SEAMSAR: SEAMLESS AND SECURE HANDOVER MODEL FOR MOBILE IPTV USING MIPV6

BY

ARMANDA CAESARIO CORNELIS

Thesis submitted in fulfillment of requirements for degree of
Master of Science

JULY 2011

ACKNOWLEDGEMENT

In the name of Allah, the most merciful, the all compassionate, Praise to Allah SWT, we seek His help, guidance and help. I want to thank to the creator of this universe for everything He gave to me.

I would like to thank to my supervisor Associate Prof. DrRahmatBudiarto for his patience, motivation, encouragement, support, and guidance to finish this thesis. I also want to thank to my co-supervisor Dr. Wan Tat Chee for his guidance and comments. Likewise, I want to thank to dean of School of Computer Sciences Prof.Rosni Abdullah for providing me support during conduct my research and write this thesis.

I would like to thank my lovely parents, my kindhearted Robbie HalimMandagie and my lovely mother DyahUmiyati for their tireless support and encouragement. In addition, I want to thank to my auntie SitiRomadhona for her patience, support and encouragement. Special thanks to my cousins AriniWidhiasi, MitaZoraida and Dr. Muhammad Fermi Pasha for their encouragement and help to finish this thesis. I also want to thank to all of my relatives who always stood beside me and encouraging me during my studies.

Finally yet importantly, I would like to thank to my colleagues at postgraduate lab for their comments and encouragement, and my friends who always gave me supports

TABLE OF CONTENTS

LIST OF TABLES

Page

LIST OF FIGURE

Page

LIST OF ABBREVIATION

AAA	Authentication and Authorization
AAAH	Authentication and Authorization Home
AAAF	Authentication and Authorization Foreign
AR	Access Router
BU	Binding Update
BA	Binding Acknowledgement
CN	Correspondent Node
FA	Foreign Agent
FBU	Fast Binding Update
FBack	Fast Binding Update Acknowledgement
HA	Home Agent
Hack	Handover Initialization Acknowledgement
HI	Handover Initialization
HoA	HA Authentication and Authorization Acknowledegement
HoR	HA Authentication and Authorization Request
MN	Mobile Node
NAR	Next Access Router
PAR	Previous Access Router

SEAMSAR: MODEL PENYERAHAN YANG SELAMAT DAN TAK BERKELIM UNTUK IPTV MUDAH ALIH MENGGUNAKAN MIPv6

ABSTRAK

Multimedia telah menjadi satu kandungan yang paling dikehendaki dalam dunia Internet moden. Sejak Protokol Internet Mudah alih versi 6 (Mobile Internet Protocol 6 -MIPv6) dicadangkan sehingga sekarang banyak penyelidik telah mencuba untuk mengembangkan kaedah dan protokol untuk meningkatkan prestasi perkhidmatan multimedia mudah alih. Penyerahan adalah satu proses peralihan ketika satu nod mudah alih berpindah dari rangkaian asal kepada rangkaian asing. Peralihan ini menyebabkan masa lengah yang berpengaruh terhadap penghantaran data. Dalam perkhidmatan multimedia mudah alih, masa lengah yang panjang dalam penghantaran data boleh menyebabkan ketidakselesaan kepada pengguna.

Tesis ini mencadangkan satu model penyerahan tak berkelim dan selamat dengan memperkenalkan satu proses kemas kini ikatan secara serentak pada nod koresponden dan agen rumah, Proses kemas kini ikatan secara serentak mengurangkan masa lengah dibandingkan dengan FMIPv6 yang asal, yang menggunakan proses kemas kini ikatan secara berturutan. Kemas kini ikatan secara serentak memerlukan satu alamat sementara (*care* of-*address*) yang unik secara global. Penyelidikan ini juga memperkenalkan penggunaan pengenal antara muka*International Mobile Subscriber Identification*(IMSI) untuk membuat alamat sementara. Kerana IMSI unik secara global, maka alamat sementara yang dibangun oleh kaedah yang dicadangkan adalah unik secara global, oleh itu proses pengesanan alamat bertindih tidak diperlukan pada kemaskini ikatan di agen rumah.

Prestasi model yang dicadangkan telah disahkan menerusi simulasi menggunakan OMNET++. Keputusan percubaan menunjukkan bahawa model yang dicadangkan secara purata mengurangkan masa lengah masing-masing 46%, 47%, dan 47% bagi senario laju rendah, sederhana dan tinggi. Disamping itu, pengesahan keselamatan menggunakan peralatan CMurphi menunjukkan bahawa model yang dicadangkan adalah selamat.

SEAMSAR: SEAMLESS AND SECURE HANDOVER MODEL FOR MOBILE IPTV USING MIPV6

ABSTRACT

Multimedia becomes one of the most wanted content in the modern Internet world. Since the Mobile Internet Protocol version 6 (MIPv6) was proposed until today many researchers have been trying to develop methods and protocols, in order to improve the performance of mobile multimedia services. Handover is a transition process when a Mobile Node (MN) moves from home network towards foreign network. This transition causes a latency that affected the data delivery. In mobile multimedia service, extensive latency in data delivery may introduce inconveniences on the user's side.

This thesis proposed a seamless and secure handover model by introducing a simultaneous binding update process at Correspondent Node (CN) and Home Agent HA. Performing the binding update processes simultaneously reduces the latency compared to the original FMIPv6, which performs the binding update processes sequentially. The simultaneous binding update needs a globally unique care of-address. This research also introduced the use of International Mobile Subscriber Identification (IMSI) as interface identifier for constructing the care of-address. Since the IMSI is globally unique, then the care of-address constructed by the proposed method should be globally unique as such, the Duplicate Address Detection (DAD) process is not needed in the (HA) binding update.

The performance of the proposed model was verified by performing simulation on OMNET++. The experiment results showed that the proposed model in average reduced the latency by 46%, 47% and 47% for the low, medium, and high speed scenarios, respectively. In addition, the security verification by the CMurphi tool confirmed the secureness of the proposed model.

CHAPTER ONE
INTRODUCTION

1.1. Introduction to Mobile Internet Protocol

Mobile computing has become one of the most important technologies due to the emerging use in the number of portable devices such as smartphone and portable computers. Besides, the desire to have continuous connectivity to the Internet also boosts up the mobile computing users. The rapid growth on the mobile computing area has pushed up the current technology to its limit. Moreover, multimedia has become one of the major demands requested by the users on these days.

1.1.1. Mobile Internet Protocol (MIP)

In the network layer, the Internetis viewed as a set of linked autonomous networks system in a hierarchical order and Internet Protocol (IP) acts asa tool that connects these networks together. The basic function of this tool is to deliver data from a network source to other network destination. In order to ensure the data is sent to thecorrect node, the IP identifies each node using IP address where each node is represented by one unique address.

In order to deliver the packet to the destination, the IP executes two major functions as follows:

- **Packet Routing**

  This function has a purpose to decide the route that each packet has to travel in order to reach the destination.The route is decidedby using a routing table

of a pair of destination addresses and next hop at each router and this function involves the use of protocols like BGP, RIP, or OSP.

- **PacketForwarding**

  This function has a purpose to deliver packet to the end node once it has arrived at the destination network and normally is done by discovering the hardware address of the host corresponding to its IP address. This function involves the use of protocols like ARP, proxy ARP, etc.

The IP decides the next-hop for a packet by extracting the network datagram from the destination IP address of the packet. At the same time, higher level layer protocol such as TCP maintains the information about connectionthat are indexed by a quadruplet containing the IP addresses of both endpoints and the port numbers.

The problememerged when engineers try to create mobility support on the Internet under the existing protocol suite. They have to deal with two mutually conflicting requirements:

- A Mobile Node (MN) has to change its IP address whenever moves to one point of attachment to others. This condition has a purpose to ensure that the destined packethas been routed correctly.

- In order to retain the existing TCP connections, the MN has to maintain the same IP address. Changing the IP address will cause connection lost and the packet data will belost or dropped by the router.

With the intention ofaddressing the mobility support problems, the Internet Engineering Task Force(IETF) proposesthe Mobile Internet Protocol (MIP) through

RFC 2002 in October 1996. The MIP is an extension to the Internet protocol that enables mobile device, to have an IP address,to stay connected to the Internet regardless of their location. Built on top of existing IP infrastructure the MIPis designed to makemobility transparent to the applications and higher-level protocols such as TCP.

1.1.2. Mobile IPTV

Human society and culture are shaped by how peopleview things in their life, and it is a natural fix people love to share their opinionsto influence others. People do this in order to prove they opinion are right or change other people perspective. Television has powerful effect to unified view on how things are shared.

Technology developments push people to combine conventionaltelevision technology with the latest one. In this case, people have tried to combine theIP technology and television to widening their influence effect and they called it as Internet Protocol Television(IPTV).

IPTV is defined as multimedia services, such as video, audio, text, graphics, and data, delivered over IP-based networks managed to support quality of service (QoS), quality of experience, security, interactivity, and reliability(Park and Jeong, 2009). The interpretation of IPTV has been developed into new era since MIP was introduced.People combine both technologies;MIP and IPTV to form a new technology called Mobile IPTV.There are four approaches of mobile IPTV from user perspective according to (Soohong, 2008):

(a) Mobile TV plus IP

Mobile TV plus IP uses a traditional digital broadcast networks to deliver IP-based audio, video, graphics and other broadband data to mobile users.This approach aims to build an environment in a stable broadcasting facilities and content combines with varieties ofInternet-based services. Additionally mobile TV plus IP uses wide area wireless networks, such as cellular networks to support interactivity.

(b) IPTV Plus Mobile

This approach has a lot of similar services with traditional IPTV that are already well recognized by the publics. The traditional IPTV services originally target fixed terminals such as set-top boxes. Furthermore, this idea of IPTV has been developed into mobility possibilities

(c) Cellular

In order to provide IP-based broadcast services in mobile environment, the Open Mobile Alliance's Broadcasting (OMA BCAST) has been working on technologies to provide the related services. The technique main goals are to define an end-to-end framework for mobile broadcasting and compile the set of necessary enablers.

(d) Internet

Internet or web TV comprises of numerous Internet video services worldwide. In this approach, user can either be the consumer or the

providerroles. However, the Quality of Service (QoS)cannot be guaranteedbecause the approach is based on the best-effort service model.

1.2. Background

Mobile IP (MIP) is an IP layer mobility protocol designed to provide seamless roaming support for mobile devices (Smart phone, etc) to the Internet. The MIP has to perform handover process in order to accommodate the mobility. This process is called as Binding Update (BU) process.

The Binding Update process involves authentication and authorization mechanisms. In MIPversion 4 (MIPv4), the Binding Update (BU) process uses triangle routing mechanism as security mechanism which is time consuming and not efficient. These happen because every packet destined to the MN must be routed via the HA. On the other hand MIP version 6 (MIPv6) introduced a mechanism called return routability which allows the MN to communicate directly to the CN. This mechanism is unquestionably less time consuming and more efficient in packet delivery.

Thetriangle routing and the return routability mechanisms are intended to ensure the data is delivered to the authenticated MN.This process is time consuming and may cause the data reception on the MN encounter disturbance.Application such as Mobile IPTV needs a seamless connection. The delay carries by Handover grounds a problem for the Mobile IPTV user reception. The delay between handover packets reducesthe data quality.

1.3. Problem Statement and Research Question

As mentioned in Section 1.2, the security mechanism during the Handover process requires authentication and authorization of MN by HA and CN, which produces latency. FMIPv6, HMIPv6, and PMIPv6 have already addressed this issue. However, their authenticationapproach still based on thetraditional way in which the authentication processes in Home Address (HA) and CNis performed in sequential manner or sequentially.

In addition,the authentication process in HA itself involves the Duplication Address Detection (DAD) to assure the uniqueness of the MN's IP address. The DAD process is used because the current MN's IP address based on Medium Access Control (MAC) address. Thus, the main problem in this research domain is to seek a new mechanism that decreases latency while maintain the level of security.

Furthermore, most of the mobile device's users depend on Global System for Mobile Communication (GSM) technology to get connected to Internet. This mean MIPv6 is widely used by the mobile phone users and the numbers of mobile phone user affected the IP address duplication on the network.

The fundamental research question is "what is the significant factor causing MIPv6 handover latency? This question leads to the following research questions:

- What are the main components in handover latency?
- What is the most time consuming process in handover latency?
- How to reduce the handover latency?
- What is the effect of reducing the handover latency?

1.4. Research Objectives

The objectives of this thesis are:

- To identify the most significance factor that influence to handover process and the best Mobile IPv6 model as referenced model.
- To propose seamless and secure handover mechanism to reduce handover latency for mobile phone device.
- To verify the proposed model.

1.5 Importance of the Research

Mobile applications require a seamless and secure handover to avoid service interruption when they moveto different new network nodes. Latency and security during the handover process are tradeoffs. Decreasing the latency will compromise the security.

This research attempts to reduce the latency on the handover without decreasing the secureness of the handover process itself.We hope the outcome of this research can contribute towardsmaterializing the seamless and secure mobile application such as IPTV.

1.6 Research Scope

The research of this thesis focuses on reducing the Mobile IPv6 handover latency that can minimize packets delay when performing the binding update process. Any other subjects such as network security (outside the handover

process).Quality of Service (QoS), file compression or chunking technique on video file are beyond the research scope.

1.7 Contribution

At the end of the research, we expecta new seamless and secure Mobile IPv6 handover model, which can reduce the overall handover latency time without scarifying the security requirements.

1.8 Organization of the Thesis

The rest of the thesis is organized as follows:

Chapter 2: Discusses the literature review and critical analysis on previous works.

Chapter3: Providesthe proposed works (simultaneous binding update and the IMSI-based interface identifier)

Chapter 4: Discusses the experiments setup on Omnet++ and CMurphi.

Chapter 5: Analyzes the performance and the security reliability of the proposed model.

Chapter 6: Provides conclusion of the research and future work suggestion

CHAPTER TWO
LITERATURE REVIEW

2.1. Introduction

This chapter discusses the Mobile Internet Protocol version 6 (MIPv6) as successor of Mobile Internet version 4 (MIPv4). The discussion comprises limitations of the MIPv4 mechanism that affect the of handover latency. Furthermore, the idea on how the MIPv6 overcome the limitation is presented in detail. This chapter also discusses the concept of MIPv6 mobility header as one of the important feature in the Mobile IP technology.

Subsequently, the component of mobile IP that influences the whole handover process is presented thoroughly. This chapter concludes with the discussion of some related works on reducing handover latency.

2.2. Mobile Internet Protocol version 6 (MIPv6)

The MIPv6 is a standard that proposed by Internet Engineering Task Force (IETF) to provide transparent host mobility within IPv6 network environment. The MIPv6 technology allows mobile device to move from one network to another network without changing their IP addresses. Whenever a mobile move from a network domain to the other domain it is considered as roaming to other domain that needs authentication and authorization from visiting domain and home domain. This process is referred as handover.

A MN is constantly addressable by its home address, which is the IPv6 address that is allocated to the node within its home network. When aMN is on a foreign network, packets can be routed to MN using the node's home address. In this way, the movement of node between networks is indistinguishable to the transport layer and other higher layer protocol.

Each MN has a persistent home address, which can be used to address the MN irrespective of its existing point of attachment to the IPv6 network. The IPv6 network matches the home address's prefix is known as the Home Network. If the MN roams to another network, IPv6 access router called HA intercepts any packet that is directed to the MN or forwarded by the MN.

In addition, the HA is operating as access router when MN is attached to its home network. Once MN moves to a foreign network, it uses IPv6 auto-configuration to discover the new network and create a care-of address within the address space of that network. On the other hand, to make sure the IPv6 packets intended for the MN's home address gets in touch with the proper location, the routing information relates to the MN's home address must be updated in both HA and every related CNs.

The MIPv6 system contains of several components, which are MN, Home Link, Foreign Link, Home Address, Care-of address (CoA), Binding Update Process, HA and CN. The detail of each component is as follows(Johnson, Perkins and Arkko, 2004).

- **Mobile Node**

  MN is a node that able to change its location within the network. The movement is a result of node's physical movement within the network or internetwork. Otherwise, the movement can be a result of changes in the network that make the MN has to be attached to other router (e.g., router failure).

- **Correspondent Node**

  CN is every node that communicates with the MN and act as server. In other words, CNprovides data that is requested by MN. Therefore, a MN can also act as CN in case other MN requested data from it. Usually CN is a FTP, HTTP, or mail server.

- **Home Address**

  Home address is a static IP address that belongs to the MN. This address is used by CN to communicate with MNs. Home address is formed based on 64-bit prefix assigned to the home link and combined with the MN's interface identifier. Any IP packets addressed to the home address will be routed to the home link using standard routing protocol.

- **Foreign Link**

  Foreign link is any link thatis visited by MN and not a home link. Furthermore this link is always located outside the area of home network, and used as point of attachment for MN

- **Home Agent**

  HA is an IPv6 router that located on the home link. The HA is responsible for forwarding any packet that is addressed to a MN's home address to the current point of attachment. Moreover, to forward the packets HA uses IP in IP tunneling.

- **Care-of Address**

  Care-of Address is IP address that assigned to the MN when roaming to foreign network. Care-of address is formed based on the prefix of the foreign agent link combine with the MN's interface identifier.

- **Home Link**

  Home link is a link to which the home address is assigned. This link connects the MN with the HA.

- **Binding Update (BU)**

  Binding update is the association process of MN's home address for a certain period. The association is between the stable address and the temporary address of MN. This allows the HA to forward any packet to the MN's current location. The binding update occurs once MNs request a new care-of address.

- **Binding Cache**

  Binding cache is a cache that stored in volatile memory containing a number of bindings for MNs. This cache is maintained by the CN and the HA. All

entry in the binding cache includes the MN's home address, care-of address, and the entry lifetime that designates the validity of the entry.

Packet routing and packet delivery is the main subject in the mobile IP technology. In MIPv4, the HA intercepts all packets addressed to MN. The rules of packet deliveryare changed when MN goes to roaming area where it attached to a foreign agent (Node that provides Care-of address in MIPv4).

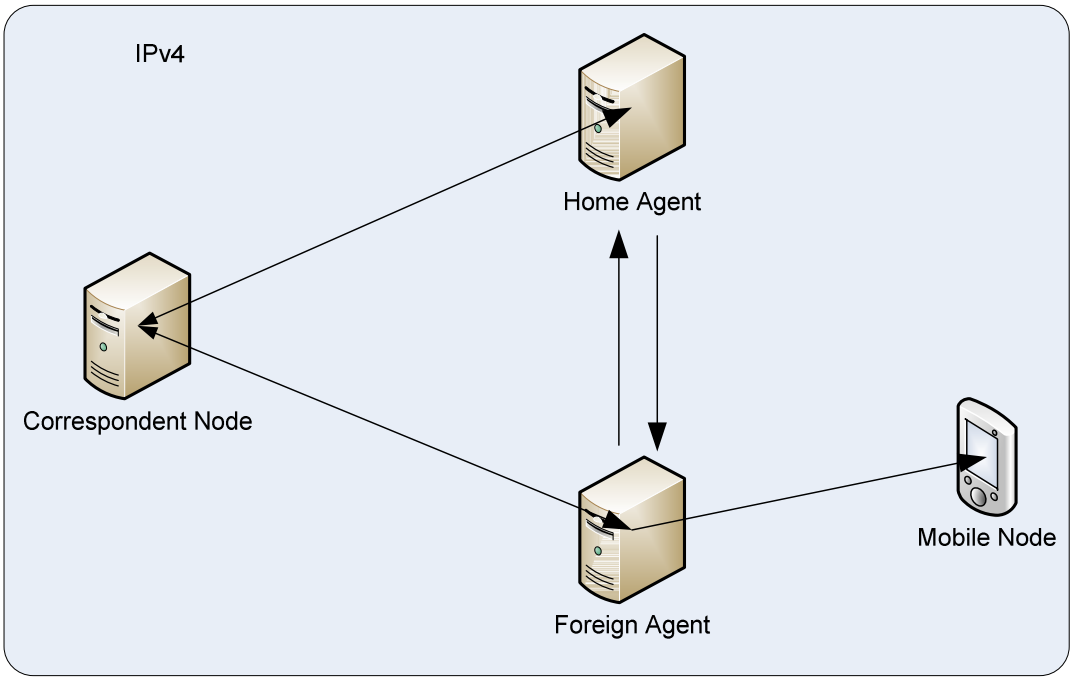

Figure 2.1: MIPv4 Triangle Routing

Figure 2.1 shows routing mechanism in MIPv4. This mechanism requires Foreign Agent to intercept any packet that addresses to MN (if MNroams to foreign network). This mechanism may affect the packets transmission to the MN because the foreign agent may experience overload and degrade the performance.

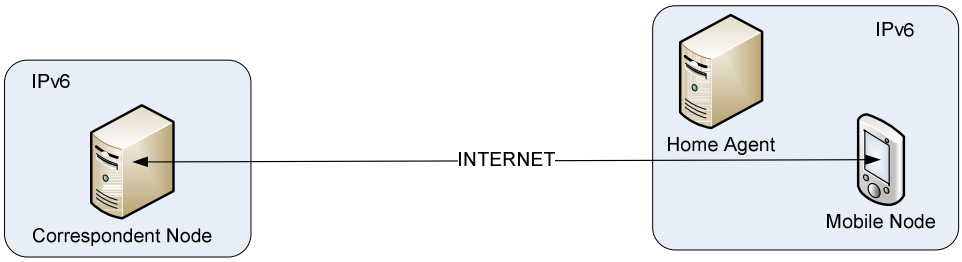

Figure 2.2: MIPv6 Routing

As shown in Figure 2.2, Different from MIPv4 routing, in MIPv6 has a route optimization procedure as such the MN can communicate directly with the CN. This procedure reduces the possibility of overload on Foreign Agent and optimizes the packets transmission for MN. The CN does not have any determined security policy with a MN, but route optimization is the direct communication betweenMN and the CN.

This communication can only be established if trusts between these two components aredeveloped. The trust can be attained by creating an authentication mechanism between them. There are a series of security designs aiming to protect the integrity and confidentiality of control and data message and alleviate the risk of network threats:

1. The secure tunnel between a MN and a HA to protect the confidentiality and integrity of information from being transferred on this path. The HA is able to guarantee that all requests are from a valid MN, and vice versa.

2. Cryptography functions are used to protect the integrity and authenticity of binding update messages. These functions depend on

random numbers and keys exchanged between a MN and its correspondents.

3. The return routability procedure provides an infrastructureless method to ensure the binding update sent to the CN is a valid message from a legitimate MN. The binding management key (K_{bm}) is formed in this process.

4. The binding management guarantees the integrity of binding updates. To ensure that the messages must be verifiable by both parties, thus they can enable all operations to the bindings while a MN is running route optimization with its peers.

IPv6 defines a number of extension headers for mobility that can be used to carry options of IP packet. The extension header follows the main IPv6 header and before the upper layer header (e.g TCP or UDP header). One of the extension headers, the hop-by-hop header, contains information intended for each router on the path. This header therefore has to be examined by each router on the path. However, in general, the extension headers contain information that only intended for the final destination of the packet.

This means that these extension headers do not need to be examined by the intermediate router. For example ESP header (extension header for IPSec) and fragmentation header (in case packet is fragmented), both of these headers have explicit and specific purposes for final destination router.

MIPv6 defines a new extension header, called Mobility Header (MH), to carry the MIPv6 messages. All messages used in MIPv6, including the binding update and the binding acknowledgement are defined as MH types. RFC 3775(Johnson, Perkins and Arkko, 2004) states the recommended order in which they should be chained in an IPv6 packet as follows in Table 2.1:

Table 2.1: Order of IPv6 Header Fields- RFC 3775(Johnson,Perkins and Arkko, 2004)

Order	Header Type	Next Header code
1	IPv6 main header	N/A
2	Hop-by-Hop Options header (if present, it MUST be the first one following the main/regular index)	0
3	Destination Option header	60
4	Routing header	43
5	Fragment header	44
6	Authentication header	51
7	Encapsulating Security Payload header	50
8	Destination header	60
9	Upper-layer header	135
	No Next header	59
Upper layer	TCP	6
Upper layer	UDP	17
Upper layer	ICMPv6	58

The extension header should not be viewed as an obscure feature of IPv6 that would be encountered only at later stages of the network and service deployment. Extension header is an intrinsic part of IPv6 protocol and it supports some basic functions and certain services.

2.2.1. Handover in Mobile IP

MIPv6 defines an IP-layer mobility management scheme to provide MNs (MN) with continuous Internet access while they move from one domain of access point (AP) to another AP. This process of changing AP is called as handover. During this process the MN may be unable to neither send nor receive packets due to the delay of the handover process. According to(Vassiliou and Zinonos, 2010)this process consists of series of the task shown in Figure 2.3:

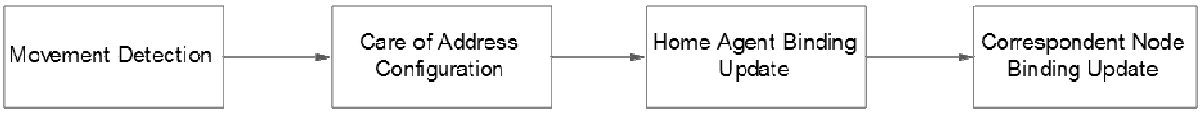

Figure 2.3: Handover Step

Each task is compulsory to be performed because MNis unable to receive IP packets until the whole task finished. Time period between the last packet received by MN in the previous connection and the first packet received by MN in the new connection is considered as handover latency. The handover latency is influenced by several components that defined as follows(Vassiliou and Zinonos, 2010):

- **Link Layer Establishment Delay**

  The time required by physical interface to establish a new association. This is the layer 2 handover between access routers.

- **Movement Detection Delay**

  The time required for MN to receive beacons from the new access router, after disconnecting from the old router.

- **Duplicate Address Detection**

  The model is to recognize the uniqueness of an IPv6 address before MN could obtain the Address from linked Foreign Agent during care of address configuration.

- **Binding Update Registration Delay**

  The time elapsed between the sending of binding update from the MNto the home address and the arrival and transmission of the first packet through the new access router.

2.2.2. Movement Detection and CoA Acquisition

Router discovery and address auto-configuration are new features in IPv6 that make task in MIPv6 much easier. It can auto-detect its movement based on new router advertisement that being received from a different router. Once a new router advertisement is received, a MN can automatically obtain its new care-of-address (CoA), using auto-configuration based on the prefix advertised in the new router advertisement. In addition, MIPv6 eliminates the need for foreign agent, whose function in MIPv4 was to provide the MN with a CoA and to tunnel the packets received from the HA. Therefore, when an IPv6 MN changes location, it automatically detects its movement using router discovery and automatically obtains a new CoA using IPv6 Address Auto-configuration.

In MIPv4, every packet destined to aMNis routed via HA. This mechanism does not allowthe MN communicates directly to the CN. In case the MN is in a foreign network, the HA will tunnel every packet destined to the MN to the foreign agent before the packets routed to the MN. This mechanism is called triangle routing.

While the Route Optimization capability for all nodes is optional in IPv4, all Mobile IPv6 nodes are designed with this capability. Route Optimization provides the MN an opportunity to eliminate the inefficient triangle routing for its correspondent nodes. Therefore, it may choose to inform the CN of its new CoA using binding update, thereby allowing the correspondent nodes to send packets directly to the Mobile node and avoid triangle routing(Ahmed et al., 2007).

2.2.3. Secure Tunnel

Consequentially to avoid attacks such as man in-the-middle, hijacking and impersonation, the traffic between a MN and it'sHA must be protected. MIPv6 suggests building a virtual bidirectional tunnel between a MN and its HA using IPsec Encapsulating Security Payload(Johnson, Perkins and Arkko, 2004). Control messages are exchanged through secure tunnel. Besides, it can be used for protecting data messages as well.

The secure tunnel decreases the chances of being attacked because the packets are encrypted. Thus, the integrity and privacy of information being carried onin the tunnel are protected.

2.2.4. Duplicate Address Detection (DAD)

(Thomson, Narten and Jinmei, 1998)introduced a mechanism to avoid IP address duplication on the network called Duplicate Address Detection (DAD). This mechanism is performed on unicast addresses and must take place on all unicast addresses, Regardless of whether the addresses are obtained through stateful, stateless, or manual configuration. RFC 2462 mentioned that DAD might not perform in two cases:

- Duplicate Address Detection must not perform on anycast addresses.
- Each individual unicast address should be tested for uniqueness. However when stateless address auto-configuration is used, address uniqueness is determined solely by the interface identifier.

In case a duplicate address is discovered during the process, a new identifier will be assigned to the interface or all IP address for the interface will need to be manually configured. When DAD applied to an address, it will be considered as tentative until the procedure has successfully completed.

The address duplication may occur when a MN proposed an address to the New Access Router (NAR). Even the address itself is formed by NAR prefix, the interface identifier that is proposed by MN could be the same. Fundamentally, the Mobile IPv6 and FMIPv6 already provide alternative address in case the duplicationis detected. However, the alternative address itself might have duplication on the network. The DAD mechanism may take longer time if this is happened.

According to Amos (Amos and Minoli, 2008), Interface identifier is formed based on MAC address, in which obtained from the network card. MAC address is assigned using the EUI-64 standard defined by Institute of Electrical and Electronic Engineering (IEEE). This standard is designed to generate large unique MAC addresses, Therefore, the product merely holds 90% of assigned value unique. It also in every 10 network card 2 among them has same value.

This fact justifies the use of DAD as a mechanism to avoid the duplication address on the network caused by identical MAC addresses. In the other hand, the DAD is the most time consuming among the handover process.

2.2.5. Return Routability

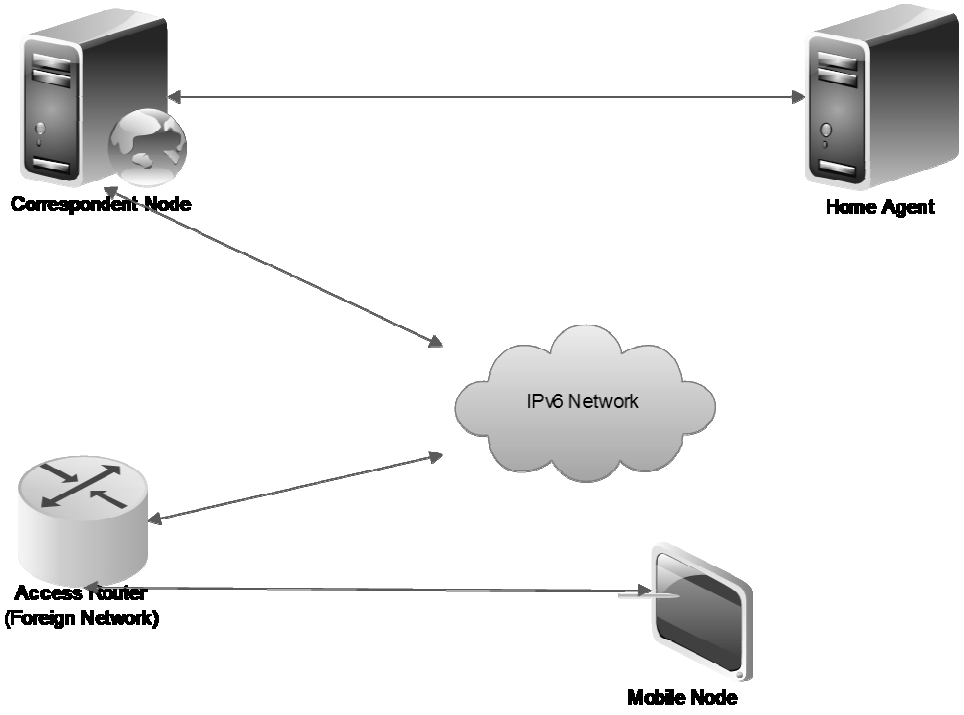

Figure 2.4 : Return Routability

The return routability procedure is a mechanism used in Mobile IP route optimization to assure a mobile mode really owns the home address and the care-of address as same as what it tells its correspondents. As shown in Figure 2.4, there are

four different messages type in this procedure, which are Home Test Init (HoTI), Home Test (HoT), Care-of Test Init (CoTI) and Care-of Test (CoT).

Home Test Init (HoTI) and Home Test (HoT) messages must pass through the home network and be tunneled between a MN and it isHA. Inthe other hand,Care-of Test Init (CoTI) and Care-of Test (CoT) messages are sent directly between a MN and a CN. They are usedto check the care-of address, therefore it is called return routability test for the care-of address.

Home Test Init and the care-of Test Init messages are generated in the MN, A HoTI is tunneled to the HA, and then forwarded to a CN in plain text, The contents ofHoTI messages are summarized as follows (Johnson, Perkins and Arkko, 2004):

Home Test Init (HoTI) message:

- Source Address = home address
- Destination Address = correspondent
- Parameters:
    - Home init cookie (64 bits)

A CoTIis sent to a CN directly in plain text. The contents of CoTI message are summarized as follows:

Care-of Test Init (CoTI) message

- Source Address = home address
- Destination Address = correspondent
- Parameters:
    - Care-of init cookie (64 bits)

The Home Test messages (HoT) is sent from a CN to a HA, and then tunneled into a MN in response to a HoTI message, The home init cookie must be included in the message and returned to the MN. A home token and a home nonce index are delivered to a MN. The contets of the HoT message are summarized as follows:

Home Test Init (HoT) message:

- Source Address = correspondent
- Destination Address = home address
- Parameters:
    - home init cookie (64 bits)
    - Home keygen token (64 bits)
    - Home nonce index

The Care-of Test message (CoT) is sent from a CN to a MN directly in response to a CoTI message. The care-of init cookie must be included in the message and returned to a MN. The contents of CoTi message are summarized as follows:

Care-of Init (CoT) message:

- Source Address = correspondent
- Destination Address = care-of address
- Parameters:
    - Care-of init cookie (64 bits)
    - Care-of keygen token (64 bits)
    - Care-of nonce index

The return routability procedure is completed by the MN having received both a HoT and CoT. More importantly, at this time, the MN is able to compute binding management key K_{bm}.

For assuring security, the return routability procedure needs to be runbefore sending any binding update to CN for any purposes, such as to refresh or to delete a Binding Cache entry. HoTI and HoT messages would spend more time on route, as they have to travel through the home network. Furthermore, the return routeability does not protect against attackers who are on the path between a home network and a CN.

2.2.6. Binding Management Message

The binding update messages and the binding acknowledgement are messages that generated by the system right after the return routability test completed. The MN generates a binding update message and sends it directly to the CN. Binding update messages are verifiable by checking the Medium Access Control (MAC).

The contents of binding update message are summarized as follows:

- Source Address = care-of address (IPv6 header)
- Destination Address = correspondent (IPv6 header)
- Parameters:
    - home address (within the Home Address destination option if different from the source address, carried by destination option extension header with next header of 60)
    - Sequence number (within the binding update message header)
    - Home nonce index (within the Nonce Indices option)
    - Care-of nonce index (within the Nonce Indices option)
    - Lifetime (16-bit unsigned integer. The number of time units remaining before the binding must be considered expired. The value