INTEGRATING IDENTITY-BASED ENCRYPTION (IBE) IN THE RETURN ROUTABILITY PROTOCOL (RRP) TO ENHANCE SIGNALS SECURITY IN MOBILE IPv6

MAJED SALAM S. ALSAYFI

UNIVERSITI SAINS MALAYSIA

2010

INTEGRATING IDENTITY-BASED ENCRYPTION (IBE) IN THE RETURN ROUTABILITY PROTOCOL (RRP) TO ENHANCE SIGNALS SECURITY IN MOBILE IPv6

BY

MAJED SALAM S. ALSAYFI

Thesis submitted in fulfillment of the requirement for the

degree of Master of Science

June 2010

DECLARATION

Name: MAJED SALAM S. ALSAYFI

Matric No: P-COM0012/08

School: School of Computer Science

Thesis Title: INTEGRATING IDENTITY-BASED ENCRYPTION (IBE) IN THE RETURN ROUTABILITY PROTOCOL (RRP) TO ENHANCE SIGNALS SECURITY IN MOBILE IPv6

I hereby declare that this thesis I have submitted to **School of Computer Science** on **3 June 2010** is my own work. I have stated all references used for the completion of my thesis.

I agree to prepare electronic copies of the said thesis to the external examiner or internal examiner for the determination of amount of words used or to check on plagiarism should a request be made.

I make this declaration with the believe that what is stated in this declaration is true and the thesis as forwarded is free from plagiarism as provided under Rule 6 of the Universities and University Colleges (Amendment) Act 2008, University Science Malaysia Rules (Student Discipline) 1999.

I conscientiously believe and agree that the University can take disciplinary actions against me under Rule 48 of the Act should my thesis be found to be the work or ideas of other persons.

Students Signature: ……. Date: **3 June 2010**

Acknowledgement of receipt by: ……. Date: **3 June 2010**

ACKNOWLEDGEMENT

بسم الله الرحمن الرحيم

In the name of Allah, the Most Gracious, the Most Merciful. First and foremost, all praise to Allah for blessing me with the will, the dream, and the resources to complete this task.

My appreciation and special thanks go to my supervisor, Dr. **Wafaa A.H Ali Alsalihy** for her invaluable support and guide. She has always been an enthusiastic supporter of my work, providing a nearly unending supply of ideas. She helped made this thesis accomplishable. To her, I shall forever remain thankful.

I would like to express my deepest sincere gratitude to Associate Professor Dr. Azman Samsudin for his valuable advice and assistance through useful comments.

I thank all my friends and fellow participants who helped me from time to time. I am particularly grateful to Ahmed, Hani and Basim. I would also to thank my relatives and my friends in Saudi Arabia for their prayers, assistance, and encouragement throughout my study.

My gratitude goes to King Abdullah, for granting me scholarship to pursue my master degree. I also thank Universiti Sains Malaysia (USM) for all the support.

Last but certainly not the least, I wish to express my gratitude to my family. Special words of thanks go to my father, mother, brothers and sisters for their encouragement. I am especially indebted to my wife Um-Eyaed for her endless support throughout the entire period of my studies; her love has always been a constant source of inspiration for me.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATION

Abbreviation	Full
AH	Authentication Header
AVP	Attribute Value Paris
BA	Binding Acknowledgment
BC	Binding Cache
BR	Binding Request message
BRE	Binding Refresh message
BRR	Binding Error
BU	Binding Update message
CCOA	Collection Care-of Address
CGA	Cryptography Generating Address
CN	Correspondent Node
CoA	Care-of Address
CoT	Care-of Test message
CoTI	Care-of Initiation message
DH	*Diffie–Hellman* algorithm
DoS	Denial of Service
ESP	Encapsulating Security Payload
FA	Foreign Agent
HA	Home Agent
HMAC	Hash Message Authentication Code
HoA	Home Address
HoT	Home Test message
HoTI	Home Test Initiation message
IBE	Identity-Based Encryption

ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force
IPSec	Internet Protocol Security
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
IRDP	Internet Route Discovery Protocol
Kbm	Binding Management Key
Kcn	Correspondent Node Key
MAC	Message Authentication Code
MITM	Man In The Middle attack
MN	Mobile Node
NPT	Network Prefix Test message
PKG	Private Key Generator
PKI	Public Key Infrastructure
QoS	Quality of Service
RO	Router Optimization
RR	Return Routability
SHA1	Secure Hash Algorithm1
TCP	Transmission Control Protocol
vbfs	verification with a depth-first search
vdfs	verification with a breadth -first search

MENGINTEGRASI PENYULITAN BERDASARKAN IDENTIT (IBE) DALAM PROTOKOL BOLEH HALA SEMULA (RRP) UNTUK MENINGKATKAN SEKURITI ISYARAT DALAM IPv6 Mobil

ABSTRAK

IPv6 Mobil (Bergerak) membolehkan sesuatu nod dipindahkan daripada satu rangkaian ke rangkaian lain tanpa adanya sebarang gangguan komunikasi pada nod. IPv6 Mobil terdiri daripada Nod Mobil, Nod Sepadan dan Ejen Rumah. Prosedur keautentikan di antara nod adalah sangat penting untuk memastikan paket dapat dipindahkan dengan selamat (secure packet transfer) serta mobiliti internet yang selamat. Protokol boleh hala semula (return routability protocol) merupakan mekanisme yang digunakan dalam IPv6 Mobil untuk menyediakan nod dengan keautentikan tertentu. Protokol boleh hala semula tidak mampu menyediakan perlindungan sepenuhnya di antara nod mobil dan nod sepadan dalam IPv6 Mobil. Penceroboh, terutamanya ejen yang bertindak sebagai *Man-In-The-Middle*, boleh dengan mudah memintas serta memainkan semula paket, malahan ia juga boleh mengubah suai paket di antara kedua-dua nod tersebut. Nod sepadan tidak mengetahui sama ada sesuatu paket itu dipindahkan daripada mod mobil yang autentik ataupun tidak. Begitu juga dengan mod mobil, ia juga tidak mengetahui sama ada sesuatu paket itu dipindahkan daripada mod sepadan yang autentik ataupun penyerang. Oleh itu, tahap kepercayaan di antara mod adalah lemah. IPv6 Mobil tidak akan berfungsi dengan baik jika keautentikan di antara kedua-dua nod adalah gagal. Tesis ini mencadangkan penggunaan Penyulitan berasas Identiti (Identity-Based Encryption) sebagai suatu cara untuk meningkatkan keselamatan dan keautentikan dalam protokol boleh hala semula. Penyulitan Berdasarkan Identiti adalah mekanisme keselamatan yang memerlukan pihak

ketiga (iaitu, Penjana Kunci Persendirian (Private Key Generator)) untuk mengagihkannya. Keadaan ini mampu meningkatkan protokol boleh hala semula di antara kedua-dua nod mobil bagi membolehkan keautentikan dan keselamatan yang kuat. Protokol Penyulitan Berdasarkan Identiti – boleh hala semula (Return Routability-Identity-Based Encryption, RR-IBE) dinilai menggunakan penyemak model keselamatan. protokol (RR-IBE) mampu mencegah serangan Man-*In*-*The*-*M*iddle pada keselamatan nod dan mencapai keautentikan di antara nod (contoh: nod mobil dan mod sepadan) berjaya dibangunkan.

INTEGRATING IDENTITY-BASED ENCRYPTION (IBE) IN THE RETURN ROUTABILITY PROTOCOL (RRP) TO ENHANCE SIGNALS SECURITY IN MOBILE IPv6

ABSTRACT

Mobile IPv6 allows a node to move from one network to another network without any disruption in communication at the node. Mobile IPv6 consists of the Mobile Node, the Correspondent Node and the Home Agent. The authentication procedure between nodes is very important so as to achieve secure packet transfer and a secure Internet that supports mobility. Return Routability Protocol is a mechanism used in Mobile IPv6 to provide the nodes with some authentication. The Return Routability Protocol is not sufficiently secured so as to provide enough protection between the mobile and the correspondent nodes in Mobile IPv6. The attacker, particularly an agent acting as a Man-In-The-Middle attack, can easily intercept and replay packets and even modify packets between the mobile and the correspondent nodes. The correspondent node does not know whether a packet has come from a valid mobile node or a malicious node. Similarly, the mobile node does not know if the packet has come from a valid correspondent node or an attacker. Thus, the level of trust between the nodes is weak/low. The Mobile IPv6 will not function properly if the authentication between mobile and correspondent nodes fails. This thesis proposes the use of Identity-Based Encryption as a means to enhance security and authentication in the Return Routability Protocol. Identity-Based Encryption is a security mechanism which requires a third party (*i.e.* Private Key Generator) to distribute these types of keys. The enhancement in the Return Routability Protocol between the mobile and the correspondent nodes has resulted in strong authentication and security. The proposed Return Routability-Identity-Based Encryption (RR-IBE) protocol was evaluated using the

CMurphi Security Model Checker. This protocol (RR-IBE) is clearly prevents the Man-In-The-Middle from attacking the security of the nodes and obtains the authentication between the nodes (*i.e.* the mobile and the correspondent nodes).

CHAPTER 1

INTRODUCTION

1.1 Introduction

Internet Protocol Version 6 (IPv6) is the next-generation Internet protocol used to overcome the limitation in Internet Protocol Version 4 (IPv4). The IPv6 protocol, sometimes called IPNG, solves the problem of the limited number of available IP addresses, which has become a significant impediment to the rapid growth of the Internet. However, work must be done in the development of this new protocol to correct a number of weaknesses inherent in the current Internet protocol, such as a failure to provide safety and support for mobile devices that need for automatic configuration of network devices and improved Quality of Service (QoS).

Currently, mobile networks are a focus of mobility-orientated research. These networks are called Mobile IPs, and they have been categorised by the Internet Engineering Task Force (IETF) in terms of both homogenous and heterogeneous networks (Perkins *et al.*, 2003). In 1996, the IETF mapped Mobile IP onto an open standard with RFC 2002, which enables users to maintain the same IP address and stay in contact when moving between networks.

Mobile IPv6 [RFC 3375] is the Mobile IP support protocol for IPv6. Its specification has been standardised by the IETF to include several security mechanisms, such as mobility protocols (Huafei *et al.,* 2004).

The Mobile IPv6 protocol is a network layer of IPv6 that allows one node to communicate directly with another node. The mobile network allows its user to remain

connected while it changes its location to a foreign network. Any IPv6 node can access the host if the node supports Mobile IPv6 by defining its home address, regardless of the host's location. The Mobile IPv6 protocol allows a mobile node to seamlessly move from one network to another. If the care of Address (CoA) address gets changed when the mobile node moves, the Home Address (HoA) remains the same address.

The main elements comprising Mobile IPv6 are the mobile node (MN), the home agent (HA), the correspondent node (CN), the visitor list, the binding update (BU) message, the binding error (BRR) message, the binding cache (BC) entry, the request registration message and the binding acknowledgment (BA) message. These components operate within the mobile network as shown in Figure 1.1

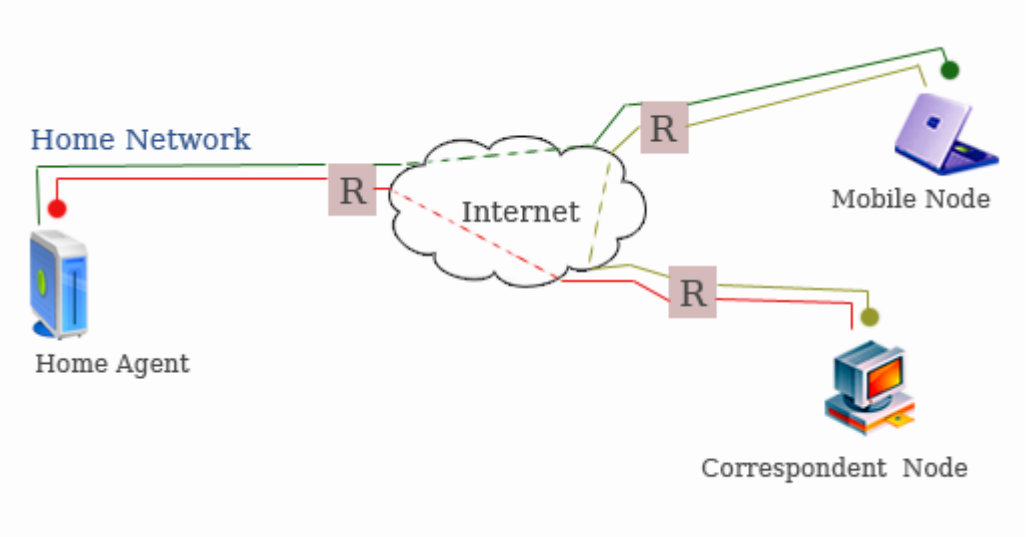

Figure 1.1: Mobile IPv6 framework

Figure 1.1 shows three routers and three components, namely the HA, the MN and the CN. The MN communicates with the CN in two ways: through HA and directly with the CN.

1.2 Background

In Mobile IPv6, the MN in the home network communicates with the CN using a static IP address HoA and CoA. Each home network involves the HA, which is in charge of sending or receiving messages between the MN and the CN successively.

When the MN moves to a foreign network, it receives a new IPv6 address, which is called CoA. It registers a new IP address in the HA by sending a BU message without returning to the foreign agent. In other words, the CN directly communicates with the MN even if it moves to another network. It cannot directly connect to the MN, and instead, must communicate via the HA is called triangular routing. After it connects with the MN using the HAs, it forwards a message to the MN via the IPSec (Internet Protocol Security) tunnel to the new location. Afterwards, they exchange messages directly between MN and CN is called Route optimization (RO). In the home network, the BU message that is sent via the MN to the HA is already protected because it uses the IPSec tunnel, as shown in Figure 1.2.

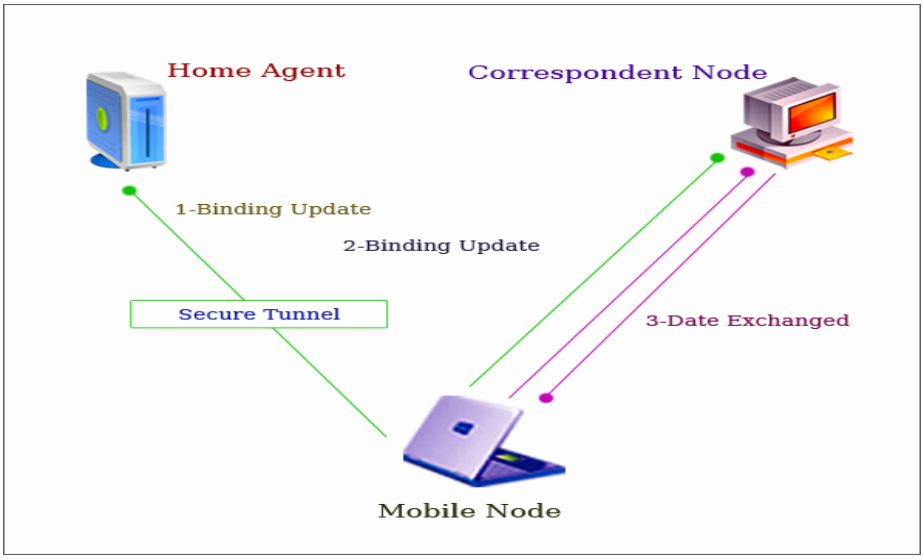

Figure 1.2: Exchange messages between MN and HA

In Figure 1.2, there is no secure tunnel between MN and CN, which means that the BU message sent directly by the MN to the CN is not secured because it does not pass through the IPSec tunnel. The integrity and authentication between MN and CN is essential to ensuring a correct movement of the BU message. In the meantime, IPSec tunnels are encapsulated between the MN and HA messages.

Methods of securing the BU message between the MN and CN include Public Key Infrastructure (PKI), Cryptography Generating Address (CGA) and the normal Return Routability (RR) Protocol. The normal RR Protocol is a mechanism to secure the BU message. This mechanism requires two cookies: Home Test Initiation message (HoTI) and Care-of Test Initiation message (CoTI). The normal RR Protocol consists of four messages: HoTI, CoTI, Home Test message (HoT) and Care-of Test message (CoT). One of the main goals of the normal RR Protocol is to verify the BU message between MN and CN (Blanchet, 2002), as illustrated in Figure 1.3.

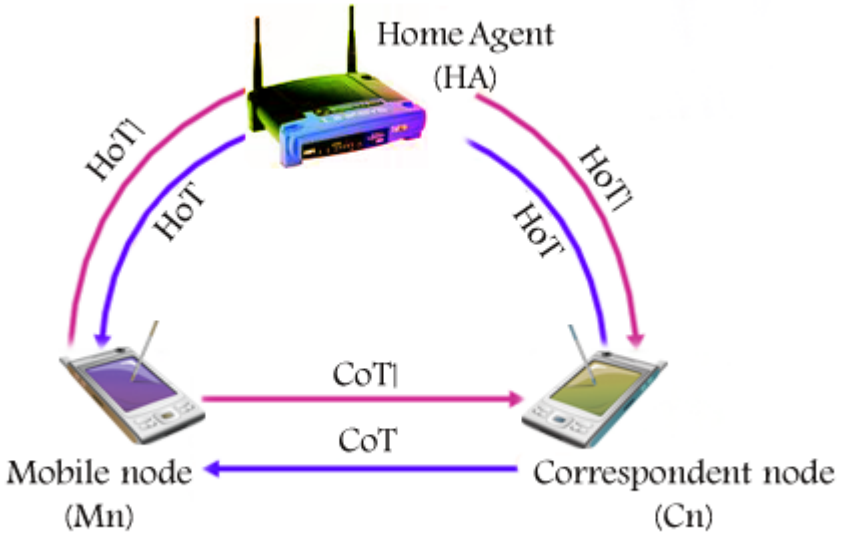

Figure 1.3: Normal RR Protocol mechanism

1.3 Problem Statement

The normal RR Protocol is a secured protocol that is used in Mobile IPv6. Securing communications between the MN and the CN can be an inefficient process. More specifically, an active intruder can hijack the BU message and change its value. This hijack occurs when the intruder sends two cookies to the CN. The CN does not know whether these messages are coming from the MN or from one of the intruders. This confusion is due to the lack of authentication between the nodes (MN and CN) when they need to exchange messages.

Researchers have studied security between nodes in RO. The RO station protocol used to protect the contract between MN and CN is called the normal RR protocol. Some researchers have suggested to replace normal RR protocol to new protocols to improve RO security, but others prefer to focus on enhancing the normal RR protocol (Kavitha, *et al*. 2009; Ahmed *et al*. 2007; Susanto and Kim, 2009; Mehdizadeh et al. 2008). Despite these researchers' attempts to enhance the RR protocol, a lack of authentication between the MN and CN still exists. A Man-In-The-Middle Attack (MITM) can change the data without alerting the other node. In this thesis, a new method will be proposed to enhance the security of the normal RR protocol, including improving the authentication between nodes when they exchange messages as illustrated in Figure 1.4. This method is called RR- Identity-Based Encryption (RR-IBE) protocol. The question posed is as follows: "Can RR-IBE protocol achieves better security and overcome weak authentication in the normal RR protocol while exchanging messages between MN-CN and CN-MN in Mobile IPv6?"

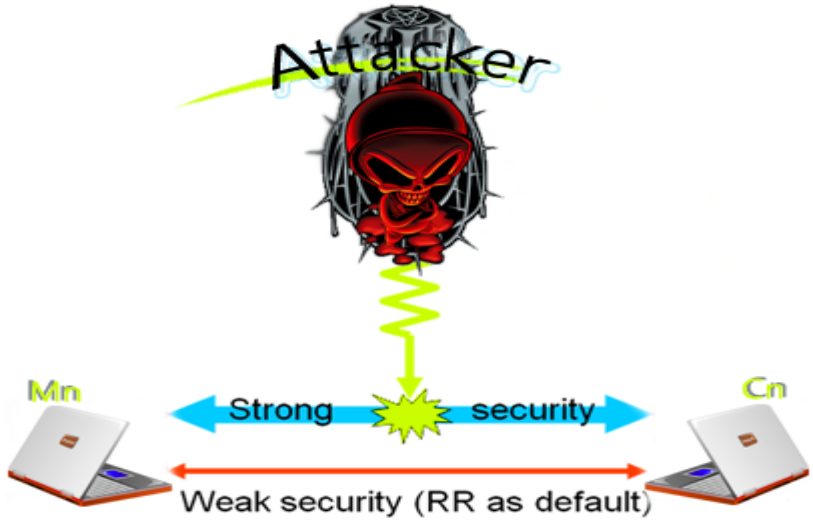

Figure 1.4: Weak security in the normal RR Protocol between MN and CN

1.4 Research Objectives

Generally, the main objective of this thesis is to achieve security in the RO communications in Mobile IPv6. Specifically, these objectives are:

- To enhance the normal RR Protocol with IBE in order to overcome security shortcomings of the existing RO approach in Mobile IPv6.
- To evaluate the proposed RR-IBE protocol by using the CMurphi model checker.

1.5 Motivations

There has been a significant increase in the number of wireless devices. These devices need to be in constant contact during transitions this is especially true for laptops and mobile devices in relation to satellite navigation. This need is the primary motivation behind this research. The second motivation is to better support the continual increases in the numbers of users of these devices. A third motivation is to address the limitations in the authentication process between nodes when CN receives messages and re-sends them without any knowledge about the source.

1.6 Scope of the Study

The transition process in the normal RR Protocol can be broken down into two routes. The first is from the MN to the CN through the HA. The second is directly from the MN to the CN. Both methods need to be more secure in their transition processes. This study will focus on the path between the MN and CN and the security threats of MITM who may alter messages as they travel to the other party. The process of authentication is essential to ensuring the secure transfer of messages.

1.7 Contribution of this Thesis

The main contribution of this thesis involves creative methods of implementing IBE for the Mobile IPv6 with normal RR protocol. The goal is to provide secure communication and mutual authentication, to prevent MITM and to achieve the security and authentication between MN-CN, CN-MN and from HA to CN.

1.8 Organization of this Thesis

There are six chapters in this thesis. The first chapter introduces the material and the problem to be solved and discusses the thesis goals. In addition, motivations and key contributions are outlined. In the second chapter, the general background of Mobile IPv6 is introduced, and related works are discussed. The third chapter presents the proposed methodology and research design. In the fourth chapter, explain the proposed work, the fifth chapter highlights the evaluation process and related results. The evaluation and comparison of our proposed method is then mapped against the results of other works. The sixth chapter offers conclusions along with future recommendations.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

Mobile IPv6 is a version of the Mobile IP. In the network layer, the Mobile IPv6 protocol allows a node to directly talk with another node. The Mobile IPv6 allows a user to remain connected while the user changes his/her location to a foreign network. Mobile IPv6 is important in many applications for the military, aircrafts, hospitals, and mobile devices, between others. Mobile IPv6 is important because it enables the user to stay connected while moving between networks.

Mobile IP is based on the concepts of MN, CN and HA, HOA, COA, Collection care-of address (CCOA), Binding cache message (BC), Binding request message (BRE), Binding error message (BRR), Binding registration message (BR), Binding update message (BU), Binding Acknowledgement message (BA), Tunnel, Foreign Agent and visitor list (number of MNs in a foreign network).

1- Mobile node: This node has two addresses. These are static IP addresses called HoA and CoA. HoA is never changed, but CoA does change when the MN moves to a new network. When the MN loses its connection or movement, it must immediately tell HA its new CoA.

2- Correspondent node: This is a node that communicates either directly with the MN or through the HA.

3- Home address: This is a standing IP address that is referred to the MN when it is in the home network.

4- Foreign network: This is any new network visited by the MN.

The primary CoA is the current CoA for the MN. When the MN moves across two networks - for example, when each primary CoA moves through two different foreign networks - a new CoA1, which is called the primary address, will be obtained. However, when the MN roams on the adjacent foreign network B, another CoA2, also called primary (the primary address moves from sCoA1 to CoA 2), will be obtained.

5- Home agent: This router is located on the home network and it provides services to the MN. The HA also receives packets from all of the MN, the CNs and foreign networks. Each node has a binding cache message that defines the authentication cache. the cache message contains the CoA of the MNs. For each move, HA must update the binding cache.

6- Binding request message: This message is sent by any node to request the current location of a MN.

7- Binding error message: This message tells the node to update its binding cache. The BU message is used to declare where the MN is currently located.

8- Tunnel: A tunnel is used when a packet is sent from a foreign agent to the HA to register with a new CoA of the MN, as shown in Figure 2.1.

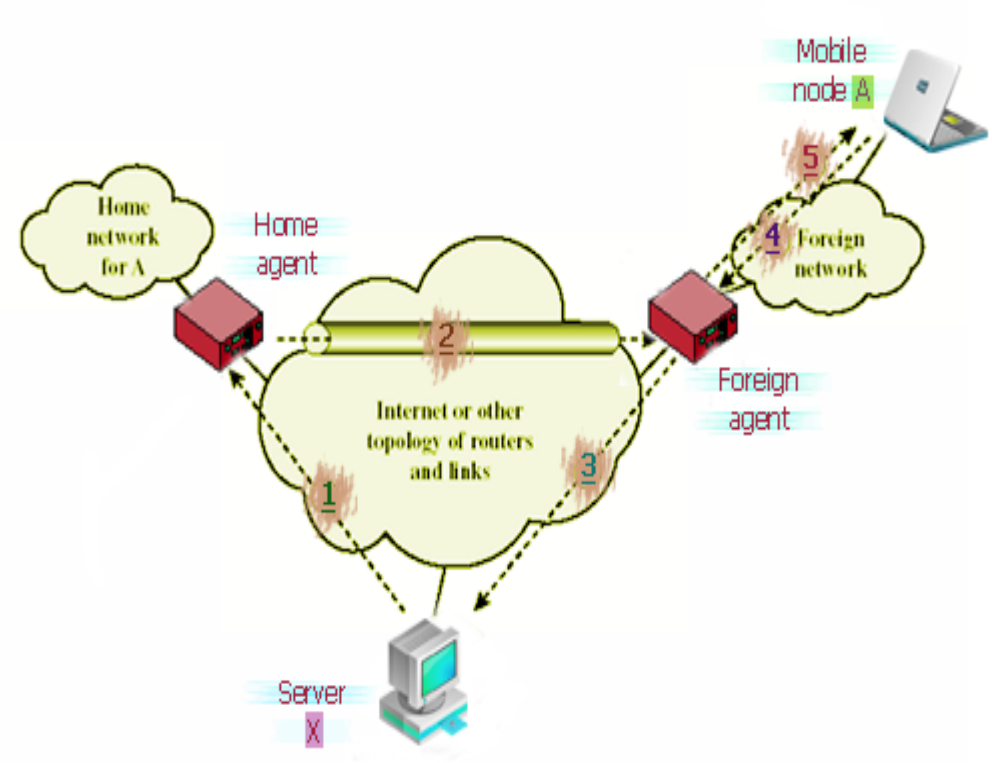

Figure 2.1: Tunnelling between the HA and FA in Mobile IPv4

In Figure 2.1, the MN **A** in the foreign network CN (server) sends a message to the MN via the HA, then the HA repeats the same thing in the foreign agent via the tunnel. After this step, the foreign agent sends a message to the MN **A**. The MN **A** receives the message and forwards it again to the foreign agent, which will send it directly to the CN without returning to the HA.

The Mobile IPv6 works when the MN sends both HoA and CoA messages via the IPSec to the HA and tot CN. The HA receives an encapsulation message from the MN and re-capsulates it, so that it can be sent to the CN. The path between the HA and MN is secured by the IPSec tunnel, as the end-to-end framework is secured by IPv6.

However, MN can send the packet directly to the CN. The path between these two is not secured by the IPSec tunnel, as illustrated in Figure 2.2.

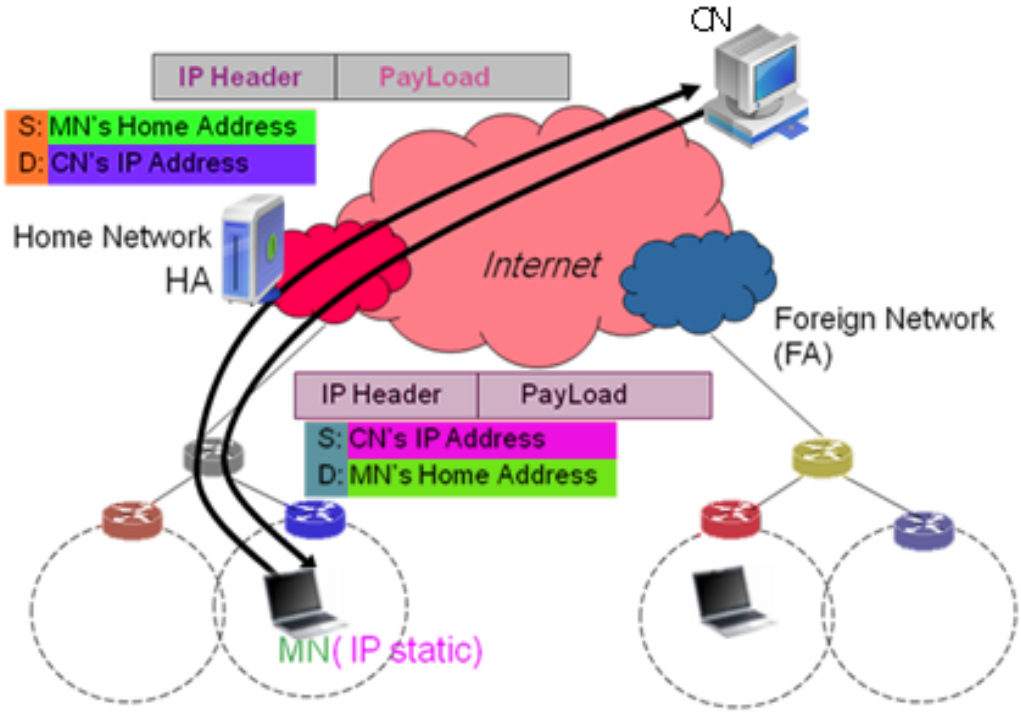

Figure 2.2: A message transmission in Mobile IPv6

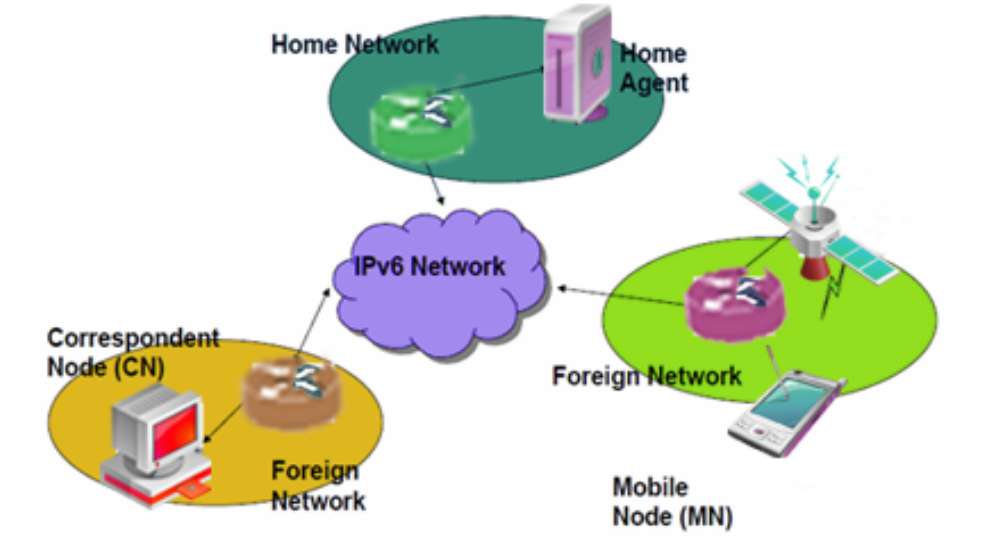

Figure 2.3: The CN and the MN exchanging messages between different networks

As shown in Figure 2.3, when both the MN and the CN communicate with the foreign network, the MN sends a registration message to the HA by sending a BU message.

2.2 Mobility header:

The mobility header contains the following: payload prototype, Header Len, MH type, Reserved, checksum, and message (Li *et al*. 2009), as shown in Figure 2.4. The mobility header features a subsection that contains other headers, as described in (Li *et al*. 2009; koodli and Perkins, 2007; Soliman, 2004; Stojmenovic, 2002).

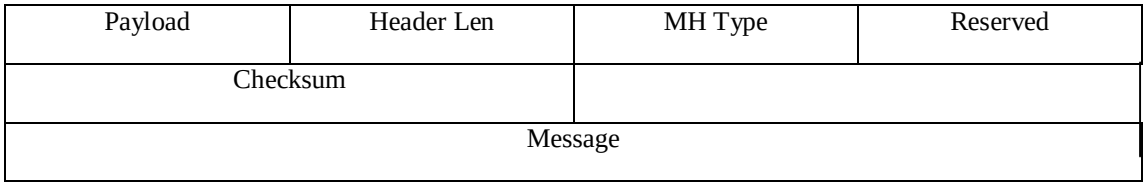

Figure 2.4: Mobility Header

2.2.1 Binding Update Message

A BU message is used by the MN when it switches to another network to register its current location. The BU message is also used for transport between the CN and the MN to update the BC entry. The MN on the home network sends the BU message in two ways. First, it sends this message directly from the MN to the CN without IPSec tunnelling. Second, when the transmission of this message occurs from the HA to the CN, it is moved via the IPSec tunnel between the MN and the HA.

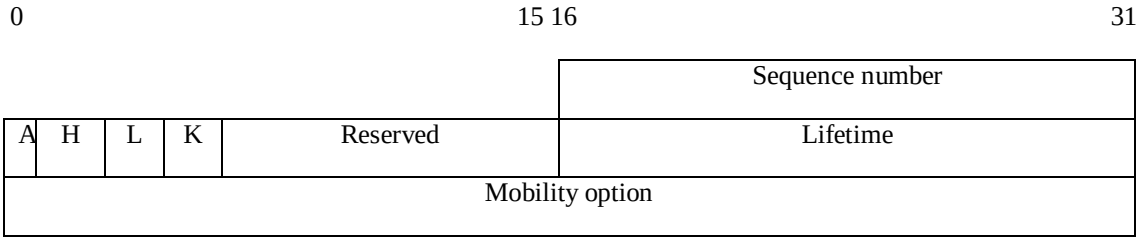

Figure 2.5: Binding Update message

As shown in Figure 2.5, the BU message contains four fields and four flags. The first field is the sequence number field, which contains a sequence number. The second field is the reserved field. The third field is the lifetime field, which is what binds the information. The fourth field is the mobility header, which consists of a set of messages. Table 2.1 illustrates the four flags.

Table 2.1: Binding update message flags

Flags	Description
A	Requires binding acknowledgment to respond to the binding update message
H	Home registration
L	Link-local address compatibility
K	Key management mobility

The BU message is protected between the HAs and MNs because it is usually processed through the IPSec:

- In the BU message, the Encapsulating Security Payload (ESP) encapsulation and the BA between HA and MN must be used and efficiently supported.

- In the HoTI, the ESP encapsulation between HA and MN must also be used and efficiently supported.
- In the ICMPv6, the prefix discovery is considered the basis of the ESP's encapsulation use and support.
- To maintain and protect the authenticity of Mobile Prefix Solicitations and Advertisements, an IPSec security association must be used by the HA and the MN. Accordingly, the IPv6 end-to-end security is the basis of this usage.
- Connectionless integrity, optional anti-replay security and data origin authentication is provided. The ESP header is used and supported by both MN and HA. This action is performed with a non-null payload authentication algorithm in the transport mode.

2.2.2 Binding Acknowledgment message

The Binding Acknowledgment (BA) message sends effective BU messages to the HA or the CN. The source address for this binding is in either the HA or the CN, and the destination address is the CoA of MN. This message contains the MAC, the sequence number and the status.

In Figure 2.6, the BA message contains five fields and one flag. The first field is the status, which is the definite outcome of the received BU message. The second field is the reserved field. The third field is the sequence number, which indicates the number of copies that contain the latest BU message and the latest sequence number when MN sends the BU message, which is sent by MN once it moves to another network. The lifetime is the fourth field, which is used for binding the information. The fifth field is

the mobility header. The flag (K) is the key to management mobility, which follows directly after the status.

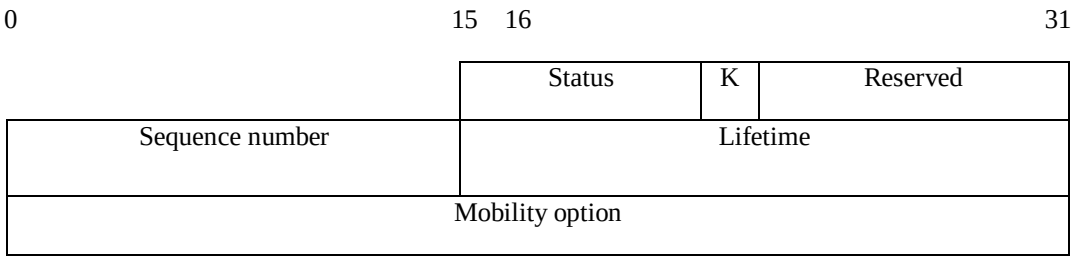

Figure 2.6: Binding Acknowledgment Message

2.2.3 Updating Binding Caches

Before the CN sends any message to the MN, it conducts operations such as checking the BC's entry. The CN immediately sends a CoA message to the MN when it locates the BC entry. The HA receives a datagram from the CN and forwards it to the MN via the IPSec tunnel. At the same time, the HA sends an authenticated BU message to CN to inform it of MN's current location. Hence, every binding has a lifetime, especially the BU message, as shown in Figure 2.7.

Figure 2.7: Steps of updating the binding cache

In Figure 2.7, the CN sends packets to the HA in the home network. Then, the HA sends an authentication BU message that in turn delivers packets to the foreign agent. The MN then receives packets from the foreign agent. Finally, a communication link is established between the MN and the CN.

2.2.4 Binding Error Message (BERR)

The BERR reports errors in a BU message as shown in Figure 2.8, which is normally sent by a CN.

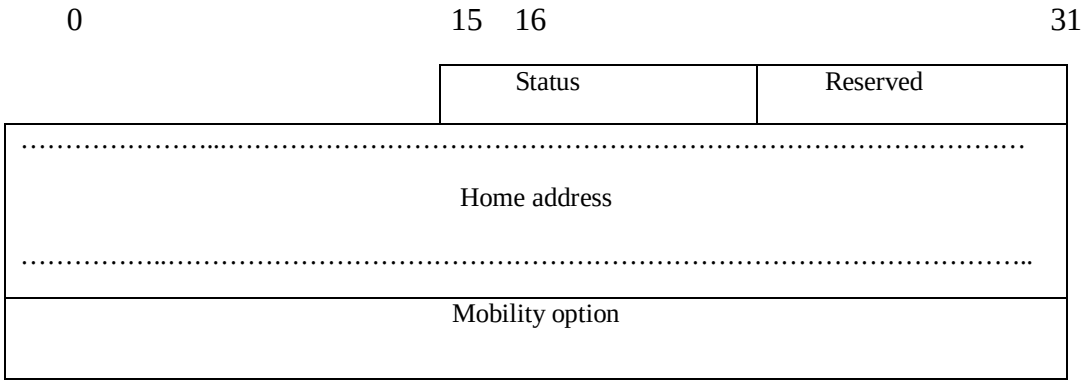

Figure 2.8: Binding error message

Some mobility messages can contain mobility message options. The following options (Johnson *et al*. 2004; Li *et al.* 2009) are defined:

1-The Pad1 option:

The Pad1 option is used when one byte of padding meets the partial requirements of one or more mobility options, upon which a padding signal is inserted (Li *et* al. 2009) as shown in Figure 2.9.

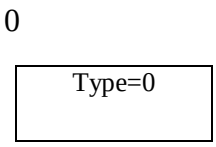

Figure 2.9: Pad1 option

2-The PadN option:

The PadN option uses two or more bytes of padding. This option meets certain requirements related to the mobility option (Li *et al*. 2009), as shown in Figure 2.10.

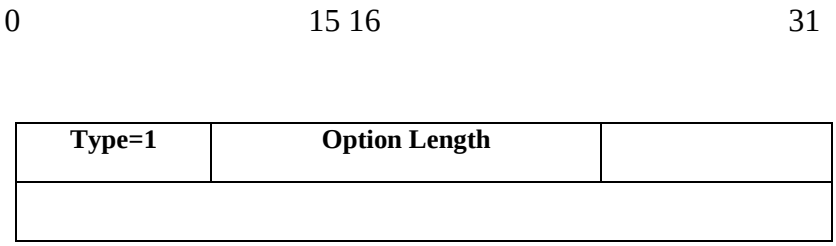

Figure 2.10: PadN option

2.2.5 Binding Refresh advice option

The Binding Refresh (BR) advice option is used to recommend that a portion of the BU message update the binding information. The binding refresh advice option uses BA sent from HA to MN, and it determines the amount of time before MN sends a new registration. The option is shown in Figure 2.11.

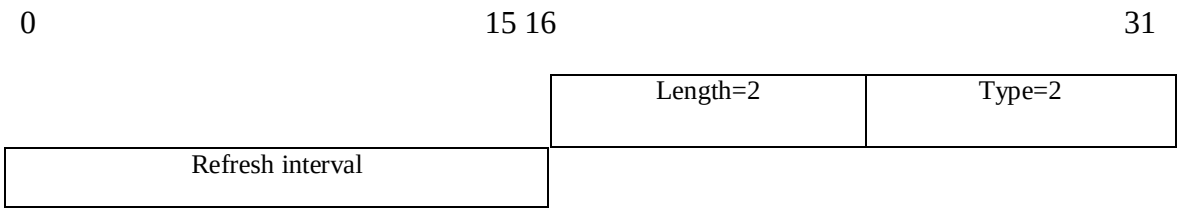

Figure 2.11: Binding Refresh Advice option

2.2.6 Alternate Care-of-Address Option

The alternate CoA option uses two case scenarios with BU messages. In the first scenario, the MN needs to a static address (HoA) to any nodes in the home network. The second option is to save or protect the CoA information over the path. In the home registration (home network), the BU message must be protected by IPSec between MN and HA. The source address in IPv6 always uses CoA, as shown in Figure 2.12.

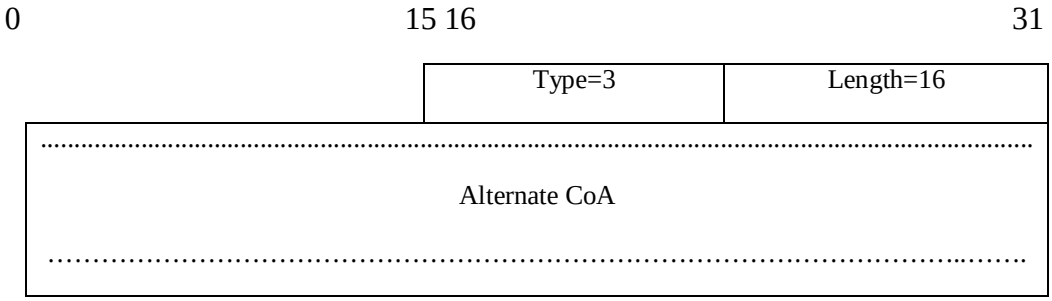

Figure 2.12: Alternate CoA option

2.2.7 Binding Authorisation Data Option

The binding authorisation data option is used to store a hash value computed for the BA message and the BU message. This option includes cryptography information (e.g., the secret key (*Kcn*)), as shown in Figure 2.13.

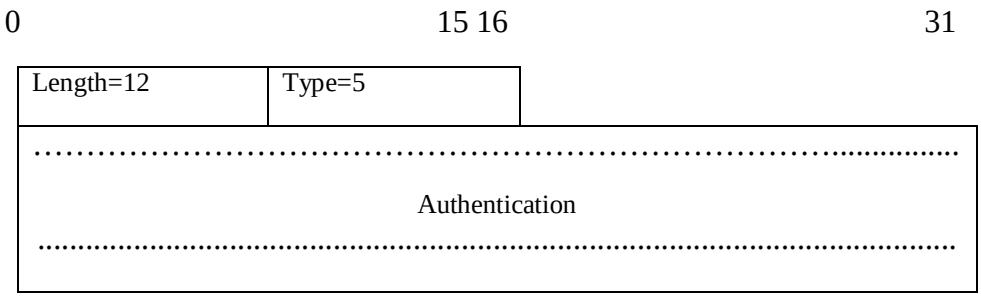

Figure 2.13: Binding Authorisation Data Option

Nonce Indices Option

The Nonce Indices option is used with the binding authentication data option because it needs to determine the binding key. This option is shown in Figure 2.14.

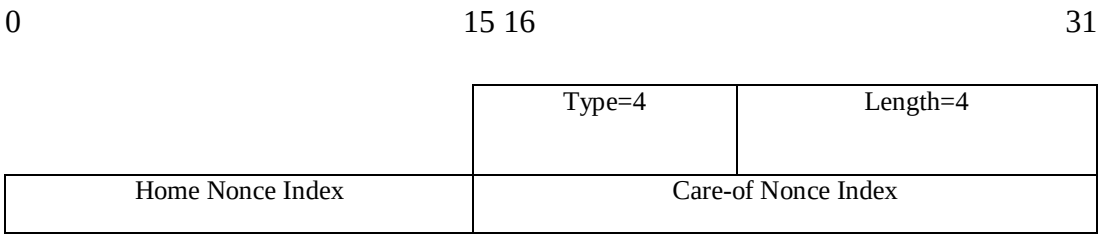

Figure 2.14: Nonce Indices option

2.3 Mobile IP Stages.

2.3.1 Agent Discovery stage

A MN is discovered by the home network or the foreign network as part of the agent discovery stage. By using the Internet Control Message Protocol (ICMP) and internet Router Discovery Protocol (IRDP), HA and the foreign agent will send an advertised message to the MN, as shown in Figure 2.15. This action is performed by leasing the mobile IP extension. MNs are known as the existing point of attachment for these advertising messages. If the MN cannot obtain these messages, it might request that the HA or the foreign agent send an advertisement after receiving a solicitation message, as shown in Figure 2.16. These types of server agent may be identified by the MN.

Figure 2.15: HA or FA sends advertisementmessage to MN

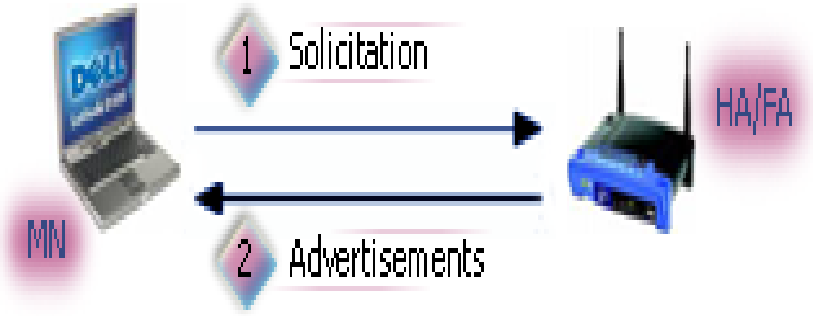

Figure 2.16: The MN begins sending a solicitation message to receive an advertisement message from the HA or from the foreign agent

2.3.2 Registration stage

An MN changes its IP address when it moves to another network. At each move, it gets a new CoA that requires registration through the HA. The MN sends a registration request message to the HA through the foreign agent (FA) in Mobile IPv4, as shown in Figure 2.17. However, in Mobile IPv6, the same message is sent directly to the HA without passing through the FA, as shown in Figure 2.18, to register its CoA (current location). The registration request message that is sent by the MN to the HA is called the

BU message. To successfully deliver packets to and from the MN, the registration message should be authenticated. The HA sends a registration reply message to the foreign agent or directly to the MN. The Registration message is requested by tunnelling between the HA and the FA. Before the time expires, the MN should register its current location (i.e., in the FA or the HA of Mobile IPv4). After this step, the HA and the FA update the binding cache and visitor list entry for the FA.

Figure 2.17: The MN sends a registration request message to HA via a FA in Mobile IPv4

Figure 2.18: The MN directly registers its current location through the HA in Mobile IPv6

2.3.3 Tunnelling stage

In the tunnelling stage, one end of the secured tunnel encapsulates the data packets and the other end of the tunnel is de-capsulated; this occurs when the CN sends packets via the HA to the MN. If the MN is at the home network, the HA will receive the packets and encapsulate them after they have been forwarded to the MN via the IPSec tunnel.

When the MN is away, the CN sends packets to the HA, which then encapsulates the packets and sends them to the foreign agent. The FA de-capsulates the packets and sends them to the foreign agent, as shown in Figure 2.19. The MN uses the HA when the packets are sent to the FA. This agent encapsulates the data packets, then sends them to the HA via tunnelling The HA delivers the packets to the CN after they have been de-capsulated, as shown in Figure 2.20.

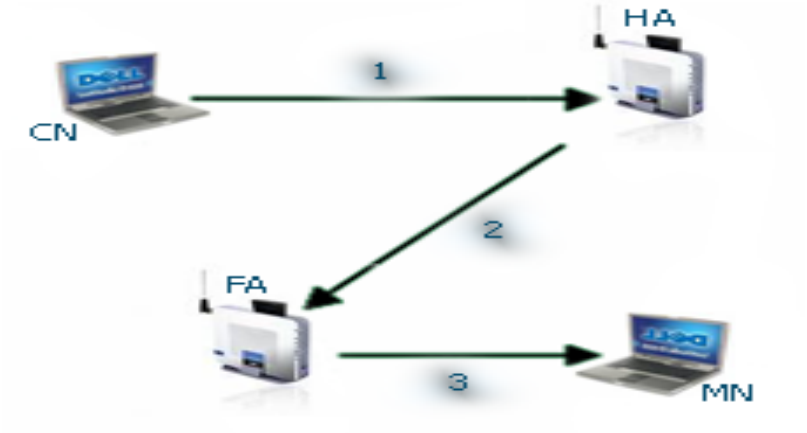

Figure 2.19: The CN starts to send packets to MN on the foreign network

Figure 2.20: The MN sends packets to CN via foreign network

2.3.4 Smooth Handoff

When the MN moves from the home network to the foreign network, it receives a new IP address. The MN registers the request message IP address in the HA either via the FA or directly using a CCoA. When the MN moves to a new foreign network, it receives gets a new CoA that is different from the previous one. The MN then informs the previous foreign agent about its current location, using a process that is called a smooth handoff. These handoffs are provided to notify the previous FA about the new location of the mobility binding (Kavitha *et al*. 2009). The HA sends a BU message to the MN in the old location before it knows about the movement of the MN. The FA sends a BERR message to the HA to announce that the MN is not available.

A new FA is registered with the previous FA by sending a BU message. When the CN communicates with the MN in the foreign network, it sends packets to the HA, before forwarding BU message to the first FA. The first FA then sends these packets to a new FA and then agent forwards them to the MN. Thereafter, MN replays the message

in the same way. Thus the CN communicates directly with the MN in the new location, as shown in Figure 2.21.

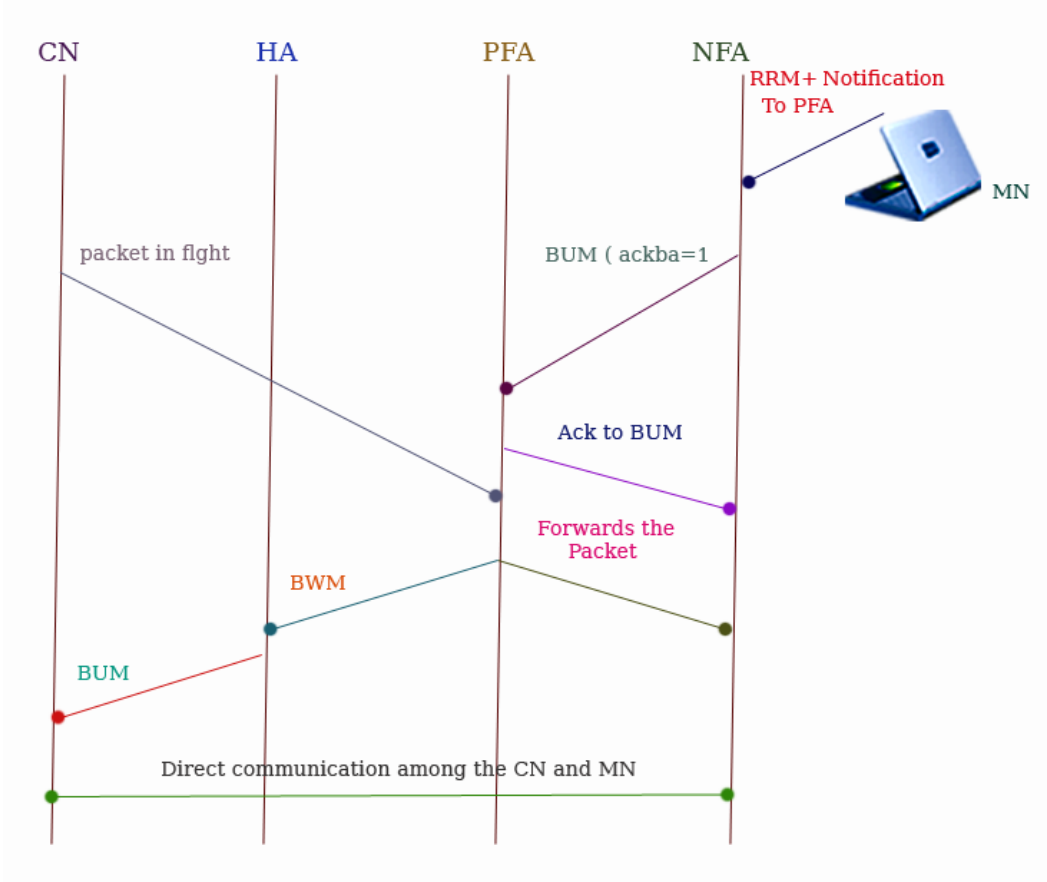

Figure 2.21: Basic Smooth Handoffs under Mobile IPv4

Figure 2.21 shows three agents: the HA, the previous agent, the new FA and one node (CN). The CN sends packets to the previous foreign agent via the MN. The previous FA sends a BERR message for the HA to require that the MN move into another foreign network. A new foreign agent sends a BU message to the previous foreign agent to announce a new available CoA. Afterwards, it replays to the BA a message for the new FA. The previous foreign agent sends to the HA a binding request