 requires that every time there is a handover, the MN has to register its new CoA with it's HA and, if route optimization is implemented, with the CN(s) it is communicating with. Due to the number of control messages involved in the HA and CN binding update processes, the handover latency can become significantly large. To minimize this handover latency, IP micromobility protocols have been proposed. To enhance user experience in the face of multiple handovers, micromobility protocols support fast and seamless mobility within a localized domain. These protocols aim to handle local MN movements without interaction with the Mobile IP enabled Internet. However, beyond these local movements, the node mobility is managed by usual MIPv6 mechanisms.

2.3.1. Hierarchical MIPv6

Hierarchical MIPv6 (HMIPv6) [29] takes the help of a local anchor point which allows Mobile IPv6 to benefit from reduced mobility management related signaling with external networks. It introduces a new MIPv6 node – the *Mobility Anchor Point* (MAP) which can be located at any level in a hierarchical network of routers. A MAP essentially functions as a local Home Agent.

A MN entering a MAP domain receives Router Advertisements containing information on one or more local MAPs. The MN can bind its current CoA with an address on the MAP's subnet – the latter known as the *Regional CoA* (RCoA). This RCoA needs to be registered with the HA and the CN(s) following usual MIPv6 procedures.

Acting as a local HA, the MAP receives all packets on behalf of the MN it is serving. The MAP then encapsulates and forwards these packets directly to the MN's current address. If the MN changes its current address within a local MAP domain – i.e., it changes the *Local CoA* (LCoA), the new address needs to be registered only with the MAP. The RCoA does not change as long as the MN moves within the same MAP domain. This makes the MN's mobility within the MAP domain transparent to the correspondent nodes it is communicating with. As a result, as long as the MN movement is restricted within the given MAP domain, no binding update messages are sent to HA and CN(s). When the MN moves out of the current MAP domain into another such domain, it configures a new RCoA with a new MAP. It is only than that HA and CN(s) registrations are required for this new RCoA.

The advantages of introducing the MAP, as long as the MN movements are localized within a given MAP domain, are:

- The mobile node sends Binding Updates to the local MAP rather than the HA (which is typically further away) and CNs.
- Only one Binding Update message needs to be transmitted by the MN to its MAP before traffic from the HA and all CNs is re-routed to its new location. This is independent of the number of CNs that the MN is communicating with.

HMIPv6 uses an additional registration between the MN and its current MAP. When a MN moves into a new MAP domain, it obtains an RCoA, an LCoA and registers the binding between these two addresses with the new MAP. The MAP then verifies whether the RCoA has not been registered yet and, if so, it creates a binding cache entry with the RCoA and LCoA. Whenever the MN gets a new LCoA, it needs to send a new BU that specifies the binding between RCoA and its new LCoA. This BU needs to be authenticated; otherwise any host could send a BU for the MN's RCoA and hijack the packets meant for the MN.

It is not feasible for the MAP to have prior knowledge of the identity of the MN or its HoA and hence no pre-configured security association between them can be implemented. As a result, the security association between the MN and the MAP need to be established using a key establishment protocols such as IKE.

2.3.2. Fast Handover

The Fast Handover [30] addresses the problem of how to allow a MN to send packets as soon as it detects a new subnet link, and how to deliver packets to a MN as soon as its attachment is detected by the new access router.

When a MN changes its attachment to a new access router, the usual MIPv6 process would entail a period of handover latency, during which no data (except for control messages) can be exchanged. However, the Fast Handover enables a MN to quickly detect its movement to a new subnet by providing the information about the new access point and the associated subnet prefix before the MN actually moves to the new subnet. For instance, a MN may discover available access points using link-layer specific mechanisms and then request subnet information corresponding to one or more of those discovered access points. The particular link-layer information available, as well as the timing of its availability, differs according to the particular link-layer technology in use [46]. The MN may request such subnet information after performing router discovery or at any time while connected to its current router. Through the interchange of control messages (RtSolPr and PrRtAdv) with its current access router, the MN formulates a prospective New CoA (NCoA) before it actually connects to the new access router's link.

To reduce the Binding Update latency, the protocol specifies a tunnel between the Previous CoA (PCoA) and the NCoA. As a result, the previous access router begins tunneling packets arriving for PCoA to NCoA. Such a tunnel remains active until the MN completes the Binding Update with its correspondents. In the opposite direction, the MN reverse tunnels packets to previous access router until it completes the Binding

Update. Such a reverse tunnel ensures that packets containing PCoA as a source IP address are not dropped due to ingress filtering.

For establishing the tunnel, the MN sends a *Fast Binding Update* (FBU) message to its previous access router when a link specific handover event occurs. The purpose of the FBU is to authorize the previous access router to bind PCoA to NCoA, so that arriving packets can be tunneled to the new location of the MN. Hence, the latency due to new prefix discovery subsequent to handover is eliminated. Furthermore, this prospective address can be used immediately after attaching to the new subnet link if the MN had received a *Fast Binding Acknowledgment* (FBack) message from the previous access router prior to its movement to the new access router's link. If it moves without receiving an FBack, the MN can still start using NCoA after announcing its attachment through a *Fast Neighbor Advertisement* (FNA) message. The new access router responds to FNA if the tentative address is already in use thereby reducing NCoA configuration latency. Under some limited conditions in which the probability of address collision is considered insignificant, it may be possible to use NCoA immediately after attaching to the new link.

The protocol allows exchanges of messages among the access routers to confirm that a proposed NCoA is acceptable. For instance, when an MN sends an FBU from previous access router's link, FBack can be delivered after the new access router considers the NCoA acceptable for use. This is especially useful when addresses are assigned by the access router.

However, for this protocol to be executed, the access routers must have necessary security association established by certain means.

2.3.3. Cellular IP

Cellular IP (CIP) [31] intends to provide local mobility and handoff support. The wide area support can be provided by Mobile IP. Like HMIPv6, CIP too follows a hierarchical setup of routers, which are arranged in a tree format. The root is the CIP *Gateway*, which connects the CIP network to the Internet backbone. There can be several base stations (routers) in a CIP network. These base stations transmit periodic beacon signals. The MNs use these to locate the nearest base station. While transmitting, a MN relays the packets to the nearest base station. From the base station, the packets move up the tree towards the gateway from one router to another, hop by hop. The network outside the CIP network is assumed to work using Mobile IP. The address of the gateway is stored as the CoA for the MN by the concerned HA at the home network. To manage the node mobility, the CIP nodes (routers) maintain two types of caches – *Route Cache* and *Paging Cache.*

While moving towards the Gateway, packets transmitted by the MN create and update entries in each node's Route Cache. An entry maps the MN's IP address to the neighbour from which the packet arrived to the node. The chain of cached mappings referring to a single MN constitutes a reverse path for downlink packets addressed to the same MN. As the MN migrates, the chain of mappings always points to its current location because its uplink packets create new mappings, changing the old ones. IP packets from external networks addressed to a MN reach the Gateway and are routed by the chain of cached mappings associated with the said MN. To prevent its mappings from timing out, a MN can periodically transmit control packets.

On the other hand, the Paging Caches are maintained at fewer nodes, and record the location of the MNs that are idle and not participating in any communication. The cells in a CIP network are grouped into paging areas. An idle MN roaming within a paging area need not transmit any update message. However, when they cross a paging area, they need to transmit *Paging-update* packets which are routed from the base station to the gateway using hop by hop routing. Selected nodes monitor these packets and update the Paging Cache entries for the MN pointing to the new paging area. When packets meant for the MN reach the Gateway from the Internet, the routing cache of the router is checked. If the MN was idle, there will be no entry for it in the routing cache of the router. In that case, the Paging Cache is used to route the packets. A router with a Paging Cache entry for the MN will forward the packet towards its current location in the CIP domain. If a router does not have the Paging Cache, it forwards the packets to all its downlink routers. If, on the other hand, the router has a Paging Cache without an entry for the MN, the packets are discarded. After the packet leaves the last router which has the Paging Cache, it is effectively downlink broadcast by all routers it passes.

The MN will be using one of these routers as its base station, and will receive the packet. On receiving the packet, the MN moves to active state and creates its Route Cache mappings by sending *route-update* packets.

While moving from one base station to another in the same CIP network, the MN does not send any binding update to the HA. All it does is to transmit Route-update packet (for active node) or Paging-update packet (when an idle node crosses the paging area) to map the new route to the gateway. When the MN crosses over to a new CIP network (having a new Gateway), it sends a binding update message to it's HA informing the address of the new Gateway as its care-of address. Thus the gateway is somewhat similar to MAP of HMIPv6.

Each CIP Network has a secret network key of arbitrary length known to all CIP nodes. The network key is kept secret from MNs and other nodes outside the CIP Network. Upon initial registration the Gateway must authenticate and possibly authorize the MN. This initial authentication and authorization can be based on any known symmetric or asymmetric method. After authentication the Gateway generates a ID involving the IP address of the MN and the network key. It then acquires the public key of the MN from a trusted party, encrypts this newly generated ID and sends it to the MN. This way the MN and the Cellular IP network have a shared secret which does not change during the handoff within the same CIP domain.

2.3.4. HAWAII

Handoff-Aware Wireless Access Internet Infrastructure (HAWAII) [47] uses specialized path setup schemes which install host-based forwarding entries in specific routers to support intra-domain micro-mobility and defaults to using Mobile-IP for inter-domain macro-mobility. These path setup schemes reduce mobility related disruption to user applications, and by operating locally, reduce the number of mobility related updates.

HAWAII operates entirely within the administrative domain of the wireless access network. In order to keep HAWAII transparent to mobile hosts, the mobile host runs the standard Mobile-IP protocol. To reduce the frequency of updates to the HA and avoid high latency and disruption during handoff, the processing and generation of

Mobile-IP registration messages are split into two parts: between the mobile host and the base station and between the base station and the HA.

HAWAII defines a hierarchy based on domains. There is a gateway in each domain called the *domain root router*. When moving in its home domain, the MN retains its IP address. Packets destined to the MN reach the domain root router based on the subnet address of the domain and are then forwarded over special dynamically established paths to the mobile host. For these MNs, a home agent is not involved in the data path, resulting in enhanced reliability and efficient routing.

When the MN moves into a foreign domain and the new domain is also based on HAWAII, then it is assigned a co-located CoA from its foreign domain. Packets are tunneled to the CoA by a home agent in its home domain. When moving within the foreign domain, the MN retains its CoA unchanged (thus, the HA is not notified of these movements); connectivity is maintained using dynamically established paths in the foreign domain.

HAWAII uses path setup messages to establish and update host-based routing entries for the MNs in selective routers in the domain so that packets arriving at the domain root router can reach the destined MN. When the MN powers up, it sends a Mobile-IP registration message to its nearest base station. The base station then propagates a HAWAII path setup update message to the domain root router of the current domain using a configured default route. Each router in the path between the MN and the domain root router adds a forwarding entry for the MN. Finally, the domain root router sends back an acknowledgement to the base station which then sends a Mobile-IP registration reply to the MN. At this time, when packets destined for the MN arrive at the domain root router based on the subnet portion of the MN's IP address, the packets are routed within the domain to the MN using the host-based forwarding entries just established. These host-based forwarding entries are soft-state entries that are kept alive by periodic hop-by-hop refresh messages. Other routers in the domain have no specific knowledge of this MN's IP address.

HAWAII uses two path setup schemes to re-establish path state when the mobile host moves from one base station to another within the same domain.

In the *Forwarding Scheme*, a Mobile-IP registration is first sent by the MN to the new base station. The message contains the old base station's address. The new base station then sends a path setup update to the old base station. The old base station adds a forwarding entry for the MN's IP address. It then forwards the message which traverses through the routers until the cross-over router is reached. The cross-over router adds forwarding entries that result in new packets being diverted to the mobile host at the new base station. It then forwards the message towards the new base station. Eventually the message reaches the new base station. The new base station changes its forwarding entry and sends a Mobile-IP registration reply to the MN. Only the new and old base stations, and the routers connecting them, are involved in processing the path setup message.

In the *Non-Forwarding Path Setup Scheme* the path setup message travels from the new base station to the old base station. In the process, when this message reaches the cross over router, it adds forwarding entries such that new packets are diverted directly to the MN at the new base station. This, therefore, does not result in any forwarding of packets from the old base station.

For the functioning of the protocol, HAWAII assumes the existence of a trust model among the various entities involved.

2.4. Mobility of Multihomed Nodes

A host is called multihomed if it has multiple network layer addresses. In case of IP networks this means that the host has multiple IP-addresses [37]. This does not necessarily mean that the host also has multiple link layer interfaces. Multiple IP addresses can be configured on a single link layer interface. In this section, some protocol modifications are discussed that allow a mobile node to be multihomed. The mobility management in such cases, therefore, involves administration of all its available addresses as the node moves from one network to the other.

Multihoming becomes more relevant today since the new equipments available in the market are now often shipped with interfaces supporting several access technologies (both wired and wireless) integrated in them. The main purpose of this integration is to federate all means of communications in order to access the Internet ubiquitously (from everywhere and at any time), as no single technology can be expected to be deployed everywhere. Flows may thus be redirected from one interface to the other due to the loss of connectivity or change of the network conditions. Several access technologies are also integrated in order to increase bandwidth availability or to select the most appropriate technology according to the type of flow or choices of the user. The goals and the corresponding benefits [38] that can be accrued through these multiple interfaces are:

- Permanent and Ubiquitous Access: In a heterogeneous Internet, it is impractical to expect the support for same access technology as the node moves from one network to another. Multiple interfaces bound to distinct technologies can be used to ensure that a permanent connectivity is offered, anywhere, anytime, with anyone.

- Reliability: With the availability of multiple points of attachment, the functions of a system component (e.g. interface, access network) are taken over by secondary system components when the primary component becomes unavailable. Connectivity is guaranteed as long as at least one connection to the Internet is maintained.

- Load Sharing: The multiple points of attachment can be used to spread network traffic load among several routes. When there is a large amount of data flowing across the networks, this can prevent congestion by distributing traffic across several networks.

- Load Balancing/Flow Distribution: This may lead to separation of a flow between multiple points of attachment of a node, usually choosing the less loaded connection or according to preferences on the mapping between flows and interfaces.

- Preference Settings: This allows the user or the application to choose the preferred transmission technology or access network based on cost, efficiency, policies, bandwidth requirement, delay, etc.

- Aggregate Bandwidth: This provides the user or the application with more bandwidth. Multiple interfaces connected to different links can increase the total available bandwidth through aggregation.

2.4.1. MIPv6 Based Multihoming Solution

While Mobile IPv6 [27] allows a MN to perform handover between subnets, there are no means to manage this mobility across several interfaces of the MN. *Mobile IP for Multiple Interfaces* (MMI) [39] discusses the management of multiple available interfaces to achieve this. MMI discusses different ways in which multiple interfaces of a MN can be managed. It introduces three such ways of handling these multiple interfaces:

- *Per-correspondent node mobility* – This is the ability of the MN to manage multiple flows by CN. Each CN is independently managed by the MN but all flows from one CN use the same MN interface. Thus, when a MN has two flows with the same CN, the same interface has to be used.

  In order to manage the flow spreading on several interfaces, the MN may have a policy table to decide which interface(s) is (are) preferred for which type of flow. A MN must carefully choose which CoA to register with its CN. If the MN has several flows with the same CN, all flows must use the same CoA, i.e. the same interface. Therefore the MN has to maintain a policy table that does not generate conflicts.

  This policy table maintains preferences on interfaces according to a flow discriminant. The flow discriminant can be one, several or all fields of the source/destination ports numbers, source/destination address and protocol number. For example, it can be just a destination port, or the (source port, destination port, CN address) tuple. A priority field is maintained in the policy table and is used to set a priority on the different entries and helps in case of conflict (two different mappings with the same CN).

- *Per-flow mobility* – This is the ability for the MN to manage each flow independently. Each flow can be mapped to any interface, without disturbing the existing mappings between flows and interfaces.

  Therefore, each flow can be uniquely identified and redirected between interfaces without modifying binding of other flows. Especially, flows exchanged with a single CN can be independently managed by registering a different CoA for each flow. To reach this goal, new options in Binding Update have to be defined in order to identify a flow and an entry in the binding cache since several CoAs would be bound to the same HoA.

  According to Mobile IPv6 specification, a MN is not allowed to register multiple CoAs bound to a single HoA. If a MN sends Binding Updates for each CoA, CNs would always overwrite the CoA recorded in the binding cache with the one contained in the latest received binding update. In Mobile IPv6, the HoA is the identifier of the MN, and hence it's binding. If the CN is to have several CoAs bound to the same HoA, a new identifier will be needed in the binding cache. A new field, called the *Binding Unique Identification* (BID), has been proposed to be included in the Binding Update message [41]. An extension to binding cache management has also been proposed to store the BID. The BID is assigned to either the interfaces or CoAs bound to a single HoA of a MN. The MN notifies the BID to both it's HA and CNs by means of a Binding Update. CNs and the HA record the BID into their binding cache. The HoA thus identifies a MN itself whereas the BID identifies each binding registered by a MN. Multiple bindings can then be distinguished through the use of the BID.

- *Load balancing mobility* – This is the ability of the MN to simultaneously use several interfaces with the same CN, even for the same flow. This mechanism aims to allow a multi-interfaced MN to perform load balancing across several interfaces. This requires the introduction of a new option in MIPv6 to allow a MN to register several CoAs as source or destination CoA. The new option is introduced as the *Load Balancing Mobility Option* which is used to inform the CN, when MN is the sender, about the IP addresses of the MN interfaces.

Conversely, if CN is the sender, the Load Balancing Mobility Option is used to inform the CN about the addresses of the MN interfaces and the proportion of the packets to be sent to each of these.

2.4.2. Mobile SCTP

Mobile SCTP (m-SCTP) is an extension of the transport layer protocol – SCTP. Unlike MIP, m-SCTP is a transport layer mobility solution. Mobile SCTP uses SCTP as defined in RFC2859 [48], RFC3176 [49] and RFC3199 [50] with the extension described in ADDIP [51] resulting in a mobility enabled transport protocol supporting multihoming. Such a transport layer mobility management implements the whole functionality for providing mobility to nodes in the transport layer entities at both ends of the network.

Stream Control Transmission Protocol (SCTP) provides a message-oriented data delivery service. The packets always begin with an SCTP common header that provides three basic functionalities -Source and destination ports, Verification tags, and Checksum. Apart from the header, the remainder of an SCTP packet consists of one or more chunks – the concatenated building blocks that contain either control or data information. SCTP control chunks transfer information needed for association functionality, while data chunks carry application layer data.

The general-purpose SCTP [52][53][54] was designed to expand the scope beyond TCP and UDP. One of the features of this protocol is the support for multihoming. This multihoming was proposed for mission critical systems that rely on redundancy at multiple levels to provide uninterrupted service during resource failures. Multihomed nodes are accessible from multiple IP addresses. To benefit from the availability of multiple IP addresses at the network layer, SCTP supports multihoming at the transport layer. As per this protocol, each end point chooses a single primary destination address for sending all new data chunks during normal transmission. An end point sends retransmitted data chunks to an alternate address under the assumption that alternate paths increase the probability of the chunks reaching the peer end point. Continued failure to reach the primary address ultimately results in failure detection, at which point the end point transmits all chunks to an alternate destination until the primary destination become reachable again.

This feature of SCTP has been modified and adopted in m-SCTP. As the mobile node moves towards a new network, it receives information about reaching the coverage area of another network from the physical layer of its NIC. As a consequence, in addition to its already existing link, the mobile node establishes a link to the new network and gets a new IP address assigned to its second network interface. The mobile node therefore becomes multi-homed and is now reachable by two different networks. This information is relayed to the corresponding server using the previously established transport layer connection.

On reaching the new network, the mobile node may leave the coverage of the previous access router and may loose the link for its first IP address. The data stream between server and mobile client gets interrupted and the reliability behavior of SCTP ensures that all data is sent over the second link in the case of permanent failure of the first link.

When the mobile node is convinced, by information from the physical layer, that the failure of the first link is permanent, it will inform its peer that it is now no longer reachable by the first IP address and removes this IP address from the association between the mobile node and its corresponding server.

2.4.3. Cellular SCTP

Another flavour of SCTP based mobility management solution - *Cellular SCTP* (cSCTP) [55] - suggests the use of two primary addresses simultaneously by duplicating the packet transmissions (while halving the transmission rate) during handoff to provide soft handover. In m-SCTP, before MN sets the new IP address to be the primary IP address of the association, data packets are sent to the old IP address. However, if MN is not reachable by the old IP address anymore, the retransmissions are sent to the newly added IP address (for the new link). These retransmissions will result in delays resulting in performance deterioration. By duplicating the data transfer during the handoff, cSCTP aims to mitigate these negative effects. To facilitate mobility management when Correspondent Nodes initiate the associations and need to locate MNs, cSCTP uses the mobility management function of Session Initiation Protocol (SIP) to locate the (current) location(s)/address(es) of the callee MN.

2.4.4. TraSH

Similar in principle to mSCTP or cSCTP, the basic idea behind *Transport layer Seamless Handover* (TraSH) [56] is to exploit multi-homing feature to keep the old path alive while setting up the new path, thus achieving a seamless handover between adjacent subnets. TraSH introduces a Location Manager [57] to maintain a database storing the correspondence between MN's identity and its current primary IP address.

With TraSH [58], handoffs begin after a mobile node enters a new network and receives a router advertisement and configures an address in the new network. TraSH then adds the new IP address into existing SCTP associations in addition to any old addresses in the association. As the mobile node moves further into the coverage area of the new network and discovers it is better connected there, it changes the primary destination address in its SCTP associations. At this point, the mobile node also uses the new address and new network to initiate new associations and updates its location management information. Finally, as connectivity with old networks degrades and is lost, the mobile node deletes the corresponding addresses from its SCTP associations. The architecture provides the location management services while the ASCONF extension to SCTP provides all that is needed for binding updates (new address addition, change of primary address, and removal of old addresses).

When CN wants to setup a new association with MN, it first sends a query to the Location Manager with MN's identity (home address, domain name, or public key, etc.). The Location Manager responds with the current primary IP address of MN. Once the primary address of MN is known, CN sends an SCTP INIT chunk to MN's new primary IP address to setup the association. If the domain name is used as MN's identity, then the location manager can be merged into a DNS server.

2.5. Summary

In this chapter, mobility support in IPv6 and some of the relevant works towards reducing the handover latency and towards providing multihoming support for mobile nodes have been discussed. While each of the solutions discussed above bring about positive improvement in mobility management and tend to increase the degree of seamlessness, there is still scope for further improvement. Some of their shortcomings are summarized as follows.

In HMIPv6, the local MN movement are transparent to the HA, and is managed by the MAP. However, for every new MAP domain, the registration of RCoA has to be done at the HA, involving normal MIPv6 procedures. This will result in deterioration in quality of service whenever there is an inter-domain transfer. In the security front, it is not possible to have a preconfigured security mechanism between the MN and the MAP, both belonging to different administrative domains. Thus the security between the MN and the MAP banks on trusted third party infrastructure, which MIPv6 consciously tried to avoid.

CIP uses CIP gateways similar to MAPs in HMIPv6. Accordingly CIP too will require HA participation for inter-CIP network mobility. Such mobility will therefore, result in a worsening of quality of service, analogous to HMIPv6. The security between the MN and the CIP gateway will also need external support.

HAWAII uses domain root routers which act like gateways of the other two schemes. However, in this case the HA is not informed when the movement is between two HAWAII domains. The domain root router in the home domain takes care of forwarding the packets to the corresponding router in the foreign domain. This would invariably require a trust mechanism between the domain root routers across the domains. HAWAII assumes the existence of a trust model and does not elucidate on the matter.

The micro-mobility protocols service a limited area, and require MIPv6 support for macro-mobility. Hence a movement out of MAP domain, CIP network or HAWAII domain will entail the new CoA to be registered with the HA, following usual MIPv6 procedure. With HA likely to be present at distant home network, this will result in considerable handover latency for the inter-domain transfers. Moreover, these protocol descriptions are silent on the fact that the CoA registrations at HA have finite lifetime and that the same will have to be renewed, even in the absence of MN movement. These renewals will inevitably add to the overhead, though not affecting the handover latency. In case of route optimized operation, the key with CN is set up on the fly – the process involving interchange of control messages. To complicate matters, this key is valid only for a finite lifetime and will accordingly require regeneration. Thus, even if the MN movement is restricted within an administrative domain, transfer of control packets from MN to it's HA and CN(s) – and hence the overhead – cannot be avoided.

In Fast Handover, the security between the access routes will be pre-requisite for tunneling of packets from the previous to the new access router. This will also have to be pre-configured, which might be difficult in practice; or will again depend on a trusted third party.

In multihoming through MMI, the MN informs the CN about the available interfaces through Load Balancing Mobility Option. When CN initiates the flow, this extension does not allow it to dynamically distribute the traffic based on network characteristics at different links to achieve the desired load balancing. Moreover, when a MN interface performs handover, the usual MIPv6 procedure is followed to register the new CoA at MN and CN(s). This may result in considerable overhead, particularly in presence of multiple interfaces. Besides, when an interface is connected to the home network, the single HoA will limit the usability of MN's other interfaces. As the proxy neighbour advertisement stops the moment an interface connects to the home network, the intercepting of packets by the HA and subsequent redirection will no longer be possible.

The SCTP based extensions like Mobile SCTP, Cellular SCTP and TRasH do not support load balancing or bandwidth aggregation. In addition, there may be more than one transport layer connection set up between the same set of nodes. If mobility is to be managed at the transport layer, each of these connections will have to be reconfigured individually. These individual reconfigurations of multiple transport layer connections could otherwise be avoided if mobility is managed at network layer. While TRasH introduces a Location Manager to record the correspondence between MN's identity and its current primary IP address, the other SCTP based extensions take care only of handoff management, and needs additional protocol support to deal with location management.

Chapter 3

Enhancing MIPv6 Performance using Mobile Agents

3.1. Background

Of the various mobility management mechanisms at the network layer level, Mobile IP is comparatively a more complete solution [59]. There is also a gradual progress towards *all-IP networking* solution [60]. While MIPv6 does provide connectivity as a mobile node moves across the networks, it is not really undisrupted. The mobile node cannot receive IP packets immediately after getting attached to an access router in a new subnet. The handover process has to be completed first. This process includes the IP address prefix discovery at the newly visited subnet, establishment of new care-of address (CoA), registering this care-of address with the home agent, setting up of a key with the correspondent node, and informing the correspondent node(s) about the new care-of address. The *handover latency* is the time required for completion of this handover process. There may also be an additional delay due to redirection of the packets that may have already arrived at the previous point of attachment.

This handover latency can be too pronounced, especially for real time multimedia applications. Many extensions to MIPv6 has been proposed – which are focused at reduction in this handover latency, in the number of lost packets due to the handover process, and in the signaling load on the network during the process. These extensions are particularly helpful in environments where mobile hosts change their point of attachment to the network so frequently that the base protocol introduces significant overhead in terms of increased delay, packet loss and signaling [32]. However, many of these [29][30][31] bring back the problem of binding update authentication across administrative domains, which originally existed in MIPv4 and was later taken care of in MIPv6. Moreover, these micromobility protocols — as these extensions are called

— take care of the mobility in a localized area, beyond which it is back to MIPv6 once again.

In this part of the thesis, a scheme is proposed which reduces handover latency and signaling traffic without requiring any additional preconfigured security associations, other than those already specified in the base MIPv6. Moreover the scheme operates at the macro level, in contrast to the extensions that manage mobility at the micro level. This is achieved through the use of *mobile agents*.

3.2. Proposed Scheme

As mentioned, the services of the mobile agents are utilized in this scheme to improve the MIP performance by reducing handover latency. The use of mobile agents ensures that the route used for all communication involved in mobility management is optimal or, at least, near optimal.

3.2.1. Mobile Agents Assisted Handover

Mobile Agents are processes dispatched from a source computer to accomplish a specified task. Each mobile agent is a computation along with its own data and execution state. After its initial submission, the mobile agent proceeds autonomously and independently of the sending client [61]. As these mobile agents need to move across heterogeneous architectures, they tend to be independent of platform architectures [62]. To assist them in traversing heterogeneous environments, they are almost universally written in interpreted machine-independent language [63].

The agent concept is already used heavily as a part of the service architecture of next generation networks [64]. They have also been used in case of mobile ad-hoc networking [65]. It has been shown that mobile agent provides higher flexibility and performance than many existing communication paradigms [66].

The mobile agents, in this scheme, will have to move from one network to another, and will therefore require support from the local networks. This support has to be in the form of *mobile agent platform* (MP). The implementation of this scheme would therefore involve providing MP infrastructure at the visited networks. While such a support will allow this scheme to improve performance – its absence however, will make the architecture fall back to base MIPv6, and not thwart the communication.

The mobile agents in this scheme are envisaged to

- proxy for the mobile node's home agent at the foreign networks,
- assist in registering the CoAs,
- assist in return routability procedure to set up authorization key for correspondent node binding in order to achieve route optimization,
- prevent packet drop during handover by redirecting the packets in transit to the new CoA, and
- collect information about network usage for billing, etc.

The use of the mobile agent in this scheme will result in the following benefits:

- reduced handover latency,
- reduced network traffic load in terms of number of packet hops, and
- increased robustness of the protocol due to reduced dependence on the home agent.

Apart from these, the mobile agents can also ease the management of security in case of the Hierarchical Mobile IPv6 [29] by eliminating the need for pre-configured security associations among various entities belonging to different networks (This is discussed in Chapter 5 of this thesis).

3.2.2. Modified Protocol

In the scheme discussed here – the *MIPv6 with Mobile Agent Assisted Handover (MAAH)* – a mobile agent moves along with the MN, as the latter moves from one access router to another. This introduction of the mobile agent calls for appropriate modifications in the protocol flow.

3.2.2.1. CoA Registration as MN moves out of HA

The discussion in this sub-section assumes that the MN is initially stationed at its home network and subsequently moves out into a foreign network. The steps involved in managing mobility in such case are listed below:

- As in base MIPv6, when a given MN moves out of its home network, it attaches itself to an access router – say AR1.
- After acquiring a CoA under AR1, the MN sends this binding information to its home agent HA in the form of Binding Update Message.
- The HA sends a binding acknowledgement in response to the binding update as in base MIP. In addition, under this MAAH scheme, the HA also sends a mobile agent MA1 to the router to which the MN is connected. This is possible only if MP is available at the particular router – an information previously made known to the HA through the binding update message. In case the router does not support mobile agents, the rules laid out in base MIPv6 will be followed. If there is already a mobile agent (serving other mobile nodes from the same home network) present at that access router, only the relevant information about the current MN is sent to the former. The information sent to an existing mobile agent will include the security association data – so that a secure communication can be set up between the MN, the mobile agent and the HA of the MN.

3.2.2.2. Initiation of Communication by CN

If the MN is at its home network, any CN interested in initiating a communication session with the former will forward the packet to the MN's Home Address (HoA), as in MIPv6. The MN will receive the same (at the topologically correct HoA) and may respond appropriately.

It is also possible that a CN sets up communication with the MN when the latter is away from its home network. The MN might be visiting a foreign network and be supported by a particular access router (a mobile agent will have reached the access router in the process of registering the current CoA). As in base MIPv6, the CN will send the packet to the MN's home network, where the HA will intercept and forward the same to the current CoA of the MN.

The process of communication initiation by the CN is same as in base MIP. In either of the above situations, if route optimization is desired, MN will send a binding update to CN informing its current CoA – every time the MN changes its point of attachment or its current registration lifetime expires, whichever happens earlier. Of course, this Binding Update can only be sent after a key is in place to authenticate the same. The MAAH scheme will be useful in case the route optimization is initiated for MN-CN communication. Therefore, this discussion henceforth assumes the route optimized mode of communication.

3.2.2.3. CoA registration as MN moves from one foreign network to another

When the MN moves from its earlier foreign network into a new foreign network, the MIPv6 with MAAH proceeds as follows:

- The MN, on moving into the next foreign network and attaching to access router AR2, sends the binding update message to MA1 (the mobile agent stationed at the previous router AR1) instead of the HA as in original protocol. This MN will most often be closer to the MA1 compared to it's HA, thus reducing the path traversed by the binding update and the corresponding binding acknowledgement messages.

- The MA1, whose job is to proxy for the HA, will now register the MN – i.e., authenticate the Binding Update, record the CoA and its registration lifetime – and accordingly send the binding acknowledgement. The MA1 would also send a mobile agent MA2 to the new router AR2, if a support for the same is available.

- The mobile agent MA2 to the new access router can be sent asynchronously to the new CoA registration process. This ensures that the time required for the mobile agent transfer does not introduce any additional delay in this process. Like in the previous case, if a mobile agent serving the given HA is already present in the new network, only information relevant to MN would be dispatched. The use of mobile agent at the previous access router to take care of MN registration reduces the network path involved, and thereby the latency during the registration process.

- However, to keep the HA informed about the current location of the MN, the MA1 will send binding update to the HA at fixed intervals. Such a binding update will contain information not only about the particular MN, but of all the mobile nodes served by the mobile agent MA1. The mobile agents will update the home agent at certain regular intervals asynchronous to the CoA registration process. Thus, these updates will not contribute to the handover latency.

Once the MN has registered its new CoA with MA1 (as confirmed by the binding acknowledgement), the former can send a binding update message to CN and other nodes it is communicating with, if any, to continue with route optimization. Such updates shall definitely have to be authenticated by the receiving nodes before recording the changes in their respective binding caches. The CN will then send the packets straight to the new CoA of the MN.

As mentioned previously, the MA1 at the previous network proxies for the HA, and hence will intercept any packet meant for the MN. Thus, if some packets (which were in transit during the handover process) reach the old CoA of MN when it has already moved on to a new CoA, the MA1 will redirect these packets to the new CoA. This ensures that while the MN sets up a new CoA, the packets send to the previous CoA are not lost.

While the MN remains attached to AR2, it might need to send intermittent binding updates to MA1 and CN to renew its registration before the expiry of the current registration lifetime. If the MN moves to a third foreign network, the MIPv6 with MAAH proceeds as follows:

- The MN now connects to a third access router AR3, and sends a binding update to MA2 (the mobile agent at its old access router).

- The MA2, in turn, will inform the same to MA1, in addition to registering the new CoA.

- When MA1 receives such a binding update via MA2, it infers that it no longer needs to serve the MN. Thus, it will either delete all information about the MN (if it is also serving some other nodes from same home network) or will destroy itself (if it was serving only that MN). Destruction of mobile agent will involve releasing the used resources at the MP and killing the agent process.

If MA1 does not receive any binding update from MN (directly, or via MA2) till the expiry of binding lifetime, the former assumes a network failure. In such a situation, MA1 sends a binding update to HA, instructing the latter to remove the binding for MN's CoA. On receiving acknowledgement from HA, MA1 either destroys itself or deletes information pertaining to the MN, depending on whether it is serving only one or more mobile nodes. The need for the mobile agent (MA1) at an access router previous to the last access router (MA2) is to maintain redundancy for the network usage information, which might be important for billing purposes.

After recovering from such a network failure, the MN will have to send binding update directly to HA which shall then respond with regular binding acknowledgement and send a new mobile agent to the concerned router, as already discussed. The connection with CN will have to be re-established accordingly. The modified protocol is illustrated in Figure 3.1.

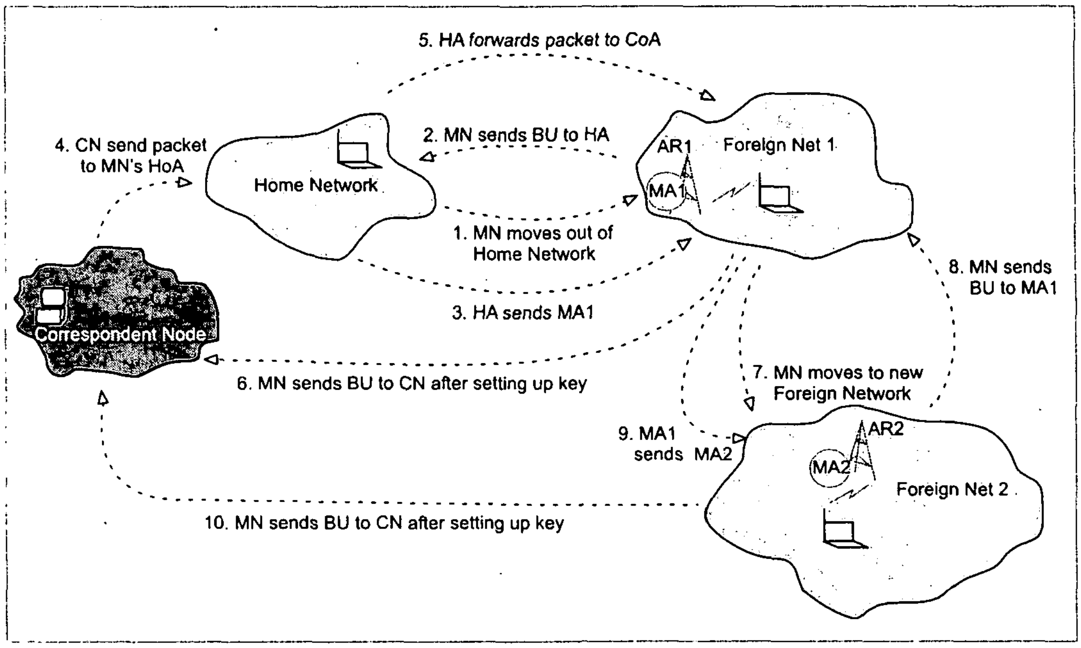

5. HA forwards packet to CoA
4. CN send packet to MN's HoA
2. MN sends BU to HA
Home Network
AR1
Foreign Net 1
MA1
1. MN moves out of Home Network
8. MN sends BU to MA1
3. HA sends MA1
Correspondent Node
6. MN sends BU to CN after setting up key
7. MN moves to new Foreign Network
9. MA1 sends MA2
AR2
MA2
Foreign Net 2
10. MN sends BU to CN after setting up key

Figure 3.1: MIPv6 with MAAH – interchange of messages

3.2.3. Managing Authentication

The authentication of messages amongst the entities is pre-requisite for the flow of MIPv6 protocol. This can be achieved by means of certain security scheme among the involved entities. A security scheme may include an authentication algorithm, a key that the algorithm uses, a lifetime over which the key will remain valid, a lifetime over which the destination agrees to use the algorithm, and a list of source addresses that are authorized to use the scheme. In order to save the space in the packet (headers), IPSec arranges for each receiver to collect all the details about a security scheme into an abstraction known as Security Association. Furthermore, IPSec does not restrict the user to a specific encryption or authentication algorithm [9].

As in MIPv6, each mobile node must have a security association with its home agent in the MAAH scheme too. The mobile agent (which belongs to the home network) should also have a security association with the home agent. The mobile agent, coming as it is from the HA, can use its security association with the HA to set up a new security association with the MN. This makes communicaiton between the home agent, and the mobile node, as well as between the mobile agent and the mobile node secure and authentic. Apart from security associations, the mobile agent will store the information about the previous care-of address of the MN, the current care-of address, and the time for which the services of the given network used.

It is possible to set up pre–configured security associations between the HA and the MN, between the HA and the MA, and thereby between MN and MA since they all belong to the same network (administrative domain), but the same may not be possible with the CN. The CNs will, at most of the time, belong to different administrative domains, and setting up pre–configured security association across various entities in diverse administrative domains will be next to impossible. A security mechanism is, however, needed between the MN and CNs so that the binding updates sent by MN can be authenticated. This is accomplished in MIPv6 by setting up security keys on the fly using Return Routability Procedure (RRP).

In MIPv6, the RRP involves the MN sending two messages—Home Test Init (HoTI) and Care-of Test Init (CoTI)—to the CN; the first one via the HA and the other directly. The CN responds to these messages by sending the Home Test (HoT) and Care-of Test (CoT) messages respectively; once again the first via the HA and the other straight to the MN. These messages contains one token each (Home Keygen token and Care-of Keygen token respectively), which are used to generate the key between the CN and MN to be used for message authentication.

In MIPv6 with MAAH, apart from the mobile agent at the previous access router being responsible for registering the MN, the former is also involved in the Return Routability Procedure.

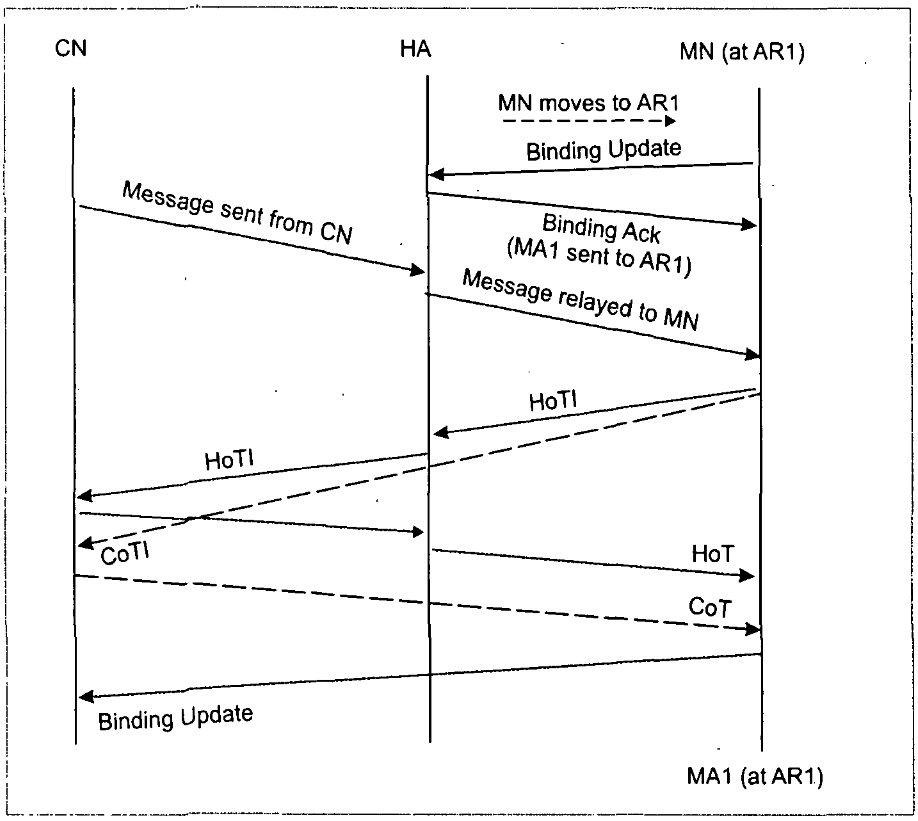


Figure 3.2: Message interchange between various entities in the modified scheme, as MN moves out of home network to the first foreign network

The RRP in MIPv6 with MAAH proceeds as follows

- The first time the RRP is performed for any MN-CN pair, the HoTI message from MN to CN is relayed through the HA as in base MIPv6. The corresponding HoT message from the CN reaches the MN via HA.

- The next time onward, these messages use the mobile agent at the previous access router instead of the HA. Thus, when MN moves to AR2, the HoTI and the corresponding HoT messages should travel via MA1 at AR1. Since the path between the CN and MN at AR1 was optimized before MN migrated to AR2, the path to CN via AR1 will be shorter after the migration than that via the HA. Hence, the time needed for setting up the key will be shortened.

The interchange of messages as the MN moves from HA to AR1 are seen in Figure 3.2, while those when the MN moves beyond AR1 are seen in Figure 3.3. The figures show the message exchange till a key is set up between the MN and the CN, and a Binding Update message sent to the CN. Beyond this, the CN-MN pair can communicate directly without involving any intermediary.

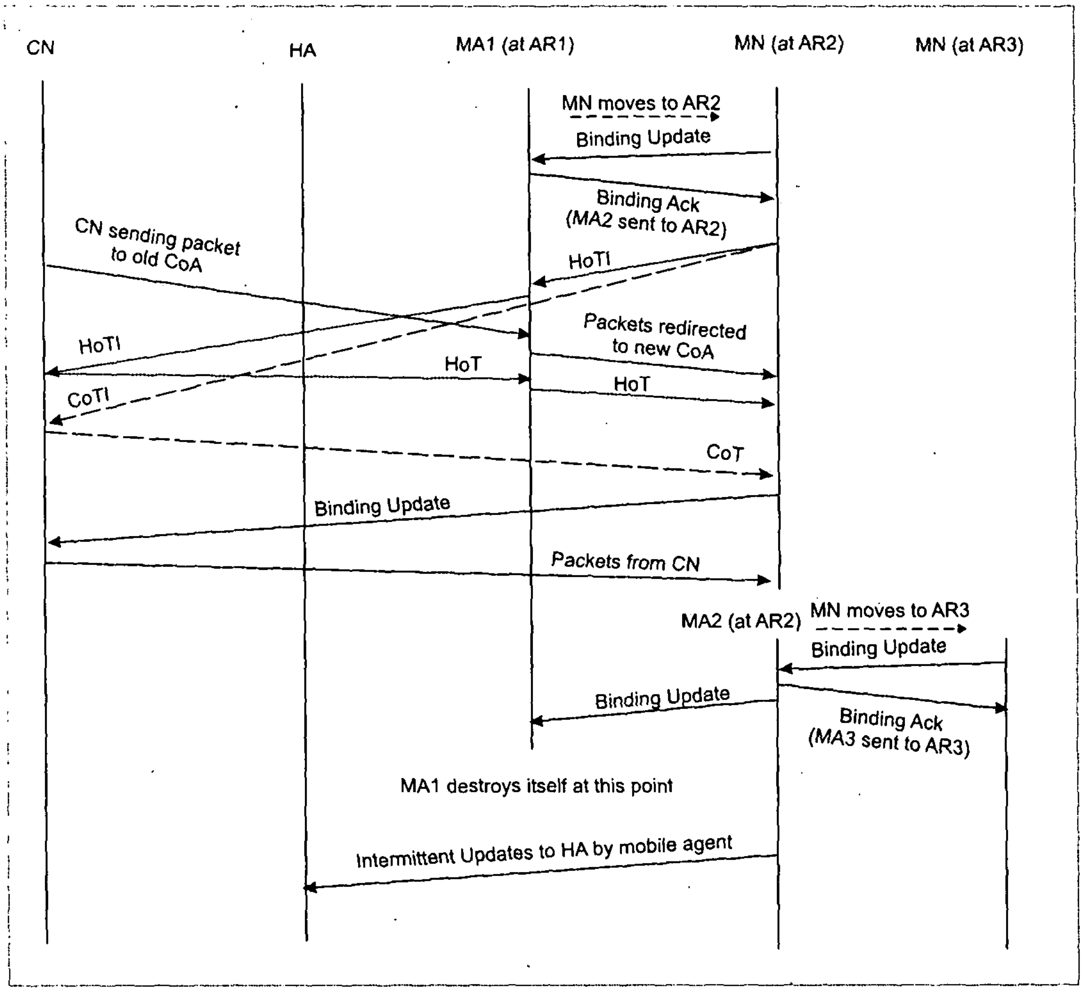


Figure 3.3: Message interchange between various entities in the modified scheme as MN moves out of one foreign network into another

```
When MN moves out of home network the first time
PROCEDURE_MN (When MN moves from HA to AR1)
    If  time_interval ≥ binding_update_interval then
       Send binding update to HA
    Endif

    If number_correspondent_node !=0 then
       If  key_exists_CN =false or key_expired =true then
          // perform RRP to set up the key
          Send Home Test Init (HoTI) message to CN via HA
          Send Care-of-Test Init (CoTI) message to CN directly
          On receiving Home Test (HoT) and Care-of Test (CoT) messages, calculate session key
          Send Binding Update to CN along with session key (Message Authentication Code)
       Endif
    Endif


When MN moves from one foreign network to another
PROCEDURE_MN (when MN moves from AR1 to other ARs)
    If  time_interval ≥ binding_update_interval then
        Send binding update to MA at previous AR
    Endif

    If number_correspondent_node!=0 then
        If  key_exists_CN =false or key_expired =true then
           // perform RRP to set up the key
           Send Home Test Init message to CN via MA in previous AR
           Send Care-of-Test Init message to CN directly
           On receiving Home Test and Care-of Test messages, calculate the session key
           Send Binding Update to CN along with session key (Message Authentication Code)
        Endif
    Endif
```

Figure 3.4: Operations performed by MN as it moves about

```
PROCEDURE_HA
    if incoming_packet = data_packet and destination_address==IPAddr_of_MN then
         \\ Check database for the COA of MN
         redirect packet to MN
    Endif

    If incoming_packet=HoTI_message then
         Authenticate HoTI_message
         Remove authentication data
         Redirect HoTI_message to CN
    Endif

    If incoming_packet=HoT_message then
         Add authentication data to HoT_message
         Redirect HoT_message to CoA of MN
    Endif

    If incoming_packet=binding_update then
         If binding_authentication = true then
             Update the binding of MN with this new CoA
             Record the Binding_Lifetime
             If MA present at new AR then
                 \\Send Home_Address of MN to MA at AR
                 Transmit Binding_info_from_HA to MA
                 Record security_association with MA
             Else
                 Create MA storing Home Address of MN
                 Set Info_packet interval (interval for updating the HA by MA)
                 Record security_association with MA
                 Send MA to AR
             Endif
         Endif
    Endif

    If incoming_packet=binding_update_from_MA then
         Update binding cache for MN(s)
         Send ack_packet to MA if specifically asked for
    Endif
```

Figure 3.5: Operations performed by HA to support mobility

```
PROCEDURE_MA
    If incoming_packet=binding_info_from_HA or binding_info_from_MA then
        //This happens when information about a MN reaches an existing
        //MA in the new netwok
        Create MN_info_array (storing network usage information of MN)
        Record Security association with MN.
        Record security association with HA
    Endif

    If incoming_packet=binding_update and security_assn=true then
        If new_COA=old_COA then
            Update binding_lifetime
        Else
            Update MN_COA to new_COA
            Increment HOP by 1
            Add MN_COA to MN_info_array
            If another mobile agent from same home network exists at new AR Then
                    Send Transmit binding_info_from_MA to the new AR
            Else
                    Create and send a MA to the new AR
            Endif
        Endif
    Endif

    If binding_lifetime ≤ 0 and binding_update = false then
        //Assume network failure and send data to HA
        Send binding_update (data from MN_info_array) to HA
    Endif

    If time_interval ≥ binding_update_interval then
        Send binding_update (data from MN_info_array) to HA
    Endif

    If incoming_packet=ack_packet (acknowledgement of BU from HA) then
        If HOP=2 (i.e., the MN does not need this MA)
            If no_MN=1 (MA was supporting only the current MN) then
                Delete MA (self)
            Else
                Delete elements of MN_info_array (pertaining to MN)
            Endif
        Endif
    Endif

    If incoming_packet=data_packet then
        If HOP=0 (i.e., the MN is at the current AR) Then
            Deliver to MN
        Else
            Redirect to MN at new_AR
        Endif
    Endif

    If incoming_packet=HoTI_message then
        Authenticate HoTI message
        Remove authentication data
        Redirect HoTI_message to CN
    Endif

    If incoming_packet=HoT message then
        Add authentication data to HoT message
        Redirect HoT_message to CoA of MN
    Endif
```

Figure 3.6: Operations performed by MA to proxy for HA

The operations performed by the various entities involved are listed in Figures 3.4, 3.5, and 3.6 as procedures. The function of CN remains mostly unchanged, except when a mobile agent is used for the MN registration, it should respond to a HoTI message with a HoT message via the old CoA of the MN (i.e., via the previous access router) rather than via the HA as envisaged in the base protocol

3.3. Comparison with MIPv6

In MIPv6, the process of handover includes setting up of a new care-of address, getting it registered with its HA, completion of return routability procedure, and sending binding updates to CN. The handover process will involve the HA (which might be at a distance), and thereby increase latency. The handover latency t_{ho} can be defined as

$$t_{ho} = t_{pd} + t_{CoA} + t_{regd} + t_{ack} + t_{rrp} + t_{bu} \qquad (3.1)$$

where

t_{pd} is the time for prefix discovery in visited network

t_{CoA} is the time to establish the care-of address

t_{regd} is the time to register the new address with the HA

t_{Ack} is the time for the registration acknowledgement to reach MN from HA

t_{rrp} is the time to set up a key with CN, and

t_{bu} is the time to send the binding update to CN

The contribution of the components t_{pd} and t_{CoA} are small compared to the rest as these involve only a single hop to the access router across the network. The contributions of $t_{regd.}$ t_{ack} and t_{rrp} will dominate t_{ho} as the messages involved will have to traverse a path to/from the HA. Handover latency in MIPv6 can hence be reduced if these three components can be reduced.

In the MIPv6 with MAAH scheme, let the corresponding values be t'_{pd}, t'_{CoA}, t'_{regd}, t'_{ack} and t'_{rrp}. Comparing the MIPv6 with MAAH to the base protocol, it can be summarized that –

- The values of t'_{pd} and t'_{CoA} will remain equal to t_{pd} and t_{CoA} respectively. The messages involved in prefix discovery and to establish the CoA does not need to travel beyond the current foreign network.

- The values of t'_{regd}, t'_{ack} and t'_{rrp} can be significantly smaller than t_{regd}, t_{ack} and t_{rrp} respectively. This is because the corresponding messages now have to traverse a much shorter path to/from the mobile agent at the previous access router which is likely to be much closer than the HA.

Of course, there will be a finite time required to get the mobile agent started at the new access router. However, this being done asynchronously with the MN registration process, will not add to handover latency. On the other hand, if there is already a mobile agent running at the access router serving the given home network, then only the information pertaining to the current MN needs to be transferred. Thus, the handover latency in the MAAH scheme will be smaller as compared to that in the original protocol.

3.3.1. Estimated Benefit of the Scheme

The use of MIPv6 with MAAH does not reduce the number of control messages required for mobility management. It, however, certainly reduces the number of hops these messages need to traverse. Furthermore, instead of sending individual messages, certain messages are aggregated to communicate information about several MNs to their corresponding HA from the mobile agent. These aggregate messages are sent asynchronously, thereby not contributing to the handover latency. In this sub-section, an estimation of the benefits accrued from the proposed scheme is undertaken, considering the number of packet hops as the metrics.

At a given network, let it be assumed that in time t there are n_1 mobile nodes coming in from network 1, n_2 nodes coming in from network 2, and so on. Let it also be assumed that the network 1 is h_1 hops away from the current network, network 2 is h_2 hops away, and so on. Thus, in time t, the total number of handovers is given by

$$ho_{tot} = \sum n_i \, .$$

Each handover is characterized by a binding update message and the corresponding binding acknowledgement to and from the home agent respectively. In terms of number of packet hops, the handover of mobile nodes from k different networks would require

$$2h_1n_1 + 2h_2n_2 + 2h_3n_3 + ... + 2h_kn_k = 2\sum_k h_in_i \text{ packet hops}$$

The number of packet hops needed for mobility management per unit time is

$$h_{tot\_mip} = \frac{2}{t}\sum_k h_in_i. \tag{3.2}$$

If a similar situation is considered for the MAAH scheme, the binding updates and the corresponding binding acknowledgements will need to travel only a single hop to the mobile agent at the previous access router (if it is assumed that the access routers are connected to one another). Apart from this, the registration process would also include an intimation to the mobile agent at the access router the mobile node was connected to, before it moved in to the previous access router. Thus the number of packet hops in time t would be:

$$2(n_1 + n_2 + n_3 + ... + n_k) + (n_1 + n_2 + n_3 + ... + n_k) = 3\sum_k n_i.$$

The packet hops per unit time in the modified scheme would be

$$h_{tot\_maah} = \frac{3}{t}\sum_k n_i \tag{3.3}$$

For the example considered above, the number of packet hops for mobility management in case of MAAH scheme as compared to base MIP is given by

$$h_{maah/mip} = \frac{h_{tot\_maah}}{h_{tot\_mip}} = \frac{3\sum_k n_i}{2\sum_k h_in_i} \tag{3.4}$$

The packet sent to HA by the mobile agent to update the former about all the mobile nodes serviced by the latter is not considered here, as this does not contribute to handover latency. The value in of $h_{maah/mip}$ in (3.4) shows that the modified scheme will always have an advantage over the existing protocol, provided the mobile node is more than one hop away from its home agent.

To get a clearer idea about the gain, if 5 mobile nodes are considered which comes into a given foreign network in unit time from the same home network 10 hops away, the total number of packet hops needed to register the CoA with the HA using MAAH scheme would be 0.15 of that needed for base MIP.

In expression (3.4) it had been considered that the previous mobile agent was one hop away from the current access router. If the previous mobile agent is h'_i hops away from the current access router for the i^{th} mobile node, then the expression would take the form

$$h'_{maah/mip} = \frac{3\sum_{k} h'_i n_i}{2\sum_{k} h_i n_i} \qquad (3.5)$$

With $h'_i << h_i$, the benefit of using the modified scheme would still be substantial.

In the above analysis, the time required to move the mobile agent to new AR is not considered. If the mobile agent is not present at the next AR, it has to be moved to that AR, which will require certain number of hops (which will be small – as it is from the previous access router to the new one). But this does not affect the registration process and hence do not add to the handover latency. Moreover, here only the reduction in packet hops for the new CoA registration of the MN at its mobile agent is considered, the latter functioning as proxy for the HA. There will also be reduction in packet hops in HoTI and corresponding HoT messages as they can now travel via the mobile agent at the previous router rather than the distant HA, which has not been considered in the above estimation.

3.4. Simulation and Results

Simulation experiments were performed to study the performance of the MAAH scheme vis-à-vis the base MIP. Two different types of network topologies were considered. For the first case, it was a network having hierarchical arrangement of routers, while in the next; it was a more regular and planer arrangement of access routers.

3.4.1. Simulation Topology 1

In the first case, a two level hierarchical topology as shown is Figure 3.7 was considered. In this topology, seven foreign networks (the figure shows only three) were considered, apart from the home network and the network where the CN was stationed. In each of these seven networks, there was one central router with two access routers connected to the central routers. The MN was made to move out of its home network and move towards the CN. The simulation parameters considered are listed below:

- Separation between the nearest ARs was set to 300m
- Separation between the central routers was set to 600m
- Domain radius of the ARs was set at 155m
- Propagation delay was set to 2μs
- Processing delay at each router was set to 1ms
- Link bandwidth of the wireline networks was set to 2Mbps.

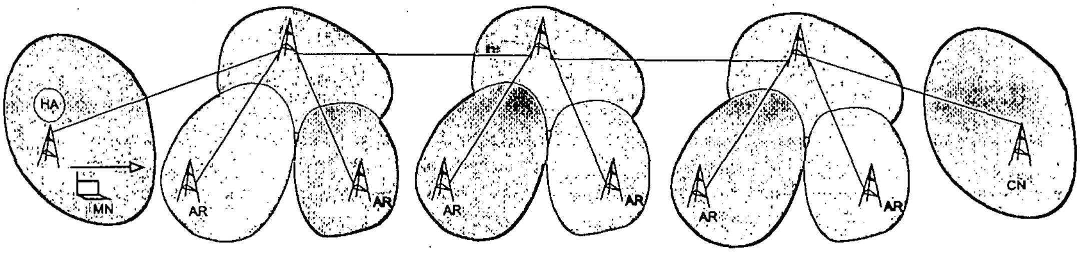


Figure 3.7: Hierarchical network topology for MAAH Simulation (topology 1)

In this simulation to study the performance of the two schemes, the individual protocols were executed as follows:

- In the base MIP simulation, the new CoA had to be registered with the HA following every change of access router. These registrations were followed by return routability procedure to set up a fresh key with the CN for route optimized operation. In the absence of router changeover, MN registration at HA needed renewal before the current registration expired.

- For MAAH scheme, the registration of the new CoA was done by the mobile agent at the previous access router. Given the topology, the previous access router could be two or three hops away depending on the current position of the MN. The registration renewals also involved only the mobile agent at the previous access router.

The comparative handover delays as the MN moved out of its home network towards the CN for the two protocols are plotted in the Figure 3.8. The results are of course, topology dependent.

The registrations in MIP (as also in MAAH) has finite lifetime. The registrations thus call for renewal before the expiry of this lifetime, even if there is no change in CoA. The horizontal line between the successive spikes show the time required for such registration renewals. Such renewals were not accompanied by return routability procedure (as there was no change of CoA at CN's binding cache), and hence required lesser time for their completion. In both MIP and MAAH protocols, there were periodic increases in this registration renewal delay, seen as spikes in Figure 3.8. These were the handover delays when the MN changed the supporting access router and acquired a new CoA. These required setting up of new key before the binding update could be sent to the CN.

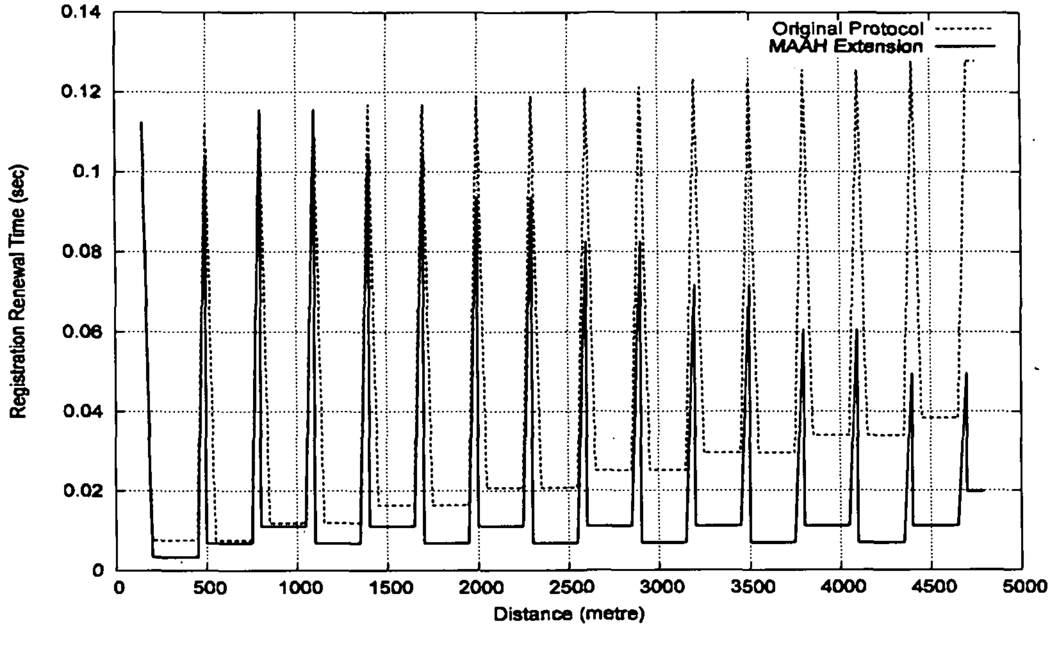


Figure 3.8: Comparative plot for MIPv6 and proposed MAAH scheme, showing handover delay as the MN moves from its home network towards the CN

In case of MIP, the time needed for every new registration increased as is seen in Figure 3.8. This is because in the topology considered, the distance between the HA and the MN went on increasing with the latter's movement, resulting in an increase in the number of hops traversed by HoTI and HoT messages, though there was a decrease in the same for CoTI and CoT messages. This increase in number of hops for HoTI and HoT messages increased the time required for completion of return routability procedure, resulting in a higher handover delay. Because of the continuous increase in HA-MN distance, even the CoA renewals required more time, as the MN moved towards the CN.

In case of MAAH scheme, the mobile agent at previous access router took care of registration. There was hardly any change in the distance from previous access router with MN movement (which varied between two and three hops). Then again, the MN moved closer to CN with time, requiring lesser number of hops for both groups of return routability procedure messages. Unlike the increasing number of hops for HoT and HoTI messages in the base protocol due to the growing CN-HA distance, the CN-MA distance in case of MAAH scheme actually decreased with MN movement. This resulted in successively lesser handover delay as MN moved towards its CN. The messages for renewal of registrations, in case of expiry of previous registration without MN movement, needed to traverse two or three hops in each case, thus remaining approximately same and not showing a continuous increase as in the previous case.

3.4.2. Simulation Topology 2

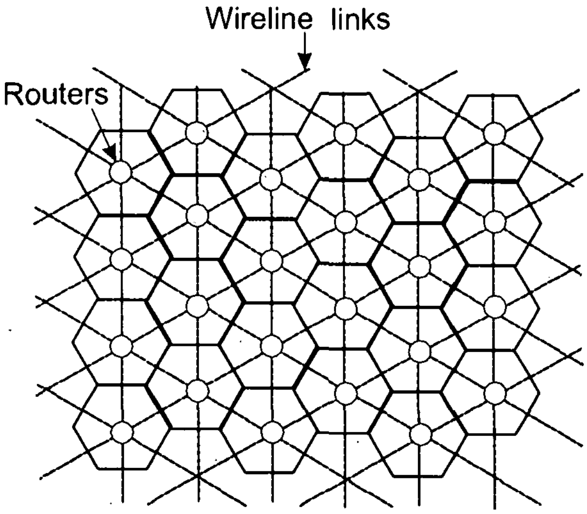


Figure 3.9: Simulation Topology (Topology 2)

In the second case, the simulation studies were carried out on a cellular like network topology shown in Figure 3.9. Though the mesh-like wireline connectivity among the base stations is not found in practice today, the rapid growth in the population of mobile devices will surely require smaller cells to allow more frequency reuse- possibly resulting in some topology similar to the one considered in the figure in not too distant a future. This might be the basestation connectivity scenario at a particular hierarchy within a given cluster, with different clusters connected to each other through a gateway node.

The handover latency was calculated as function of distance the mobile node is away from its home agent. The handover latency was estimated for both, the original MIPv6 and the proposed MAAH scheme assuming three different patterns of MN movement. The movement patterns considered were –

i. MN moving perpendicularly away from the line joining MN and HA (Figure 3.10A),

ii. MN moving diagonally away from HA (Figure 3.10B), and

iii. MN moving along the line joining HA and CN towards CN (Figure 3.10C).

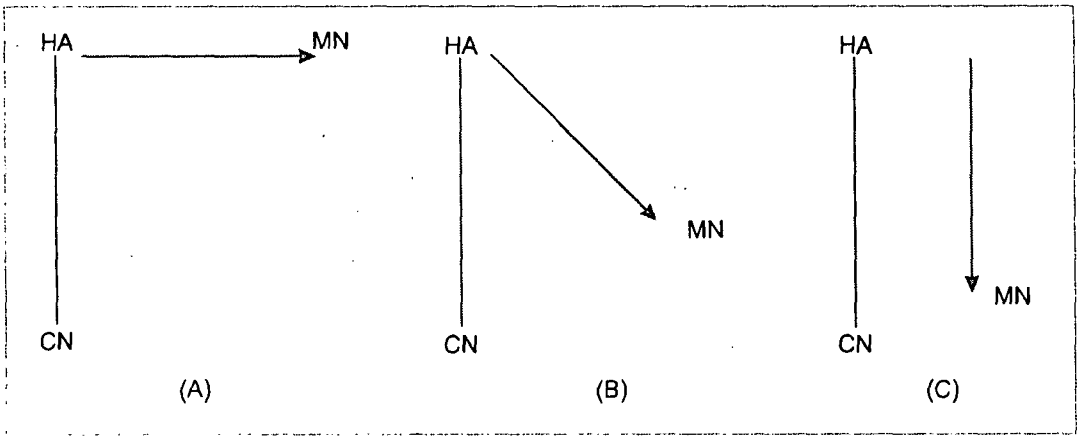


Figure 3.10: MN Movement Scenarios Simulated

The simulation topology had the following features:

- The cells were arranged in an array of 10×10 cells as in Figure 3.9
- The diameter of each cell was set to 250 metres, with access router located at the center
- The bandwidth of wireline links was set to 2 Mbps

- Processing delay at each router was set to 1 ms
- Propagation delay was set to 2 μs

The delay in completion of handover process was considered every time the MN connected to a new access router. This handover delay included the time to register the new CoA with home agent, the time consumed to send the HoTI and CoTI messages to the CN, to receive the corresponding HoT and CoT messages and ultimately to send the binding update to the CN from the MN. For the case of registration with the mobile agent, the agent was assumed to be at the previous router. In addition, the time consumed for the renewal of existing registrations before the same expired was also considered in the simulation.

The simulation results, plotted as the registration renewal time (either due to expiry of existing registration or due to change in CoA) versus the distance of MN from its HA (in metres) are seen in Figures 3.11, 3.12 and 3.13. These correspond to movement scenarios of Figures 3.10A, 3.10B and 3.10C respectively, and show significant improvement for the MAAH scheme vis-à-vis MIPv6.

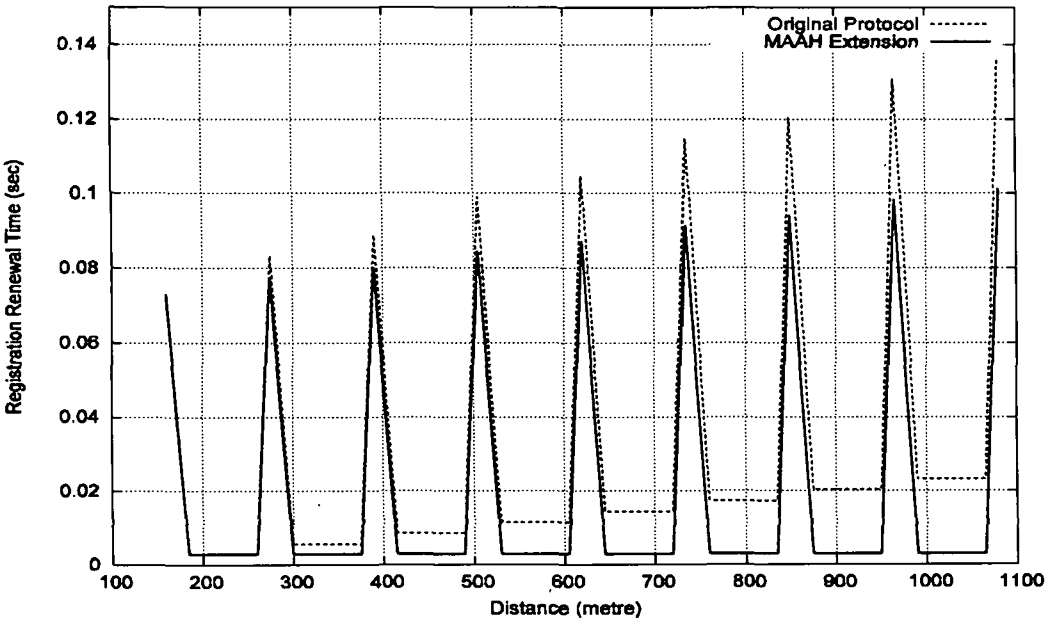


Figure 3.11: Comparative plot of original protocol vis-à-vis modified protocols when the MN is moving perpendicular to the line joining HA and CN

The distance between the MN and its HA on one hand and that between the MN and the CN on the other hand always increased as the MN moved perpendicularly away, as shown in Figure 3.10A. However, in case of MAAH protocol, the distance of the MN from its mobile agent (which acted as a proxy for the HA) always remained constant as the latter was considered to be stationed at the previous access router. Of course, the distance between the MN and the CN increased as the MN moved outwards. Thus for both schemes, an increased time was consumed for registrations of new CoAs, as the MN moved away from its HA. Figure 3.11 shows this increase. However, the increase is smaller for the MAAH scheme, since initial registration with mobile agent, and sending HoTI and HoT messages required lesser time due to the proximity of the mobile agent. In addition, the time required for renewal of existing registrations in MAAH scheme does not show any increase due to the closeness of the mobile agent. The same shows an upward trend for MIP owing to the increasing distance of MN from its HA.

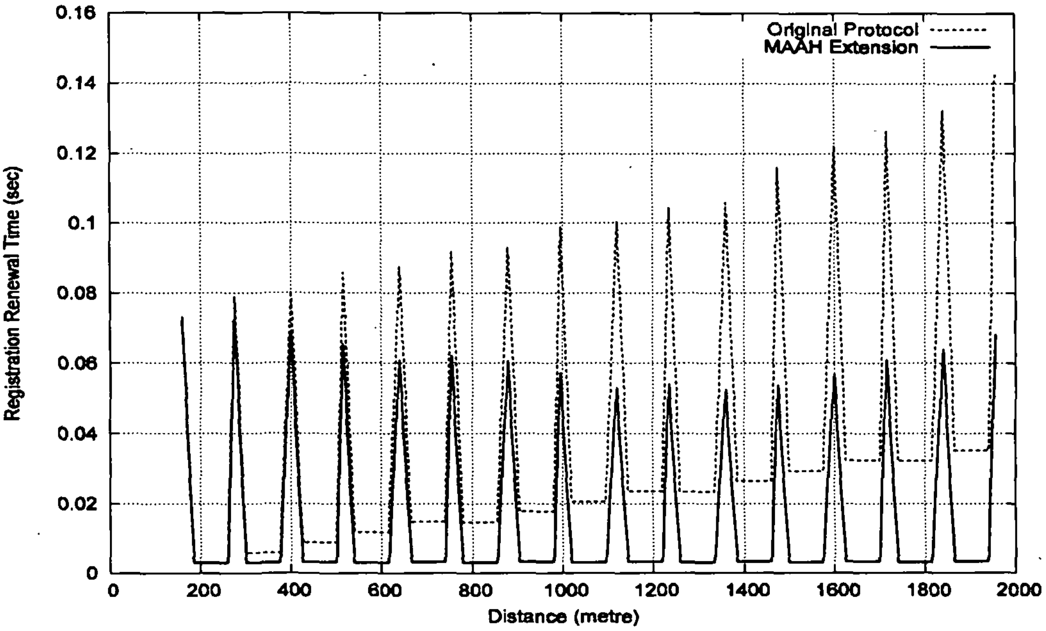


Figure 3.12: Comparative plot of original protocol vis-à-vis modified protocols when the MN is moving diagonally away from the line joining HA and CN

In case of Figure 3.12 (for movement pattern of Figure 3.10B), the MN initially moved closer to the CN in its diagonal trail, and then moved away. This explains the initial dip and later increase in handover latency for the MAAH scheme. However, for the original protocol, the messages had to pass through the HA, whose distance from MN always increased with the latter's movement. This resulted in the gradüal increase in handover latency with distance for the original scheme. This increase is smaller in the beginning as compared to Figure 3.11 because the MN-CN distance decreased initially, thereby requiring a smaller time for the CoTI message to CN, CoT message from CN and ultimately the BU message to CN. The renewal of registrations of existing CoAs showed the same trend as before.

In case of Figure 3.13 (movement pattern of Figure 3.10C), the handover latency for new registrations show a sharp decrease for the MAAH scheme. This is because the home registration of MN in the MAAH scheme does not depend on HA but on the mobile agent at the previous router. Moreover, the distance from the CN got reduced as the MN moved towards it. For the original protocol there is an increase in the latency, though gradual. This is because while the MN-CN distance decreased, the MN-HA distance actually increased.

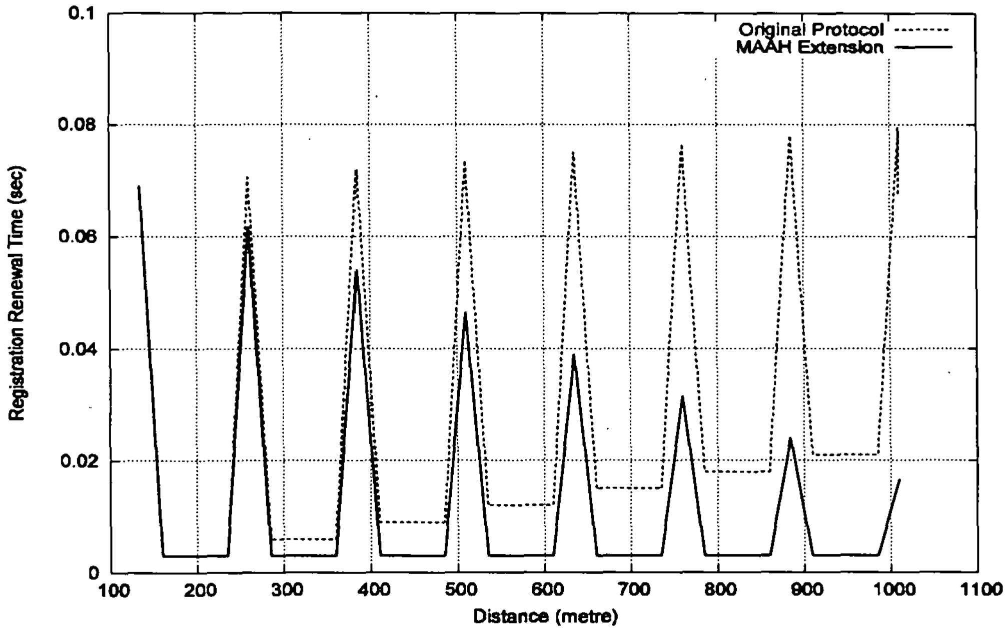


Figure 3.13: Comparative plot of original protocol vis-à-vis modified protocols when the MN is moving towards CN from HA

3.5. Summary

This chapter of the thesis discussed a modification to MIPv6 whereby mobile agents are introduced to take care of MN registration at foreign networks, thereby attempting to reduce handover latency, and hence improve performance. An analysis is also made to show the advantage of MAAH scheme for a given scenario, which indicated a decrease in handover latency in the new scheme. To study the performance of this MAAH scheme, simulated experiments were also conducted. The results of these, though highly simulation topology depenedent, show a significant reduction in handover latency for the MAAH scheme, as compared to the base protocol. The simulation using topology 1 showed an average decrease of 43.63% in registration renewal time; while for topology 2, the corresponding values were 35.73%, 59.09% and 54.19% for the perperdicular, diagonal and linear movements of the MN (Figures 3.10A, 3.10B and 3.10C) respectively.

Chapter 4

Transparent Multihomed Mobile IP

4.1. Introduction

The presence of multiple interfaces in mobile devices is becoming more of a norm rather than an exception. At the same time, more and more areas are increasingly being brought under the support of multiple networks, often resulting in availability of multiple access technologies over a given region. This feature is exploited by the likes of Next Generation Communication Systems (NGWS) [35] which integrate the best features of the individual networks. In IETF terminology, the provision of multiple network interfaces equipped with multiple network addresses is referred to as multi-homing [36][37].

In an all-IP scenario, an IP based solution will be required for integrated management of the multi-homed nodes. In its current form, MIPv6 does not support multihoming, though certain extension has been proposed for the same. This *Mobile IP for Multiple Interfaces* (MMI) [39] extension introduced the *Load Balancing Mobility Option* to inform the CN, when MN is the sender, about the IP addresses of the MN interfaces. Conversely, if CN is the sender, the Load Balancing Mobility Option is used to inform the CN about the addresses of the MN interfaces and the proportion of the packets to be sent to each of these. However, the proposed extension, while allowing for load balancing across the available network interfaces, does not take into consideration the ever changing network characteristics at those interfaces. The proportion of packets across the interfaces is decided by MN and cannot be dynamically adjusted by CN, when CN is the sender.

A solution is therefore discussed here, which allows for load balancing – taking into account the transient nature of network characteristics at different available interfaces, without adding appreciable overhead to the existing protocol. The scheme allows the use of multiple HoAs and CoAs without coupling the two, thereby also making it robust to HA failures.

4.2. Advantage of Simultaneous Use of Multiple interfaces

In order to justify the use of multiple interfaces of a mobile node, an analysis for the available bandwidth in case of multi-homed mobile nodes due to aggregation vis-à-vis that in case of single-interfaced node is presented here.

It is assumed that the total packets sent to the only interface of single-interfaced mobile node in time t be m, the fraction of the packets lost on the average due to transmission and other errors be p, the average packet size (considering only the payload) be x, and the average time the MN remains under the same access router be t sec. Δt is considered to be the handover latency (the time needed to complete a handover).

Thus the total number of packets reaching the MN interface in time t is

$$m(1-p)$$

and the total amount of data reaching MN interface in the same time is

$$xm(1-p) \text{ bytes}$$

The total amount of data reaching MN in unit time is, therefore,

$$\frac{xm(1-p)}{t} \text{ bytes}$$

However, of the total bytes reaching MN interface, no user data (except control messages) will be received during the handover (assuming hard handoff). Thus the total data accepted at MN in time t is

$$\frac{xm(1-p)}{t}(t-\Delta t) \text{ bytes}$$

The effective bandwidth at the MN interface is, therefore

$$W_{eff\_s} = \frac{xm(1-p)}{t^2}(t-\Delta t) \text{ bytes/sec} \tag{4.1}$$

The above expression (4.1) gives the effective bandwidth at MN, where the MN is equipped with only a **single interface**.

In case of **multiple interfaced** node too, it is assumed that every t secs there will be a handover. Let m_i be the number of packets sent to interface i in time t. Let p_i be the fraction of packets lost in transit, and Δt_i be the handover latency at interface i. The number of packets reaching interface i per unit time is

$$\frac{m_i(1-p_i)}{t}$$

If, as before, x is the average packet size, then the amount of data reaching the interface i in unit time is

$$\frac{xm_i(1-p_i)}{t} \text{ bytes}$$

Thus, the data accepted at interface i in time t, taking into account the handover latency Δt_i (considering hard handoff)

$$\frac{xm_i(1-p_i)}{t}(t-\Delta t_i) \text{ bytes}$$

Out of a total of n interfaces, while one interface is having a handover, $(n-1)$ other interfaces will carry on with the data transfer. The total amount of data accepted at MN through all its n interfaces in time t is

$$\frac{xm_i(1-p_i)}{t}(t-\Delta t_i)+\sum_{j\neq i,j=1}^{n} xm_j(1-p_j) \text{ bytes}$$

$$=\sum_{k=1}^{n} xm_k(1-p_k)-\frac{xm_i(1-p_i)\Delta t_i}{t} \text{ bytes}$$

where k runs over all the available interfaces, while i is the interface which performs the handover in the interval t.

Thus, the effective bandwidth at MN would be (using the multiple interfaces)

$$W_{eff\_m}=\frac{1}{t}\left[\sum_{k=1}^{n} xm_k(1-p_k)-\frac{xm_i(1-p_i)\Delta t_i}{t}\right] \text{ bytes/sec} \qquad (4.2)$$

For simplification, if it is assumed that $\sum_{k=1}^{n} m_k = nm$, and $m_i = m$, then

$$W_{eff\_m}=\left[\frac{xnm}{t}\sum_{k=1}^{n}(1-p_k)-\frac{xm\Delta t_i}{t^2}(1-p_i)\right]$$

$$=\frac{xm}{t^2}\left[nt\sum_{k=1}^{n}(1-p_k)-\Delta t_i(1-p_i)\right]$$

$$\text{or, } W_{eff\_m}=\frac{xm}{t^2}\left[nt\sum_{k\neq i}(1-p_k)+(nt-\Delta t)(1-p_i)\right] \text{ bytes/sec} \qquad (4.3)$$

Comparing expressions (4.1) with (4.3), the second term in (4.3) is greater than the value in (4.1) (assuming $p = p_i$). Thus the total bandwidth given by (4.3) will be greater. To visualize the benefits achieved by using the multiple interfaces simultaneously, W_{eff-m} / W_{eff-s} is plotted versus t and is shown in Figure 4.1. For the plot, it is considered that Δt=4 sec, p=0.1, r=50 where r is the number of packets sent per unit time, x=1500, n=2, and m=t×r.

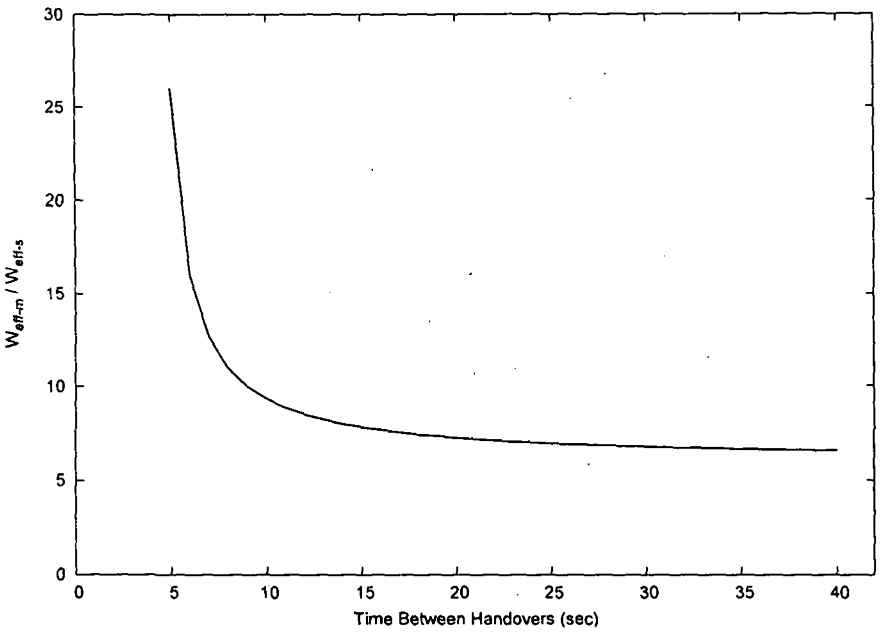


Figure 4.1: Plot of W_{eff-m} / W_{eff-s} versus t, time between successive handovers

With limited range of frequencies available, the cells will become smaller to support the increasing number of mobile devices, resulting in a reduced value for *t* (average time between handovers). However, due to required signaling, there will be no corresponding reduction in the handover latency Δ*t*, making Δ*t* comparable to *t* and resulting in the drop in W_{eff}. Thus, one must consider the use of multiple interfaces not only for enhanced reliability and seamless connectivity, but for increase in the effective bandwidth through aggregation. This is borne out by the exponential increase in W_{eff-m} / W_{eff-s} with decreasing *t*, especially at lower values of *t* (Figure 4.1).

4.3. Proposed Scheme

The proposed scheme – *Transparent Multihomed MIPv6* (TMMIPv6) - incorporates minor modifications to MIPv6 so as to support node multi-homing. This scheme envisages to

1. provide seamless mobility through horizontal and/or vertical handover, leading to ubiquitous Internet access
2. improve performance through bandwidth aggregation in scenarios where simultaneous usage of multiple interfaces is possible,

3. dynamic distribution of traffic across the available interfaces in proportions commensurate with current network conditions,
4. allow usage of multiple HoAs and CoAs without coupling the two, thereby making the protocol robust to HA failures,

The TMMIPv6 scheme proposes to achieve the above mentioned goals transparently, and without any change to the existing infrastructure, except at the communication endpoints. Towards this end, a *Convergence Module* (CM) is proposed to be introduced at layer 3 of the protocol stack.

4.3.1. Support for Multiple HoAs

The multi-interfaced mobile node may have more than one home address (HoA), registered at the same or separate networks. It is possible that a single network interface is associated with multiple HoAs, or conversely, several network interfaces share the same HoA. However, assigning a single HoA to a given network interface is more advantageous because the applications do not need to be aware of the multiplicity of home addresses [41].

To reap the full benefit of simultaneous use of multiple interfaces, the MN should have more than one HoA. This is because:

1. If all the interfaces are registered with the same HoA, it will not be possible to utilize the other interfaces once one interface gets attached to the home link. This is because if the proxy neighbour advertisements for the sole HoA are stopped, packets will always be routed to the interface attached to the home link.
2. If the proxy neighbour advertisements are not stopped, packets will never be routed to the interface attached to the home link.

Conversely, if the interfaces are registered with separate HoAs, while the proxy neighbour advertisements for one HoA is stopped (because the interface under question has returned to its home network), the same for other HoAs can continue (as the interfaces registered with these HoAs continue to be in foreign networks) as usual. However, multiple HoAs can create problems for the base protocol [27][28]:

1. The MN registers the CoA with it's HA when it moves to a new network. With more than one HoA, there would be an increase in control overhead if the MN now has to register all its CoAs with all its HAs.
2. For route optimized operation, the CoA is registered at the CN's binding cache. The key identifying the MN at CN's binding cache is its HoA. In the presence of multiple HoAs, the MN can no longer be identified by its HoA.
3. As for DNS, if all the HoAs of every single MN are to be included in the DNS, the latter might become unmanageable in the presence of numerous such MNs with their multiple HoAs.

The concept of a *Primary HoA* (PHoA) is therefore introduced. The MN will always register one of its CoAs at least with the HA corresponding to the PHoA. This PHoA can be included in the DNS, so that any CN interested in communicating with MN can send the packets to that IP address. The PHoA for every mobile node can be assigned initially, and should be invariant over node mobility.

There will be a single PHoA for every MN. This can then be the MN's identifier at CN's binding cache. Being an IP address, this PHoA will be unique over the Internet. In the face of multiple HoAs, the TCP connection will be maintained for the given flow with the help of this single static PHoA.

While PHoA identifies the MN, latter's multiple interfaces will also have to be identified uniquely. This can be achieved through the BID [41]..The binding update (BU) sent to the CN will therefore contain the PHoA, the BID for that interface, the HoA to which the CoA under question is registered, and of course, the CoA. The CM at CN will identify the node by its PHoA and the specific interface by the respective BID. Before updating the binding cache, the CN needs to authenticate the BU coming from the MN. This is done through the return routability procedure involving the HoA [27]. This requires that CN be informed of the HoA of the particular interface, in addition to the PHoA.

In this TMMIPv6 scheme, no interface needs to be permanently attached to a given HoA. An interface can use any of the available HoAs, and register its CoA at the corresponding HA. If all the interfaces are not being used,.all the HAs may not have the current CoA of the MN, except for the HA corresponding to PHoA. With multiple HAs available (corresponding to multiple HoAs) to assist in communication, the protocol will be more stable to HA failures. Once the communication starts, the PHoA is used for node identification. Thus a physical failure of even the HA corresponding to the PHoA will not effect the ongoing communication.

4.3.2. The Convergence Module

To manage the multiple IP interfaces and to perform dynamic adjustment of traffic flow from CN to the various interfaces of MN, as also the flow from MN interfaces to CN, a *Convergence Module* (CM) is introduced at layer 3 of the protocol stack. The function of the CM is to split a single flow across different interfaces at the sender, and accumulate the packets from the various interfaces to converge them into a singular flow at the receiver. The TCP connections are maintained based on the home address (or by PHoA in case of multiple HoAs) of the mobile node, which does not change with MN's movement.

In a foreign network, MN would connect to *Access Router* (AR) and would be assigned a CoA. The multiple interfaces may connect to different ARs and have distinct CoAs. At the network layer the packets will be sent or received at these topologically valid addresses, but these will be replaced by an invariant address for the consumption of the transport layer, so that the mobility is left transparent to the latter. The functions of the convergence module are-

1. to distribute the traffic across multiple interfaces,
2. to dynamically decide on the proportion of traffic at each interface, depending on network conditions prevailing at the links,
3. estimate the link characteristics to dynamically decide on the traffic distribution,
4. replace the topologically valid, but varying CoAs with the fixed HoA (or PHoA) for maintaining the TCP connection,
5. manage the handover at an interface by redistributing the traffic across the other interfaces till the handover at the given interface concludes.

To decide on the proportions of the packets it shall also be necessary to evaluate the suitability of the interfaces based on certain criteria. The possible criteria can be static ones such as – cost, security, etc. and dynamic ones such as – delay, available bandwidth, etc. While the static parameters are known a priori, it is crucial to make necessary provisions for estimating the dynamic ones.

The CM will therefore be required at both communication end points. The CM at the sender's end will estimate the link characteristics at the available interfaces with due assistance from the CM at the other end. When MN is the sender, the CM at this end will decide on the proportion of the packets to be sent through its available interfaces. On the other hand, with MN as the receiver, the CM at MN will inform its counterpart at CN about the available interfaces to which the packets pertaining to the flow can be distributed. Consequently, the CM at CN will decide on the proportion of packets to each of the MN interfaces.

In general, the CM at the sender's end will initiate the process of link quality estimation and distribute the flow accordingly, while that at the receiver's end will collect the packets pertaining to a given flow and pass them on to the transport layer after replacing the CoAs with the HoA (or PHoA in the presence of multiple HoAs), apart from assisting in link quality evaluation.

4.3.3. Estimation of Link Characteristics

To decide on the proportion of packets sent through/to a given interface, the CM at the sender will need to estimate the link characteristics at that interface. The CM at the sender's end will therefore initiate the estimation process. For this, the CM at the sender shall insert a timestamp (TS_S) into each of the outgoing packet (unless there is some restriction on this to reduce overhead). This timestamp is meant only for the CM at the other end, and can therefore be placed onto the *destination option* of IPv6 header. The CM at the receiver's end will proceed with link characteristics estimation as follows:

1. set up buffers, one for each MN interface, at the receiver of the flow,
2. record this timestamp (TS_S) in the respective buffer depending on the interface involved,

3. record the current time (TD_{Di}) in the buffer along with the packet size (PS),
4. replace the CoA with MN's HoA (or PHoA), and forward the payload to higher layer

Later on, when a packet is sent from the receiver to the sender (possibly a TCP ACK message) using the particular interface, the CM at the receiver will

5. calculate the delay (ΔT_D) between the time the last packet was received at this interface and the time when the current packet to be sent has been queued, where

   $$\Delta T_D = TS_{Df} - TS_{Di}$$

   TS_{Df} being the time when the outgoing packet is queued
6. include TS_S, PS and ΔT_D in the destination option of the IP packet to be sent through/to the particular interface

Once the CM at the original sender receives this packet, it will estimate the round trip time as

$$\Delta T = TS_r - (TS_s + \Delta T_D)$$

where TS_r is the timestamp when the current (ACK) packet is received back at the original sender. If

$$\Delta T_1, \Delta T_2, \dots, \Delta T_n$$

are the round trip times estimated at the n interfaces, then the CM at the sender can estimate the packets Δm_i of the total m packets to be sent using this particular interface i $(1 \le i \le n)$ as

$$\Delta m_i = \frac{m \times \left(1 - \frac{\Delta T_i}{\sum_{j=1}^{n} \Delta T_j}\right)}{(n-1)} \qquad (4.4)$$

Thus, if ΔT_i is large, i.e., the estimated Round Trip Time is large, the fraction of total packets sent though that interface would be small, and vice-versa. The calculation for

ΔT is done by the same module that had originally set the value for TS_S thereby avoiding the need for synchronization of clocks between CN-MN pairs.

The proposed interactions between the CMs at MN and CN for link quality estimation are shown in Figures 4.2 and 4.3.

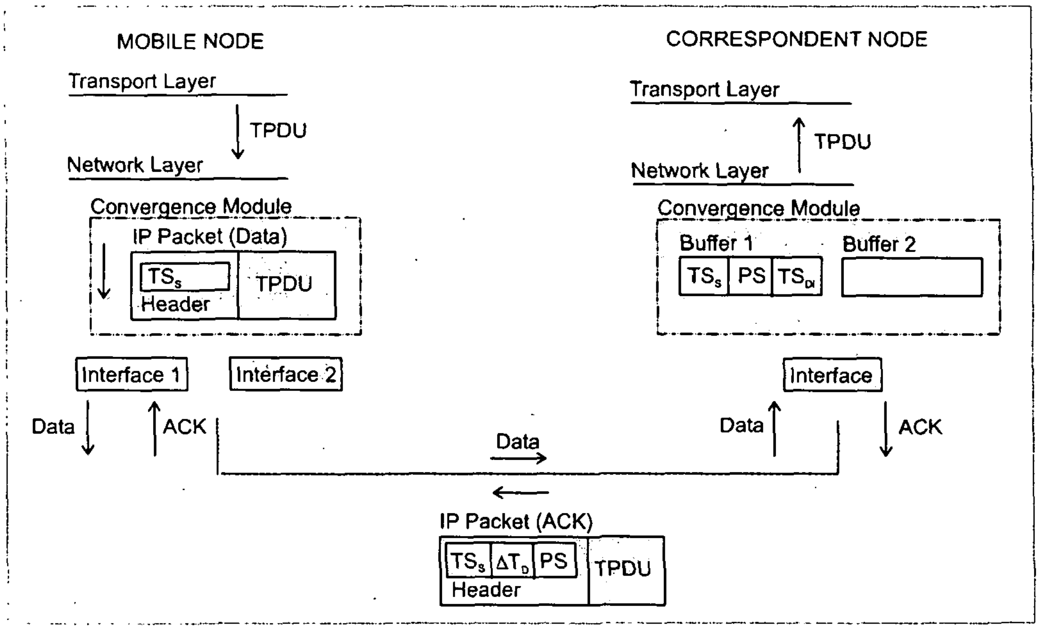


Figure 4.2: Communication from the Convergence Module of the sender to the receiver, where sender is the Mobile Node

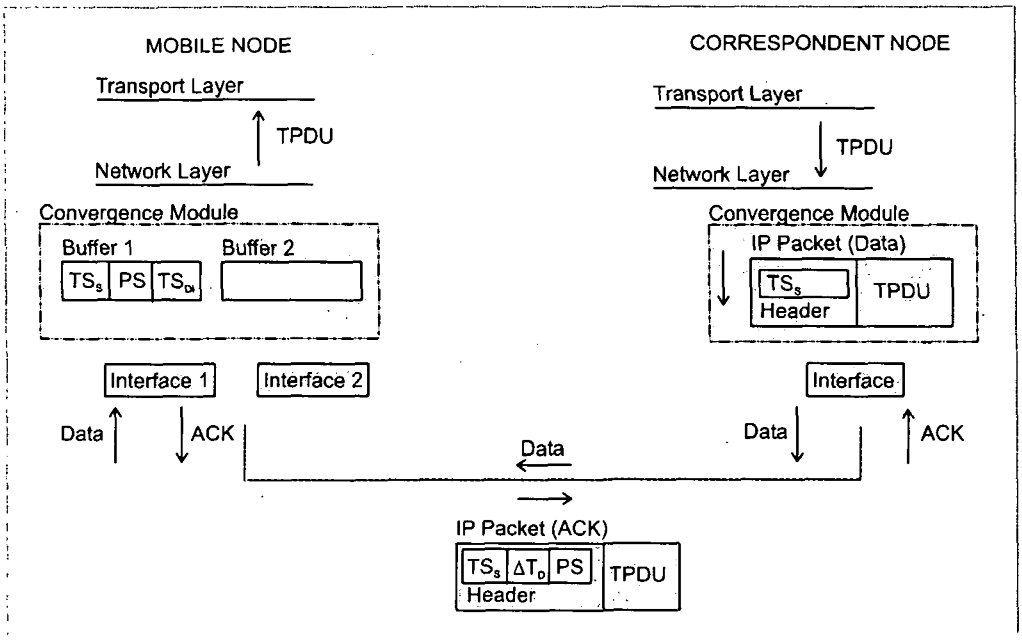


Figure 4.3: Communication from the Convergence Module of the sender to the receiver, where receiver is the Mobile Node

4.4. The Modified Protocol

With the introduction of CM at the communication endpoints, the flow of the protocol has to be appropriately amended. The protocol will now progress as follows:

1. When MN is not communicating with any CN and moves out of its home network, its CM will send BUs to its HA as envisaged in [27], except that it will now be sent to the HA corresponding to PHoA. In the absence of any communication, simultaneous use of multiple interfaces does not accrue any benefit. Therefore, in spite of having multiple interfaces, the MN will use only a single interface at this point, and that too preferably the one that's least expensive on communication cost (unless of course, other considerations like security, etc. are involved). As MN moves to yet another foreign network, it will attempt to configure a new CoA at the previous interface, failing which it will try to configure some other interface in increasing order of cost.

2. When MN initiates a communication with CN, the former will get CoAs assigned for its other available interfaces and register them with it's HA (or HAs) to benefit from bandwidth aggregation. The CM at MN will then send BUs to CN (for route optimization), which the CN must authenticate before registering. The CM at MN will also distribute the outgoing traffic to CN across these CoAs. Initially this distribution will be uniform, but with time the link characteristics will get estimated (as in Section 4.3.3) and the proportions of packets sent through these links accordingly readjusted. When a handover takes place at an interface, MN will set the proportion of packets handled by the interface to zero. On completion of handover (after new CoA is registered at HA and CN), the CM at MN will once again start sending packets through this interface at the previous rate. If the new link has different characteristics, this rate will get readjusted on link characteristics estimation.

   While the above tasks are done by the CM at MN, the one at CN will collect the packets of the same flow originating from different MN interfaces, forward them to higher layer after replacing the source IP address with the HA (or PHoA) and assist in the link quality estimation process.

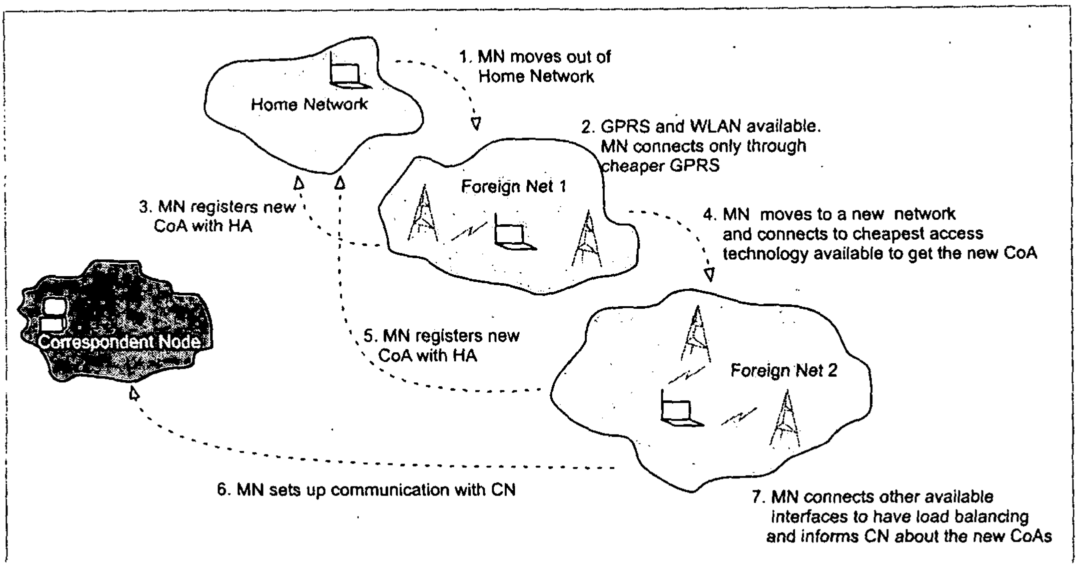

1. MN moves out of Home Network
Home Network
2. GPRS and WLAN available. MN connects only through cheaper GPRS
Foreign Net 1
3. MN registers new CoA with HA
4. MN moves to a new network and connects to cheapest access technology available to get the new CoA
Correspondent Node
5. MN registers new CoA with HA
Foreign Net 2
6. MN sets up communication with CN
7. MN connects other available interfaces to have load balancing and informs CN about the new CoAs

Figure 4.4: Protocol - when MN initiates the flow

3. If instead, CN initiates the communication, the packets will be sent to the HA (corresponding to PHoA) of MN. As in [27], the HA will then redirect the same to the CoA of MN. On receipt, MN will activate its available interfaces, register the CoAs with HA, and send BU to CN, informing the latter about the available CoAs. The CM at CN will authenticate these CoAs and thereafter send traffic distributed over them. As before, this will be a uniform distribution to begin with, followed by readjustments commensurate to link capacities. For a MN interface handover, the CM at MN will inform the same to its corresponding CM at CN if the former can preempt the same (by an L2 trigger, say). Alternatively the CM at CN will infer the same by the absence of (ACK) packets from the other direction. Apart from this, the node may also detect a binding invalidation by ICMP error messages such as ICMP_UNREACHABLE. In such a case, the CM at CN will stop sending packets to that interface, till it receives a BU for that interface. The proportion of packets sent to the new CoA will be guided the same principle as before.

The flow of the proposed protocol is shown in Figures 4.4 and 4.5.

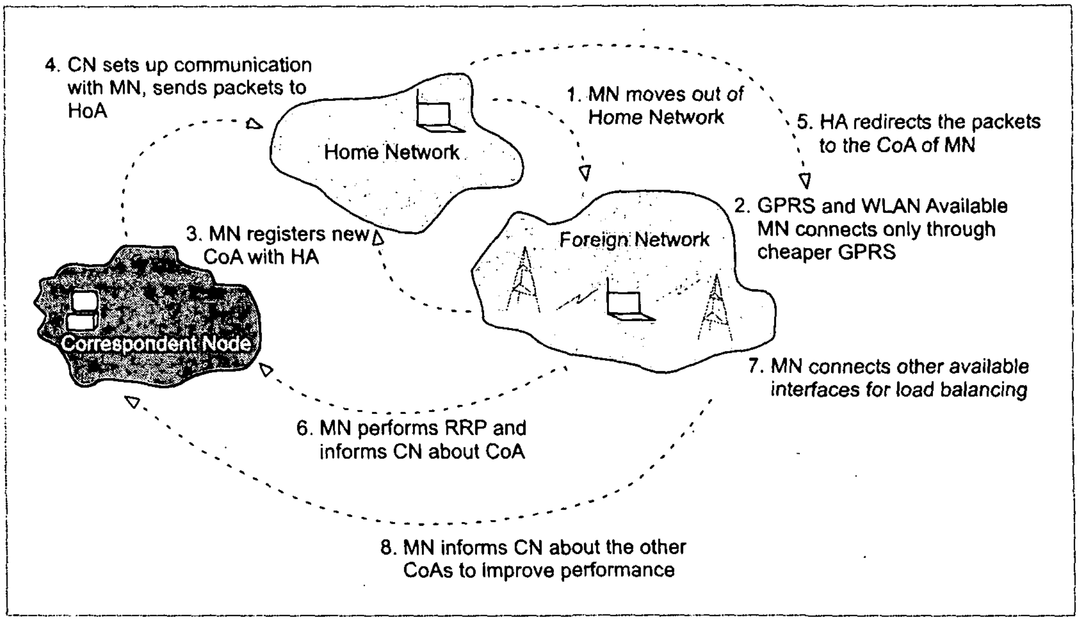

4. CN sets up communication with MN, sends packets to HoA
1. MN moves out of Home Network
5. HA redirects the packets to the CoA of MN
Home Network
2. GPRS and WLAN Available MN connects only through cheaper GPRS
3. MN registers new CoA with HA
Foreign Network
Correspondent Node
7. MN connects other available interfaces for load balancing
6. MN performs RRP and informs CN about CoA
8. MN informs CN about the other CoAs to improve performance

Figure 4.5: Protocol - when CN initiates the flow

If route optimization is not desired (for example, for location privacy), then the CM at MN will inform the CN (via HA corresponding to PHoA) of its other HoAs (instead of CoAs), when MN is the sender. This allows the CN to expect packets from these HoAs. Conversely, if CN is the sender, then the CM at CN will distribute the traffic over these MN's HoAs, once the former is informed about the other MN HoAs.

4.5. Simulation and Results

Simulation experiments were conducted using NS2 to compare the performance of multi-interfaced mobile nodes vis-à-vis those with only one interface. For the simulation, the NS2 version 2.28 [67] was used. The multi-interfaced mobile node was equipped with two interfaces. TCP was used as the transport layer protocol, which was made to run over IP at the network layer, and the node mobility was managed by MIP. The mobile node was considered to be the recipient of an ftp flow from a correspondent node. The general outline of the simulation topology is shown in Figure 4.6.

The topology considered had the access routers placed with a lateral separation of 250 metres. That is, the horizontal component of the distance between two nearest access routers (horizontally) was 250 metre, but these two access routers were on different links. The distance between two successive access routers on the same link was therefore 500 metre. The mobile node was made to move away from its Home Agent at a uniform speed of 10m/s, keeping equal distance from the two links. The two links were separated by a distance of 400 m.

The same characteristics were maintained for all the nodes. The wireline link delay was set to 2 ms. In order to compare TMMIPv6 scheme with base MIP, these simulations were run alternately with mobile nodes equipped with single and double interfaces. The simulations were conducted separately for base station range of 400m and 500m respectively.

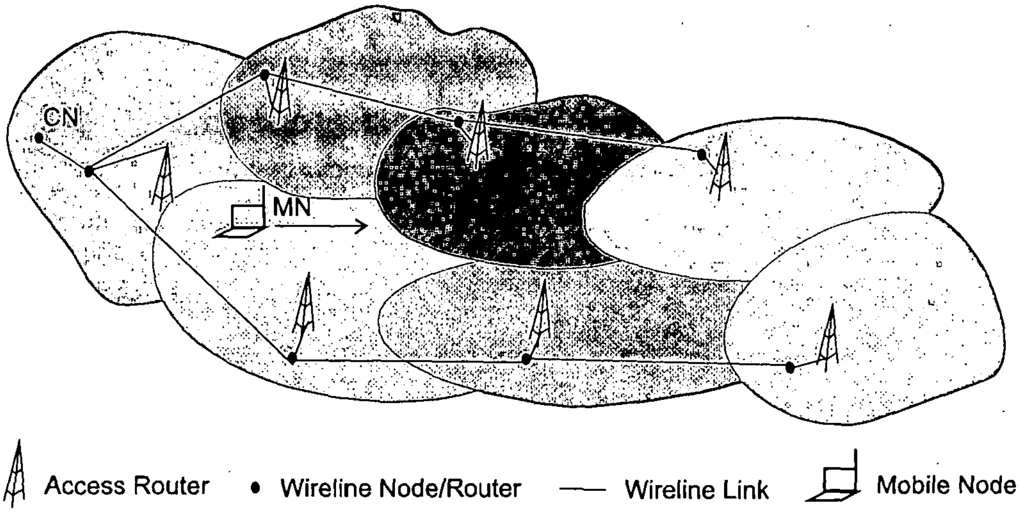


Figure 4.6: Simulation Topology

In the simulations conducted, all the packets from the CN were made to pass through the HA, and not directly to the MN as envisaged in route optimization. This is because the route optimization has not been implemented in the simulator. Thus if all the parameters are kept same, the CN-HA link might result in a bottleneck, constricting the traffic at the two individual nodes. In order to avoid this bottleneck, the CN-HA link bandwidth was set to double of that between the HA and the base stations link. The bandwidth of the wireline link was, therefore, set to 256 kbps, except that between the correspondent node and the home agent, which was set to 512 kbps. For each base station range, two groups of simulations were conducted:

- In the first case, the two interfaces were allowed to connect to any base station once they move out of the home network, except that the both could not simultaneously connect to the same base station. This would be the situation, if the interfaces of mobile node support same access technology in real life.
- In the other case, a restriction was introduced on the base stations a mobile node interface could connect to. Only one set of base stations was now made accessible to one interface, while the second interface of the multihomed mobile node was allowed access to the other set. This would be the situation, if the two interfaces of the mobile node support distinct technologies. As for the single interfaced node, it was allowed to connect only to one of these two sets, while the base stations in the other set were made transparent to the node.

The results with the base station range set to 400m is shown in Figure 4.7, while that with the base station range of 500m is shown in Figure 4.8.

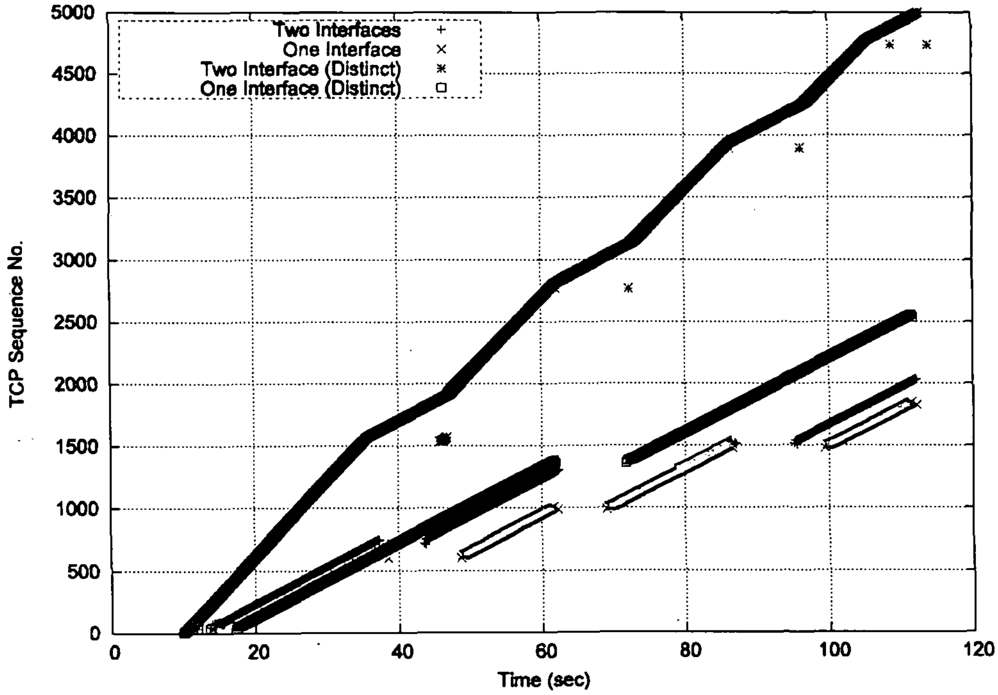


Figure 4.7: Simulation result with base station range set to 400m

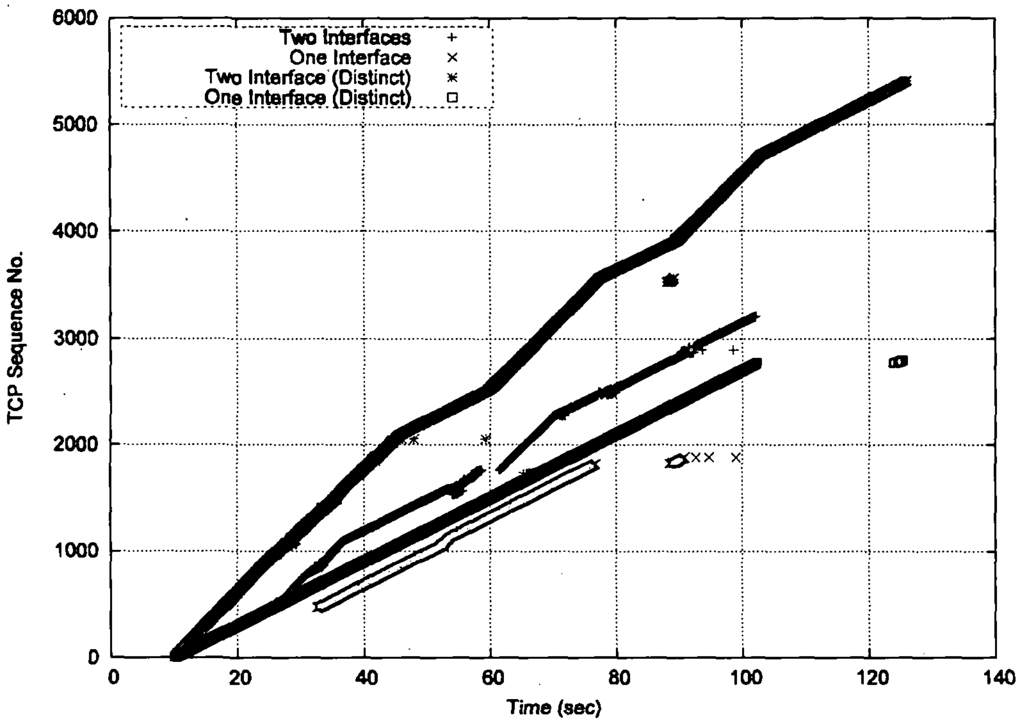


Figure 4.8: Simulation result with base station range set to 500m

In all the plots of Figures 4.7 and 4.8, it is seen that the performance, in terms of number of tcp packets reaching the destination, is mostly better (and never worse) in case of the multi-interfaced mobile node as compared to the one with a single interface. There is also a marked decrease in the handover delay in the two interfaced case. The result is surely better in cases where each interface was allowed to connect to a distinct set of base stations (marked *Distinct* in the plot legends), compared to the other cases. This is because the router advertisements from one link is received by only one interface and is ignored by the other, resulting in fewer handovers. For the *Distinct* cases, the improvement is more remarkable for the smaller range of 400m compared to the 500m range. The reduced base station range minimizes number of distinct router advertisements that the mobile node received, which results in better performance.

The packet latency – the time required for the packets to reach the destination from their source – for each of the above simulation scenarios was also considered. Figure 4.9 plots this latency for simulation carried out with the base station range set to 400m and the MN interfaces allowed to connect to any of the base stations. Figure 4.10 shows the

result when the two MN interfaces were allowed to connect to distinct set of base stations.

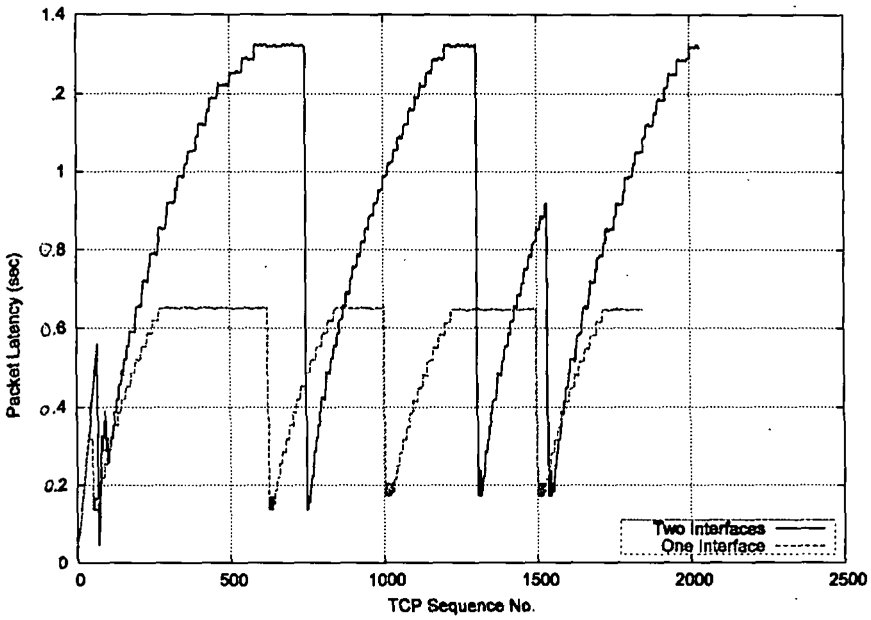


Figure 4.9: Packet Latency, AR range - 400m, Interface allowed to connect to any base station

It is noticed that the packet latency is comparatively smaller at the beginning of the simulation, as well as immediately after a handover to a new access router, which then increases to a maximum value until the next handover.

This is because once a handover is performed; a new frequency is allocated to the MN by the base station supporting it. When the first packet reaches the base station and is forwarded to the mobile node, there is no interference since there was no signal emanated into the medium at that frequency just before that. But as more and more packets traverse the medium, the reflected signals will interfere with the original ones, resulting in increased time to reach the destination. An added reason is also the fact that the wireline link has better characteristics as compared to the wireless link. This might result in buffering of packets at the base station. This buffer, being empty at the beginning, does not introduce any delay for the initial packets.

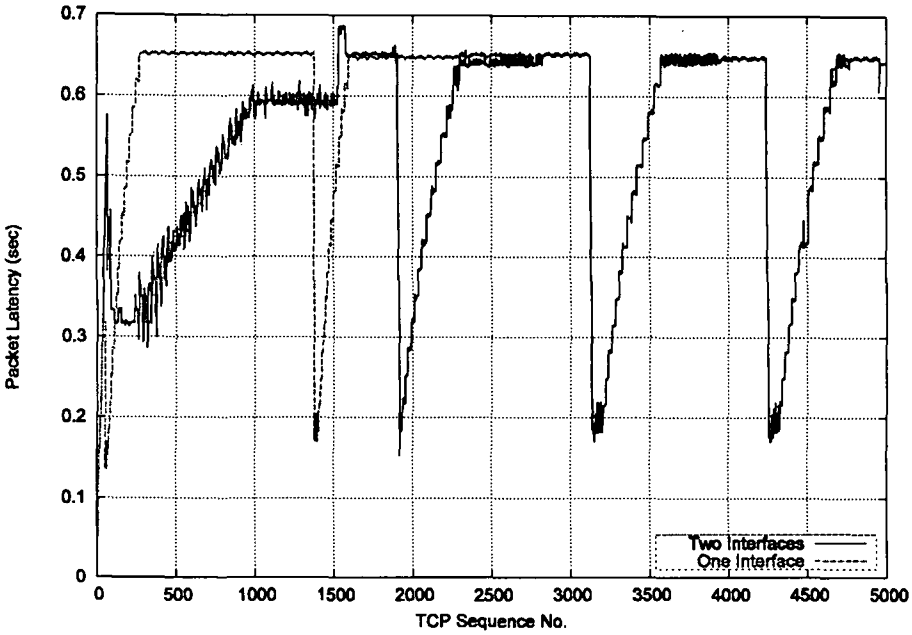


Figure 4.10: Packet Latency, AR range - 400m, Interface allowed to connect to distinct set of base stations

If the packet latency for single and multi-interface plots in Figures 4.9 and 4.10 are considered, it is seen that it is quite high (on the average) for multi-interfaced node as compared to that for the single interface. This is because there are more router advertisements reaching the mobile node in multi-interfaced case. The node therefore needs to check more frequently as to whether it should perform a handover. There are more disturbances in the wireless medium too because of the advertisements. However when there is a restriction in the number of base stations that the MN can connect to, this latency (on the average) becomes similar to that in case of single interfaced node.

The similar packet latency for the simulation with the base station range of 500m are shown in Figures 4.11 and 4.12.

In the Figures 4.11 and 4.12 too, it can be noticed that the performance of the multi-interfaced node is better when the interfaces are restricted to connect to a given set of base stations. Comparing this packet latency, the results are in general seen to be better for the base station with a range of 400m (Figures 4.9 and 4.10) as the jitter is considerably lesser in this case.

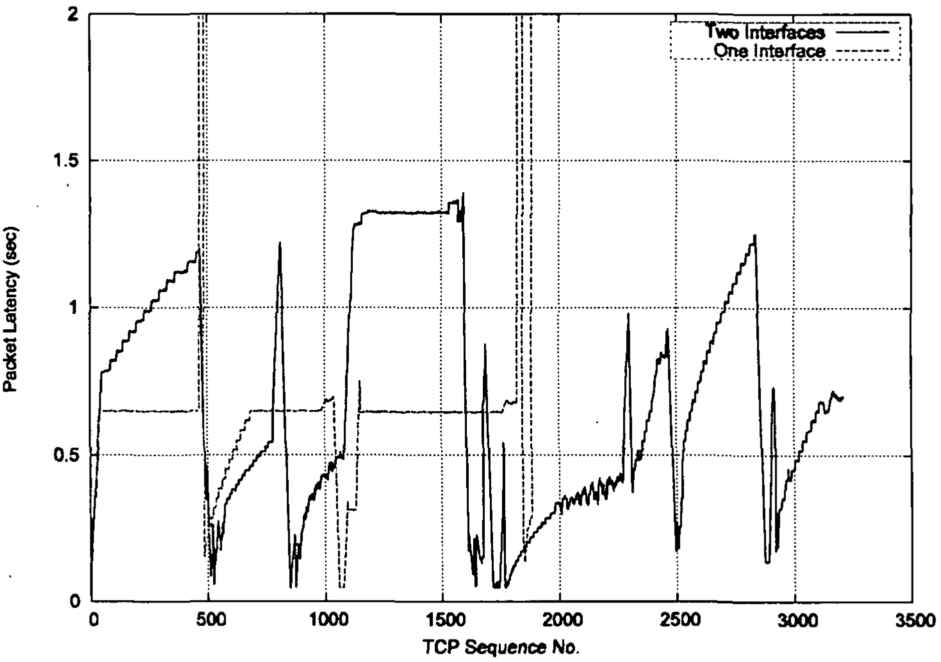


Figure 4.11: Packet latency, AR range - 500m, Interface allowed to connect to any base station

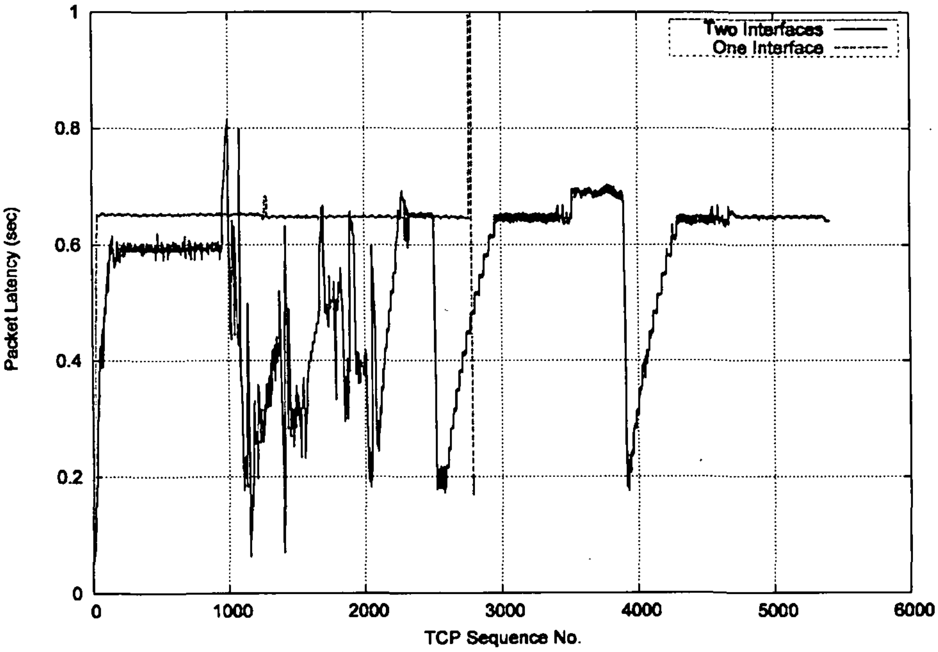


Figure 4.12: Packet latency, AR range - 500m, Interface allowed to connect to distinct set of base stations

These experiments indicate that the use of multi-interfaced node will certainly result in better performance as far as the number of packets reaching the destination is concerned.

Moreover, the experiments also indicate that the benefit due to multi-interfaces can be appreciable if the interfaces under consideration support distinct, rather than the same wireless access technologies. In such a case, a higher data rate can be achieved without any unnecessary increase in packet latency. In addition, the simulation results discourages the use of very high range for the base stations which, in turn satisfies the condition that the base station ranges be kept small for frequency re-utilization and reduced interference.

4.6. Security Issues

The security implication of the proposed modification to MIPv6 - whereby the node will be able to split any flow across multiple interfaces, the proportion of traffic across each interface determined dynamically based on prevailing network conditions – was also studied. There are two issues relating to security in the modified protocol:

- One relates to optimization in return routability procedure to set up the key between the MN and the CN

- The other relates to the vulnerability in the link quality estimation process and is critical to the flow of the protocol itself.

In the following paragraphs, these issues and their possible solutions are discussed.

4.6.1. Return Routability Procedure Optimization

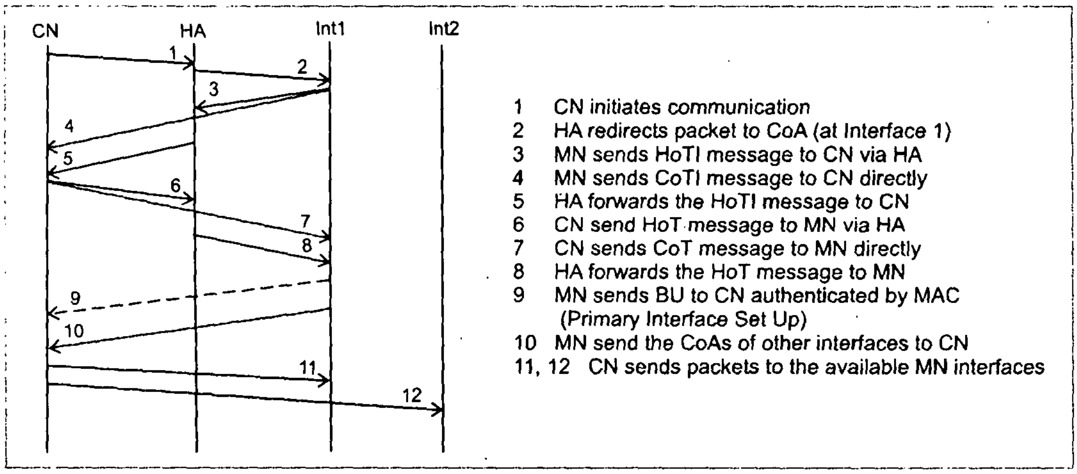
While using more than one interface, return routability procedure [27] has to be performed for every interface to authenticate the binding update for these CoAs at the CN [41]. This is a pre-requisite before any packet can be sent from/to these interfaces. However, in the presence of several interfaces, this will result in a substantial overhead – considering the fact each return routability procedure will involve four message exchanges before the binding update for an individual CoA can be forwarded.

To enhance the usability of the scheme, a proposal is presented to reduce the number of messages exchanged during the key setup procedure. Contrary to the requirement in

MIPv6, the binding update for all CoAs except that for the primary CoA (the interface originally configured with PHoA) will be clubbed together and sent through the primary interface (the interface having the primary CoA) to the CN in this TMMIPv6 scheme, informing the latter about the available interfaces. This resulting binding update will be authenticated using the key set up by return routability procedure involving the primary CoA.

It is essential to use the PCoA to send the binding updates for all other CoAs, since the key set up using the primary CoA can be used only for messages through the primary interface. MN generates the key for binding update authentication based on two tokens – home keygen and care-of keygen tokens – that it receives from the CN. However, the care-of keygen token involved in the process is created by CN [27] as

Care-of keygen = First(63, HMAC_SHA1(Kcn, (Care-of address|nonce|1)))



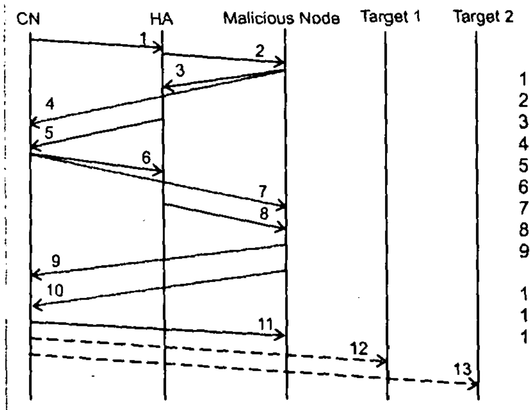
1 CN initiates communication
2 HA redirects packet to CoA (at Interface 1)
3 MN sends HoTI message to CN via HA
4 MN sends CoTI message to CN directly
5 HA forwards the HoTI message to CN
6 CN send HoT message to MN via HA
7 CN sends CoT message to MN directly
8 HA forwards the HoT message to MN
9 MN sends BU to CN authenticated by MAC (Primary Interface Set Up)
10 MN send the CoAs of other interfaces to CN
11, 12 CN sends packets to the available MN interfaces

Figure 4.13: Message diagram if primary interface is used to inform about all available CoAs

Hence, the key – being dependent on the care-of address – cannot be used with another interface having a different CoA. Once the CN is made aware of the various CoAs, it can be expected that the CN will start sending packets to the various available interfaces. The resulting message flow is seen in Figure 4.13.

4.6.1.1 Security Loophole

The above optimization however, comes with the risk of bombing attack. In this attack, a malicious node may send the address of another node in the guise of CoA for one of its interfaces. If the CN does not confirm the validity of the address on receiving the BU, the new CoA, which is the target for the attack, will start receiving the packets from the CN. The malicious node can then stop receiving packets from the CN. In the absence of feedback, the convergence module at CN will infer that the original CoA is no longer reachable, and all the packets will thus be forwarded to the targeted node. The malicious node can actually use this technique to bomb many nodes simultaneously by providing their IP addresses in the pretext of CoAs for its own interfaces. This message flow involved in such attack is seen in Figure 4.14.



1 CN initiates communication
2 HA redirects packet to CoA (at Interface 1)
3 Malicous node sends HoTI message to CN via HA
4 Malicious node sends CoTI message to CN directly
5 HA forwards the HoTI message to CN
6 CN send HoT message to the Malicious node via HA
7 CN sends CoT message to Malicous node directly
8 HA forwards the HoT message to Malicious node
9 Malicious node sends BU to CN authenticated by MAC (Primary Interface Set Up)
10 Malicious node sends the addresses of target nodes to CN
11 CN sends packets to the MN
12, 13 CN sends packets to the target nodes

Figure 4.14: Bombing attack in case key is not set up for each interface individually

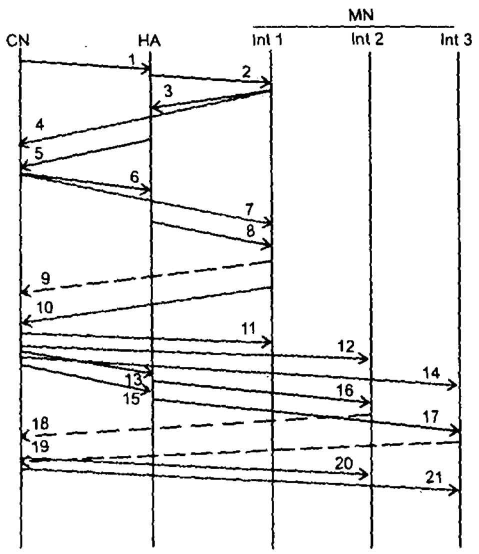
Of course, if there are no packets coming from the receiver's end, the convergence module at the sender will infer a link failure and stop sending packets after sometime. In addition, the address of the target, as registered by the malicious node at the CN, is valid only for the lifetime of the binding, beyond which packets will not be sent. However, if such an attack is coordinated against a target by a group of conspiring nodes, this may result in denial of service attack at the target.

4.6.1.2 Security Solution

The above optimization of sending all the CoAs using a single binding update through PCoA without further verification is thus, not tenable. While such a clubbed binding update will surely reduce the number of messages involved, the same cannot be used by the CN without additional corroboration.

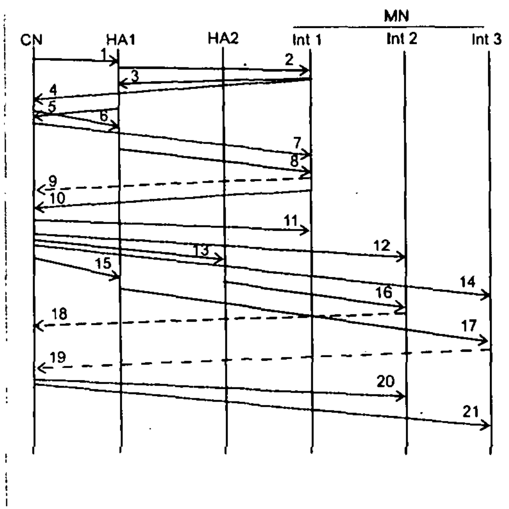
For this the CN will send the Home Test (HoT) and Care-of Test (CoT) messages containing the Home Keygen and Care-of Keygen tokens to each of the CoAs included in the clubbed binding update. However, as the Home Test and Care-of Test messages in this case are sent by CN without receiving the usual cookies from the target CoA (used for validating the HoT and CoT messages), these fields will include the last received Home Cookie and Care-of Cookie respectively from the given MN.

On receipt of these Home Test and Care-of Test messages, the MN will compare the Home Cookie and Care-of Cookie (included in these messages) with the values it had stored previously (those generated when the MN had sent the original HoTI and CoTI messages [27] before sending the BU through PHoA). If these match, each interface should respond with a Binding Update message. The CN, on receiving this update will authenticate the CoA, and proceed to send/receive packets from the given interface. This scenario is seen in Figure 4.15.



1 CN initiates communication
2 HA redirects packet to CoA (at interface 1)
3 MN (interface 1) sends HoTI message to CN via HA
4 MN (interface 1)sends CoTI message to CN directly
5 HA forwards the HoTI message to CN
6 CN send HoT message to the MN (interface 1) via HA
7 CN sends CoT message to MN (interface 1) directly
8 HA forwards the HoT message to MN (interface 1)
9 MN sends BU to CN authenticated by MAC
(Primary Interface Set Up)
10 MN (Interface 1) sends CoAs of interfaces 2 and 3 to CN
11 CN sends packets to MN (interface 1)
12 CN sends CoT message to MN (interface 2) directly
13 CN sends HoT message to MN (interface 2) via HA
14 CN sends CoT message to MN (interface 3) directly
15 CN sends HoT message to MN (interface 3) via HA
16 HA forwards HoT message to MN (interface 2)
17 HA forwards HoT message to MN (interface 3)
18 MN (interface 2) sends a BU to CN
19 MN (interface 3) sends a BU to CN
20, 21 CN sends packets to the MN at interfaces 2 and 3

Figure 4.15: Message diagram for the proposed security optimization



HA1 is the home agent for Interfaces 1 and 3 while that of interface 2 is HA2

1 CN initiates communication
2 HA redirects packet to CoA (at interface 1)
3 MN (interface 1) sends HoTI message to CN via HA
4 MN (interface 1)sends CoTI message to CN directly
5 HA forwards the HoTI message to CN
6 CN send HoT message to the MN (interface 1) via HA
7 CN sends CoT message to MN (interface 1) directly
8 HA forwards the HoT message to MN (interface 1)
9 MN sends BU to CN authenticated by MAC
(Primary Interface Set Up)
10 MN (interface 1) sends CoAs of interfaces 2 and 3 to CN
11 CN sends packets to MN (interface 1)
12 CN sends CoT message to MN (interface 2) directly
13 CN sends HoT message to MN (interface 2) via HA
14 CN sends CoT message to MN (interface 3) directly
15 CN sends HoT message to MN (interface 3) via HA
16 HA forwards HoT message to MN (interface 2)
17 HA forwards HoT message to MN (interface 3)
18 MN (interface 2) sends a BU to CN
19 MN (interface 3) sends a BU to CN
20 CN sends packets to the MN at interface 2
21 CN sends packets to the MN at interface 3

Figure 4.16: Message diagram for the proposed security optimization, in case the interfaces have different home addresses

It is also possible that the various interfaces of the MN have different Home addresses and are supported by different home agents. Figure 4.16 shows the scenario when the interfaces 1 and 3 are supported by the home agent HA1 while the interface 2 is supported by HA2.

The above discussion centres on the use of non-primary interfaces once the primary interface has been registered with the CN. However, if there is a change in the primary CoA, the authorization key should be set up by normal procedure detailed out in [27]. Moreover, the nonce used by CN in generating the keygen tokens might also get changed over time. Any binding update to CN using key based on a nonce created before MAX_NONCE_LIFETIME [27] seconds will be rejected, and an error code in Binding Acknowledgement will be sent to MN. The MN will then perform return routability procedure once again, using the interface that it designates as primary CoA.

4.6.2. Timestamp Protection

The traffic distribution over the various available MN interfaces under this scheme is done dynamically on the basis of link characteristics, as estimated by the convergence module at the sender's end. For proper functioning of the scheme, it is imperative that these estimates must give the actual state of these accessible links. A malicious node trying to fail the protocol may therefore interfere in the process of this estimation.

When a packet is sent, the convergence module at the sender will insert a timestamp on to it (section 4.3.3). However, after generating the timestamp, no state is maintained at the sender. When a packet is later on sent from the other end to the original sender, the convergence module at that end will insert the original timestamp, the packet size, and the delay – the time lapsed since the receipt of the original packet and the sending of the current packet – into this outgoing packet.

A malicious node, to disrupt the functioning of the protocol, may want to temper with this timestamp. If the timestamp is changed to an earlier value, the link characteristic calculated based on this value will result in a lower figure compared to the actual link bandwidth. Thus, the data rate over this link will get reduced from what it should have actually been. The malicious host can therefore reduce the data rate over a better interface while increasing the same over a worse one – which may result in packet loss and eventually, disruption of communication. Since no state is maintained at the original sender, the integrity of the timestamp cannot be verified.

To ensure that such tempering of the timestamp is not possible without being detected, the original sender of the timestamp will encrypt the same. The receiving node need not understand this value, and is just required to insert it on to the outgoing packet, destined for the original source. The encryption key, therefore, need not be shared with any other entity. The link characteristic estimation based on this timestamp is undertaken by the same entity which had originally generated it, thereby avoiding the need for any key exchange for this encryption.

4.7. Mobility Management for Multihomed nodes at Transport versus Network layer

The TMMIPv6 manages the multiplicity of interfaces at the network layer. To bring out the advantage of managing mobility at the network layer rather than the transport layer, especially for a multi-interfaced MN, a comparison of the packet overhead between the

TMMIPv6 modified scheme vis-à-vis SCTP (which is seen as a possible transport layer mobility management scheme) is presented in this sub-section.

It is not obligatory that there will only be one transport connection open at a given time. Conversely, it is more likely that there be multiple transport layer connections open at the same time to/from the mobile node. If SCTP (or one of its extensions) is used at the transport layer, then there will be as many associations present. SCTP does not support multihoming for load balancing. Even if SCTP is modified to support load balancing for multihomed nodes, the following considerations result in excessive signaling load to support node mobility.

Whenever the mobile node changes its CoA at any one interface, the same has to be recorded at the other end of the association. To this end, the mobile node (SCTP at transport layer) has to send an ASCONF chunk to the other end containing the ADDIP parameter [37]. The other end must acknowledge the same using the ASCONF-ACK chunk back to the mobile node before the latter can use the new CoA. If there are p transport connections, and the mobile node changes q CoAs in time t, then this would lead to the SCTP layer at the mobile node's end to send

pq chunks in time t,

or, $\frac{pq}{t}$ chunks per unit time

Moreover, as each ASCONF chunk must be acknowledged with ASCONF-ACK chunk, the total number of chunks involved in managing node mobility per unit time will be

$$n_{sctp} = 2\frac{pq}{t} \qquad (4.5)$$

In contrast, if MIP with modifications described in TMMIPv6 is used with TCP at transport layer, then the total number of Binding Updates sent would be

q in time t,

or, $\frac{q}{t}$ per unit time.

In MIP, binding acknowledgement is optional. Even if it is considered, the total number of binding update messages to manage the mobility would be

$$t_{tmmip} = 2\frac{q}{t} \qquad (4.6)$$

independent of the number of transport layer connections.

When compared to expression (4.6), expression (4.5) shows that the overhead for mobility management, in terms of control information transferred between MN and CN, is lower for a network layer mobility solution.

4.8. Summary

In this chapter, the TMMIPv6 extension to MIP have been discussed that would allow dynamic sharing of flow among available interfaces and thereby experience an enhanced bandwidth. This scheme will allow seamless mobility across overlaid networks with heterogeneous access technologies. The concept of PHoA would allow a mobile node to be registered with more than one HoA. The available HoAs may no longer be coupled with particular interfaces, but can be used by any interface depending on availability. Simulated experiments have carried out to evaluate the basic premise of the scheme – sharing of load among multiple interfaces to enhance performance – and have shown that under various conditions, a multi-interfaced mobile node will experience a better throughput with seamless mobility as compared to its single-interfaced counterpart. These simulations showed up to 95.66% increase in throughput, as compared to the single interfaced node. Obviously two interfaces will have a higher combined throughput compared to a single one, the main advantage – as evident from simulation results – was the absence of discontinuity in packet transfer due to handovers. In addition, this chapter talks about reduction in the number of message exchanges involved in return routability procedure to set up the key for route optimized operation. Securing the link quality estimation process is also discussed. Finally, a discussion is presented in favor of mobility management at network layer vis-à-vis transport layer.

Chapter 5

Interoperation of Schemes

The two extensions to MIPv6 – MAAH extension and TMMIPv6 - discussed in this thesis are aimed towards decreasing the handover latency and thereby, improving the performance of the base protocol. The decrease in handover latency is achieved either through assistance from mobile agent or through simultaneous use of multiple interfaces.

However, these protocols need not be made to work all by themselves, and can also be interfaced with each other as well as other related extensions of MIP. In this chapter, the following two interoperation scenarios are discussed:

- Interoperation of MAAH scheme with micromobility protocols, and
- Interoperation of MAAH scheme with TMMIPv6 extension

5.1. Interoperation of MAAH scheme with Micromobility Protocols

In this section, the interoperation of the MAAH scheme with micromobility protocols – such as Hierarchical Mobile IPv6 [29], Fast Handover [30], and Cellular IP [31] – is investigated. Fast Handover is already claimed to work with HMIPv6 [30]. In Fast Handover, the access routers act as local home agents, which hold binding caches for the MNs and receive binding updates. This makes this access routers function like MAP specified in HMIPv6. Also, it is quite possible that the access routers are not directly connected, but communicate through an aggregate router. Such an aggregation router is an ideal position for MAP functionality in case of HMIPv6.

For the HMIPv6 to function securely, there must be some security mechanism existing between the MAP and the supported MN(s) to handle the local registrations at the former. When the MN enters a domain, it needs to make a regional registration to advertise its new broad location to it's HA and CN(s). It indicates a Regional Care-of Address (RCoA) for the domain. Later, after each movement between the routers in the same domain, the MN has to send a local registration to the MAP to update its localization in the domain. Thus with the RCoA of the MN remaining invariant, all MN movements within the domain are hidden from the home agent and correspondent node(s). However, when the MN moves out of the current domain, there will be a change in it's RCoA and it will accordingly have to send new updates to it's HA and CN(s) as in base MIP.

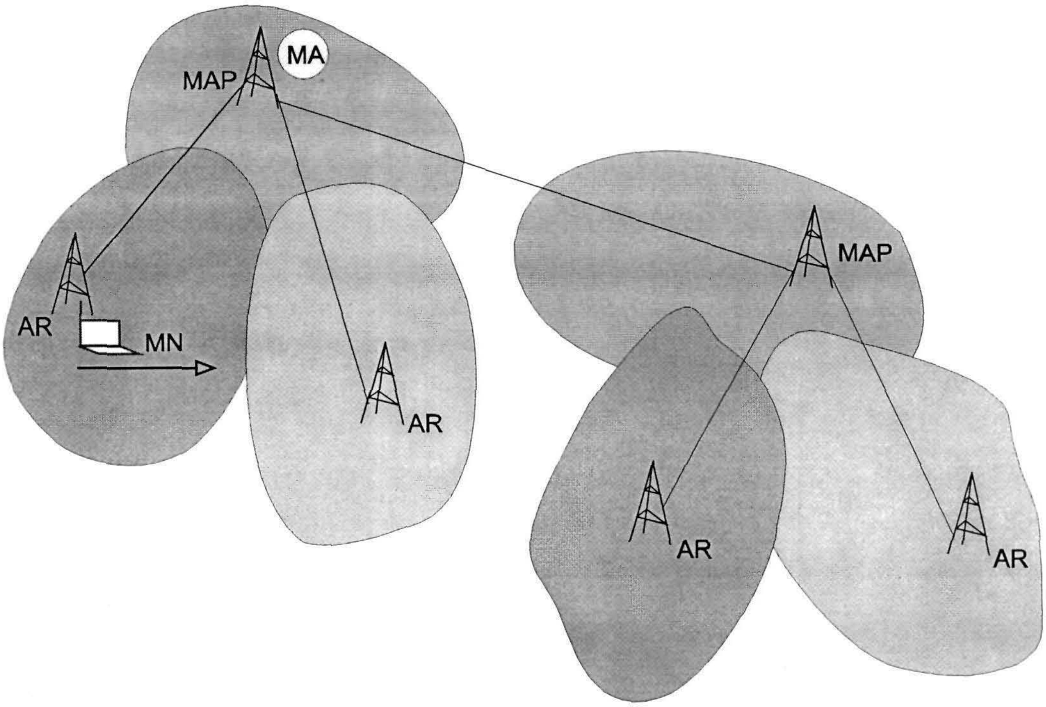


Figure 5.1: Using Mobile Agent with HMIPv6

Micromobility protocols reduce the handover latency when the MN movement is within a localized area, but whenever such a movement takes place across these areas, there will be the usual delay due to handover, as in MIPv6. To reduce this delay while moving across these areas (such as from one MAP domain to another in HMIPv6), MAAH scheme can be applied over the micromobility protocol. The mobile agent can be stationed at the MAPs (in case of interoperation with HMIPv6) as shown in Figure 5.1. The mobile agent at the previous MAP can proxy for the MN's HA for such inter-domain movements. Thus, when the MN changes its RCoA, the new RCoA can be registered by the mobile agent at previous MAP. This will speed up the process of RCoA registration during inter-domain transfers, and in doing so, also reduce the network traffic. Moreover, like all other registrations, RCoA registration will also be valid for a finite lifetime, beyond which the same will require re-registration even in the absence of any movement. As per HMIPv6, there re-registrations will involve the HA, and hence the necessary control messages will have to travel to and fro the MN-HA distance. In these registrations too, the mobile agent at the previous router can be involved instead to hasten up the process, and improve protocol efficiency.

An identical solution can be applied to Cellular IP too. The Gateways in CIP are similar to the MAPs of HMIPv6. The mobile agents can therefore be stationed at the CIP Gateways. When the MN moves to a new CIP network, instead of informing the HA about the address of the new CIP Gateway as its new CoA, it can inform the same to the mobile agent at the previous CIP Gateway. The mobile agent can later, asynchronously, inform the HA about the same. The mobile agent can move from one CIP Gateway to another, similar to the case where it was moving from one access router to the next.

5.1.1. Handling Authenticaion in HMIPv6

In case of HMIPv6, a mobile node has to make two registrations –

- with it's HA for the global CoA (RCoA)
- with the MAP for the local CoA.

All binding updates between the MN and the MAP must be authenticated. This requires that the MN should share an authentication key with all the MAPs it may visit.

The requirement of setting up of a shared key between the MAP and the mobile node, and the infrastructure needed thereof can be taken care of by the mobile agent, if MAAH is interoperated with HMIPv6. The job of authentication may be left to the mobile agent instead of MAP. Unlike the MN and the MAP; the MN, it's HA and the mobile agent belong to the same administrative domain. Thus, setting up a shared security association between the MN, its HA and the mobile agent will be less challenging than setting up the same between the MN and the MAPs the former may visit.

With mobile agent of MAAH scheme taking over the validation procedure, the mobile agent at the previous MAP can authenticate the binding update for the first RCoA. Once this is done, the mobile agent will move to the MAP currently supporting the MN. From this point onward, as long as the MN moves within the local domain, it can be authenticated by the mobile agent stationed at the MAP of the current domain. When it moves to the next domain, the mobile agent at the previous MAP rather than the HA will perform the registration. After the registration, a new mobile agent will be forwarded to the next MAP. Thus, the MN need not have a shared key with the MAP. It will be enough to have the shared key with the mobile agent stationed at the MAP.

5.1.2. Simulation and Results

Simulated experiments were performed to study the MAAH interoperation with HMIPv6 vis-à-vis the base MIP as well as HMIP in a hierarchical network topology. The simulation topology is shown in the Figure 5.2.

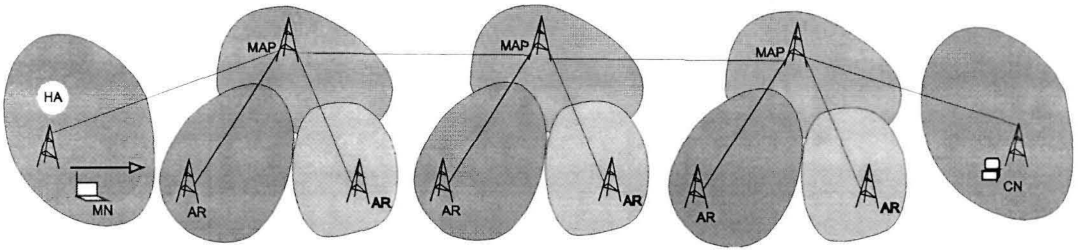


Figure 5.2: Simulation topology for a hierarchical network scenario

In this simulation topology, seven foreign networks (the figure shows only three) were considered, apart from the home network and the network where the CN was placed. In each of these seven networks, there was one MAP (Mobility Anchor Point). Two access routers were connected to each of these MAPs. The simulation parameters considered are listed below:

- Separation between the nearest ARs was set to 300m
- Separation between the adjacent MAPs was set to 600m
- Domain radius of the ARs was set at 155m
- Propagation delay was set to 2μs

- Processing delay at each node was set to 1ms
- Link bandwidth of the wireline networks was set to 2Mbps.

For individual protocols, the simulation experiments were conducted as follows:

- For the base MIPv6 protocol, the MN had to register its CoA with the home agent every time it moved from one access router to another, as envisaged in the original protocol. These registrations were followed by the return routability procedure to set up a fresh key with the CN. On expiry of registration lifetime, the same was renewed, but these renewals were not followed by renewal of CN-MN key through return routability procedure.

- For the HMIP simulation, the registration with the home agent was done only when the MN moved out of the range of one MAP into that of another. These home registrations were followed by return routability procedure. However, as long as the MN moved within the same MAP domain, the registrations were forwarded only till the MAP. Such registrations were not followed up by the return routability procedure and consequent binding update to the CN. The re-registration of the RCoA with the CN or the home agent was not considered. However, re-registration of local CoA with the MAP was taken care of. This, of course, will not be the case in practice as there will be a finite lifetime for the RCoA registration at the home agent and CN – beyond which the same will have to be renewed.

- For the mobile agent assisted protocol over HMIP, the mobile agent was considered to be placed at the MAP. Since the MA's mandate is to proxy for the home agent, the registration of CoA as well as the return routability procedure involved the MA at the previous MAP. As before, home registration (now taken care of by the MA at the previous MAP) and the return routability procedure was considered only when the MN moved out of one MAP to another.

The comparative values of handover delays as the MN moved out of its home network and traveled towards the CN for each of the three separate protocols are plotted in the Figure 5.3. The plot shows periodic spikes indicating MN handovers. The line between two successive spikes indicates the time consumed for re-registration of CoAs.

In case of the base MIP, the handover delay increased continuously whenever there was a change of access router, as the MN moved towards the CN. This is seen as increasing height of the spikes in the plot. The increase can be attributed to the fact that with MN's movement, the distance between the MN and its home agent increased constantly, thereby increasing CoA registration time, as well as the time consumed for completion of return routability procedure.

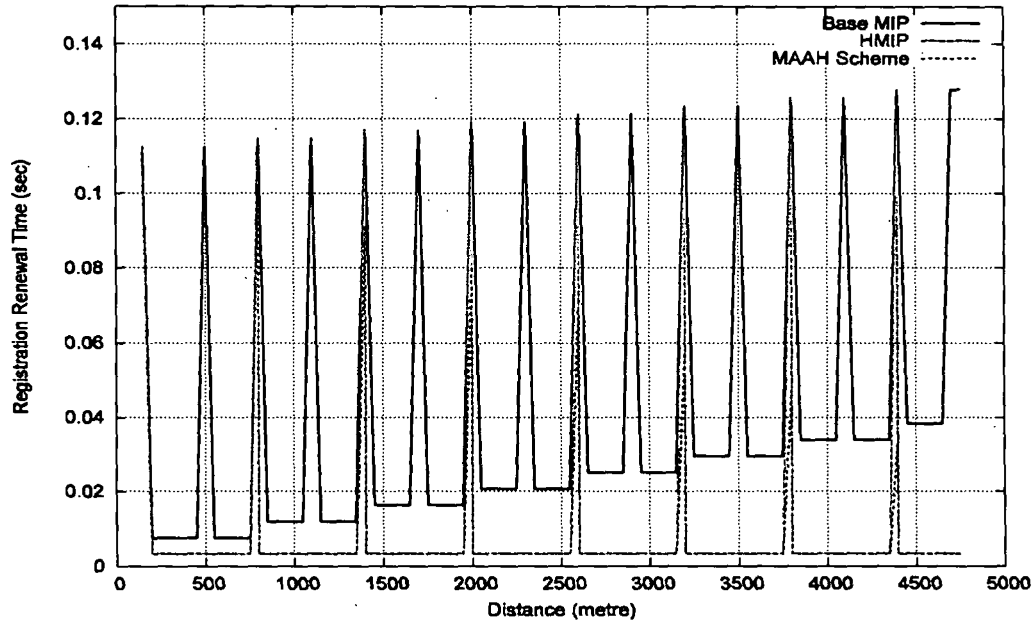


Figure 5.3: Comparative plot for MIPv6, HMIPv6, and MAAH over HMIPv6 in a hierarchical topology

In case of HMIP, the registration with the MAP within the same MAP domain resulted in a very small delay. However, whenever there was an inter-domain movement, the home registration and the consequent return routability procedure followed by binding update to the CN resulted in a higher handover delay. As a result, the spikes are seen only for such inter-domain transfers and not for every access router transfer as was the case with MIPv6. Thus, the handover latency is reduced for intra-domain handoffs. In addition to the spikes due to RCoA registration, in practice there will be many more spikes in the plot to account for the renewal of RCoA registration at the home agent and the CN. These registrations, like every other registration, these have finite lifetime and the renewals will occur even in the absence of MN movement. These re-registrations, while not directly leading to handover latency, will however affect the efficiency of the protocol.

In case of the MAAH interoperation with HMIPv6, there was no change in the handover delay for intra-domain MN movement. However, the handover latency for inter-domain MN movement got reduced compared to the HMIP case as the MN continued moving towards CN. This is because the return routability procedure and binding update to CN required less time as the MN-CN distance decreased. As for the home agent registration, the same was taken care of by the MA at the previous MAP. As in case of HMIP, there will also be spikes for home/mobile agent re-registration and binding update to CN even without inter-domain movement at the expiry of RCoA lifetime.

The plot demonstrates that the performance of mobile agent assisted scheme is never worse than the HMIP. In fact, the performance for the former improves with decreasing MN-CN distance. The overall performance improvement will be quite remarkable if the re-registration of the RCoA was also considered. Of course, there will most possibly be more access routers within a given MAP domain making inter-domain handovers less frequent than considered in this simulation. Nevertheless, considering the benefit derived in the form of reduced handover latency and the decreased RCoA renewal time, the MAAH interoperation certainly seems to be a better option.

5.2. Interoperation of MAAH Scheme with Multihomed MIP

Of the two extensions to MIP discussed in this thesis, the first one – MAAH scheme – suggested modification to MIPv6 whereby mobile agents were used to proxy for the home agent at the foreign network. Thus to support this scheme, the foreign network must provide support for the mobile agent functioning. It is pointed out that while the availability of such mobile agent platform at the foreign networks will speed up the handover process, their absence will not prevent the communication to proceed, but will allow it to fall back on base MIP. The second scheme – TMMIPv6- is applicable for mobile nodes that are equipped with multiple interfaces. These multiple interfaces can then be used simultaneously to improve performance through bandwidth aggregation, the process being administered by the *Convergence Module* at layer 3.

However, there can be a scenario where the mobile node is equipped with multiple interfaces and the foreign networks have operational mobile agent platform as well. In such a case, the two schemes can be made to inter-operate in order to achieve further reduction in handover latency. In this section, such interoperation of the MAAH and TMMIPv6 schemes are discussed.

The TMMIPv6 scheme described in Chapter 4 takes care of handover latency by shifting the flow to the other available interfaces, when a given interface performs a handover. While the flow is taken care of by the other interfaces, the interface under question performs the handover as described in base MIP. Once this handover is over, the CN will be informed of the new CoA for the said interface through a binding update using the PCoA. This will be true if the interface under consideration is not the one having the PCoA. The CN will then send the HoT and CoT messages to convince itself about the validity of the new CoA, which it does through the resulting binding update from the given interface.

However, while the data traffic is shared among the other interfaces, the interface performing the handover will be practically out of action for the duration equivalent to handover latency. If the foreign network is equipped with mobile agent platform, then the period of practical inactivity of the said interface can be reduced by adopting the MAAH scheme for the handover. This will allow the mobile node to use all its available interfaces for a greater fraction of time.

Interoperation of MAAH and TMMIPv6 schemes is shown in Figure 5.4. The MN here is equipped with two interfaces – *Int1* and *Int2*. Initially, these interfaces are connected to access routers AR1 and AR2 respectively. As described in the MAAH scheme, the mobile agents MA1 and MA2 are stationed at these routers. As the MN moves, its interface *Int1* requires handover to a new access router – a handover from AR1 to AR3. While this handover takes place, the traffic will be shifted to *Int2*. However, in order to hasten up the process of handover at *Int1*, it can obtain a new CoA from AR3 and register the same with the mobile agent MA1 at AR1, instead of HA as per base MIP.

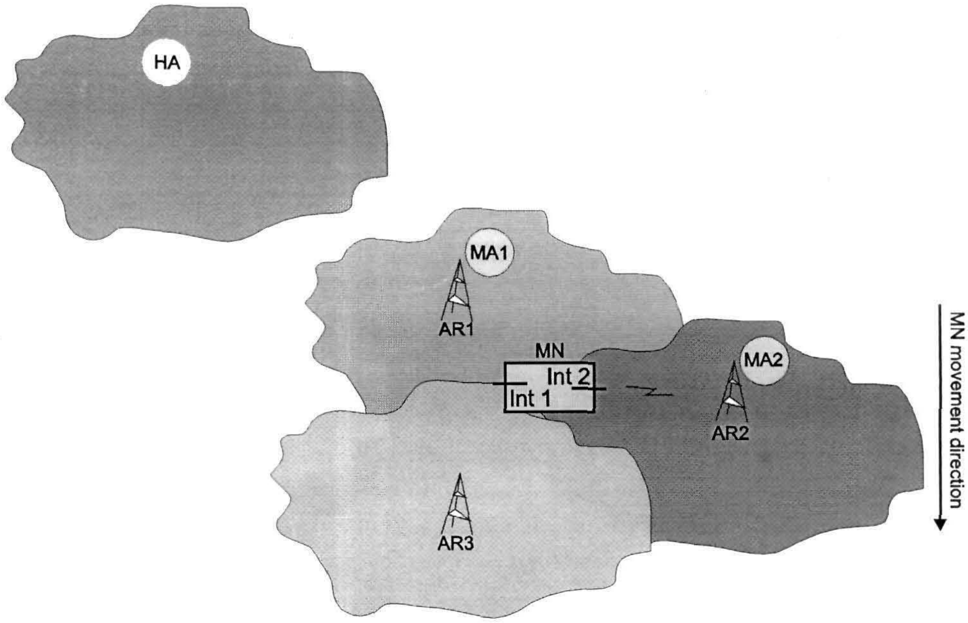


Figure 5.4: Interoperation of Multihoming scheme with MAAH scheme

Once registered, the MN can inform the CN about its new CoA for interface *Int1* through the primary interface – assumed to be *Int2*. To verify the validity of the new CoA, the CN will forward HoT and CoT messages containing the respective tokens and in return, expecting a binding update from the MN containing the new authentication code. The HoT message can be forwarded through MA1, instead of the usual HA, in order to lessen the network path traversed. However, if *Int1* is the primary interface (one having the PCoA), then the full return routability procedure has to be undertaken to set up the key before the CN can be informed about the new CoA. In that case, the mobile agent MA1 will assist in redirecting the HoTI message from the MN to CN and the HoT message from CN to the MN, as envisaged in MAAH scheme.

This interoperation will therefore allow the MN to use its available interfaces with minimum interruption due to handover at these interfaces. This will result in a higher throughput as compared to the proposed TMMIPv6 alone, without any assistance from the mobile agents.

5.3. Summary

This chapter describes the interoperation of MAAH scheme with micromobility protocols as well as with the TMMIPv6 scheme.

The interoperation with micromobility protocols allows MAAH scheme to reduce the handover delay resulting during inter-domain node movements and to take care of necessary authentication. Results obtained from simulated experiments are presented as well to visualize the advantage. As per the simulation results, there was a reduction of 28.74% in the total time consumed for registration renewal. While using MAAH with HMIPv6 to improve inter-domain handover latency, the mobile agent stationed at the MAP can also be used to take care of message authentication. This eliminates the need for additional infrastructure; since the MN and the mobile agent, belonging to same home domain, can set up a security association between them.

The interoperation of MAAH scheme with TMMIPv6 is also discussed. These two schemes can be operated in conjunction to improve MIP performance in presence of multiple node interfaces as well as mobile agent platform support at the access routers. It is argued that the handover at individual interfaces can be improved by MAAH scheme, while the multiplicity of interfaces is being managed by TMMIPv6 scheme.

Chapter 6

New/Modified Message Formats & Their Handling

Two schemes, proposed with the view to reduce the often pronounced handover latency in case of MIPv6, are discussed in Chapters 3 and 4. The handover latency is reduced in the proposed schemes either through support from mobile agents or through multi-homing of the mobile nodes. The schemes, as discussed, envisage functioning along with MIPv6 and through minimum possible changes to the existing protocol. However, a few new control messages become necessary to support the proposed extensions. In addition, certain modifications in formats are also needed for some of the existing messages. This chapter describes the message formats, new as well as the modified ones, considered necessary to execute the proposed extensions to MIPv6. While section 6.1 discusses additional /modified formats of control messages for MAAH scheme, section 6.2 describes the same as needed for TMMIPv6 scheme.

6.1. Mobile Agent Assisted Handover (MAAH) Scheme

To support the MAAH scheme, introduction of a new mobility option is proposed:

- Home Agent Binding Mobility Option

Apart from this, the following message formats of MIPv6 [27] need to be modified:

- Binding Update Message
- HoTI Message
- Router Advertisement Message

Slight modifications are also envisaged in the way the following messages are handled by the respective entities:

- Binding Update Message
- Binding Acknowledgement Message
- HoTI Message
- HoT Message

Some data structures at various entities storing relevant information essential for the protocol implementation needs to be augmented as well.

6.1.1. Home Agent Binding mobility option

In the MAAH scheme the mobile agent, instead of the usual HA, takes care of registering the MN, once the latter moves out of its home network. Thus, while the mobile agent at the previous access router will be aware of every new CoA of MN, same will not any longer be true for the HA. To keep the HA somewhat updated, the mobile agent will (asynchronous to mobile node registration process) send periodic updates for all the MNs it is serving at that given time.

The *Home Agent Binding* mobility option, a new option proposed in the MAAH scheme, precisely does this. This option contains the CoA of all the MNs serviced by the mobile agent, along with their HoAs. The HoA identifies the precise MN at HA's binding cache. This mobility option will be sent to the HA periodically, at an interval previously configured by it. This option will be included in the Binding Update message to be sent to the HA from the mobile agent.

The *Lifetime* field of the Binding Update message in this case will contain a value, which is the minimum of the registration lifetime value of all the MNs supported by the mobile agent. This is so set, since sending all the individual registration lifetimes will add considerable overhead. It is expected that a new Binding Update containing this option will be sent on expiry of this *lifetime* value. There is of course, the pre-configured interval for sending a message message containing this option, which might be greater than the said lifetime. This might lead to a small delay in new connection setup by a CN, if the comcermed HA does not have the fresh binding for the MN. However, this will be a small price to pay for providing better user experience for ongoing communications.

The Binding Update message should have the *M* bit (discussed in Section 6.1.2) set to inform the HA that the said message has originated from a mobile agent and not the MN. The source address of the binding update message can be set to the CoA of any of the MNs serviced by the mobile agent. This CoA (source address) will therefore not be included within this moblity option (since the HA will know this CoA from the binding update message, and not from this accompanying mobility option). The HoA of the said CoA will be informed through Home Address option [27]. The Binding Authorization Data Option [27] will, in such case, contain authorization information for the mobile agent and not for the MN. The format of this mobility option is shown in Figure 6.1.

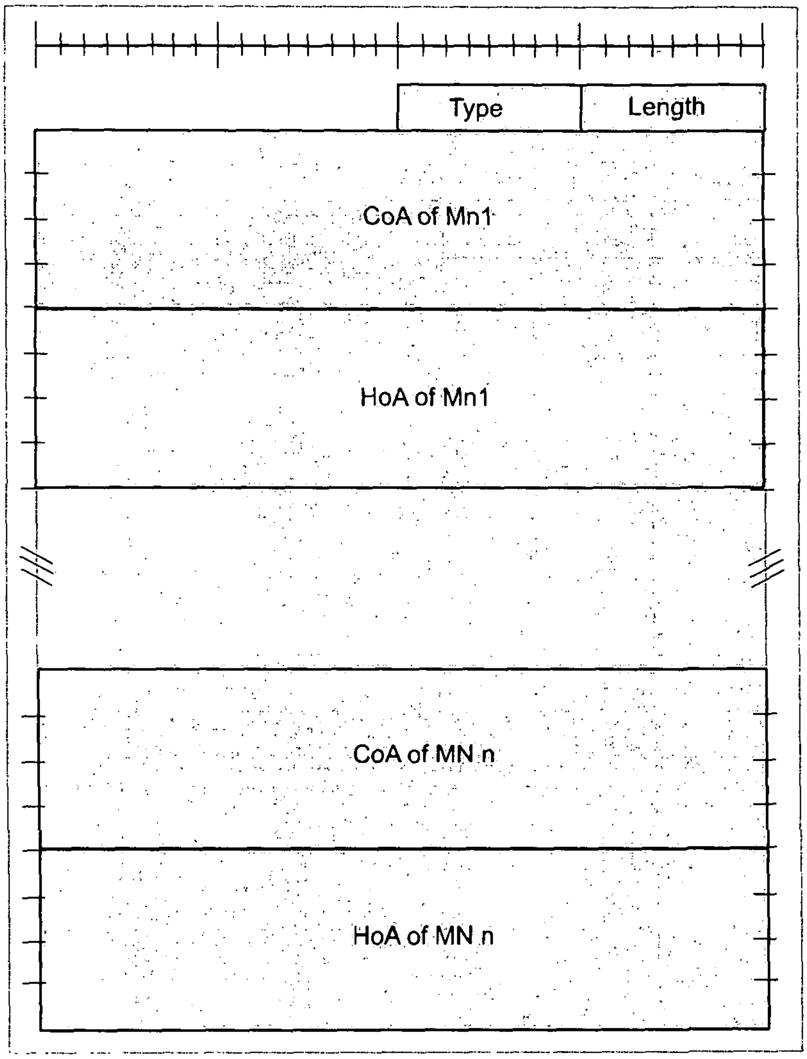


Figure 6.1: Home Agent Binding Mobility Option

This being a new option, its *Type* value has to be accordingly assigned. The value of *Length* field is the number of octets, excluding the *Type* and *Length* fields, and will be set to $16 \times 2 \times Number\ of\ CoAs$ (since each IPv6 address is 16 octets long).

6.1.2. Binding Update (BU) Message

A MN uses the Binding Update (BU) message to inform its HA and optionally, the CN(s), about its CoA. This becomes necessary when the MN changes it CoA, and registers a new CoA for itself. This will also be necessary when the old CoA is retained, but the registration lifetime is about to expire. In the latter case, the MN sends the Binding Update message to renew its registration lifetime.

However, in the MAAH scheme, the MN registers its CoA with the mobile agent at the previous access router, except the first time it moves out of its home network. The Binding

Update message will then be required to register a new CoA or update an exisiting registration's lifetime at the mobile agent.

To distinguish between Binding Update messages sent to the HA and those sent to the mobile agent, the *Mobile Agent* (M) bit is introduced.

- This *M* bit will be set by the MN when it sends the binding update message to the mobile agent in the previous router after moving to a new access router.

- The *M* bit may also used in the Binding Update message, when the MN needs to renew its binding lifetime at the mobile agent.

In case the MN is registering a new CoA with the mobile agent, the Acknowledgement (A) bit will also be set along with the M bit. As usual, the Home Address Destination option will also be included.

While the source address for the binding update message will be set to the new CoA, the destination address will be set to the previous CoA. The binding update will therefore reach the previous access router where the concerned mobile agent will intercept the packet since it is addressed to the old CoA of MN (for which the mobile agent has a valid binding) and in view of the fact that the *M* bit is set. The *M* bit included in an incoming message indicates that the packet is meant for the mobile agent. The mobile agent will then register the new CoA or renew the existing binding, after due authentication.

The M bit will also be set in the binding update messages sent from the mobile agent to the HA containing the *Home Agent Binding* mobility option (Section 6.1.1), informing the latter about the CoA of all its MNs currently served by the concerned mobile agent. This will allow the HA to realize that the binding update message is sent from a mobile agent, and not from the usual MN. The modified format introducing the *M* bit (and thereby reducing the *Reserved* field by one bit) is shown in Figure 6.2.

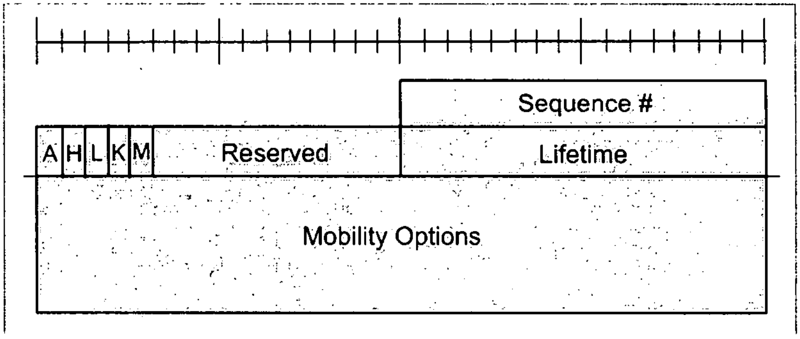


Figure 6.2: Modified Format for Binding Update Message

6.1.3. HoTI Message

The HoTI message is one of the four messages involved in Return Routability Procedure used to generate the key needed to authorise the binding update. In the base protocol, this message is sent by the MN to its CN with which it desires to set up the key. This message is tunneled through the HA in MIPv6.

In the MAAH scheme, the mobile agent takes up the functions of HA at a foreign network. As a result, when the MN moves from one foreign network into the next, it registers its new CoA with the mobile agent at the previous access router. It is therefore imperative that the return routability procedure should be handled by the mobile agent in the previous AR, instead of the HA.

Towards this end, the HoTI message will now be sent to the mobile agent at the previous access router. Like the packets sent from the MN to its HA using reverse tunneling, this packet will also be reversed tunneled using IPv6 encapsulation. The addresses of the tunneled packet will be set as follows:

- The source address will be set to the new CoA (one already registered with the concerned mobile agent).
- The destination address will be set to the previous CoA of MN.

When this message reaches the previous AR, the mobile agent will intercept the same, given that it was destined to the old CoA of MN. The mobile agent will then pass the encapsulated packet to the CN. The encapsulated packet will have its addresses set as follows:

- The source address will be set to the previous CoA of MN (for which CN will have a valid entry in its binding cache)
- The destination address will be set to that of the CN

While sending this encapsulated packet to the CN, the mobile agent will also include the Home Address option so that the CN can uniquely identify the record pertaining to the given MN in its binding cache.

In order to distinguish between the HoTI message redirected via the HA and the one via the mobile agent, a *Mobile Agent (M)* flag is included in the reserved portion of the HoTI message. This flag will be useful for the receiving CN, since it has to send the corresponding HoT message to the same mobile agent, instead of the usual HA. The format of the modified HoTI message is shown in Figure 6.3

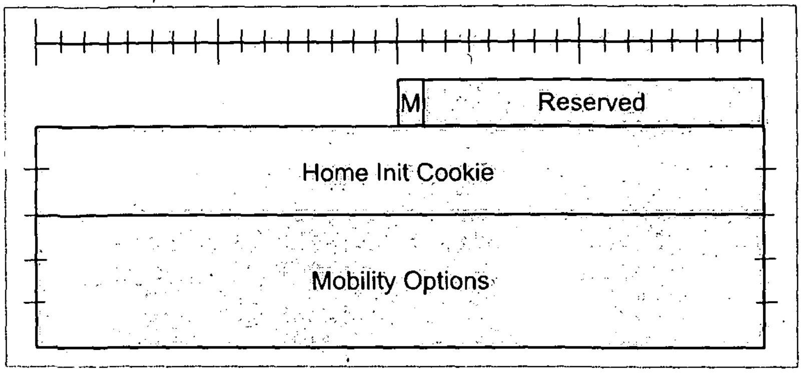


Figure 6-3: Modified Format for HoTI Message

6.1.4. Router Advetisement Message

As discussed in Chapter 3, the MAAH scheme functions with the help of mobile agents. For these mobile agents to function and to be transferred from one router to the next, the router must provide the required Mobile Agent Platform (MP). If such platform support is available, the MAAH scheme will manage the handover, while its absence will compel the system to fall back on the base protocol.

In view of this, the router must inform the MN as to whether it is capable of providing the MP. This will be done while the router announces its presence through the Router Advertisement Message. To include the aforesaid information, a new flag bit – Agent (A) is suggested to be included in the Router Advertisement message. This, in turn, will reduce the Reserved field from five to four bits. The modified format is shown in Figure 6.4. The remaining fields have meanings described in [27] and [68].

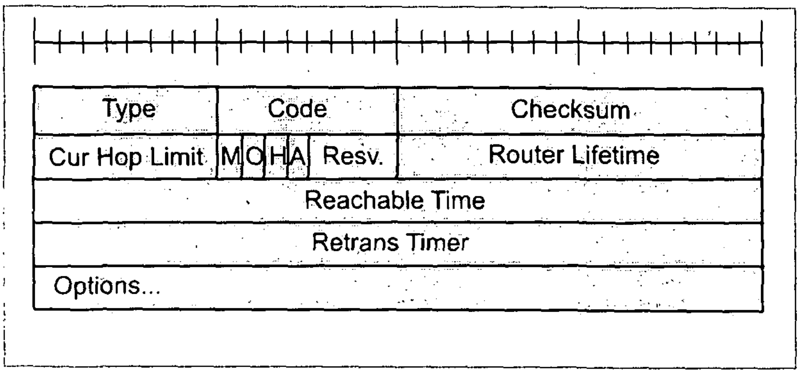


Figure 6.4: Modified Format for Router Advertisement Message

6.1.5. Addition to Existing Data Structures

In addition to the data stored at MN and HA in the base protocol, few more information needs to be stored to support the modifications proposed in MAAH scheme:

- The HA, as in MIPv6, will store information about the MNs which are currently located at different networks. The additional information required are about the mobile agents proxying for the HA. This information will include data about the mobile agents' security association, and their locations.

- Apart from those envisaged in MIPv6, the MN needs to keep track of its previous CoA (since the mobile agent will be available at that address) as well. Aditionally, it will store information as to whether the current router supports mobile agents through MP. This information will be required while sending binding updates to HA and/or mobile agent. This information will also be needed when the MN moves to the next network. The MN can gain this information from the Router Advertisement Message (with modifications proposed in Section 6.1.4).

- The mobile agent needs to store the binding for the MN(s) – including the current and previous CoAs; the security association related to HA, MN and neighbouring mobile agents; and the interval at which it is supposed to send BUs (using Home Agent Binding mobility options, discussed in Section 6.1.1) to HA. The mobile agent will also store information about the presence, or otherwise, of other such agents belonging to the same home network in the adjoining networks and their corresponding authentication values.

- No changes would be necessary as far data storage at the CNs is concerned.

6.1.6. Amendment in Messages Handling

The MAAH scheme envisages certain changes in the way some of the messages are handled in MIPv6 by the entities involved in the protocol.

6.1.6.1.Binding Update Message

In the MAAH scheme, the binding update message will be used in different scenarios as follows:

- The MN will send this message to inform the receiver about its current CoA. When the MN moves out of its home network and connects to the first foreign network, this message will be sent to the HA. However, if the *A* bit is included in the Router Advertisement (section 6.1.4), the MN will include the *M* bit in the BU message (section 6.1.2). As usual, the source address of this message will be the CoA and the destination address will be that of HA. This will also contain the Home Address

Option. When the HA receives this BU containing the M bit, it will register the CoA as usual and send a mobile agent to the router the MN is currently attached to.

- When the MN moves from one foreign network to the next, the binding update message will be sent to the mobile agent in the previous network (if such support was available at that network). The source address of this message will be set to the new CoA, while the destination address will be set to the old CoA of the MN. If the new router provides MP support, this message will also have the *M* bit (Section 6.1.2) set. As usual, it will also contain the Home Address option. The mobile agent intercepts all the packets meant for the MN it is currently supporting. Thus, when the mobile agent at the previous router receives a binding update message addressed to the old CoA, it infers that the MN has set up a new CoA, and will therefore register the same after due authentication. On registering, it will forward a new mobile agent to the new router. However, if there is a mobile agent from the same home network already serving the new network, then it will only forward the information pertaining to the given MN. The original mobile agent will henceforth store the new CoA information.

- The binding update message may also be sent to increase the lifetime of an existing binding before it expires. If such a message is sent to HA or MA, the receiver will extend the registration lifetime after necessary authentication and send the consequent acknowledgement to the MN.

- If, on moving to the new network, the MN receives the Router Advertisement message without the *A* option (Section 6.1.4), it will send a binding update message to de-register from the mobile agent at the previous router, and send a binding update message for registration at the HA as in the original protocol.

- If the HA receives a binding update message containing the Home Agent Binding mobility option (Section 6.1.1), it will infer that this message has come from a mobile agent. Such a message will have the destination address set to that of the HA, and the source address set to the CoA of one of the MNs supported by the mobile agent. The HA should therefore update its binding cache for all the nodes mentioned in the option after due authorization. If an acknowledgement has been asked for, it should send the same to the source address of the received binding update message.

6.1.6.2. Binding Acknowledgement Message

There is no change envisioned in the format of Binding Acknowledgement message. However, apart from the HA and CN, the mobile agent will also send the Binding Acknowledgement message, when it receives a binding update message with the Acknowledgement (A) bit set.

6.1.6.3. HoTI Message

This message is usually sent by the MN to CN through its HA. However, if the MN had registered with a mobile agent at the previous access router, then this message should be tunneled to the CN via that mobile agent (Section 6.1.3). Such HoTI message will include the *M* flag.When CN receives such a message, it will send the corresponding HoT message to the old CoA of MN which is available in its binding cache.

6.1.6.4. HoT Message

In MIPv6, this message is sent by the CN to the MN via the latter's HA. In MAAH scheme, the HoT message will be sent as envisaged in the base protocol if the original HoTI message did not have the M bit set (Section 6.1.3). On the other hand, if the M bit was set in the HoTI message indicating that it had been tunneled via the mobile agent and not the home agent, the CN will send the corresponding HoT message to the MN via the same mobile agent.

A packet carrying this HoT message will have its addresses set as follows:

- The source address will be set to the address of the sending CN
- The destination address will be set to the source address of the initiating HoTI message, i.e., the previous CoA of the MN under question.

This HoT message will reach the previous access router of the MN, and will be intercepted by the mobile agent. The latter will then tunnel the message to the new CoA of MN.

The remaining control messages in MAAH will follow the same format and will be handled as discussed in the base MIPv6 protocol.

6.2. Transparent Multihomed MIPv6 (TMMIPv6) Scheme

The TMMIPv6 scheme described in Chapter 4 supports multi-homing through dynamic traffic management with due assistance from the convergence module and with minimum modifications to MIPv6. Moreover, the protocol will not come in the way of communication between nodes where the convergence module support is not available at either or both ends.

The communication, in such a case, will flow as per base MIPv6. To support the proposed TMMIPv6 scheme, certain new messages/mobility options need to be defined:

- Primary Home Address Destination Option
- Link Quality Estimation Init Destination Option
- Link Quality Estimation Destination Option
- Multi-CoA Mobility Option

Moreover, certain modifications are needed in the ways the following messages are handled:

- Binding update
- Home Address Option
- Type 2 Routing Header

Likewise, the conceptual data structures storing information at certain entities will have to be augmented for smooth flow of the TMMIPv6 extension.

6.2.1. Primary Home Address Destination Option

In MIPv6, there is only one HoA for every MN. This HoA is therefore, unique for every MN and is used to identify a MN in CN's binding cache. However, in the face of multiple interfaces of a given MN associated with separate HoAs, the latter will not longer be able to uniquely identify a MN. The TMMIPv6 scheme proposes introduction of a *Primary HoA* (PHoA) to identify the MN uniquely in the presence of multiple HoAs. The PHoA, being an IP address, will have a distinct value in the Internet, and can thus aptly perform the role of node identifier. Thus, in TMMIPv6, the PHoA will identify the MN, the BID [41] will identify the node, and the HoA will be used in return routability procedure when a new CoA is to be registered at the CN.

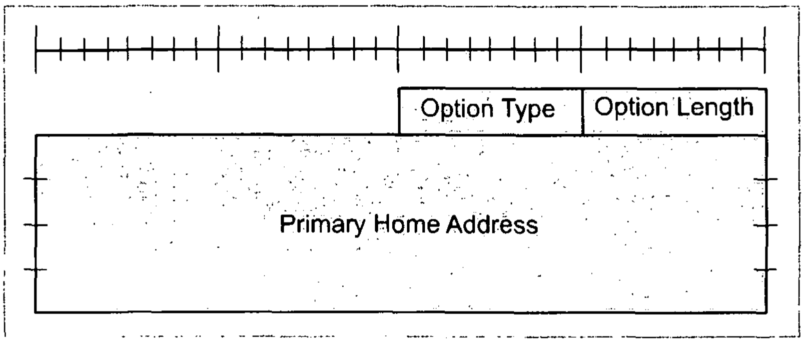


Figure 6.5: Primary Home Address (PHoA) Destination Option

Whenever a binding update is sent to the CN, the PHoA of the concerned MN must also be intimated, so as to assist the CN in identifying the MN in its binding cache. Towards this, a new option – *Primary Home Address Option* – is proposed in TMMIPv6. This new option will be carried by the Destination Option Extension Header of IPv6 packet. It will be included in the binding update message to CN. The format of this new option is shown in Figure 6.5.

The value of the *Option Type* has to be assigned as this is a newly introduced option. The value of *Option Length* is the length of this option in terms of number of octets, excluding the *Option Type* and *Option Length* fields. The value of this *Option Length* field will thus be set to 16 (since an IPv6 address is 16 octets long). The remaining field in this option should contain the PHoA of the concerned MN.

6.2.2. Link Quality Estimation Init Destination Option

TMMIPv6 distributes the traffic to/through the available interfaces of the MN depending on the link characteristic at those interfaces. This is done by the convergence module at the sender, with due participation from the corresponding convergence module at the receiver. The estimation process is initiated when the sender attaches its timestamp to an outgoing packet (Section 4.3.3).

The *Link Quality Estimation Init* option is introduced to carry this timestamp for the estimation of the link quality at an interface. This new option will be carried in the Destination Option Extension header of the IPv6 packet, since this value is of interest only to the other communication end point. Moreover, this option is not specific to mobility management messages and can be included in any outgoing packet to the destination. The format of this option is shown in Figure 6.6.

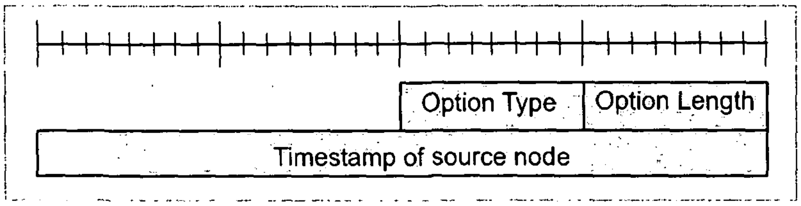


Figure 6.6: Link Quality Estimation Init Destination Option

The value of the *Option Type* has to be assigned as this is another new option introduced. The value of *Option Length* is the length of this option in terms of number of octets, excluding the *Option Type* and *Option Length* fields. The value of this *Option Length* field will be set to 4. The remaining field will contain the timestamp (TS_s as described in Section 4.3.3) inserted by the sender (of original flow) when the packet got queued at the source.

6.2.3. Link Quality Estimation Destination Option

On receiving the Link Quality Estimation Init option, the convergence module at the receiving node will store the contained timestamp along with the size of the received packet and the time when the option was received. Later on, when a packet is queued at the original receiver to be sent to the original sender (a TCP ACK message, for example), the convergence module at the original receiver will include the previously received timestamp, the received packet size. and the delay between receiving the original packet and queuing of the current packet.

A new option – *Link Quality Estimation* option- is introduced to carry the above mentioned information back to the original sender. Being only of interest to the original sender, this option will be included in the Destination Option Extension header of the IPv6 packet. The format of this new option is shown in Figure 6.7.

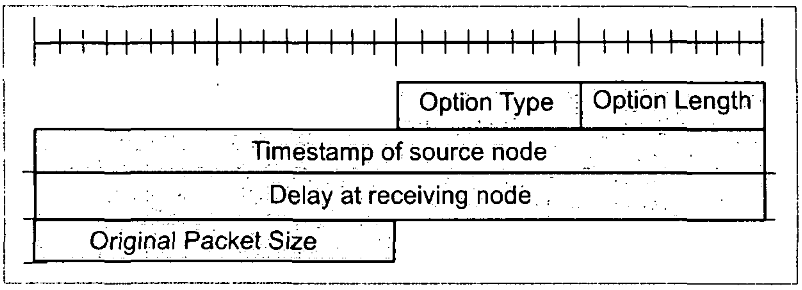


Figure 6.7: Link Quality Estimation Destination Option

As in the previous cases, the *Option Type* value has to be assigned. The option length should be set to 10 – 4 octets for Timestamp of Source Node (TS_s of Section 4.3.3), 4 octets for Delay at Receiving Node (ΔT_D of Section 4.3.3), and 2 octets for Original Packet Size (TS_s of Section 4.3.3).

6.2.4. Multi-CoA Mobility Option

In TMMIPv6 scheme, once the PCoA is registered at the CN, the MN sends the CoAs for all other available interfaces to the CN using the PCoA in a single message, instead of sending binding update messages for each of those CoAs separately. Thus a new option – *Multi-CoA* option –is introduced for this purpose. The format of this option is shown in Figure 6.8.

This mobility option will be included in the binding update message to CN after the key to authorize the binding for PCoA has been established through normal return routability procedure. If this option is included in the binding update message, then the Primary Home Address Destination Option (Section 6.2.1) must also be included for CN to correctly identify the MN under question, if the MN is equipped with multiple HoAs. Once the CN receives this option along with the binding update message, the convergence module at that end should initiate Return Routability Procedure at these CoAs individually. However, the CN will send the HoT and CoT messages for all other interfaces except for the one having PCoA without receiving the corresponding HoTI and CoTI messages. These messages will therefore contain the Home and Care-of Cookies received in HoTI and CoTI messages received during PCoA set up.

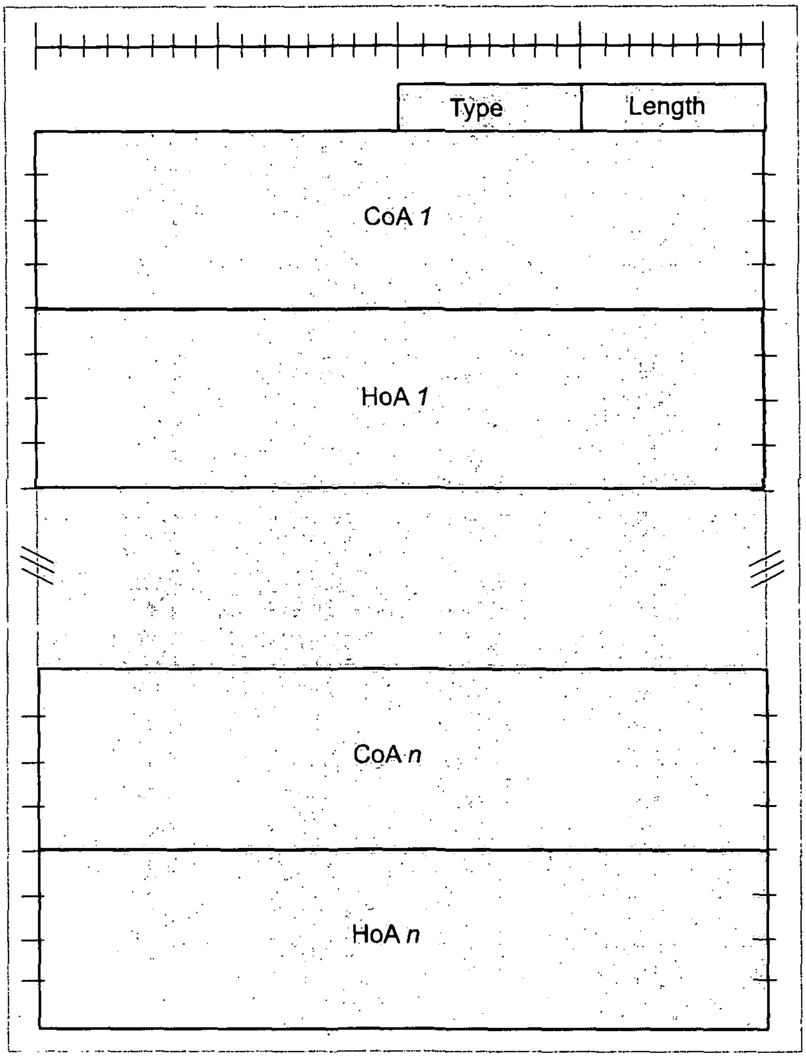


Figure 6.8: Multi-CoA Mobility Option

The *Type* value has to be assigned for this new mobility option. The *Length* field will include the number of octets in the option except the *Type* and *Length* fields. This value will therefore be *16×2×Number of CoAs*.

Apart from the new messages described above, an appropriate message with corresponding status value must be defined to be included in Binding Acknowledgement message to inform the MN in case a PHoA Destination Option, included in the binding update message to a node which does not have a convergence module, is ignored.

6.2.5. Addition to Conceptual Data Structures at MN and CN

In addition to the data stored at the MN and the CN [27], a few more data items will have to be stored to support the proposed TMMIPv6 modifications.

The concept of PHoA has been introduced in the TMMIPv6 scheme, and this value will have to be stored in the binding cache of the CN for every binding. This value will also have to be stored at the MN. At the CN, this value will be required to identify the node in the face of multiple CoAs for multiple interfaces. At the mobile node, this value will be needed in binding update messages sent to the CN(s), and for the consumption of transport layer which is oblivious of the existence of the multiplicity of interfaces.

Apart from PHoA, the CN should have its binding cache modified to store some other additional information. The values of the Home and Care-of Cookies received from a given node in its last Home Test Init (HoTI) and Care-of Test Init (CoTI) messages must also be recorded. These would be required when the correspondent node responds to Multi-CoA Mobility Option (Section 6.2.4) with Home Test (HoT) and Care-of Test (CoT) messages to those CoAs (Section 4.5.1.2).

Additionally, both the MN and the CN will record the BID [41] for every mobile node interface.

The link quality estimation, which determines the proportion of packets through/to a given interface, may be done by placing the timestamp in every outgoing packet. Optionally, to reduce the overhead, the link quality estimation may be done only intermittently. In that case, the sender will not include the Link Quality Estimation Init destination option (Section 6.2.3) in every outgoing packet, but will include the same only at specified intervals, or when a new CoA gets registered. The sender will, therefore, need to record the number of seconds before the next Link Quality Estimation Init option should be included in the outgoing packet.

6.2.6. Message Handling

The TMMIPv6 scheme envisages minor changes in the way the mobility and destination options are handled compared to the base MIPv6 [27]. The MN-HA communication will flow exactly the way it is envisaged in MIPv6. The changes will be required only when route optimization is implemented and there is direct MN-CN traffic. Hence, the modifications in messages are mainly discussed focusing on the MN-CN traffic. The only exception to this will be the one informing the CN about other MN HoAs (in addition to PHoA) when route optimization is not endeavored. Following sub-sections discuss the handling of new messages as well as changes in handling of existing messages.

6.2.6.1. Binding update

The binding update message, as usual, will be sent to the CN after return routability procedure has been completed successfully. If the MN has only a single HoA, then the Primary Home

Address Destination Option will not be included in the binding update message. However, if the MN has multiple HoAs, the binding update message must include the Primary Home Address Destination option along with the usual Home Address Option. The Primary Home Address Destination option is needed to inform the CN about the MN's identity (PHoA), while the Home Address Option is needed to carry the HoA so that the CN can verify the Binding Management Key (kbm) which, apart from CoA, also involves the HoA. In addition, the binding update will also contain the Binding Unique Identifier sub-option [41], which identifies the exact interface bearing the new CoA. Optionally, if the MN needs to inform CoAs of multiple interfaces, the binding update must also include Multi-CoA mobility option (Section 6.2.4). The following error conditions may arise while registering a CoA at the CN:

- When a CN – which is not equipped with the convergence module to support this multi-homing protocol – receives a binding update message with Primary Home Address Destination Option, it will send a Binding Acknowledgement message with appropriate status value. This will allow the convergence module at MN to infer the absence of the same at CN, and reverse the protocol operation back to the base MIP.
- If a CN, which does not support the proposed TMMIPv6 scheme, receives a binding update message containing a Multi-CoA mobility option, it will send an appropriate status value in the Binding Acknowledgement message, informing MN about its inability to support the proposed protocol.

On the other hand, if the binding update message containing a Multi-CoA mobility option is accepted successfully, the convergence module at CN should sent Home Test (HoT) and Care-of Test (CoT) messages to all the CoAs included in the said mobility option. Since these HoT and CoT messages are sent without the corresponding Home Test Init (HoTI) and Care-of Test Init (CoTI) messages from the MN, the Home Init Cookie and Care-of Init Cookie in the HoT and CoT messages will be replaced by the corresponding values used in last HoTI and CoTI messages sent from the same MN. If these Home Init and Care-of Init cookies match with those previously recorded at MN, the convergence module at MN will send binding updates for each CoA using respective kbm.

The convergence module at MN may also use the binding update message to inform the corresponding module at the CN about the unavailability of a given interface. For this, the convergence module at MN will send an explicit binding update with registration lifetime value set to zero and the CoA to the home address as in MIPv6. However, to allow the CN to identify the exact binding to be deleted, such a binding update message must also include the

Primary Home Address Option (to identify the node) and the Binding Unique Identifier sub-option (to identify the CoA to be deleted).

As per base MIPv6, the binding update message is sent to the CN only when route optimization is used. However, in TMMIPv6 scheme, the MN may need to inform the CN about its other HoAs, even if route optimization is not envisioned. This will be required to inform the CN about its HoAs other than the PHoA. The CN can then send packets distributed over these available HoAs, which will then be tunneled by the HAs to the respective MN interfaces. Similarly, CN can expect packets reaching it after being reverse tunneled to the HAs corresponding to those HoAs. Towards this end, the MN will initially send the HoTI message using each HoA, and follow it up with binding update message after it has received the corresponding HoT message from the CN. In this case, the kbu should be calculated by replacing the CoA with zero. Such a binding update message will contain the Primary Home Address Destination Option, but not the Home Agent Option (since the particular HoA will now be included as the source address in the IP header). Obviously, this entire procedure will not be needed if the MN has only a single HoA.

6.2.6.2. Link Quality Estimation Init Destination Option

If the Link Quality Estimation Init option is to be included in a packet queued at the sender (as inferred from the time remaining before next such option is sent), the convergence module at the sender will record its timestamp in the appropriate field.

When the receiver accepts such a packet, it will store the timestamp of source node in the appropriate buffer. The buffer for the given interface will be identified by the source/destination address and the home. If such a buffer does not exist, the receiving convergence module will set up the same. The convergence module will also record it own timestamp and the packet size in the buffer as discussed in Section 4.3.3.

6.2.6.3. Link Quality Estimation Destination Option

When a (acknowledgement) packet is queued at the receiver at/for a particular interface, and the corresponding buffer has a recorded timestamp from a previously received Link Quality Estimation Init option, the convergence module at that end will include the *Link Quality Estimation* option and fill in the appropriate field as discussed in Section 6.2.3.

When the original sender receives a packet containing this option from/at a particular interface, the convergence module at this end now estimates the link characteristics as described in Section 4.3.3. This estimation will henceforth be used in determining the proportion of packets sent to/from the given interface.

6.2.6.4. Home Address Option

The CN may receive packets from the MN containing the Home Address Option. This is used for exchanging the HoA from the Home Address Option into the IPv6 header and replacing the original source address for the consumption of higher layers. Such a replacement of source address makes mobility transparent to the layers above the network layer.

If the packet containing this option is a binding update message, it should be handled as discussed in section 6.2.6.1. For other messages, the CN must reject the packet if the HoA in the option is not found in the binding cache of the CN [27]. However, if the home address is found in the CN's binding cache and the corresponding CoA is actually the source of the said packet, the convergence module at CN will replace the source address of the packet with the corresponding PHoA found against the HoA in its binding cache (and not by HoA as in MIPv6). The PHoA acts as the node identifier in the TMMIPv6 scheme, and is used for the upper layers' consumption.

6.2.6.5. Type 2 Routing Header

As discussed in [27], this routing header is included in packets routed directly from the CN to the MN's CoA. This header contains the HoA, which accordingly replaces the destination address before the packet is forwarded to transport layer.

However, in TMMIPv6 scheme, instead of the HoA, the PHoA is used for identifying the transport layer connection. Thus, the convergence module at MN will use the HoA in this Routing Header to identify the PHoA from its binding cache, and use the later to replace the destination address in the IP header.

6.3. Summary

In this chapter, the new message formats required for execution of the MAAH as well as the TMMIPv6 schemes are discussed. While the MAAH scheme brings in one new message, the TMMIPv6 requires the introduction of four such messages. Apart from the new ones, a few message formats underwent minor modifications, while there were changes in the way some others are handled. Except for the messages mentioned here, none of the other messages will require any change – either in their format or in the way they are handled by the respective entities.

Chapter 7

Conclusions

The research works reported in this thesis are aimed at reducing handover latency in MIPv6. Such a reduction in handover latency will make MIPv6 more acceptable for today's real time applications. While MIPv6 allows retaining the TCP connection uninterrupted in the face of changing location of the Mobile Nodes (MNs), it introduces substantial delays while managing handovers. This delay results from the requirement of registration at the Home Agent (HA) and the correspondent node (CN) for every handover that MN performs. The requirement of these registrations, every time the MN changes its point of attachment, may give rise to intermittent increase in packet latency, and result in deterioration of service and consequently the user experience, to the extent of connection disruption. In addition, during the process of registering new CoA at HA or CN, the packets reaching the old access router (AR) may be forwarded to the new CoA, or they may be dropped. In case the packets are forwarded to the new access router, the more time the new CoA registration consumes, more will be the number of packets reaching the MN redirected by the previous AR. These packets pass through an un-optimized route via the previous network, and an increase in their number will also worsen the quality of service due to increased packet latency. On the other hand, if the packets reaching the previous access router are dropped, a high handover latency will result in greater packet drop and consequent re-transmissions, thereby increasing the load on the network. Moreover, every registration at HA or at CN(s) has a finite lifetime. These registrations therefore, need to be renewed at the expiry of the registration lifetime, even in the absence of any node movement. A decrease in the time consumed for these re-registrations will also add to efficiency of the system.

This thesis proposes two enhancements to MIPv6 – the MIPv6 with Mobile Agent Assisted Handover (MAAH) scheme, and the Transparent Multihomed MIPv6 (TMMIPv6) scheme. The first scheme presumes that the MN is a single interfaced one. It utilizes the assistance of mobile agents to reduce the effective path traversed by the registration messages. The second scheme is applicable to multi-interfaced MNs. It allows for splitting of a single flow across multiple interfaces and diverting the traffic from one interface in case of handover through a process of soft handover.

7.1. MAAH Scheme

The MAAH scheme employs mobile agents to ensure optimal or near optimal path for the registration related messages. However, to make these mobile agents execute, the network must provide adequate support for the same. This scheme therefore, requires the presence of *Mobile Agent Platform* (MP) at the ARs to support the mobile agents. The absence of MP at ARs will nonetheless, allow the ongoing communication to continue – only that the process will fall back on base Mobile IP.

The mobile agent is stationed at the previous AR, last visited by the MN before it connected to the current AR. One of the functions of this mobile agent is to proxy for the MN's HA. The registration messages from the MN can thus be forwarded to this mobile agent. Being present at the previous AR, the path traversed by this message is considerably reduced. Apart from registration messages sent to the HA, the MN also needs to send the same to the CN(s). However, to authenticate such registration messages, the MN will need to set up key(s) with its CN(s). In MIPv6, this is achieved by a challenge-response mechanism know as the Return Routability Procedure. This requires the MN to send two messages – one via it's HA and other directly – to the CN. The CN responds to each of these, and these messages follow the reverse path of the initiating messages. In MAAH scheme, the messages passing via the HA are made to instead pass via the mobile agent. In route optimized operation, since the path between the CN and the previous AR was optimized when the MN was present under that AR, the message from the new AR to the CN via the old AR will be a near optimal one. This will also contribute towards handover latency reduction.

While the MN at the previous access router participates in the registration process in lieu of the HA, the former will intermittently inform the latter about the current CoAs of all the MNs belonging to the given network serviced by the concerned mobile agent. This, as is done asynchronously with the handover process, will not contribute to the handover latency.

Simulation experiments were conducted to investigate the benefit of the scheme. While the actual extent of gain is topology dependent, the results show performance improvement for all the scenarios considered in the simulation.

7.2. TMMIPv6 Scheme

The TMMIPv6 scheme utilizes the availability of multiple interfaces at the nodes and the overlap of service areas of different service providers; the latter providing services through same or diverse access technologies. With multiple interfaces available – which may support different access technologies, a given flow can be split across these interfaces to profit from bandwidth aggregation. Moreover, when a given interface performs a handover, the traffic destined from/to that interface can be diverted to other available interfaces. This eliminates the requirement for packet redirection and possibility of packet loss at the time of handover. The additional packet latency due to handover is avoided. Once the particular interface completes the handover process, the traffic can once again flow through it at the previous rate, or at a rate supported by the current link characteristics.

To assist in the management of this splitting of flow, it is proposed that a *convergence module* (CM) be introduced at layer 3 of the protocol stack. While the sender node can split the flow across the interfaces, the receiving node will have to accumulate the packets belonging to the same flow. The CM will therefore be responsible for both splitting and accumulation of packets of a given flow. As flow splitting and consequent accumulation will be required at the communication end-points, the CM needs to be introduced at these positions. The CM will also be responsible for diverting the traffic from an interface which is performing a handover, and reallocate the same over other available interfaces. Once the handover process is over, the CM will take care of redistributing the traffic once again.

On completion of handover at an interface, the traffic should again be allowed to pass through that interface. This will require that the CN be informed about the newly configured CoA. The BU carrying this information to CN has to be authenticated before the latter updates its binding cache. The return routability procedure (RRP), which sets up the authentication key, involves interchange of four messages before the BU can be forwarded. With multiple interfaces per MN performing intermittent handovers, this will lead to a considerable increase in total number of control messages. This scheme, therefore, proposes that, for handover of non-primary interface, HoT and CoT messages be sent by the CN without receiving the initiating HoTI and CoTI messages respectively, as was envisaged in MIPv6. This will reduce the number of control messages to two per RRP.

With different interfaces supporting possibly diverse access technologies with dissimilar data transfer characteristics, the traffic across the interfaces will have to be appropriately distributed. The proportion of packets through the available interfaces should be decided dynamically, guided by the current network state at those interfaces. The CM also aids in estimating the link characteristics across the existing interfaces, and accordingly decides on the share of the flow across them. This estimation process involves the CMs at both ends, the one at the sender actually doing the estimation with due assistance from that at the receiver.

Additionally, the TMMIPv6 scheme introduces the concept to *Primary HoA* (PHoA) to identify the MN in presence of multiple HoAs. The presence of multiple HoAs is desirable, as it will allow the MN to receive packets at its other interfaces, when one or more of its interface(s) get attached to their respective home networks. In addition, to reduce the load on DNS servers – of all the HoAs, only the PHoA is included in the former.

Simulation experiments were carried out to illustrate the basic premise of the scheme-the benefit accrued through load balancing across multiple interfaces. The variation in packet latency was also studied, and compared to that of the base protocol. It is shown that under certain base station range, the packet latency variation can be kept similar to that of the base protocol, while increasing the data rate through bandwidth aggregation.

7.3. Interoperation of Schemes

This thesis also discusses the interoperation of micromobility schemes – particularly HMIPv6 – with the MAAH schemes. Interoperation of MAAH scheme along with TMMIPv6 is considered too.

The micromobility protocols aim to reduce the handover latency by making the MN movement within a region transparent to the HA. Within these regions, there is an authority – like Mobility Anchor Point (MAP) in HMIPv6 or CIP Gateway in case of Cellular IP – which takes care of MN movement inside the region. However, when the MN moves out of the given region, it has to once again register its bindings with it's HA. The regional authority also requires some type of security arrangement with the MN, so that the packets meant for the later cannot be hijacked by any malicious host.

The MAAH scheme, while interoperating with micromobility protocols like HMIPv6 or Cellular IP, can take care of MN registration when the latter moves across the micromobility domains. The mobile agent can be placed at the MAP or CIP Gateway, for example, and can support MN registration when there is an inter-domain movement. In addition, the mobile agent can see to the MN authentication for intra-domain MN movement. The MN, it's HA and mobile agent all belongs to the same administrative domain, and hence can have pre-configured security association. A similar association with MAPs or CIP Gateways will be next to impossible, given the number of MNs and the possible domains that they can visit.

The MAAH scheme can also be made to inter-operate with the TMMIPv6 scheme. This will be beneficial when the access routers are equipped with MP and the MNs are outfitted with multiple interfaces. In TMMIPv6 scheme, when an interface performs handover, the traffic is shifted to other available interfaces. However, the interface performing the handover does so following the usual MIPv6 procedure. The associated delay due to handover forces the given interface to remain idle, as far as data traffic is concerned, for that much time. If the handover delay at the interface can be reduced, there will be a proportional increase in the 'up-time' of the interface.

When a multi-interfaced node moves across ARs having mobile agent support, the MAAH scheme can be used to speed up the handover process. The interface undergoing handover can then register with the mobile agent at the previous AR, and use latter's assistance in its return routability procedure preceding the CN binding, as envisaged in MAAH scheme. In such a situation, the available interfaces will be accessible for most of the time resulting from a decreased 'down-time', consequential to speedier handovers.

7.4. New/Modified Message Formats

The thesis describes some new messages that would be required to manage the protocol modifications as well as the way in which they are handled. It also discusses certain modifications to existing message formats for supporting the proposed alterations to the base protocol.

For the MAAH scheme, a new mobility option - Home Agent Binding Mobility option – is introduced. The mobile agent uses this option with the Binding Update message to periodically update the home agent about the current locations of the MNs the former is serving. Apart from this, the Binding Update Message, HoTI Message and Router Advertisement Message are modified to suit the alterations in the protocol. In addition, there are slight changes in the way in which Binding Update Message, Binding Acknowledgement Message, HoTI Message and HoT Message are handled in the base protocol. The changes in the format and handling of above mention existing messages are necessitated by the introduction of the mobile agent.

For the TMMIPv6 scheme, three new IPv6 destination options and one mobility option have been defined – Primary Home Address Destination Option, Link Quality Estimation Init Destination Option, Link Quality Estimation Destination Option, and Multi-CoA Mobility Option. The Primary Home Address Destination Option is introduced to support the concept of the Primary Home Address (PHoA) discussed in this thesis. The Link Quality Estimation Init and the Link Quality Estimation Destination Options are used by the CMs at either end to estimate the quality of links at the available interfaces. This is required since the flow is split across the interfaces at proportions determined dynamically by this estimate. With the availability of multiple interfaces leading to multiple CoAs, the Multi-CoA Mobility option is used to intimate the CN of the existing CoAs.

Furthermore, the handling of existing Binding Update Message, Home Address Option and Type 2 Routing Header has been modified. These modifications are introduced to support and utilize the PHoA as an identifier for the MN.

7.5. Advantage of Proposed Schemes

The two schemes, MAAH and TMMIPv6, discussed in this thesis have certain advantages over other proposed schemes for handover delay reduction of single and multihomed mobile nodes.

Like other micro-mobility protocols, the MAAH scheme builds on the base MIP. In all the micromobility protocols, there is a central local authority – the Mobility Anchor Point in case of HMIPv6, CIP Gateway in case of Cellular IP and Domain Root Router in case of HAWAII – which takes care of MN's movement within its domain.

- The MN's CoA registration in the micromobility protocols is bifurcated into two distinct parts – registering the local domain address with the HA, and registering the actual location with the local central authority. The later may be done explicitly by MN with the appropriate authority, or may be achieved implicitly with the intermediate routers (between MN and the central authority of the concerned domain) recording an entry for the MN as they forward the packets originating from it. The second part of the registration procedure will require a trust mechanism between the router(s) of the visited domain and the MN. Such a trust mechanism may be difficult to achieve in practice, and may depend solely on a trusted third party. The MAAH scheme does not require any third party support to set up the communication between the concerned entities, just as envisaged in MIPv6.

- The micromobility protocols highlight the reduction in handover delay as long as MN confines its movement with a local domain, and limits the registration with the distant HA only for inter-domain migration. However, the registration of the local domain address (configured with central authority) with it's HA will have a definite lifetime like any other MIP CoA registration, and will have to be renewed before the expiry of this finite lifetime. The performance degradation due to such registration renewals at the HA are not discussed for the micromobility protocols. As for the MAAH scheme, with all registrations taken care of by the mobile agent at a nearby access router, the time required for such registrations and their consequent renewals will not have any appreciable effect on the efficiency of the protocol.

- When there is a new CoA registration or registration renewal for the local domain address, the CN will have to be informed about the same too for route optimized operation. The micromobility protocols, once again, do not discuss the effect of return routability procedure on the protocol performance. The MAAH scheme proposes the use of mobile agents at the previous access router to assist in the return routability procedure to optimize the path traversed by the HoT and HoTI messages, thereby reducing the resultant handover latency.

For mobile nodes equipped with multiple interfaces, MMI has been proposed to take advantage of the available interfaces for improved performance. Extensions to the transport layer protocol – SCTP – have also been defined to manage mobility at the transport layer.

- In MMI, the MN uses Load Balancing Mobility Option to inform the CN about the available interfaces. If CN is the sender, it is also informed about the proportions of packets to be sent to the different interfaces. However, the CN does not have any means to evaluate the link characteristics dynamically and accordingly determine the proportion of packets to be sent to those interfaces. The proportion is only determined by the MN. The TMMIPv6 scheme allows the sender (whether CN or MN) to dynamically estimate the link characteristics and accordingly distribute the packets over the interfaces.

- With multiple interfaces, each CoA has to be registered with the CN to achieve route optimized operation. Each of the binding update messages sent to the CN will require authentication before the binding cache at the CN is updated. While MMI follows the usual MIPv6 method to generate a key for every such authentication, TMMIPv6 introduces the concept of primary MN interface which is used to inform CN about the MN interfaces –thereby reducing the number of messages involved in the key setup procedure to half the MIPv6 requirement.

- The current extensions, proposed to support multi-homing, do not discuss the possibility for multiple HoAs. A single HoA will restrict the flow in the event of any one interface connecting to the home network. TMMIPv6 scheme, which proposes multiple HoAs for the MN, will allow the flow to/through all the interfaces, even if one or more interfaces are connected to their respective home networks.

- At any given time there is likely to be several transport layer connections from a host. In case of SCTP based mobility management solutions, any new addition or dropping of CoA has to be configured in the host individually for every such connection. This will lead to a lot of computational overhead and reconfiguration traffic overhead. In TMMIPv6 such overhead due to duplication of efforts do not arise as any addition or deletion of CoAs will be handled at the network layer keeping these transparent to the transport layer.

The results arrived through the simulation experiments indicate significant advantage for the proposed schemes, though the results are dependent on topology and the direction of movement of the mobile node. The improvement on account of the proposed schemes can be summarized as follows:

- For MAAH scheme, two topologies were used to perform the simulation experiments. The simulation in Chapter 3 using topology 1 showed aan average of 43.63% decrease in registration renewal time; while for topology 2 discussed in the same Chapter, the corresponding decreases were 35.73%, 59.09% and 54.19% for the perperdicular, diagonal and linear movements (Figures 3.10A, 3.10B and 3.10C) respectively.

- For TMMIPv6 scheme, simulations for the multi-interfaced node showed up to 95.66% increase in throughput, as compared to the single interfaced node. While it is evident that a multi-interfaced node – with its two interfaces – will have a higher throughput; the main advantage of these nodes, as borne out by the simulation experiments, was the absence of discontinuity in packet transfer due to handover, and that the same was achieved maintaining transparency to the higher layers.

7.6. Future Works

Some of the studies that can be carried out as a follow-up of the work presented in this thesis are-

- The return routability procedure needs the exchange of control messages between the MN and the CN, thereby significantly contributing to handover latency. It may be worthwhile to study the possibility of using the mobile agents in the authentication of the binding updates as it will significantly reduce the latency as well as signaling traffic.
- It may be useful to verify the performance of the proposed schemes in .real wireless network environment.
- Experimental studies may also be carried out to observe the performance of the TMMIPv6 scheme vis-à-vis SCTP based multihomed mobility support protocols that have been proposed recently.

Glossary

Mobility Related Terminology

This glossary describes the terms used in this thesis in relation to node mobility. Section 1 discusses the terms proposed in this thesis, while Section 2 lists out the existing terms with their meanings.

1. Terms proposed in this thesis

Convergence Module (CM)

The Convergence Module (CM) is introduced at the layer 3 of the protocol stack to manage the multiplicity of network interfaces. The function of the CM is to split a single flow across different interfaces at the sender, and accumulate the packets from the various interfaces to converge them into a singular flow at the receiver. This splitting at the sender's end and subsequent accumulation at the other end is done by keeping the interface multiplicity transparent to the transport layer above, so that the widely deployed TCP can function unaltered.

Primary Care-of Address (PCoA)

The Primary Care-of Address is redefined in this thesis to mean one of the care-of addresses out of the available ones that has been registered with the primary home address. The interface having this care of address is called the Primary Interface.

Primary Home Address (PHoA)

The Primary Home Address (PHoA) is any one of the home addresses assigned to the MN. When multiple home addresses are available for the multi-interfaced mobile node, this primary home address will function as the node's identifier in the correspondent node's Binding Cache. Any particular home address of the MN can be pre-designated as the Primary Home Address. In the presence of multiple home addresses, this invariant primary home address is used to retain the TCP connection undisrupted

2. Existing mobility related terminology [27][69]

Access Router (AR)

The mobile node's default router

Binding

The association of the home address of a mobile node with a care-of address for that mobile node, along with the remaining lifetime of that association

Binding Authorization

Correspondent registration needs to be authorized to allow the recipient to believe that the sender has the right to specify a new binding

Binding Management Key (kbu)

A binding management key is a key used for authorizing a binding cache management message. Return routability procedure provides a way to create a binding management key

Binding Update (BU)

A message indicating a mobile node's current mobility binding, and in particular its care-of-address

Care-of Address (CoA)

An IP address associated with a mobile node while visiting a foreign link; the subnet prefix of this IP address is a foreign subnet prefix.

Care-of Init Cookie

A cookie sent to the correspondent node in the Care-of Test Init message, to be returned in the Care-of Test message

Care-of Keygen

A keygen token sent by the correspondent node in the Care-of Test message

Control Message

Information passed between two or more network nodes for maintaining protocol state, which may be unrelated to any specific application.

Cookie

A cookie is a random number used by a mobile node to prevent spoofing by a bogus correspondent node in the return routability procedure

Correspondent Node (CN)

A peer node with which a mobile node is communicating.

Correspondent Registration

The return routability procedure followed by a registration, run between the mobile node and correspondent node.

Destination Option

Destination options are carried by the IPv6 Destination Options extension header. Destination Options include optional information that need to be examined only at the IPv6 node given as the destination address in the IPv6 header.

Foreign Subnet Prefix

A bit string that consists of some number of initial bits of an IP address which identifies a node's foreign link with the Internet topology.

Home Address (HoA)

An IP address assigned to a mobile node, used as the permanent address of the mobile node. This address is within the mobile node's home link.

Home Agent (HA)	A router on a mobile node's home link with which the mobile node has registered its current care-of address. While the mobile node is away from home, the home agent intercepts packets on the home link destined to the mobile node's home address, and forwards them to the registered care-of address
Home Init Cookie	A cookie sent to the correspondent node in the Home Test Init message, to be returned in the Home Test message
Home Keygen	A keygen token sent by the correspondent node in the Home Test message
Home Link	The link on which a mobile node's home subnet prefix is defined
Home Registration	A registration between the mobile node and its home agent, authorized by the use of IPSec
Home Subnet Prefix	A bit string that consists of some number of initial bits of an IP address which identifies a mobile node's home link within the Internet topology.
Host	Any node that is not a router
Interface	A node's attachment to a link
Keygen Token	A keygen token is a number supplied by a correspondent node in the return routability procedure to enable the mobile node to compute the necessary binding management key for authorizing a binding update
L2 Handover	A process by which the mobile node changes from one link-layer connection to another.

L3 Handover

Subsequent to an L2 handover, a mobile node detects a change in an on-link subnet prefix that would require a change in primary care-of address

Link

A communication facility or physical medium that can sustain data communication between multiple network nodes.

Link-layer Address

A link-layer identifier for an interface

Link-layer Trigger

Information from L2 that notifies L3 of the detailed events involved in handover sequencing at L2.

Mobile Agent Platform (MP)

The Mobile Agent Platform provides the concepts and mechanisms for agent management. The mobile agents can execute their task at a given host only if such a platform is present to provide the necessary support

Mobile Agents (MA)

Mobile Agents are processes dispatched from a source computer to accomplish a specified task. Each mobile agent is a computation along with its own data and execution state. After its initial submission, the mobile agent proceeds autonomously and independently of the sending client. As these mobile agents need to move across heterogeneous architectures, they tend to be independent of platform architectures. To assist them in traversing heterogeneous environments, they are almost universally written in interpreted machine-independent language

Mobile Node (MN)

A node that can change its point of attachment from one link to another, while still being reachable via its home address

Multihomed Mobile Node

A node is said to be multihomed when it has multiple IPv6 addresses, either because multiple prefixes are advertised on the link(s) the node is attached to, or because the node has multiple interfaces.

Nonce

Nonces are random numbers used internally by the correspondent node in the creation of keygen tokens related to the return routability procedure. The nonces are not specific to a mobile node, and are kept secret within the correspondent node.

Packet

An IP header plus payload

Prefix

A bit string that consists of some number of initial bits of an address.

Primary Care-of Address

Among the multiple care-of addresses that a mobile node may have at any given time, the one registered with the mobile node's home agent is called its *Primary Care-of Address*. (This is re-defined in this thesis, and is explained in the previous section)

Registration

The process during which a mobile node sends a Binding Update to its home agent or a correspondent node, causing a binding for the mobile node to be registered

Return Routability Procedure

The return routability procedure authorizes registrations by the use of cryptographic token exchange

Router

A node that forwards IP packets not explicitly addressed to itself.

Security Association

An IPSec security is a cooperative relationship formed by the sharing of cryptographic keying material and associated context.

Topology

A network can be viewed abstractly as a graph whose topology at any point in time is defined by a set of points connected by edges.

Bibliography

1. James Weatherall, Alan Jones: *Ubiquitous Networks and Their Applications*, IEEE Wireless Communications, February 2002, pp. 18-29

2. Mark Weiser: *Some Computer Science issues in Ubiquitous Computing*, Comm. ACM, Vol. 36, No. 7, July 1993, pp. 75-84

3. Nigel Davis, Keith Cheverst, Adrian Friday, Keith Mitchell: *Future Wireless Applications for a Networked City: Services for Visitors and Residents*, IEEE Wireless Communications, February 2002, pp.8-16.

4. Ian F Akyldiz, Jiang Xie, Shantidev Mohanty: *A Survey of Mobility Management in Next-Generation All-IP Based Wireless Systems*, IEEE Wireless Communications, August 2004, pp. 16-27.

5. John Markoulidakis, George Lyberopoulos, D Tsikas, E Sykas: *Mobility Modelling in Third Generation Mobile Telecommunications Systems*, *IEEE Personal Comm.*, pp. 41-56, Aug 1997

6. John Williams Floroiu, Reinhard Ruppelt, Dorgham Sisalem, Jerome Voglimacci Stephanopoli: *Seamless Handover in Terrestrial Radio Access Networks: A Case Study*, IEEE Communications Magazine, November 2003, pp. 110 - 116

7. William Stallings: *Data & Computer Communications*, 6th Ed., Prentice Hall of India, 2002

8. Andrew S Tanenbaum: *Computer Networks*, 4th Ed., Prentice Hall of India, 2002

9. Douglas E Comer: *Internetworking with TCP/IP – Principles, Protocols and Architectures*, Prentice Hall of India, 2002.

10. Dave Wisely, Philip Eardley, Louise Burness: *IP for 3G: Networking Technologies for Mobile Communications*, John Wiley & Sons Ltd., 2002.

11. Keiji Tachikawa: *A Perspective on the Evolution of Mobile Communications*, IEEE Communications Magazine, Oct 2003, pp. 66-73

12. Tomas Robles, Arndt Kadelka, Hector Velayos, Antti Lapperelainen, Andreas Kasler, Hui Li, Davide Mandato, Jussi Ojala, Bernhard Wegmann: *QoS Support for an All-IP System Beyond 3G*, IEEE Comm. Mag., August 2001, pp.64-72

13. Stefano M Faccin, Poornima Lalwaney, Basavaraj Patil: *IP Multimedia Services: Analysis of Mobile IP and SIP interactions in 3G Networks*, IEEE Communications Magazine, January 2004

14. Ted Taekyoung Kwon, Mario Gerla, Sajal Das, Subir Das: *Mobility Management for VoIP Service: Mobile IP vs. SIP*, IEEE Wireless Communications, October 2002, pp. 66-75.

15. *3rd Generation Partnership Project (3GPP)* , http://www.3gpp.org/

16. Lieve Bos and Suresh Leroy: *Toward an All-IP-Based UMTS System Architecture*, IEEE Network, Jan. 2001, pp. 36–45.

17. Peter J. McCann, Tom Hiller: *An Internet Infrastructure for Cellular CDMA Networks using Mobile IP*, IEEE Personal Communications, August 2000

18. Christophe Jelger, Thomas Noel: *Multicast for Mobile Hosts in IP Networks: Progress and Challenges*, IEEE Wireless Communications, October 2002, pp. 58-64

19. Auhutosh Dutta, Jasmine Chennikara, Wai Chen, Henning Schulzrinne: *Multicasting Streaming Media to Mobile Users*, IEEE Communications Magazine, Oct 2003, pp. 81-89

20. Ji-Hoon Lee, Tae-Ho Jung, Suk-Un Yoon, Chul-Hee Kang: *An Adaptive Resource Allocation Mechanism Including Fast and Reliable Handoff in IP-Based 3Gwireless Networks*, IEEE Personal Communications, Dec 2000, pp. 42-47.

21. Aurelian Bria, Fredrik Gessler, Olav Queseth, Rickard Stridh, Matthias Unbehaun, Jiang Wu, Jens Zander: *4th-Generation Wireless Infrastructures: Scenarios and Research Challenges*, IEEE Personal Communications, Dec 2001, pp. 25-31

22. Peter Newman: *In Search of the All-IP Mobile Network*, IEEE Radio Communications, December 2004, pp. S3-S8

23. Suk Yu Hui, Kai Hau Yeung: *Challenges in the Migration to 4G Mobile Systems*, IEEE Communications Magazine, December, 2003, pp. 54-59

24. Wesley M Eddy: *At What Layer Does Mobility Belong?*, IEEE Communications Magazine, October 2004, pp. 155-159

25. Nilanjan Banerjee, Wei Wu, Sajal K Das: *Mobility Support in Wireless Internet*, IEEE Wireless Comm, October 2003, pp. 54-61

26. Soojin Kim, Hyung Joon Cho, Hee Hyuck Hahm, Sang Yun Lee, Myung Sung Lee: *Interoperability Between UMTS and CDMA2000 Networks*, IEEE Wireless Communicaitons, February 2003, pp. 22-28

27. David Johnson, Charles Perkins, Jari Arkko: Mobility *Support in IPv6*, IETF Network Working Group RFC 3775, June 2004

28. Charles Perkins, Ed.: *IP Mobility Support for IPv4*, IETF Network Working Group RFC 3344, August 2002

29. Hesham Soliman, Claude Castelluccia, Karim El-Malki, L. Bellier: *Hierarchical MIPv6 Mobility Management*, IETF Network Working Group RFC 4140, August 2005

30. Rajeev Koodli Ed.: *Fast Handovers for Mobile IPv6*, IETF Network Working Group RFC 4068, July 2005

31. Andrew T Campbell et al: *Cellular IP*, Internet Draft (Expired), Jan 2000

32. Andrew T. Campbell, Javier Gomez, Sanghyo Kim, Chieh-Yih Wan: *Comparison of IP Micromobility Protocols*, IEEE Wireless Comm., Feb 2002, pp 72-82

33. Eva Gustafsson, Annika Jonsson: *Always Best Connected*, IEEE Wireless Communications, February 2003, pp. 49-55

34. Pedro Marques, Hekder Castro, Manuek Ricardo, *Monitoring Emerging IPv6 Wireless Access Networks*, IEEE Wireless Communications, Feb 2005, pp. 47-53

35. Ian F. Akyildiz, Shantidev Mohanty, Jiang Xie: *A Ubiquitous Mobile Communication Architecture for Next-Generation Heterogeneous Wireless Systems*, IEEE Radio Communications, June 2005, pp. S29-S36

36. Nicolas Montavont, Ryuji Wakikawa, Thierry Ernst, Thomas Noel, C. Ng, *Analysis of Multihoming in Mobile IPv6*, IETF MIP6 Working Group Internet Draft (Work in Progress), June, 2006.

37. Maximilian Riegel, Michael Tuexen: *Mobile SCTP*, IETF Network Working Group Internet Draft (Work in Progress), October 2006

38. Thierry Ernst, Nicolas Montavont, Ryuji Wakikawa, Eun Kyoung Paik, C. Ng, K. Kuladinithi, Thomas Noel, *Goals and Benefits of Multihoming*, Internet Draft (Expired), October, 2005

39. Nicolas Montavont, Thomas Noel, Kassi, K.: *Mobile IPv6 for Multiple Interfaces*, IETF Mobile IP Working Group Internet Draft (Expired), July, 2005

40. Mobile Nodes and Multiple Interfaces in IPv6 (monami6) Working Group Official Charter, http://www.ietf.org/html.charters/monami6-charter.html

41. Ryuji Wakikawa, Thierry Ernst, K. Nagami: *Multiple Care-of Address Registration*, MIPv6 Working Group (Work in Progress), October 2006

42. Ian F Akyildiz, Janise McNair. Joseph Ho. Huseyin Uzunalioglu Wenye Wang: *Mobility Management in Next-Generation Wireless Systems*, Proc. Of IEEE, pp. 1347 – 1384, Aug 1999

43. Stephen E. Deering, Robert Hinden: *Internet Protocol, Version 6 (IPv6) Specification*, IETF Network Working Group RFC 2460, 1998

44. Information Sciences Institute, University of Southern California: *Internet Protocol - DARPA Internet Program Protocol Specification*, IETF RFC 791,1981

45. Jari Arkko, Vijay Devarapalli, Francis Dupont.: *Using IPSec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents*, IETF Network Working Group RFC 3776, 2004

46. Pete McCann: *Mobile IPv6 Fast Handovers for 802.11 Networks*, IETF Network Working Group RFC 4260, November 2005

47. Ramachandran Ramjee, Thomas F. La Porta, Sandra R. Thuel, Kannan Varadhan, Luca Salgarelli: *IP micro-mobility support using HAWAII*, IETF Internet Draft (Expired), Jul 2000

48. Randall R. Stewart, Qiaobing Xie, Ken Morneault, Chip Sharp, Hanns Juergen Schwarzbauer, Tom Taylor, Ian Rytina, Malleswar Kalla, Lixia Zhang, Vern Paxson: *Stream Control Transmission Protocol*, RFC 2960, October 2000

49. Lyndon Ong , John Yoakum: *An Introduction to the Stream Control Transmission Protocol (SCTP)*, RFC3286, May 2002

50. Jonathan Stone, Randall Stewart, Douglas Otis: *Stream Control Transmission Protocol (SCTP) Checksum Change*, RFC 3309, September 2002

51. Randall Stewart: *Stream Control Transmission Protocol (SCTP) Dynamic Address Reconfiguration*, IETF Network Working Group Internet Draft (Work in Progress), October, 2006.

52. Randall Stewart, Chris Metz: *SCTP: New Transport Protocol for TCP/IP*, IEEE Internet Computing Mag., November-December 2001, pp. 64-6

53. Armando L Caro, Janardhan R Iyengar, Paul D Amer, Sourabh Ladha, Gerard J Heinz, Keyur C Shah.: *SCTP: A Proposed Standard for Robust Internet Data Transport*, IEEE Computer Mag., November 2003, pp. 56-63

54. Fu, S., Atiquzzaman, Md., *SCTP: State of the Art in Research, Products, and Technical Challenges*, IEEE Comm. Mag., April 2004, pp. 64-76

55. Ilknur Aydin, Chien-Chung Shen: *Cellular SCTP: A Transport-Layer Approach to Internet Mobility*, IETF Network Working Group Internet Draft (Expired), October 2003

56. Shaojian Fu, Mohammed Atiquzzaman, Justin S. Jones, Yong-Jin Lee, Song Lu, Liran Ma: *TraSH: A Transport layer Seamless Handover scheme*, Tech. Rep., Computer Science, University of Oklahoma,, November 2003

57. Mohammed Atiquzzaman, Shaojian Fu, William Ivancic: *TraSH-SN: A Transport Layer Seamless Handoff Scheme for Space Networks*, Proc. Of NASA Earth Science Technology Conference (ESTC2004), Palo Alto, CA, 2004

58. Wesley M. Eddy, Joseph Ishac, Mohammed Atiquzzaman: *An Architecture for Transport Layer Mobility*, IETF Network Working Group Internet Draft (Expired), August, 2004

59. Thomas R Henderson: *Host Mobility for IP Networks: A Comparison*, IEEE Network, Nov-Dec 2003, pp. 18-26

60. Petri Mahonen et al: *Hop-by-Hop Towards Future Mobile Broadband IP*, IEEE Comm. Mag., March 2004, pp. 138-146

61. George Samaras: *Mobile Agents: What about them? Did they deliver what they promised? Are they here to stay?*, Proc. Of 2004 IEEE Intl. Conf. on Mobile Data Management, 2004

62. Amitabh Mishra, Ketan Nadkarni, Animesh Patcha: *Intrusion Detection in Wireless Ad-Hoc Networks*, IEEE Wireless Comm. Mag, Feb 2004, pp. 48-60

63. Michael S. Greenberg, Jennifer C. Byington, David G. Harper: *Mobile Agents and Security*, IEEE Comm. Mag., July 1998, pp. 76-85

64. Vn Anh Pham, Ahmed Karmouch: *Mobile Software Agents: An Overview*, IEEE Comm. Mag. July 1998, pp. 26-37

65. Shivanajay Marwaha, Chen Khong Tham, Dipti Srinivasan: *Mobile Agents Based Routing Protocol for Mobile Ad Hoc Networks*, Proc. Of IEEE Global Telecommunications Conference, 2002

66. Eung-Gu You, Keum-Suk Lee: *A Mobile Agent Security Management*, Proceedings of the 18th International Conference on Advanced Information Networking and Application (AINA'04), IEEE Computer Society, 2004

67. URL: http://www.isi.edu/nsnam/ns/

68. Thomas Narten, Erik Nordmark, William Allen Simpson: *Neighbor Discovery for IP Version 6 (IPv6)*, IETF RFC 2461, December 1998

69. Jukka Manner (ed.), Markku Kojo (ed.): *Mobility Related Terminology*, IETF RFC 3753, June 2004

Author's Publications

1. Basav Roychoudhury, Dilip K Saikia: *Optimization of Mobile IP Binding Update Traffic*, Proc. Of Intl. Wksp. On Distributed Computing, Kolkata, Dec 2001, pp. 103-108.

2. Basav Roychoudhury, Dilip K Saikia: *Reducing Handover Latency in MIPv6 Using Mobile Agents*, Proc. Of Sixth Intl. Conf. on Information Technology, Bhubneswar, Dec 2003, pp. 574-575.

3. Basav Roychoudhury, Dilip K Saikia: *Mobility Management – A Survey*, Proc. Of Natl. Wksp. On Trends and Issues in Wireless Networks and Mobile Computing, Tezpur, Aug 2004, pp. 63-81.

4. Basav Roychoudhury, Dilip K Saikia: *Performance Enhancement of Mobile IPv6 Through Mobile Agents*, Proc. Of Natl. Wksp. On Trends and Issues in Wireless Networks and Mobile Computing, Tezpur, Aug 2004, pp. 25-36.

5. Basav Roychoudhury, Dilip K Saikia: *A Macro-Mobility Scheme for Reduction in Handover Delay and Signaling Traffic in MIPv6*, Proc.of 6th Intl. Wksp on Distributed Computing – LNCS 3326, Springer Varlag Publication, Dec 2004, pp.186-191.

6. Basav Roychoudhury, Dilip K Saikia: *Transparent Multihoming Protocol Extension for MIPv6 with Dynamic Traffic Distribution across Multiple Interfaces*, To appear in Proc. Of International Joint Conferences on Computer, Information, and Systems Sciences, and Engineering (CIS^{2}E 06), Bridgeport, December, 2006.

7. Basav Roychoudhury, Dilip K Saikia: *Transparent Multihomed Mobile IP – An Extension for Mulihomed Mobile Nodes*, Communicated.