# ANALYSIS AND DESIGN OF MOBILE IP PROTOCOLS SECURITY

*Thesis submitted in partial fulfillment of the requirements for the award of degree of*

**Master of Engineering**

in

**Computer Science and Engineering**


*Submitted By*

**Amit Gupta**

**(Roll No. 801032002)**

Under the supervision of:

**Dr. Maninder Singh**
Associate Professor
Computer Science & Engg. Dept.
Thapar University, Patiala.

**Mr. Sumit Miglani**
Assistant Professor
Computer Science & Engg. Dept.
Thapar University, Patiala.



COMPUTER SCIENCE AND ENGINEERING DEPARTMENT

THAPAR UNIVERSITY

PATIALA – 147004


**June 2012**

# CERTIFICATE

I hereby certify that the work which is being presented in the thesis entitled, "***Analysis of Mobile IP Protocols Security***", in partial fulfillment of the requirements for the award of degree of Master of Engineering in *Computer Science and Engineering* submitted in Computer Science and Engineering Department of Thapar University, Patiala, is an authentic record of my own work carried out under the supervision of ***Dr. Maninder Singh*** & ***Mr. Sumit Miglani*** and refers other researcher's work which are duly listed in the reference section.

The matter presented in the thesis has not been submitted for award of any other degree of this or any other University.

**(Amit Gupta)**

This is to certify that the above statement made by the candidate is correct and true to the best of my knowledge.

**(Dr. Maninder Singh)**
Associate Professor
CSE Department
Thapar University, Patiala

**(Mr. Sumit Miglani)**
Assistant Professor
CSE Department
Thapar University, Patiala

**Countersigned by**

**(Dr. Maninder Singh)**
Associate Professor & Head
CSE Department
Thapar University, Patiala

**(Dr. S. K. Mohapatra)**
Dean (Academic Affairs)
Thapar University
Patiala

# Acknowledgement

*I wish to express my sincere gratitude to Dr. Maninder Singh, HOD, Computer Science & Engineering Department and Mr. Sumit Miglani, Assistant professor, Computer Science & Engineering Department for providing invaluable guidance and suggestions which inspired me to submit this thesis report.*

*I would also like to thank all the staff members of Computer Science & Engineering Department who were always there at the need of the hour and provided with all the help and facilities, which I required, for the completion of this work.*

*Last, but not the least I wish to thank my colleagues, who have given me moral support and their relentless advice throughout the completion of this work.*

**Amit Gupta**

# Abstract

This thesis work describes the route optimization between Mobile IPv6 nodes which introduced several vulnerabilities in mobile environment. The new technology 4G will be based on the transmission of Internet packets only, using an architecture known as mobile IP. So there is a need of fast data processing, low consumption of resources and high security. This will feature many advantages, however security is still a fundamental issue to be resolved. One particular security issue involves the route optimization technique, which deals with binding updates. This allows the corresponding node to by-pass the home agent router to communicate directly with the mobile node. There are a variety of security vulnerabilities with binding updates, which include the interception of data packets, which would allow an attacker to eavesdrop on its contents, breaching the users confidentiality, or to modify transmitted packets for the attackers own malicious purposes. Other possible vulnerabilities with mobile IP include address spoofing, redirection and denial of service attacks. For many of these attacks, all the attacker needs to know is the IPv6 addresses of the mobile's home agent and the corresponding node.

So firstly, in this thesis work, all the issues related to Route Optimization will be discussed. Threats which breach the security will be covered in the next part, but more security means more consumption of resources, latency problems, so there should be a balance between security and low end devices functionality. In the next part, all possible defense mechanism will be discussed for different type of connectivity like true relationship between nodes and lack of PKI infrastructure between mobile nodes.

There are a variety of security solutions to prevent these attacks from occurring. But all these solutions are strongly based on cryptography and authentication. Cryptography allows the transmitted data to be encrypted using some key in such a way resulting in any intercepted packets being illegible to the attacker. Only the party possessing the relevant key will be able to decrypt the message. Authentication is the process of verifying the identity of the user or device which is bound to that communication. Different architectures exist for authentication however many of

them rely on a central server to verify the users, resulting in a possible single point of attack. But that will overburden the centralized system and some problems like deadlock and latency problem may arise, so decentralized authentication mechanisms would be more appropriate for the nature of mobile IP and several protocols are discussed. However they all are resource intensive or give away vital address data, which can be used to mount an attack. As a result, a security solution is proposed to address the security vulnerabilities found in binding updates and attempts to overcome the weaknesses of the examined security solutions. At the end, analyses of different defense mechanism through comparative study is done and best solution for Mobile IP is found which may be more efficient and less complex.

# TABLE OF CONTENTS

# List of Figures

# List of Tables

# Chapter1. Introduction

## 1.1 A Brief Review of Mobile IPv6

After the evolution from 2G to 3G and now 3G to 4G, 4G will be based on the transmission of IP packets only, using an architecture known as mobile IPv6. Mobile IP [1] was introduced first to support mobility environment, it's a protocol that co-ordinates among different components of mobility environment such as home agent, foreign agent for mobility management to facilitate reachability of mobile nodes. The home agent has a static address while the mobile node's address changes every time it moves to a new location with a new point of attachment. The home agent keeps track of the mobile node's current address, so that if a correspondent does not know it, it may send the packets to the home address, which will forward the packets to the mobile node.

Initially one mobile node couldn't communicate directly with another mobile node because all traffic passed through the home agent and then to the foreign agent. But as Mobile IPV6 [2] was introduced, the communication among mobile node and correspondent node had gone directly and thus improving the performance of mobility protocols by reducing delay with direct communication. Next Chapters will investigate the mobile IP architecture in more depth and also look at some of the surrounding protocols. Because 4G require a fast response, so IPv6 will feature many advantages, however security is still a fundamental issue to be resolved. One major security issue involves the route optimization (RO) technique, which deals with binding updates. This allows the corresponding node to communicate directly with the mobile node by passing the home agent router. Before route optimization, binding updates are exchanged between mobile node, home agent and correspondent node which causes a variety of security vulnerabilities. Binding updates include the interception of data packets, which would allow an attacker to eavesdrop on its contents or to modify transmitted packets for the attacker's own malicious purposes. There are other possible vulnerabilities with mobile IP like address spoofing, IP redirection and denial of service attacks. But to perform these attacks, all the attacker

needs to know is the IPv6 addresses of the mobile's home agent and the corresponding node.

To implement route optimization the mobile host sends a Binding Update (BU) to the correspondent node for direct communication by informing the current location of the mobile host, thereby a Binding Acknowledgement (BA) message sent by correspondent node starts direct communication among mobile node and correspondent node. Here an attacker can send the false Binding Update message to fool mobile host, home agent or the correspondent node. And so route optimization has introduced new scope for an attacker by sending malicious Binding Update and thus produced security vulnerabilities to mobility protocols.

To prevent these attacks two of the main solutions are cryptography and authentication. Cryptography allows the transmitted data to be in encrypted form resulting in non-readable form of the intercepted packets. Only the authorized party possessing keys will be able to decrypt the message. Encryption provides the confidentiality of the data and can be done in two ways, symmetric and asymmetric. Symmetric key cryptography is useful for low powered devices and participants use the same key to encrypt and decrypt. The main problem is PKI infrastructure and without it, how the keys will be distributed. Asymmetric key cryptography has two types of keys as encryption and decryption keys. This is useful for the distribution of the keys and can help with authentication with the use of digital signatures. The drawback however is that processing consumption is higher than symmetric cryptography. Second solution is authentication to verify the identity of the user or device one is in communication with. The components implementing authentication will include techniques such as hashes, digital signatures, address based keys and cryptographically generated addresses. There are different authentication schemes exist however many of them rely on a certification authority and consumes resources. So decentralized authentication mechanisms would be more appropriate for the nature of mobile IP. But in spite of all these facts, the main focus of true communication will be either cryptography or authentication or mixing of both.

Thus the objective of this work is to analyze the existing security threats and possible security threats that may arise due to existing solutions and compare the existing defense mechanisms to these threats and propose some future solutions that are less complex and concrete. Effort of this work is to remove or reduce the limitation of existing defense mechanism and discuss their pros and cons upon previous solutions. That is the focus of this work is on authenticating the binding updates.

## 1.2 Scope Limitation

Although several attacks are considered into account but the limitation to provide the secure interface is limited to route optimization only, otherwise there may be so many attacks possible instead of the attacks discussed for mobile environment in this work. So this research basically based on securing the binding update message in route optimization.

## 1.3 Structure of Dissertation

The structure of this work is as follows:

Chapter 1 gives an introduction part of the work telling about Mobile IPv6 and gives bird-eye view to the work.

Chapter 2 explores the Mobile IPv6 architecture with background research and explains the concept of the binding update in route optimization technique. Chapter 2 also discusses the flaws and possible attacks which can occur to binding updates.

Chapter 3 discusses the problem definition and research questions arose for Mobile IPv6 in real environment.

Chapter 4 discusses the defense mechanism which may combat the possible attacks discussed in the previous chapter.

Chapter 5 explores the comparison of different existing defense protocol and discusses the proposed solutions to combat the remaining attacks after comparison.

Chapter 6 gives the conclusion of this work or thesis.

# Chapter2. Literature Survey

## 2.1 NETWORK ARCHITECTURE FOR ROUTE OPTIMIZATION

When a mobile node starts communication by sending packets to the correspondent node, Home Agent (true relationship between mobile node and its home agent) intercepts the packets through an IPSec secure tunnel and forwards them to the correspondent node. When the mobile node moves to a new location, mobile node tells about its new current location called as care-of address (CoA) to the home agent (HA). It causes HA to update the secure tunnel so that packets are routed to and from the new CoA. Authentication and encryption of the binding update (BU) and the following binding acknowledgement (BA) are possible due to preconfigured IPSec security association in tunnel-mode between the mobile and the home agent. But this routing is not optimal and so Route Optimization (RO) technique is used in which MN sends BU directly to correspondent node (CN) and tells CN about its CoA. But there is a need to authenticate that BU among them. To implement this Internet Engineering Task Force (IETF) proposed Mobile IP which aims mainly two problems [6] at the same time:

i. First, Mobile IP allows transport layer sessions (TCP or UDP) and IPSec security associations to continue between the mobile and other hosts even if the underlying host(s) are roaming and changing their IP addresses.
ii. Second, it allows a host to be reached through a static IP address (home address) for new connections.

The first problem matters in case if protocol is stateful, but does not affect stateless protocols such as HTTP. Since stateful protocol saves the state and important parameters for ongoing session to make communication fast. The second problem is most important for servers but not client computers. The route optimization [8] protocol is shown in Figure 2.2. BU may be sent either when the mobile has data to send to CN or when mobile receives the data from CN and mobile node moves from one network to another. When a mobile node changes its current location, it sends BU initial message to CN which contains mobile's home address (HoA) [9] and current care-of address (CoA). The CN node then verifies the initial update message is sent by authenticated user or not, if it is authenticated CN sends some keygen token to

MH. MH then generates a binding secure symmetric key and hashes the BU and device information with that binding key and send it to CN. CN after confirmation sends the binding acknowledge (BA) and stores the new location information in its binding cache for future communication but cache may not be updated, so cache needs to be refreshed after every few minutes to continue communication even if the mobile stays at the same CoA. In case if cache entry expires then the same procedure of BU and BA will start again and it continues in this way.

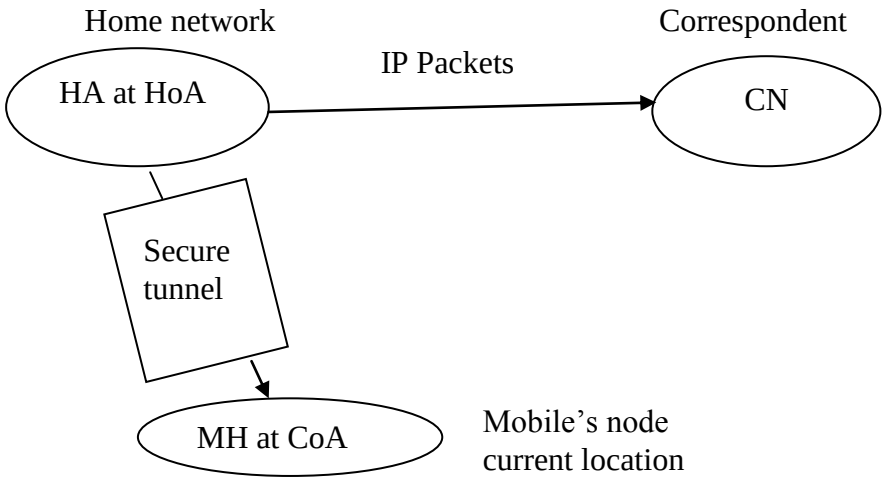


**Figure 2.1 Communications before Route Optimization**

The transparent mode of Mobile IPv6 operation is shown in Figure 2.2. Only one packet is sent via the unoptimized route. But after the binding has been created, the mobile node and the correspondent node can communicate directly. A mobile that is about to send a packet to a correspondent uses the CoA as the source IP address and inserts the home address destination option (HAO), which contains HoA in it, in a type-2 routing header (RH) after IP header. When the CN receives the packet, it overwrites the source IP address with the HoA from the HAO, and thus re-creates the original packet. But actual current address is CoA so when CN sends the packets to the mobile it contains the HoA in a type-2 routing header (RH), it compares this destination address against the HoA in its binding cache. If a binding entry exists in the cache memory, it replaces the destination IP address with the actual destination CoA and inserts the RH after the IP header. The mobile node after receiving the packet, copies the HoA from the RH header back into the destination address field and removes the RH, thus re-create the original packet. In this way, upper layers in OSI network model including IPSec and the transport layer are made transparent for

mobility. And upper layers always see HoA for mobile node. That is, the source address of outermost IP header always belongs to the subnet from which the packet is sent and thus packet is not dropped by ingress filtering. Thus HAO and RH provides the tunneling header for direct communication among MN and CN.

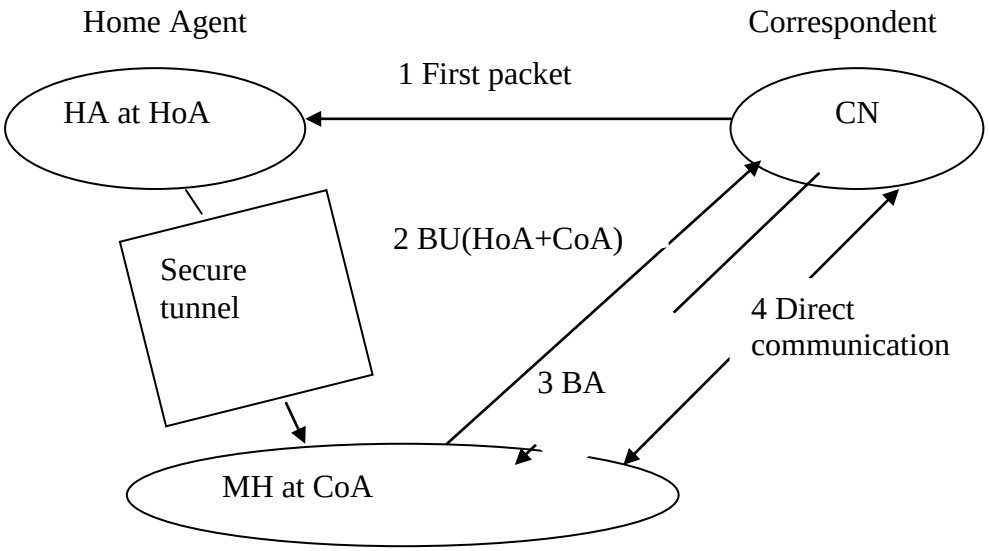


**Figure 2.2 Communications after Route Optimization**

## 2.2 Related Work

Time to time so many researchers tried to find the security threats and their solution in mobile environment. P. Nikander et al. [3] explains the Mobile IP version 6 route optimization security design background. J. Arkko et al. [4] discusses how to authenticate unknown principals without trusted parties. D. Hu et al. [5] describes the security threats in mobility environment and propose solution with a public Key Infrastructure (PKI) and secret key based approach for it. But there is a lack of concrete solution to mitigate the attacks (existing as well as new possible or identified threats). Some of the security threats are traffic redirection attack, man-in-the-middle attack, replay attack, bombing attack, reflection and amplication, home agent poisoning etc. These attacks may be serious for data, resources of mobile nodes as well as network resources and thus can break the main principle of network security and also degrades the performance of network and network components.

There are several schemes are proposed to mitigate these threats against the vulnerabilities of mobility protocols, such as binding update (BU) authentication,

return routability protocol, IPSec protocols, PKI and secret key-based approaches like cryptographic address generation. But these protocols do not provide a complete solution and have several limitations. PKI and secret key based schemes can be implemented with the existence of infrastructure as trusted certification authority. The return routability protocol can't be implemented if the attacker is on the path between the HA and CN. IPSec protocol works securely if the nodes have a true relationship in between them. Protocols involving cryptographic solutions require higher processing power, and that would not be suitable for low end devices. So there is a need of computationally less expensive and low latency solutions to mitigate security attacks with low processing power, so that the main objective for seamless connectivity of mobility protocol is not affected.

## 2.3 Attacks on Mobile IP Protocol

Mobility protocols, because of lack of secure infrastructure, may lead to so many threats that must be checked out for mobile nodes communication. All attacks are concerned with false binding updates, usually resulting in Denial-of-Service attacks. Different threats discussed here are Traffic Redirection Attack, Connection Hijacking or Man-in-the-Middle Attack, Bombing Attack, Replay Attack, Reflection and Amplication Attack, Home Agent Poisoning, Resource Exhaustion and State Storage Exhaustion.

### 2.3.1 Traffic Redirection Attack

An attacker sends a false BU to the CN while CN is communicating with the authenticated mobile node and claims in BU that current location of MH has changed to a fake receiver IP or a non existing receiver. If such malicious BU is accepted by the CN, it will start sending packets to the new current location as CoA (fake receiver) and the victim node will not get any traffic. In case, if the redirected node does not exist, then the message "destination host not reachable" is sent to the correspondent node and so correspondent node will stop to send the traffic further to the mobile node. But still there are some servers as correspondent node that will continue to send the traffic to the non existing mobile node. Even if the data is encrypted by any means, an attacker can redirect the traffic, because BU is transparent to upper layer and only thing is required the IP addresses of the communicating nodes. Therefore, nodes with well-known IP addresses, such as public servers, DNS servers or file

servers are more vulnerable to such attacks. Figure 2.3 shows how the communication is redirected towards the third user by sending false BU.

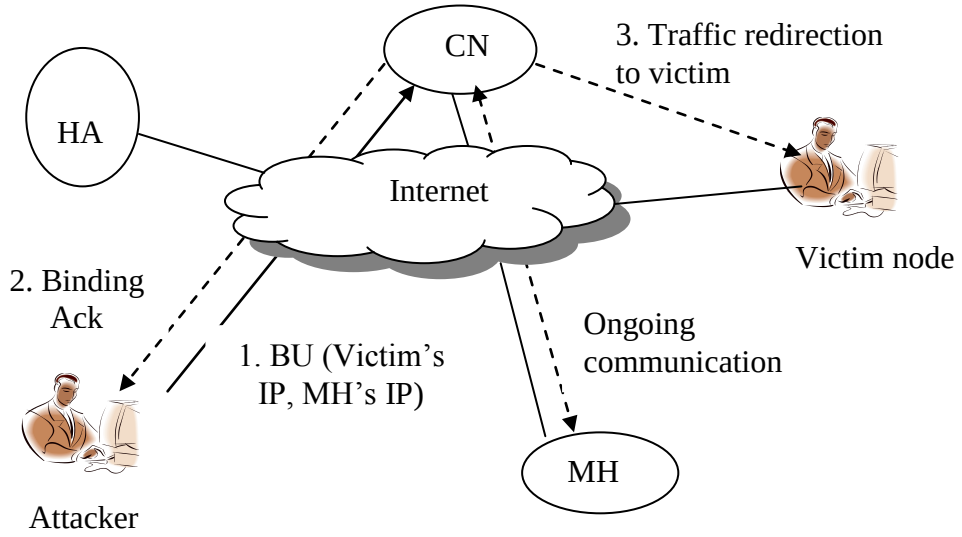


**Figure 2.3 Traffic Redirection Attack**

### 2.3.2 Connection Hijacking Attack

An attacker sends a false BU to the CN while CN is communicating with the authenticated mobile node and claims in BU that current location of MH has changed to its own IP. If such malicious BU is accepted by the CN, it will start sending packets to the attacker's IP. The attacker now will be able to learn the information of the message if message is not encrypted and so can modify the information before forwarding it to the MH. And so intermediate attacker called as a man in the middle getting all-important private data which was for the victim (MH) without the knowledge of the CN and the MH. Even if the data is encrypted an attacker can change or redirect the encrypted data while it is not able to learn the data.

### 2.3.3 Bombing Attack

Bombing attack may cause due to false change in current location through BU from attacker's actual IP to victim's (MH) IP. In this attack, an attacker is MH itself, first starts to download the data from server (CN) after performing TCP handshake and note down the sequence number of ongoing communication. And then he sends a forge BU involving victim address as care-of address. If this BU is accepted by CN a huge amount of unsolicited data traffic are redirected to the victim node (or a network) to degrade its performance as well as to waste its bandwidth. Thus while the BU is authenticated but it is not true because of lack of verification of care-of address.

So an attacker may exploit real-time streaming servers which are very common and known for this kind of attack. Figure 2.4 shows the bombing attack on a MH which overwhelms MH with unsolicited data packets and degrades its performance.

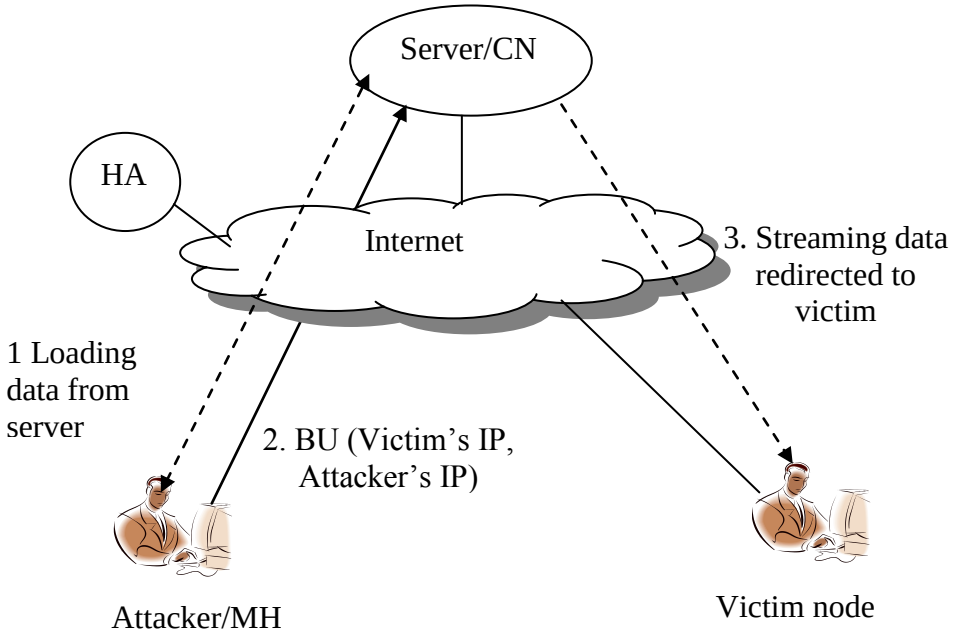


**Figure 2.4 Bombing Attack**

But when data packets are forwarded towards the victim node, victim node will not accept those unsolicited (streaming data) packets and will not send the acknowledgement for those unnecessary packets, thereby stopping the communication. But because an attacker knows the sequence number of ongoing communication it can spoof acknowledgement towards the server making a continuous flow of data streams sent to the victim. One TCP Window (may consist huge data) requires only one acknowledgement and so requires less spoofed acknowledgement to send a large data stream to victim node. Still there is a facility at the transport layer to stop the unnecessary data streams, victim node can send a TCP RESET signal. But it may not work because when the victim node reads the routing header of data packets at the network or IP layer then it encounters a strange address of an attacker as home address, so victim node will not allow to flow the packet up in transport layer and so victim can't change or reset TCP sequence number. So no TCP reset signal will be sent to the server and victim can't stop to coming data streams.

The bombing attack may be serious since an attacker can send a huge amount of unwanted data to any Internet node and the target node have nothing to stop the data

stream, thereby losing its bandwidth without knowing about the attack. If an attacker does not know an individual address, it may target a network by redirecting the data to one or more IP addresses within its address range. And thus attack becomes severer and called as distributed denial-of-service (DDoS) attack.

### 2.3.4 Replay Attack

In this type of attack, an attacker first intercepts the authenticated BU sent by MH to CN and then stores it. Now attacker replays this stored BU later on when MH moves in future to a new location. And thus misguides the CN by interrupting the ongoing communication in between MH and CN. But an attacker may capture the packets for binding update (BU) only if the attacker and the MH are in the same network. BU here is authenticated but replayed and so there is a need to confirm the freshness of packets for BU. Packets start to flow towards another host may be still IP address of another node or not. Though replay attack can be mitigated by introducing time stamping but because time clock for mobile devices may be different, so it is not so useful. Further it was thought that sequence numbered BUs may be used to prove the freshness of packet but still an attacker can intercept the sequence number and delayed for later attack. So to mitigate replay attack there should generate a random number as nonce index in RR protocol that may be known at both sides and so can signify the freshness of packet.

### 2.3.5 Reflection and Amplication Attack

In reflection attack, an attacker takes the advantage of the BU security protocol in some earlier design (earlier design of return routability test), because in the earlier design of BU security protocol, to validate the BU authentication CN sends two messages to the MH, one through home agent via secure tunnel and another one directly . CN could initiate route optimization signaling whenever CN receives spoofed initial BU message packet through an attacker, and this can lead to reflection attack. Route optimization is initiated at home address that is included in the Home Address option. Fig. 2.5 shows the reflection attack. When an attacker sends a false BU message to the CN, MH receives every packet sent by the attacker twice due to BU security protocol action. Thus an attacker may amplify a packet flooding attack against a target MH by a factor of two. And both the messages arriving at the target

have the CN's address as the source address, so the identity of the attacker is also hidden at the MH.

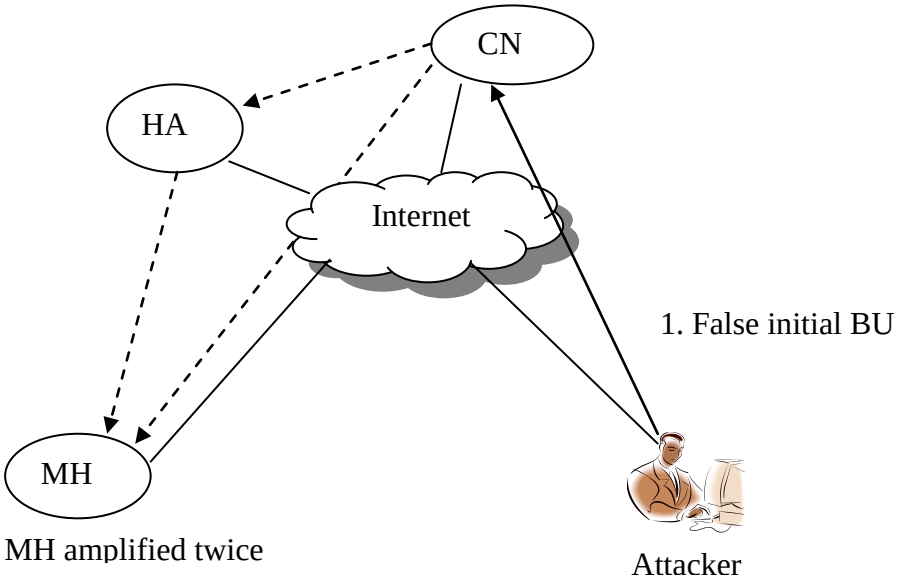


**Figure 2.5 Reflections and Amplification Attack**

To mitigate this attack RR protocol was improved in which one additional initial parallel messages as cookie are sent by MH to CN directly as well as through HA which will be discussed in detail in RR protocol.

### 2.3.6 Home Agent poisoning

HA can be made poison if there is no secure tunnel in between the HA and MH .HA keeps the mapping of Home address to CoA for MH. So if a MH moves to a new location, updates are sent to HA to update the database entry, here an attacker may send the fake BU to HA to corrupt its database entry if the tunnel between HA and MH is not secure. Now all the subsequent messages will be sent to the wrong IP address and thus MH will not be reachable by any means through any internet node. Therefore, the subsequent query to the HA by any CN (for the MH) will produce wrong reply.

### 2.3.7 Attack on Access Network or Resource Exhaustion

An attacker first establishes a number of connections with MH by changing its IP address. Therefore, whenever a victim node moves to a new location, it has to send legitimate BU to all these imaginary IP addresses and so MH requires huge processing power to deal with unnecessary BUs. Attacker can block MH from sending legitimate BU by launching brute-force attack on the radio link or by a

flooding attack. At this time, the attacker can send fabricated BUs to the CNs and the HA, thereby redirecting MH's traffic towards the attacker. Thus attacker can easily perform session hijacking and all other attack.

### 2.3.8 State-storage Exhaustion

In a stateful protocol, whenever an attacker sends an initial BU message, the CN responds with two secret values by storing them in its memory cache until it receives the authenticated BU. An attacker takes the advantage of this and sends initial BU message so many times to exhaust the state storage and thus prevent the legitimate mobiles from using route optimization with the CN. This attack can be mitigated by making CN stateless and CN stores only the master key value Kcn (as in RR protocol) which is used to compute two secret keygen token values send to HA and MH. CN recomputes the keygen token when it receives authenticated BU. And thus no state-storage exhaustion takes place. It is very difficult to find which end of communication should be stateless, but responder or CN (more often server) is necessitating being stateless.

## 2.3.9 Summary

Route optimization for mobile IPv6 can cause so many security vulnerabilities with binding updates as different kind of threats discussed above. An attacker can take advantages of these attacks. But still an attacker should have known about the IPv6 addresses of the mobile's home agent and the corresponding node.

The chapter 4 will discuss the security solution to combat these threats which will be basically based upon cryptography, protection of binding updates and authentication of data.

# Chapter 3 Problem Statement

## 3.1 Identification of Gaps

To authorize the binding updates in Mobile IPv6 involves several gaps as:

1. The first gap identified is the vulnerability produced during the exchange of binding updates and binding update message is crucial for the route optimization to take place.

2. Second gap is the security solutions which are used to combat the threats produced during binding update authentication. It was determined that there were holes in these solutions that attackers could take advantage to eavesdrop the packets.

With the introduction of the proposed security techniques, these holes no longer exist, however other gaps in have arisen as:

- How long the distribution authentication protocol can protect from attackers as attacker can take advantage of load distribution on network and may cause congestion and may perform malicious activity?
- How Mobile Home Agent should be programmed so that their robust programming may prevent from malicious Mobile Agents?

These are all questions, which could be answered, in future work.

## 3.2 Unanswered Research Questions

The biggest question arises about the fact of infrastructure in Mobile IPv6, whether the solutions against the security vulnerabilities of the binding update in route optimization protocol may be developed using the existing infrastructure? The solution would have to combat the security issues of attacks which are responsible for sending false binding updates to redirect data traffic for interception and eavesdropping of packets or the prevention of communication via denial of service attacks. And at the same time, nodes can exchange the security keys effectively

facilitated without a central authentication authority, there should be a distribution approach to ensure about latency problems and fast processing.

If anyhow a solution is proposed without PKI infrastructure approach, can it be used to improve its effectiveness and make it less vulnerable to certain types of attack? Another research question arises, can these solution will give a surety to combat new possible attacks due to some flaws in security? All of these questions can have a answer only if comparison between different protocols is done for their working in mobile network and then by observing all possible advantages and disadvantages of current security systems. After considering these facts either researchers may be able to design a completely new design of security protocol or may modify the existing solution to make them more effective and concrete. Instead of this, if possible then different protocols can be combined collectively combining their advantages. Route optimization is a focal discussion point in this work which is a need to overcome the latency issues like in triangle routing. So another question may arise can the solution for Mobile IPv6 may reduce latency in triangle routing with same security and location privacy? Can a solution which is required in infrastructure changes as a software change is possible to combat attacks rather than hardware changes?

## 3.3 Problem Definition

Because of introducing the new technology like 4G, Mobile IPv6 becomes the most important technology for fast communication. In mobile IPv6, two mobile nodes can communicate directly called route optimization, but the binding update in route optimization protocol suffers from security vulnerabilities, through which an attacker may send false binding updates to redirect data traffic for interception and eavesdropping of packets or the prevention of communication and thus causes the denial of service attacks. There is no current secure protocol which may effectively authenticate the legitimacy of the users or hide the location data of the home agent and care of address, leaving the participants vulnerable to attack. And if there exists a solution, then they are resource intensive in terms of processing power required, which is unavailable with mobile devices.

Thus the proposed solution will address these issues without modifying the established mobile IPv6 architecture. Its main focus is to provide the authentication to user and device while providing an option for distributed authentication to aid with processor intensive situations. The solution will also take latency into consideration during designing and will protect the nodes from false binding updates attempting to denial of service.

## 3.4 Objectives

1) To study the different threats arose due to route optimization technology.

2) To analyze the present existing protocol for mitigation of different possible threats.

3) To verify whether the security is breached or not after comparison of the existing protocol.

4) To design the protocol to secure the network from remaining possible threats.

# Chapter 4 Analysis of Security Mechanism against Threats

Different mechanisms are used to secure the mobile network against threats but all of them should have particular goals which are as follows:

1) To prevent or mitigate all possible security attacks.

2) Simple and computationally less expensive algorithm to be implemented in mobile nodes with low processing power.

3) Low latency solutions.

4) To prevent the attack arises due to security protocol itself.

5) Need of infrastructure less authentication.

## 4.1 Consideration for Designing Protocol against Threats

The goal of the IETF working group was that the Mobile IPv6 protocol should be *at least as secure as the current non-mobile IPv4 Internet*.

Our ambition was limited to making sure that Mobile IPv6 does not introduce any new major vulnerability to the Internet. Because of inclusion of home-address destination option (HAO) (it hides the CoA address), mobility is transparent to the upper layers including IPSec and transport layer. So End-to-end encryption and integrity protection with authenticated SSL or IPSec can prevent the attacks against data secrecy and integrity but not denial-of-service. That is an attacker is able to redirect the encrypted data even though it can't read it. The obvious solution to the BU spoofing is to authenticate the binding updates. The problem is that the authentication needs to work between any mobile Internet node and any correspondent. Currently there does not exist any infrastructure in between two mobile nodes that could be used to authenticate all IPv6 nodes. While IPSec tunneling can be used between mobile node and home agent but it can't be used between two mobile nodes due to lack of infrastructure. Firstly in this paper, the security in between mobile node and home agent will be discussed and then security in between mobile and correspondent node will be considered.

## 4.2 Encryption

### 4.2.1 Symmetric Vs Asymmetric

Encryption is of two types which are symmetric and asymmetric. Symmetric encryption uses a single key to encrypt and decrypt data and this is a fast algorithm to implement but it requires a PKI infrastructure for certification and so a lot of hardware. While Asymmetric key encryption uses two keys, one to encrypt the other to decrypt called the public and private keys. It uses RSA algorithm and if the key is intercepted, the attacker will only be able to encrypt data not decrypt it. But Asymmetric key cryptography is slow, more power consuming and resource intensive which may be a big problem for mobile environment. Thus it is better to use them after combining their features.

## 4.3 IP Security Protocol (IPSec protocol)

As we know, an IP packet consists of two portions: IP header and the actual data. IPSec [5] defines two IP extension headers: one for authentication and another for confidentiality. So IPSec consist of two protocols mainly as Authentication Header protocol (AH), Encapsulating Security Payload protocol (ESP) and a supporting protocol as Internet Key Exchange Protocol (IKE).

### 4.3.1 IKE Protocol

IKE [10] is the initial phase of IPSec, where the algorithms and keys are decided. The output of the IKE phase is a Security Association (SA). SA is an agreement between the communicating parties about factors such as the IPSec protocol version in use, mode of operation (transport mode or tunnel mode), algorithms, keys, lifetime of keys etc. once this is done, both major protocols of IPSec (i.e. AH and ESP) make use of SA for their actual operation. Moreover, an SA is simplex, i.e. unidirectional. Therefore, at a second level, we need two sets of SA per communication party that is one for incoming and another for outgoing transmission. Thus if two communicating parties use both AH and ESP, each one will require four sets of SA. So Security Association Database (SAD) is maintained at both communicating node which contains active SA entries.

*IPSec key Management Scheme*

This key management in IPSec consists of two aspects: Key agreement and distribution. The protocol used in IPSec for key management is called Oakley protocol. Oakley is based on the Diffie-Hellman key exchange protocol, with a few variations. It fulfills our aim for mobility protocols:

a) To create secret keys as and when required.
b) It has features to defeat Replay Attack.
c) It implements a mechanism called as cookies to defeat resource exhaustion (attack by sending forge BU) at victim node.
d) It provides authentication mechanisms to thwart man-in-the-middle attacks.

But there should be true relationship between the communicating nodes to implement key management through this mechanism. So we can ensure key management in between mobile node and its home agent, while not between mobile node and correspondent node. We can use IPSec tunnel mode to provide security between MN and HA. And to provide authentication, integrity, confidentiality of packets IPSec is used with AH protocol or ESP protocol or both.

### 4.3.2 Authentication Header protocol

AH [11] protocol provides connectionless integrity and data origin authentication of IP packets and anti-replay service using sequence number if required. This protocol consist a cryptographic checksum similar to message digest for the content of binding updates, so Internet Key Exchange (IKE) infrastructure with certificate authentication is required. On receipt of an IP packet, receiver processes the AH first to know about content of packet whether it is tampered or not. AH protocol can be used in tunnel mode or transport mode, but it needs a true relationship between MH and CN. Therefore, use of AH protocol to authenticate the BUs between the MH and CN is not feasible. But MH has a prior relationship with HA, so IPSec AH protocol is suitable to be used to authenticate BU between MH and HA. Figure 4.1 shows the use of AH protocol for securing BUs from MH to the HA and to achieve this first Security Associations (SA) are performed between them.

By establishing security associations between MH and HA, both nodes know the IPSec protocol version, mode of operation (tunnel or transparent) and algorithms used with keys etc. And thus a secure tunnel is formed in between MH and HA and these

nodes are ready to use AH protocol. Therefore, when MH moves to a new network, it sends BU message in which the authentication header is inserted after the IP header and before the next layer protocol header (transport mode) or before an encapsulated IP header (tunnel mode). This ensures the binding update is from MH itself, not a fake one. This is AH which ensures MH node and it is possible due to the public key infrastructure (PKI).

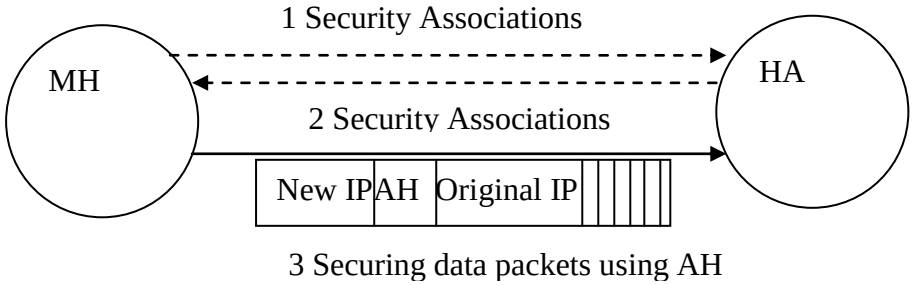


**Figure 4.1 Security association and AH in Tunnel Mode**

### 4.3.3 Encapsulating Security Payload protocol

AH protocol is used between the HA and MH to authenticate the BU and was possible due to a relationship between them. But AH protocol cannot provide confidentiality of data contents. Therefore, Encapsulating Security Payload (ESP) [12] protocol can be used alone to provide confidentiality of data or within AH protocol to provide authentication also. When ESP is used in conjunction with AH, receiving node first check authentication, data integrity and then decrypt the content by extracting keys and algorithm (chosen during SAs were established) associated with ESP. At the time of security association establishment the set of services can be chosen ESP protocol or ESP with AH protocol or simply AH protocol depending on requirement. An encryption algorithm is used to encrypt the data packet by using a key to form a special format with ESP header, trailer and authentication data is combined into a packet and transmitted to the destination as shown in Figure 4.2. ESP protocol can also be used in tunnel or transport mode.

Therefore, MH and HA can communicate securely for the binding updates because of true relationship between them and so IPSec with AH and ESP can be used between them. Now the main concern is for MH and CN because of no true relationship, so there should be a need to authenticate both of the nodes first and then the data should

be encrypted by some binding key through binding update. Return Routability protocol is designed for this purpose as explained in next section.

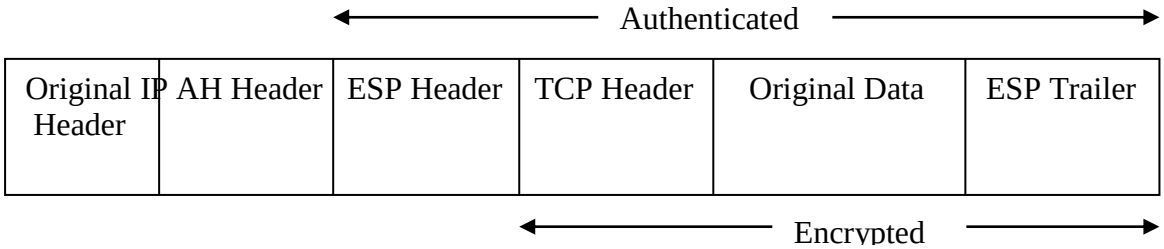


**Figure 4.2 ESP with AH in Transport mode**

## 4.4 Cryptographically Generated Address

The use of Cryptographically Generated Address (CGA) [13] can reduce the chance of attack on a victim node. It is intermediate level security which is above no authentication. This idea was first introduced in a BU authentication protocol known as CAM [14]. After that so many approach was proposed on basis of CGA approach. In this approach, the least significant interface identifier 64-bits of the IP address is selected by computing a 64-bit one-way hash of node's public signature key. The main focus of this approach was to bind the IP address of node with its public key to provide authentication of BU. Therefore, mobile host signs the binding update with its private key and sends the public key along with the signed data. The recipient of the binding update hashes the public key and compares the hash to the address before verifying the signature on the location data. Thus the node having authenticated update can send BU because its address is associated with its public key. The main advantage of this approach is that it provides public-key authentication of the IP address without any trusted third parties or PKI. But there is a limitation to verify CoA means no checking for the location of CoA in this scheme and may cause bombing attack.

A major problem may produce if an attacker can create its own CGA address but in this scenario an attacker will not be able to spoof someone else's address since address is binded with the key which is only known to the authenticated user. Another problem is that CGA assures the interface identifier part of the address, but still does not care for the reachability at the identifier. As a result, CGA needs to be used together with a reachability test such as return routability. So CGA offers the main advantages:

1. It sign messages with the owner's private key and so the spoofing attack against the IPv6 address becomes much harder.
2. CGA approach does not need any update or extra infrastructure to implement this approach.

It may be possible that an attacker may replay old signed messages by the key owner, however this can be rectified by associating the CGA owner with the address. The exact address of the sender must be known when a CGA address is used to authenticate messages from the IPv6 node. So CGA approach may prevent spoofing of IPv6 Addresses but it may not tell which address is the correct one. So CGA is not a complete authentication solution for all purposes and so return routability is used for this purpose.

## 4.5 Return Routability Protocol

Routing in the mobile environment is semi-reliable. Security can be achieved using IPSec between the nodes of trusted relationship. Now this protocol is designed to implement the security between the nodes which don't have true relationship that is between MH and CN. But in order to sniff or intercept a packet, the attacker needs to be on its route. This test is performed to authenticate the BU. This is shown in Figure 4.3

**Message 1(a)**

Initially HA receives the Home Test Init (HoTI) as home init cookie C1 (random generated 64-bit number) message sent by the MH and then forwards it to the CN.

**Message 1(b)**

MH also sends a Care of Test Init (CoTI) as care of init cookie C2 (random generated 64-bit number) to CN directly. Both HoTI and CoTI should be returned back to MH to authenticate the communication.

**Message 2(a)**

Each correspondent node is assumed to maintain a secret key (20 bytes) Kcn and a key generating function as HMAC SHA1() involving parameters as Kcn, Home (or Care-of) address and some nonce index and a byte index (0 for HoA and 1 for CoA) to calculate a MAC (message authentication code) involving a secure cryptographic hash function SHA-1. The first 64-bit output of function is used as keygen token k1 as

h(Kcn,HoA,0) and k2 as h(Kcn,CoA,1) send by CN in HoT and CoT as return messages to MN. So CN sends HoT (home init cookie C1+ home keygen token K1 + home nonce index) to HA and HA forward it to MH.

**Message 2(b)**

CN also sends CoT (care-of init cookie C2 + care-of keygen token K2 + care-of nonce index) to MH directly. Nonce (random generated number) in HoT and CoT is used to prevent the replay attack to tell the freshness of packet.

**Message 3**

MH, after matching the received cookies as send by it in HoTI and CoTI, hashes both the home keygen and care-of keygen tokens together and results in a 20-byte Kbm (binding management key) using the SHA-1 function. Then MH records the value of Kbm as h (K1, K2) and the nonce indices correspond to HoT and CoT messages sent by CN, and use them in the binding update.

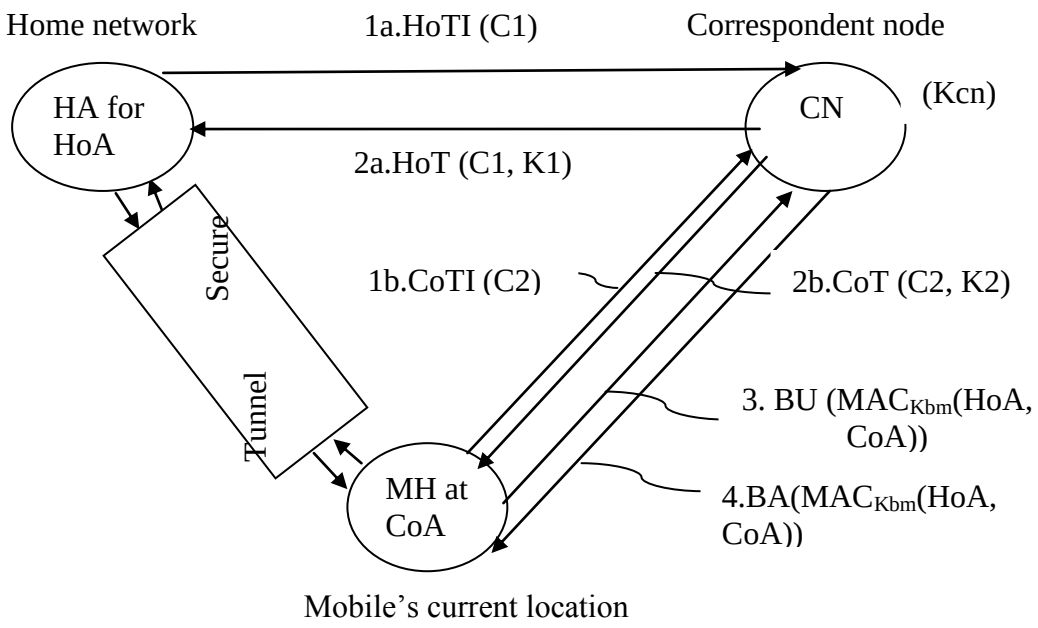


**Figure 4.3 Return Routability Test Protocol Working**

**Message 4**

After getting authenticated binding update (BU) from MH, CN sends a binding acknowledgement (BA) using same key as in BU to MH and communication starts among them at optimized path.

Because the key sent by the CN is again used by MH to send binding update to the CN so it is called return routability test. In this way, the CN node verifies that the mobile is able to receive messages at the home address.

**Limitations:**

1. Because the nodes are mobile so there is no prior relationship or security association exists between these nodes. An Attacker which is in path between CN and HA can act as a mobile node and can sniff all the packets and it can capture the keys in between path and can send his fabricated keys to CN and HA and thus can harm the reliability of this protocol by spoofing the BU.
2. Vulnerability for spoofing BU is also possible when the CN is also another mobile node at an access network which is insecure. For that case, an attacker in such network may capture the keygen tokens to spoof BU. Channel between the HA and MH is assumed to be secure to send the right key to the MH.
3. Key sent in communication as plain text that is not encrypted and so attacker in between path can read them easily.
4. The two reachability tests can lead to a handoff delay unacceptable for many real-time or interactive applications such as Voice over IP (VoIP) and video conferencing.
5. Finally, periodically refreshing a registration at a correspondent node implies a hidden signaling overhead.

**Advantages:**

1. The number of potential attackers and targets are reduced. The attacker must be on the route of the hijacked connection. That is in between path of CN and HA.
2. The RR protocol uses less CPU processing power since it uses inexpensive encryption and light one-way hash function unlike other complex authentication method.
3. It does not store the state until CN has authenticated the MH, while it stores the key of their communication.
4. The RR protocol uses nonce (home keygen token) to avoid replay attack since nonce (random generated) in token also tells the freshness of the BU. On the

other hand, sequence numbered BUs can be interrupted by an attacker after looking on sequence number.

5. The RR protocol also verify the location of CoA to authenticate BU, this can be used to overcome the Bombing Attack in which authenticated mobile node can send false care-of address in forge BU.
6. Initial messages are directed by MH as cookie (without init cookies anyone could spoof the HoT and CoT messages and thus can determine the value of the binding management key) prevents the reflection and amplication attack because MH initiates BU authentication to avoid reflection and the correspondent sends as many as messages as it receives to prevent amplication.
7. Correspondent node is stateless (prevents stage-storage exhaustion) because it responds according to received messages as HoTI with a HoT and CoTI with a CoT.

## 4.6 Ingress Filtering:

Ingress filtering means to deploy a gateway or router which checks upon all the ongoing traffic to and fro from the local network. It act as a firewall that checks the source addresses of all packets that are leaving the local network and drops those ones which are not originated from the local network. This can limit the number of potential attacker and their targets. But ingress filtering to be effective if it is applied on the attacker's local network because an attacker's false BU will be filtered out by the gateway in this case. But it can't protect attack targets to victim's network. Also there is a problem in Mobile IPv6 that it uses care-of address as sub-option means sending a false care-of address without spoofing source address. Such an address is not subject to inspection by ingress filtering and would have to be verified through other means. But still ingress filtering can be used to reduce the potential attacks.

## 4.7 Stateless Mobile Nodes (CN)

CN node should be stateless for receiving and replying to BU messages, otherwise an attacker can exhaust the memory or resources containing legitimate states and then can send fake BU to take advantage of exhaust memory. Therefore stateless [15] approach can prevent the corresponding node from Denial of Service attacks by

malicious agents. But to make CN stateless, the BU will have to contain enough information so that accounting can be done for legitimate BUs which on the other hand may delay the communication process.

## 4.8 Time bound Binding Update

It is better to limit the binding entry lifetime to mitigate the attack based on the spoofed binding update, rather than complete stateless or stateful binding cache of CN. This approach may reduce the delay as it was in case of stateless protocol. As a result, binding entry is removed from the cache of the CN, if it is not refreshed after some time or any further BU is not received. Therefore, the attacker cannot perform replay attack and can't take advantage of the old binding entry when the MH is inactive for some time. But still refreshing binding cache again and again causes the wastage of bandwidth and network resources of the MH and the CN or HA, and sometimes in legitimate situations.

## 4.9 Summary

Numerous security solutions have been proposed and each has their advantages and disadvantages. Based on these solutions, some facts may be discussed that there are two main types of security are encryption and authentication. Encryption is of two types which are symmetric and asymmetric. Symmetric encryption uses a single key to encrypt and decrypt data and this is a fast algorithm to implement but it requires a PKI infrastructure for certification and so a lot of hardware. While Asymmetric key encryption uses two keys, one to encrypt the other to decrypt called the public and private keys. It uses RSA algorithm and if the key is intercepted, the attacker will only be able to encrypt data not decrypt it. But Asymmetric key cryptography is slow, more power consuming and resource intensive which may be a big problem for mobile environment. Thus it is better to use them after combining their features.

Authentication allows users to verify that they are communicating with validated participants. There are so many approaches available for authentication but these approaches use the central authentication database but in case of Mobile IPv6 environment, it is better to use distributed approach to speed up the communication

and to prevent a single point of attack. However, cryptographically generated addresses have the advantage that no trusted third parties are required.

IPSEC security can be implemented to provide security through tunnel.But there should be true relationship between the communicating nodes to implement key management through this mechanism. So we can ensure key management in between mobile node and its home agent, while not between mobile node and correspondent node. We can use IPSec tunnel mode to provide security between MN and HA. And to provide authentication, integrity, confidentiality of packets IPSec is used with AH protocol or ESP protocol or both.

Security protocols designed for the protection of binding updates has a drawback that they give away the location of the home agent, the mobile node and the correspondent. This is the basis for many of the possible attacks to these nodes. So a solution must be designed to make the location information private. However location privacy is achieved to some extent with the introduction of cryptographically generated addresses. This allows users to assert their ownership over an address preventing spoofing. And when this solution is combined with return routability, it becomes a secure solution. What is needed is a system can be developed that can fulfil the security needs of mobile IP’s vulnerabilities by existing infrastructure with low latency and with less power consuming resources.

# Chapter 5 Comparative Study and Proposed Solutions

## 5.1 Comparison for different Security Protocols

Security protocols discussed above focus security between MH and CN, MH and HA. Because MH and HA have true relationship, they use IPSec protocol security which provides them authentication of data origin, integrity of data, confidentiality of data using AH and ESP protocol in transparent mode or tunnel mode. While the security between MH and CN uses less complex protocol with less computation using one way hash function known as return routability protocol. To mitigate the different kind of attacks, there is a need of different approach, but there is a need a concrete less complex protocol which can mitigate all kind of attacks. Based on above discussed protocol, an analyses is made to security protocol whether they are able to mitigate different possible threats, this is shown in table given below.

In this table, major security threats and possible defense mechanism are compared. Table 1 lists the major security threats and corresponding defense mechanisms along with their advantages and disadvantages. Among the defense mechanisms of the mobility protocols, the IPSec protocols (AH and ESP) can be used for securing the tunnel between the MH and the HA as they have prior trust relationship. The CGA-based scheme can reduce the chance of attack on a victim node by authenticating the user's address with its public key and is also infrastructure less. The RR protocol is intended to authenticate the BU between the MH and the CN and confirm the reachability of mobile node through different routes. There is always a need for limiting the lifetime of binding entry to restrict the potential attack by unauthenticated binding updates sent by an attacker. At the last, MH or the CN should not store states until authentication to avoid CPU and memory exhaustion by DoS attacks.

Attack on binding updates between MH and HA can be protected by the use of IPSec ESP protocol. This protects against certain types of traffic analysis and provides privacy. However, use of ESP does not protect against misbehaving MH that may use spoofed CoA in BU to launch DoS attacks. Attack on binding updates between MH and CN can be prevented by the return routability of Mobile IPv6. This makes sure that the MH sending the BU has the right to use the CoA. However, vulnerabilities

possible if the attacker is on the path between HA and CN. Instead of this, vulnerability is also possible because of lack of location privacy. Traffic redirection attack can be prevented by IPSec AH protocol where the BUs are authenticated using this protocol though privacy and confidentiality are not ensured. This type of attaks can be mitigated if the victim node dynamically changes its IP address or uses CGA. Nodes with fixed IP addresses are more vulnerable to such attack. Man-in-the-middle attack can be prevented by IKE or PKI based schemes through strong mutual authentication. These approaches are difficult to break. However, it requires use of complex and expensive cryptographic operations in order to establish shared keys between the parties involved. Replay attack is usually countered by using sequence number or nonce index number.

**Table 5.1 Comparison of Different Mobile Security Protocol**

| **Security protocol** | **Threats mitigated** | **Advantage** | **Limitations** |
|---|---|---|---|
| IPSec protocol | Attack on BU, Home Agent Poisoning and all kind of threats | Authentication of data origin, Integrity and Confidentiality of data using AH and ESP, provides secure tunnel between MH and HA | Requires true relationship between nodes, so MH and CN can't use this protocol to authenticate BU. |
| CGA protocol | Spoofed BU, Traffic Redirection attack, Connection Hijacking | Public key is associated with IP address of MH | Do not check for CoA, so vulnerable to Bombing Attack |
| Ingress Filtering | Spoofed BU | Filter spoofed BU if applied attacker's network, reduces potential attackers | IPV6 uses CoA as sub option, so ingress filtering not effective |
| Stateless Mobile Nodes | Resource exhaustion, | Attacker have to send legitimate BU | Bandwidth wastage, Mobile |

| | | | |
|---|---|---|---|
| | Spoofed BU blocking legitimate BU, DoS attack by resource exhaustion | after some time again and again and can't take advantage of previous stored state | node have to keep information about legitimate BU. |
| Time Bound BU | Resource exhaustion, Spoofed BU blocking legitimate BU, DoS attack by resource exhaustion | Attacker can't take advantage of previous stored cache entry when MH is inactive for some time. | Bandwidth wastage, sometimes entry expires for legitimate user also. |
| Return Routability Protocol | Redirection Attack or Connection Hijacking Attack on BU (MH-CN), Replay Attack, Bombing Attack, Reflection and Amplication Attack. | Reduces the potential attackers, requires less computational algos, stateless CN, verify location of CoA. | Can't ensure security if attacker is on path between CN and HA, can't provide location privacy. |

The binding entry in the HA can be prevented by authenticating and protecting data between the MH and the HA through the use of IPSec protocol suites, such as AH or ESP protocol. This will provide strong protection mechanism at the expense of CPU power. To prevent the DoS attacks that can cause CPU and memory exhaustion, the MH or the CN can act as a stateless agent. Therefore, the MH or CN will not have to keep track of the current states of the half-open requests, thereby saving its resources. However, it might have to do more works for the valid requests and thus can increase processing delay. To mitigate the attack on the MH's radio access network, the MH may keep on trying to send BU message in spite of failures in several attempts. This will ensure the binding entry in the HA or the CN is corrupted by the attackers. However, this will impose additional overhead on the low-end mobile devices.

## 5.2 Mitigation of Vulnerability

Vulnerability in Return Routability protocol is due to the presence of an attacker in between the path of CN and HA, but this vulnerability can be mitigated if the home agents of both mobile nodes also have a secure tunnel between them. That is CN also has a secure tunnel with its HA and correspondent node's HA will communicate to the mobile node's HA. So in this case, CN should tunnel the HoT message through its own home agent. Thus it prevents the attacker to spoof the packets or BU at the correspondent node's local network and also correspondent network is also assumed to be secured (Note that IPSec tunneling can be used between nodes to router as well as router to router provided they have a true relationship). It is shown in Figure 5.1.

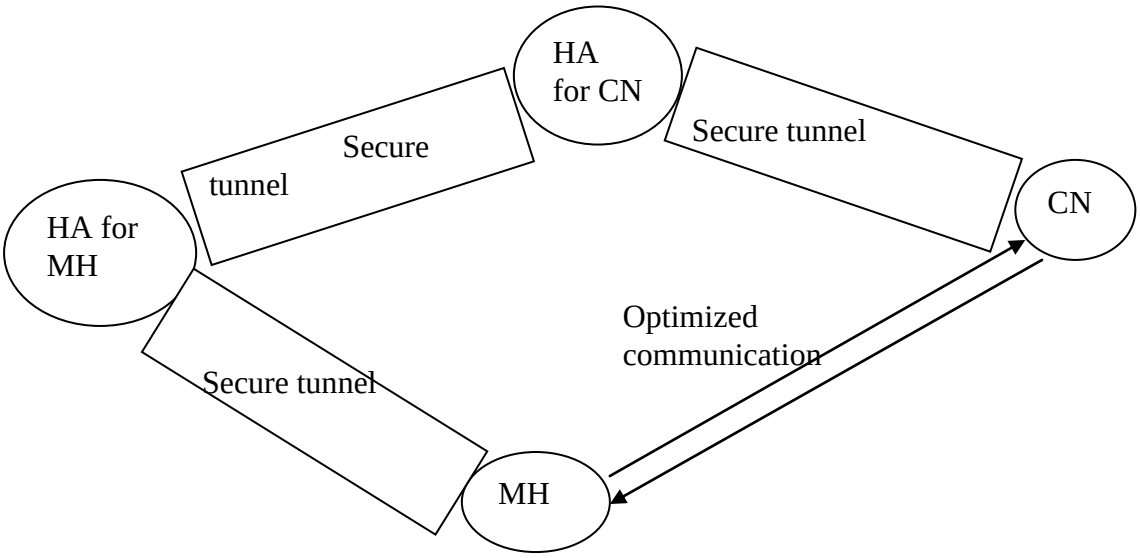


**Figure 5.1 RR protocol through secure tunneling on both sides**

But this is not a proper solution because it again creates a delay in communication and requires the infrastructure.

## 5.3 Protocol Design Considerations

To provide a security solution in route optimization technique requires the following main concerns:

1. Address of the user (MH) should not be spoofed.
2. The communicating device is present at the claimed IP address and again verifies spoofed address.
3. Device should be authenticated and can be identified in case of theft.

4. Location information of the communicating node should not be known to unauthorized user.

Most of vulnerabilities are a result of the attacker knowing location information of the communicating nodes. But how can you transmit your location data without giving your address information to another node. Possible logical solution would be to encrypt the data. But again to send encrypted data, a secret key must first be exchanged between the communicating nodes and to perform it, both of the communicating node must know each other's addresses. And so a loop is created and thinking goes towards authorized third party and key establishment without revealing the location of the communicating parties until they have been authenticated. Asymmetric cryptographic may be the best option should be chosen over symmetric, for the secure transmission of the binding update data, as it provides more security such as digital signatures to authenticate user data. But still there is a problem that asymmetric key cryptography is more processor consuming than symmetric key cryptography and so there is a need of light weight algorithm to reduce latency and fast response.

Use of Cryptographically Generated Addresses ensures that address of the user is owned by him or not spoofed since in this technique address of user is linked to the user's public key. Return Routability test can be used to verify that the communicating device is present at the claimed IP address. So combining these both techniques as Cryptographically Generated Addresses and Return Routability, may provide a strong and complimentary solution. Thus the proposed protocol would not require trusted third party and so expensive algorithms and certificates can be avoided in the environment where resources are the main concern. The proposed protocols are designed to keep in mind that the new technology should be compatible with the existing one means mobile IPv6 architecture should not be changed.

## 5.4 The Proposed Protocol

During the design of the proposed solution, we assume that every mobile node will be registered to a network provider, which in turn will provide the user with a home agent. And home agent will be the authenticated and secure point of contact when a

mobile device wishes to communicate with the mobile device as the home agent is constantly tracking and monitoring its current location. Instead of this current mobile system uses a sim card, which contains a sim number and the phone number. And the device also has an IMEI number, which is the hardware serial number. All of these are registered with the home agent through service provider. Thus all these information will be the basis for the new security solution.

### 5.4.1 Distributed Authentication Protocol

As previously discussed that the load of authentication messages can be distributed between nodes to reduce the latency problems and overcome the problem of more infrastructure. So for key exchange through cryptograhically generated address and verification of claimed IP through return routability test may be distributed and their messages can run parallel. Therefore in distributed authentication protocol there are three technologies are combined as:

1. Cryptographically Generated Addresses technique
2. Return Routability Test
3. Authentication verification process

The first two technologies are discussed in chapter 4 and are well-established techniques. The third has been modified specifically for the protection of binding updates. The third aspect is included for extra care of devices to provide device authentication and can be expanded to include user authentication in case of device theft.

Because adding more security may require more messages exchange and so to compensate this factor distributed authentication architecture is used which involve other nodes such as the Home Agent to aide with processing task. The Correspondent Node in case of return routability test requests authentication data from the Home Agent and the Mobile Node, so these two nodes should transfer messages in a secure manner to protect it from an attacker in between communication. The Home agent stores the data as a hash, which is unreadable by any attacker who would try to intercept it when transmitted. But the Mobile Node sends the data in plain text form so require some attention. So this plain text is encrypted with the binding key created

from the Return Routability stage. Correspondent node get both pieces of authentication data message, one from HA and another from MH, where both these information are compared, the encrypted data sent by MH is decrypted with same binding key as used in return routability and then the data is hashed received from HA, if both pieces of information matches the authentication process gets successful.

Each Mobile Nodes have the data such as its Care of Address, Sim No, IMEI, Phone No., is stored to its own Home Agent which is maintained by the Internet Service Provider. This provides a safe and secure authentication infrastructure without any one single point of attack. The Distributed Authentication Protocol provides a decentralized authentication approach in which there is no central authority. Even if a Home Agent is attacked by an attacker it will not affect anyone else using the system as each Mobile Node has its own Home Agent. The protocols are designed by considering the fact that either the mobile node MH is communicating to the mobile CN or a mobile node communicating with a static correspondent.

#### 5.4.1.1 Distributed Authentication in Mobile-to-Mobile Communication

At the very first, both the communicating nodes should be using cryptographically generated address, it means their IP address is linked with their public key which may be created as:

Host ID = HASH 64(public key)

The first 64 bits are the network prefix and are unchanged, however the last 64 bits of the address are now bound to the public key. The node now is the sole owner of this address and can be authenticated using public key signature of that node. Now protocol sends its first message:

**Message 1.**

When a mobile node MH moves to a new location, it attempts to make a connection to correspondent node CN. But initially MH does not know its current location so it begins the Return Routability procedure by signing its care of address CoA and home address HoA with private key MHK- as used in CGA and is sent with the Mobile Node's public key, MHK+, to correspondent home agent as HA2.

MH ⟶ HA2: MHK+, MHK-(CoA+HoA).

**Message 2.**

HA2 uses secure IPSEC protocol to forward the data to the correspondent node. Because IPSec protocol is a secure tunnel in which data is encapsulated by adding another packet header to the data with the destination address of the Corresponding node.

HA2 ⟶ CN: MHK+, MHK-(CoA, HoA).

**Message 3.**

The CN uses the public key MHK+ to decrypt the message received from home agent containing CoA and HoA addresses which is responsible to authenticate user. The CN then compares the mobile node's public key MHK+ by hashing it, with that of its claimed CGA address' least significant 64-bit, if after comparing they both match then Return Routability and device authentication will proceed, otherwise the request will be dropped.

In the next step CN will perform the reachability for home address and the care of address. The correspondent node will send a home test (HoT) packet to the home agent of MH, and HA will tunnel it to the mobile node. The HoT packet consists of a home keygen token generated by hashing the secret key Kcn only known to the correspondent as it was discussed in return routability test. A nonce index $N_H$ is also included as in return routability to allow the CN to find the freshness of packet. The nonces are randomly generated bit strings that are changed periodically. This is then sent to the home agent of MH.

Home keygen token K1 = hash ( Kcn | source address | 0 )

CN ⟶ HA: HoT(K1+ $N_H$).

**Message 4.**

The Home Test packet HoT is then forwarded to the mobile node's care of address .

HA ⟶ MH: HoT(K1+ $N_H$).

**Message 5.**

The CN node also performs a care of address test (CoT) at the same time as message 3, which is similar to the home address test, however now the token generated is

slightly different. The nonce of the Care-of token is $N_C$ which is different from $N_H$. CoT is then sent directly to the mobile node.

Care-of keygen token K2 = hash ( Kcn | source address | 1 )

CN ⟶ MH: CoT(K2+ $N_C$).

**Message 6.**

The mobile node MH receives both HoT and CoT tokens from both the test packets sent. It then creates a binding key Kbm by hashing the two tokens together.

Kbm = hash ( home token HoT | care-of token CoT )

This key is used now as symmetric key of communication between these two nodes. The mobile node MH then sends a binding update request using this binding symmetric key Kbm to the correspondent node. Only node who know Kbm is Correspondent node CN because it also have both tokens.

MH ⟶ HA2: Kbm(BU)

**Message 7.**

MH still sends the binding messages to HA2, not directly to CN because still message exchange is not fully authenticated. After receiving BU message, HA2 forwards the packet to the correspondent node CN using sufficient security.

HA2 ⟶ CN: Kbm(BU)

**Message 8.**

The correspondent node CN would now decrypt the data using binding key Kbm and accept the binding update, after completing distributed authentication protocol. This is to avoid possible denial of service attacks with repeated decryption requests. Because this authentication takes place parallel with return routability message exchange and can be checked at home agent also. Now CN sends a request message for authentication data (RAD) of mobile node.

CN ⟶ MH: RAD

**Message 9.**

MH sends its authentication data to CN via HA2 using binding key Kbm, which includes its current address, its sim number, IMEI number, phone number.

MH ⟶ HA2: Kbm(CoA, Sim No, IMEI, Phone No., Timestamp)

**Message 10.**

HA2 ⟶ CN: Kbm(CoA, Sim No, IMEI, Phone No., Timestamp)

**Message 11.**

Simultaneously to message 8, CN sends a request for authentication data message to the home agent to verify the information got from MH.

CN ⟶ HA: RAD

**Message 12.**

But the home agent HA does not have the binding key so it hashes the authentication data to send it to CN.

HA ⟶ HA2: Hash(CoA, Sim No, IMEI, Phone No., Timestamp)

**Message 13.**

HA2⟶ CN: Hash(CoA, Sim No, IMEI, Phone No., Timestamp)

**Message 14.**

Now CN has both the authentication data encrypted with the binding key from MH and the hash of the authentication data from HA. There are now two options, whether nodes want to distribute the load or not as:

1. CN may perform the authentication comparison process by decrypting the binding key and hashing the authentication data received from the mobile node and then comparing this to the hash received by the home agent. Go to Message 16.
2. But if CN is overwhelmed it may send the hash and the decrypted authentication data to the correspondents home agent via a secure tunnel where it will perform the comparison.

CN ⟶ HA2: (Hash(CoA, Sim No, IMEI, Phone No., Timestamp), (CoA, Sim No, IMEI, Phone No., Timestamp))

**Message 15.**

The HA2 after getting data from CN hashes the authentication data and compares it to the sent hash. If both of these match then the authentication is successful and an authorization successful message is sent to CN.

HA2 ⟶ CN: AOK

**Message 16.**

If the authentication is successful, then the BU received in message 7, Kbm(BU) is decrypted using the shared key Kbm as the protocol uses symmetric key cryptography. The binding update is accepted and a binding acknowledgement BA is sent to achieve the route optimization between MH and CN.

CN ⟶ MH: BA

Now of course fewer messages will be needed as the mobile node can now communicate directly with the correspondent. All messages shown in Figure 5.2

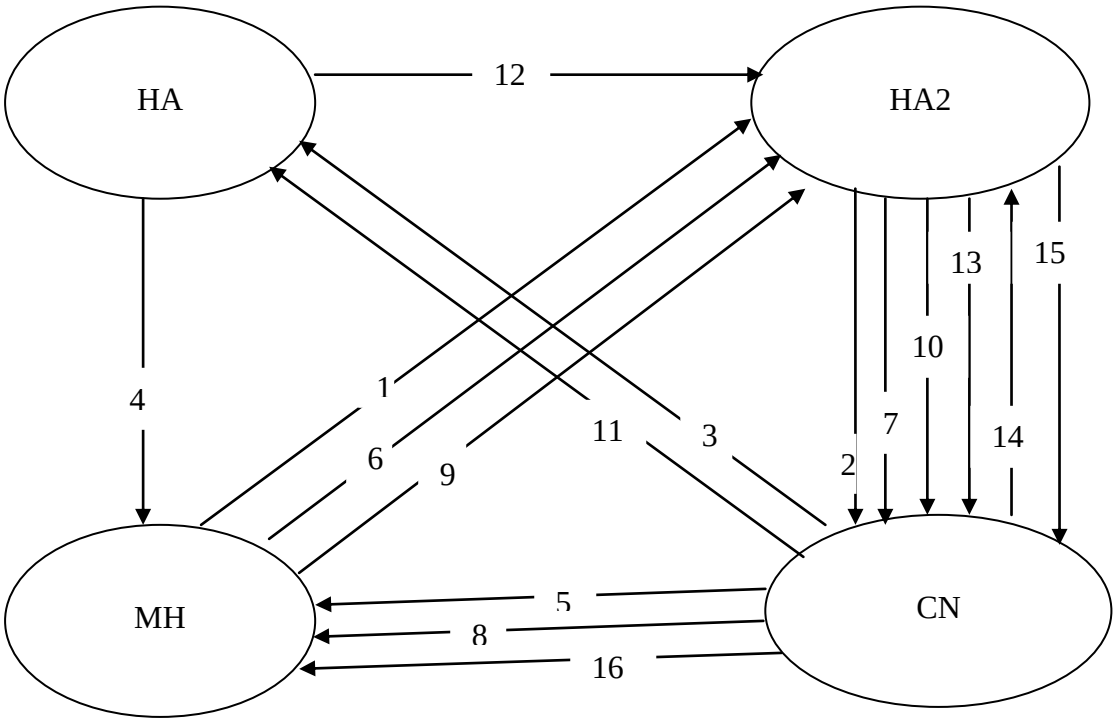


**Figure 5.2 Distributed Authentication in Mobile-to-Mobile communication**

### 5.4.1.2 Distributed Authentication in Mobile-to-Static Communication

The basic principle is same as the mobile-to-mobile communication however in this case, correspondent is static and it does not have a home agent and so cannot perform distributed authentication. But that will not create a problem because correspondent node is static and it is assumed CN may have more processing power to deal with communication messages and so distributed authentication would be unnecessary. All

the messages will go through the same scenario but in this case messages will not pass via the correspondent's home agent. All messages can be seen in Figure 5.3.

**Message 1.**

When a mobile node MH moves to a new location, it attempts to make a connection to correspondent node CN. Initially MH begins the Return Routability procedure by contacting with the correspondent node. The mobile node signs its care of address CoA and home address HoA with private key MHK- as used in CGA and is sent with the Mobile Node's public key, MHK+, to CN.

MH ⟶ CN: MHK+, MHK-(CoA+HoA).

**Message 2.**

The CN uses the public key MHK+ to decrypt the message received from home agent containing CoA and HoA addresses which is responsible to authenticate user. The CN then compares the mobile node's public key MHK+ by hashing it, with that of its claimed CGA address' least significant 64-bit, if after comparing they both match then Return Routability and device authentication will proceed, otherwise the request will be dropped.

In the next step CN will perform the reachability for home address and the care of address. The correspondent node will send a home test (HoT) packet to the home agent of MH, and HA will tunnel it to the mobile node. The HoT packet consists of a home keygen token generated by hashing the secret key Kcn only known to the correspondent as it was discussed in return routability test. A nonce index $N_H$ is also included as in return routability to allow the CN to find the freshness of packet. The nonces are randomly generated bit strings that are changed periodically. This is then sent to the home agent of MH.

Home keygen token K1 = hash ( Kcn | source address | 0 )

CN ⟶ HA: HoT(K1+ $N_H$).

**Message 3.**

The Home Test packet HoT is then forwarded to the mobile node's care of address.

HA ⟶ MH: HoT(K1+ $N_H$).

**Message 4.**

The CN node also performs a care of address test (CoT) at the same time as message 2, which is similar to the home address test, however now the token generated is slightly different. The nonce of the Care-of token is $N_C$ which is different from $N_H$. CoT is then sent directly to the mobile node.

Care-of keygen token K2 = hash ( Kcn | source address | 1 )

CN ⟶ MH: CoT(K2+ $N_C$).

**Message 5.**

The mobile node MH receives both HoT and CoT tokens from both the test packets sent. It then creates a binding key Kbm by hashing the two tokens together.

Kbm = hash ( home token HoT | care-of token CoT )

This key is used now as symmetric key of communication between these two nodes. The mobile node MH then sends a binding update request to the correspondent node, which is protected with the binding key Kbm. As the Correspondent node CN also have both tokens, so it is the only node capable of decrypting the binding update.

MH ⟶ CN: Kbm(BU)

**Message 6.**

The correspondent node CN would now decrypt the data using binding key Kbm and accept the binding update, after completing distributed authentication protocol. This is to avoid possible denial of service attacks with repeated decryption requests. Because this authentication takes place parallel with return routability message exchange and can be checked at home agent also. Now CN sends a request message for authentication data (RAD) of mobile node.

CN ⟶ MH: RAD

**Message 7.**

MH sends its authentication data to CN using binding key Kbm, which includes its current address, its sim number, IMEI number, phone number.

MH ⟶ CN: Kbm(CoA, Sim No, IMEI, Phone No., Timestamp)

**Message 8.**

Simultaneously to message 6, CN sends a request for authentication data message to the home agent to verify the information got from MH.

CN ⟶ HA: RAD

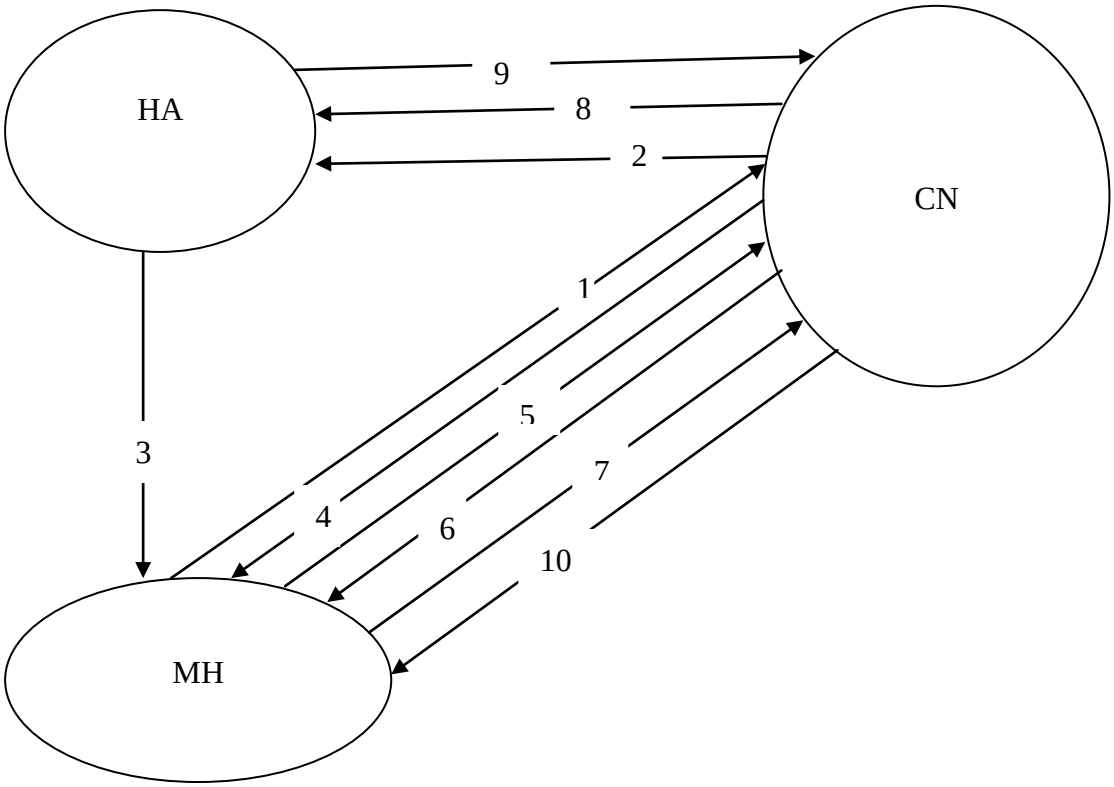


**Figure 5.3 Authentications in Mobile-to-Static Communication**

**Message 9.**

But the home agent HA does not have the binding key so it is very risky to send authentication data as such, instead of this, the home agent hashes the authentication data together and sends that to the correspondent.

HA ⟶ CN: Hash(CoA, Sim No, IMEI, Phone No., Timestamp)

**Message 10.**

Now CN will have both the authentication data encrypted with the binding key from MH and the hash of the authentication data from HA. The correspondent performs the authentication comparison by decrypting the binding key and hashing the authentication data received from the mobile node then comparing this to the hash received by the home agent.

If the result of the authentication is successful then the BU received in message 5, Kbm(BU) is decrypted using the shared key Kbm as the protocol uses symmetric key cryptography only known to the Mobile and Correspondent Nodes. The binding update is accepted and a binding acknowledgement BA is sent to the mobile node allowing it to communicate directly with the correspondent.

CN ⟶ MH: BA

#### 5.4.1.3 Summary

The protocol is mainly made up of three components. Cryptographically Generated addresses, to assert ownership of the IP address the node claims to reside on. Return Routability, a solution to determine the node is at the location it claims to be and is reachable. Both these solutions currently exist. The third element proves the owner of the node is authorized to communicate across the network using a distributed authentication mechanism where authentication data from the ISP is compared to that stored on the home agent and mobile node which provides low resource consumption solution. The advantages of using a distributed authentication protocol is that processing speed is increased concerning the completion of security techniques which at the same time not over burdening the mobile processor with all the work. But there is a advantage that network traffic is increased but still optimization may reduce this.

### 5.4.2 Mobile Home Agents

Till now thesis work has discussed two methods of communication between the mobile and correspondent node in Mobile IPv6 environment. The first method is triangle routing, in which all communication to the mobile node is via the home agent. Because the home agent' IP address is static and first point of contact and all traffic passed by it through the secure tunnel so it is a safe communication. But the disadvantage here is that when a mobile node travels from the home agent to a new location, further data packets will have to travel to reach their destination. The second method is the use of a route optimization technique, which allows direct communication between the mobile node and correspondent node. This can be achieved with the use of authenticated binding updates. But here is also a disadvantage that the current location of the mobile node is revealed to any correspondent in communication with it, which could be a potential security risk. So

this section introduces an alternative method, which provides the best of both solutions without the disadvantages.

#### 5.4.2.1 Mobile Agents Technology Introduced in to Mobile IPv6

Mobile agents are software programs which are embedded at point of attachment for mobile node. Thus mobile agents act as a proxy between the mobile node and the correspondent node. The mobile agent is a piece of software responsible for routing messages from other nodes to the mobile node without change in hardware and at the same time provide location privacy by acting as a proxy and masking the true IP address of the mobile node. As this mobile agent produces again a triangle routing but there is negligible latency. And this software of mobile agent act just like a home agent so it is called as a mobile home agent. As this software moves as mobile nodes' point of attachment changes, and will further handle all the communication responsible for that mobile node. However the mobile home agent would not lose communication with the mobile node as the software is autonomous and capable of duplicating itself to the new point of attachment and resuming its role in the network. The beauty of this approach is that to the Correspondent, the Mobile Home Agent (MHA) will seem to be as Mobile Node, as it changes its IP address with every new location and sends a binding update to the Correspondent.

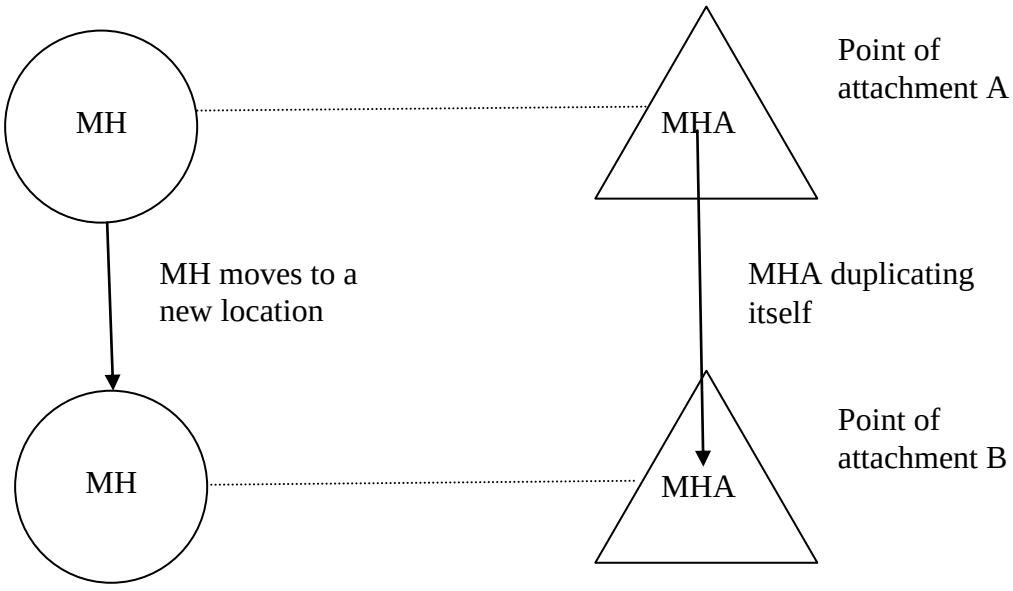


**Figure 5.4Mobile Home Agent Duplication as MH Migrates**

So location privacy is achieved even if mobile nodes move from one location to another along with the advantages of low latency solution using the mobile home agents. This is shown in Figure 5.4

**5.4.2.2 Mobile Home Agent used in a Mobile-to-Mobile Communication.**

At the very first, both the communicating nodes should be using cryptographically generated address, it means their IP address is linked with their public key which may be created as:

Host ID = HASH 64(public key)

The first 64 bits are the network prefix and are unchanged, however the last 64 bits of the address are now bound to the public key. The node now is the sole owner of this address and can be authenticated using public key signature of that node. Now protocol sends its first message:

**Message 1.**

When a mobile node MH moves to a new location, it attempts to make a connection to correspondent node CN. But initially MH does not know its current location so it begins the Return Routability procedure by signing its care of address CoA and home address HoA with private key MHK- as used in CGA and is sent with the Mobile Node's public key, MHK+, to correspondent home agent as HA2.

MH ⟶ HA2: MHAK+, MHAK-(MHA+HoA).

**Message 2.**

HA2 uses secure IPSEC protocol to forward the data to the correspondent node. Because IPSec protocol is a secure tunnel in which data is encapsulated by adding another packet header to the data with the destination address of the Corresponding node.

HA2 ⟶ CN: MHAK+, MHAK-(MHA, HoA).

**Message 3.**

The CN uses the public key MHK+ to decrypt the message received from home agent containing CoA and HoA addresses which is responsible to authenticate user. The CN then compares the mobile node's public key MHK+ by hashing it, with that of its

claimed CGA address' least significant 64-bit, if after comparing they both match then Return Routability and device authentication will proceed, otherwise the request will be dropped.

In the next step CN will perform the reachability for home address and the care of address. The correspondent node will send a home test (HoT) packet to the home agent of MH, and HA will tunnel it to the mobile node. The HoT packet consists of a home keygen token generated by hashing the secret key Kcn only known to the correspondent as it was discussed in return routability test. A nonce index $N_H$ is also included as in return routability to allow the CN to find the freshness of packet. The nonces are randomly generated bit strings that are changed periodically. This is then sent to the home agent of MH.

Home keygen token K1 = hash ( Kcn | source address | 0 )

CN ⟶ HA: HoT(K1+ $N_H$).

**Message 4.**

The Home Test packet HoT is then forwarded to the mobile node's care of address directly because a secure tunnel is assumed between mobile node and home agent, so no need to send this message to MHA .

HA ⟶ MH: HoT(K1+ $N_H$).

**Message 5.**

The CN node also performs a care of address test (CoT) at the same time as message 3, which is similar to the home address test, however now the token generated is slightly different. The nonce of the Care-of token is $N_C$ which is different from $N_H$. CoT is then sent directly to the mobile node as correspondent thinks, but in fact, CoT is sent to MHA.

Care-of keygen token K2 = hash ( Kcn | source address | 1 )

CN ⟶ MHA: CoT(K2+ $N_C$).

**Message 6.**

Mobile home agent tunnels the CoT message to MH.

MHA ⟶ MH:CoT(K2+$N_C$)

**Message 7.**

The mobile node MH receives both HoT and CoT tokens from both the test packets sent. It then creates a binding key Kbm by hashing the two tokens together.

Kbm = hash ( home token HoT | care-of token CoT )

This key is used now as symmetric key of communication between these two nodes. The mobile node MH then sends a binding update request using this binding symmetric key Kbm to the correspondent node. Only node who know Kbm is Correspondent node CN because it also have both tokens.

MH ⟶ HA2: Kbm(BU)

**Message 8.**

MH still sends the binding messages to HA2, not directly to CN because both nodes are mobile and the MH would have to accept a binding update from the correspondent before being able to communicate directly. After receiving BU message, HA2 forwards the packet to the correspondent node CN.

HA2 ⟶ CN: Kbm(BU)

**Message 9.**

The correspondent node CN would now decrypt the data using binding key Kbm and accept the binding update, after completing distributed authentication protocol. This is to avoid possible denial of service attacks with repeated decryption requests. Because this authentication takes place parallel with return routability message exchange and can be checked at home agent also. Now CN sends a request message for authentication data (RAD) of mobile node to MHA.

CN ⟶ MHA: RAD

**Message 10.**

Mobile home agent tunnels the data authenticate request to MH.

MHA⟶MH:RAD

**Message 11.**

MH sends its authentication data to CN via HA2 using binding key Kbm, which includes its current address, its sim number, IMEI number, phone number.

MH ⟶ HA2: Kbm(CoA, Sim No, IMEI, Phone No., Timestamp)

**Message 12.**

HA2 ⟶ CN: Kbm(CoA, Sim No, IMEI, Phone No., Timestamp)

**Message 13.**

Simultaneously to message 9, CN sends a request for authentication data message to the home agent to verify the information got from MH.

CN ⟶ HA: RAD

**Message 14.**

But the home agent HA does not have the binding key so it is very risky to send authentication data as such, instead of this, the home agent hashes the authentication data together and sends that to the correspondent.

HA ⟶ HA2: Hash(CoA, Sim No, IMEI, Phone No., Timestamp)

**Message 15.**

HA2⟶ CN: Hash(CoA, Sim No, IMEI, Phone No., Timestamp)

**Message 16.**

Now CN will have both the authentication data encrypted with the binding key from MH and the hash of the authentication data from HA. The correspondent performs the authentication comparison by decrypting the binding key and hashing the authentication data received from the mobile node then comparing this to the hash received by the home agent. But If the correspondent node is overwhelmed by the current processing constraints it may opt to send the hash and the decrypted authentication data to the correspondents home agent via a secure tunnel where it will perform the comparison. (Notice the key is not sent as this would be a security vulnerability. The decryption is done by the CN.) but here by taking first option, If the result of the authentication is successful then the BU received as Kbm(BU) is decrypted using the shared key Kbm as the protocol uses symmetric key cryptography only known to the Mobile and Correspondent Nodes. The binding update is accepted and a binding acknowledgement BA is sent to the mobile node allowing it to communicate directly with the correspondent.

CN ⟶ MHA:BA

**Message 17.**

The mobile home agent MHA passes the binding acknowledgement to the mobile node to let it know that the process has been successful.

MHA ⟶ MH: BA

Now the above message exchange communication also has their location privacy by implementing mobile home agent at the point of attachment of mobile node. Correspondent node communicates directly with the mobile nodes through mobile home agent, acting as a secure proxy with negligible communication latency. The whole of the communication is shown in the Figure 5.5.

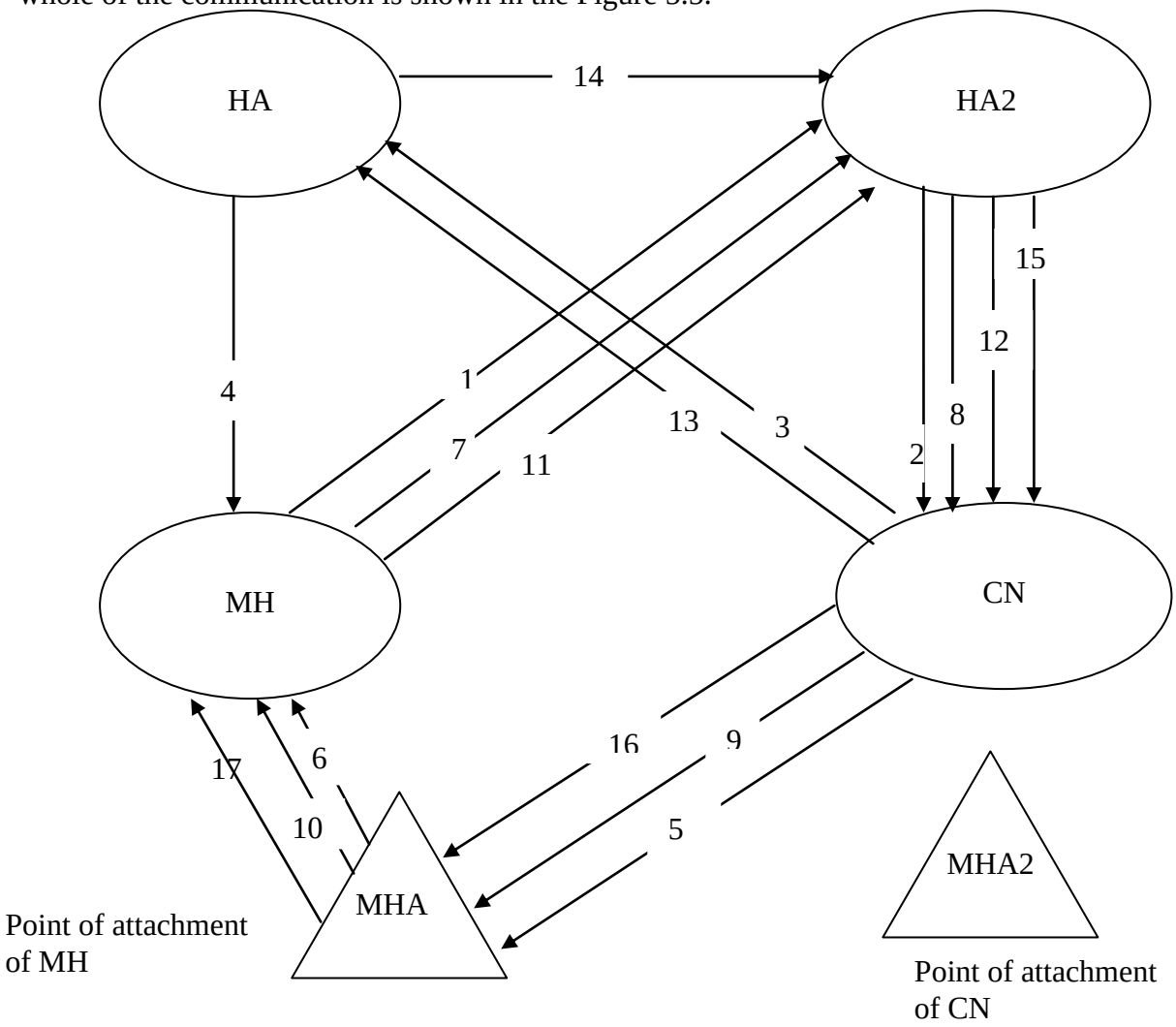


**Figure 5.5 Mobile Home Agent message exchange in mobile-to-mobile comm$^{n}$.**

Once the protocol has completed all type of authentication, whether it is data authentication, user's authentication and binding update authentication, of the mobile and correspondent nodes then direct route optimized communication can take place

between the communicating nodes via the Mobile Home Agents on the points of attachment shown in Figure 5.6. The extra burden due to the mobile agent software not running on the mobile device itself but running on the points of attachment is negligible and this provides low latency communication with the benefit of a non processor intensive location privacy security solution.

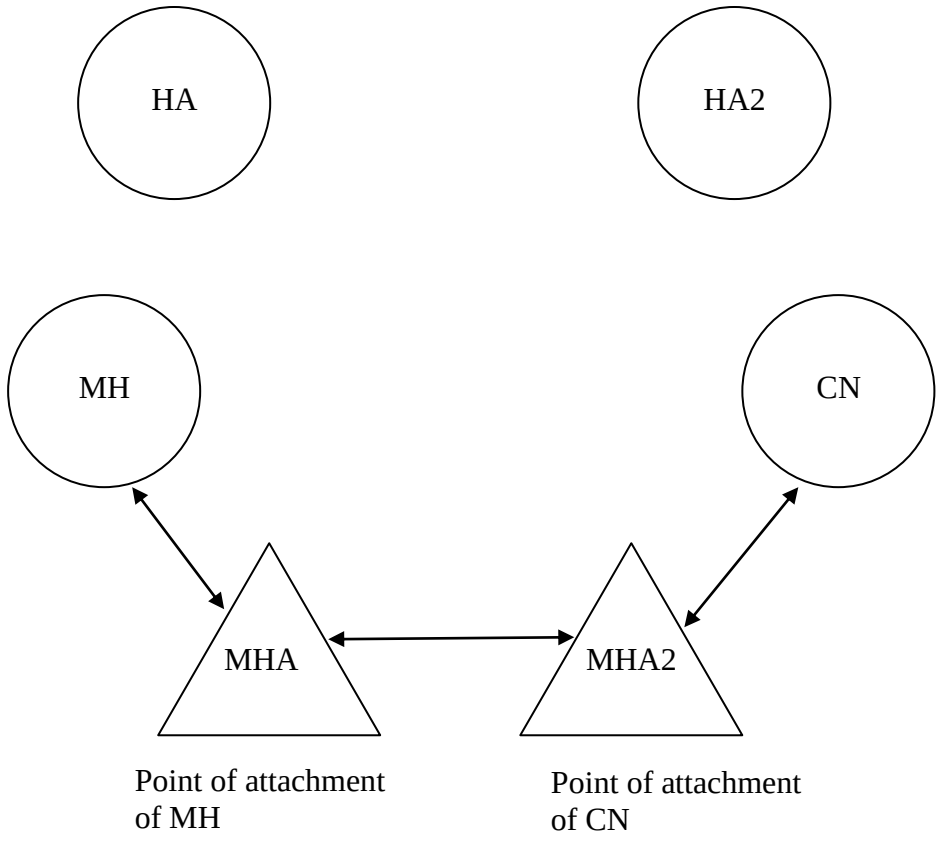


**Figure 5.6 Mobile nodes comm$^{n}$ via mobile home agents on points of Attachment**

### 5.4.2.3 Mobile Home Agent used in a Mobile-to-Static Communication.

Mobile home agent has increased the speed of node communication by protecting the identity of the mobile nodes' current location. The basic principle is same as the mobile-to-mobile communication however in this case, correspondent is static and it does not have a home agent and so cannot perform distributed authentication. But that will not create a problem because correspondent node is static and it is assumed CN may have more processing power to deal with communication messages and so distributed authentication would be unnecessary. All the messages will go through the same scenario but in this case messages will not pass via the correspondent's home agent. All messages can be seen in Figure 5.7. At the very first, both the

communicating nodes should be using cryptographically generated address, it means their IP address is linked with their public key which may be created as:

Host ID = HASH 64(public key)

A cryptographic hash function is applied on the public key, called the Host ID, and this is used as the interface identifier part of the Mobile IPv6 address. The first 64 bits are the network prefix and are unchanged, however the last 64 bits of the address are now bound to the public key. The node now can claim ownership of the address by reversing the procedure, which can be done with a conventional public key signature. Now protocol sends its first message:

**Message 1.**

When a mobile node MH moves to a new location, it attempts to make a connection to correspondent node CN. Because CN is a static node, so it begins the Return Routability procedure by contacting with the correspondent node CN directly. The mobile node signs its care of address and home address with private key MHK- as used in CGA and is sent with the Mobile Node's public key, MHK+, to CN. But now the CoA address of MH node is not the current location address of MH, while it is the proxy address of mobile home agent (MHA). It is done to provide location privacy.

MH ⟶ CN: MHAK+, MHAK-(MHA+HoA).

**Message 2.**

The CN now uses the public key MHAK+ to decrypt the message containing MHA and HoA addresses which proves that the sender is the only one who can encrypt and sign the messages. The CN then compares the mobile node's public key MHAK+ with that of its claimed CGA address, MHA, and determines if they match. This is computed by hashing the public key of the Mobile Node and comparing it with least significant 64- bit of the interface identifier of the Mobile Nodes' claimed address. If they match then address ownership has been proven. If after comparing they both match then Return Routability and device authentication will proceed, otherwise the binding update request is denied. In this case public key and claimed CGA address will be of MHA.

In the next step CN will perform the reachability for home address and the care of address. The correspondent node will send a home test (HoT) packet to the home agent of MH, and HA will tunnel it to the mobile node. The HoT packet consists of a home keygen token generated by hashing the secret key Kcn only known to the correspondent as it was discussed in return routability test. A nonce index $N_H$ is also included as in return routability to allow the CN to find the freshness of packet. The nonces are randomly generated bit strings that are changed periodically. This is then sent to the home agent of MH.

Home keygen token K1 = hash ( Kcn | source address | 0 )

CN ⟶ HA: HoT(K1+ $N_H$).

**Message 3.**

The Home Test packet HoT is then forwarded to the mobile node's care of address directly because a secure tunnel is assumed between mobile node and home agent, so no need to send this message to MHA .

HA ⟶ MH: HoT(K1+ $N_H$).

**Message 4.**

The CN node also performs a care of address test (CoT) at the same time as message 2, which is similar to the home address test, however now the token generated is slightly different. The nonce of the Care-of token is $N_C$ which is different from $N_H$. CoT is then sent directly to the mobile node as correspondent thinks, but in fact, CoT is sent to MHA.

Care-of keygen token K2 = hash( Kcn | source address | 1 )

CN ⟶ MHA: CoT(K2+ $N_C$).

**Message 5.**

Mobile home agent tunnels the CoT message to MH.

MHA ⟶ MH: CoT(K2+$N_C$)

**Message 6.**

The mobile node MH receives both HoT and CoT tokens from both the test packets sent. It then creates a binding key Kbm by hashing the two tokens together.

Kbm = hash ( home token HoT | care-of token CoT )

This key is used now as symmetric key of communication between these two nodes. The mobile node MH then sends a binding update request to the correspondent node, which is protected with the binding key Kbm. As the Correspondent node CN also have both tokens, so it is the only node capable of decrypting the binding update.

MH ⟶ CN: Kbm(BU)

**Message 7.**

The correspondent node CN would decrypt the data using binding key and accept the binding update, however before this begins it must wait for the result of the distributed authentication protocol to complete. This is to avoid possible denial of service attacks with repeated decryption requests. This authentication takes place simultaneously with return routability. Now CN sends a request message to the mobile node for its authentication data (RAD).

CN ⟶ MHA: RAD

**Message 8.**

Mobile home agent tunnels the data authenticate request to MH.

MHA⟶MH: RAD

**Message 9.**

MH sends its authentication data, which includes its current address, its sim number, IMEI number, phone number. This is sent to the CN encrypted with the binding key Kbm.

MH ⟶ CN: Kbm(CoA, Sim No, IMEI, Phone No., Timestamp)

**Message 10.**

Simultaneously to message 7, CN sends a request for authentication data message to the home agent to verify the information got from MH.

CN ⟶ HA: RAD

**Message 11.**

But the home agent HA does not have the binding key so it is very risky to send authentication data as such, instead of this, the home agent hashes the authentication data together and sends that to the correspondent.

HA ⟶ CN: Hash(CoA, Sim No, IMEI, Phone No., Timestamp)

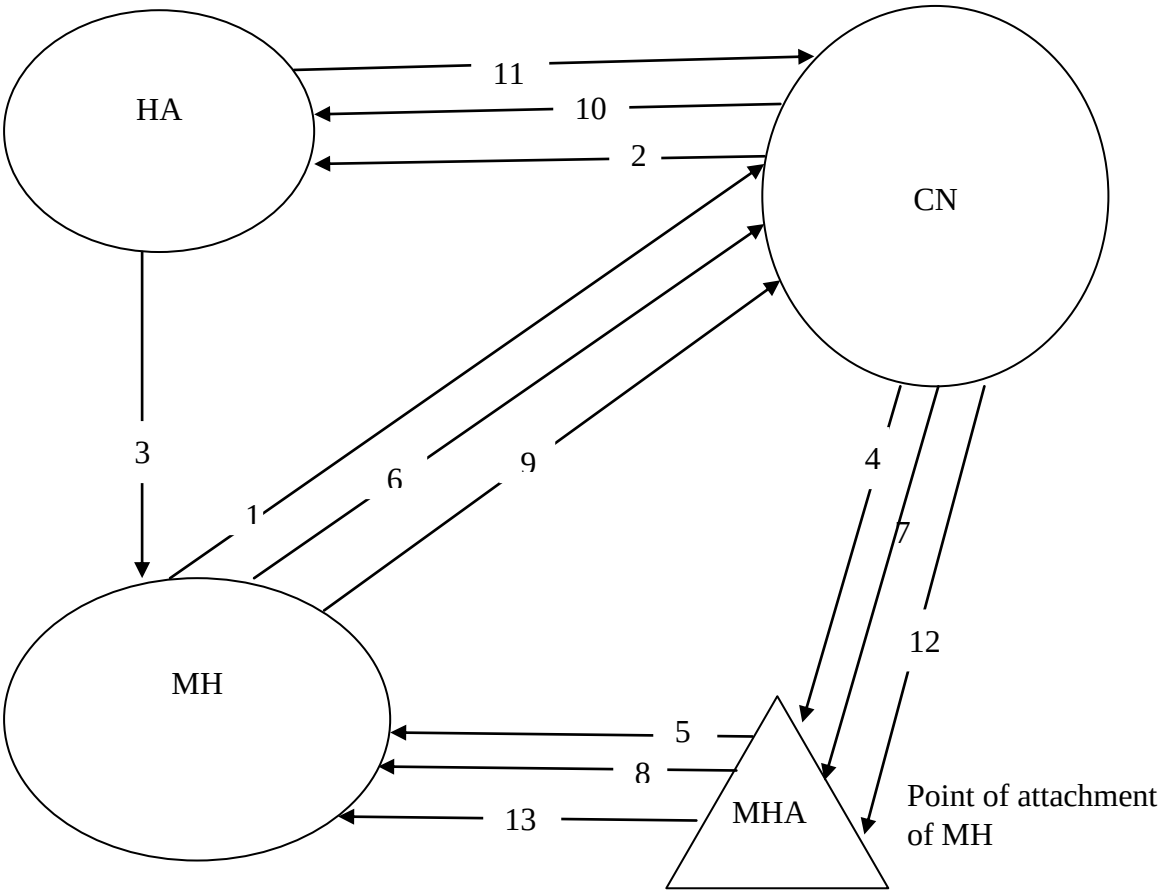


**Figure 5.7 Mobile Home Agent message exchange in mobile-to-static comm$^{n}$.**

**Message 12.**

Now CN will have both the authentication data encrypted with the binding key from MH and the hash of the authentication data from HA. The correspondent performs the authentication comparison by decrypting the binding key and hashing the authentication data received from the mobile node then comparing this to the hash received by the home agent. If the result of the authentication is successful then the BU received as Kbm(BU) is decrypted using the shared key Kbm as the protocol uses symmetric key cryptography only known to the Mobile and Correspondent Nodes. The binding update is accepted and a binding acknowledgement BA is sent to the mobile node allowing it to communicate directly with the correspondent.

CN ⟶ MHA: BA

**Message 13.**

The mobile home agent MHA passes the binding acknowledgement to the mobile node to let it know that the process has been successful.

MHA ⟶ MN: BA

Now the above message exchange communication also has their location privacy by implementing mobile home agent at the point of attachment of mobile node. Correspondent node communicates directly with the mobile nodes through mobile home agent, acting as a secure proxy with negligible communication latency. The whole of the communication is shown in the Figure 5.7

### 5.4.2.4 Summary

From above chapters it was shown that the Mobile IPv6 route optimization protocol is vulnerable to a variety of attacks which are possible because of breach in location privacy. Several security solutions were investigated which were specifically designed to protect location privacy. But there was always a problem of infrastructure and latency increment between communication of the mobile node and the correspondent. So a second technology, mobile agents, were investigated which are autonomous software based programs and this technology potentially changes the way networks operate. The beauty of this software is that they work well in heterogeneous networks and are capable of managing network messages.

Mobile home agents act as a proxy home agent which follows the mobile node as it moves from point of attachment to point of attachment. Even though now the solution is following the concept of triangular routing but in reality there is negligible latency increase because the mobile home agent resides on the point of attachment itself and the data packet would have to pass via the point of attachment anyway to reach the mobile node.

In this way, the mobile home agent provides location privacy by acting as a proxy for mobile nodes and passing all messages to the mobile node via a secure tunnel. When the mobile node moves to a new location and so to a new point of attachment the

mobile home agent duplicates itself and is transmitted to the new point of attachment and there it continues to act as the proxy for the mobile node. The home agent for a mobile node has to keep track of both of these entities to ensure they are reachable.

Thus the proposed solution has a advantage that mobile home agent are software based solution so new change in infrastructure hardware making it a very cost effective option. In spite of this, the location privacy for a mobile node is achieved with negligible increase in latency. The proposed solution has only disadvantage that the mobile home agent is autonomous and so its behavior relies heavily on its robust programming and that every point of attachment may have to be modified to accept mobile agents.

# Chapter 6 Conclusions

## 6.1 Conclusions

Today wireless communication technologies have become a part of life. Several improvements have been seen with jump from 2G to 3G in terms of security. Yet security issues persist and will continue to 4G technology also if not addressed. Because 4G require a fast response, so IPv6 will feature many advantages, however security is still a fundamental issue to be resolved. One major security issue involves the route optimization (RO) technique, which deals with binding updates. This allows the corresponding node to communicate directly with the mobile node by passing the home agent router. Before route optimization, binding updates are exchanged between mobile node, home agent and correspondent node which causes a variety of security vulnerabilities. Binding updates include the interception of data packets, which would allow an attacker to eavesdrop on its contents or to modify transmitted packets for the attacker's own malicious purposes. There are other possible vulnerabilities with mobile IP like address spoofing, IP redirection and denial of service attacks. But to perform these attacks, all the attacker needs to know is the IPv6 addresses of the mobile's home agent and the corresponding node.

To prevent these attacks two of the main solutions are cryptography and authentication. Cryptography allows the transmitted data to be in encrypted form resulting in non-readable form of the intercepted packets. Only the authorized party possessing keys will be able to decrypt the message. Encryption provides the confidentiality of the data and can be done in two ways, symmetric and asymmetric. Symmetric key cryptography is useful for low powered devices and participants use the same key to encrypt and decrypt. The main problem is PKI infrastructure and without it, how the keys will be distributed. Asymmetric key cryptography has two types of keys as encryption and decryption keys. This is useful for the distribution of the keys and can help with authentication with the use of digital signatures. The drawback however is that processing consumption is higher than symmetric cryptography. Second solution is authentication to verify the identity of the user or device one is in communication with. The components implementing authentication will include techniques such as hashes, digital signatures, address based keys and

cryptographically generated addresses. There are different authentication schemes exist however many of them rely on a certification authority and consumes resources. So decentralized authentication mechanisms would be more appropriate for the nature of mobile IP.

A solution must be developed that allows for the crucial location information to be transmitted and yet the nodes retain their location privacy. However location privacy is achieved with the introduction of cryptographically generated addresses. This allows users to assert their ownership over an address preventing spoofing. This combined with return routability may provide secure solution.

What is needed is a system that can fulfil the security needs of mobile IP's vulnerabilities by using a combination of the security technologies available, which operate without over taxing the computing resources available and package them into an easy to implement solution. It has been design to work within the existing infrastructure without modifying the standard architecture. The combined use of Cryptographically Generated Addresses and Return Routability provides address ownership and reachability validation.

However the lack of authentication has been resolved with the introduction of the Distributed Authentication Protocol and Mobile Home Agent technologies, which provides a low cost solution with benefits under processor intensive situations. The fact that the protocol has not modified the standards of Mobile IPv6 means that it will be compatible with future implementations with little to no modification necessary. The only drawback of the protocol are the increase in network messages however the user can choose if they require the distributed feature of the solution and choose not to use it under certain circumstances.

## 6.2 Addressed Research Questions

**Can a security solution be developed for binding updates security without changing existing infrastructure?**

Distributed Authentication Protocol was created to address this question. The use of a Home Agent to store the hash of the Mobile Nodes identification data allows authentication to take place in a distributed manner without the need for a central authentication authority. Home agent is a reliable one because it is provided by the Internet Service Providing Company. The use of hashed data means the solution can operate with very low processing requirements and does not requires extra key exchange between Home Agent and Correspondent Node.

**Can an existing security solution be improved to make it less vulnerable to certain types of attack?**

Combination of CGA with Return Routability improves the effectiveness of protocol by providing user's authentication and reconfirmation of reachability of MH's home agent and new current address of mobile node MH. Data authentication embedded with this technology has provided extra security because home agent is static nodes and more secure than any other node. Some messages increases in binding update authentication, but some messages run in parallel so latency time does not increase significantly.

**Can Mobile IPv6 infrastructure be improved to reduce the latency of triangle routing packets to the Home Agent while maintaining or enhancing binding update security and location privacy?**

The solution for this question is Mobile Home Agents. Initially routing was possible through triangle routing via home agent and so caused the latency problems. The introduction of Mobile Home Agents solves this problem as a software agent on point of attachment of mobile node which acts as a proxy home agent. And as Mobile Node moves to other location mobile agents duplicates itself and thus reduces the latency.

This approach has advantages that even though traditional triangle routing takes place via the Mobile Home Agent, but security and speed is increased as the Mobile Home Agent acts as a proxy and firewall for the Mobile Node to the network. Thus whenever an Attacker will try to redirect packets from the Home Agent, it will not be possible due to proxy mobile home agent. As the Mobile Home Agent is in the same location as the mobile node, it is feasible to give its address to nodes on the public network as if it was the Mobile Node. Thus another security layer of protection is added to protect it from direct attack, as it hides the true IP address of the Mobile Node.

## 6.3 Main Contributions

The thesis provides unique contributions:

**A. Return Routability Test:** This is the basic solution to authenticate the binding updates within the existing Mobile IPv6 infrastructure, which also has some limitations when an attacker is on path between home agent and correspondent node.

**B. Cryptographically Generated Address:** This is one of the best possible ways to authenticate the user identity without any PKI infrastructure approach in which user interface's IP address is used to bind with the key to provide authentication.

**C. The Distributed Authentication Protocol:** This provides a de-centralized authentication solution within the existing Mobile IPv6 infrastructure, which can be used on its own or in combination with other security techniques.

**D. Mobile Home Agents:** This provides a software approach to embed in Mobile IPv6 infrastructure which provides location privacy to the mobile node and reduces the chances of attacks. This technology can also be combined with other technologies. When the Mobile Node moves to another point of attachment, Mobile Home Agent also duplicates itself to the new point of attachment. This provides a layer of security to the Mobile Node, as the Mobile Home Agent can't be as easily attacked, due to its mobility and dynamic nature, unlike that of a static Home Agent. This allows for binding updates to be less susceptible to types of Denial of Service attack. It also

provides a reduction in communication latency for packets destined for the Home Agent, as comparison to traditional triangle routing.

## 6.4 Future Research Improvements to Solutions

**1. The Distributed Authentication Protocol.**

Distributed Authentication Protocol may be improved by possible combining this security step with other steps in the solution, therefore reducing the latency before a binding update can take place. Because mobile node authentication data is also retrieved from Home Agents by the correspondent, so home agent security to store data should be enhanced to protect it from going to corrupt and protect it from malicious use.

**2. Dual Identity Protocol for Multiple SIM Mobile Devices.**

Because of the era of multiple SIM cards on a single device, another improvement needs to process authentication from both networks on that mobile. For the solutions of mobile devices to work, require the devices' operating system to be upgraded to handle this new feature. The only drawback of the solution is the increase of data sent and received that can congest the network and may slow or may interrupt to each other's networks.

**3. Mobile Home Agents**

Mobile Home Agents have to change its location as mobile moves to a new location so an extra intelligence required for a mobile home agent to work with a very high level of artificial intelligence to handle autonomous operation in a potentially hostile foreign network. They must be able to reproduce the same service as Home Agents while at the same time managing the tunneling of data to the Mobile Node and its own migration to the current point of attachment. During this transmission an attacker may exploit the software and may cause a denial of service to the network.

# References

[1] D. Johnson, C. E. Perkins, and J. Arkko, “Mobility support in IPv6,” IETF RFC 3775, June 2004.

[2] Hesham Soliman, “Mobile IPv6: Mobility in a Wireless Internet,” Addison-Wesley, 2004.

[3] P. Nikander, J. Arkko, T. Aura, G. Montenegro, and E. Nordmark, “Mobile IP version 6 route optimization security design background,” IETF RFC 4225, Dec. 2005.

[4] J. Arkko and P. Nikander, “How to authenticate unknown principals without trusted parties,” in Proc. of the 10th International Workshop, Security Protocols. Cambridge, UK. Springer, Apr. 2002, pp. 5–16.

[5] D. Hu, D. Zhou, and P. Li, “PKI and secret key based mobile IP security,” in International Conference on Communications, Circuits and Systems, Guilin, China, June 2006, pp. 1605– 1609.

[6] Tuomas Aura, Michael Roe,” Designing the Mobile IPv6 Security Protocol”, Vol. 61 no. 3-4, March-April 2006, Network and information systems security.

[7] S. Thomn and T. Narten, “1Pv6 Stateless Address Autoconfiguration,” Internet Engineering Task Force, Dccember 1998.

[8] John Ioannidis, “Protocols for Mobile Internetworking,” PhD thesis, Columbia University in the City of New York, 1993.

[9] Christian Huitema, “Routing in the Internet,” Prentice Hall, 1995.

[10] C. Kaufman, P. Hoffman, Y. Nir, and P. Eronen, “Internet Key Exchange Protocol Version 2 (IKEv2),” IETF RFC 5996, September 2010.

[11] S. Kent, “IP Authentication Header,” IETF RFC 4302, Dec 2005.

[12] S. Kent, “IP Encapsulating Security Payload (ESP),” IETF RFC 4303, Dec 2005.

[13] T. Aura, “Cryptographically Generated Addresses (CGA),” IETF RFC 3972, March 2005.

[14] G. O’Shea and M. Roe, “Child-proof authentication for MIPv6 (CAM),” ACM Computer Communications Review, vol. 31, no. 2, April 2001.

[15] Thomas Narten and Richard Draves, “Privacy extensions for stateless address auto configuration in IPv6,” RFC 3041, IETF, January 2001.

[16] J. Laganier, “Authorizing Mobile IPv6 Binding Update with Cryptographically Generated Addresses,” draft-laganier-mext-cga-01, Internet-Draft, October 26, 2010.

[17] J. Arkko et al, “Enhanced Route Optimization for Mobile IPv6,” Request for Comments: 4866, http://tools.ietf.org/html/rfc4866, 2007.

[18] Tuomas Aura and Jari Arkko, “MIPv6 BU attacks and defenses,” Internet Draft draft-aura-mipv6-bu-attacks-01, IETF Mobile IP Working Group, February 2002. Archived at http://www.watersprings.org/pub/id/draft-aura-mipv6-buattacks-01.txt.

[19] Philip Karn and William A. Simpson, “Photuris: session-key management protocol,” RFC 2522, IETF Network Working Group, March 1999.

[20] James Kempf, Jari Arkko, and Pekka Nikander, “Mobile IPv6 security,” Kluwer Wireless Personal Communications special issue on Security for Next Generation Communications, 29(3-4):389-414, June 2004.

[21] Brian E. Carpenter, Jon Crowcroft, and Yakov Rekhter, “IPv4 address behavior today,” RFC 2101, IETF, February 1997.

[22] Gabriel Montenegro and Claude Castelluccia, “SUCV identifiers and addresses,” Internet Draft draft-montenegro-sucv-02, November 2001. Archived at http://www.watersprings.org/pub/id/draft-montenegro-sucv-02.txt.

[23] Petrescu, A., Olivereau, A., Janneteau, C. and Lach H.-Y., "Threats for Basic Network Mpbility Support (NEMO threats)," Internet Draft, IETF,January 2004.

[24] R. Deng, J. Zhou & F. Bao, "Defending against redirect attacks in Mobile IP" in Proc. on 9th ACM Conference on Computer and Communications Security, 59-672002.

[25] Qiu, Y., Zhou, J., Bao, F., "Protecting All Traffic Channels in Mobile IP Network" in Proc. WCNC 2004, November 2002.

[26] A. Georgiades, Y. Luo, A. Lasebae and R. Comley, “Location Privacy in Mobile IPv6 Distributed Authentication Protocol Using Mobile Home Agents,” Recent Advances in Electronics, Hardware, Wireless and Optical Communications. Proceedings of the 8th WSEAS International Conference on Electronics, Hardware, Wireless and Optical Communications (EHAC ’09), Cambridge, UK, February 21-23, 2009. WSEAS Press, ISBN: 978-960-474-053-6

[27] Georgiades, Y. Luo and A. Lasebae "Trinity Protocol for Authentication of Binding Updates in Mobile IPv6", WSEAS, Issue 3, V 3, July 2004, ISSN 1109-2742.

[28] A. Georgiades, Y. Luo, A. Lasebae and R. Comley, “Distributed Authentication Protocol for the security of Binding Updates in Mobile IPv6,” Proceedings of the 9th WSEAS International CSCC Multiconference: Circuit ’05, Systems ’05, Computers ’05 Communications ’05. Vouliagmeni, Athens, Greece, July 11-16, 2005. ISBN:960-8457-29-7.

[29] Krawczyk, H., Bellare, M. and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, February 1997.

[30] W.Stallings, W.Cryptography and Network Security, Third Edition, Englewood Cliffs, NJ: Prentice-Hall, 2002.

[31] Vern Paxson, “An analysis of using reflectors for distributed denial-of-service attacks,” ACM Computer Communications Review (CCR), 31(3), July 2001.

[32] Charles Perkins, editor, “IP mobility support for IPv4,” RFC 3344, IETF, August 2002.

[33] Rescorla, E., "A Survey of Authentication Mechanisms", Internet Draft, IETF, March 2004.

[34] Michael Roe, Tuomas Aura, Greg O'Shea and Jari Arkko, Authentication of Mobile IPv6 binding updates and acknowledgments. Internet Draft draft-roemobileip-updateauth-01, November 2001. Archived at http://www.watersprings.org/pub/id/draft-roe-mobileip-updateauth-01.txt.

[35] Christoph L. Schuba, Ivan V. Krsul, Markus G. Kuhn, Eugene H. Spaffold, Aurobindo Sundaram and Diego Zamboni, “Analysis of a denial of service attack on TCP,” In Proc. 1997 IEEE Symposium on Security and Privacy, pages 208-223, Oakland, CA USA, May 1997. IEEE Computer Society Press.

[36] Tatu Ylönen, “SSH - secure login connections over the Internet,” In Proc. 6th USENIX Security Symposium, pages 37-42, San Jose, CA USA, June 1996. USENIX Association.

[37] T. Ernst., H-Y. Latch., "Network Mobility Support Terminology," Internet Draft, IETF,October 2004.

[38] Conta, A. and S. Deering, "Generic Packet Tunneling in IP Specification", RFC 2473, December 1998.

[39] Thierry Ernst, Ludovic Bellier, Castelluccia Claude, Hong-Yon Lach, “Mobile Networks Support in Mobile IPv6,” Internet Draft, draft-ernst-mobileip-v6-network-00.txt, Work in Progress, July 2000.

[40] X. Zhang, J. Castellanos, A. Campbell, K. Sawada, M.Barry, "P-MIP: Minimal Paging Extensions for Mobile IP," Internet Draft, draft-zhang-pmip-00.txt, Work in Progress, July 2000.

[41] Yingchun Xu, et all, "Mobile IP Based Micro Mobility Management Protocol in The Third Generation Wireless Network," Internet Draft, draft-ietf-mobileip-3gwireless-ext-04.txt, Work in Progress, June 2000.

[42] S. Glass, T. Hiller, S. Jacobs, C. Perkins, "Mobile IP Authentication, Authorization, and Accounting Requirements," Internet Draft, draft-ietf-mobileip-aaa-reqs-04.txt, Work in Progress, June 2000.

[43] Thomas Dreibholz, Andreas Jungmaier, and Michael Tüxen, "A new scheme for IP-based Internet mobility," in Proc. 28th Annual IEEE Intl. Conference on Local Computer Networks (LCN '03), IEEE Computer Society, pages 99-108, Königswinter, Germany, October 2003.

[44] Md. Shohrab Hossain, Mohammed Atiquzzaman and William Ivancic, "Security Vulnerabilities and Protection Mechanisms of Mobility Management Protocols", IEEE Aerospace conference, Big Sky, Montana, USA, March 2011.

# List of Published Paper

[1] Amit Gupta, Sumit Miglani and Maninder Singh, Analysis of Mobile IP Protocols Security. *International Journal of Computer Applications* 46(4):1-9, May 2012. Published by Foundation of Computer Science, New York, USA.