Investigating Cryptographically Generated Addresses in Mobile IPv6

Kuang Shilei

A Thesis Submitted in Partial Fulfillment of the Requirements for the Degree of

Master of Engineering in Computer Engineering

Prince of Songkla University

2008

Investigating Cryptographically Generated Addresses in Mobile IPv6

Kuang Shilei

A Thesis Submitted in Partial Fulfillment of the Requirements for the Degree of

Master of Engineering in Computer Engineering

Prince of Songkla University

2008

Thesis Title Investigating Cryptographically Generated Addresses to Mobile IPv6

Author Mr. Kuang Shilei

Major Program Computer Engineering

Major Advisor

……………………………………

(Mr. Robert Elz)

Co-advisor

……………………………………

(Assoc. Prof. Dr. Sinchai Kamolphiwong)

Examining Committee:

……………………………...Chairperson

(Dr. Nittida Elz)

..….…………………...….…..Committee

(Assoc. Prof. Dr. Sinchai Kamolphiwong)

...….……………………..….…Committee

(Assoc. Prof. Thossaporn Kamolphiwong)

...….……………….………..…Committee

(Dr. Panita Pongpaibool)

The Graduate School, Prince of Songkla University, has approved this thesis as partial fulfillment of the requirements for the Master of Engineering Degree in Computer Engineering

…………………………………………

(Assoc. Prof. Dr. Krerkchai Thongnoo)

Dean of Graduate School

Thesis Title	Investigating Cryptographically Generated Addresses in Mobile IPv6
Author	Mr. Kuang Shilei
Major Program	Computer Engineering
Academic Year	2008

ABSTRACT

Mobile IPv6 is designed to provide mobility support on top of the existing IP infrastructure, without requiring any modifications to routers or applications. The key benefit of Mobile IPv6 is that even though the mobile node changes locations and addresses, existing connections are maintained.

This work investigates standard Mobile IPv6 and IPv6 Route Optimization to observe correct operation. After that we investigate and implement Enhanced Route Optimization for Mobile IPv6. The Return Routability Procedure was designed with the objective to provide a level of security that compares to that of today’s non-mobile Internet. The IETF created Enhanced Route Optimization for Mobile IPv6 which provides lower handoff delays, increased security, and reduced signaling overhead. We investigate and implement Enhanced Route Optimization for Mobile IPv6. The focus of Enhanced Route Optimization is to apply Cryptographically Generated Addresses (CGAs). However the use of CGAs requires computationally expensive algorithms. We suspect the Correspondent Node will have to protect itself against potential denial-of service attempts from attackers by limiting the amount of resources it spends on CGA verification. In this thesis we measure the costs of Enhanced Route Optimization for Mobile IPv6 to verify this.

Keywords: IPv6, Mobile IPv6, CGA, RR Procedure, Route Optimization

ACKNOWLEDGEMENT

Foremost, I would like to express my deepest gratitude to my thesis advisor Mr. Robert. I have enjoyed working with him since I came here. His encouragement and support have made difficult times during my thesis studying less frustrating. His understanding, patience, encouragement, and being a role model have been the most important factors in increasing my confidence and improving my skills.

I would like to sincerely thank another thesis advisor, Assoc. Prof. Dr. Sinchai Kamolphiwong, who provided valuable information and advice at individual discussions.

I would also sincerely thank committee members Dr. Nittida Elz, Assoc. Prof. Thossapom Kamolphiwong, and Dr. Panita Pongpaibool to review and give the comment this work to be better.

I would like to thank the graduate School, the staff of faculty of Engineering and the staff of Department of Computer Engineering to give the convenient for me and everything.

I would like to thank my friends in CNR and CoE for their supports and assistances.

Finally, I would like to thank my parents for their loves, supports, for instilling upon me the value of education, and for always encouraging me to pursuit my aspirations.

Kuang Shilei

CONTENTS

Page

CONTENTS(CONTINUED)

Page

CONTENTS(CONTINUED)

Page

LIST OF TABLES

Table Page

LIST OF FIGURES

LIST OF FIGURES (CONTINUED)

LIST OF ABBREVIATIONS AND SYMBOLS

AH	Authentication Header
BA	Binding Acknowledgment
BU	Binding Update
CBA	Credit Based Authentication
CGA	Cryptographically Generated Address
CGAP	Cryptographically Generated Address Parameters
CN	Correspondent Node
CoA	Care-of Address
CoT	Care-of Test
CoTI	Care-of Test Init
DoS	Denial-of Service
ECC	Elliptic Curve Cryptography
ERO	Enhanced Route Optimization
ESP	Encapsulating Security Payload
HA	Home Agent
HoA	Home Address
HoT	Home Test
HoTI	Home Test Init
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6

LIST OF ABBREVIATIONS AND SYMBOLS (CONTINUED)

KAME	KarigoME[1]
MIP	Mobile IP
MIPv4	Mobile IPv4
MIPv6	Mobile IPv6
MN	Mobile Node
NGN	Next Generation Networking
PDA	Personal Digital Assistant
PHKT	Permanent Home Keygen Token
RO	Route Optimization
RRP	Return Routability Procedure
SEND	Secure Neighbor Discovery
TCP	Transmission Control Protocol
UDP	User Datagram Protocol

[1] KArigoME means “turtle” in Japanese

CHAPTER 1

INTRODUCTION

1.1 Motivation

With the rapid Mobile IP [3] technology development, most computing devices, including notebooks, PDAs and cell phones, will eventually anywhere anytime arbitrarily change the location that they connect to the internet. Mobile IP technology becomes more convenient to human's work, study and life. The total number of devices connected to the internet is increasing usage or consumption rapidly, which makes the address usage problem of IPv4 [1] even worse. Recently, a new vision IPv6 [2] was developed by the Internet Engineering Task Force (IETF) to satisfy the requirements of the Next Generation Networking (NGN). To a great extent, IPv6 is a conservative extension of IPv4, though mobility is a feature of IPv6 where Mobile IPv6 avoids Mobile IPv4 **t**riangular routing and is therefore almost as efficient as normal IPv6. This advantage is mostly hypothetical, assuming that Mobile IPv6 [5, 6] will be widely deployed in future.

In Mobile IPv4 [4] when a Mobile Node changes location, it obtains a Care-of address and informs its Home Agent of its new Care-of address. The Home Agent encapsulates and tunnels any packets it receives for the Mobile Node on its home network to this Care-of address. Therefore, every time a correspondent node sends a packet to the Mobile Node, while the Mobile Node is away from its home link, the packet first travels to the home network via the Home Agent before reaching the Mobile Node. This inefficient routing is called Triangle routing [4].

In Mobile IPv6 when a Mobile Node changes location, there are two possible modes for communications between the Mobile Nodes and Correspondent Nodes. One mode is called Bi-directional tunneling [5]. In this mode, packets from the Correspondent Node are routed to the home agent and then tunneled to the Mobile Node. Packets to the Correspondent Node are tunneled from the Mobile Node to the Home Agent (''reverse tunneled'') and then routed normally from the home network to the Correspondent Node. This is the same triangle routing used by Mobile IPv4. The other mode is called Route Optimization [6], and requires the Mobile Node to send a Binding Update message to register its current care-of address at the

Correspondent Node. This allows the Mobile Node to directly send packets to the Correspondent Node. Route Optimization eliminates the inefficient Triangle routing and Bi-directional tunneling.

However, the Binding Update message is quite a dangerous message [15, 18, 19]. If a node accepts the message without any verification, an attacker can easily redirect packets sent to the Mobile Node to the attackers. In order to prevent attacks, the IETF have proposed two different methods to protect Binding Update messages. First, a Binding Update message to a Home Agent is protected by the IPsec mechanism [8]. Second, a Binding Update message to a Correspondent Node is protected by the Return Routability Procedure [5]. The RR Procedure uses HoTI/HoT and CoTI/CoT messages respectively to test the Mobile Node's Home address and Care-of address reachability. The Return Routability Procedure was designed with the objective to provide a level of security that compares to that of today's non-mobile Internet [21]. This issue will be described in chapter 2.

Several enhancements to the RR procedure have been proposed. The IETF has created Enhanced Route Optimization for Mobile IPv6 which is intended to provide lower handoff delays, increased security, and reduced signaling overhead. The purpose of HoTI/HoT is ensuring packets can only be redirected by the legitimate recipient. The legitimate recipient is identified through the home address, and only the legitimate recipient is expected to receive the Home Keygen Token sent to the home address.

Cryptographically Generated Addresses (CGA) can provide the same functionality without sending a packet to the home address. A node that uses a CGA at a certain time can prove at a later time that it is still the same node when it uses this CGA again. But instead of relying on a routing property, as with the home-address test, this proof can be drawn from the CGA's special interface identifier. The CGA owner signs important packets with its private key and includes its public key along with the auxiliary data in these packets. Since it is computationally hard to produce another public/private-key pair that hashes to the same CGA, the recipient of the signed message can verify, by recomputing the hash and comparing it with the CGA's interface identifier, that the sender must be the legitimate owner of this CGA.

Unfortunately, CGAs use computationally expensive algorithms. This may be an issue for small mobile devices with low processing power. It is likely to be an issue for correspondent nodes that simultaneously communicate with a large number of mobile nodes, such as publicly accessible servers. Aside from the computational overhead required for dealing with legitimate mobile nodes, a correspondent node will have to protect itself against potential denial-of service (DoS) [34, 35] attempts from attackers by limiting the amount of resources it spends on CGA verification.

In this thesis first we investigate and implement standard Route Optimization for Mobile IPv6 [5, 6]. After that we build a MIPv6 Testbed to investigate and implement Enhanced Route Optimization for Mobile IPv6. Moreover, we are concentrating upon the costs particularly for the Correspondent Node. The costs of Enhanced Route Optimization for Mobile IPv6 are not negligible. So, we evaluate Enhanced Route Optimization using utility code to calculate computation cost of the CGA algorithm and the RSA algorithm in Enhanced Route Optimization. In addition, we also calculate the cost to the correspondent node of processing many incoming invalid Enhanced Route Optimization requests. Finally we give experiment results and analyze this data, suggest related work, and give the conclusion to this thesis.

1.2 Objectives

1) To investigate and implement standard Route Optimization for Mobile IPv6 (Code for this should be available with any existing Mobile IPv6 implementation).

2) To investigate and implement Enhanced Route Optimization for Mobile IPv6 (Applying CGA to Mobile IPv6 code for this will need to be written).

3) To discover any possible improvements to the Enhanced Route Optimization algorithm, and test their effectiveness.

4) Evaluate Enhanced Route Optimization and make a conclusion.

1.3 Advantages

1) We expect to provide lower handoff delay for Mobile IPv6 Route Optimization.

2) We expect to increase security for Mobile IPv6 Route Optimization.

3) We expect to reduce signaling overhead for Mobile IPv6 Route Optimization.

4) We expect to provide a case study of network security.

5) We expect to practice and evolve students' skill to solve problems.

1.4 Scope of work

1) Study Mobile IPv6 technique and CGA technique, investigate Enhanced Route Optimization for Mobile IPv6.
2) Investigate and implement the standard Route Optimization in Mobile IPv6 Network.
3) Investigate and implement the Enhanced Route Optimization in Mobile IPv6 Network.
4) Use experimental network to test and evaluate.
5) The implementation will be done on a UNIX system.

1.5. Work Plan

1) Investigate and Research standard Route Optimization for Mobile IPv6.
   Investigate and Research the Security Problem in Mobile IPv6 Route Optimization.
   Investigate Enhanced Route Optimization for Mobile IPv6.
2) Proposal writing.
3) Design the experimental network topology in order to test Both Conservative Route Optimization and Enhanced Route Optimization.
4) Build Mobile IPv6 Testbed.
5) Implement and test the Conservative Route Optimization in Mobile IPv6 Testbed.
6) Implement, Investigate and test Enhanced Route Optimization in Mobile IPv6 Testbed.
7) Analyze implementation data make conclusion.
8) Collecting the results and write final report.

1.6 Outline

This document is organized in 7 chapters as follows:

Chapter 1, Introduction, is the motivation, objective and scope of this work. In addition, it presents the work plan to evaluate and investigate enhanced Route Optimization for Mobile IPv6.

Chapter 2, Background of Mobile IPv6, it presents Mobile IPv6 techniques and principles. Included are Mobile IPv6 terminologies, Mobile IPv6 Basic Operation and Mobile IPv6 Security.

Chapter 3, Investigating Enhanced Route Optimization for Mobile IPv6, gives the background and principles of CGA. It also presents the background of Enhanced Route Optimization for Mobile IPv6. Finally, it discusses requirements to evaluate and investigate Enhanced Route Optimization for Mobile IPv6.

Chapter 4, Mobile IPv6 TestBed and Testing, introduces the testing and implementation to survey Mobile IPv6 testbed network.

Chapter 5, Implementation and testing, presents prototype implementation and method to test Enhanced Route Optimization for mobile IPv6. Also it discusses some of the issues with applying CGA to Mobile IPv6.

Chapter 6, Provides the results from measurements made of the costs of ERO and some discussion of those results.

Chapter 7, Discussion, conclusion and analysis. This also presents some limitations and suggests future work required in this area.

Chapters 4, 5 and 6 represent the primary work of this thesis and chapter 7 is the conclusion.

CHAPTER 1

INTRODUCTION

1.1 Motivation

With the rapid Mobile IP [3] technology development, most computing devices, including notebooks, PDAs and cell phones, will eventually anywhere anytime arbitrarily change the location that they connect to the internet. Mobile IP technology becomes more convenient to human's work, study and life. The total number of devices connected to the internet is increasing usage or consumption rapidly, which makes the address usage problem of IPv4 [1] even worse. Recently, a new vision IPv6 [2] was developed by the Internet Engineering Task Force (IETF) to satisfy the requirements of the Next Generation Networking (NGN). To a great extent, IPv6 is a conservative extension of IPv4, though mobility is a feature of IPv6 where Mobile IPv6 avoids Mobile IPv4 triangular routing and is therefore almost as efficient as normal IPv6. This advantage is mostly hypothetical, assuming that Mobile IPv6 [5, 6] will be widely deployed in future.

In Mobile IPv4 [4] when a Mobile Node changes location, it obtains a Care-of address and informs its Home Agent of its new Care-of address. The Home Agent encapsulates and tunnels any packets it receives for the Mobile Node on its home network to this Care-of address. Therefore, every time a correspondent node sends a packet to the Mobile Node, while the Mobile Node is away from its home link, the packet first travels to the home network via the Home Agent before reaching the Mobile Node. This inefficient routing is called Triangle routing [4].

In Mobile IPv6 when a Mobile Node changes location, there are two possible modes for communications between the Mobile Nodes and Correspondent Nodes. One mode is called Bi-directional tunneling [5]. In this mode, packets from the Correspondent Node are routed to the home agent and then tunneled to the Mobile Node. Packets to the Correspondent Node are tunneled from the Mobile Node to the Home Agent (‘‘reverse tunneled’’) and then routed normally from the home network to the Correspondent Node. This is the same triangle routing used by Mobile IPv4. The other mode is called Route Optimization [6], and requires the Mobile Node to send a Binding Update message to register its current care-of address at the

Correspondent Node. This allows the Mobile Node to directly send packets to the Correspondent Node. Route Optimization eliminates the inefficient Triangle routing and Bi-directional tunneling.

However, the Binding Update message is quite a dangerous message [15, 18, 19]. If a node accepts the message without any verification, an attacker can easily redirect packets sent to the Mobile Node to the attackers. In order to prevent attacks, the IETF have proposed two different methods to protect Binding Update messages. First, a Binding Update message to a Home Agent is protected by the IPsec mechanism [8]. Second, a Binding Update message to a Correspondent Node is protected by the Return Routability Procedure [5]. The RR Procedure uses HoTI/HoT and CoTI/CoT messages respectively to test the Mobile Node's Home address and Care-of address reachability. The Return Routability Procedure was designed with the objective to provide a level of security that compares to that of today's non-mobile Internet [21]. This issue will be described in chapter 2.

Several enhancements to the RR procedure have been proposed. The IETF has created Enhanced Route Optimization for Mobile IPv6 which is intended to provide lower handoff delays, increased security, and reduced signaling overhead. The purpose of HoTI/HoT is ensuring packets can only be redirected by the legitimate recipient. The legitimate recipient is identified through the home address, and only the legitimate recipient is expected to receive the Home Keygen Token sent to the home address.

Cryptographically Generated Addresses (CGA) can provide the same functionality without sending a packet to the home address. A node that uses a CGA at a certain time can prove at a later time that it is still the same node when it uses this CGA again. But instead of relying on a routing property, as with the home-address test, this proof can be drawn from the CGA's special interface identifier. The CGA owner signs important packets with its private key and includes its public key along with the auxiliary data in these packets. Since it is computationally hard to produce another public/private-key pair that hashes to the same CGA, the recipient of the signed message can verify, by recomputing the hash and comparing it with the CGA's interface identifier, that the sender must be the legitimate owner of this CGA.

Unfortunately, CGAs use computationally expensive algorithms. This may be an issue for small mobile devices with low processing power. It is likely to be an issue for correspondent nodes that simultaneously communicate with a large number of mobile nodes, such as publicly accessible servers. Aside from the computational overhead required for dealing with legitimate mobile nodes, a correspondent node will have to protect itself against potential denial-of service (DoS) [34, 35] attempts from attackers by limiting the amount of resources it spends on CGA verification.

In this thesis first we investigate and implement standard Route Optimization for Mobile IPv6 [5, 6]. After that we build a MIPv6 Testbed to investigate and implement Enhanced Route Optimization for Mobile IPv6. Moreover, we are concentrating upon the costs particularly for the Correspondent Node. The costs of Enhanced Route Optimization for Mobile IPv6 are not negligible. So, we evaluate Enhanced Route Optimization using utility code to calculate computation cost of the CGA algorithm and the RSA algorithm in Enhanced Route Optimization. In addition, we also calculate the cost to the correspondent node of processing many incoming invalid Enhanced Route Optimization requests. Finally we give experiment results and analyze this data, suggest related work, and give the conclusion to this thesis.

1.2 Objectives

1) To investigate and implement standard Route Optimization for Mobile IPv6 (Code for this should be available with any existing Mobile IPv6 implementation).

2) To investigate and implement Enhanced Route Optimization for Mobile IPv6 (Applying CGA to Mobile IPv6 code for this will need to be written).

3) To discover any possible improvements to the Enhanced Route Optimization algorithm, and test their effectiveness.

4) Evaluate Enhanced Route Optimization and make a conclusion.

1.3 Advantages

1) We expect to provide lower handoff delay for Mobile IPv6 Route Optimization.

2) We expect to increase security for Mobile IPv6 Route Optimization.

3) We expect to reduce signaling overhead for Mobile IPv6 Route Optimization.

4) We expect to provide a case study of network security.

5) We expect to practice and evolve students' skill to solve problems.

1.4 Scope of work

1) Study Mobile IPv6 technique and CGA technique, investigate Enhanced Route Optimization for Mobile IPv6.
2) Investigate and implement the standard Route Optimization in Mobile IPv6 Network.
3) Investigate and implement the Enhanced Route Optimization in Mobile IPv6 Network.
4) Use experimental network to test and evaluate.
5) The implementation will be done on a UNIX system.

1.5. Work Plan

1) Investigate and Research standard Route Optimization for Mobile IPv6.
   Investigate and Research the Security Problem in Mobile IPv6 Route Optimization.
   Investigate Enhanced Route Optimization for Mobile IPv6.
2) Proposal writing.
3) Design the experimental network topology in order to test Both Conservative Route Optimization and Enhanced Route Optimization.
4) Build Mobile IPv6 Testbed.
5) Implement and test the Conservative Route Optimization in Mobile IPv6 Testbed.
6) Implement, Investigate and test Enhanced Route Optimization in Mobile IPv6 Testbed.
7) Analyze implementation data make conclusion.
8) Collecting the results and write final report.

1.6 Outline

This document is organized in 7 chapters as follows:

Chapter 1, Introduction, is the motivation, objective and scope of this work. In addition, it presents the work plan to evaluate and investigate enhanced Route Optimization for Mobile IPv6.

Chapter 2, Background of Mobile IPv6, it presents Mobile IPv6 techniques and principles. Included are Mobile IPv6 terminologies, Mobile IPv6 Basic Operation and Mobile IPv6 Security.

Chapter 3, Investigating Enhanced Route Optimization for Mobile IPv6, gives the background and principles of CGA. It also presents the background of Enhanced Route Optimization for Mobile IPv6. Finally, it discusses requirements to evaluate and investigate Enhanced Route Optimization for Mobile IPv6.

Chapter 4, Mobile IPv6 TestBed and Testing, introduces the testing and implementation to survey Mobile IPv6 testbed network.

Chapter 5, Implementation and testing, presents prototype implementation and method to test Enhanced Route Optimization for mobile IPv6. Also it discusses some of the issues with applying CGA to Mobile IPv6.

Chapter 6, Provides the results from measurements made of the costs of ERO and some discussion of those results.

Chapter 7, Discussion, conclusion and analysis. This also presents some limitations and suggests future work required in this area.

Chapters 4, 5 and 6 represent the primary work of this thesis and chapter 7 is the conclusion.

CHAPTER 2

BACKGROUND INFORMATION

This Chapter presents the background information for Mobile IPv6. The Mobile IP technology is introduced in section 2.1. The information of Mobile IPv6 is presented in section 2.2. The overview of Mobile IPv6 Basic Operation is described in section 2.3. Section 2.4 present Mobile IPv6 Security mechanisms. The Return Routability procedure security mechanism is described in section 2.5. A summary of this chapter is in section 2.6.

2.1 Introduction

As the number of Mobile Device increases greatly, mobile terminal units requiring to connect to the internet are beginning to change our perceptions. A need has been generated to allow mobile devices to attach to any domain convenient to their current location. That demands a mobile networking technology to provide seamless and continuous connectivity to the internet [5, 6].

Mobile IP technology is designed to satisfy this requirement [3]. Mobile IP provides an efficient, scalable mechanism for roaming within the Internet. Using Mobile IP, nodes may change their point of attachment to the Internet without changing their IP addresses. This allows them to maintain transport and higher-layer connections while moving. With the shortage of IPv4 [1] address space, IPv6 [2] will be the protocol for all IP-Network. The implementation of IPv6 provides an upgrade event to allow Mobile IP technology to be added to all nodes.

2.2 Mobile IPv6

Mobile Internet Protocol version 6 (MIPv6) [5, 6] (see Figure 2.1) allows an IPv6 node to be mobile—to arbitrarily change its location on an IPv6 network—and still maintain reachability. Connection maintenance for mobile nodes is not done by modifying Transport layer protocols, but by handling the change of addresses at the Internet layer using Mobile IPv6 messages, options, and processes that ensure the correct delivery of data regardless of the mobile node's location. The Mobile IPv6 terminologies [5, 6] are as follows:

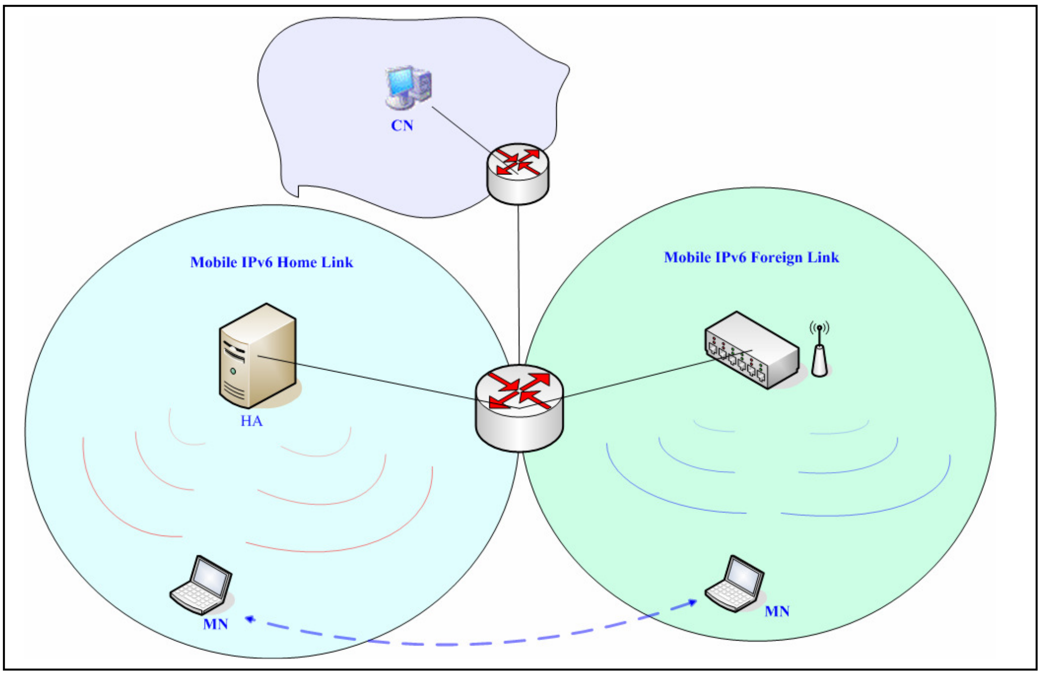


Figure 2.1 Mobile IPv6 Components

Home link: The link that is assigned the home subnet prefix, from which the mobile node obtains its home address. The home agent resides on the home link.

Foreign link: A link that is not the mobile node's home link.

Home address (HoA): An address assigned to the Mobile Node when it is attached to the home link and through which the Mobile Node is always reachable, regardless of its location on an IPv6 network. If the Mobile Node is attached to the Home link, Mobile IPv6 processes are not used and communication occurs normally. If the Mobile Node is away from home (not attached to the home link), packets addressed to the Mobile Node's home address are intercepted by the Home Agent and tunneled to the Mobile Node's current location on the IPv6 network. Because the Mobile Node is always assigned the home address, it is always logically connected to the home link.

Care-of Addresses (CoA): An address used by a Mobile Node while it is attached to a foreign link. For stateless address configuration, the care-of address is a combination of the foreign subnet prefix and an interface ID determined by the Mobile Node. A Mobile Node can be assigned multiple care-of addresses; however, only one care-of address is registered as the primary care-of address with the Mobile Node's Home Agent. The association of a home address with a care-of address for a mobile node is known as a binding. Correspondent nodes and home agents keep information on bindings in a binding cache.

Home Agent (HA): A router (usually) on the home link that maintains registrations of Mobile Nodes that are away from home and the different addresses that they are currently using. If the Mobile Node is away from home, it registers its current address with the Home Agent, which tunnels data sent to the Mobile Node's home address to the Mobile Node's current address on an IPv6 network and forwards tunneled data sent by the mobile node.

Mobile Node (MN): An IPv6 node that can change links, and therefore addresses, and maintain reachability using its home address. A Mobile Node has awareness of its home address and the global address for the link to which it is attached (known as the care-of address), and indicates its home address/care-of address mapping to the Home Agent and Mobile IPv6-capable nodes with which it is communicating. A node that moves, but re-initializes or re-establishes connections is not a mobile node for mobile IPv6.

Correspondent Node (CN): Any IPv6 node communicating with a Mobile Node.

2.3 Basic Operation of Mobile IPv6

Mobile nodes will have assigned to their network interface(s) at least three IPv6 addresses whenever they are roaming away from their home subnet. One is its home address, which is permanently assigned to the mobile node in the same way as any IP node. The second address is the mobile node's current Link-Local address [2]. Mobile IPv6 adds a third address, known as the mobile node's care-of address, which is associated with the mobile node only while visiting a particular foreign subnet. The network prefix of a mobile node's care-of address is equal to the network prefix of the foreign subnet being visited by the mobile node, and thus packets addressed to this care-of address will be routed by normal Internet routing mechanisms to the mobile node's location away from home.

Each time the mobile node moves its point of attachment from one IP subnet to another, the mobile node will configure its care-of address by stateless address auto-configuration or altematively by some means of stateful address auto-configuration such as DHCPv6 [16] or PPPv6[17]. The decision about which manner of automatic address configuration to use is made according to the methods of IPv6 Neighbor Discovery (ND) [14]. A mobile node may have more than one care-of address at a time, for example if it is link-level attached to more than one (wireless) network at a time or if more than one IP network prefix is present on a network to which it is attached. The association between a mobile node's home address and its care-of address, along with the remaining lifetime of that association, is known as a binding. The central data structure used in Mobile IPv6 is a cache of mobile node bindings, maintained by each IPv6 node, known as a Binding Cache.

While away from home, a mobile node registers one of its bindings with a router in its home subnet, requesting this node to function as the home agent for the mobile node. The care-of address in this binding registered with its home agent is known as the mobile node's primary care-of address, and the mobile node's home agent retains this entry in its Binding Cache, marked as a "home registration," until its lifetime expires. While it has a home registration entry in its Binding Cache, the home agent uses proxy Neighbor Discovery to intercept any IPv6 packets addressed to the mobile node's home address on the home subnet. It tunnels each intercepted packet to the mobile node's primary care-of address indicated in this Binding Cache entry. To tunnel the packet, the home agent encapsulates it using IPv6 encapsulation.

In addition, Mobile IPv6 provides two mechanisms for IPv6 correspondent nodes communicating with a mobile node, we present as following:

2.3.1 Bi-directional Tunneling Mode

In this mode, if a Mobile Node moves to foreign network or the Mobile Node moves from one network to another network, the Mobile Node gets a care-of address that it uses in communication with other nodes. The Mobile Node sends a message which is called a Binding Update (BU) message to the Home Agent. The message includes the care-of address and the home address of the Mobile Node. Such information is called binding information, since it binds a care-of address to the home address of a Mobile Node. When a Home Agent receives the message and accepts the contents of the message, the Home Agent replies with a Binding Acknowledgment (BA) message to indicate that the Binding Update message is accepted. This process we called home registration which we presented above. Whenever the Mobile Node moves anywhere it must send a Binding Update message to the Home Agent. Then the Home Agent can always know where the Mobile Node is.

After the process of home registration, the Home Agent creates a bi-directional tunnel connection from its address to the care-of address of the Mobile Node. The Mobile Node also creates a bi-directional tunnel connection from its care-of address to the Home Agent when it receives the acknowledgment message. After successful tunnel creation, all packets sent to the home address of the Mobile Node are intercepted by the Home Agent at the home network and tunneled to the Mobile Node. Also, all packets originated at the Mobile Node are tunneled to its Home Agent and forwarded from its home network to destination nodes. Figure 2.2 shows the concept.

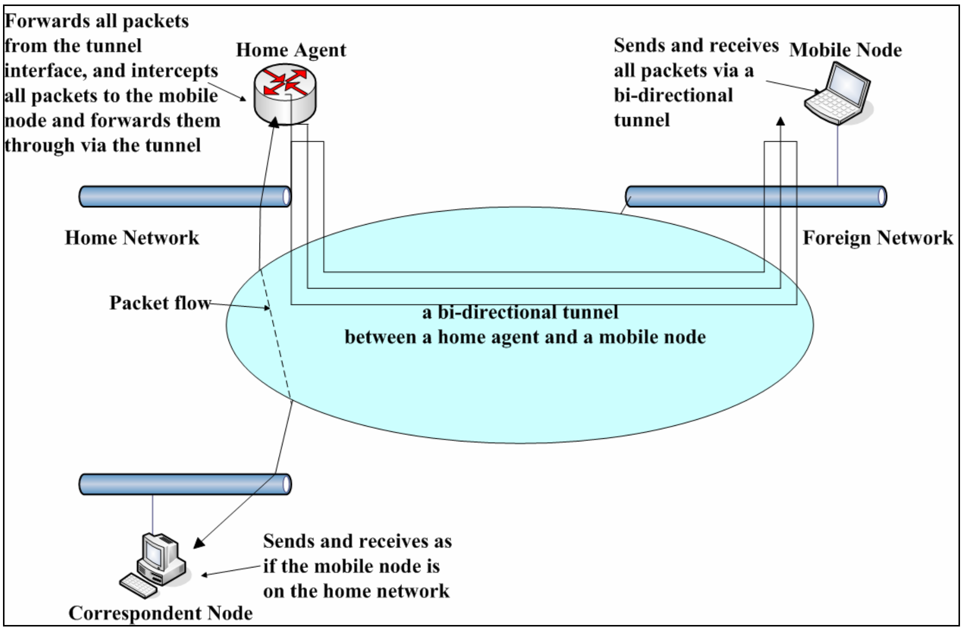

Forwards all packets from the tunnel interface, and intercepts all packets to the mobile node and forwards them through via the tunnel
Home Agent
Sends and receives all packets via a bi-directional tunnel
Mobile Node
Home Network
Foreign Network
Packet flow
a bi-directional tunnel between a home agent and a mobile node
Sends and receives as if the mobile node is on the home network
Correspondent Node

Figure 2.2 Bi-directional tunneling

2.3.2 Triangle Route Problem

In Mobile IPv6, the communication path between a mobile node and a correspondent node use Bi-directional tunneling. When a correspondent node (Mobile IPv6 capability) initiates communication with a mobile node and sends packets to the mobile's home address, the home agent intercepts the packets and forwards them to the mobile node. The mobile node replies directly to correspondent node, see figure 2.3. This inefficient process is called the "**triangle route problem**".

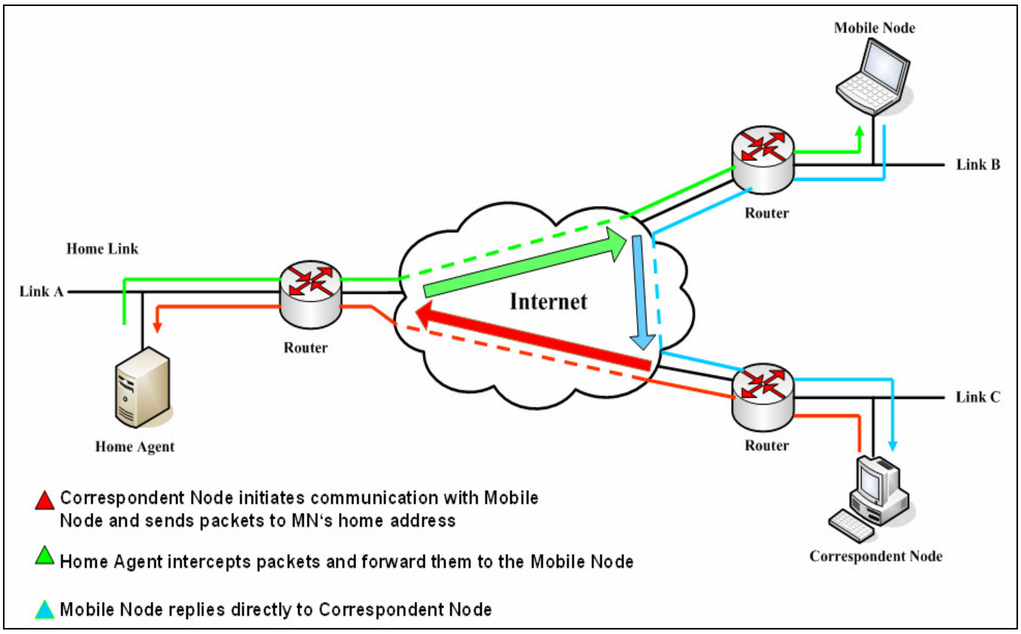

Mobile Node
Link B
Router
Home Link
Link A
Router
Internet
Link C
Router
Home Agent
Correspondent Node
▲ Correspondent Node initiates communication with Mobile Node and sends packets to MN's home address
▲ Home Agent intercepts packets and forward them to the Mobile Node
▲ Mobile Node replies directly to Correspondent Node

Figure 2.3 Triangle Route Problem

This method may be inefficient in many cases. Figure 2.4 shows the worst case: A Mobile Node and a Correspondent Node are on the same network. The packets exchanged between them are always sent to the home network of the Mobile Node, even if they are directly accessible to each other using the local network. One way to improve this inefficient communication path is called Route Optimization.

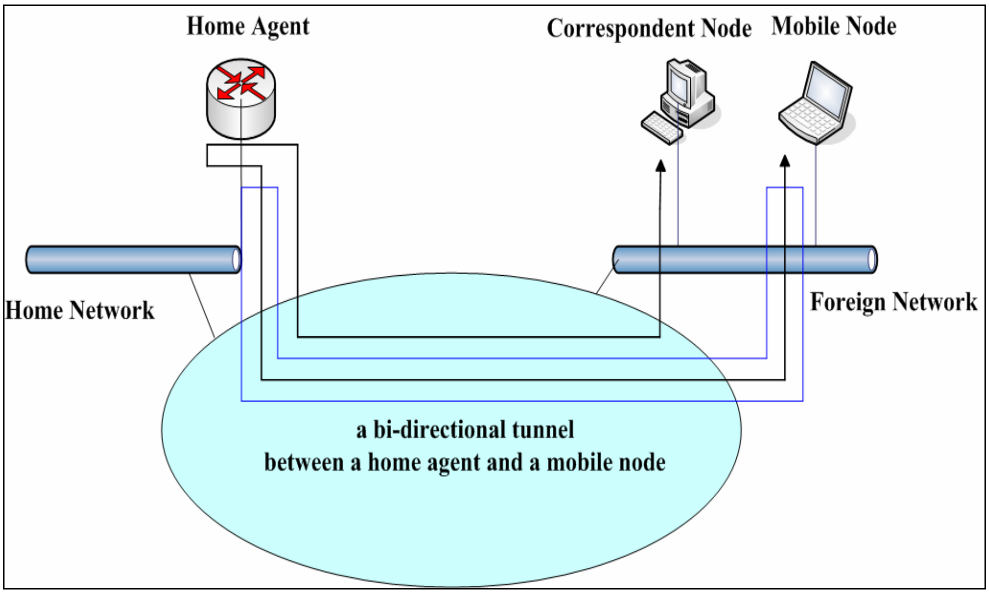


Figure 2.4 The worst case of bi-directional tunneling

2.3.3 Route Optimization Mode

In this mode, when a Mobile Node is away from its home link, the Mobile Node sends a Binding Update message to register its current care-of address at the correspondent node. This process we call *Correspondent registration*. The Correspondent Node receives the message and accepts the contents of the message, after that replies with a Binding Acknowledgment (BA) message to indicate that the Binding Update message was accepted. This packet is directly sent to the care-of address of the Mobile Node. After that the Mobile Node data packets are sent directly from the Mobile node to the Correspondent Node. Figure 2.5 shows the procedure.

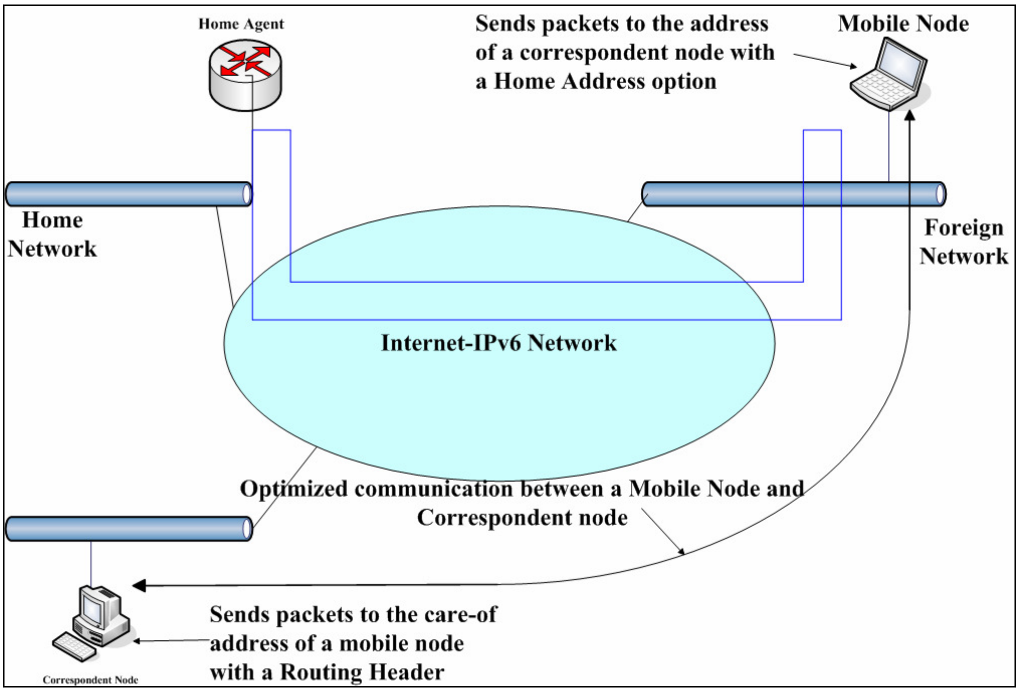

Home Agent
Sends packets to the address of a correspondent node with a Home Address option
Mobile Node
Home Network
Foreign Network
Internet-IPv6 Network
Optimized communication between a Mobile Node and Correspondent node
Sends packets to the care-of address of a mobile node with a Routing Header
Correspondent Node

Figure 2.5 Optimized communication between a MN and a CN

So we can find in the worst case of bi-directional tunneling. If a correspondent node supports the route optimization mechanism, the mobile node and the correspondent node can communicate directly without detouring through the home agent. Figure 2.6 shows the procedure.

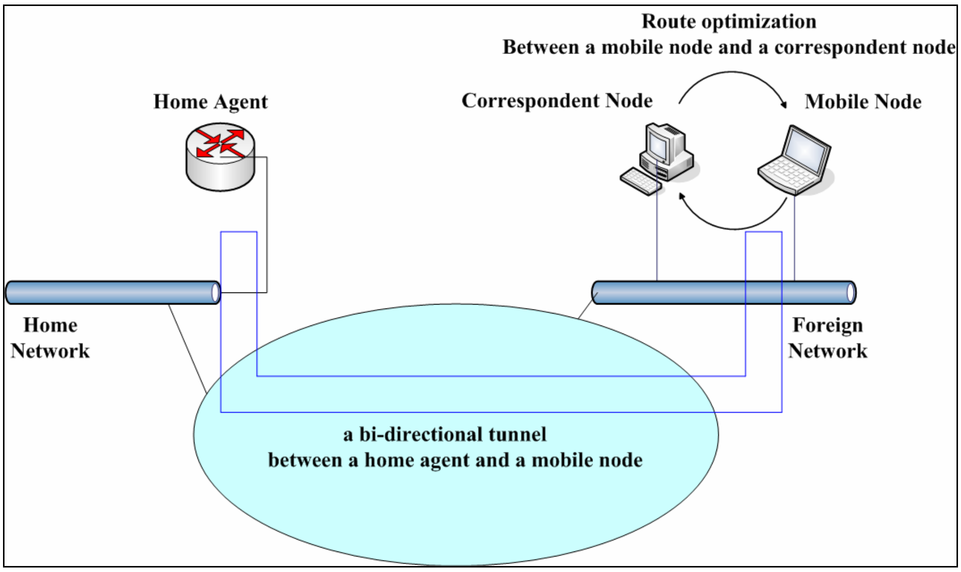


Figure 2.6 Optimized communications in worse case

2.4 Mobile IPv6 Security

Mobile IPv6 can be considered as a mobility extension for the basic IPv6 functionality. From the data security perspective, the basic objective during the development of Mobile IPv6 has been that it must be at least as secure as basic IPv6 or IPv4 from the Mobile Node perspective and it should not introduce any new security threats to IPv6 from the network and other nodes' perspective. This thesis emphasis considers Binding Update message security problem. We especially emphasize threats against route optimization with Correspondent Node. In Mobile IPv6, when the Mobile node is away from its home, it will send binding update messages to the home agent and the correspondent node to register its current care-of address. If a node accepts the message without any verification, an attacker can easily redirect packets sent to the mobile node to the attacker.

2.4.1. False Binding Update Attack

In Mobile IPv6 spoofed Binding Updates may be sent to Home Agents and Correspondent Nodes. By spoofing Binding Updates, an attacker can redirect traffic to itself or another node and prevent the original node from receiving traffic destined to it. For example, shown as figure 2.7, let us say nodes A and B have been communicating with each other, then, an attacker, node C, sends a spoofed Binding Update packet to node B, claiming to be node A with a Care-of Address of node C. This would cause node B to create a binding for node A's Care-of Address and subsequently send further traffic to node C, believing it to be node A's new Care-of Address. Node A would not receive the data it was intended to receive, and, if the data in the packets is not cryptographically protected, node C will be able to see all of node A's sensitive information.

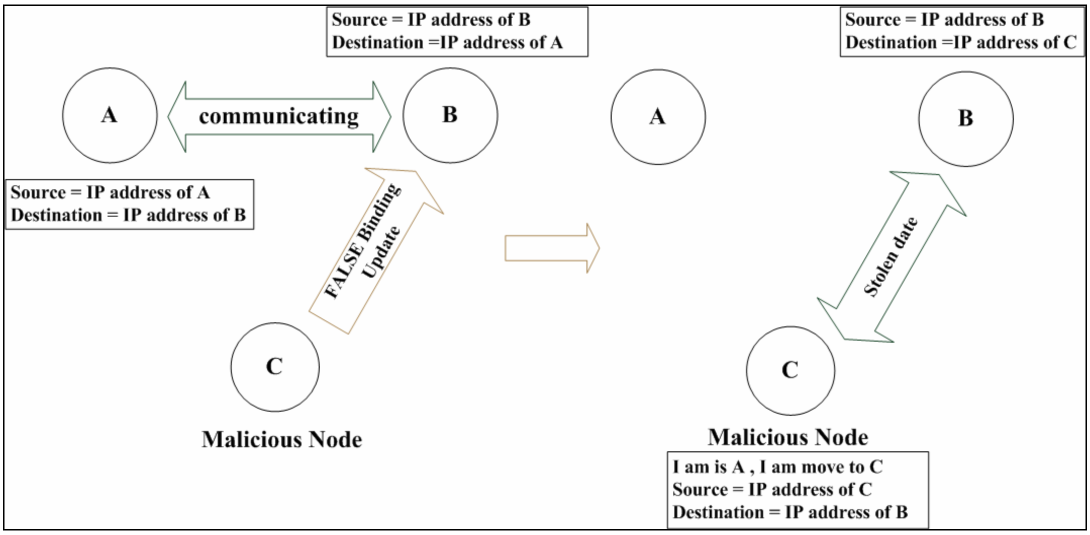


Figure 2.7 False Binding Update Attacks

2.4.2. Man-in-the-Middle Attack

A more serious problem could occur if the attacker spoofs the mobile node to the correspondent node and simultaneously spoofs the correspondent node to the mobile node. Each node now believes the attacker is its partner. All data between the correspondent node and mobile node now flows through the attacker. For example, shown as figure 2.8, if node A and node B are communicating, the attacker could send both nodes a spoofed Binding Update with the Care-of Address set to its own address. This would cause both nodes A and B to send all packets to node C rather than to each other, and therefore, results in attacks against secrecy and integrity. (Note that without Route Optimization, an attacker would have to be in the path between the nodes in order to capture and read packets)

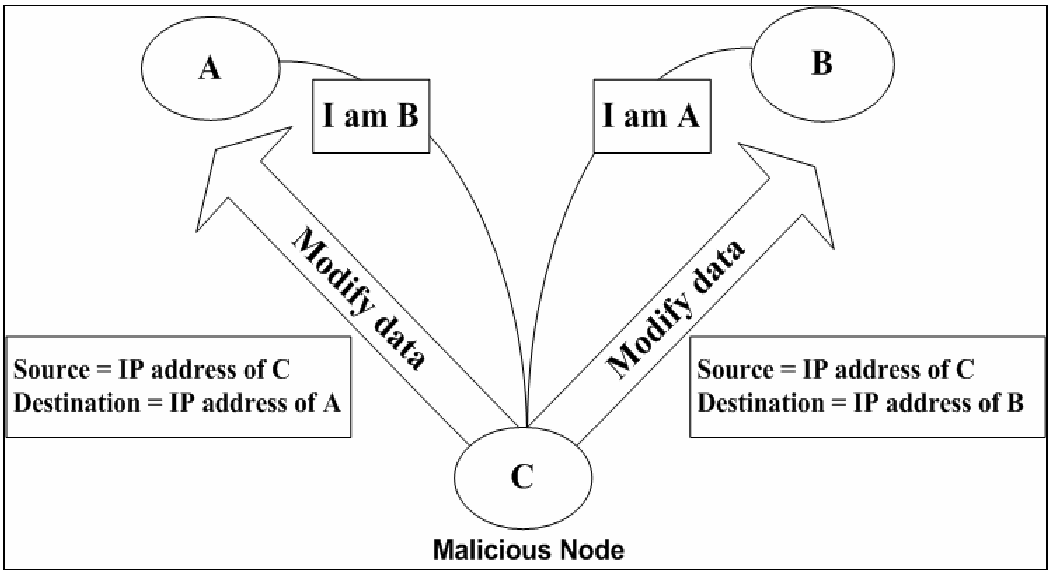


Figure 2.8 Man-in-the-Middle Attacks

2.4.3. Denial-of-Service Attack (DoS)

By sending a spoofed Binding Update an attacker could also send large amounts of unwanted traffic to overwhelm the resources of a single node or those of a network. The attacker could first find a site with streaming video or another heavy data stream and establish a connection with it. Then it could send a BU to the correspondent node, saying to redirect subsequent data traffic to the attacker's new location, that of an arbitrary node. For example see figure 2.9. Node B has a Video on Demand (VOD) service, node A establishes a connection with B which causes a heavy data stream exchange between them. If node A would like attack node C, it can send a BU to B to tell it "I have moved to C." This will cause large amounts of data to be sent to C. This node C would be then bombed with a large amount of unnecessary traffic. Similarly, the attacker could also use spoofed BUs to redirect several streams of data to random addresses with the network prefix of a particular target network, thereby congesting an entire network with unwanted data.

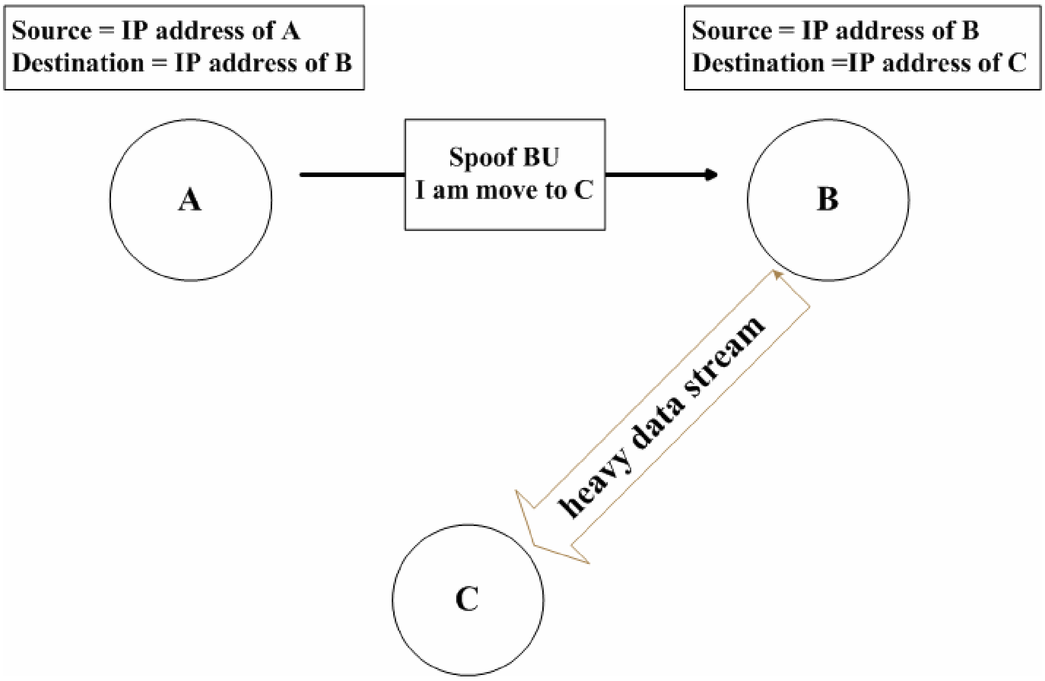


Figure 2.9 Denial-of-Service Attacks

Secondly, the adversary may also try to attack the BU protocol itself, and thus prevent the protocol participants from correctly completing the protocol. Basically, these types of attacks can be identified as DoS attacks. The stateful protocols are known to expose the protocol participants to DoS attack. ‘‘In particular, if a host stores a state in a protocol run that someone else has initiated and before authenticating the initiator, an attacker can initiate the protocol many times and cause the host to store a large number of unnecessary protocol states’’ [46]. Other attacks of this type include reflection and amplification attack and replay attack [46]. In reflection and amplification attacks, packets are sent into a looping path to the target (amplification); the attacker can also hide the source of packets by reflecting the traffic from other node (reflection), and therefore, the protocol participant nodes can be tricked into sending many more packets than they receive from the attacker. In a replay attack, the attacker captures the BUs of the MN, and tries to replay them after the MN moved away.

Note that the different attacks assume different conditions and requirements of the attackers and therefore, the security threats vary largely. However, Route Optimization provides a Mobile Node the opportunity to eliminate the inefficient triangle routing with its Correspondent Node and therefore, greatly improves the network performance. But unauthenticated or malicious

Binding Update message would provide an intruder with an easy means to launch various types of attack. In order to prevent attacks the IETF has proposed two different methods to protect Binding Update messages. The Binding Update message to a Home Agent is protected by the IPSec [8] mechanism. IPSec is designed to provide interoperable, high quality, cryptographically-based security for IPv4 and IPv6. Currently, IPSec is used in protecting messages exchanged between the Mobile Node and the Home Agent. The use of the mandatory IPSec Authentication Header (AH) and the Encapsulating Security Payload (ESP) [11] and key management mechanism help to ensure the integrity of the Binding Update messages between the Mobile Node and Home Agent. In this Thesis we do not investigate "using IPSec to Protect Mobile IPv6 Signaling between Mobile Nodes and Home Agents" [8], because we believe the IPSec mechanism brings enough safety for Home registration. Security between Mobile Node and Correspondent node is this thesis objective. A Binding Update message to a Correspondent Node is protected by the Return Routability Procedure [5, 6]. IPSec has been also proposed to protect between Mobile and Correspondent IPv6 Nodes [9].

2.4.4. Using IPSec to Protect MIPv6 Signaling Between MN and HA

The IPSec protocol suite is used to provide privacy and authentication services at the IP layer. It provides a set of security algorithms plus a general framework that allows a pair of communicating entities to use whichever algorithms provide security are appropriate for the communication.

This section discusses security mechanisms for the control traffic between the mobile node and the home agent. If this traffic is not protected, mobile nodes and correspondent nodes are vulnerable to man-in-the-middle, hijacking, passive wiretapping, impersonation, and denial-of-service attacks. Any third parties are also vulnerable to denial-of-service attacks.

In order to avoid these attacks, the base specification uses IPSec Encapsulating Security Payload (ESP) to protect control traffic between the home agent and the mobile node. See figure 2.10. The biggest problem with the IPSec method is the key distribution. Key distribution of the IPSec, which is called Internet Key Exchange (IKE) [12], uses either pre-shared secrets or public keys in the key exchange. When authentication is needed between a MN and a HA, which must have some relationship in advance, because the MN uses services of the HA, the needed secrets might be exchanged beforehand or some private public key distribution can be utilized.

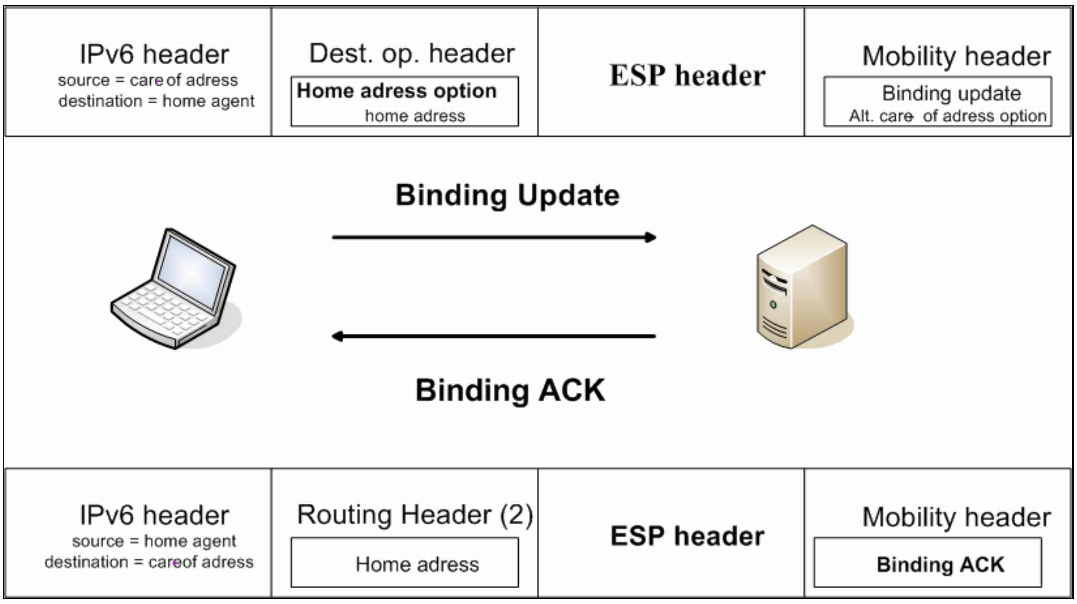


Figure 2.10 IPSec protected between MN and HA

2.4.5. Using RR Procedure to Protect MIPv6 Signaling Between MN and CN

A Mobile Node sends two messages: see Figure 2.11. One message is sent from its home address and the other message is sent from its care-of address. Respectively, the messages are called a *Home Test Init (HoTI)* message and a *Care-of Test Init (CoTI)* message. A Correspondent Node replies to both messages with a *Home Test (HoT)* message to the first and a *Care-of Test (CoT)* message to the second. These reply messages include values for tokens which are computed from addresses of the Mobile Node and secret information which is only kept in the Correspondent Node. A mobile node generates a shared secret from the two token values and puts a signature in a Binding Update message using the shared secret. This mechanism suggests that the home address and the care-of address are assigned to the same Mobile Node.

The Return Routability Procedure messages are used to validate the addresses. When a Mobile Node moves away from its home link, to a foreign link, it will obtain a care-of address it must use in all communication with other nodes. The Correspondent Node must verify that the home address and care-of address both represent the Mobile Node. The real return routability checks are the message pairs (Home Test, BU) and (Care-of Test, BU). The Home Test Init (HoTI) and Care-of Test Init (CoTI) packets are only needed to trigger the test packets, and the Binding Update message acts as a combined routability response to both of the tests. See as following:

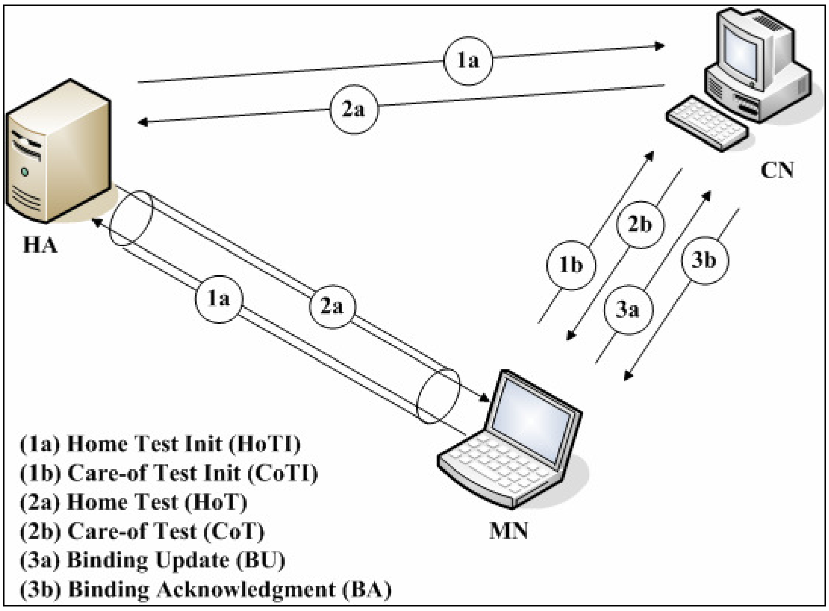


Figure 2.11 Return Routability Procedure

Home address check: The Home Address check consists of a Home Test (HoT) packet and a subsequent Binding Update. The HoT is assumed to be tunneled by the Home Agent to the Mobile Node. The HoT contains a cryptographically generated token. **home token =** $\mathbf{h(K_{cn}\backslash HoA\backslash n_i\backslash 0)}$, which is formed by calculating a hash function over the concatenation of a secret key K_{cn} known only by the Correspondent Node, the source address of the HoTI packet, and a nonce n_i. The index i is also included in the HoT packet and returned in the BU, allowing the correspondent node to easily find the appropriate nonce.

Care-of address check: From the Correspondent Node's point of view, the care-of address check is very similar to the Home address check, but the packet is sent directly to MN's CoA. Furthermore, the token is created in a slightly different manner in order to make it impossible to use home tokens for care-of tokens or vice versa *(***care-of token =** $\mathbf{h(K_{cn}\backslash CoA\backslash nj\backslash 1)}$). For the first Binding update, when the mobile node has received both the HoT and CoT messages, it creates a binding key **K_{bm}: Kbm = h (care-of token\home token)** by taking a hash function over the concatenation of the tokens received. This key is used to protect the first and the subsequent binding updates, as long as the key remains valid.

2.5 RR Procedure Problems

The Return Routability procedure was designed with the objective to provide a level of security that compares to that of today's non–mobile Internet. As we know the Return Routability procedure must repeated HoTI/HoT and CoTI/CoT. So the Return Routability procedure is vulnerable to attackers that are in a position where they can interpose, snoop and inject packets in the home or care-of address test. One possible attack against the Return Routability procedure is to pretend to be a neighboring node. To launch this attack, the mobile node established route optimization with some arbitrary correspondent node. While performing the Return Routability tests and creating the binding management key Kbm, the attacker uses its real home address but faked care-of address. Indeed, the care-of address would be the address of the neighboring node on the local link. The attacker is able to create the binding since it receives a valid Home Test normally, and it is able to eavesdrop on the Care-of Test, as it appears on the local link. This attack would allow the mobile node to divert unwanted traffic towards the neighboring node, resulting in a flooding attack.

2.6 Summary

This chapter introduces the basic Mobile IPv6 concepts and Mobile IPv6 terms. Among them we focus on Mobile IPv6 basic operation. Route Optimization technology provides a Mobile Node the opportunity to eliminate the inefficient triangle routing with its correspondent node and therefore, greatly improves the network performance. But unauthenticated or malicious Binding Update message would provide an intruder with an easy to launch various types of attack the security problem like False Binding Update Attack and Man-in-the-Middle Attack.

In order to prevent attacks the IETF proposed IPsec and Return Routability Procedure respectively to protect Home Registration and Correspondent Registration. In this chapter we presented the technique of the IPsec and Return Routability procedures and explained the mechanism to authenticate a Binding Update message.

In this Thesis we believe the IPsec provides enough safety for Home registration. But the Return Routability Procedure was designed with the objective a level of security that compares to that of today's non-mobile Internet. As such, it protects against impersonation, denial-of-service, and flooding threats that do not exist in the non-mobile Internet. Therefore, in order to prevent attack the Route Optimization should increase security.

CHAPTER 3

INVESTIGATING ENHANCED ROUTE OPTIMIZATION FOR MOBILE IPV6

In Mobile IPv6, Route Optimization enables a Mobile Node to directly communicate with a Correspondent Node while the Mobile Node moves. In order to provide lower handoff delays, increased security, and reduced signaling overhead, the IETF has created Enhanced Route Optimization for Mobile IPv6.

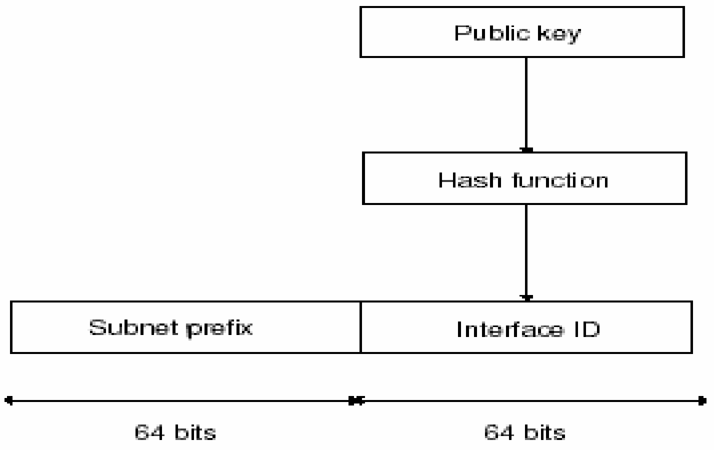
This chapter presents the investigation of Enhanced Route Optimization for Mobile IPv6 in detail. The background of Cryptographically Generated Addresses is presented in section 3.1. Section 3.2 shows how CGAs can be used to assist Route Optimization. An overview of Enhanced Route Optimization is given in section 3.3. Section 3.4 presents an evaluation of Enhanced Route Optimization. The summary is in section 3.5.

3.1 Cryptographically Generated Addresses Overview

A Cryptographically Generated Address (CGA) [7] aims at preventing address stealing (see figure 3.1) with a method for securely associating a cryptographic public key with an IPv6 address in the Secure Neighbor Discovery (SEND) protocol [13]. The basic idea is to generate the interface identifier (i.e., the rightmost 64 bits) of the IPv6 address by computing a cryptographic hash of the public key and some other parameters. The resulting IPv6 address is called a cryptographically generated address. The corresponding private key can then be used to sign messages sent from the address.

To verify the association between the address and the public key, the verifier needs to know the address itself, the public key, and the values of the auxiliary parameters. The verifier can then go on to verify messages signed by the owner of the public key (i.e., the address owner). No additional security infrastructure, such as a public key infrastructure (PKI), certification authorities, or other trusted servers, is needed.

Note that an attacker can always create its own CGA but he will not be able to spoof someone else's address since he needs to sign the message with the corresponding private key which is assumed to be known only by the real owner.



3.1 Cryptographically Generated Addresses

3.1.1 CGA Hash extension Theory and It's Component

In order to increase CGA security, IETF has created CGA Hash extensions [7] see figure 3.2. Each CGA is associated with public key and auxiliary parameters -- a security parameter (Sec) and a CGA Parameters data structure (CGAP). Figure 3.3 shows the format of CGAP. Sec is a 3-bit unsigned integer and determines the security strength against brute-force attacks. CGAP = (128-bit Modifier, 64-bit Subnet Prefix, 8-bit Collision Count, variable length public key, optional variable length Extension Fields). The process of generating a new CGA takes three input values: a subnet prefix, the public key of the address and the Sec. The output of the address generation algorithm is a new CGA and a CGAP. CGA verification takes as input an IPv6 address and a CGAP. The protocol for CGA generation is as follows:

1. Set the modifier field to a random 128-bit value.
2. Hash the concatenation of the modifier, 64+8 zero bits, and the encoded public key. The leftmost 112 bits of the result are Hash2.
3. Compare the 16*Sec leftmost bits of Hash2 with zero. If they are all zero (or if Sec=0), continue with Step (4). Otherwise, increment the modifier and go back to Step (2).
4. Set the collision count value to zero.
5. Hash the concatenation of the modifier, subnet prefix, collision count and encoded public key. The leftmost 64 bits of the result are Hash1.

6. Form an interface identifier by setting the two reserved bits in Hash1 both to 1 and the three leftmost bits to the value Sec.
7. Concatenate the subnet prefix and interface identifier to form a 128-bit IPv6 address.
8. If an address collision with another node within the same subnet is detected, increment the collision count and go back to step (5). However, after three collisions, stop and report the error.

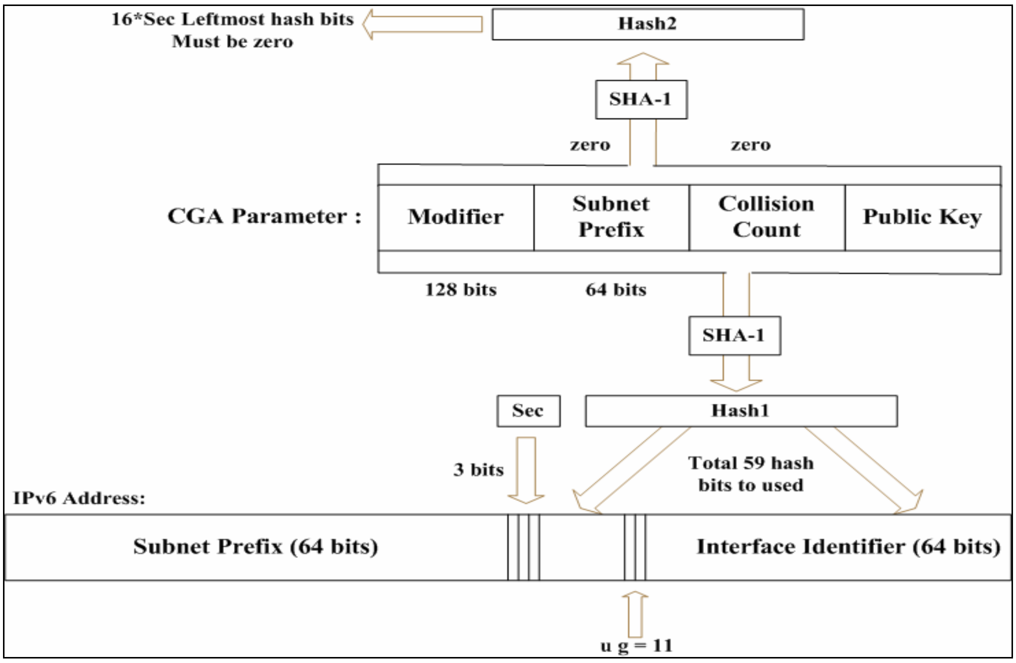


Figure 3.2 CGA Hash extension

Protocol for CGA verification is as follows:

1. Check that the collision count value is 0, 1 or 2, and that the subnet prefix value is equal to the subnet prefix (i.e. leftmost 64 bits) of the address. The CGA verification fails if either check fails.
2. Hash the concatenation of the modifier, subnet prefix, collision count and the public key. The 64 leftmost bits of the result are Hash1.
3. Compare Hash1 with the interface identifier (i.e. the rightmost 64 bits) of the address. Differences in the two reserved bits and in the three leftmost bits are ignored. If the 64-bit values differ (other than in the five ignored bits), the CGA verification fails.
4. Read the security parameter Sec from the three leftmost bits of the interface identifier of the

address.

5. Hash the concatenation of the modifier, 64+8 zero bits and the public key. The leftmost 112 bits of the result are Hash2.
6. Compare the 16*Sec leftmost bits of Hash2 with zero. If any one of these is nonzero, CGA verification fails. Otherwise, the verification succeeds.

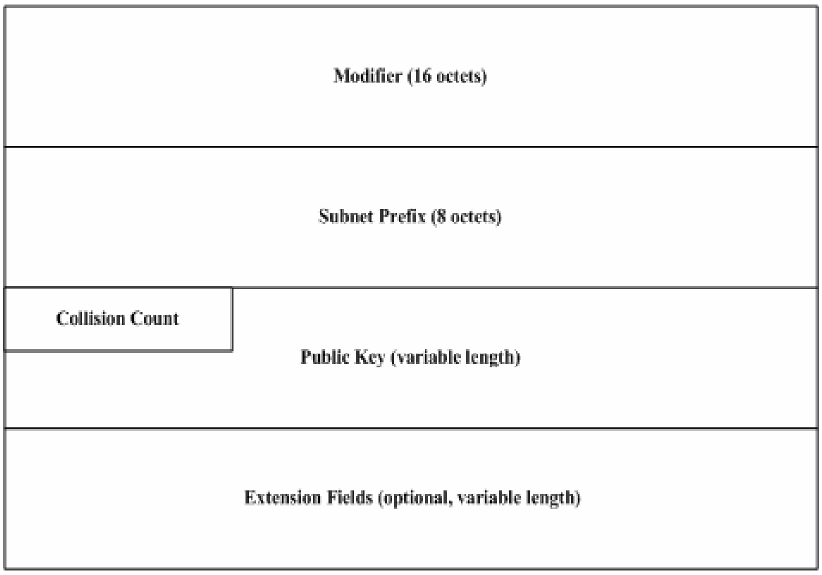

Modifier (16 octets)
Subnet Prefix (8 octets)
Collision Count
Public Key (variable length)
Extension Fields (optional, variable length)

Figure 3.3 CGA Parameters Format

3.1.2 Digital Signature Theory

In cryptography, a digital signature is a type of asymmetric cryptography used to simulate the security properties of a signature in digital, rather than written, form. Digital signature schemes normally give two algorithms, one for signing which involves the user's secret or private key, and one for verifying signature which involves the user's public key. The output of the signature process is called the "digital signature." Digital signatures, like written signatures, are used to provide authentication of the associated input, usually called a "message." Messages maybe anything, from electronic mail to a contract, or even a message sent in a more complicated cryptographic protocol. Digital signatures are used to create public key infrastructure (PKI) schemes in which a user's public key is tied to a user by a digital identity certificate issued by a certificate authority. PKI schemes attempt to unbreakably bind user information to a public key can be used as a form of identification.

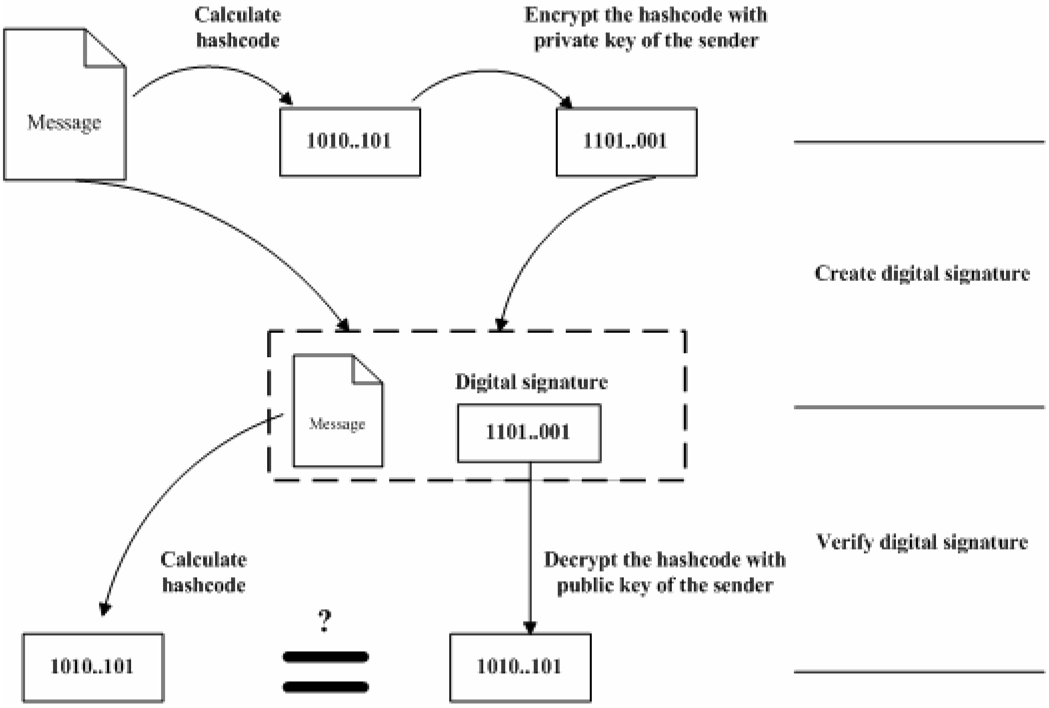


Figure 3.4 The procedure of Digital Signature

To create a digital signature see figure 3-4:

1. Calculate the hash value *h* of message *m*, using a hash function (one-way hash function) *H*: *H (m) = h.*

2. Encrypt the hash value using the private key *p* to create the digital signature *s : E(p,h) = s.*

3. Send the message with the digital signature appended.

The receiver verifies the authenticity and integrity of the message:

1. Calculate the hash value *h'* over the received message excluding the signature: *H (m) = h'*

2. Decrypt the digital signature s using the public key *q* to recover the sent hash value: *D (q,s) = h.*

3. Compare h with h'. If they are identical, then the contents of the message have not been changed, and only the encryptor, the owner of the private key, could have generated the message.

3.2 The Use of CGAs in Enhanced Route Optimization

The purpose of HoTI/HoT is ensuring packets can only be redirected by the legitimate recipient. The legitimate recipient is identified through the home address, and only the legitimate recipient is expected to receive the Home Keygen Token sent to the home address.

CGA can provide the same functionality without sending a packet to the home address. A node that uses a CGA at a certain time can prove at a later time that it is still the same node when it uses this CGA again. But instead of relying on a routing property, as with the home-address test, this proof can be drawn from the CGA's special interface identifier. The CGA owner signs important packets with its private key and includes its public key along with the auxiliary data in these packets. Since it is computationally hard to produce another public/private-key pair that hashes to the same CGA, the recipient of the signed message can verify, by recomputing the hash and comparing it with the CGA's interface identifier, that the sender must be the legitimate owner of this CGA.

Enhanced Route Optimization (ERO) uses a CGA rather than use HoTI/HoT to prove the ownership of Mobile Node's home address. A mobile node uses a CGA as its home address, and it signs BUs with its private key. The correspondent node can thus verify that the BU is from the same mobile node that used this home address before. Unfortunately, HoTI/HoT are still required to prove the association with the prefix in the home address because CGA does not ensure that a mobile node can indeed receive packets at the home address it claims to own. This property could be misused for a flooding attack against the home network.

ERO attends to these problems by combining CGAs with HoTI/HoT and CoTI/CoT. A HoT is performed at first contact between a Mobile Node and a Correspondent Node. This test verifies that the mobile node is the legitimate owner of the home address. Since the home address is cryptographically generated, the correspondent node will recognize the mobile node as the owner of this home address during subsequent registrations without having to do the home address test again.

But CGA-based authentication involves public-key cryptography and is hence computationally much less efficient than authentication through a shared secret key. ERO proposes use an initial CGA-based authentication to securely exchange a secret Permanent Home

Keygen Token (PHKT) between a mobile node and correspondent node.

3.3 Enhanced Route Optimization

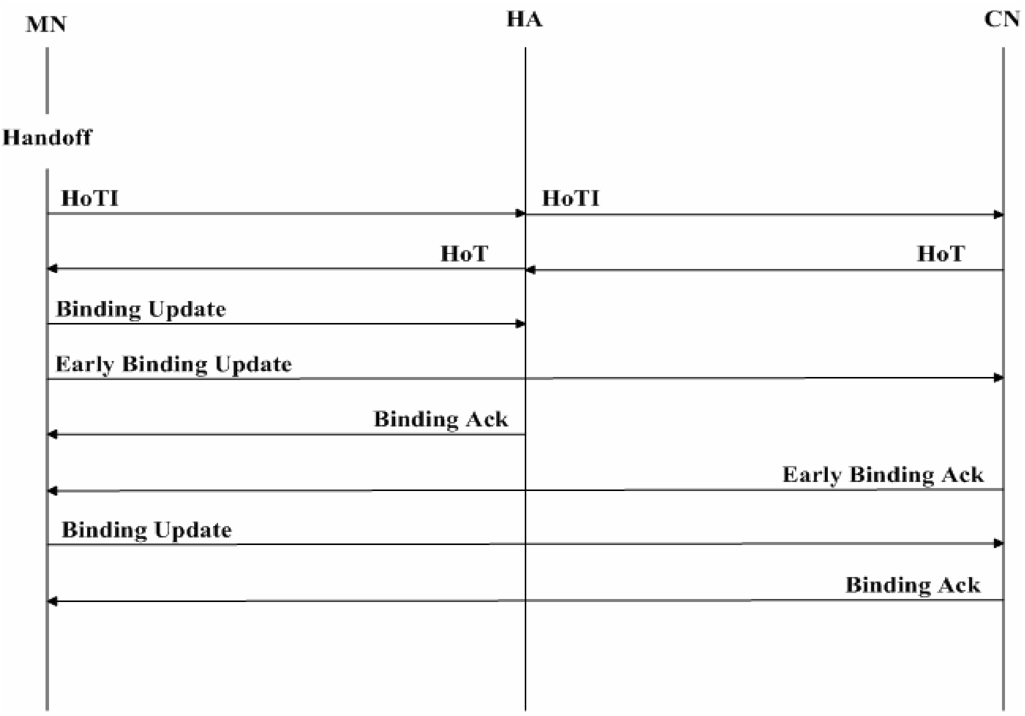


Figure 3.5 HoTI/HoT process after MN handoff

In the Standard RR procedure, the BU is delayed until both the HoTI/HoT and CoTI/CoT tests complete. The HoTI/HoT may itself be delayed until the Home Agent has been informed (using a BU protected and authenticated using IPsec [2]) of the new location of the Mobile Node. An aggressive Mobile Node however can send the HoTI packet immediately after the Home Agent BU is transmitted, trusting the network to deliver the packets in order, and the Home Agent to accept and process the BU ready for the following HoTI. Arkko, Vogt and Haddad [5] claim that Mobile Node should not be aggressive this way, the justification being the possible loss of the HoTI/HoT messages. This however seems to be a small price to pay if we assume that usually the BU at the Home Agent is successfully processed and the gain when it is is significant. Regardless, the HoTI/ HoT combination will almost always limit the timing of the BU to the Correspondent Node. Both HoTI/HoT and CoTI/CoT involve a round trip between Mobile Node and Correspondent node, but the HoTI/HoT takes a detour via the Home Agent, so it should normally be slower than the CoTI/CoT.

Moreover, ERO allows a correspondent node to send payload packet to a mobile node's new care-of address before the mobile node has been found to be reachable at the care-of address. When the mobile node changes IP connectivity, it first updates its binding at the correspondent node to the new care-of address without providing a proof of reachability [21]. However without additional protection this would enable an attacker to trick a correspondent node into temporarily redirecting payload packets, which would otherwise be addressed to the attacker itself, to the IP address of a victim. ERO through the use of Credit-Based Authorization protects against attack [21] by limiting the amount of data that will be sent to the CoA before it is verified.

ERO uses a CGA to validate the mobile node's home address and request a concurrent care-of address test for increase handoff efficiency. In figure 3.5, after the mobile node changed IP connection, it performed HoTI/HoT. However, the HoTI/HoT may be performed before the mobile node changed location as in figure 3.6. In order to remove another delay source, ERO permits deferred CoTI/CoT—actually performing the CoTI as an option in the first BU which is called Early Binding Update (EBU) [5] and with the CoT merged with the Early Binding Acknowledgement (EBA). The BA or EBA that follows the CGA protected BU carries the PHKT, which is used to authenticate future BUs from this Mobile node to the same correspondent node, Figure 3.7 shows the formats of the various packets.

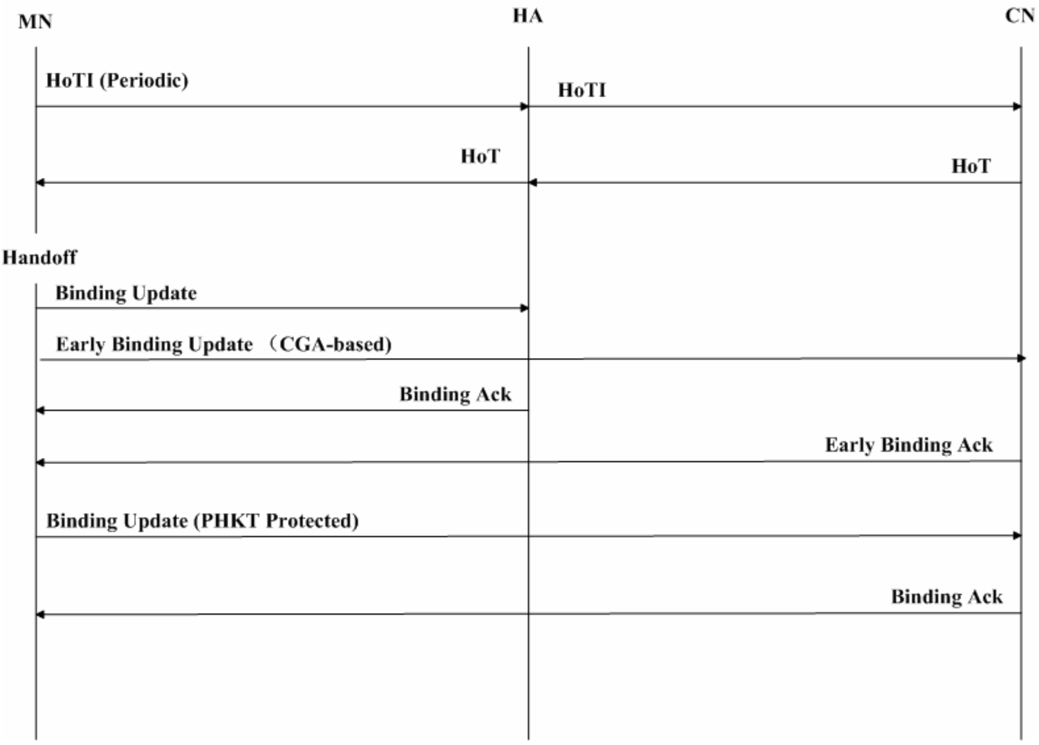


Figure 3.6 HoTI/HoT process before MN Handoff

To avoid attacks upon an unauthenticated victim care-of address, a Correspondent Node processing a deferred CoT limits the amount of data it will send to the Mobile Node’s care-of address. This is known as Credit Based Authentication (CBA) and means that the Correspondent node does no more harm to a victim at the care-of address than the Mobile node could have done by sending its packets directly at the care-of address.

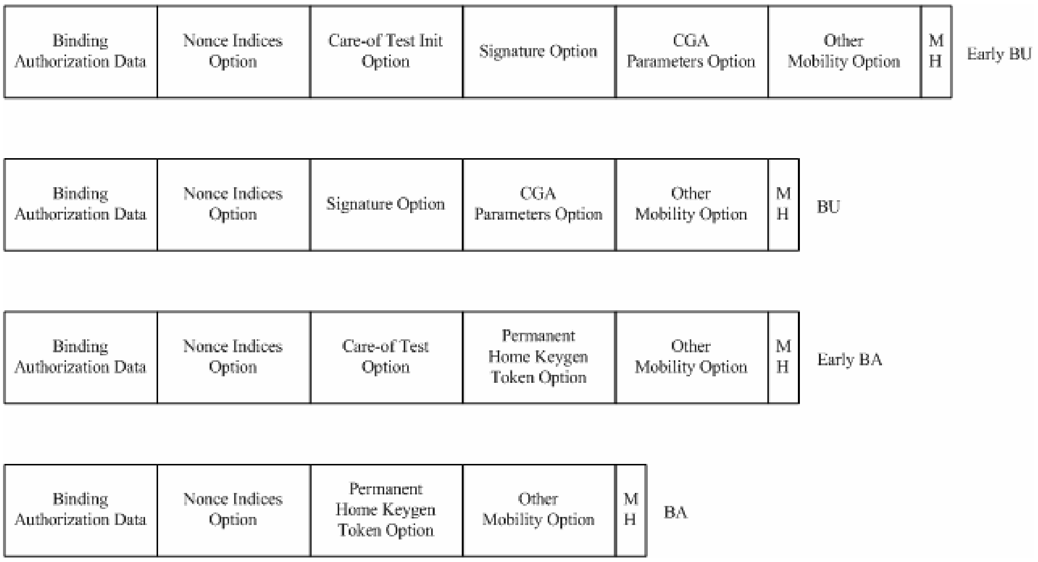


Figure 3.7 ERO's BU/BA Format

3. 4 Evaluation of Enhanced Route Optimization

It is clear that for the first BU to a particular Correspondent Node (before the permanent token is obtained) to gain any performance enhancement the HoTI/HoT sequence must have completed before movement. Otherwise the delay waiting for this process (particularly if the aggressive process is not adopted) would allow the CoTI/CoT to occur, and the regular RR procedure would be just as quick, without either CGA Public Key computations or credit calculations.

ERO will benefit only if either HoTI/HoT can be performed before movement, or if we can expect the association between Mobile Node and Correspondent Node remain active for more than one movement event, so that subsequent movement Binding Updates reap the benefits established during the first. To send proactive HoTI/HoT the mobile node could commence this procedure as soon as an association with a Correspondent Node is established, assuming that the mobile node will move before that association terminates, or in the words of [12] "The Mobile Node can invoke proactive home-address test on a just-in-time basis, if its link layer provides a trigger announcing imminent handoff." While certainly plausible with certain link level technologies, imminent handoff trigger events are not something we have encountered in practice, and even if one was to occur, we cannot see how we could conclude from link layer handover that IP layer mobility will occur, just that it might.

In practice a Mobile Node that does not anticipate long continuous associations (through multiple movements) with most Correspondent Nodes, and that desires the speedy ERO handovers will need to perform early HoTI/HoT exchanges with relevant Correspondent Nodes. Further, since Mobile IP processing is typically (by design) well separated from the applications, there generally is no knowledge of which Correspondent Nodes need speedy handover, or which may remain associated for lengthy periods and thus expect to remain existing when any motion occurs. Thus, in practice, the mobile node is likely to simply perform the HoTI/HoT tests whenever a new Correspondent Node association is formed, and then repeat that before the expiry of the lifetime of the returned token, or perform an early no-motion BU to obtain a "permanent token" [21].

There is also no way to distinguish a Mobile Node from any other node which is "mobile" in the Mobile IP sense which merely implies that the node's address has altered. Often this will be because the node has physically moved, but there are other causes. All nodes should be able to benefit from the Mobile IP procedures, not just the portable ones. The effect of thousands or millions of nodes performing HoTI/HoT exchange with the more popular internet servers, even if those servers refuse to participate needs further study.

To determine the effectiveness of ERO we need to determine the practicality of performing the HoTI/HoT sequence before the Mobile Node moves, the effectiveness of the CBA scheme, and evaluate the cost of using CGA with the associated RSA[38] Public Key algorithms. To avoid repeating the computations involved in authenticating using CGAs, ERO instead uses the Public key provided with CGA to encrypt and send from the Correspondent Node to the Mobile Node a secure token that can be used in later exchanges to authenticate BUs without any Public Key computation costs. While the specification does not specifically suggest it, we have implemented a mode of early BU (a de-registration without previous registration) that allows this "Permanent" token to be obtained before the mobile node moves. See Figure 3.8. This allows the periodic HoTI/HoT sequence to be halted whereas normally the lack of security in those messages requires frequent repetition to lessen the effects of packet snooping attacks.

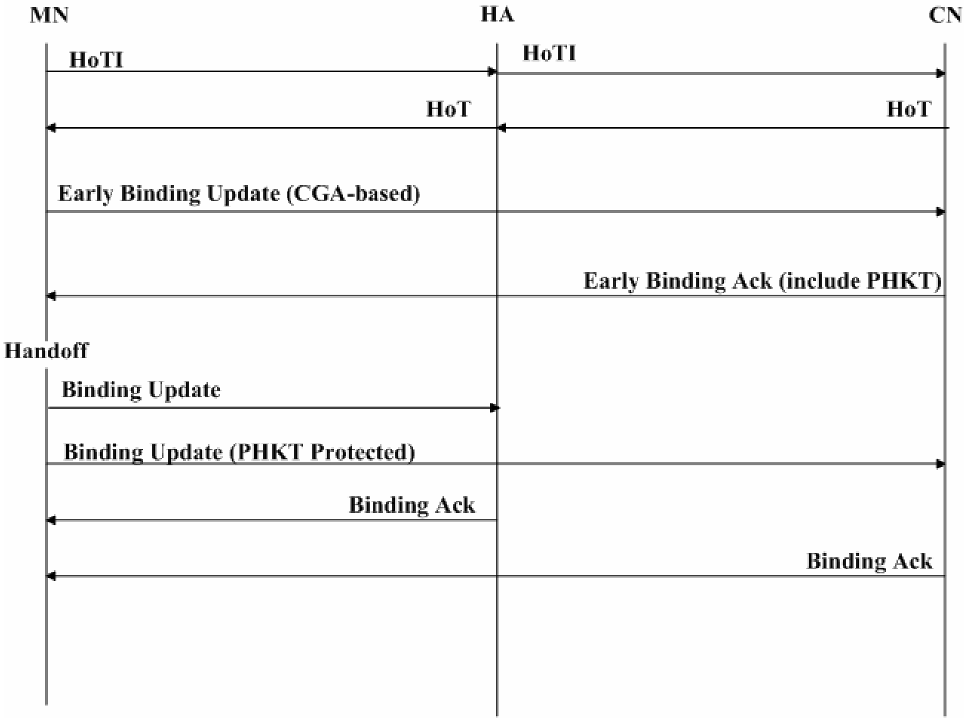

MN
HA
CN
HoTI
HoTI
HoT
HoT
Early Binding Update (CGA-based)
Early Binding Ack (include PHKT)
Handoff
Binding Update
Binding Update (PHKT Protected)
Binding Ack
Binding Ack

Figure 3.8 Early BU Process before handoff

3.5 Summary

In this section, we presented Enhanced Route Optimization for Mobile IPv6. ERO applies Cryptographically Generated Addresses (CGAs) to improve security and reduce handover delay. However the use of CGAs requires computationally expensive algorithms. This may be an issue for small mobile devices with low processing power. It might be a problem for correspondent nodes that simultaneously communicate with a large number of mobile nodes, such as publicly accessible servers. We evaluated ERO for Mobile IPv6 and proposed Permanent Home Keygen Token (PHKT) process before handoff that may remove the need for frequent HoTI/HoT exchanges.

CHAPTER 4

MOBILE IPv6 TESTBED AND TESTING

Today many people wish to deploy and gain experience of Mobile IPv6 in order to help realize the new mobile applications and services of the next generation Internet [2]. Mobile IPv6 implementations have begun to appear since1998. There are many Mobile IPv6 implementations [24, 25] which include KAME, Cisco, MIPL, Monarch, NEC, 6WINDGate, NUS, ULANC MIPv6, Bull, Nokia, Ericsson, SFC-MIP6 and Microsoft. This chapter describes our Mobile IPv6 Testbed. We started by selecting a Mobile IPv6 implementation Program [24□ 25]. We found the KAME-SHISA open source project [26] is the best choice for MIPv6 implementation and is good for our future research. Then we designed, deployed and tested a Testbed network using KAME-SHISA. When testing the Testbed network we focus on the Mobile IPv6 basic operation performance, Route Optimization and Return Routability Procedure.

The equipment and software is presented in section 4.1 along with the network topologies designed and deployed. The testing and results are in section 4.2. The summary is in section 4.3.

4.1 Test Deployment of Mobile IPv6

4.1.1 Equipment and Software

For the requirements of this work, a simple Testbed mobile IPv6 network is all that is required. This Testbed consists of three FreeBSD nodes playing the roles of the Mobile Node, Home Agent and Correspondent Node. Sometimes we may pick up some wireless node by way of an access point but in our Testbed that not necessary.

KAME [26] is a big project containing all of the IPv6 implementation including the SHISA [26] project which is the name of the Mobile IPv6 implementation. When this project started, we chose the last version of Mobile IPv6 implementation which is kame-20061106-FreeBSD. For details of Equipment and software used see table 4.1.

Testbed Component	Software
Home Agent (Router HA) CPU pentium2 400HZ; 256MB RAM ;40G hard disc	Freebsd 5.4-RELEASE and kame-20061106-freebsd54
Mobile Node (MN) CPU pentium4 2.8GHZ; 1G RAM; 80G hard disc	Freebsd 5.4-RELEASE and kame-20061106-freebsd54
Correspondent Node (CN) CPU pentium4 2.8GHZ; 512MB RAM; 80G hard disc	Freebsd 5.4-RELEASE and kame-20061106-freebsd54

Table 4.1 Equipment and software of nodes

SHISA consists of several user space programs and the modified kernel [39] programs. Table 4.2 shows the programs used by the SHISA stack [39] and Table 4.3 lists the necessary program modules used by each type of node.

mnd	Mobile Host Functions
had	Home Agent Functions
cnd	Route Optimization Function
babymdd	A simple movement detector
mrd	Mobile Router Functions
nemonetd	Tunnel setup for NEMO BS
Kernel	Forwarding, tunneling processing

Table 4.2 SHISA consists of 6 programs

Based on the node type, one or several SHISA programs run on a node. In addition, a user can choose to drop or replace functions by stopping or changing programs. In other words users can have modified function run the same node type.

Node type	**Used Program**
Mobile Node	mnd babymdd cnd
Home Agent	had cnd
Correspondent Node	cnd

Table 4.3 SHISA programs categorized by the node types

4.1.2 Network Design

We require only a simple network design able to implement and test our work, so we have implemented the minimum MIPv6 network as described above. Figure 4.1 shows the architecture.

To allow the mobile node to move, we require at least two attachment points. We use PC-based IPv6 routers instead of commercial IPv6 routers to allow the latest IPv6 features to be easily deployed.

The resulting network requires just three computers, a hub, and several cables. One node acts as both router and home agent. Another is the mobile node, attaching to the router/HA via either a “home” or “foreign” link. Motion is simulated by moving the Ethernet cable so the node attaches to the other link. The third node acts as correspondent node and attaches to a third network at the router.

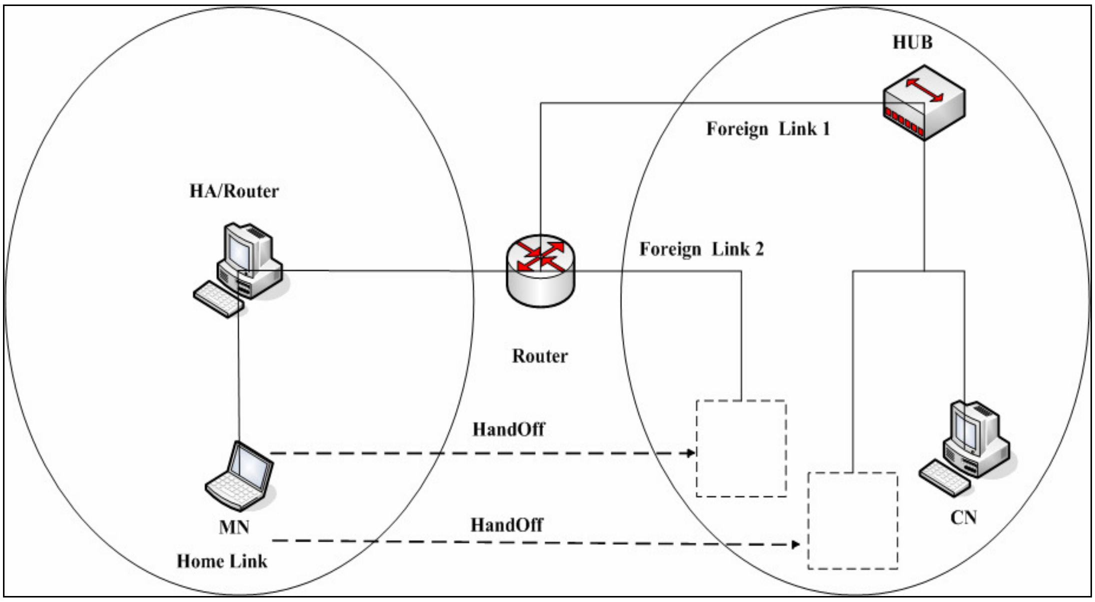


Figure 4.1 Mobile IPv6 Testbed architecture

4.1.3 Network Configuration

The Testbed Network was configured to use IPv6 exclusively. The configuration of Testbed is as follows:

1. The Home link is assigned the network prefix **2005:ffff:cafe:babe:: /64**
2. The Foreign link 1 is assigned the network prefix **2005:ffff:ffff:face:: /64**
3. The Foreign link 2 is assigned the network prefix **2005:ffff:feed:face:: /64**
4. The Mobile Node is assigned the address **2005:ffff:cafe:babe::b**
5. The Home Agent's home interface address is **2005:ffff:cafe:babe::a**
6. The Correspondent Node's address is **2005:ffff:ffff:face:213:d4ff:fef2:3a50**

4.1.4 Host Configure (Mobile Node, Home Agent, Correspondent node)

1. Mobile Node: The Mobile Node configuration is different than other nodes, the home address is configured on the pseudo interface **mip.** The Home address is also assigned to the physical interface attached to the home network while the Mobile Node is at home. When the Mobile Node moves to a foreign network, the home address cannot stay there. Instead the **mip** pseudo interface is defined as a placeholder for the home address and as a virtual home interface.

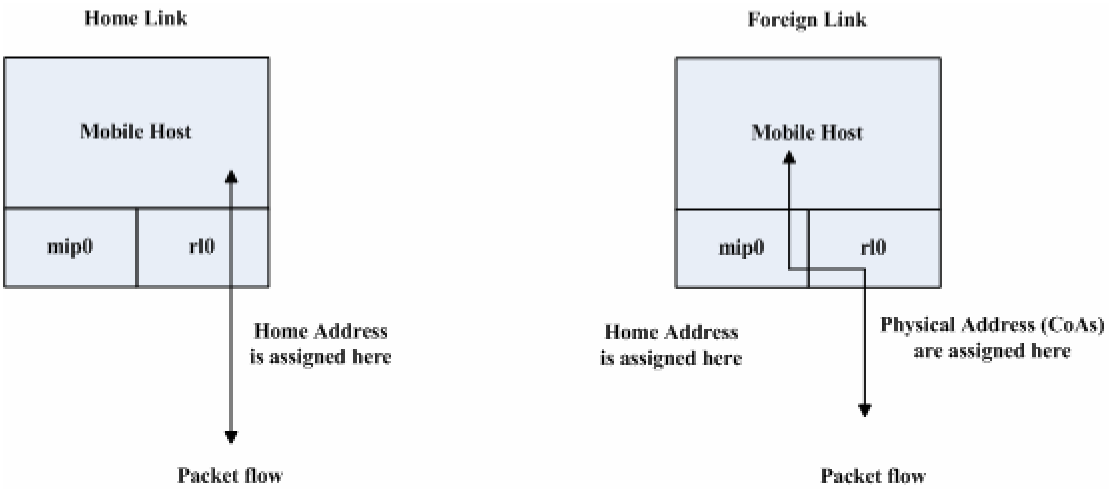

Home Link
Mobile Host
mip0
rl0
Home Address is assigned here
Packet flow
Foreign Link
Mobile Host
mip0
rl0
Home Address is assigned here
Physical Address (CoAs) are assigned here
Packet flow

Figure 4.2 Mobile Node interfaces

When the Mobile Node is at home, all packets are sent to physical addresses (home address) rl0 of the Mobile Node, the virtual interface is not used. But when the Mobile Node is at a foreign link all packets are sent to the mobile node’s physical address (care-of address) and then delivered to the virtual interface (**mip** interface) where the home address is assigned. So at the Mobile node the /etc/rc.conf configuration is as follows:

```
ipv6_enable = “Yes”
ipv6_gateway_enable= “No”
ipv6_network_interfaces = “rl0 mip0”        (mip0 is the Pseudo interface)
ipv6_ifconfig_rl0 = “up”          (rl0 is the Ethernet card interfaces)
ipv6_ifconfig_mip0 = “2005:ffff:cafe:babe::b home”
```

```
ipv6_mobile_enable = “YES”
  ipv6_mobile_nodetype = “mobile_node”
  ipv6_mobile_security_enable = “NO”     (Configure IPSec)
```

2. Home Agent: In our Testbed home agent not only provides home agent function but also provides the router functions between all networks, so three Ethernet network cards exist in the home agent. The interfaces are xl0, rl0 and pcn0. The detailed configuration of the home agent /etc/rc.conf is as follows:

```
ipv6_enable = “YES”
ipv6_gateway_enable = “YES”
ipv6_router_enable = “YES”
ipv6_router = “/usr/local/v6/sbin/route6d”
rtadvd_enable = “YES”
rtadvd_interfaces = “xl0 rl0”
ipv6_network_interfaces = “pcn0 xl0 rl0”
ipv6_ifconfig_pcn0 = “2005:ffff:cafe:babe::a prefixlen 64”      (home link interface)
ipv6_ifconfig_xl0 = “2005:ffff:cafe:feed:face::2 prefixlen 64” (foreign link 1 interface)
ipv6_ifconfig_rl0 = “2005:ffff:ffff:face::1 prefixlen 64” (foreign link 2 interface )
ipv6_mobile_enable = “YES”
ipv6_mobile_nodetype = “home_agent”
ipv6_mobile_home_interface = “pcn0”
ipv6_mobile_security_enable = “NO”
```

3. Correspondent Node: In a Mobile IPv6 network, each IPv6 node that communicates with a mobile node is called a correspondent node. If a correspondent node wants to support route optimization it needs to add mobile IPv6 function for which the configuration is as follows:

```
  ipv6_enable = “Yes”
  ipv6_gateway_enable= “No”
  ipv6_network_interfaces = “rl0”
  ipv6_ifconfig_rl0 = “2005:ffff :ffff :face: 213:d4ff:fef2:3a50”
  ipv6_mobile_enable = “YES”
ipv6_mobile_nodetype = “correspondent_node”
```

4.2 Testing and Result

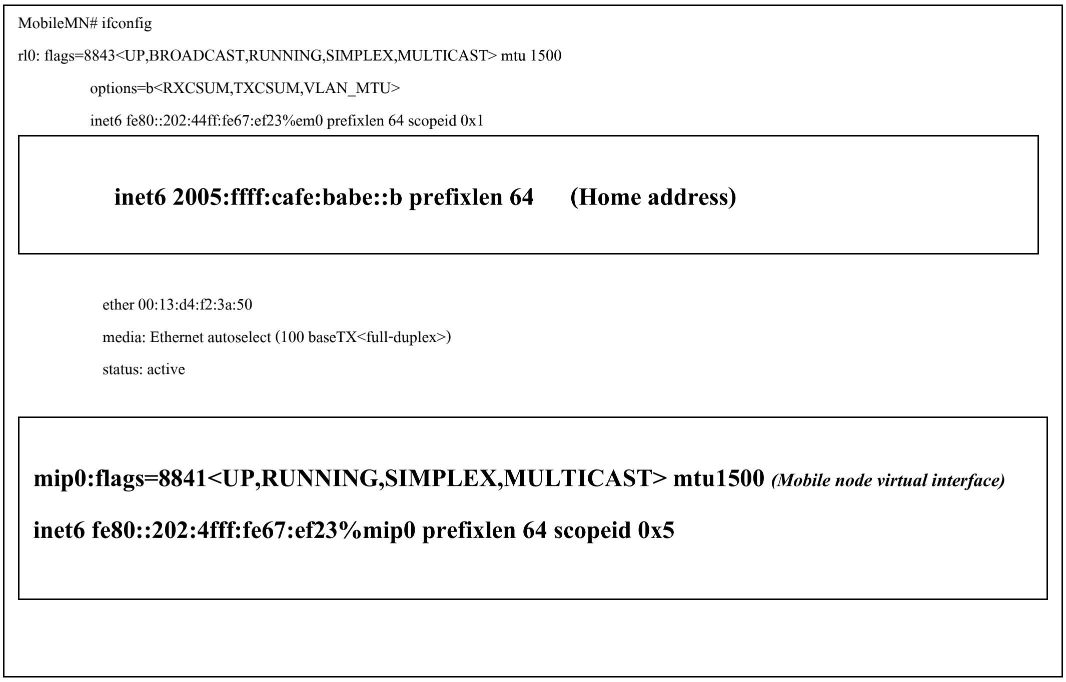
4.2.1 Testing Process

The first step is to determine whether all of the basic mobile IPv6 functionality is correctly operating. We observe this using the following methods:

1. Mobile Node assigns a home address to one of its **mip** interfaces.
2. Every node has system log (**syslog** [30]) files can which record the Mobile IPv6 daemon (**mnd, had, cnd**) information and status.
3. Using the Telnet protocol, the management ports of the daemon processes can be contacted and status extracted.
4. By using a network protocol analyzer ***Wireshark*** [40] **or** ***tcpdump*** [30, 41] data from the network can be captured and analyzed.

4.2.2 Testing Detail

With the Mobile Node at the home link**:** the Home address **2005:ffff:cafe:babe::b** is assigned to the physical interface. The virtual interface **mip0** has no address. When the mobile node is attached to its home link, an address is assigned to the physical interface, and mip virtual interface remains unused. See figure 4.3 for the configuration output.



```
MobileMN# ifconfig
rl0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 1500
          options=b<RXCSUM,TXCSUM,VLAN_MTU>
          inet6 fe80::202:44ff:fe67:ef23%em0 prefixlen 64 scopeid 0x1

      inet6 2005:ffff:cafe:babe::b prefixlen 64      (Home address)

           ether 00:13:d4:f2:3a:50
           media: Ethernet autoselect (100 baseTX<full-duplex>)
           status: active

mip0:flags=8841<UP,RUNNING,SIMPLEX,MULTICAST> mtu1500 (Mobile node virtual interface)
inet6 fe80::202:4fff:fe67:ef23%mip0 prefixlen 64 scopeid 0x5
```

Figure 4.3 IP address configuration of MN at home link

With the mobile node still connected to its home link we use the SSH [42] and Ping6 [30] programs to communicate with the Correspondent Node. At the same time one of the ***Wireshark*** or ***tcpdump*** programs is used to monitor this process. See figure 4.4, the Mobile Node gets its home address **2005:ffff:cafe:babe::b** from the home link **2005:ffff:cafe:babe::/64**. When the Mobile Node sends a packet to the Correspondent node, the source address of the packet is set to the home address of the Mobile Node. The destination address of the packet is the address of the Correspondent node **2005:ffff:ffff:face:213:d4ff:fef2:3a50**. When the correspondent node sends a packet to the Mobile Node, the source and the destination address are respectively set to the Correspondent node address and the home address. The Packet exchange while the Mobile Node is at the home link is just like an ordinary IPv6 network.

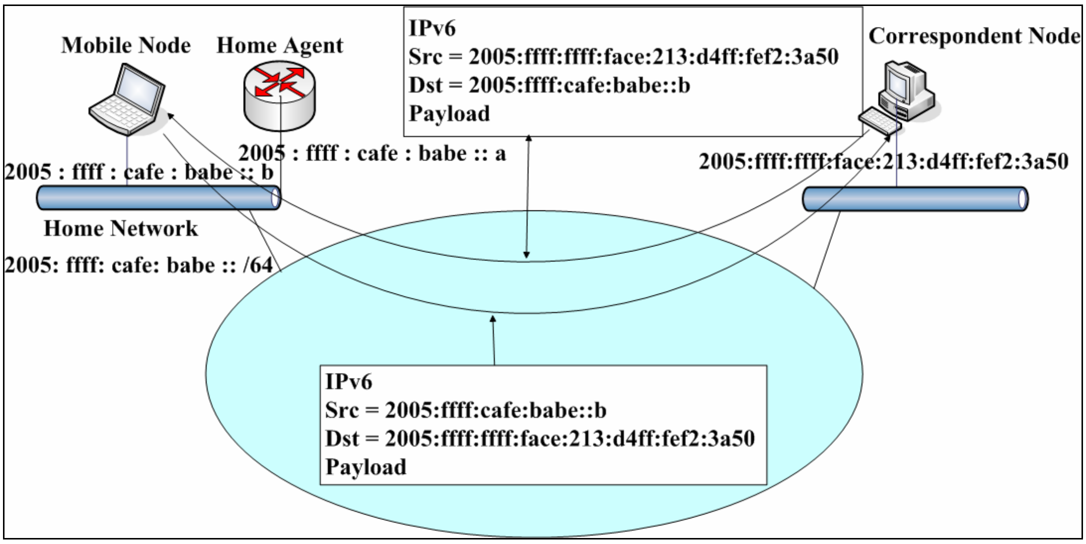

Mobile Node
Home Agent
IPv6
Src = 2005:ffff:ffff:face:213:d4ff:fef2:3a50
Dst = 2005:ffff:cafe:babe::b
Payload
Correspondent Node
2005 : ffff : cafe : babe :: a
2005 : ffff : cafe : babe :: b
2005:ffff:ffff:face:213:d4ff:fef2:3a50
Home Network
2005: ffff: cafe: babe :: /64
IPv6
Src = 2005:ffff:cafe:babe::b
Dst = 2005:ffff:ffff:face:213:d4ff:fef2:3a50
Payload

Figure 4.4 Packet exchange while a MN at home

Mobile Node Movement: When the Mobile Node moves to a foreign link there are two possible communication paths to the Correspondent Node. These are bi-directional tunnel mode and route optimization mode. The cnd daemon program provides Route Optimization function in the Correspondent Node. If the Correspondent Node has the cnd daemon running, route optimization is used, otherwise the mobile node falls back to tunnel mode.

When the Mobile Node moves to the foreign network, it is assigned the care-of address **2005:ffff:feed:face:202:4fff:fe67:ef23** from the foreign network, as shown in figure 4.5. The

Mobile node home address **2005:ffff:cafe:babe::b** moves to the ***virtual interface*** **mip0**, the care-of address is assigned to the physical interface.

```
MobileMN# ifconfig
rl0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        options=b<RXCSUM,TXCSUM,VLAN_MTU>
        inet6 fe80::202:4fff:fe67:ef23%em0 prefixlen 64 scopeid 0x1

inet6 2005:ffff:feed:face:202:4fff:fe67:ef23     prefixlen 64 autoconf ( care-of-address)

          ether 00:13:d4:f2:3a:50
          media: Ethernet autoselect (100 baseTX<full-duplex>)
          status: active

mip0:flags=8841<UP,RUNNING,SIMPLEX,MULTICAST> mtu 1500     (Mobile node virtual interface)
          inet6 fe80::202:4fff:fe67:ef23%mip0 prefixlen 64 scopeid 0x5
inet6 2005:ffff:cafe:babe::b prefixlen 64     (Home address)
```

Figure 4.5 IP address configuration of MN at Foreign link

Bi-directional Tunnel mode (no cnd daemon): When the Mobile Node and the Home Agent complete the exchange of binding information, these nodes create a bi-directional tunnel between the Home Agent and the Mobile Node. In this mode, packets from the Correspondent node are routed to the home agent **2005:ffff:cafe:babe::a** and then tunneled to the mobile node home address **2005:ffff:cafe:babe::b** via its current care-of address **2005:ffff:feed:face:202:4fff:fe67:ef23.** Packets to the Correspondent node are tunneled from the Mobile Node to the Home Agent (‘‘reverse tunneled’’) and then routed normally from the home network to the correspondent node. All of packets between the mobile node and the correspondent node must be routed via the home agent. More detail about this procedure can be seen in figure 4.6.

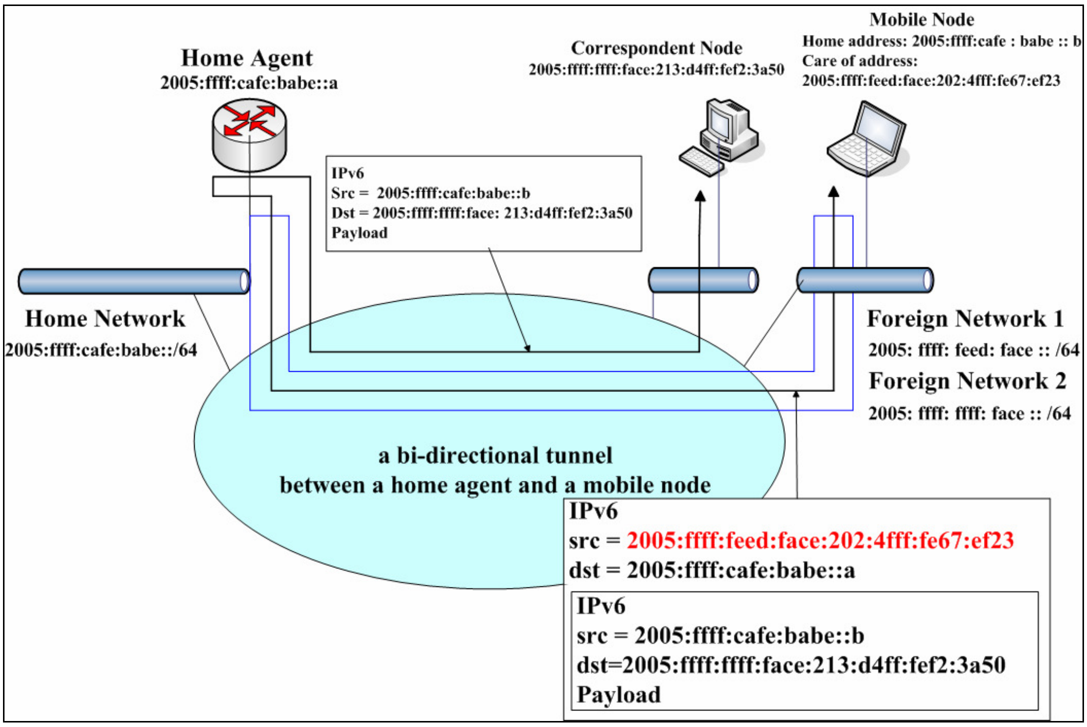

Home Agent
2005:ffff:cafe:babe::a
Correspondent Node
2005:ffff:ffff:face:213:d4ff:fef2:3a50
Mobile Node
Home address: 2005:ffff:cafe : babe :: b
Care of address:
2005:ffff:feed:face:202:4fff:fe67:ef23
IPv6
Src = 2005:ffff:cafe:babe::b
Dst = 2005:ffff:ffff:face: 213:d4ff:fef2:3a50
Payload
Home Network
2005:ffff:cafe:babe::/64
Foreign Network 1
2005: ffff: feed: face :: /64
Foreign Network 2
2005: ffff: ffff: face :: /64
a bi-directional tunnel
between a home agent and a mobile node
IPv6
src = 2005:ffff:feed:face:202:4fff:fe67:ef23
dst = 2005:ffff:cafe:babe::a
IPv6
src = 2005:ffff:cafe:babe::b
dst=2005:ffff:ffff:face:213:d4ff:fef2:3a50
Payload

Figure 4.6 Sending packets by a tunnel connection

Route Optimization (cnd daemon): The path between the Mobile Node and the Correspondent Node can be optimized allowing direct communication between Mobile Node and Correspondent Node. Before route optimization starts, the Mobile Node will initiate the Return Routability Procedure which is used to protect Route optimization security.

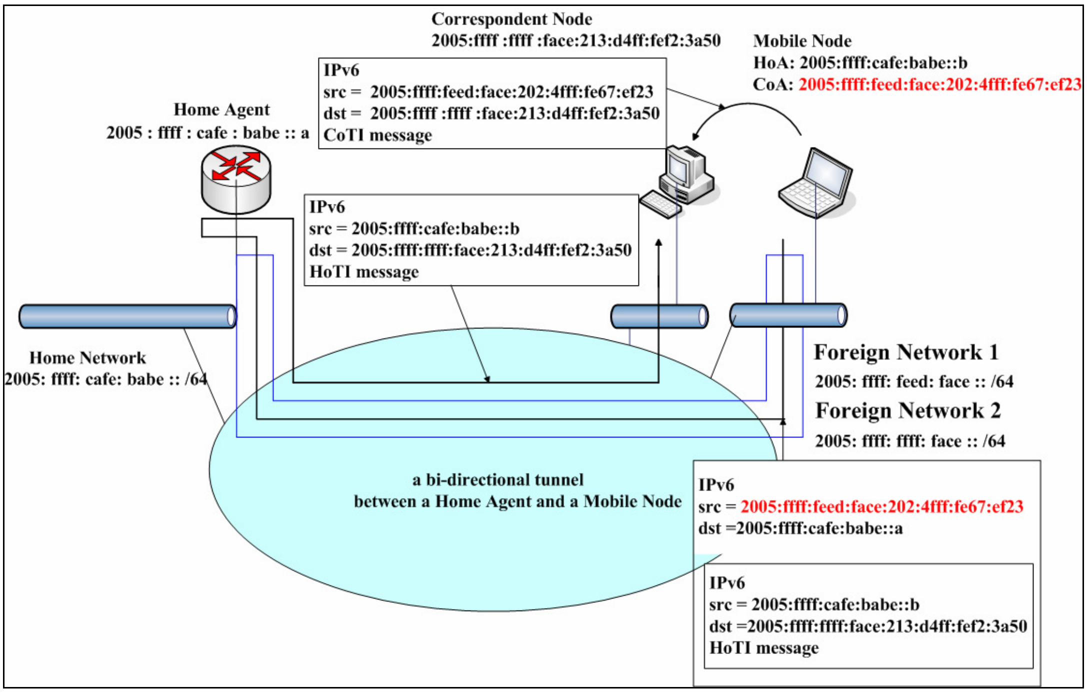
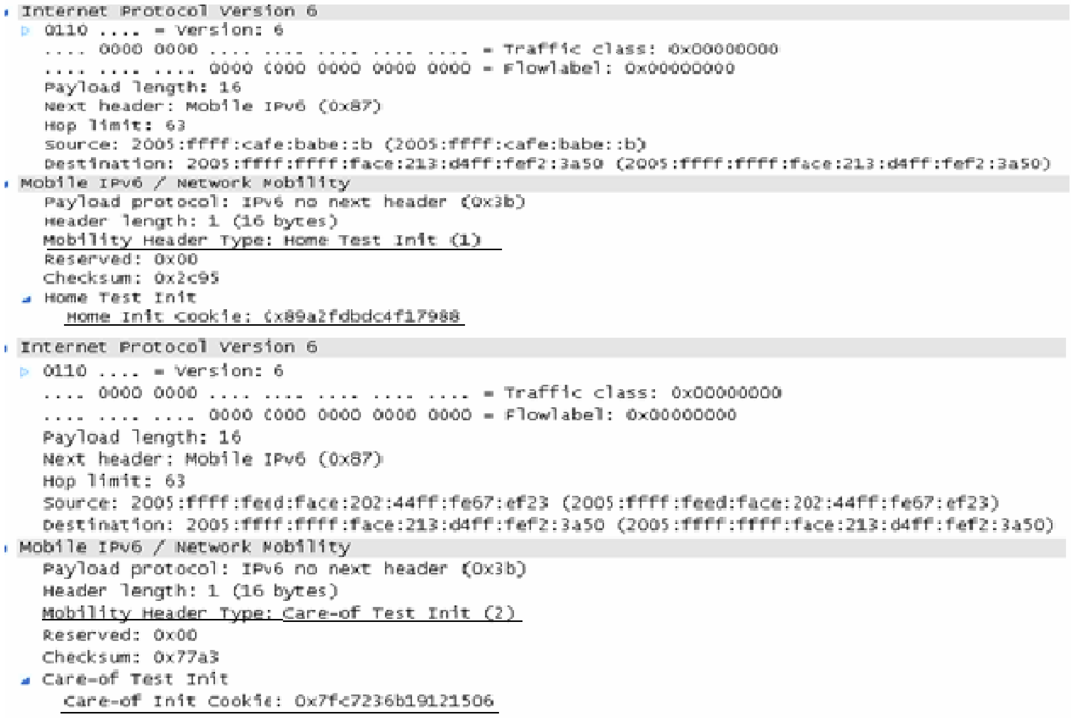

Correspondent Node
2005:ffff :ffff :face:213:d4ff:fef2:3a50
Mobile Node
HoA: 2005:ffff:cafe:babe::b
CoA: 2005:ffff:feed:face:202:4fff:fe67:ef23
IPv6
src = 2005:ffff:feed:face:202:4fff:fe67:ef23
dst = 2005:ffff :ffff :face:213:d4ff:fef2:3a50
CoTI message
Home Agent
2005 : ffff : cafe : babe :: a
IPv6
src = 2005:ffff:cafe:babe::b
dst = 2005:ffff:ffff:face:213:d4ff:fef2:3a50
HoTI message
Home Network
2005: ffff: cafe: babe :: /64
Foreign Network 1
2005: ffff: feed: face :: /64
Foreign Network 2
2005: ffff: ffff: face :: /64
a bi-directional tunnel
between a Home Agent and a Mobile Node
IPv6
src = 2005:ffff:feed:face:202:4fff:fe67:ef23
dst =2005:ffff:cafe:babe::a
IPv6
src = 2005:ffff:cafe:babe::b
dst =2005:ffff:ffff:face:213:d4ff:fef2:3a50
HoTI message

Figure 4.7 Mobile Node Sending Initial Messages

Return Routability Procedure: A Home Test Init (**HoTI**) message is sent from the home address **2005:ffff:cafe:babe::b** of the Mobile Node. Such a packet whose source address is a home address cannot be sent directly from a foreign network. The Home Test Init message is sent through a tunnel connection between the Mobile Node **2005:ffff:feed:face:202:4fff:fe67:ef23** and its Home Agent **2005:ffff:cafe:babe::a**. The correspondent node **2005:ffff:feed:face:213:d4ff:fef2:3a50** will receive the message as if it were sent from the home network of the mobile node as seen in Figure 4.7. A Care-of Test Init (**CoTI**) message is sent from the care-of address **2005:ffff:feed:face:202:4fff:fe67:ef23** of the mobile node. This message can be sent directly from the foreign network. To monitor this process we use the output in figure 4.8. We have marked, by underlining, the mobility header to highlight the message types, and to show the cookies transmitted.



```
Internet Protocol Version 6
  0110 .... = Version: 6
  .... 0000 0000 .... .... .... .... .... = Traffic class: 0x00000000
  .... .... .... 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
  Payload length: 16
  Next header: Mobile IPv6 (0x87)
  Hop limit: 63
  Source: 2005:ffff:cafe:babe::b (2005:ffff:cafe:babe::b)
  Destination: 2005:ffff:ffff:face:213:d4ff:fef2:3a50 (2005:ffff:ffff:face:213:d4ff:fef2:3a50)
Mobile IPv6 / Network Mobility
  Payload protocol: IPv6 no next header (0x3b)
  Header length: 1 (16 bytes)
  Mobility Header Type: Home Test Init (1)
  Reserved: 0x00
  Checksum: 0x2c95
  Home Test Init
    Home Init Cookie: 0x89a2fdbdc4f17988
Internet Protocol Version 6
  0110 .... = Version: 6
  .... 0000 0000 .... .... .... .... .... = Traffic class: 0x00000000
  .... .... .... 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
  Payload length: 16
  Next header: Mobile IPv6 (0x87)
  Hop limit: 63
  Source: 2005:ffff:feed:face:202:44ff:fe67:ef23 (2005:ffff:feed:face:202:44ff:fe67:ef23)
  Destination: 2005:ffff:ffff:face:213:d4ff:fef2:3a50 (2005:ffff:ffff:face:213:d4ff:fef2:3a50)
Mobile IPv6 / Network Mobility
  Payload protocol: IPv6 no next header (0x3b)
  Header length: 1 (16 bytes)
  Mobility Header Type: Care-of Test Init (2)
  Reserved: 0x00
  Checksum: 0x77a3
  Care-of Test Init
    Care-of Init Cookie: 0x7fc7236b19121506
```

Figure 4.8 Wireshark monitor Mobile Node sending Initial message

When the Correspondent Node receives a Home Test Init or a Care-of Test Init message from a Mobile Node, it replies to the Mobile Node with a Home Test message (**HoT**) or a Care-of Test(**CoT**) message. The Home Test message is sent to the home address, **2005:ffff:cafe:babe::b** of the Mobile Node. The message is delivered to the home network of the Mobile Node and intercepted by the home agent **2005:ffff:cafe:babe::a**. The Mobile Node receives the message from the tunnel connection between the node and its home agent. The Care-of Test message is sent to the care-of address **2005:ffff:feed:face:202:4fff:fe67:ef23** of the Mobile Node directly. Figure 4.9 shows this process.

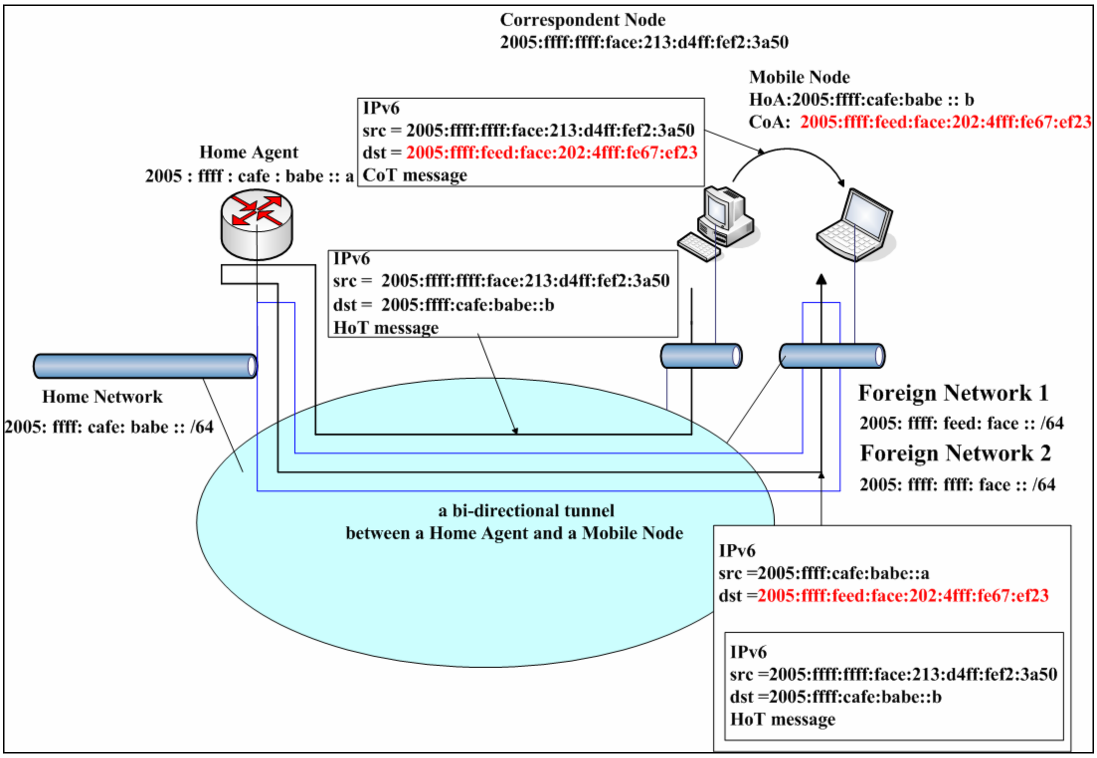
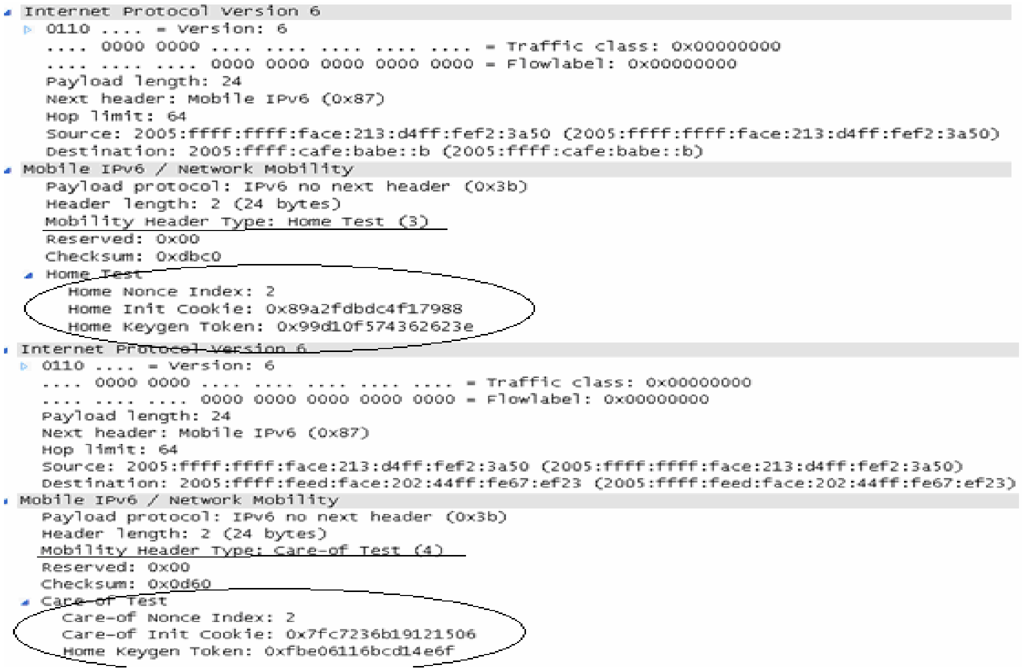

Correspondent Node
2005:ffff:ffff:face:213:d4ff:fef2:3a50
Mobile Node
HoA:2005:ffff:cafe:babe :: b
CoA: 2005:ffff:feed:face:202:4fff:fe67:ef23
IPv6
src = 2005:ffff:ffff:face:213:d4ff:fef2:3a50
dst = 2005:ffff:feed:face:202:4fff:fe67:ef23
CoT message
Home Agent
2005 : ffff : cafe : babe :: a
IPv6
src = 2005:ffff:ffff:face:213:d4ff:fef2:3a50
dst = 2005:ffff:cafe:babe::b
HoT message
Home Network
2005: ffff: cafe: babe :: /64
Foreign Network 1
2005: ffff: feed: face :: /64
Foreign Network 2
2005: ffff: ffff: face :: /64
a bi-directional tunnel
between a Home Agent and a Mobile Node
IPv6
src =2005:ffff:cafe:babe::a
dst =2005:ffff:feed:face:202:4fff:fe67:ef23
IPv6
src =2005:ffff:ffff:face:213:d4ff:fef2:3a50
dst =2005:ffff:cafe:babe::b
HoT message

Figure 4.9 CN sending responding message



```
Internet Protocol Version 6
  0110 .... = Version: 6
  .... 0000 0000 .... .... .... .... .... = Traffic class: 0x00000000
  .... .... .... 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
  Payload length: 24
  Next header: Mobile IPv6 (0x87)
  Hop limit: 64
  Source: 2005:ffff:ffff:face:213:d4ff:fef2:3a50 (2005:ffff:ffff:face:213:d4ff:fef2:3a50)
  Destination: 2005:ffff:cafe:babe::b (2005:ffff:cafe:babe::b)
Mobile IPv6 / Network Mobility
  Payload protocol: IPv6 no next header (0x3b)
  Header length: 2 (24 bytes)
  Mobility Header Type: Home Test (3)
  Reserved: 0x00
  Checksum: 0xdbc0
  Home Test
    Home Nonce Index: 2
    Home Init Cookie: 0x89a2fdbdc4f17988
    Home Keygen Token: 0x99d10f574362623e
Internet Protocol Version 6
  0110 .... = Version: 6
  .... 0000 0000 .... .... .... .... .... = Traffic class: 0x00000000
  .... .... .... 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
  Payload length: 24
  Next header: Mobile IPv6 (0x87)
  Hop limit: 64
  Source: 2005:ffff:ffff:face:213:d4ff:fef2:3a50 (2005:ffff:ffff:face:213:d4ff:fef2:3a50)
  Destination: 2005:ffff:feed:face:202:44ff:fe67:ef23 (2005:ffff:feed:face:202:44ff:fe67:ef23)
Mobile IPv6 / Network Mobility
  Payload protocol: IPv6 no next header (0x3b)
  Header length: 2 (24 bytes)
  Mobility Header Type: Care-of Test (4)
  Reserved: 0x00
  Checksum: 0x0d60
  Care-of Test
    Care-of Nonce Index: 2
    Care-of Init Cookie: 0x7fc7236b19121506
    Home Keygen Token: 0xfbe06116bcd14e6f
```

Figure 4.10 Wireshark monitor Mobile Node sending responding message

Figure 4.10 shows the HoT/CoT messages monitored by the wireshark software. It shows the Mobility Header type (underlined). We can also see the HoT/CoT message detail. The Home nonce Index and the Care-of Nonce Index are both 2, the Home Init and Care-of Init cookie are the same as in figure 4.8 which shows that Figure 4.10 is response to the HoTI/CoTI from figure 4.8. Moreover we also can see the Home Keygen Token data in both HoT and CoT messages which are generated by the correspondent node.

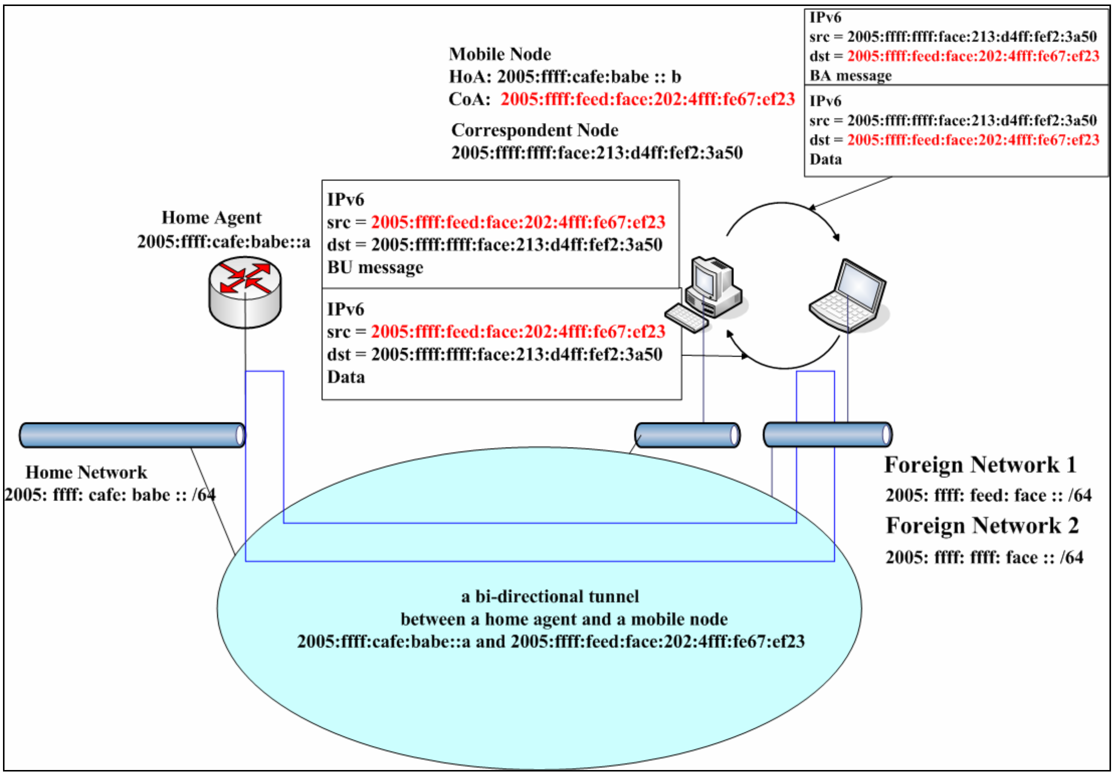
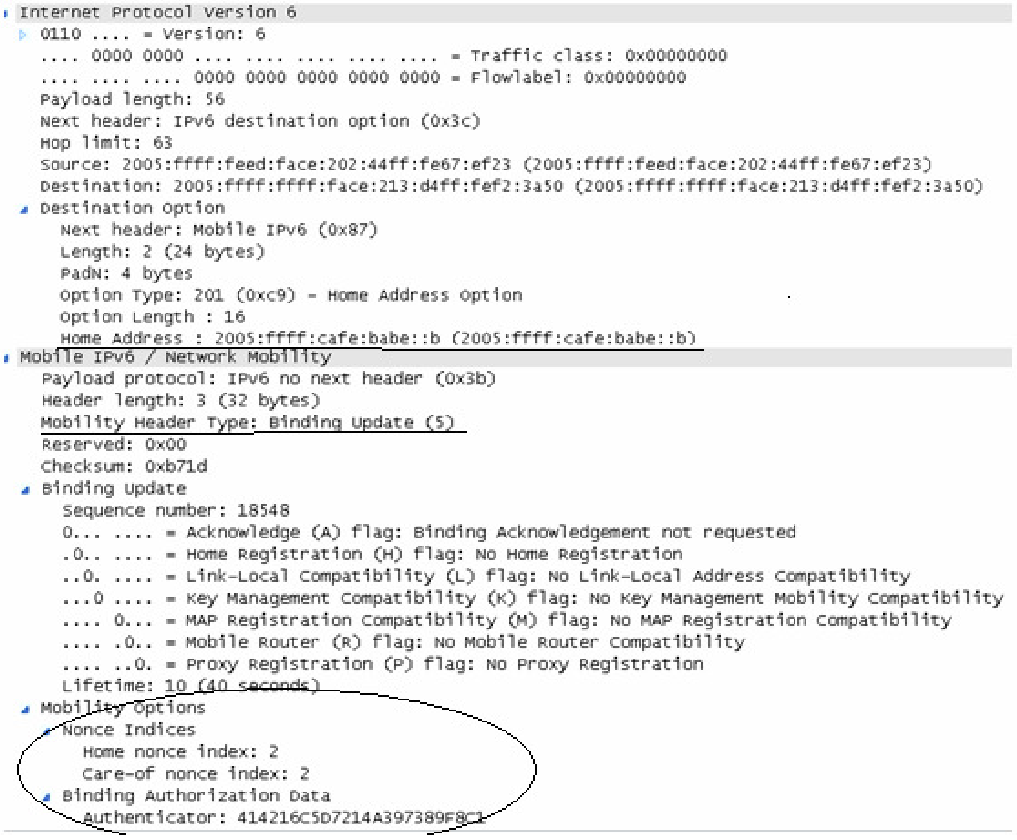

Mobile Node
HoA: 2005:ffff:cafe:babe :: b
CoA: 2005:ffff:feed:face:202:4fff:fe67:ef23
Correspondent Node
2005:ffff:ffff:face:213:d4ff:fef2:3a50
IPv6
src = 2005:ffff:ffff:face:213:d4ff:fef2:3a50
dst = 2005:ffff:feed:face:202:4fff:fe67:ef23
BA message
IPv6
src = 2005:ffff:ffff:face:213:d4ff:fef2:3a50
dst = 2005:ffff:feed:face:202:4fff:fe67:ef23
Data
Home Agent
2005:ffff:cafe:babe::a
IPv6
src = 2005:ffff:feed:face:202:4fff:fe67:ef23
dst = 2005:ffff:ffff:face:213:d4ff:fef2:3a50
BU message
IPv6
src = 2005:ffff:feed:face:202:4fff:fe67:ef23
dst = 2005:ffff:ffff:face:213:d4ff:fef2:3a50
Data
Home Network
2005: ffff: cafe: babe :: /64
Foreign Network 1
2005: ffff: feed: face :: /64
Foreign Network 2
2005: ffff: ffff: face :: /64
a bi-directional tunnel
between a home agent and a mobile node
2005:ffff:cafe:babe::a and 2005:ffff:feed:face:202:4fff:fe67:ef23

Figure 4.11 Directly send date packet between MN and CN

After the Return Routability procedure the Mobile Node directly sends the Binding Update message to the Correspondent Node telling the care-of address. See figure 4.11. After the binding update the correspondent sends a Binding Acknowledgement to the Mobile Node indicating the Binding Update success. Communication between the Mobile Node's care-of addresses **2005:ffff:feed:face:202:4fff:fe67:ef23** and the Correspondent Node **2005:ffff:ffff:face:213:d4ff:fef2:3a50** uses Route Optimization to directly send data to each other. Information from the wireshark monitor when the Mobile Node sends the BU message is given in figure 4.12. In the Mobility option, we can see both the nonce Index and Binding authorization data options.



```
Internet Protocol Version 6
  0110 .... = Version: 6
  .... 0000 0000 .... .... .... .... .... = Traffic class: 0x00000000
  .... .... .... 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
  Payload length: 56
  Next header: IPv6 destination option (0x3c)
  Hop limit: 63
  Source: 2005:ffff:feed:face:202:44ff:fe67:ef23 (2005:ffff:feed:face:202:44ff:fe67:ef23)
  Destination: 2005:ffff:ffff:face:213:d4ff:fef2:3a50 (2005:ffff:ffff:face:213:d4ff:fef2:3a50)
  Destination Option
    Next header: Mobile IPv6 (0x87)
    Length: 2 (24 bytes)
    PadN: 4 bytes
    Option Type: 201 (0xc9) - Home Address Option
    Option Length : 16
    Home Address : 2005:ffff:cafe:babe::b (2005:ffff:cafe:babe::b)
Mobile IPv6 / Network Mobility
  Payload protocol: IPv6 no next header (0x3b)
  Header length: 3 (32 bytes)
  Mobility Header Type: Binding Update (5)
  Reserved: 0x00
  Checksum: 0xb71d
  Binding Update
    Sequence number: 18548
    0... .... = Acknowledge (A) flag: Binding Acknowledgement not requested
    .0.. .... = Home Registration (H) flag: No Home Registration
    ..0. .... = Link-Local Compatibility (L) flag: No Link-Local Address Compatibility
    ...0 .... = Key Management Compatibility (K) flag: No Key Management Mobility Compatibility
    .... 0... = MAP Registration Compatibility (M) flag: No MAP Registration Compatibility
    .... .0.. = Mobile Router (R) flag: No Mobile Router Compatibility
    .... ..0. = Proxy Registration (P) flag: No Proxy Registration
    Lifetime: 10 (40 seconds)
  Mobility Options
    Nonce Indices
      Home nonce index: 2
      Care-of nonce index: 2
    Binding Authorization Data
      Authenticator: 414216C5D7214A397389F8C1
```

Figure 4.12 Wireshark monitor MN send BU message

4.3 Summary

This chapter presents the design and deployment of the Testbed network, and showed the correct operation of the Mobile IPv6 protocol using standard route optimization. We will use the same Testbed network to test the enhancement presented in the following chapter.

Chapter 5

IMPLEMENTATION AND TESTING

The investigation of Standard Route Optimization for Mobile IPv6 was presented in chapter 4. This chapter will describe the Enhanced Route Optimization implementation and testing. This chapter consists of experimental design in sections 5.1 and 5.2. The set up and network configuration are presented in section 5.3. Then the ERO implementation was tested and results are provided in section 5.4. Section 5.5 shows results of testing with large RSA keys. We conclude with a summary in section 5.6.

5.1 Overview of the Implementation

This part presents the prototype implementation of Enhanced Route Optimization for Mobile IPv6. The main focus is to apply Cryptographically Generated Addresses to Mobile IPv6 to improve security and reduce handover delays. The Mobile IPv6 implementation from KAME-SHISA [26] does not support ERO so we need modify the existing Mobile IPv6 implementation that works on FreeBSD, a Unix Operating system to add this new functionality. The original CGA implementation is for testing the Secure Neighbor Discovery (SEND) [13] protocol and is from DoCoMo labs [27]. We use this only to generate and verify CGAs for Mobile IPv6 ERO. The OpenSSL project [28] provided the RSA [38] algorithms we use to sign and verify Binding Update and to encrypt and decrypt the permanent home keygen token. After Enhanced Route Optimization for Mobile IPv6 was implemented, we use wireshark [40] and tcpdump [41] which can provide network protocol analysis.

1. CGA Function

This function is used in Binding Update message. It contains part of the mobile node's CGAP. [21] limits mobility header options to a maximum length of 255 bytes, excluding the option type and option length fields. Since the CGAP size is likely to exceed this limit, multiple CGAP options may have to be concatenated to carry the complete CGAP.In practice, we use Home link subnet prefix generated CGA.

2. Signature Function

This function is used in Binding Update message which is sent by the mobile node to the correspondent node. It contains a signature that the mobile node generated with its RSA private key over one or more preceding CGA Parameter options. The specification [21] does not allow for more than one signature option however when larger RSA keys are used the generated signature will exceed the maximum option data length of 255 bytes. Since we needed to test with keys large enough to cause this situation, we implemented the obvious and copied the method defined to permit multiple CGAP options.

Our system can sign ERO packets in the method specified by the standard [21] and can verify the correctness of received signatures, or reject those which are invalid.

3. Encrypt and Decrypt Permanent Home Keygen Token

The Permanent Home Keygen Token option is used in Binding Acknowledgement messages. It contains a Permanent Home Keygen Token, which the correspondent node sends to the mobile node after it has received a binding Update message containing a CGAP option directly followed by a Signature option from the mobile node.

Just as with the Signature option, the PHKT option can be required to handle data larger than can be represented using a single mobility option field. As with the signature option the standard [21] does not provide a mechanism to handle this case. We adopted a similar solution, based on the mechanism specified for handling multiple CGAP options, and simply divide the data into suitably sized pieces, encapsulate each in a PHKT option, and include them in order. The receiver reconstructs the token by taking the data from the several PHKT options, in order as received, and concatenating that.

4. Concurrent Care-of Address Tests and Credit-Based Authorization

As we have presented in chapter 3, the ERO use Concurrent Care-of address Test to reduce handoff delay and signaling overhead. In our implementation we have implemented the Concurrent Care-of Address Test but the Credit-Based Authorization is not yet supported. In our tests we simply assume no attempt is being made to subvert the CoA.

5. Parallel Home and Correspondent Registration

ERO enables the mobile node to pursue a correspondent registration in parallel with the respective home registration. Our implementation does not yet attempt this.

5.2 Experiment Environment

The experimental Testbed consists of three FreeBSD [14] nodes playing the roles of the Mobile Node, Home Agent and Correspondent Node as introduced in Chapter 4. Figure 5.1 illustrates the Testbed topology. The Mobile Node may attach to its Home Agent or to either of the access routers in the visited domains. The exterior interfaces of all routers and the Correspondent Node connect to the "Internet-IPv6 network".

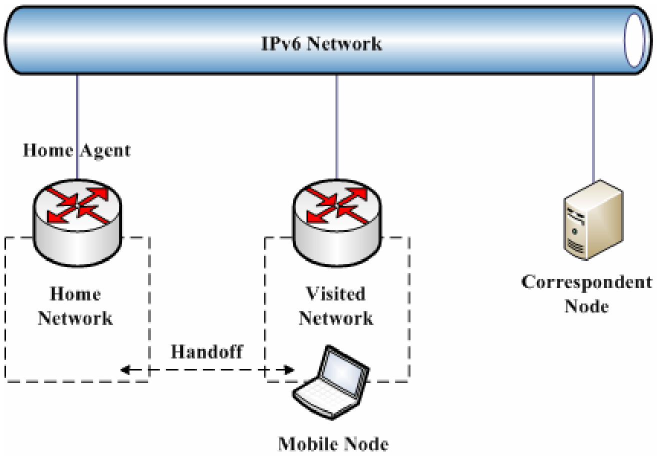


Figure 5.1 Mobile IPv6 Testbed Topology

5.3 Setup and Configuration

In order to implement the Enhanced Route Optimization function, the Testbed network configuration has been setup to provide CGA functions and cryptography. Route Optimization must be enabled to support CGA authentication. That requires both the Mobile Node and Correspondent Node daemons to be modified to support this function.

IP address and network configurations have been assigned as in Chapter 4, except the subnet prefix changed from 2005 to 2007 just to be different. In our implementation the Mobile Node's home-address is a CGA, so we manually configure the mobile's home address in /etc/rc.conf. Our testing will involve different RSA key sizes so we need several different Private/Public key pairs with different key sizes and, as the CGA depends upon the public key, we obtain a different CGA for each different key length. The CGAs actually used for the various key lengths are shown in table 5.1.

RSA key Length	CGA Home Address	Size of CGAP
512 bits	2007:ffff:cafe:babe:2c6e:99bd:b2c0:80e0	119 bytes
768 bits	2007:ffff:cafe:babe:3427:55eb:93d5:108b	151 bytes
1024 bits	2007:ffff:cafe:babe:3c69:21f:1e22:50a	187 bytes
1280 bits	2007:ffff:cafe:babe:2490:66dc:fe4c:c0cf	219 bytes
1536 bits	2007:ffff:cafe:babe:34af:c8d7:8abf:4402	251 bytes
1575 bits	2007:ffff:cafe:babe:38d2:c8c5:49cc:6cbe	255 bytes
1792 bits	2007:ffff:cafe:babe:3027:ebf3:3ff8:1f11	283 bytes
2040 bits	2007:ffff:cafe:babe:2092:a879:a63f:3023	318 bytes
2048 bits	2007:ffff:cafe:babe:3c6e:12f:67:3b41	319 bytes
2560 bits	2007:ffff:cafe:babe:2092:a879:a63f:3023	383 bytes
3072 bits	2007:ffff:cafe:babe:2420:f6a5:1d50:10c2	447 bytes

Table 5.1 Different RSA key Length Generated CGA list

5.4 Testing and Result

Handoff performance is a significant part of Mobile IPv6 Route Optimization, and Enhanced Route Optimization for Mobile IPv6 [21] provides some enhancements to improve Handoff performance. This section details the various different ERO scenarios tested and the results of those tests.

5.4.1 Proactive home-address tests in ERO

A Mobile node acquires a home keygen token for a future hand off during a proactive home-address test. This saves a possibly long round trip through the home agent during the critical handoff period. The mobile node can invoke proactive home-address test on a just –in-time basis if its link layer provides a trigger indicating imminent handoff, or periodically whenever the most recently obtained home keygen token is about to expire.

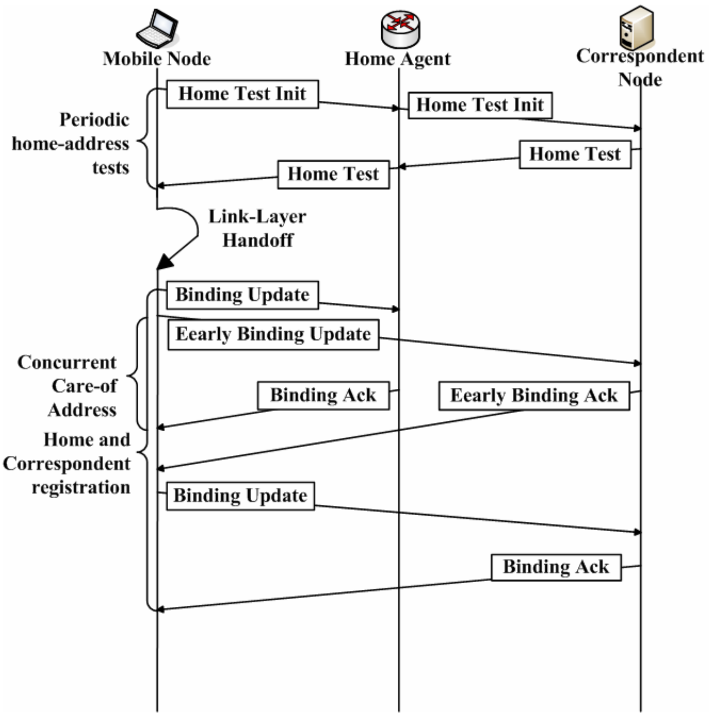
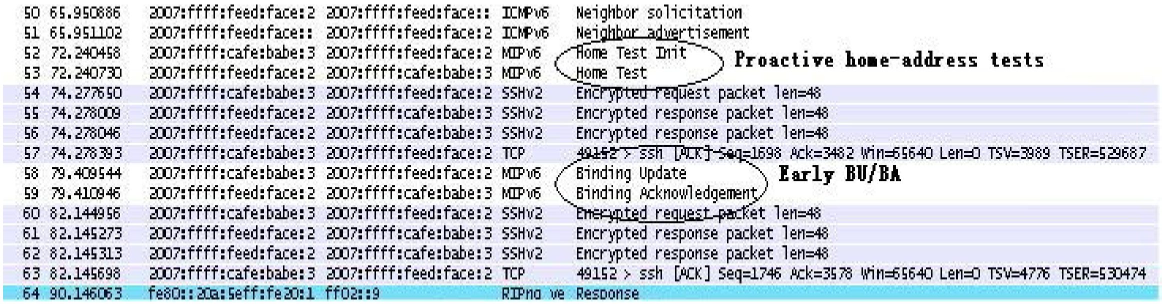


Figure 5.2 Enhanced Route Optimization procedure

This scenario shown in figure 5-2 is easy to implement in our experimental environment, but is too hard to use in practice as mentioned in chapter 4. In the experiment environment testing, we can generate an imminent trigger event code, this trigger event use UNIX interrupt signal (simulate Mobile Node just-in-time handoff) to start testing the proactive home-address tests process. We can trigger interrupt signal, let Mobile Node and Correspondent Node exchange HoTI/HoT to acquire a temporary home keygen token in home link, permitting the Mobile Node to issue a Binding Update message directly after the handoff. The Binding update message is early, and a care-of keygen token is delivered to the Mobile Node along with the Binding Acknowledgment message.

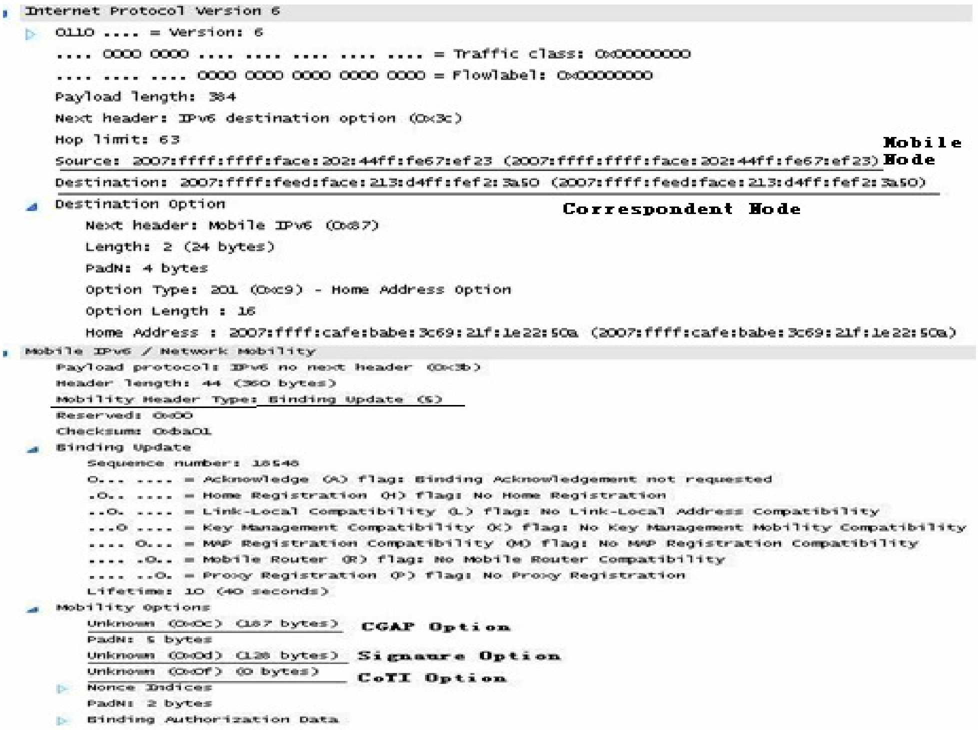
In testing, at the Mobile Node we use the SSH program to make a TCP connection with Correspondent node, at the Correspondent Node side we use the wireshark program to monitor this process. We start testing with the ERO trigger interrupt signal, let the Mobile Node and Correspondent Node exchange HoTI/HoT before Mobile Node handoff. After Mobile Node handoff the Mobile Node and Correspondent Node exchange Early BU/BA. Figure 5-3 shows the packets captured by the wireshark program running on the correspondent node during the Enhanced Route Optimization procedure where the HoTI/HoT is performed before handover. After that the early binding update message is immediately sent to the correspondent node



```
50 65.950886  2007:ffff:feed:face:2 2007:ffff:feed:face:: ICMPv6  Neighbor solicitation
51 65.951102  2007:ffff:feed:face:: 2007:ffff:feed:face:2 ICMPv6  Neighbor advertisement
52 72.240458  2007:ffff:cafe:babe:3 2007:ffff:feed:face:2 MIPv6   Home Test Init
53 72.240730  2007:ffff:feed:face:2 2007:ffff:cafe:babe:3 MIPv6   Home Test
54 74.277650  2007:ffff:cafe:babe:3 2007:ffff:feed:face:2 SSHv2   Encrypted request packet len=48
55 74.278009  2007:ffff:feed:face:2 2007:ffff:cafe:babe:3 SSHv2   Encrypted response packet len=48
56 74.278046  2007:ffff:feed:face:2 2007:ffff:cafe:babe:3 SSHv2   Encrypted response packet len=48
57 74.278393  2007:ffff:cafe:babe:3 2007:ffff:feed:face:2 TCP     49152 > ssh [ACK] Seq=1698 Ack=3482 Win=65640 Len=0 TSV=3989 TSER=529687
58 79.409544  2007:ffff:cafe:babe:3 2007:ffff:feed:face:2 MIPv6   Binding Update
59 79.410946  2007:ffff:feed:face:2 2007:ffff:cafe:babe:3 MIPv6   Binding Acknowledgement
60 82.144956  2007:ffff:cafe:babe:3 2007:ffff:feed:face:2 SSHv2   Encrypted request packet len=48
61 82.145273  2007:ffff:feed:face:2 2007:ffff:cafe:babe:3 SSHv2   Encrypted response packet len=48
62 82.145313  2007:ffff:feed:face:2 2007:ffff:cafe:babe:3 SSHv2   Encrypted response packet len=48
63 82.145698  2007:ffff:cafe:babe:3 2007:ffff:feed:face:2 TCP     49152 > ssh [ACK] Seq=1746 Ack=3578 Win=65640 Len=0 TSV=4776 TSER=530474
64 90.146063  fe80::20a:5eff:fe20:1 ff02::9               RIPng ve Response
```

Figure 5.3 Proactive Home-address Tests in ERO

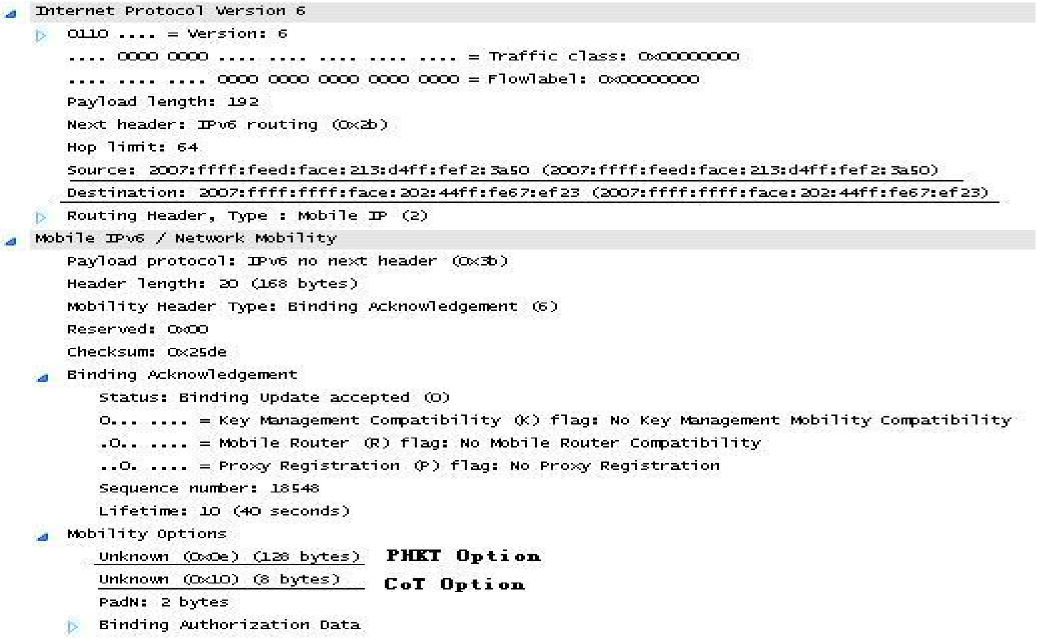
More detail of the Early BU for ERO process is presented in Figure 5.4. This shows the packets captured by the wireshark program running on the correspondent node. We can see the all information about the Early BU including source and destination addresses which have been highlighted in the figure. There are three Mobility options unknown by wireshark in ERO which are those new options required by the ERO procedures: CGAP option (0x0c), Signature option (0x0d) and CoTI option (0x0f).



```
Internet Protocol Version 6
    0110 .... = Version: 6
    .... 0000 0000 .... .... .... .... .... = Traffic class: 0x00000000
    .... .... .... 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
    Payload length: 384
    Next header: IPv6 destination option (0x3c)
    Hop limit: 63
    Source: 2007:ffff:ffff:face:202:44ff:fe67:ef23 (2007:ffff:ffff:face:202:44ff:fe67:ef23)
    Destination: 2007:ffff:feed:face:213:d4ff:fef2:3a50 (2007:ffff:feed:face:213:d4ff:fef2:3a50)
    Destination Option
        Next header: Mobile IPv6 (0x87)
        Length: 2 (24 bytes)
        PadN: 4 bytes
        Option Type: 201 (0xc9) - Home Address Option
        Option Length : 16
        Home Address : 2007:ffff:cafe:babe:3c69:21f:1e22:50a (2007:ffff:cafe:babe:3c69:21f:1e22:50a)
Mobile IPv6 / Network Mobility
    Payload protocol: IPv6 no next header (0x3b)
    Header length: 44 (360 bytes)
    Mobility Header Type: Binding Update (5)
    Reserved: 0x00
    Checksum: 0xba01
    Binding Update
        Sequence number: 18548
        0... .... = Acknowledge (A) flag: Binding Acknowledgement not requested
        .0.. .... = Home Registration (H) flag: No Home Registration
        ..0. .... = Link-Local Compatibility (L) flag: No Link-Local Address Compatibility
        ...0 .... = Key Management Compatibility (K) flag: No Key Management Mobility Compatibility
        .... 0... = MAP Registration Compatibility (M) flag: No MAP Registration Compatibility
        .... .0.. = Mobile Router (R) flag: No Mobile Router Compatibility
        .... ..0. = Proxy Registration (P) flag: No Proxy Registration
        Lifetime: 10 (40 seconds)
    Mobility Options
        Unknown (0x0c) (187 bytes)
        PadN: 5 bytes
        Unknown (0x0d) (128 bytes)
        Unknown (0x0f) (0 bytes)
        Nonce Indices
        PadN: 2 bytes
        Binding Authorization Data
```

Figure 5.4 Wireshark monitor Early BU in ERO Process

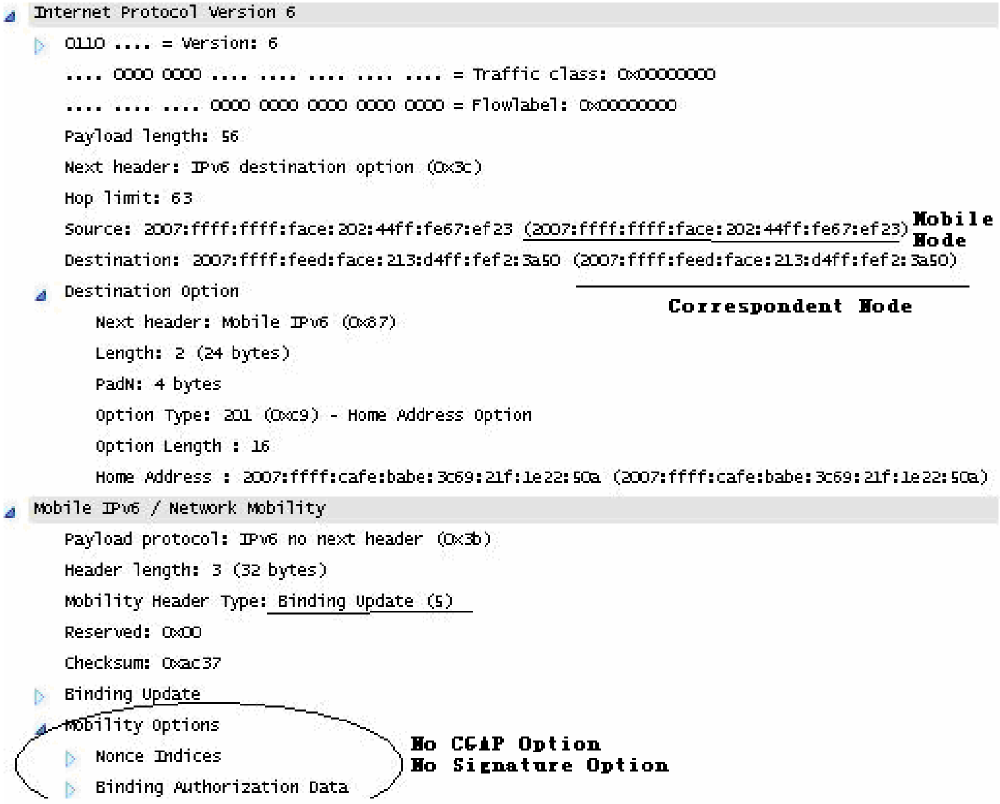
Figure 5.5 is shows the Early BA in the ERO process, the captured data of EBA shows two options unknown by wireshark in ERO which are those new options required by the ERO procedures: PHKT option (0x0e) and CoT option (0x10).



```
Internet Protocol Version 6
    0110 .... = Version: 6
    .... 0000 0000 .... .... .... .... .... = Traffic class: 0x00000000
    .... .... .... 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
    Payload length: 192
    Next header: IPv6 routing (0x2b)
    Hop limit: 64
    Source: 2007:ffff:feed:face:213:d4ff:fef2:3a50 (2007:ffff:feed:face:213:d4ff:fef2:3a50)
    Destination: 2007:ffff:ffff:face:202:44ff:fe67:ef23 (2007:ffff:ffff:face:202:44ff:fe67:ef23)
    Routing Header, Type : Mobile IP (2)
Mobile IPv6 / Network Mobility
    Payload protocol: IPv6 no next header (0x3b)
    Header length: 20 (168 bytes)
    Mobility Header Type: Binding Acknowledgement (6)
    Reserved: 0x00
    Checksum: 0x25de
    Binding Acknowledgement
        Status: Binding Update accepted (0)
        0... .... = Key Management Compatibility (K) flag: No Key Management Mobility Compatibility
        .0.. .... = Mobile Router (R) flag: No Mobile Router Compatibility
        ..0. .... = Proxy Registration (P) flag: No Proxy Registration
        Sequence number: 18548
        Lifetime: 10 (40 seconds)
    Mobility Options
        Unknown (0x0e) (128 bytes)
        Unknown (0x10) (8 bytes)
        PadN: 2 bytes
        Binding Authorization Data
```

Figure 5.5 Wireshark monitor Early BA in ERO Process

The subsequent BU for ERO is protected by the PHKT, so subsequent BU mobility options do not include the CGAP and Signature Options. We captured the subsequent BU with wireshark program and show it here in figure 5.6. We can see no CGAP or Signature options, only the Nonce and Binding Authorization Data options are present.



```
Internet Protocol Version 6
  0110 .... = Version: 6
  .... 0000 0000 .... .... .... .... .... = Traffic class: 0x00000000
  .... .... .... 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
  Payload length: 56
  Next header: IPv6 destination option (0x3c)
  Hop limit: 63
  Source: 2007:ffff:ffff:face:202:44ff:fe67:ef23 (2007:ffff:ffff:face:202:44ff:fe67:ef23)
  Destination: 2007:ffff:feed:face:213:d4ff:fef2:3a50 (2007:ffff:feed:face:213:d4ff:fef2:3a50)
  Destination Option
    Next header: Mobile IPv6 (0x87)
    Length: 2 (24 bytes)
    PadN: 4 bytes
    Option Type: 201 (0xc9) - Home Address Option
    Option Length : 16
    Home Address : 2007:ffff:cafe:babe:3c69:21f:1e22:50a (2007:ffff:cafe:babe:3c69:21f:1e22:50a)
Mobile IPv6 / Network Mobility
  Payload protocol: IPv6 no next header (0x3b)
  Header length: 3 (32 bytes)
  Mobility Header Type: Binding Update (5)
  Reserved: 0x00
  Checksum: 0xac37
  Binding Update
  Mobility Options
    Nonce Indices
    Binding Authorization Data
```

Figure 5.6 Wireshark Monitor Subsequent BU in ERO

5.4.2 After Handoff home-address tests in ERO

ERO can have selected message exchanges. Since a proactive home-address test is hard to implement in practice, a mobile node will normally use an after handoff home-address test. For that scenario see figure 5.7. The only difference is that the Early BU to Correspondent node must wait until after the HoTI/HoT is exchanged.

In testing, home-address tests are after handoff, subsequent ERO operation is the same as the proactive home-address tests in ERO. Since there is nothing new to show, we omit the details of this testing in this section.

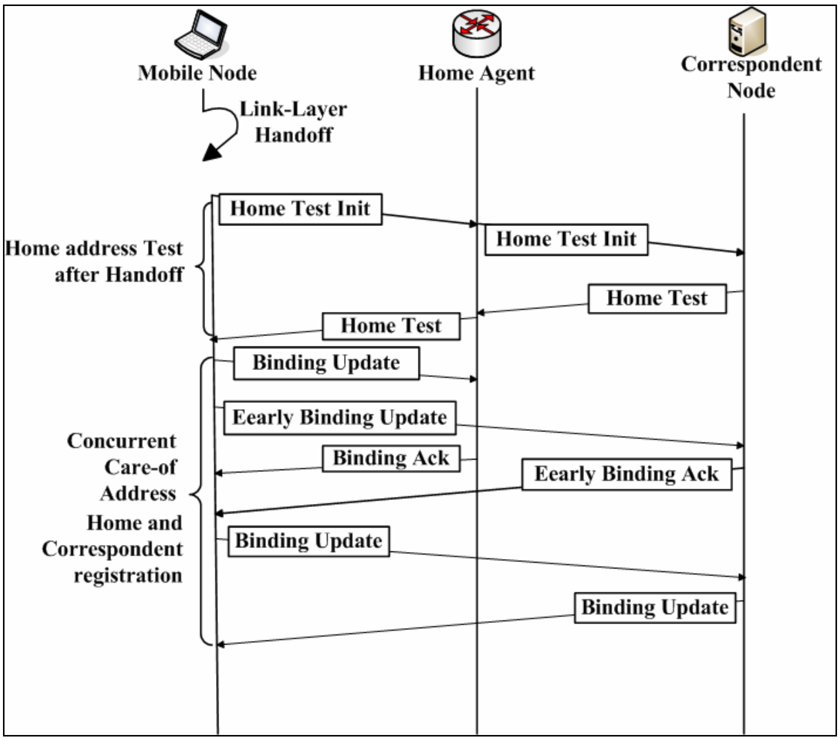


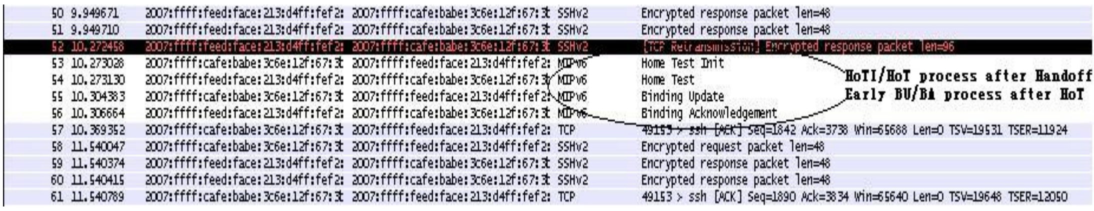
Figure 5.7 ERO Procedures (HoTI/HoT after handoff)

5.5 Multiple Signature Options and PHKT Options

We expect the costs of ERO to be dominated by the costs of the Public Key computations (RSA algorithms). That cost is controlled by the size chosen for the modulus parameter from which the keys are generated. Thus we vary that over a selection of values ranging from 512 to 3072 bits. Table 5-1 shows the CGA list which was used in this testing. Values smaller than 512 bits (probably including 512 bits) are too small to be secure. Values larger than 1575 bits cause the generated public keys, encoded as specified in [5, 6, 7], with the other CGA parameters [3] to exceed the capacity of a single CGA parameter option. [21] allows for this, permitting several options to be used to carry the complete CGA parameter block.

At key modulus sizes greater than 2040 bits, the packet signature no longer fits in a single option, nor does the returned Permanent Home Keygen Token (PHKT). [21] does not provide for those option size limits to be exceeded; to enable measurements to be made with longer keys, we copied the solution for CGA parameter blocks, and permit multiple options to be combined to carry a single large parameter value

Figures 5.8 to 5.10 show an example of use of a long RSA key (2048 bits) in an after handoff home-address test of ERO. In this example, because the RSA key exceeds 1575 bits, the CGAP data required two options. Similarly when the key length exceeds 2040 bits the Signature and PHKT are separated into two options as in figures 5.9 and 5.10. Figure 5.8 shows the ERO operation.

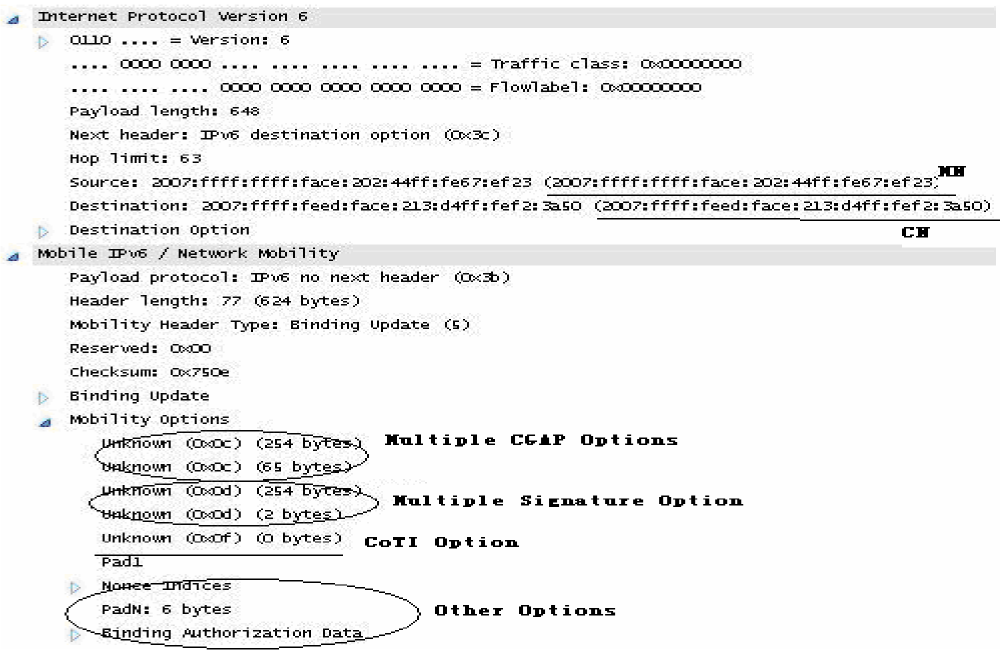


```
50 9.949671   2007:ffff:feed:face:213:d4ff:fef2: 2007:ffff:cafe:babe:3c6e:12f:67:3t SSHv2   Encrypted response packet len=48
51 9.949710   2007:ffff:feed:face:213:d4ff:fef2: 2007:ffff:cafe:babe:3c6e:12f:67:3t SSHv2   Encrypted response packet len=48
52 10.272458  2007:ffff:feed:face:213:d4ff:fef2: 2007:ffff:cafe:babe:3c6e:12f:67:3t SSHv2   [TCP Retransmission] Encrypted response packet len=96
53 10.273028  2007:ffff:cafe:babe:3c6e:12f:67:3t 2007:ffff:feed:face:213:d4ff:fef2: MIPv6   Home Test Init
54 10.273130  2007:ffff:feed:face:213:d4ff:fef2: 2007:ffff:cafe:babe:3c6e:12f:67:3t MIPv6   Home Test
55 10.304383  2007:ffff:cafe:babe:3c6e:12f:67:3t 2007:ffff:feed:face:213:d4ff:fef2: MIPv6   Binding Update
56 10.306664  2007:ffff:feed:face:213:d4ff:fef2: 2007:ffff:cafe:babe:3c6e:12f:67:3t MIPv6   Binding Acknowledgement
57 10.369352  2007:ffff:cafe:babe:3c6e:12f:67:3t 2007:ffff:feed:face:213:d4ff:fef2: TCP     49153 > ssh [ACK] Seq=1842 Ack=3738 Win=65688 Len=0 TSV=19531 TSER=11924
58 11.540047  2007:ffff:cafe:babe:3c6e:12f:67:3t 2007:ffff:feed:face:213:d4ff:fef2: SSHv2   Encrypted request packet len=48
59 11.540374  2007:ffff:feed:face:213:d4ff:fef2: 2007:ffff:cafe:babe:3c6e:12f:67:3t SSHv2   Encrypted response packet len=48
60 11.540415  2007:ffff:feed:face:213:d4ff:fef2: 2007:ffff:cafe:babe:3c6e:12f:67:3t SSHv2   Encrypted response packet len=48
61 11.540789  2007:ffff:cafe:babe:3c6e:12f:67:3t 2007:ffff:feed:face:213:d4ff:fef2: TCP     49153 > ssh [ACK] Seq=1890 Ack=3834 Win=65640 Len=0 TSV=19648 TSER=12050
```

\

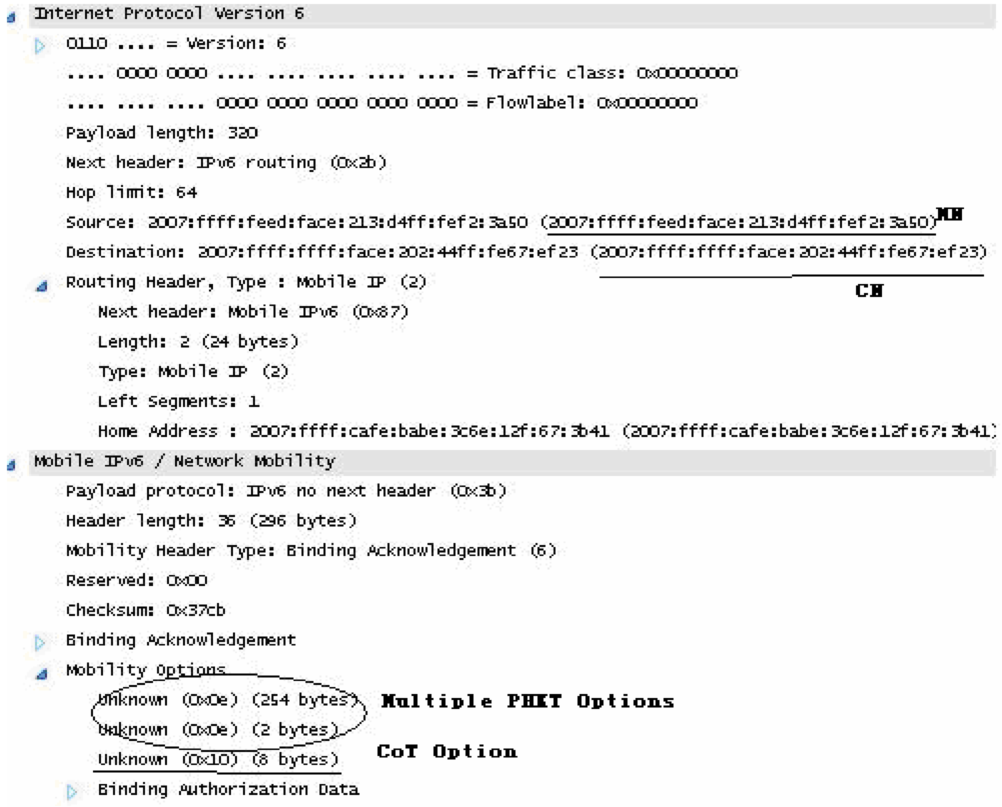
Figure 5.8 Large RSA Key length Generated CGA process in ERO

Figure 5.9 shows a large RSA key length in an ERO BU for Mobile IPv6. The BU presents the separate CGAP and Signature data as two CGAP options (0x0C) and Signature options (0x0d). The first CGAP option is 254 bytes, the other is 65 bytes. The first signature option is 254 bytes the other is 2 bytes. Note that, the maximum data length of each Mobility Option is 255 bytes, in our implementation if the data size exceeds 255 bytes (not include 255 bytes) these data need to split.



```
Internet Protocol Version 6
  0110 .... = Version: 6
  .... 0000 0000 .... .... .... .... .... = Traffic class: 0x00000000
  .... .... .... 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
  Payload length: 648
  Next header: IPv6 destination option (0x3c)
  Hop limit: 63
  Source: 2007:ffff:ffff:face:202:44ff:fe67:ef23 (2007:ffff:ffff:face:202:44ff:fe67:ef23)
  Destination: 2007:ffff:feed:face:213:d4ff:fef2:3a50 (2007:ffff:feed:face:213:d4ff:fef2:3a50)
  Destination Option
Mobile IPv6 / Network Mobility
  Payload protocol: IPv6 no next header (0x3b)
  Header length: 77 (624 bytes)
  Mobility Header Type: Binding Update (5)
  Reserved: 0x00
  Checksum: 0x750e
  Binding Update
  Mobility Options
    Unknown (0x0c) (254 bytes)
    Unknown (0x0c) (65 bytes)
    Unknown (0x0d) (254 bytes)
    Unknown (0x0d) (2 bytes)
    Unknown (0x0f) (0 bytes)
    Pad1
    Nonce Indices
    PadN: 6 bytes
    Binding Authorization Data
```

Figure 5.9 Early BU including multiple CGAP and Signature Options



```
Internet Protocol Version 6
  0110 .... = Version: 6
  .... 0000 0000 .... .... .... .... .... = Traffic class: 0x00000000
  .... .... .... 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
  Payload length: 320
  Next header: IPv6 routing (0x2b)
  Hop limit: 64
  Source: 2007:ffff:feed:face:213:d4ff:fef2:3a50 (2007:ffff:feed:face:213:d4ff:fef2:3a50)
  Destination: 2007:ffff:ffff:face:202:44ff:fe67:ef23 (2007:ffff:ffff:face:202:44ff:fe67:ef23)
  Routing Header, Type : Mobile IP (2)
    Next header: Mobile IPv6 (0x87)
    Length: 2 (24 bytes)
    Type: Mobile IP (2)
    Left Segments: 1
    Home Address : 2007:ffff:cafe:babe:3c6e:12f:67:3b41 (2007:ffff:cafe:babe:3c6e:12f:67:3b41)
Mobile IPv6 / Network Mobility
  Payload protocol: IPv6 no next header (0x3b)
  Header length: 36 (296 bytes)
  Mobility Header Type: Binding Acknowledgement (6)
  Reserved: 0x00
  Checksum: 0x37cb
  Binding Acknowledgement
  Mobility Options
    Unknown (0x0e) (254 bytes)
    Unknown (0x0e) (2 bytes)
    Unknown (0x10) (8 bytes)
    Binding Authorization Data
```

Figure 5.10 Early BA including multiple PHKT Options

Figure 5.10 shows the BA that follows a BU which used a long RSA key. In this message two PHKT options occur, the first carrying the first 254 bytes of the permanent home keygen token, the second the remaining two bytes. The CoT option is 8 bytes and is in the BA message following the PHKT option.

5.6 Summary

The result of implementation and testing show that Enhanced Route Optimization for Mobile IPv6, which can provide lower handoff delays, increased security, and reduced signaling overhead, functions correctly. We have tested Enhanced Route Optimization in two kinds of scenario, one is the HoTI/HoT performance before handoff the other is HoTI/HoT performance after handoff. From result of Implementation and testing both scenarios work well.

However, during our testing of larger RSA key lengths in ERO, we found values larger than 1575 bits cause the generated public keys, with the other CGA parameters to exceed the capacity of a single CGA parameter option. [21] allows for this, permitting several options to be used to carry the complete CGA parameter block. At key modulus sizes greater than 2040 bits, the packet signature no longer fits in a single option, nor does the returned permanent home keygen token (PHKT). [21] does not provide for those option size limits to be exceeded.

CHAPTER 6

MEASURING THE COSTS OF ENHANCED ROUTE OPTIMIZATION

Enhanced Route Optimization for Mobile IPv6 applies Cryptographically Generated Addresses (CGAs) to improve security and reduce handover delays. However the use of CGAs requires computationally expensive algorithms. This may be an issue for small mobile devices with low processing power. It is likely to be a problem for correspondent nodes that simultaneously communicate with a large number of mobile nodes, such as publicly accessible servers. This chapter investigates Enhanced Route Optimization for Mobile IPv6, concentrating upon the costs particularly for the Correspondent Node. The costs of implementing Enhanced Route Optimization for Mobile IPv6 are not negligible. The Correspondent Node will have to protect itself against potential denial-of service attempts from attackers by limiting the amount of resources it spends on CGA verification.

This chapter defines a Denial-of-service attack in section 6.1, and shows some methods of Denial of service attack in section 6.2. Section 6.3 presents the Enhanced Route Optimization Problem Statement and Experiment Scenarios. Experiment Results and analysis are in section 6.4. We conclude with a summary in section 6.5.

6.1 Overview Denial-of-service attack

A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a computer resource unavailable to its intended users. Although the means to, motives for, and targets of a DoS attack may vary, it generally consists of the concerted, malevolent efforts of a person or persons to prevent an Internet site or service from functioning efficiently or at all, temporarily or indefinitely.

Perpetrators of DoS attacks typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateways, and even DNS root servers. One common method of attack involves saturating the target (victim) machine with external communications requests, such that it cannot respond to legitimate traffic, or responds so slowly as to be rendered effectively unavailable. In general terms, DoS attacks are implemented by either forcing the targeted computer(s) to reset, or consume its resources so that it can no longer provide its intended service or obstructing the communication media between the intended users and the victim so that they can no longer communicate adequately.

6.2 Methods of Attack

A "denial-of-service" attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service. Attacks can be directed at any network device, including attacks on routing devices and web, electronic mail, or Domain Name System servers. A DoS attack can be perpetrated in a number of ways. The five basic types of attack are:

1. Consumption of computational resources, such as bandwidth, disk space, or processor time
2. Disruption of configuration information, such as routing information.
3. Disruption of state information, such as unsolicited resetting of TCP sessions.
4. Disruption of physical network components.
5. Obstructing the communication media between the intended users and the victim so that they can no longer communicate adequately.

6.3 Problem Statement and Experiment Scenario

Section 6.2 explained one DoS attack method as the consumption of computational resources, such as bandwidth, disk space. Enhanced Route Optimization for Mobile IPv6 uses Cryptographically Generated Addresses which require computationally complex public key cryptography and so might result in causing a DoS or DDoS attack.

To determine the burden of implementing and using ERO we must measure its costs. In particular, one of the requirements of [21] is:

> *Attackers should not be able to cause denial of service against mobile or correspondent nodes through exploiting expensive computations involved in the*

mobility protocol.

We seek determine whether or not ERO meets this requirement.

Experiment Scenario: An attacker might send many useless EBU packets to its target. Determining that they are forged requires signature verification, which means decryption using public key algorithms. This is likely to require much computation. If an attacker were to send many fraudulent EBU packets, each CGA authenticated to a target node that node would need to determine the failure of the RSA signature verification, consuming CPU in so doing. We measured and report that cost. For comparison we also measured the CPU cost to a target of processing several other packet flooding attacks, in comparison to the network resources required to launch them. The cost of the standard Route Optimization Return Routability Procedure authentication is lightweight, so the cost of ERO for our proposes, amounts to the elapsed CPU time to perform the necessary CGA and signature calculations.

To avoid the reported measurements depending upon the actual CPU used in our experiments and as we are most interested in the relationship between the various measurements, we have chosen a time unit we call N, all times reported will be given as multiples of N. N is just a measure of time, some number of microseconds that will vary from processor to processor. The relevance is that is an operation is reported as consuming ten times as many Ns as another operation, it can be expected that however fast the two operations are on a particular processor the first will be approximately 10 times slower than the second. The Measuring code of this experiment scenario is embedded in the ERO code. Moreover, for comparison, we also measured the network bandwidth an attacker would need to consume to achieve a 100% CPU utilization of a victim node using several other possible packet types like Pingv4/v6 flood, UDPv4/v6 flood. For these measurements we arranged a process to run on the target system, doing nothing but consuming all available CPU for a particular period. During that period we attack the target with a packet storm and measure how much longer the process took due to the cost to the target of dealing with the incoming packets. We also measured the volume of incoming data and combine the two figures to determine the bandwidth that would need to be consumed to exhaust the target CPU. Clearly a smaller result indicates a more effective attack. Figure 6.1 illustrates this process. All measurement was repeated many times to obtain good confidence in the accuracy of the results.

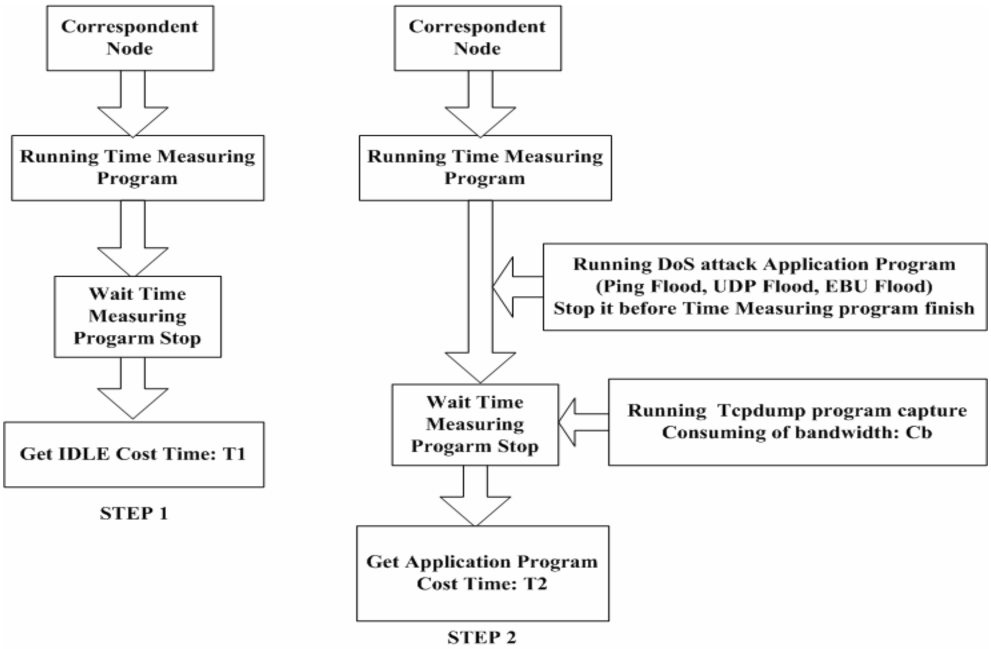

Correspondent Node
Running Time Measuring Program
Wait Time Measuring Progarm Stop
Get IDLE Cost Time: T1
STEP 1
Correspondent Node
Running Time Measuring Program
Running DoS attack Application Program (Ping Flood, UDP Flood, EBU Flood) Stop it before Time Measuring program finish
Wait Time Measuring Progarm Stop
Running Tcpdump program capture Consuming of bandwidth: Cb
Get Application Program Cost Time: T2
STEP 2

Figure 6.1 Measuring 100% CPU Consume network bandwidth

After obtaining T1, T2, and Cb as indicated in the figure, we calculate the network bandwidth required to achieve a 100% CPU saturation as follows:

CPU cost fraction = [(T2-T1)/T2]

This is the fraction of the CPU consumed by the attack.

100%CPU Consume bandwidth = Cb / CPU Cost rate

That is, if Cb were 1 Mbps and that consumed 1/10 the available CPU, we calculate 10Mbps would consume 100%.

6.4 Experiment Results and Analysis

For each selected key length Fig 6.2 shows the time required to generate the RSA signature used to authenticate the CGA-based EBU (CGA-Sign), the time taken to verify that signature from a received packet (CGA-Verify), the time taken to encrypt a Permanent home keygen token to return (PHKT-Encrypt), and the time taken to decrypt the Permanent home token at the Mobile Node (PHKT-Decrypt). Note the use of a logarithmic scale on the vertical axis to permit all results to be adequately represented.

It is immediately obvious that the most expensive operations are generating the signature (CGA-Sign) and decrypting the Permanent home keygen token (PHKT-Decrypt); operations using the much larger Private Key. Both of these functions are performed by the Mobile Node, at its option, and hence are not a significant concern here.

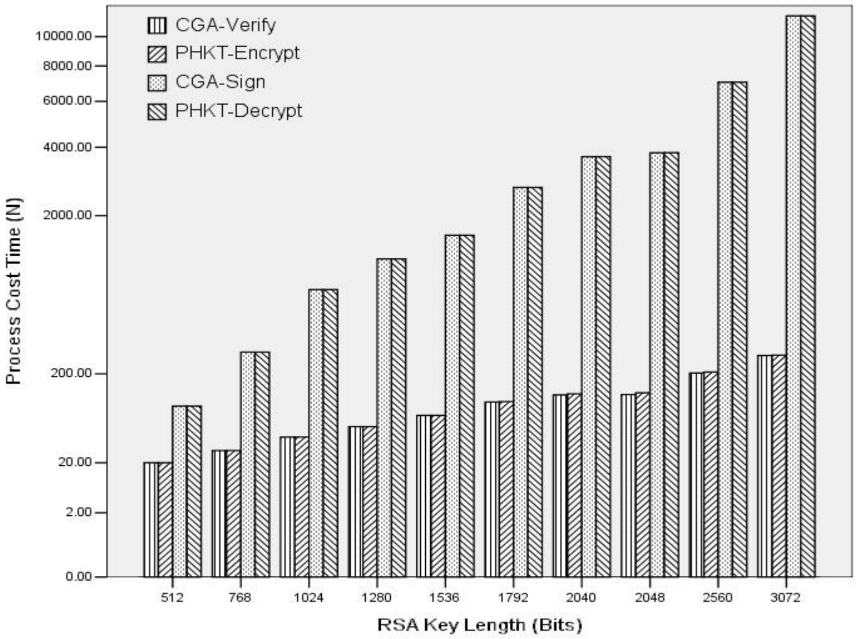


Figure 6.2 Process Cost time for CGA-based authentication

While the other operations, those performed by the Correspondent Node, are considerably cheaper, the costs are not negligible, and clearly grow as the key size increases. To obtain a better feel for the Correspondent Node costs, we also measured the total time to process an enhanced EBU. Those results are provided in Fig 6.3. We also include there the cost of processing a received EBU where the signature verification fails as it might in a Denial of Service attack upon the Correspondent Node. Clearly the time to process the Standard BU does not depend upon the key length (there is no key involved).

However it can be seen that as the key size increases the cost to the Correspondent Node increases rapidly. With greater key length than we were able to test the cost of even discarding a BU with an invalid signature may become intolerable. On the processor we used, with a key modulus of 3072 bits, the Correspondent Node would exhaust its processor time merely validating, and rejecting, approximately 500 invalid BU packets a second, and can respond to only half that number of valid BUs carrying CGA parameters requesting a permanent home keygen token be received.

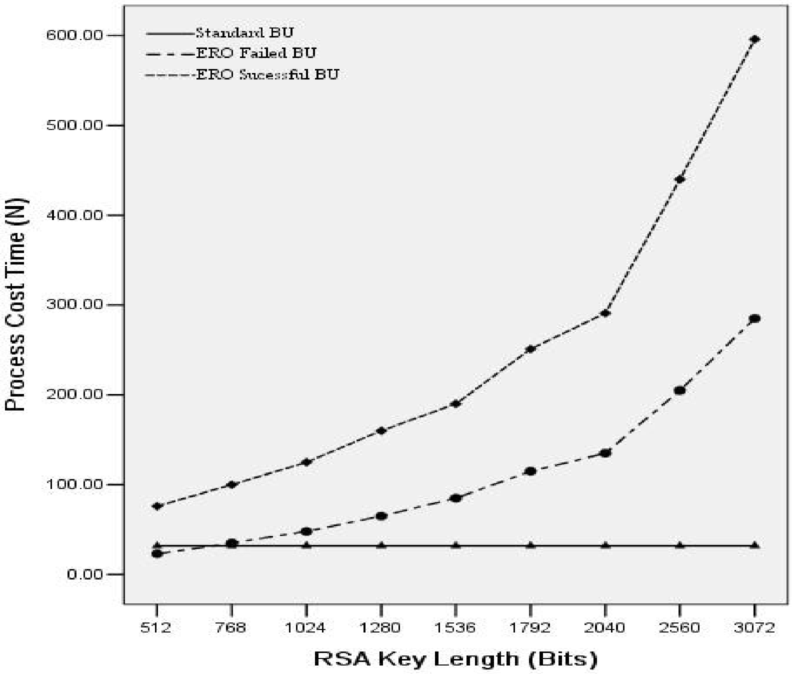


Figure 6.3 Compare Process BU with Process Receive BU

That is, a Correspondent Node server of this power could handle connections from at most 250 distinct clients per second, if each was to prepare itself for possible later rapid mobile IP handover using ERO.

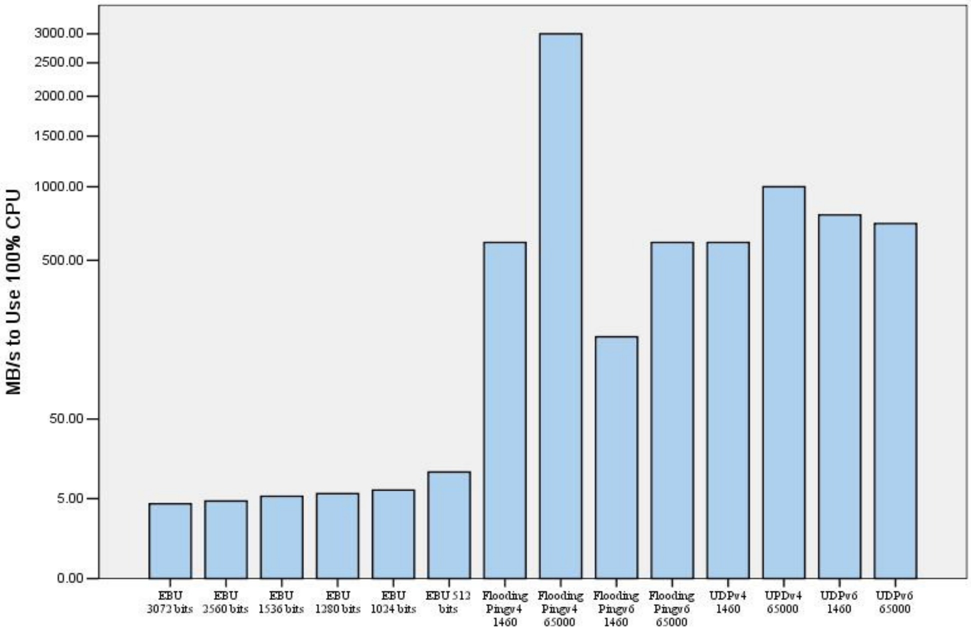


Figure 6.4 **100% CPU Cost of Flooding EBU, Flooding v4/v6 and UDPv4/v6**

For comparison, we also measured the network bandwidth an attacker would need to consume to achieve a 100% CPU utilization of a victim node using several other possible packet types. Figure 6.4 shows those results. It can be seen that EBU consuming less than 5 MB/Sec would saturate the CPU, whereas IPv4, ICMP Echo (ping) packets 65KB big require more than 3 GB/sec to achieve the same result. This makes EBU a much more effective denial of service (by CPU exhaustion) attack than ICMP echo, or any of the other methods we tested.

6.5 Summary

Enhanced Route Optimization applies CGA to increase its security. But attackers may use denial of service against correspondent nodes through exploiting expensive computations involved in the mobility protocol. In this chapter we have shown the costs to the Correspondent Node implementing Enhanced Route Optimization for Mobile IPv6 are not negligible, we suspect that with large keys the costs may be considerably greater than reasonable for a busy correspondent node.

We suggest that implementation of correspondent nodes at the very least rejects very large keys without processing. An easy way to achieve this would be to reject packets containing multiple CGA parameter options. The maximum key length then will be about 1575 bits, which seems as if it may be manageable. The security issues of limiting the key size are not significant, as all we seek to achieve here is to do better than sending tokens in the clear and hoping there is no sniffing occurring.

CHAPTER 7

CONCLUSION AND DISCUSSION

This chapter presents the conclusion of the work applying CGA to Mobile IPv6. It summarizes the advantages and the limitations of the developed module. In addition, it presents the discussion of this work and suggests some future work.

7.1 Conclusion

This work surveys a Mobile IPv6 Route Optimization security issue, as apart of Enhanced Route Optimization for Mobile IPv6, applying CGA to Mobile IPv6. There is no question that ERO can increase Route Optimization security, but from testing and evaluation of ERO, it was found that applying CGA in general is risky in that it involves computationally expensive algorithms.

7.1.1 Standard Route Optimization for Mobile IPv6

This work surveys an existing implementation of Mobile IPv6, studying, Testing and investigating standard route Optimization for Mobile IPv6. The objective is to understand standard Route Optimization and its security mechanism the Return Routability procedure. Simultaneously, the Testbed was prepared for the implementation of Enhanced Route Optimization for Mobile IPv6.

7.1.2 Enhanced Route Optimization for Mobile IPv6

Enhanced Route Optimization for Mobile IPv6 provides lower handoff delays, increased security, and reduced signaling overhead. In this work we focus on implementing, investigating and evaluating the application of CGAs to Mobile IPv6. From the testing result, we found that ERO works well in our Testbed. We found that the standard for ERO [21] lacks specification of the mechanism to handle long keys in the signature and PHKT options. In chapter 5 we gave a solution. From evaluation of ERO, we proposed allowing the EBU CGA-based process before Mobile Node handover which not only reduces handover delay but also reduces Periodic HoTI/HoT and packet snooping attacks. However, we also found a problem with applying CGA in general is that they involve computationally expensive algorithms. Because of this, [21] requires use of Semi-Permanent Security Associations to increase ERO efficiency. But the first BU CGA-based will still be the problem for small mobile device with low processing power. Similarly any Correspondent Node that communicates simultaneously with many mobile nodes may find its resources pressured by the costs of the CGA algorithms. Even more seriously, a CN must protect against being attacked by fraudulent EBU packets. Knowing the cost of recognizing the bad packets is useful information and to be able to draw conclusions we measured the cost of processing both valid and invalid ERO packets.

7.2 Discussion

The result of this work produces several benefits. However, there are many limitations which require improvements. This part discusses the procedure and result of this work.

Advantages:

1. Applying CGA to Mobile IPv6 Route Optimization can be increase Route Optimization Security which can be defended by impersonation, DoS/DDoS, and flooding threats.
2. Apart from Enhanced Route Optimization protocol design, we are evaluating and investigating this protocol and propose use of Permanent Home Keygen token process before handoff which not only can increase Route Optimization security but also can reduce handoff delay.
3. We suggest implementation of correspondent nodes to at the very least reject very large keys without processing. An easy way to achieve this is to reject packets containing multiple CGA parameter options. So the key length range for RFC4866 should be 512bits to 1572bits.

Limitations:

1. In our implementation the MN manually configures the home address as a CGA.

2. When we are implementing Enhanced Route Optimization for Mobile IPv6 in a real-network "the proactive home-address test on a just-in-time basis, if its link layer provides a trigger announcing imminent handoff" is very hard to use in a real network.

3. CGA method is depend on a public-key algorithms that involve computationally expensive operations that allows a DoS attack by CGA verification in which attacker can use a long key length that will consume target CPU time doing verification

7.3 Future work

The Enhanced Route Optimization for Mobile IPv6 provides lower handoff delays, increased security, and reduced signaling overhead. For our work we are implementing, investigating and evaluating this protocol in a real network. It has just been a prototype implementation to test the feasibility of Enhanced Route Optimization for Mobile IPv6. It is required to extend several functions to provide a practical solution. The extension in the future should be around the following issues:

1. In order to solve the manual configure CGA problem we may be can put some function provide Auto configure CGA for home address.

2. In order to solve "Periodic the proactive home-address test" problem we can use Permanent home keygen token process before handoff.

3. There seems to be no absolute solution to the DoS attack problem if we are to use CGA with Route Optimization. However we can reduce the security of an attack by limiting the acceptable key sizes. An easy way for the CN to achieve this is to reject BU requests containing multiple CGA parameter options. We might also use ECC [47, 48] algorithms replace RSA algorithms in CGA method which might reduce the DoS attack possibility.

REFERENCES

[1] J. Postel, “Internet Protocol”, RFC 791, Sept. 1981

[2] S. Deering and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, Dec.1998.

[3] C. Perkins, “IP Mobility Support”, RFC2002, Oct. 1996

[4] C. Perkins, “IP Mobility Support for IPv4”, RFC 3344, Aug. 2002.

[5] D. Johnson, C. Perkins and J. Arkko, “Mobility Support in IPv6”, RFC 3775, Jun. 2004.

[6] Microsoft Corporation, “Understanding Mobile IPv6”, Apr. 2004.

[7] T. Aura, “Cryptographically Generated Addresses (CGA)”, RFC 3372, Mar. 2005.

[8] J. Arkko, V. Devarapalli and F. Dupont, “Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents”, RFC 3376, Jun. 2004.

[9] F. Dupont and J-M. Combes, “Using IPsec between Mobile and Correspondent IPv6 Nodes”, draft-ietf-mip6-cn-ipsec-08.txt, Aug. 2008

[10] S. Kent and R. Atkinson, “Security Architecture for the Internet Protocol”, RFC 2401, Nov. 1998.

[11] S. Kent and R. Atkinson, “IP Encapsulating Security Payload (ESP)”, RFC 2406, Nov. 1998.

[12] D. Harkins and D. Carrel, “The Internet Key Exchange (IKE)”, RFC 2409, Nov. 1998.

[13] J. Arkko, J. Kempf, B. Zill and P. Nikander, “SEcure Neighbor Discovery (SEND)”, RFC3971, Mar 2005

[14] Narten, E. Nordmark and W. Simpson, “Neighbor Discovery for IP Version 6 (IPv6)”, RFC 1970, Aug. 1996

[15] P. Nikander, J. Arkko, T. Aura, G. Montenegro and E. Nordmark, “Mobile IP Version 6 Route Optimization Security Design Background”, RFC 4225, Dec. 2005

[16] R. Droms, J. Bound, B. Volz, T. Lemon, C. Perkins and M. Carney, “Dynamic Host Configuration Protocol for IPv6 (DHCPv6)”, RFC 3315, Jul. 2003

[17] D. Haskin and E. Allen, IP Version 6 over PPP, RFC 2472, December 1998

[18] Kui Ren, Wenjing Lou, Kai Zeng, Feng Bao, Jianying Zhou and Robert H. Deng, “Routing optimization security in mobile IPv6”, Computer Networks 50 (2006), 2401–2419

[19] Khaled Elgoarany and Mohamed Eltoweissy, “Security in Mobile IPv6: A Survey”, Information Security Technical Report (2007), doi: 10.1016/j.istr.2007.02.002

[20] C. Vogt, R. Bless, M. Doll and T. Kuefner, “Early Binding Updates for Mobile IPv6”, Proceeding. WCNC 2005 – New Orleans, LA, USA. IEEE, Wireless Communications and Networking Conference.

[21] J. Arkko, C. Vogt and W. Haddad, “Enhanced Route Optimization for Mobile IPv6”, RFC 4866, May. 2007

[22] J. Jonsson and B. Kaliski, “Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1”, RFC 3447, Feb. 2003.

[23] International Telecommunications Union, “Information Technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)”, ITU-T Recommendation X.690, Jul. 2002.

[24] 6NET, “Survey and evaluation of MIPv6 implementations”, May. 2002

[25] 6NET, “Initial MIPv6 Support Guide”, Feb. 2003

[26] “KAME-SHISA”, Mobile IPv6 for FreeBSD 5.4 [Online] http://www.kame.net/newsletter/20041211/shisa.html

[27] DoCoMo USA Labs announces its Open Source SEND Project[Online], http://www.docomolabsusa.com/lab_osrc_guide.html

[28] OpenSSL project [Online], http://www.openssl.org/

[29] OpenSSL project[Online], OpenSSL: Open source library written in C with ECC library, http://www.openssl.org/

[30] FreeBSD [Online], http://www.freebsd.org

[31] C. Vogt, “A Comprehensive and Efficient Handoff Procedure for IPv6 Mobility Support”, Proceedings of the 2006 international Symposium on a world of Wireless, Mobile and Multimedia.

[32] C. Vogt and M. Doll, "Efficient End-to-End Mobility Support in IPv6", Proceedings of the IEEE Wireless Communications and Networking Conference, IEEE, Apr. 2006.

[33] Shariq Haseeb and Gopakumar Kurup, “Performance Analysis of MIPL based Mobile IPv6 Testbed”, Proceedings of the 2007 IEEE International Conference on Telecommunications and Malaysia International Conference on Communications, 14-17 May. 2007, Penang, Malaysia.

[34] M. Handley and E. Rescorla, “Internet Denial-of-Service Considerations”, RFC4732, Nov. 2006.

[35] Denial-of-service attack [Online] , http://en.wikipedia.org/wiki/Denial-of-service_attack

[36] J.Postel, “Internet Control Message Protocol”, RFC792, Sept.1981

[37] A. Conta and S. Deering, “Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification”, RFC 2463, Dec.1998.

[38] Menezes, Alfred; van Oorschot, Paul C and Vanstone, Scott A. “Handbook of Applied Cryptography”. CRC Press, Oct. 1996. ISBN 0-8493-8523-7

[39] Keiichi Shima, Koshiro Mitsuya, Ryuji Wakikawa, Tsuyoshi Momoseand and Keisuke Uehara. “SHISA: The Mobile IPv6/NEMO BS Stack Implementation Current Status”, Asia BSD Conference 2007 Tokyo, Japan.

[40] Wireshark [Online], http://www.wireshark.org/

[41] Tcpdump [Online] , http://www.tcpdump.org/

[42] OpenSSH [Online], http://www.openssh.org/

[43] M. Roe, T. Aura, G. O'Shea, J. Arkko, Authentication of Mobile IPv6 Binding Updates and Acknowledgments, draft-roe-mobileip-updateauth-02.txt, Expired IETF Intenet draft, 2002.

[44] G. Shea, M. Roe, Child-Proof Authentication for MIPv6 (CAM), Computer Communications Review, April 2001.

[45] W.Haddad, L.Madour, J.Arkko and F.Dupont, “Applying Cryptographically Generated Address to Optimize MIPv6 (CGA-OMIPv6)”, draft-haddad-mip6-cga-omipv6-03.txt, Expired IETF Internet draft, 2004

[47] N. Koblitz, Elliptic curve cryptosystems, in Mathematics of Computation 48, 1987, pp. 203–209

[48] V. Miller, Use of elliptic curves in cryptography, CRYPTO 85, 1985.

[46] T. Aura, Mobile IPv6 security, in: Proceedings of the Security Protocols, 10th International Workshop, Cambridge, UK, April, LNCS, vol. 2467, 2002.

VITAE

Name Mr. Kuang Shilei

Student ID 4812127

Educational Attainment

Degree	Name of Institution	Year of Graduation
B.E.(ComputerEngineering)	JiangXi University of Science And Technology (JUST), China	2005

List of Publication and Proceeding

1. Shilei Kuang, Robert Elz and Sinchai Kamolphiwong, “Investigating Enhanced Route Optimization for Mobile IPv6,” in Proceeding of The Thirteenth IEEE Asia-Pacific Computer Systems Architecture Conference 2008 (ACSAC 2008), Taiwan (R.O.C). Aug. 2008.