MOBILE IP WITH A CLUSTER OF FOREIGN AGENTS

BY

RAMASAMY RAJA CHINNANCHETTY

Bachelor of Engineering

University of Madras

Chennai, India

2000

Submitted to the Faculty
of the Graduate College of
Oklahoma State University
in partial fulfillment of
the requirements for
the Degree of
MASTER OF SCIENCE
December 2002

MOBILE IP WITH A CLUSTER OF FOREIGN

AGENTS

Thesis Approved:

Thesis Advisor

Dean of the Graduate College

Preface

The Internet world is rapidly progressing from a wired era to a wireless era. New protocols are designed for this transition. Mobile IP is one protocol that enables the user to remain connected irrespective of the physical location. Key performance issues of Mobile IP are latency of update messages and frequent updates (control messages) to home agents and communicating nodes. This thesis outlines a technique to cluster the foreign agents in attempts to reduce latency with respect to communication with Mobile Nodes, and also reduce the frequency of updates to the home agents and the communicating nodes. Apart from the reduction in frequency of messages, we also improve the rate at which the information is updated about the mobile node's location, and yield better results for increased rate of mobility of the node.

ACKNOWLEDGEMENTS

I wish to express my sincere appreciation to Dr. Johnson Thomas for his guidance and assistance at Oklahoma State University. I would also like to thank my committee members, Dr. G.E. Hedrick and Dr. John.P.Chandler, for their helpful contributions and advice.

A heart-felt thanks goes to my parents and my sister for their unending encouragement and emotional support throughout the years.

Finally I would like to thank all my friends who stood beside me with their unfailing and indispensable support.

Table of Contents

Chapter 4 Problems With Mobile IP

Chapter 5 Proposed Solution

Chapter 6 Simulation and Results

Chapter 7 Conclusions

List of Figures

Figure **Page**

List Of Symbols

ARP	-	Address Resolution Protocol.
CH	-	Cluster Head.
CN	-	Correspondent Node.
FA	-	Foreign Agent.
HA	-	Home Agent.
IP	-	Internet Protocol.
ICMP	-	Internet Control Message Protocol.
MN	-	Mobile Node.
TCP	-	Transmission Control Protocol.

Chapter 1

Introduction

1.1 Computing World

Computers has transformed from an Analytical Engine to super Computers that have greater user convenience, processing power, more storage, and better display technologies. Just as there has been an unstoppable trend towards having additional computing power at one's fingertips, the world of networked computing has similarly advanced at an amazing pace, approximately doubling in connectivity and reach, every year. This implies that the number of computer users connected to the network next year is likely to exceed the total number of network-connected people in each previous year added together. This rate of growth has caused revolutionary changes in network technology development and has created social, business, and legal advances for integrating the technology into everyday life.

Over the past few years, there has been an explosive growth in the number of notebook and laptop computer sales and correspondingly, in the number of nodes that are connected to the internet. Nowadays these laptops are comparable to desktop computers with similar or superior processing capabilities. Researchers are expecting that the future growth of internet is likely to be fueled in large part by these very laptop computers, since they account for the part of the computer market that is growing the fastest. There is

also a steady growth of the market for wireless communication devices. These device can only have the effect of increasing the options for making connections to the internet. In the near future communicating via laptop computers should be as natural as using a telephone. The day will arrive when no person will ever feel lost or out of touch using mobile computing.

1.2 Mobility and Portability

Until the mid 90s mobile computer users have had to be satisfied with portable operation. That is, the computer can be operated at any set of points of attachment, but not when the computer is in motion. When the computer is moved from one place to another, then its network connections have to be shut down and reinitialized at the new point of attachment to the network. In the near future, mobile users will not be satisfied with this portable operation; rather, they would need a truly mobile operation, so that the laptop can remain in almost continuous contact with the network when the node is in motion.

1.3 Types of Mobility

There are two basic types of mobility – Nomadic and Cellular.

- Nomadic mobility is typically associated with a laptop user, especially those who travel from place to place and use their laptop in each place, but switches it off in between. Most of their mobility problems can be solved with dynamic addressing schemes like Dynamic Host Configuration Protocol (DHCP) or Point-to-Point (PPP).

- Cellular mobility is the requirement for the device to transmit data while in motion. This includes embedded applications, cellular applications etc.

Based on the geographic area the two types of mobility that can be termed are Micro-Mobility and Macro-Mobility.

As the name implies, Micro mobility involves smaller geographic area. Here we have fast and frequent handoffs. Macro mobility involves larger geographic area. We have fewer handoffs compared to micro mobility.

Some issues of mobility are latency and frequent updates to the Home Agent (HA). In this thesis we have proposed techniques to reduce the frequency of update messages sent to the HA and the latency time. This provides a more reliable Mobile IP with fast handoffs. We have simulated the existing and proposed methods and also compared their performances.

The organization of this thesis is as follows. In Chapter 2, background information on Mobile IP and related work is provided. Chapter 3 describes the operating mechanisms of Mobile IP and Route Optimizations extensions provided to Mobile IP. The typical problems in Mobile IP are discussed in Chapter 4. In Chapter 5, the description of the proposed approaches is given. Chapter 6 evaluates the performance of the proposed approaches, and in the last Chapter the thesis is concluded with pointers for future research.

Chapter 2

Mobile IP: A Primer

2.1 Overview of IP and Routing

Routing protocols within the internet allow the routers to exchange information about the networks they inter-connect. When the routing information flows across the network each router will eventually learn enough to send any datagram along the correct route to the destination. Routers have to decide how to forward each packet they receive, selecting from several outgoing interfaces. They keep track of a small proportion of the total number of routes within the internet. Routers attempts to find an appropriate route for each packet they receive, and if they fail in their attempt, the packet is forwarded to another default router for further handling. The packets proceed in this way until they reach the correct network in a few local hops, or they have go across national and international routers to be delivered to the destination.

IP network address allocation and administration have historically assumed that there is a close relationship between a computer's IP address and its physical location. This is because of the assumption that a network is built using a wire (a Ethernet cable), and can be localized. The network is addressed by a single prefix and all computers in that network share the same prefix. This implies that two computers connected to the same network can communicate with each other without using a router.

IP addresses have two parts (refer Figure 2.1)

1. Network Prefix defines the network on which the address resides.
2. Host Address that identifies the node/host with in that network.

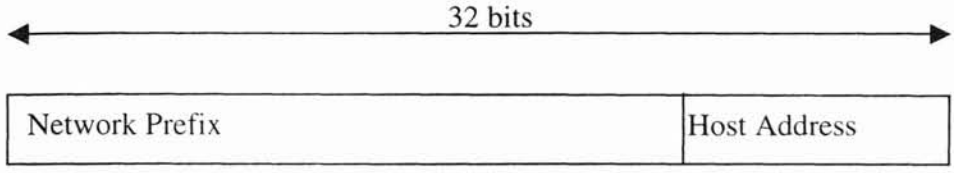


Figure 2.1 IP Address Structure

All IP address addresses are split up into subnet prefixes and host addresses. The router has entries that refer to larger sets of hosts, namely, those that are located together on a subnet. The routers use a kind of topological addressing and make the assumption that hosts with the common routing prefixes can share a common route.

2.2 Mobility Using IP

IP addresses are often thought of as semantically equivalent to Domain Name Server's (DNS) "Fully Qualified Domain Names" (FQDNs). Conceptually one can either use an IP address or a FQDN to identify one particular node out of the millions of nodes in the internet. The TCP keeps track of the internal session state between the communicating end points by using the IP address of the two communicating endpoints, along with the port numbers.

However, IP addresses are also used to find a route between the endpoints. The route does not have to be the same in both directions. Modelling the session as a bi

directional byte stream, the IP destination address for datagrams going in one direction would be the same as the IP source address for datagrams going in the opposite direction. The route selected depends on the IP destination address. It is a contradictory situation for mobile computing. On one hand, a mobile computer needs to have a stable IP address in order that it might be stably identifiable to other internet computers. On the other hand, if the address is stable, then the routing to mobile computer is stable and the packets also go to the same place and so, no mobility. So using the current internet protocol, mobile computing isn't possible.

In IP networking, an IP address indicates the point of the attachment for each node, which is similar to the telephony network. For example each telephone socket has a fixed telephone number. Likewise, when a laptop connects to a different network, it needs a new IP address to indicate its current location and keep its communication with the internet. Otherwise the packet addressed to the node connected to different network becomes unreachable and unroutable. As a consequence a key issue of Mobile IP design is **how to make the IP address transparent**.

2.3 Mobile IP Design Principles

Mobile IP was designed with the following characteristics in mind as the baseline requirements:

1. A MN must be able to communicate with other nodes, after changing its link-layer point of attachment to the Internet, without changing its IP address.
2. A MN must be able to communicate with other nodes that do not implement Mobile IP. No protocol enhancements are required in hosts or on routers unless they are performing the functions of one or more of the new architectural entities.

3. All messages used to transmit information to another node about the location of a MN must be authenticated to protect against remote redirection attacks.

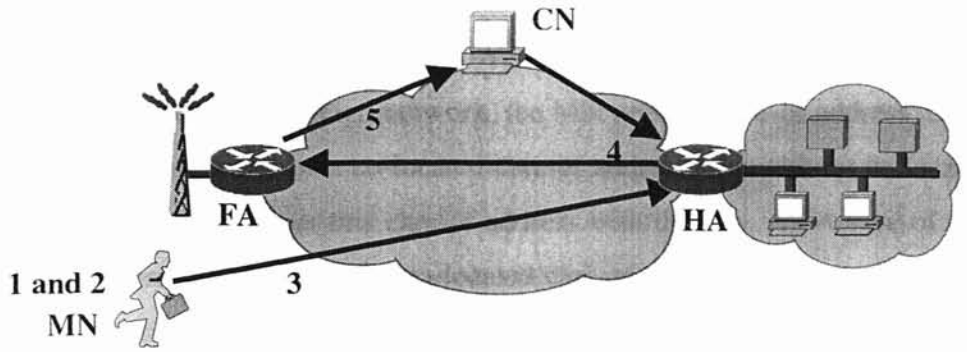
4. The link by which a MN is directly attached to the Internet may often be a wireless link. This link may thus have a substantially lower bandwidth and higher error rate than traditional wired networks. Moreover MNs are likely to be battery powered, and minimizing power consumption is important. The number of administrative messages sent over the link by which a MN is directly attached to the Internet should be minimized, and the size of these messages should be kept as small as possible.

5. Mobile IP places no additional constraints on the assignment of IP addresses. This implies that a mobile node can be assigned an IP address by the organization that owns the machine. In particular, the address does not have to belong to any globally constrained range of addresses.

Mobile IP enables mobility across homogenous and heterogeneous media (for e.g., from Ethernet segment to a Wireless LAN). This is because Mobile IP does not place any restriction on the layer-2 operation of a MN.

2.4 Mobile IP Overview

When a Mobile Node (MN) is away from the home network and attaches to the visited network as shown in the Figure 2.2, the procedure followed by mobile IP consists of Registration and Datagram Delivery.



1. MN discovers Agent **2. MN obtains COA (Care Of Address)**

3. MN registers with HA **4. HA tunnels packets from CN to FA**

5. FA forwards packets from MN to CN

Figure 2.2 Basic principle of Mobile IP [34]

2.4.1 Registration

The major aspects in registration of a MN are:

1. Mobility agents such as a Foreign Agent (FA) and a Home Agent (HA) periodically broadcast an Agent Advertisement message around its network. The message indicates the presence of the mobility agent and the services they are willing to provide for the mobility support. Besides, the routers within a network also broadcast or multicast their Router Advertisements to inform other routers and nodes of their existence.

2. After receiving the message the MN determines whether it is in the home network or in a foreign network. The MN compares its network prefix with the mobility agent's network prefix (obtained from the advertisement message) and detects its location and movement.

3. If the MN is in its home network then the packet sent to the MN or from the MN contains the MN home address. But if the MN just returned to its home

network, then it has to deregister to the HA by sending a Registration update with its lifetime set to 0.

4. If the MN is in the foreign network, the MN needs a care-of address, either a FA care-of address, or a co-located care-of address representing its location. The MN has to register this care-of address with the HA. A FA care-of address is preferred rather than the co-located care-of address in order save the address space.

When the MN is in the foreign network, the procedures that it follows to obtain the FA care-of address are as follows:

1. The MN listens to an Agent advertisement that contains information like FA care-of addresses. The MN can select any one address and the services that are provided by the FA.
2. If the MN doesn't receive any agent advertisements it broadcasts an Agent solicitation message among the foreign network. The FA unicasts an Agent advertisement to the MN after the solicitation message.
3. The MN then registers the care-of address with the HA using a Registration Request message via the FA. The HA then decides whether to accept the request or to decline it.
4. When the request is rejected the HA has to send back an ICMP message including the reason for rejection.
5. The HA sends a Registration Acknowledgement message back to the FA after accepting the request and a binding entry with the lifetime is entered in the HA.
6. The Registration process is completed successfully once the MN receives the Registration Acknowledgement from the FA.

2.4.2 Datagram Delivery

When the registration is complete, the home agent announces to the other routers within the home network about receiving packets on behalf of the MN. This is done using Gratuitous ARP and Proxy ARP (Refer Sec. 2.6).

1. When the CN sends a packet to the MN, the packet is sent to the MN's home network where the HA intercepts the packets, encapsulates it, and tunnels it to the FA. Upon reception the FA decapsulates the packet and delivers the original packet to the MN using its link layer address.
2. When the MN communicates with the CN, packets from the MN bear the MN's home address as its source address and the packets are delivered in the conventional way. The entire procedure is called a Triangle route.
3. If the MN moves to a new FA packets sent to the old FA are entirely lost in the wireless environment.

2.5 Home Agent Discovery

If the mobile node does not know its home agent's address before sending the Registration Request, it has to find a home agent in its home network to register. In this case, the Registration Request will be direct-broadcasted to its home network. One regulation of the registration mechanism is that a home agent accepts Registration Request when the destination address matches the home agent's unicast IP address. Therefore, all home agents deny the direct-broadcasted request. In addition to replying an error message to reject the request, the home agent also pads out the error message with its unicast address. As receiving several rejections, the mobile node will pick up one out of them to be its home agent. Afterwards, the mobile node tries to register again by

sending the Registration Request whose destination address is set to the home agent's unicast address.

2.6 Gratuitous ARP and Proxy ARP

Gratuitous ARP and Proxy ARP (refer Figures 2.3 and 2.4) are messages sent by HAs in the Home Network using which they can intercept packets to the MN's home address when they are away. After accepting a Registration Request from the MN, the HA using these messages informs the other routers that it would be receiving messages on behalf of the MN.

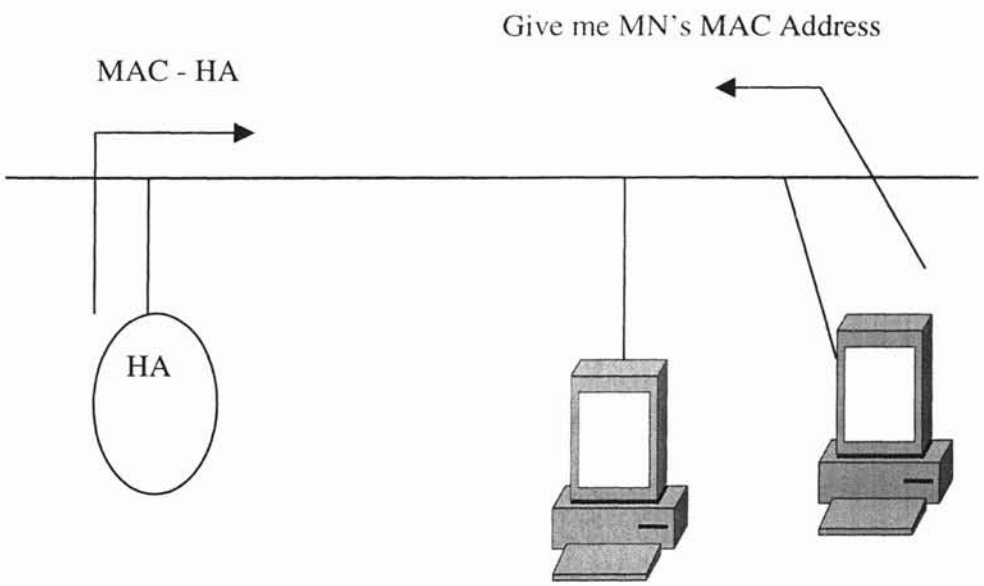


Figure 2.3 Proxy ARP

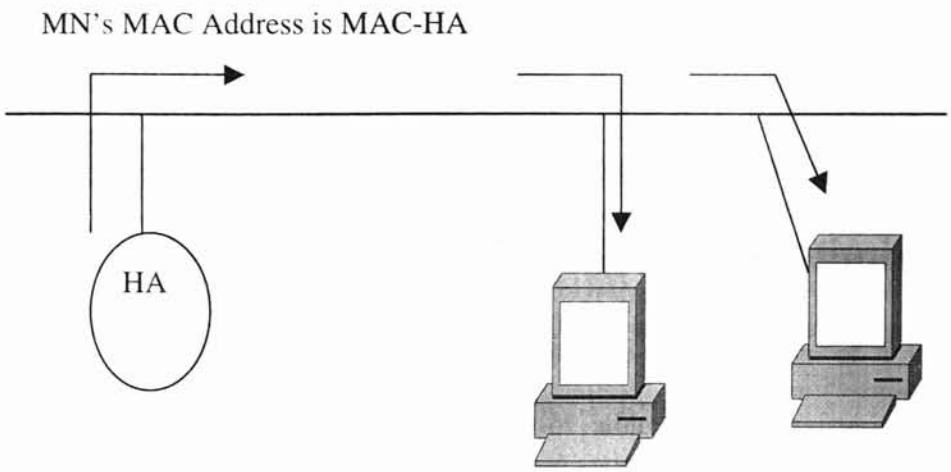


Figure 2.4 Gratuitous ARP

Chapter 3

Mechanisms in Mobile IP and Route Optimization

Mobile IP can be best understood as the co-operation of four separable mechanisms [R1]- (1) Discovering the care-of address, (2) Registering the care-of address, (3) Tunneling to the care-of address and (4) Deregistration all of which are described in the sections below.

3.1 Discovering the Care-of Address

The Mobile IP discovery process is based on an existing standard protocol-Router Advertisement [R2]. The Router Advertisement messages carry the default router information and about one or more care-of addresses. These Router Advertisements are also called as 'Agent Advertisements'. Home Agents and Foreign Agents broadcast the advertisements at regular intervals (every few time units). If a Mobile Node needs a care-of address and doesn't wish to wait for agent advertisements it can send (multicast or broadcast) an 'Agent Solicitation' message that is answered by the appropriate Mobility Agents.

The functions performed by a Mobility Agent advertisement are:

1. Allows for the detection of mobility agents,
2. Lists one or more available care-of addresses,

3. Informs the mobile node about special features provided by foreign agents, for example, alternative encapsulation techniques,
4. Lets the MN determine the network number and status of their link to the Internet and
5. Lets the MN know whether the agent is a home agent, a foreign agent, or both, and therefore whether it is on its home network or a foreign network.

Mobile Nodes use the Agent Solicitation [R2] to detect the changes in the set of mobility agents available at the current point of attachment. When a mobile node doesn't receive/detect any advertisements from a foreign agent that previously had offered a care-of address to the mobile node, then it has to assume that foreign agent is no longer within the range of the mobile nodes network interface. Now the mobile node has to start looking for a new care-of address using the agent advertisement or agent solicitations.

When the mobile node cannot contact its home agent, mobile IP has a mechanism that lets the mobile node try to register with another unknown home agent on it home network. This process known as "Automatic Home Agent Discovery" works by using a broadcast IP address instead of the home agent's IP address in the registration request. When the broadcast packet gets to the home network, other home agents on the network will send a rejection to the mobile node. The rejection notice will contain their address for the MN to use in its subsequent registration messages. Broadcast is not internet wide broadcast, but a directed local broadcast that reaches only IP nodes on the home network.

3.2 Registering the Care-of Address

When a mobile node has a care-of address, its home agent must have the information about the MN's new address. So the mobile node with the help of foreign

agent sends a Registration Request to the home agent with the care-of address information. The home agent, after receiving the message, makes the necessary modifications (updates) in its routing table and sends a Registration Reply to the Mobile Node.

In order to authenticate the entire procedure, Registration Requests contain parameters and flags that characterize the tunnel through which the home agent will deliver packets to the care-of address. The Home Agent that accepts the request maintains a triplet that contains the home address, care-of address and registration lifetime. The triplet is called 'Binding' for the mobile node. A registration request can be considered as a binding update sent by the mobile node. The Binding update sent by the mobile node is a remote redirect request, because it is sent remotely to the home agent, which affects the home agents routing table. The home agent must be certain that the message originated from the mobile node and not from any malicious node otherwise a malicious node could cause the home agent to change its routing table resulting in the mobile node becoming unreachable for future communications.

To secure the registration information each mobile node and home agent must share a security association and use the Message Digest 5 protocol [R3] with 128–bit keys to create unforgeable digital signatures for the registration requests.

3.3 Tunneling to the care-of Address

The default encapsulation mechanism that must be supported by all mobility agents using Mobile IP is IP-within-IP. Using this, the tunnel source (Home agent) inserts a new tunnel header (IP header) in front of the IP header of any datagram addressed to

the mobile node's home address. The new tunnel header uses the mobile node's care-of address as the destination IP address (tunnel destination). The tunnel header uses 4 as the higher-level protocol number, specifying that the next protocol header is again an IP header. The entire original IP header is preserved as the first part of the payload of the tunnel header. To recover the original packet the foreign agent merely has to eliminate the tunnel header and deliver the rest of the packet to the mobile node.

3.4 Deregistration

After the mobile node returns home, it deregisters with its home agent to drop its registered care-of address. In other words, it sets its care-of address back to its home address. The mobile node achieves this by sending a registration request directly to its home agent with the lifetime set to zero. With respect to the foreign agent, MN need not deregister because the service expires automatically when the service time expires.

3.5 Issues in Basic Mobile IP and Route Optimization Extensions

Using the base mobile IP protocol, all datagrams destined to a mobile node are routed through that mobile node's home agent, which then tunnels each datagram to the mobile node's current location. Using these protocol extensions, correspondent nodes (nodes communicating with the MN) may cache the binding of a mobile node and then tunnel their datagrams for the mobile node directly to the care-of address, by passing the mobile node's home agent. Extensions are also provided to allow datagrams in flight

when a mobile node moves, and datagrams are sent based on an out-of-date cached binding, to be forwarded directly to the mobile nodes new binding.

3.6 Binding Caches

Route Optimization [5] provides a means for any node to maintain a binding cache containing the care-of address of one or more mobile nodes. When sending a datagram, if the sender has a binding cache entry then it sends it directly to the mobile node's care-of address. In the absence of a binding cache entry then the packets are routed using the base mobile IP (i.e. the correspondent node sends the data to the home network to which the mobile node belongs). The nodes may maintain a binding cache to optimize its communication with the mobile node. A node creates or updates a binding cache entry for a mobile node when it receives an authenticated message for the mobility binding. When the binding cache time has elapsed the entry is deleted.

3.7 Foreign Agent Smooth Handoff

When a mobile node leaves a foreign agent and registers under a new foreign agent the mobile node doesn't notify the previous foreign agent about its new address in the original base Mobile IP. In route optimization, the previous foreign agent of the mobile node is notified about the mobile node's current mobility binding. This is because any datagrams in flight to the mobile node's previous foreign agent can be forwarded to the new foreign agent. Also, if there are any resources consumed by the mobile node at the previous foreign agent they are released immediately, rather than waiting for its registration lifetime to expire. The two foreign agents must have a security association to

authenticate the notification; otherwise, any other malicious node can change the mobility binding of the mobile node and disrupt the communication.

3.8 Route Optimization Message Formats

Four types of messages are defined for managing binding cache entries. They are as follows.

3.8.1 Binding Warning Message

This message is transmitted when one or more correspondent nodes/foreign agents need Binding update (Location information of the MN). This message is transmitted when the nodes don't have a binding cache or an out-of-date binding cache entry for some mobile node. When any node detunnels a datagram destined for the mobile node and if it is not the current foreign agent for the destination mobile node, then it should send a binding warning message to the mobile node's home agent. If it does not know the mobile node's home agent it should send the message to the sender (i.e. the correspondent node) of the datagram. If a foreign agent receives a packet for a mobile node for which there is not any visitor list or binding cache information available, the foreign agent should send the binding warning to the correspondent node that transmitted the undeliverable message.

When a MN receives a new Care-of Address, it may send a Binding Warning message to its HA, requesting that the HA send Binding Update messages to one or more correspondent nodes. The MN may use this feature when it returns to its home network, so that the HA will send out Binding Updates with zero lifetimes to all the mobile node's

correspondent nodes. It is important for the correspondent nodes to delete their binding cache entries for the mobile node when the mobile node no longer has a Care-of Address.

3.8.2 Binding Request Message

A node uses this message to request a mobile node's current mobility binding from a mobile node or the mobile node's home agent to a foreign agent. When a home agent receives a Binding Request message its home list is checked and determines the correct binding information to be sent to the requesting node. The request is satisfied based on whether or not the mobile node has allowed the information to be disseminated.

3.8.3 Binding Update Message

A node's current mobility binding is notified using this message. This message is sent in response to a binding request message, or in response to a binding warning message, or in response to the reception of a binding warning extension to a registration request, or in response to the reception of a packet destined for a mobile node.

A Binding Update should also be sent by the mobile node, or by the foreign agent with which the mobile node is registering, when notifying the mobile node's previous foreign agent that the mobile node has moved. Each Binding Update message should indicate the maximum lifetime of the binding. When a node receives a Binding Update message, it is required to verify the authentication in the message using the mobility security association it shares with the sender's home agent. All these messages should be authenticated failing which any malicious node can send a binding update and the mobile node would be unreachable.

3.8.4 Binding Acknowledgement Message

This message is to acknowledge the Binding Update message. The node receiving the Binding Update message sends the acknowledgement to the home agent. It is sent just to confirm that CN has received the new address of the MN and has updated it table. After sending this message the MN sends the data packets to the new care-of address.

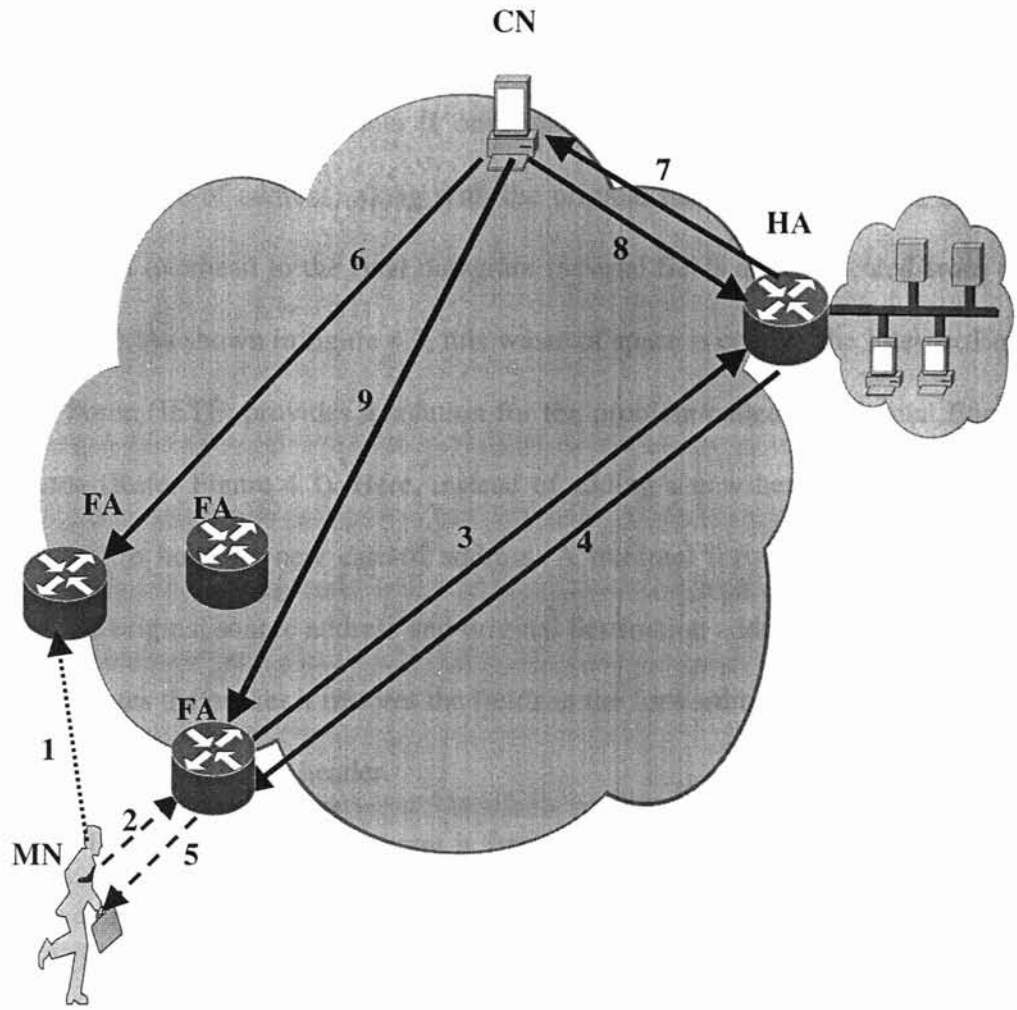
Chapter 4

Problems With Mobile IP

4.1 Triangle Routing

Consider a mobile node that moves to the same sub network as the correspondent node with which it is communicating. The sequence of steps that will take place in the above communication, based on the base Mobile IP protocol, is as follows: the correspondent node will send the datagram all the way to the mobile node's home agent, which may be far away; its home agent will then forward the datagram to its care-of-address, which might just take less than half second to reach if the datagram is sent directly from the correspondent node. This kind of "indirect routing" is inefficient and undesirable.

We can resolve the problem by sending a Binding update message to the CN. So the CN has a binding for the MN's new address (temporary address) and its home address. In the future as the MN changes its location, the HA updates the binding address (Refer Figure 4.1).



1.MN's Previous FA

2.Registration Request (MN – FA)

3.Registration Request (FA – HA)

4.Registration Reply (HA - FA)

5.Registration Reply (FA – MN)

6.CN communicating with Old FA

7.Binding Update (HA – CN)

8.Binding Ack (CN – HA)

9. CN communicating with New FA.

Figure 4.1 Route Optimization Scheme [D1]

4.2 Too Many Unwanted Duplicated Fields in "IP within IP"

According to the base mobile IP, the way to encapsulate the datagram is to put the original datagram inside another IP envelope, of which the whole packet will be outside IP header (care-of address) along with the original datagram. The fields in the outer IP header add overhead to the final datagram (several fields are duplicated from then inner IP header). As shown in figure 4.2, this waste of space is costly. The Internet Engineering Task Force (IETF) provides a solution for the problem called as Minimal Encapsulation scheme (Refer Figure 4.3). Here, instead of adding a new header the original header is modified to hold the new care-of address. A minimal forwarding header is inserted to store the original source address and original destination address. When the foreign agent decapsulates the packet it restores the fields in the forwarding header to the IP header and removes the forwarding header.

But if the original datagram is fragmented, then minimal encapsulation must not be used, as there is no room left to store fragmentation information- this is a restriction.

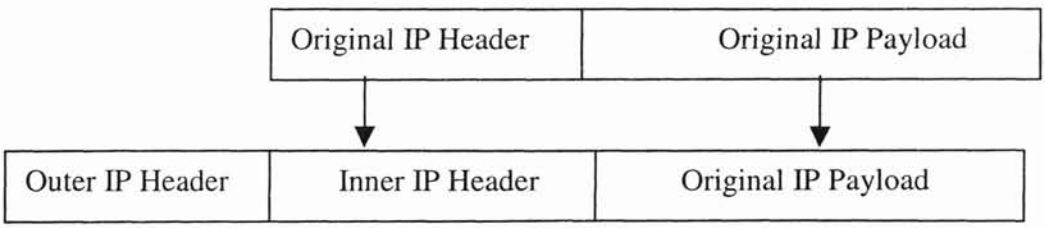


Figure 4.2 IP in IP

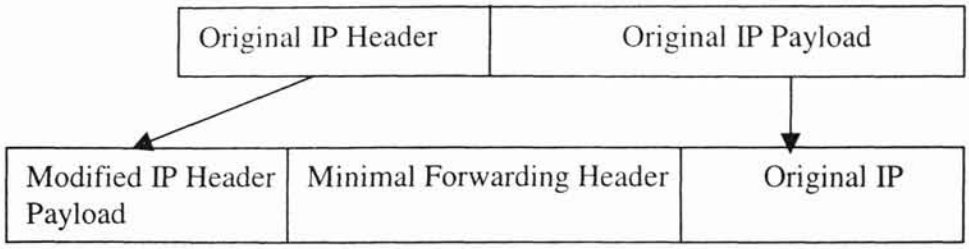


Figure 4.3 Minimal Encapsulation Scheme

4.3 A Fragile Single Home Agent Model

A single home agent model is easy to build and use, although it has the problem of fragility. The mobile node would be unreachable once the home agent breaks down. A possible solution would be to support multiple home agents.

4.4 Unbearable Frequent Reports To The Home Agent

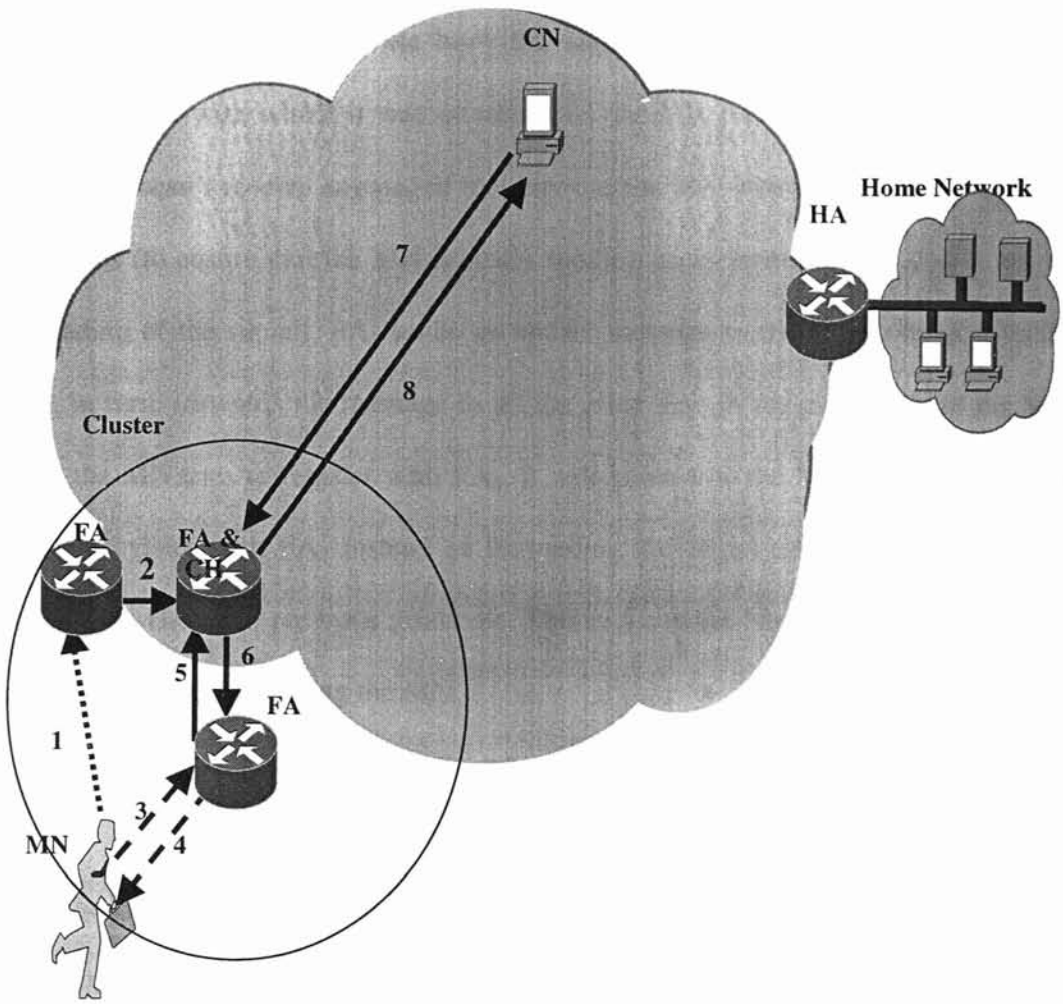
Mobile IP would have to constantly report about its new care-of address if a node is in a moving vehicle and roaming around the neighborhood. This degrades the performance and delays the datagram transmission. One possible solution is to support foreign agent clustering. The idea is **that by making a cluster of foreign agents, moves only from cluster to cluster have to be notified to the home agent**. This approach is expected to reduce the number of times a highly mobile node needs to report to its home agent.

Chapter 5

Proposed Solution

5.1 Clustered Foreign Agents

The FAs are clustered based on their location proximity. So, the movement of the MN from one location to another with in the cluster would be transparent to the HA and the CN. The Cluster Head (CH) takes care of binding the new address with its home address. Therefore the number of updates to be sent to the HA is reduced (Frequency of the control messages is reduced) as well as the datagram transmission time is reduced. Using the Route Optimization method we have a Registration Request from MN to FA, a Registration Request from FA to HA, a Registration Reply from HA to FA, a Registration Request from FA to MN, a Binding Update from HA to CN and a Binding Acknowledgement from CN to HA – total of 6 messages for one movement of a node. In the proposed approach we have an Update Message from FA to CH about the MN's location, a Registration Request from MN to FA, a Registration Request from FA to CH, a Registration Reply from CH to FA, and a Registration Request from FA to MN – total of 5 messages. The diagrams below explain the new technique (Refer Figure 5.1).



1.MN's Previous FA

2.FA1 informing CH about MN moving out

3.Registration Request from MN to FA

4.Registration Reply from new FA to MN

5.Registration Request from FA to CH

6.Registration Reply from CH to FA

7.CN communicating with CH

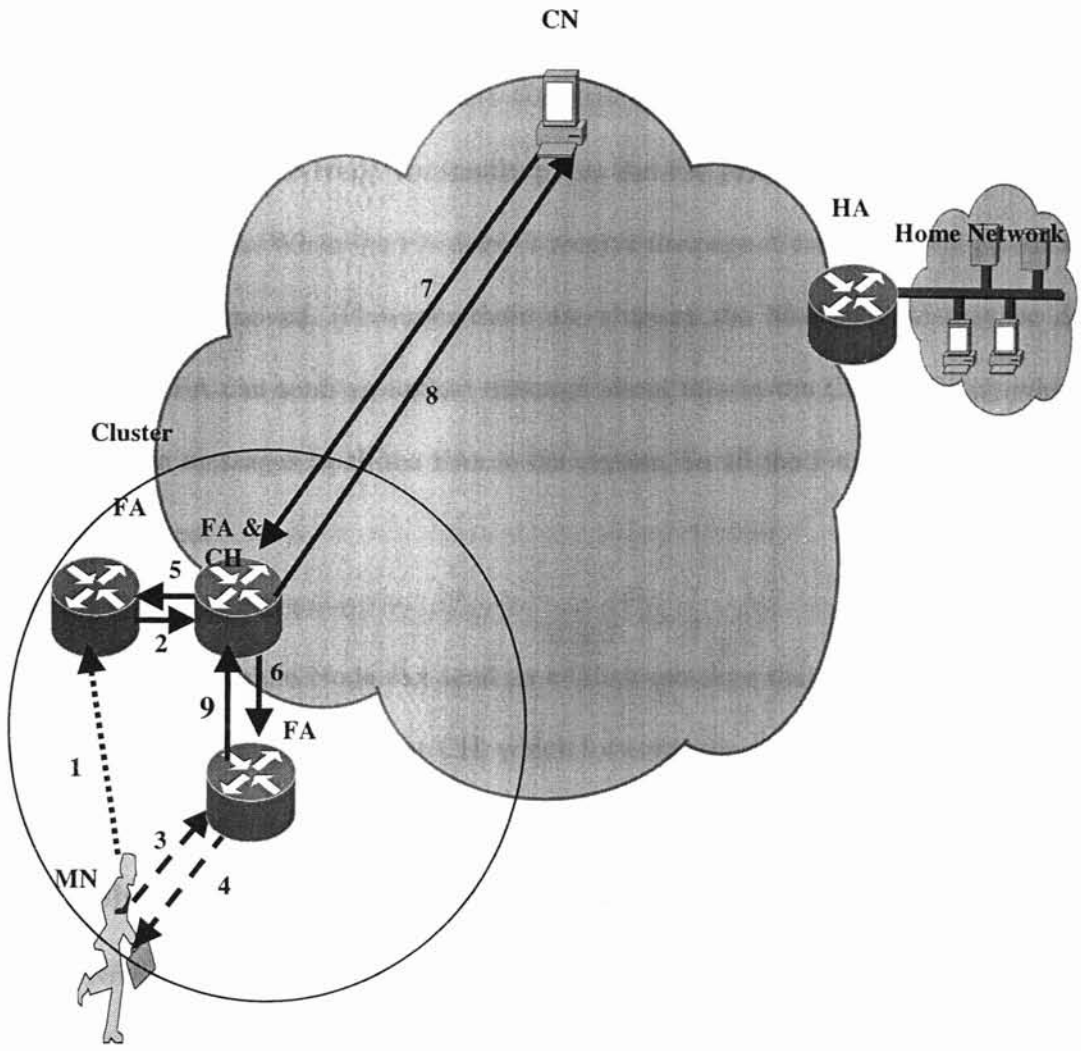
8.MN communicating to CN using FA and CH

Figure 5.1 Mobile IP with Clustering [34]

5.2 Clustered Foreign Agents With Automatic Updates

In this approach we have the same setup of clustered FAs and the MN paging the FA with which it was attached. As the MN moves away from FA_1 towards FA_2, FA_1 doesn't receive any paged messages as the MN moves away from it. After few time units (to ensure that the MN is really moving away from the FA_1 and is not due to any fading of the signal), FA_1 sends an update message to the cluster head. The cluster head, in turn, forwards the message to all the other FAs in the cluster about the MN. So when the MN tries to register with FA_2, it will know that the MN is legitimate and can directly register with FA_2 instead of forwarding the registration request to the cluster head or the HA as in previous protocols. This reduces the latency involved and FA_2 can immediately begin servicing the MN.

Since all the mobility agents are clustered the HA would also be in a cluster (because the HA can be a FA to some other MN). Initially when the MN moves away from the HA it sends an update to its cluster head that its node is moving away which gets propagated to all the other agents in the cluster. This not only reduces the number of control messages but also saves a lot of time (Refer Figure 5.2).



1.MN's Previous FA

2.FA informing CH about MN moving out

3.Registration Request from MN to FA

4.Registration Reply from new FA to CH

5.Update from CH to FA

6.Update from CH to FA

7.CN communicating with CH

8.MN communicating to CN using FA and CH

9.FA updating the location of MN to CH.

Figure 5.2 Mobile IP with Clustering and Automatic Update [34]

5.3 Cluster Head Detection Of Mobile Node's Departure

Implicit:

The Mobile Node constantly pages the FA [17] about its link with the FA every few time units. When the FA doesn't receive the page it can implicitly presume the mobile node has moved. (However there are chances the Mobile node may be down instead). The FA can send an update message about this to the Cluster Head, which in turn sends the messages to all the FAs in the cluster. So all the FAs know that a Mobile Node has moved.

Explicit:

The Mobile Node can send an explicit message that it is leaving, to the FA. The message can be updated to the CH, which forwards the update to all the FAs.

5.4 Algorithms for Cluster Formation

Nodes are clustered to enhance network manageability, channel efficiency, and energy economy. Clustering can be defined as grouping of nodes into manageable set. A Cluster consists of groups of nodes with one of them elected as CH. A Cluster is identified by its unique CH ID. Clusters can be overlapping or disjoint. All the nodes in the cluster know its corresponding CH and thereby the cluster to which it belongs. There are several clustering algorithms [35] to group ad hoc networks.

5.4.1 Highest Degree Heuristic [35]

In this approach we compute the degree of a node based on the distance between that node from others. A node X is considered to be a neighbor of another Node Y if X lies within the transmission range of Y. The node with the maximum degree is chosen to be a cluster head and any tie is broken by the lowest node id, which is unique. The neighbors of a cluster head become members of that cluster and can no longer participate in the election process. This heuristic is also known as the highest-connectivity algorithm.

5.4.2 Lowest-ID Heuristic [35]

Another simple heuristic is that by assigning a unique id to each node and choosing the node with the minimum id as a cluster head. However, the cluster head can delegate its duties to the next node with the minimum id in its cluster. A node is called 'gateway' if it lies within the transmission range of two or more clusters.

5.4.3 Node Weight Heuristic [35]

Node-weights are assigned based on the suitability of a node being a cluster head. A node is chosen to be a cluster head if its node-weight is higher than any of its neighbor's node-weights. The smaller node id is chosen to break a tie.

We can use the same algorithms with some modifications to support clustering of static nodes.

5.4.4 Combined Higher Connectivity Lower ID clustering Algorithm [35]

1. One of the nodes initiates the clustering algorithm process by flooding requests for clustering to all other nodes.
2. All nodes are aware of their k-hop neighbors (that is, neighbors at a distance of at most k-hops).
3. Node whose ID is lowest among all their k-hop neighbors (local lowest ID nodes) broadcast their decision to create clusters (with them as CHs) to all their k-hop neighbors.
4. Other nodes retransmit the decision (and similarly the decision of other nodes later on) until all nodes at distances up to k hops are reached.
5. If all k-hop neighbors that have lower ID broadcasted their decisions and none declared themselves as a CH, the node decides to create its own CH and broadcasts its ID as cluster ID. Otherwise it chooses a k-hop neighboring CH with lowest ID and broadcasts such decision.
6. Thus each node broadcasts its clustering decisions after all its k-hop neighbors with lower IDs have already so.
7. Every node can determine its cluster and only one cluster, and initiates the broadcast for only one message during the algorithm.
8. Here the node degree is used as the primary key and ID as the secondary key in cluster decisions.
9. Whenever the connectivities are same, we compare ID to make decisions.
10. A node has cluster head priority over the other if it has higher connectivity, or in case of equal connectivity, if it has lower ID.

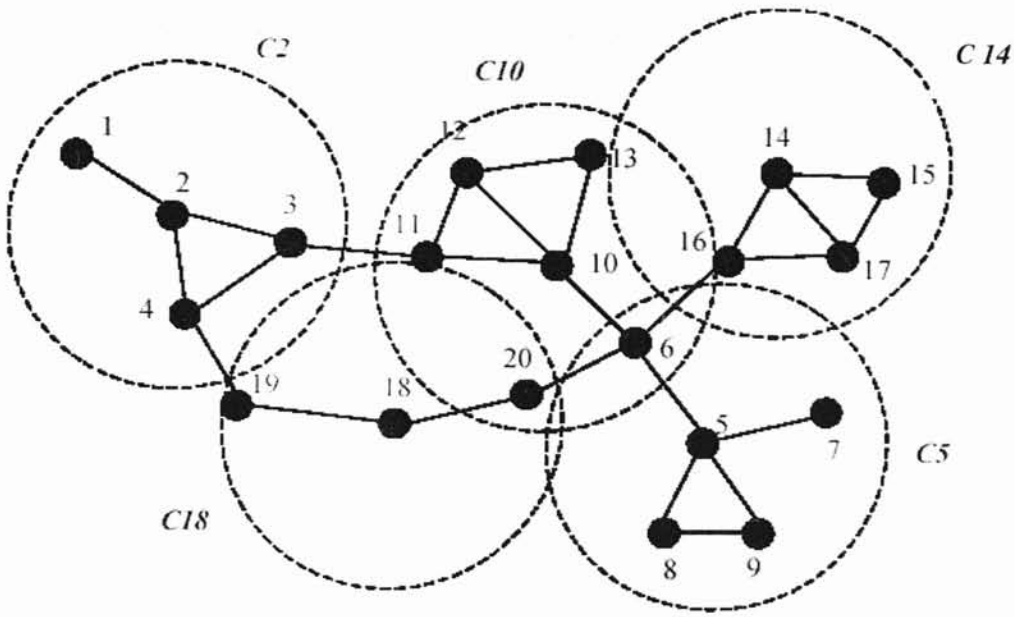


Figure 5.3 Combined Higher Connectivity Lower ID Clustering

When a node switches on, it checks whether it is at distance up to *k* hops from any of existing cluster heads, and, if so, joins these clusters. Otherwise, the node creates a new cluster with itself as cluster head, and invites its k-hop neighbors to join the cluster (Refer Figure 5.3).

When a node switches off, no change is made if the node was not a CH. In case of CH failure, nodes in the cluster elect a new CH using the number of *k*-hop neighbors within the cluster as the main criterion (overall number of *k*-hop neighbors as secondary, and ID as ternary criterion). Nodes that are not included in the new cluster repeat this procedure until all of them are included in a cluster. This procedure may result in splitting a cluster into two or more new clusters.

5.5 Reduction in Vulnerability Time

When the MN leaves one FA and tries to register with another FA there is some time lapse. During this time lapse there is high possibility of datagrams being lost. This time period is called as Vulnerable Time.

5.5.1 Handoff in Basic Mobile IP [24]

When a MN moves from one FA to another, it has to create a new link with the new FA, and register it to the HA. This procedure is known as Handoff (Refer Figure 5.4).

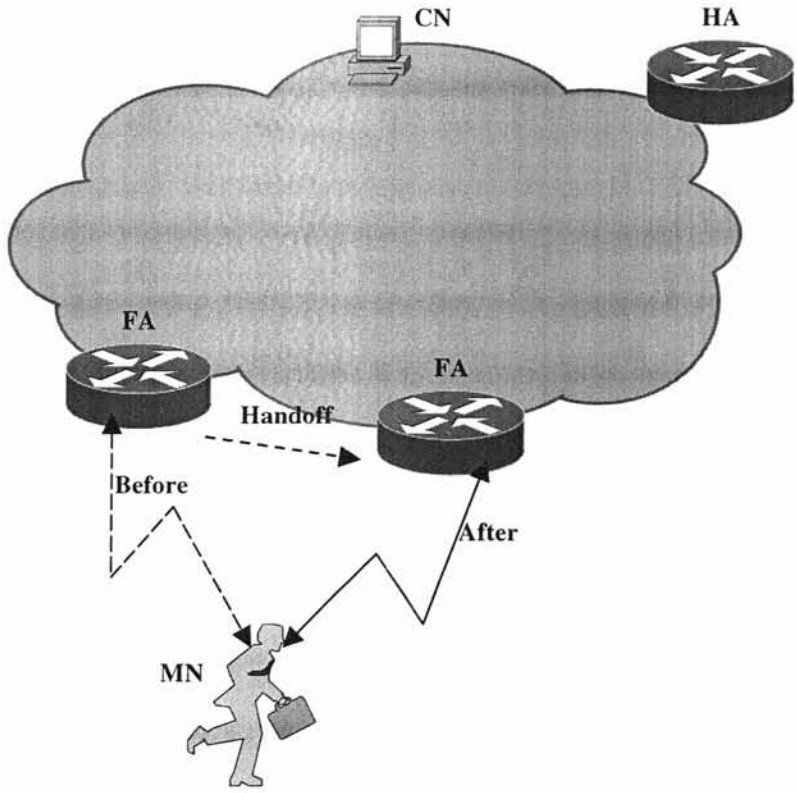


Figure 5.4 Mobile Handoff Scenario [34]

During Handoff there is a vulnerable period in which datagrams in transit to the MN can be lost. The timing diagram that is given below clearly illustrates this scenario. The system is vulnerable as soon as the MN leaves the previous FA, since the new FA doesn't have a validated binding yet. T_{VUL} is the vulnerable time, in which datagrams in transit to the MN are potentially lost and is evaluated as,

$$T_{VUL} = D_{HF1} + D_{F2H},$$

where D_{HF1} is the delay for datagrams sent prior to the handoff to reach the old FA (FA1) via the HA and D_{F2H} is the delay for the new registration request to reach the HA via the new FA (FA2) (Refer Figure 5.5).

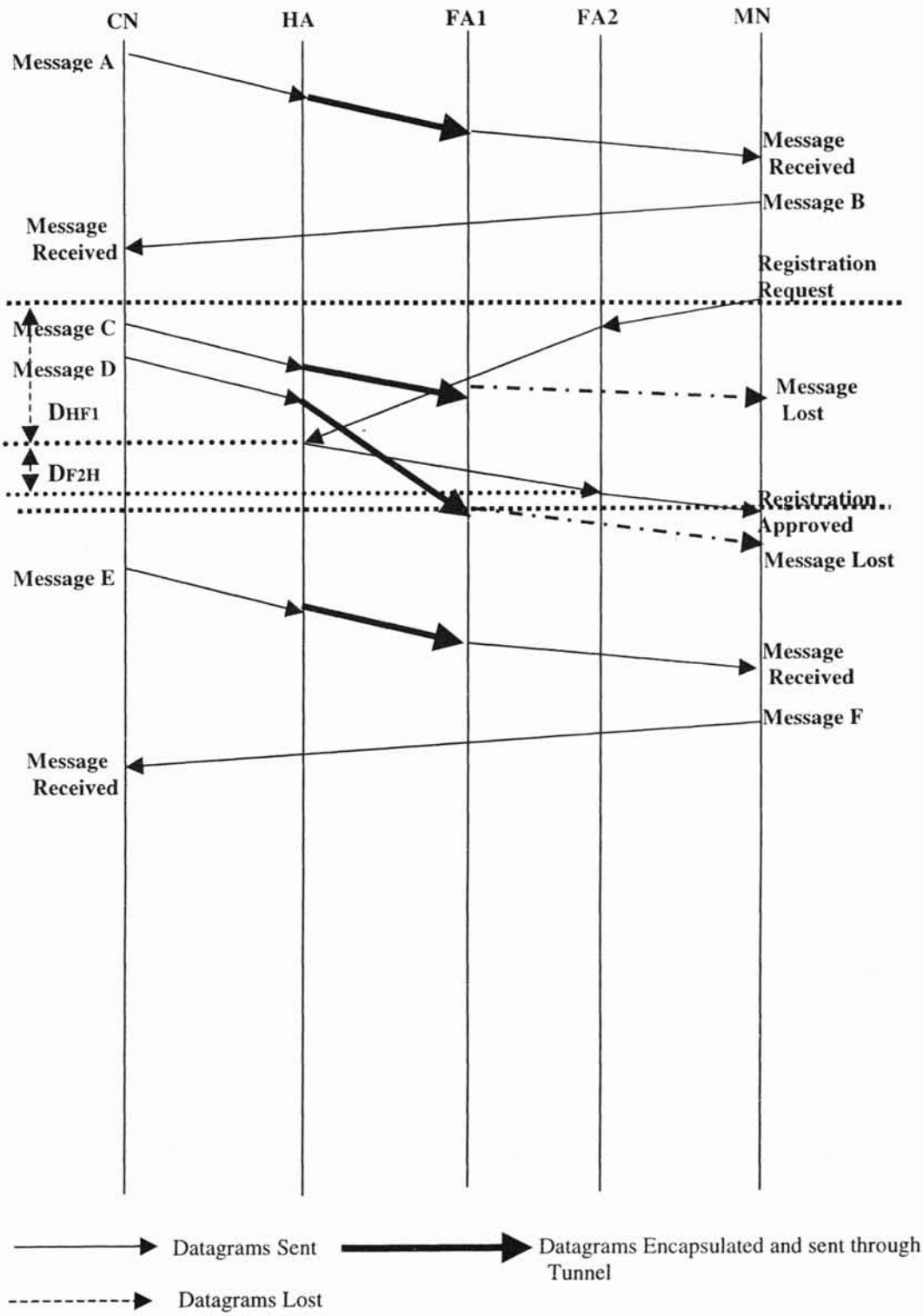


Figure 5.5 Timing Diagram During Hand off in Basic Mobile IP [24]

From Figure 5.5 it is evident that datagrams forwarded by HA to MN within the T_{VUL} will be incorrectly routed. After the registration is authenticated at the HA a new tunnel can be established from the HA to the MN and packets can be redirected to the MN via the FA2.

5.5.2 Route Optimization Method

Using the route optimization scheme, the network traffic is reduced due to elimination of triangular routing. But during handoffs it is necessary to exchange extra control messages to update the mobility binding in the CN, in addition to the registration messages required in the basic mobile IP. These additional control messages during handoffs could result in a longer vulnerable period. Tvul is evaluated as

$$T_{VUL} = D_{CF1} + D_{F2H} + \min (D_{HF2} + D_{F21}, 3D_{HC}),$$

where D_{CF1} is the delay for datagrams sent prior to the handoff to reach the old FA (FA1) via the HA, D_{F2H} is the delay to register the new binding with the HA after handoff, D_{HF2} is the delay for the HA to reply with a registration confirmation, D_{F21} is the delay for the FA_2 to give the FA_1 the new binding. $3D_{HC}$ is the delay for the HA to update the binding cached at the CN (Refer Figure 5.6). Depending on the current congestion over the internet, the vulnerability time with route optimized scheme can easily exceed the vulnerability time without route optimized scheme. TCP performance will suffer under high rate of hand offs or if the delays are long.

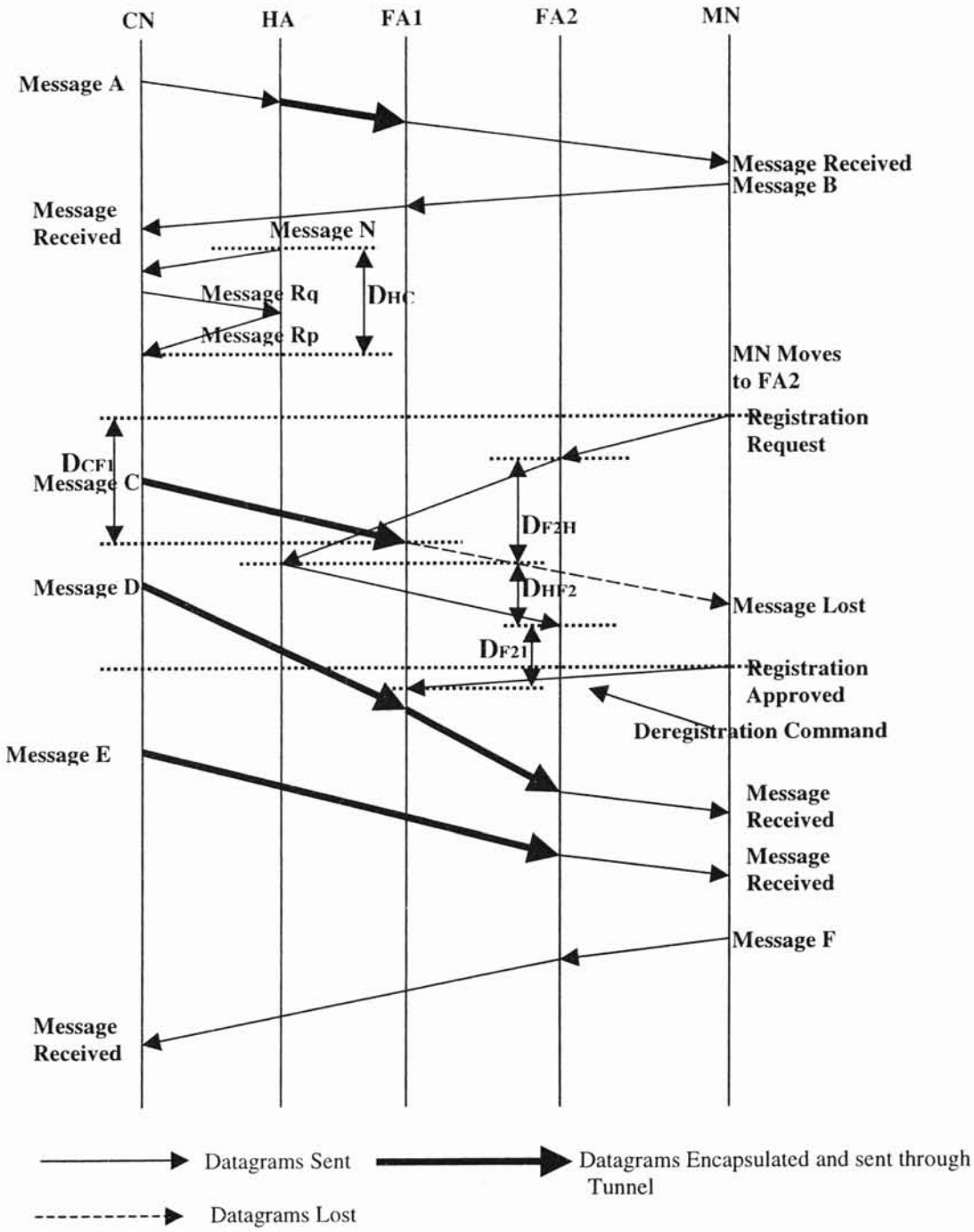


Figure 5.6 Timing Diagram During Hand off in Route Optimization Scheme [24]

5.5.3 Clustering Method

In the proposed approach the movement of MN within the Cluster is transparent to the HA and the CN. So the handoffs are fast when compared to the previous two methods. The MN's new location has to be informed to the CH in the cluster and not to the HA in this approach. When the MN is in the cluster all messages that have to be authenticated by the HA is done by the CH. So the registration messages are authenticated locally at the CH. This reduces the vulnerability time. Also compared to the route optimized scheme the extra control messages are not needed. The CN keeps sending the datagrams to the CH and it is forwarded to the new FA with which the MN is associated. The vulnerability time T_{VUL} is evaluated as

$$T_{VUL} = D_{HFC} + D_{RF2},$$

where D_{HFC} is the delay to update the cluster head about the mobile node that is moving out (delay to hint the CH about the MN). D_{RF2} is the delay for the MN to register with a new FA (FA2). Compared to the delay in route optimized scheme, here the delay is to get the registration reply from the new FA with which mobile node is associated with (Refer Figure 5.7).

In this method once the old FA sends message (to the CH) about the MN moving out, the CH can buffer datagrams that arrive before the MN registering with any new FA. Once it has done so, all the packets can be forwarded to it. But it has an additional cost of extra memory that has to be dealt with. Also after some predefined time units the CH has to flush the buffer else it would occupy the memory forever if the MN has moved out of the cluster.

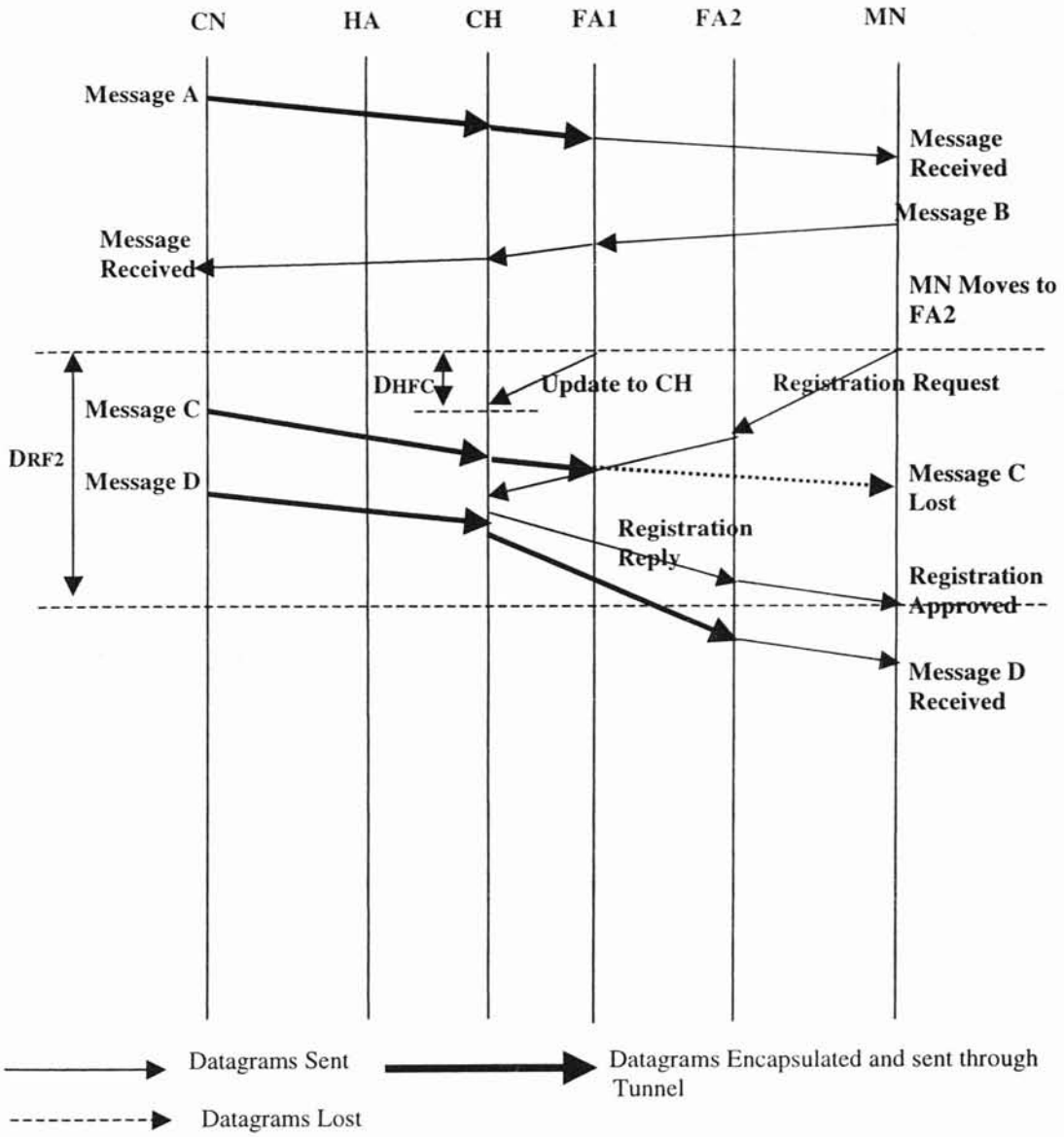


Figure 5.7 Timing Diagram During Hand off Using Clustered FAs

5.5.4 Clustering Method with Automatic Update

Here the information about the MN's location is propagated to all the FAs in the cluster otherwise it is very much like the previous approach. Once the MN leaves the old

FA, the FA doesn't receive any paged messages from MN regarding its association with it. This hint is forwarded to the CH as that the MN has left the old FA. The CH in turn broadcasts these messages to all the FAs in the cluster about the MN. So as soon as the MN tries to register with a new FA in the cluster, the new FA would have known from the broadcast message about this particular MN and immediately services the request of the MN. Also the FA sends an update message to the CH that the MN is associated with it. The vulnerability time here is less compared to the previous methods and the possibility of data loss is reduced significantly. The vulnerability time T_{VUL} is evaluated as

$$T_{VUL} = D_{HFC} + D_{CFS},$$

where D_{HFC} is the delay to update the cluster head about the new mobile node. D_{CFS} is the delay to send update messages to all the FAs in the Cluster (Refer Figure 5.8). Observe that the CH can buffer the datagrams to a particular MN in the cluster when it has not yet registered with a new FA and forward it once the MN has registered with a FA.

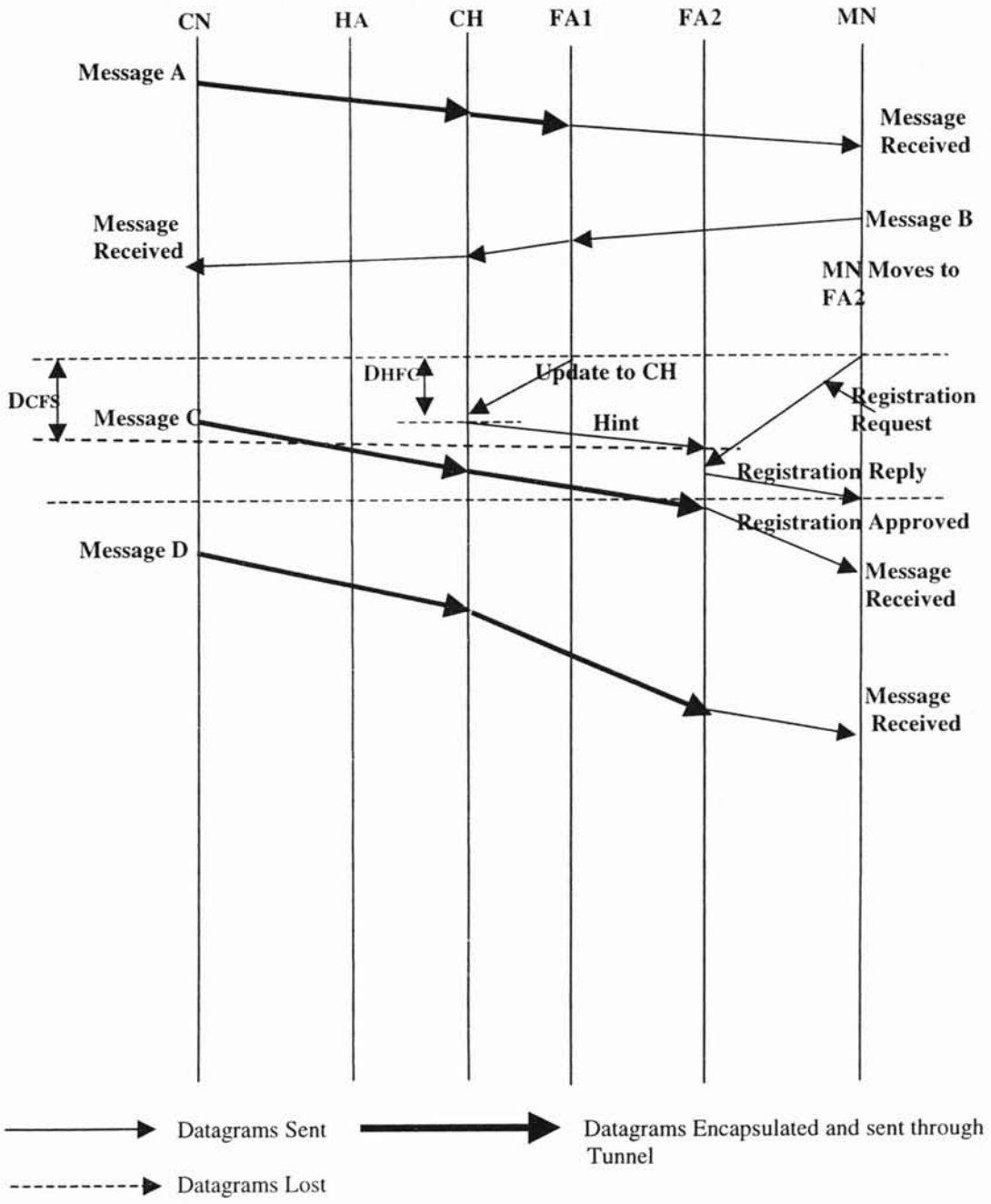


Figure 5.8 Timing Diagram During Hand off Using Clustered FAs and Automatic Update

5.6 Cost incurred in this approach

The CH has to send the update messages to all the FAs in the cluster. This consumes some bandwidth. The CH in the cluster is also a FA that additional workload maybe incurred to CH.

The CH should also allocate some space to remember the mobility bindings. But as the technology is improving, constraints related to memory can be dealt with easily and it is not a great factor to worry about.

5.7 High traffic in the Cluster Head's Network

If the CH doesn't send update messages to all the FAs due to high traffic in its network or if the message is lost somehow, the FA that gets the Registration request from the MN in turn queries the CH about the MN and the Registration proceeds with the automatic update. That is the FA forwards the Registration Request to the CH and the CH registers its new care-of address and redirects the datagrams to the new address.

5.8 Possible Enhancements To Mobile IP

Translation Fix at the Routers

In order to solve the 'Triangle Routing Problem' (Refer Sec 4.1) and the potential bottleneck at HA (since it has to tunnel packets) in the case of heavy network traffic, we can enable the routers in the Internet to cache the Mobility Binding and route packets accordingly. The packets addressed to the MN can be detected when they are being routed as packets that need tunneling to a new address and can be routed as such.

Chapter 6

Simulation and Results

To investigate the performance of the foretold approach we have created classes (using C++) for the various entities like HA, FA, MN, Cluster, and CH. MN's movement in real time is random. In order to simulate this we have a random number generator, and the decision to move out of a FA or back to the home network, by the MN is made on some probability. Also each MN has a pre defined count in it. Each time when the MN gets a chance to move out and if the probability is not satisfied, the predefined count is decremented. The MN moves out of the FA on one of the condition, if the probability is satisfied or if the count becomes 0.

6.1 Route Optimization Scheme

When the MN moves out, the following messages are transmitted in a sequence.

- MN's Registration Request to the next FA.
- FA retransmits the Registration Request to the HA.
- HA accepts/rejects the Registration Request and Replies.
- FA retransmits the Reply.
- Previous FA sends a Binding Warning to the HA.
- HA sends a Binding Update to the CN.
- CN acknowledges the Binding Update.

All the entities keep a count on the number of messages sent and the time taken for the Registration and Binding.

6.2 Clustered FAs Scheme

When the MN moves out from one FA to another within the Cluster, the following messages are transmitted in a sequence.

- Old FA sends a message to the CH about the location of MN.
- MN's Registration Request to the next FA.
- FA retransmits the Registration Request to the CH.
- CH accepts/rejects the Registration Request and Replies.
- FA retransmits the Reply.

Again all the entities keep a count on the number of messages sent and the time taken for the Registration and Binding.

6.3 Clustered FAs With Automatic Update Scheme

When the MN moves out from one FA to another within the Cluster, the following messages are transmitted in a sequence.

- Old FA sends a message to the CH about the location of MN.
- CH locally Broadcasts this message to all FAs.
- MN's Registration Request to the next FA.
- FA accepts/rejects the Registration Request and Replies.
- FA updates CH about the MN new location.

Again all the entities keep a count on the number of messages sent and the time taken for the Registration and Binding.

In the simulation the number of the MNs is varied and results are shown in figures 6.1, 6.2, 6.3.

6.4 Charts

The total number of control messages sent by the MNs is measured by varying the number of MNs. From figure 6.1 we can clearly see that the proposed schemes are more efficient compared to route optimized scheme in the number of control messages transmitted.

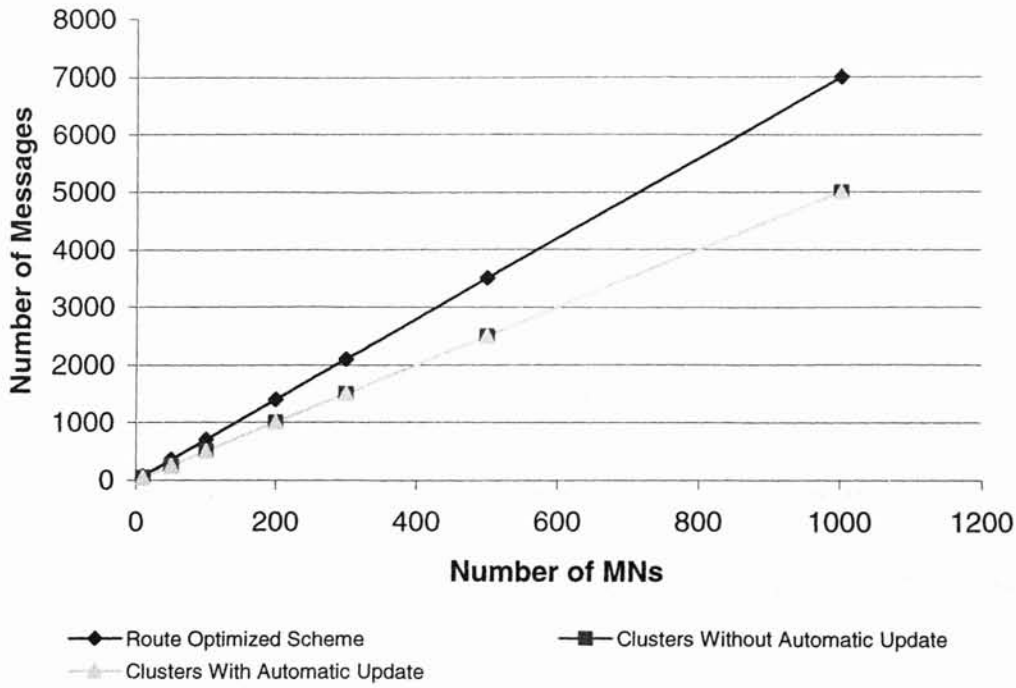


Figure 6.1 Number of MNs Vs Number of Messages (1 Handoff Per Node)

We can see from the figures 6.1, 6.2, 6.3 that the proposed approach performs better than the route optimized scheme. Using the new proposed methods network traffic is reduced. Apart from the reduction in number of control messages the bottleneck at the HA is also relieved. The bottleneck at the HA is distributed among the CHs and so processing the control messages is distributed.

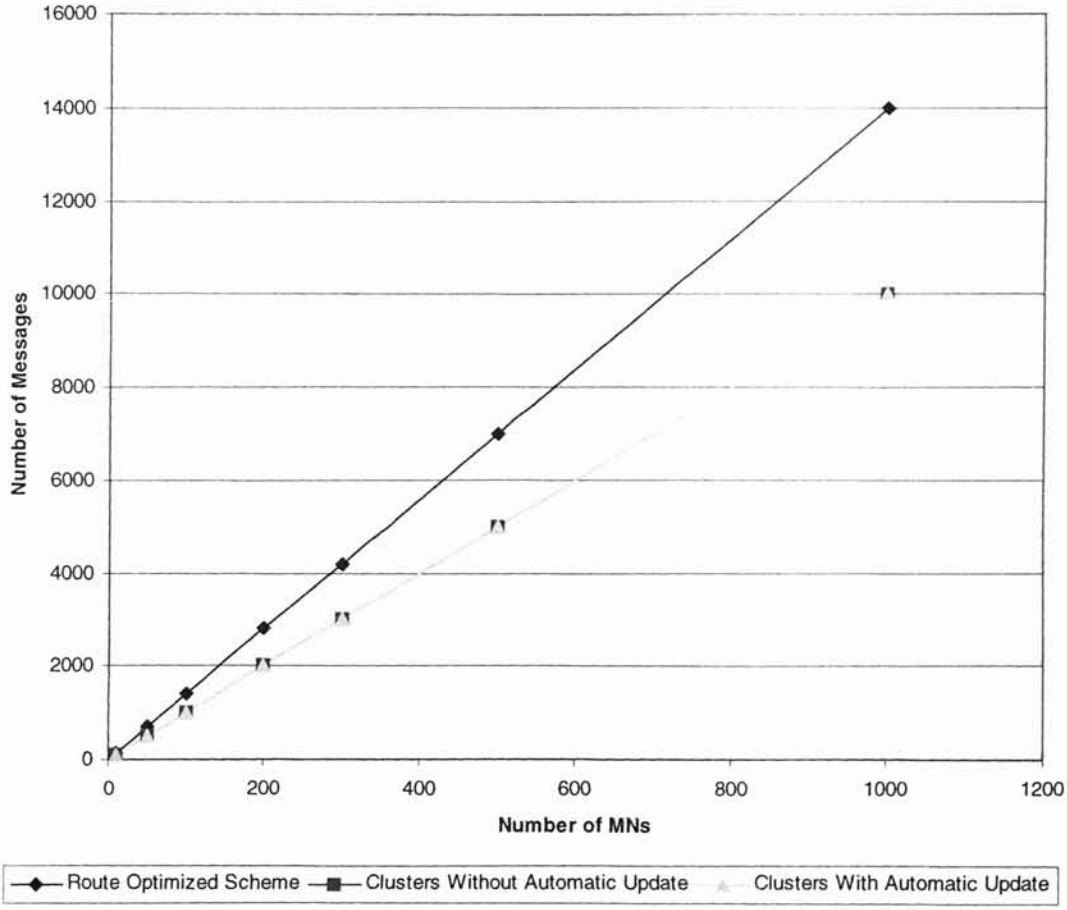


Figure 6.2 Number of MNs Vs Number of Messages (2-Handoffs Per Node)

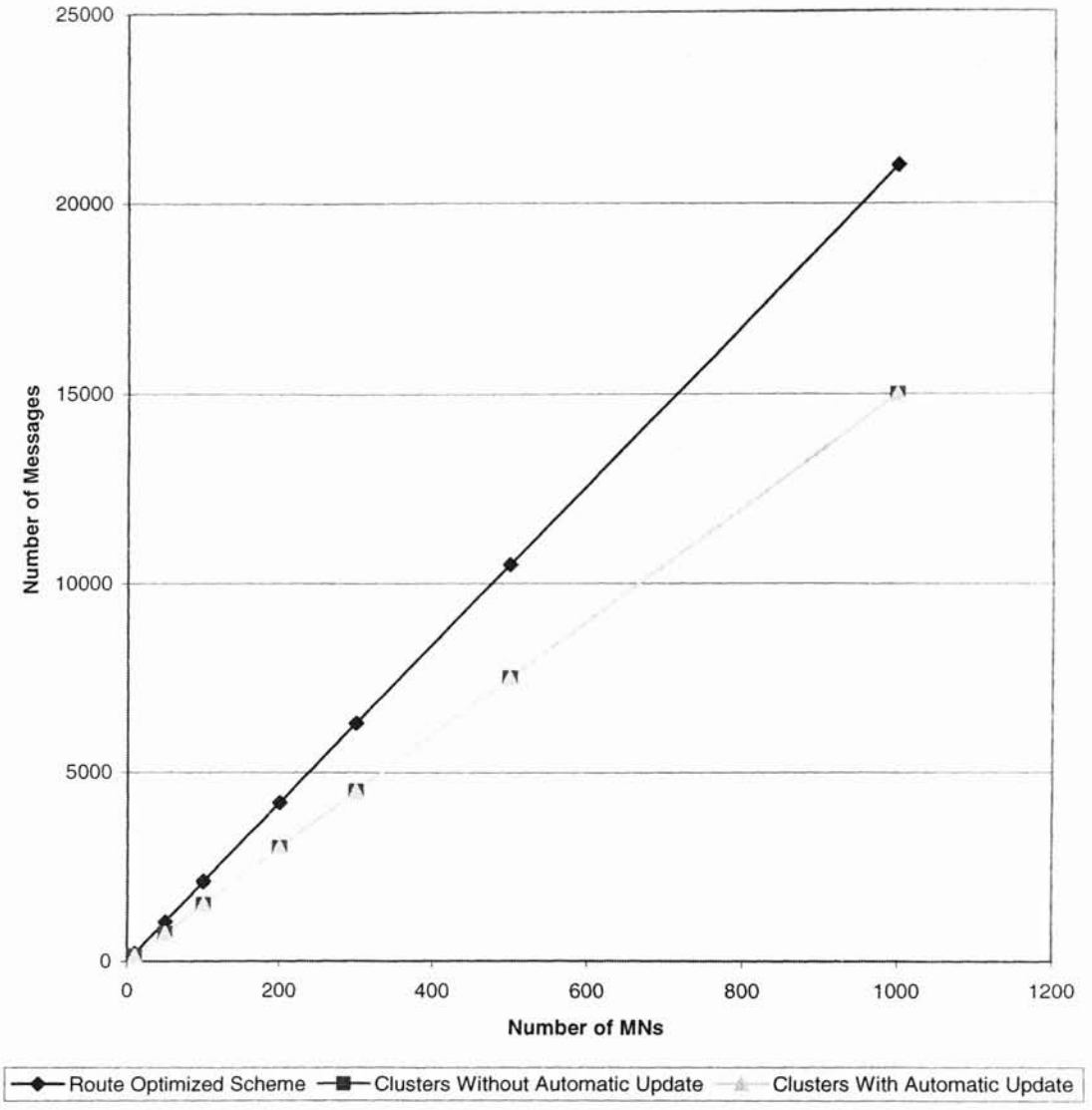


Figure 6.3 Number of MNs Vs. Number of Messages (3 Handoffs Per Node)

From the figures we can see that as the number of handoffs increase the number of control messages that are sent out also increase proportionately in the route optimized scheme. Proposed approaches perform better in these cases. Also we can see that the amount of processing that the HA has to perform is distributed to all the CHs.

The time taken for the MN to Register with the HA is measured. A graph is also plotted for Number of Handoffs vs. Total Logical Time Units to register with the HA/CH. We can see the performance difference between proposed approaches and the route optimized scheme is better (Refer Figure 6.4). This is because the MN registers with the CH locally, instead of the HA as in the route optimized scheme.

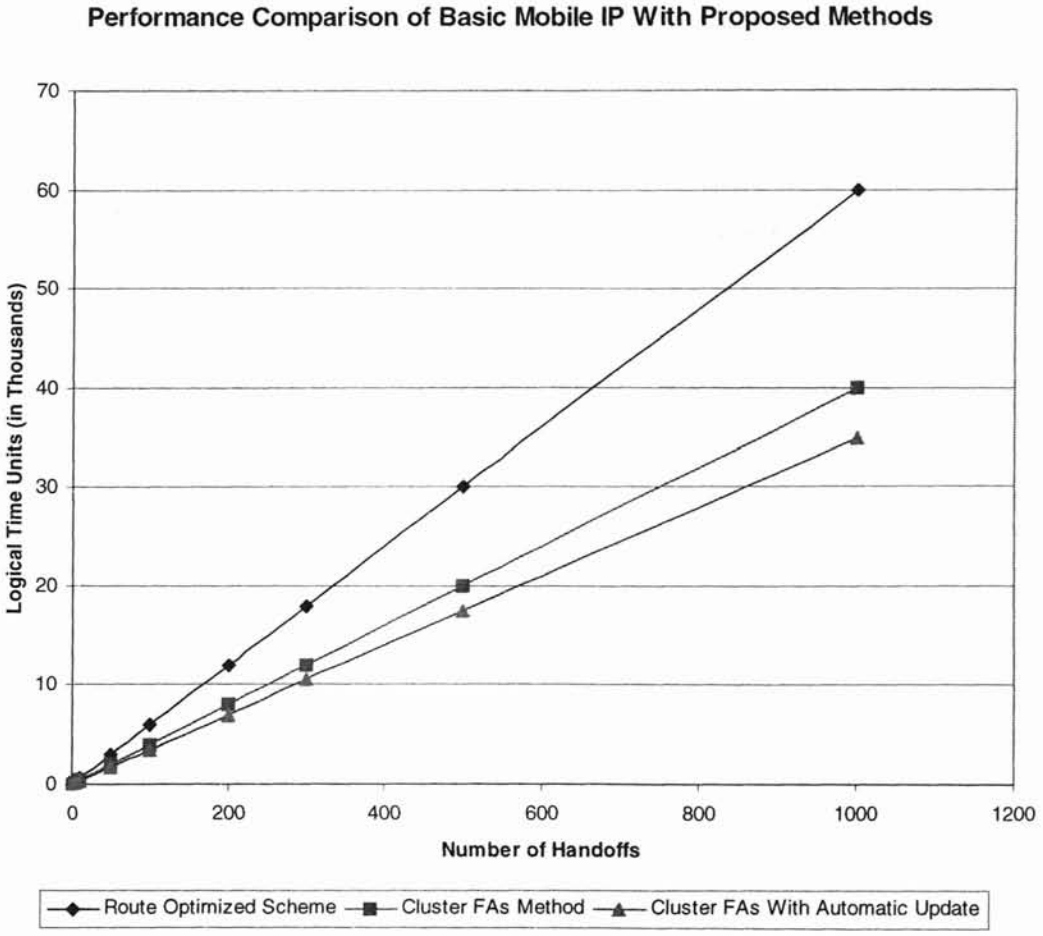


Figure 6.4 Number of Handoffs Vs. Total Logical Time Units

The time taken by the MN to register is also plotted for numerous handoffs. Both inter cluster and intra cluster hand offs are considered. Apart from the registration time the route optimization scheme has binding time involved which is not shown here. In the proposed approaches for intra cluster movements there are no binding times involved and if there is a inter cluster movement the binding time would be same as the route optimized scheme (Refer Figure 6.5). For inter cluster movements the MN has to register with the HA, which causes the increase in time for registration.

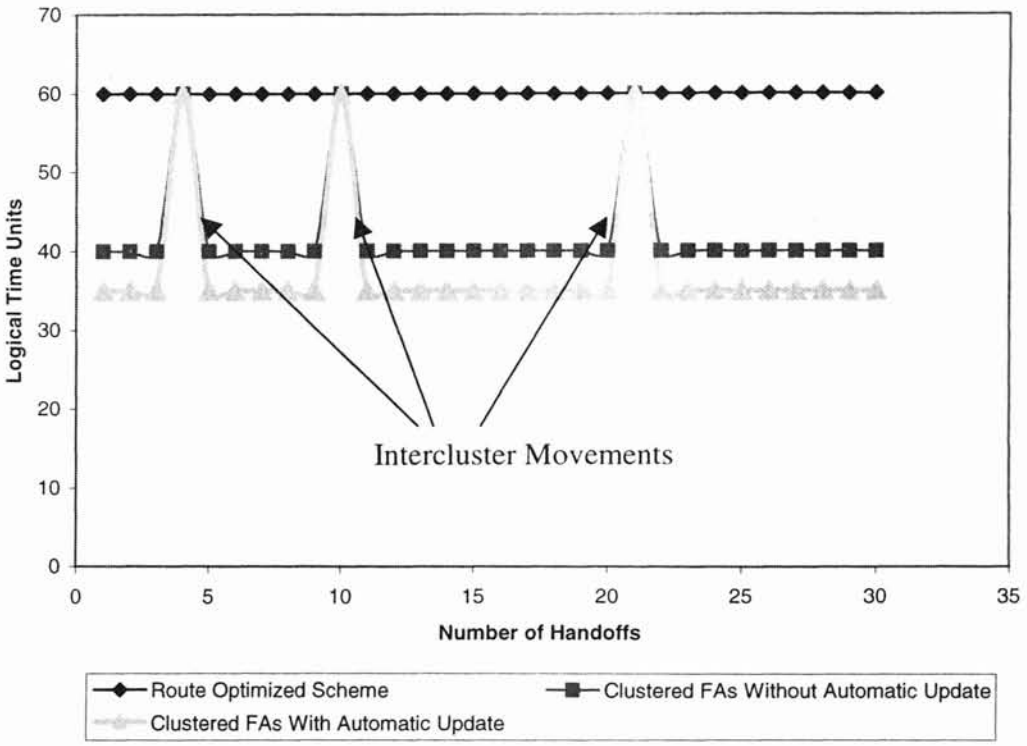


Figure 6.5 Registration Time Vs. Number of Handoffs

6.5 Results

Using the simulation the following observations were made.

1. The number of messages sent to the home agent is reduced.
2. The number of messages between the home agent and the correspondent node is reduced.
3. The time taken for the propagation of information about MN's location is reduced.
4. The Vulnerability time/Latency time is reduced.
5. The bottleneck problem at the HA is resolved, as the MN registrations are distributed to the CHs.

Also from figure 6.5 we can see that if there is intra cluster movement the time taken to register the care-of address is less compared to the inter cluster movement. Last but not least the automatic update overhead might impact performance at the cluster head when the number of MNs inside the cluster increases.

Chapter 7

Conclusions

7.1 Conclusions

Mobile IP with its extensions supports host mobility. When the MN is highly mobile, the handoff rates are high and it degrades the performance. We have proposed techniques that deliver optimal performance at all handoff rates. The simulation results show us the same. The approach is just to cluster the FAs and handoffs within the cluster is transparent to the HA and CN. This scheme minimizes the loss of datagrams, and also enhances the performance under high handoff rates, minimizes registration delays.

7.2 Future Work

1. Routers can be enabled to cache the Mobility Bindings and route packets accordingly.
2. Optimal Cluster Size can be determined.
3. The above approach can be implemented in Network Simulator and the results can be studied.

References

[1] Festag, A., "*Mobility Support in IP-Based Networks: A Multicast-based Approach*", Telecommunication Networks Group, Technical University Berlin. <www-tkn.ee.tu-berlin.de/publications/ papers/festag_mobility.pdf>

[2] Hac, A. and Huang, Y., "*Location Update and Routing Scheme for a Mobile Computing Environment*", International Journal of Network Management Volume 10, 2000, pp. 191 – 214.

[3] Campbell, A.T. and Gomez, J., "*IP Micro-Mobility Protocols*", ACM SIGMOBILE Mobile Computer and Communication Review (MC2R) Volume 4, October 2001, pp. 45-53.

[4] Perkins, C., "*Mobile IP Design Principles and Practices* ", 1998, Addison-Wesley Wireless Communications Series.

[5] Perkins, C. and Johnson, D., *"Route Optimization in Mobile IP*" IETF Mobile IP Working Group Internet Draft February 2002. <http://www.phptr.com/solomon/html/drafts/draft-ietf-mobileip-optim.txt>

[6] Perkins, C.E. and Wang, K.Y., " *Optimized Smooth Handoffs in Mobile IP*", IEEE International Symposium on Computers and Communications, 1999, pp. 340 -346.

[7] Tan, C.L., Lye, K.M. and Pink.S., "*A Fast Handoff Scheme for Wireless Networks*", Proceedings of the Second ACM international workshop on Wireless Mobile Multimedia August 1999, pp. 83-90.

[8] Milojicic, D., Douglis, F. and Wheeler, R., "*Mobility Processes, Computers and Agents*", 2nd Printing February 2000. (Chapter 10-Mobile IP).

[9] Ghosh, D., "*Mobile IP*", ACM Crossroads Student Magazine <http://www.acm.org/crossroads/xrds7-2/mobileip.html>

[10] Soliman, H., Castelluccia, C., El-Malki, K. and Bellier, L., *"Hierarchical MIPv6 Mobility Management*" IETF Mobile IP Working Group Internet-Draft <http://www.ietf.org/internet-drafts/draft-ietf-mobileip-hmipv6-06.txt>

[11] Kim, H.Y. and Hwang, C.S., "*An Efficient Connection Scheme for Mobile IP*", Ninth IEEE International Conference on Networks, 2001, pp. 396-400.

[12] Lai, J. and Liao, W., "*Mobile Multicast with Routing Optimization for Recipient Mobility*", IEEE Transactions on Consumer Electronics, Volume 47, February 2001, pp. 199-206.

[13] Lin, J.P., Kuo, S.Y. and Huang, Y., "*A Cluster Based Checkpointing Scheme for Mobile Computing On Wide Area Network*", Discrete Mathematics and Theoretical Computer Science Workshop Mobile Networks and Computing March 25-27,1999, pp. 177-194.

[14] Chakraborty, K., Misra, A., Das, S., McAuley, A., Dutta, A. and Das, S.K "*Implementation and Performance Evaluation of TeleMIP* ", IEEE International Conference on Communications, Volume 8, 2001, pp. 2488 - 2493.

[15] Khalil, M. and Pillai, K., "*Architecture For IP Mobility*", Emerging Technologies Symposium on Broadband, Wireless Internet Access, IEEE, 2000, pp. 5-10.

[16] Skehill, R.J and McGrath, S., "*IP Mobility Management*", <http://telecoms.eeng.dcu.ie/symposium/papers/F4.pdf>

[17] Ramjee, R., Li, L., La Porta, T. and Kasera, S., "*IP Paging Service for Mobile Hosts*", Proceedings of The Seventh Annual International Conference on Mobile Computing and Networking 2001 July 16-21, 2001, Rome, Italy, pp. 332-344.

[18] Vadali, R., Li, J., Wu, Y. and Cao, G., "*Agent-Based Route Optimization for Mobile IP*", Vehicular Technology Conference, IEEE Volume 4, 2001, pp. 2731-2735.

[19] Cheshire, S. and Baker, M., "*Internet Mobility 4x4*", ACM SIGCOMM Computer Communication Review, Conference Proceedings on Applications, Technologies, Architectures, and Protocols for Computer Communications August 1996, pp. 318-329.

[20] Tanenbaum, S.A., "*Computer Networks* ", Third Edition, 1996. <http://www.iprg.nokia.com/~charliep/txt/optim/optim.txt>

[21] La Porta, T.F., Sabnani, K.K. and Gitlin, R.D., "*Challenges for Nomadic Computing: Mobility Management and Wireless Communications*", <www.bell-labs.com/user/tlp/nomad.pdf>

[22] Ihara, T., Ohnishi, H. and Takagi, Y., "*Mobile IP Route Optimization Method for a Carrier-Scale IP Network*", Sixth IEEE International Conference on Engineering of Complex Computer Systems, 2000, pp.120-121.

[23] Blackwell, T., Chan, K., Chang, K., Charuhas, T., Gwertzman, J., Karp, B., Kung, H. T., Li, W. D., Lin, D., Morris, R., Polansky, R., Tang, D., Young, C. and Zao, J., "*Secure Short-Cut Routing for Mobile IP*", Conference Proceedings of Usenix Summer Technical Conference, Boston, Massachusetts, June 6-10, 1994, pp. 305-316.

[24] Woo, W. and Leung, V., "*Handoff Enhancement in Mobile-IP Environment*", 5th IEEE International Conference on Universal Personal Communications, Volume 2, 1996, pp.760-764.

[25] Solomon, J.D., "*Mobile IP The Internet Unplugged*", 1998, Prentice Hall PTR.

[26] Flademuller, A. and De Silva, R., "*The effect of Mobile IP handoffs on the performance of TCP*", Mobile Networks and Applications, Volume 4, No. 2, May 1999, pp.131-135.

[27] Eardley, P., Mihailovic, A. and Suihko, T., "*A Framework for the Evaluation of IP Mobility Protocols*", BT, Advanced Communications Technology Centre, King's College, London, Nokia / VTT Information Technology, The 11th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, Volume 1, 2000, pp.451-457.

[28] Forsberg, D., Malinen, J.T., Weckstrom, T. and Tiusanen, M., "*Distributing mobility agents hierarchically under frequent location updates*", IEEE International Workshop on Mobile Multimedia Communications, 1999, pp.159-168.

[29] Nikolaus, A. F. and Gorg, C., "*A Complete Comparison of Algorithms for Mobile IP Hand-offs with Complex Movement Patterns and Internet Audio*", Department of Communication Networks (ComNets), Center for Information and Communication Technology (ikom), <http://www.mobileip.org>

[30] Avancha, S., Chakraborty, D., Gada, D., Kamdar and T., Joshi, A., "*Fast and Effective Wireless Handoff Scheme using Forwarding Pointers and Hierarchical Foreign Agents*", University of Maryland Baltimore County, <http://userpages.umbc.edu/~kamdar/projects/691Treport.pdf>

[31] Chen J.C. and Agrawal, P., "*Fast Link Layer and Intra-Domain Handoffs for Mobile Internet*", The 24th Annual International Computer Software and Applications Conference, 2000, pp.325 –330. <http://ce.sejong.ac.kr/~dshin/Papers/MOBILE/pdf/p1-25.pdf>

[32] Castelluccia, C., "*Extending mobile IP with adaptive individual paging: a performance analysis*", Fifth IEEE Symposium on Computers and Communications, 2000, pp.113-118.

[33] Ylianttila, M., Pichna, R., Makela, J., Zahedi, A., Krishnamurthy, P. and Pahlavan, K., "*Handoff Procedure For Heterogeneous Wireless Networks*", Future Wireless Communication System, Global Telecommunications Conference, Volume 5, 1999, pp. 2783-2787.

[34] <www.cisco.com>

[35] Chen, G., Nocetti, F.G., Gonzalez, J.S. and Stojmenovic, I., "*Connectivity based k-hop clustering in wireless networks*", Proceedings of the 35th Annual Hawaii International Conference on System Sciences, 2001, pp. 2442 –2451.

Request For Comments

[R1] RFC 2002,October 1996, IP Mobility Support,
<http://www.faqs.org/rfcs/rfc2002.html>
[R2] RFC 1256, September 1991, ICMP Router Discovery Messages,
<http://www.faqs.org/rfcs/rfc1256.html>
[R3] RFC 1321, April 1992, The MD5 Message-Digest Algorithm,
<http://www.faqs.org/rfcs/rfc1321.html>
[R4] RFC 2004, October 1996, Minimal Encapsulation within IP,
< http://www.ietf.org/rfc/rfc2004.txt>
[R5] RFC 2003, *October* 1996,IP Encapsulation within IP,
<http://www.ietf.org/rfc/rfc2003.txt>

Appendix A

Glossary

Care-of Address – The IP address of the mobile node's current point of attachment to the Internet.

Cluster – A cluster consists of a group of nodes with one of them elected as a Cluster head.

Correspondent Node (CN)- A node that communicates with the mobile node. This node may be mobile or non mobile.

Foreign Agent (FA) – A mobility agent on the foreign network of the mobile node that provides services to the mobile node.

Foreign Network - A network, which the mobile node is currently visiting.

Home Address - A permanent fixed address of the mobile node, which is used by TCP and higher level layers.

Home Agent (HA) – A mobility agent on the home network of the MN that maintains a mobility-binding table.

Home Network - The network, which is identified by the home address of the mobile node.

Mobile Node (MN) - A node that changes its point of attachment to the Internet.

Mobility Agent - A node that offers some services to a MN.

Tunnel-The path, which is taken by, encapsulated (see below) packets. It is the path, which leads packets from the home agent to the foreign agent.

Vita 2

Ramasamy Raja Chinnanchetty

Candidate for Degree of

Master of Science

Thesis: MOBILE IP WITH A CLUSTER OF FOREIGN AGENTS

Major Field: Computer Science

Biographical:

Personal Data: Born in Singampunari, Tamilnadu, India, On October 21, 1978, the son of Mr.R.M.Chinnanchetty and Mrs.DaisyRani Chinnanchetty.

Education: Graduated from T.I. Higher Secondary School, Chennai, Tamilnadu, India in April 1996:Received Bachelor of Engineering in Computer Science and Engineering from the University of Madras, Chennai, Tamilnadu, India in April 2000.
Completed the requirements for the Master of Science degree with a major in Computer Science at Oklahoma State University, Stillwater, Oklahoma in December 2002.

Experience: Employed as Graduate Assistant, School of Industrial Engineering & Management, Oklahoma State University, 2001 to Present.