A NEW ROUTER CERTIFICATION AUTHORITY PROTOCOL FOR SECURING MOBILE INTERNET PROTOCOL VERSION 6

WAFAA ABDUL HADI ALI ALSALIHY

UNIVERSITI SAINS MALAYSIA

2007

A NEW ROUTER CERTIFICATION AUTHORITY PROTOCOL FOR SECURING MOBILE INTERNET PROTOCOL VERSION 6

by

WAFAA ABDUL HADI ALI ALSALIHY

Thesis submitted in fulfillment of the requirements for the degree of Doctor of Philosophy

[November 2007]

ACKNOWLEDGEMENTS

My deepest gratitude and appreciation goes to Allah (S.W.T). This thesis would never have been completed without His guidance.

I also would like to take this opportunity to convey my sincere thanks to my supervisor: Assoc. Prof. Dr. Sureswaran Ramadass, the director of the National Advance IPv6 Centre for introducing me to the field of IPv6. And my deepest gratitude goes to my second supervisor Assoc. Prof. Dr. Azman Samsudin for the encouragement and invaluable guidance provided during the preparation of this thesis.

Moreover, I would like to convey my appreciation to all National Advance IPv6 Centre members, Network Research Group members, School of Computer Sciences, Institute of Postgraduate Studies, and the university library for their help and support.

Finally and most important, I would like to express my most sincere gratitude to my husband Dr. Issam for his encouragement. He has always encouraged me, believed in me, and supported me. I also would like to thank my parents Dr. Abdul Hadi and Dr. Faliha for all the support and encouragement they give me.

TABLE OF CONTENTS

CHAPTER FOUR - SIMULATION AND FORMAL VERIFICATION OF CARC USING MURPHY

CHAPTER FIVE - VERIFICATION RESULTS AND DISCUSSIONS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATION

Section			Page
1.1	IPv6	Internet Protocol version 6	1
	IPv4	Internet Protocol version 4	1
	IP	Internet Protocol	1
	IETF	Internet Engineering Task Force	1
	NAT	Network Address Translation	3
	CIDR	Classless Inter Domain Routing	3
	TCP	Transport Control Protocol	4
	UDP	User Datagram Protocol	4
	ARP	Address Resolution Protocol	5
	IPSec	Internet Protocol Security	7
	RR	Return Routability	7
	HA	Home Agent	9
	Mn	Mobile node	9
	Cn	Correspondent node	9
	BU	Binding Update	9
	BA	Binding Acknowledgment	9
	HoA	Home of Address	9
	CoA	Care of Address	9
	MAC	Multiple Access Control	9
	EUI-64	Extended Unique Identifier- 64	9
1.2	SPD	Security Policy Database	15
	SAD	Security Association Database	15
	SA	Security Association	15
	AH	Authentication Header	15
	ESP	Encapsulation Security Payload	15
1.3	CA	Certification Authority	16
1.5	CARC	Certification Authority Router Certificate	18
2.1	t	time	19
	RO	Route Optimization	21
2.2	IKE	Internet Key Exchange	26
	ISAKMP	Internet Security Association and Key Management Protocol	26
	K_{bm}	Binding Management Key	27
	HoTI	Home Test Init	27

	CoTI	Care-of Test Init	27
	HoT	Home Test	27
	CoT	Care-of Test	27
2.3	LAN	Local Area Network	29
2.4	IPKGR	Identity-Based Private Key Generator	33
	TTP	Trusted Third Party	37
3.2	e-Commerce	Electronic-Commerce	43
	ISP	Internet Service Provider	44
3.3	ARQ	Automatic Repeat Request	51

LIST OF APPENDICES

SATU PROTOKOL AUTORITI PERAKUAN PENGHALA BARU UNTUK MENJAMIN PROTOKOL INTERNET BERGERAK VERSI 6

ABSTRAK

Protokol Internet Bergerak versi 6 (IPv6 Bergerak) telah dicadangkan sebagai satu protokol piawai untuk memberikan mobility dalam Rangkaian Generasi Seterusnya. Sebagai satu protokol baru, Protokol IPv6 Bergerak mempunyai beberapa isu yang perlu ditangani seperti memperluaskan protokol untuk memberikan mekanisma 'hand off' yang lancar dan pantas, mobility rangkaian, kualiti perkhidmatan dan pengurusan lebarjalur bagi aplikasi mobility masa sebenar. Namun, isu yang paling utama ialah kerentanan sekuriti IPv6 Bergerak kerana tanpa sekuriti yang sempurna, protokol tersebut tidak akan berguna.

IPv6 Bergerak mempunyai tiga komponen utama: nod Bergerak, nod Koresponden dan Agen Rumah. Untuk menjamin keselamatan protokol, nod Bergerak dan Agen Rumah perlu mempercayai satu sama lain. Nod Koresponden perlu mempercayai nod Bergerak kerana nod Bergerak merupakan nod yang memberikan dan mengemaskinikan maklumat ke nod Koresponden. Isyarat-isyarat di antara ketiga-tiga komponen ini seharusnya dijamin selamat dan disahkan benar.

Pada masa ini, IPv6 Bergerak ditakrifkan menggunakan penyelesaian sekuriti yang dinamakan Kebolehjalanan Kembali (*Return Routability*) yang membekalkan nod Bergerak dengan mekanisma pengesahan dan melindungi isyarat-isyarat yang dihantar di antara nod Bergerak dan nod Koresponden. IPv6 Bergerak memberikan mandat pada sokongan Sekuriti Protokol Internet (IPSec) di antara nod Bergerak dan Agen Rumahnya untuk membolehkan keduanya mempercayai satu sama lain dan untuk melindungi isyarat yang dihantar di antara keduanya. Walaupun IPSec mampu menawarkan perlindungan yang baik (bergantung kepada algoritma yang digunakan),

penggunaan IPSec dalam Kebolehjalanan Kembali tidak semestinya merangkumi semua bidang sekuriti. Penyelesaian ini tidak dapat mengatasi serangan Orang Tengah.

Objektif utama tesis ini ialah untuk mereka bentuk satu protokol sekuriti baru untuk memberikan tahap pengesahan dan sekuriti yang lebih ketat bagi IPv6. Protokol sekuriti ini perlu memberikan satu tahap sekuriti dan pengesahan yang lebih ketat berbanding dengan mekanisme yang ada sekarang iaitu Kebolehjalanan Kembali. Selain daripada itu, protokol sekuriti yang dicadangkan ini akan memberikan satu rangka kerja konsisten yang menggantikan pelaksanaan IPSec menyeluruh dalam IPv6 Bergerak. Protokol sekuriti yang dicadangkan ini dinamai Sijil Penghala Autoriti Perakuan (CARC) akan juga memastikan perlindungan daripada serangan Orang Tengah.

Protokol yang baru dicadangkan ini telah disahkan dengan jayanya dengan menggunakan dua versi pengesah Murphy, Murphy 3.1 dan Murphy Ganda Tiga. Dalam kedua-dua pengesahan, protokol yang baru telah dibuktikan lebih selamat daripada protokol Kebolehjalanan Kembali.

A NEW ROUTER CERTIFICATION AUTHORITY PROTOCOL FOR SECURING MOBILE INTERNET PROTOCOL VERSION 6

ABSTRACT

Mobile Internet Protocol version 6 (Mobile IPv6) has been proposed as a standard protocol to provide mobility in Next Generation Networks. Mobile IPv6 protocol as a new protocol has a few issues that need to be addressed such as extending the protocol to provide smooth and fast hand off mechanisms, network mobility, quality of service and the bandwidth management of real time mobility applications. However, the biggest issue is the security vulnerability of Mobile IPv6 because without proper security the protocol will be useless.

Mobile IPv6 has three main components: the Mobile node, the Correspondent node and the Home Agent. For the protocol to be secure, the Mobile node and its Home Agent should trust each other. The Correspondent node should trust the Mobile node because the Mobile node is the one giving and updating the information to the Correspondent node. The signals between all of these components should be secured and authenticated.

Mobile IPv6 is currently defined with a security solution called Return Routability that provides the Mobile node with an authentication mechanism and protects the signals between the Mobile node and the Correspondent node. Mobile IPv6 mandates the Internet Protocol Security (IPSec) support between the Mobile node and its Home Agent to let them trust each other and to protect the signals between them. While IPSec may offer strong protection (depending on the algorithm used), the use of IPSec within Return Routability does not necessarily cover all areas of security. This solution is especially vulnerable to the Man-in the-Middle attack.

The main objective of this thesis is to design a new security protocol to provide higher levels of authentication and security for Mobile IPv6. This security protocol has to provide a level of security and authentication which is higher than the current mechanism which is Return Routability. Additionally, the new proposed security protocol will provide a consistent framework replacing the comprehensive IPSec implementation within Mobile IPv6. This proposed new security protocol called Certification Authority Router's Certificate (CARC) will also ensure protection against the Man-in the-Middle attack.

The new proposed protocol was successfully verified using two versions of the Murphy verifier, Murphy 3.1 and Triple Murphy. In both verifications, the new protocol proved to be more secure than the Return Routability protocol.

CHAPTER ONE
INTRODUCTION

This chapter is divided into five sections, the first section introduces Internet Protocol Version 6 (IPv6), it then goes to give a brief description of the concept of mobility, followed by the reasons as to why Mobile IPv6 is preferred over Mobile IPv4. After that, how Mobile IPv6 works are described. The importance of Binding Update signals has been outlined. An overview of the current problem in the Mobile IPv6 security protocol is also described. Then the last sections give the proposed idea as well as the thesis contribution.

1.1 Background

The rapid increase in the number of Internet users, combined with the expected growth in the number of Mobile Internet Protocol (Mobile IP) users requires a scalable and flexible IP technology, which is not provided by IPv4 efficiently. IPv6 is the next generation protocol (Silvia, 2000, Davies, 2003, RFC2460, 1998 and IPv6 Ready, 2003) designed by the Internet Engineering Task Force (IETF) to replace the current version of the Internet Protocol, IPv4 (RFC791, 1981). IPv6 offers a big package of capabilities, of which 'addressing' is the most visible component. Even though the addressing issue gets a lot of attention (RFC2373, 1998), it is only one of many important issues that IPv6 designers have tackled. Other IPv6 capabilities include mobility, integrated quality of services, automatic configuration, and more efficient network route aggregation at the global backbone level.

Mobility support in IPv6 (RFC3775, 2004, Hesham, 2004 and HZNET, 2005) is particularly important, as mobile devices are likely to account for a majority or at least a substantial fraction of the population of the Internet during IPv6's lifetime. Mobile IPv6

is an extension of IPv6 that need to use one of the extension headers called “Mobility Header” and need to exchange Mobile IPv6 signals called “Binding Update” signals

Next section explains the idea of IP mobility and then lists the reasons as to why mobility support in IPv6 (RFC3775, 2004) is preferred compared to mobility support in IPv4 (RFC3344, 2002).

1.1.1 IP Mobility

The meaning of mobility does not necessarily indicate mobility for wireless devices as it can also mean wired devices that can be disconnected from a specific point and reconnected to other points. Mobile computing offers many advantages such as access to the Internet anytime, anywhere.

Mobile IP refers to the mobility aspect of IP that allows nodes to move to different networks all over the world while maintaining upper layer connectivity (Webopedia Computer, 2007). This is not to be confused with ‘portability’ that allows nodes to move to different networks all over the world and remain reachable, while causing upper-layer connections to be disrupted each time a node relocates as it has to obtain a new IP address at each location.

Mobile IP is intended to enable nodes to move from one IP network to another without changing the mobile node's IP address. The idea behind this is to allow a Mobile node to be always addressable by its "home address". Packets that are routed to the Mobile node will use the Mobile node’s home address regardless of the Mobile node’s current point of attachment to the Internet. The Mobile node may continue to communicate with other nodes (stationary or mobile), after moving to a new network. The movement of a Mobile node away from its home network is thus transparent to upper-layer protocols and applications.

IP Mobility in IPv4 applies the concept of Mobile IP, using the capabilities offered by the IPv4 protocol. IPv4 is proven to be robust, easily implemented and interoperable, and has stood the test of scaling, to be the size of today's Internet, using different mechanisms such as Network Address Translation (NAT) (WIKIPEDIA, 2007a) and Classless Inter Domain Routing (CIDR) (WIKIPEDIA, 2007b). However, the design of IPv4 did not take into consideration certain issues, including mobility.

IPv6 on the other hand, provides many capabilities compared to IPv4 such as having more addresses, header extension, mobility support, built-in quality of service, address auto-configuration, and host discovery.

Thus Mobile IPv6 applies the concept of Mobile IP using the capabilities offered by the IPv6 protocol and tackles the limitations that exist in Mobile IPv4. Figure 1.1 demonstrates the flow of designing the Mobile IPv6 protocol.

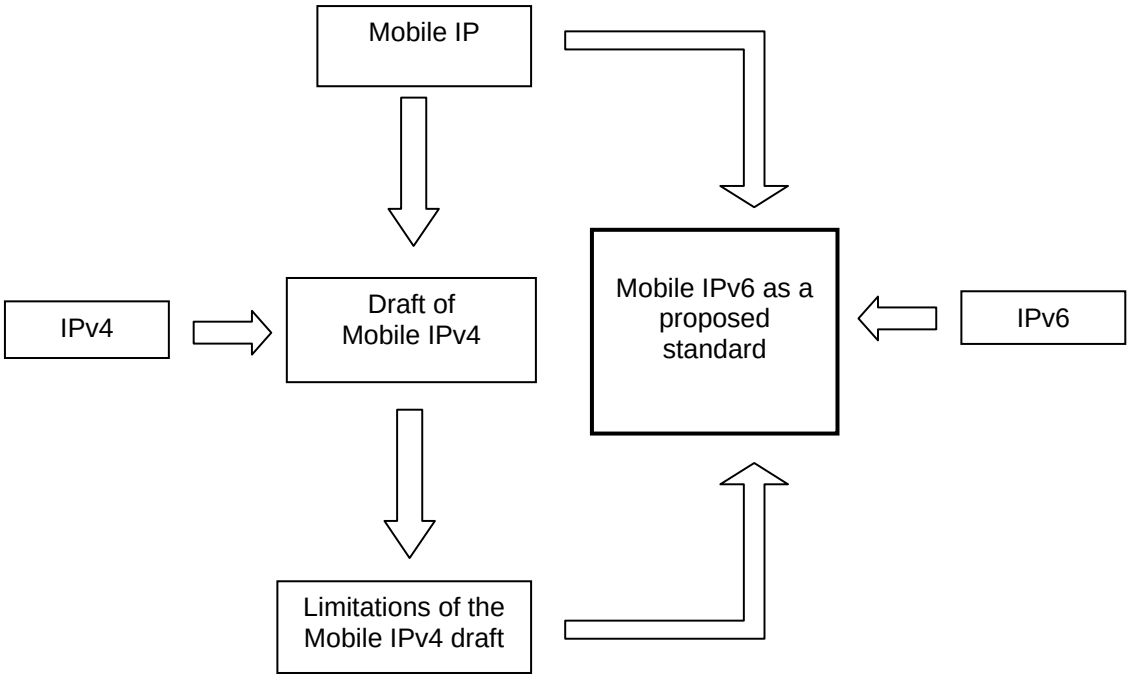

Figure 1.1: Flow of Designing Mobile IPv6 protocol

Mobile IPv6 protocol has become the standard for mobility, now and for future Internet applications rather than Mobile IPv4. The seven main reasons for this are listed below:

1- Mobile IPv6 support for Route Optimization: Route optimization is not found in Mobile IPv4 because of the inflexibility of the IPv4 header (GIAC, 2003). The Home Address Option header and Routing header which facilitate the route optimization are missing in IPv4. This integration of route optimization functionality allows direct routing from any Correspondent node to any Mobile node, without needing to pass through the Mobile node's home network. This eliminates the problem of triangle routing present in Mobile IPv4. The integration of route optimization reduces the amount of re-routing and tunnelling work for the Home Agent. This results in less traffic passing through the home link, thus reducing bottlenecks at the home link, and thereby saving 50 percent of Internet performance and bandwidth compared to using triangle routing (Nokia Research Center, 2002a).

2- Home Address Option header: Home Address Option header, which is one of the Extension Headers in IPv6 allows Mobile nodes to co-exist efficiently with routers that perform ingress filtering (Nokia Research Center, 2002b). A Mobile node now uses its care-of address as the source address in the header of packets it sends, allowing the packets to pass normally through ingress filtering routers whereas the home address of the Mobile node is carried in the Home Address Option header.

Another advantage of using a Home Address Option header is allowing the use of a care-of address in the packet to be transparent to the upper-layers such as Transport Control Protocol (TCP) and User Datagram Protocol (UDP). The ability to process correctly a Home Address option in a received packet is required in all IPv6 nodes, whether mobile or stationary, host or router.

3- Home-of Address as the Multicast source address: This can be used within each packet's IP header to simplify routing of multicast packets sent by a Mobile node (Youn-Hee and Seung-Hee, 2006). With Mobile IPv4, the Mobile node has to tunnel the multicast packets to its Home Agent in order to transparently use its home address as the source of the multicast packets. With Mobile IPv6, the Home Address Option header allows the home address to be used and still be compatible with the multicast routing that is based in part on the packet's source address.

4- Foreign agents not needed: There is no longer any need to deploy special routers as "foreign agents" as is proposed in Mobile IPv4. In Mobile IPv6, the Mobile nodes make use of the enhanced features of IPv6, such as Neighbor Discovery (RFC2461, 1998) and Address Autoconfiguration (RFC2462, 1998), to operate in any location away from home without any special support required from its local router.

5- Movement detection mechanism in Mobile IPv6: This provides bi-directional confirmation of a Mobile node's ability to communicate with its default router in its current location. This confirmation provides a detection of a "black hole" situation that may exist in some wireless environments. The link in such environments to the router does not work equally well in both directions, such as when a Mobile node has moved out of a good wireless transmission range from the router. In contrast, in Mobile IPv4, only the forward direction (packets from the router to the Mobile node) is confirmed, allowing the black hole condition to persist.

6- IPv6 Neighbor Discovery: Home Agent intercepts the packets for the Mobile node that arrive at the home network, using IPv6 Neighbor Discovery rather than Address Resolution Protocol (ARP) mechanism. The use of Neighbour Discovery improves the robustness of the protocol (Eddy and Ishaq, 2006) and simplifies the implementation of Mobile IP because it is not concerned with any particular data link

layer as is required in ARP.

7- IPv6 Anycast: The dynamic Home Agent address discovery mechanism in Mobile IPv6 uses IPv6 Anycast which returns a single reply to the Mobile node (Ata et al., 2005), rather than the corresponding Mobile IPv4 mechanism, which uses IPv4 directed broadcast and returns a separate reply from each Home Agent on the Mobile node's home link. The Mobile IPv6 mechanism is more efficient and more reliable, since only one packet needs to be sent back to the Mobile node.

The above reasons clearly indicate the advantages of Mobile IPv6 over Mobile IPv4. Next section provides an overview of Mobile IPv6 protocol.

1.1.2 Overview of Mobile IPv6 Protocol

The two main objectives of the Mobile IPv6 protocol are enabling IPv6 nodes to move from one IP network to another IP network without any interruption in connection, and optimizing the route between the nodes, thereby making the Mobile node and its Correspondent node communicate directly with each other (RFC3775, 2004). Mobile IPv6 protocol has three base operations, which are Movement Detection, Triangle Routing, and Route Optimization:

Operation one: Movement Detection has two mechanisms: “Router discovery” and Construction of the new Mobile node’s IPv6 address “Care of Address”.

Operation two: Triangle Routing has another two mechanisms whereby the first one is the “Binding Update with Home Agent”, which is the responsibility of the Mobile node to send Binding Update signals to the Home Agent to inform it about a new IPv6 address. The second mechanism is ”proxy and tunnelling” which is the

responsibility of the Home Agent to intercept the packets addressed to the Mobile node's original address and tunnel it to the Mobile node's new address.

Operation three: Route Optimization is the operation that eliminates the use of triangle routing and makes for direct communication with any other node. Route Optimization is achieved via two steps: the first step is when the Mobile node sends Binding Update signals to inform its Correspondent node about its new IPv6 address. The second step is the direct communication whereas the Correspondent node sends packets directly to the Mobile node.

The protocols used to secure the Binding Update with the Home Agent and the Binding Update with the Correspondent node respectively are considered "security extended protocols". The security protocol used to secure the Binding Update with the Home Agent is called Internet Protocol Security (IPSec) whereas the security protocol used to secure the Binding Update with its Correspondent node is called Return Routability (RR). Mobile IPv6 operations and protocols are shown in Figure 1.2.

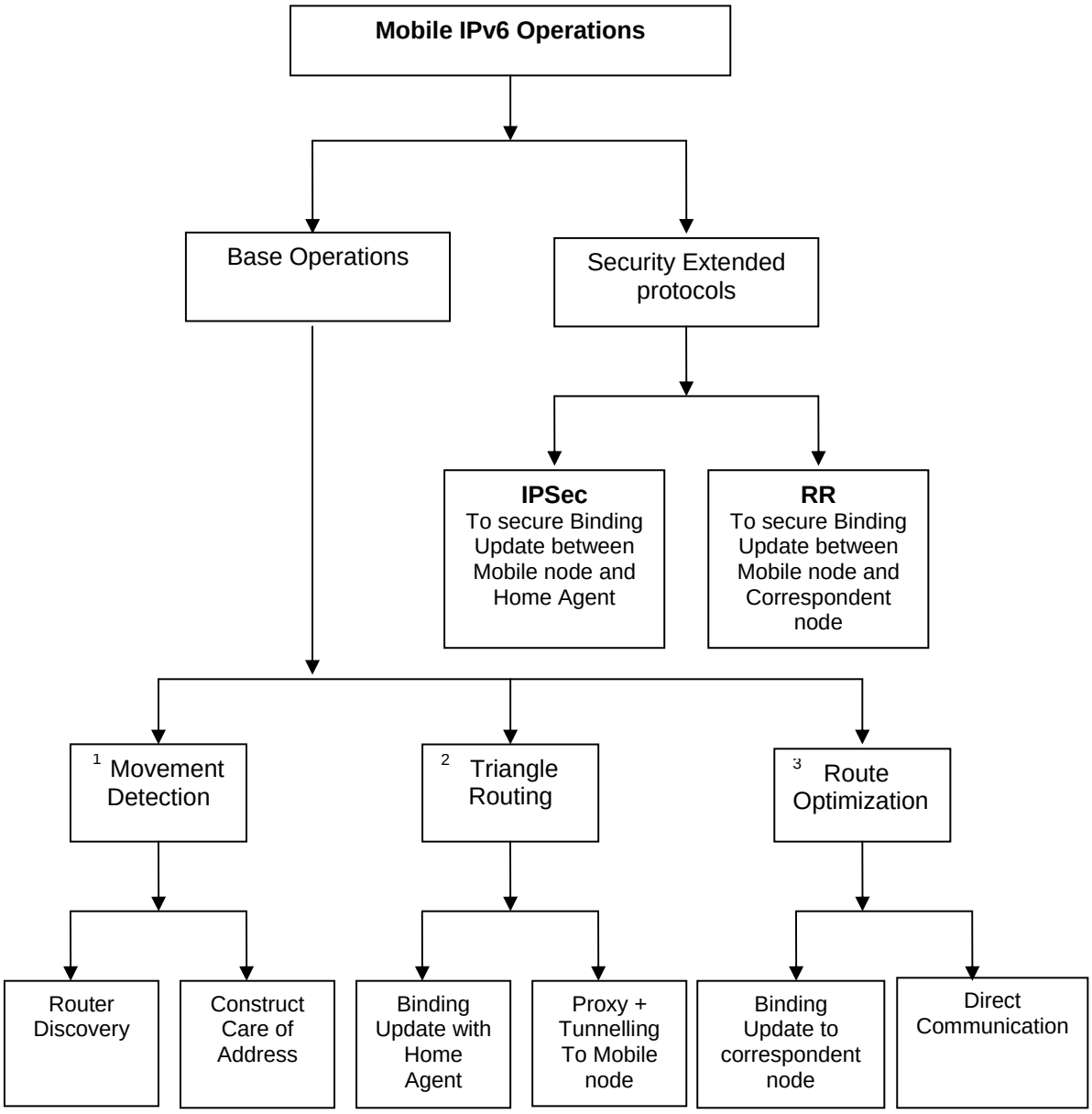

Figure 1.2: Mobile IPv6 Operations

The example given below which is about the behaviour of a laptop as a Mobile node explains one example of mobility in IPv6 in a clearer manner.

1.1.3 Mobile IPv6 Example

Figures 1.4, 1.5, 1.6 and 1.7, respectively will be used for this example. In the figures the author will use the Mobile IPv6 terminology, which is explained in the next page.

HA: The router that functions as Home Agent in home network.

Mn: A laptop as a Mobile node

Cn: Stationary or mobile PC as Correspondent node

BU: Binding Update signal

BA: Binding Acknowledgment signal

HoA: Mobile node's Home of Address

CoA: Mobile node's Care of Address

MAC: The physical address associated with the network card

If more than one device at home or in the office have an IPv6 address, then the use of a router at that place is needed. The Home Agent is a router that advertises its prefix to the nodes within its home network. Then the Mobile node can construct its IPv6 address which is called Home of Address from the prefix of the router combined with the interface identifier of the device. Interface identifier is the MAC address mapped to the Extended Unique Identifier (EUI-64) address as shown in Figure 1.3.

Figure 1.3: IPv6 Address

The home network is the network where the Mobile node (laptop in this example) has been booted and configured for the first time with the attached Home Agent. Any node or device that leaves the home network for a while to another network is considered a Mobile node. The network that the node visits, or moves to is called foreign network. In this example, the home network is setup at home and the foreign network is considered at office, as shown in Figure 1.4

Any other node that communicates with the Mobile node is considered its Correspondent node. The Correspondent node can be in the same visited network or from the other network as shown in Figure 1.4.

Figure 1.4, shows the movement of a Mobile node from a home network to an office network. In the office network, the Mobile node, which is the laptop, has to discover the local router by using the Neighbour Discovery mechanism. The laptop then constructs its new IPv6 address from the router prefix and laptop's MAC address using the Stateless Autoconfiguration mechanism. The newly constructed address is called Care of Address.

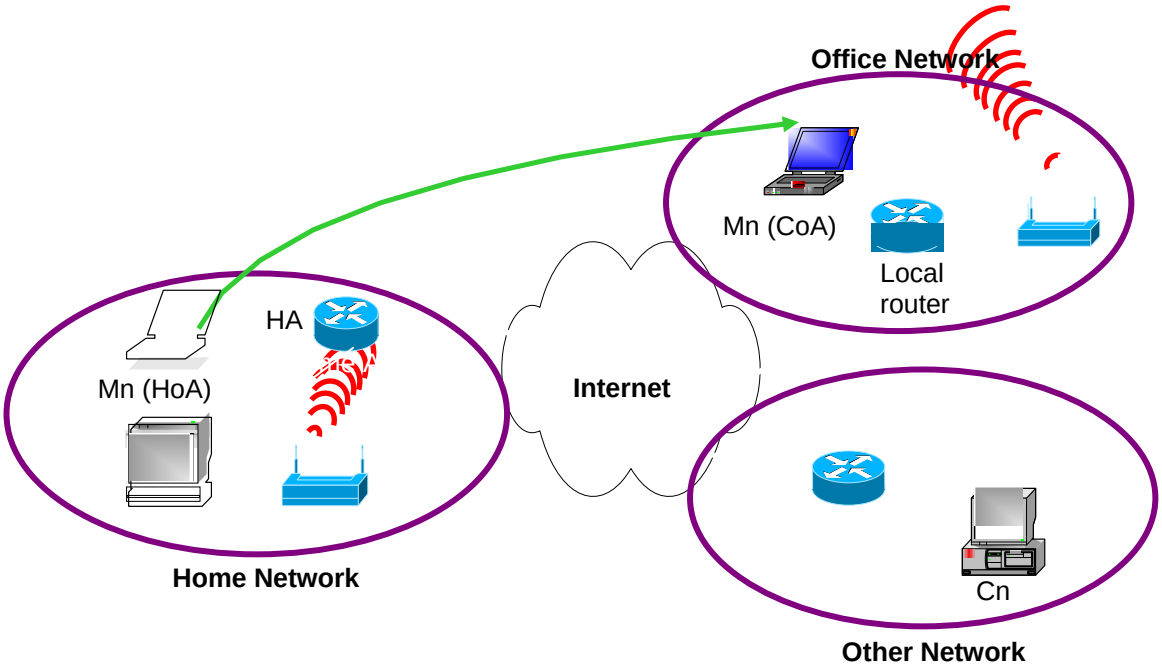

Figure 1.4: Mobile node's Movement Detection

After the Mobile node has constructed a new IPv6 address, the Mobile node should inform its Home Agent about this new address using the Binding Update signal as shown in Figure 1.5, Message 1. The Home Agent replies with a Binding Acknowledgment as shown in Message 2.

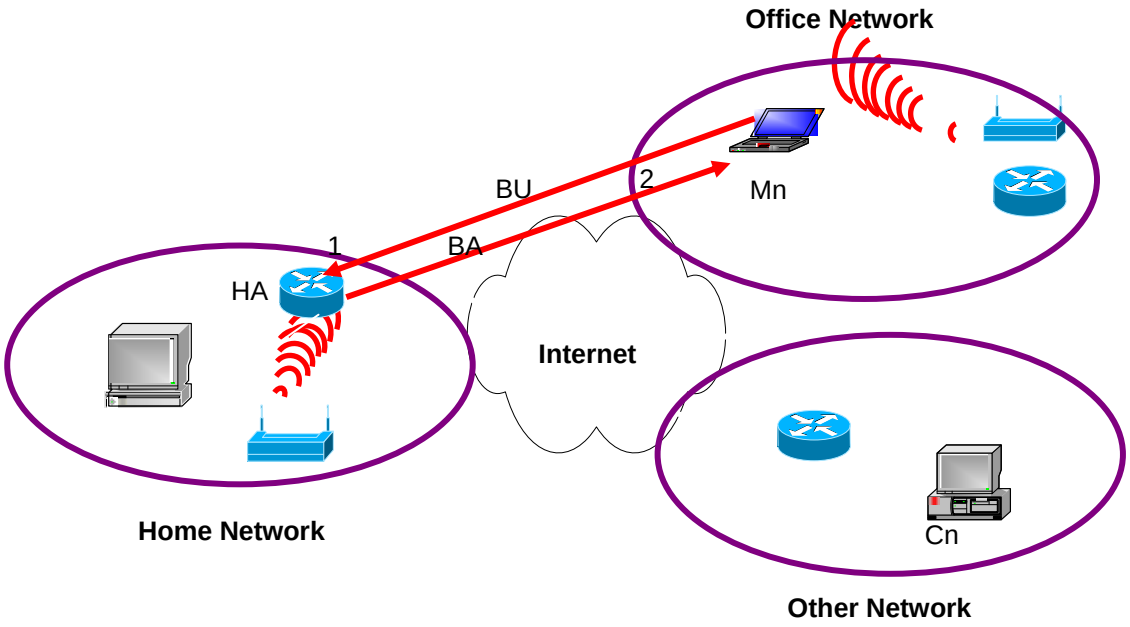

Figure 1.5: Binding Update with Home Agent

The Correspondent node from the other network (Figure 1.6), which sends packets to the Mobile node's original address as shown in Message 1, does not know about the new address of the Mobile node. The Home Agent will intercept the packets by using a proxy mechanism and then tunnel the packets to the Mobile node's new address in Message 2.

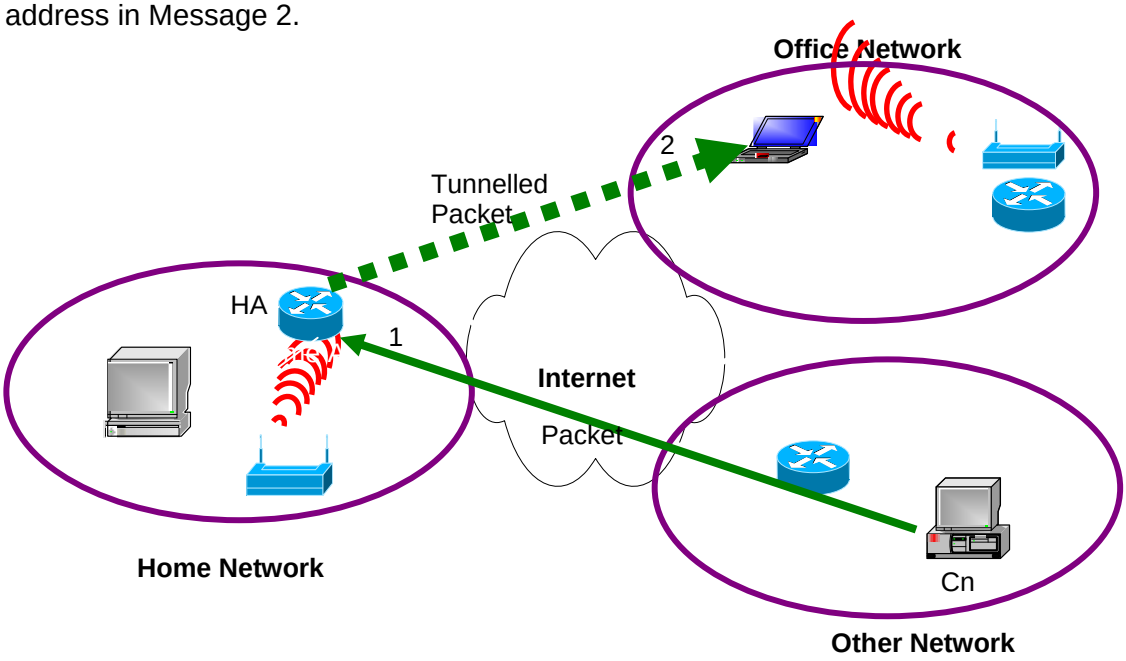

Figure 1.6: Triangle Routing

Upon receiving the tunnelled packets, the Mobile node will send Binding Update signals to inform the Correspondent node about the Mobile node's new address as shown in Figure 1.7. The Correspondent node will reply with a Binding Acknowledgment to Mobile node. After exchanging the binding signals, the direct communication between the Mobile node and its Correspondent node can be achieved.

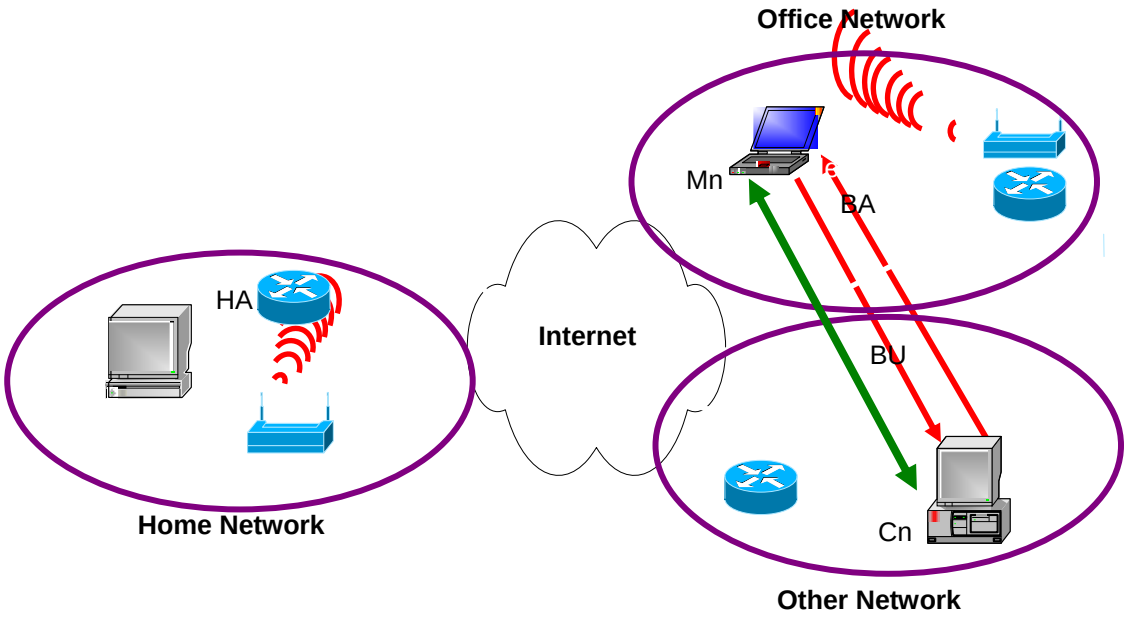

Figure 1.7: Route Optimization

In Mobile IPv6, binding signals are considered to be one of the cornerstones of the protocol. Only binding signals can keep the Mobile node reachable at any location with any IPv6 address, which is the main goal of Mobile IPv6. The next section defines binding signals in Mobile IPv6.

1.1.4 Binding Update in Mobile IPv6

The association between a Mobile node's Home of Address and the Mobile node's Care of Address for a specific life time is known as Binding. If the Mobile node informs the other nodes about this association, then the Mobile node is doing Binding

Updates. Other nodes that receive this Binding Update signal will confirm receiving it with a Binding Acknowledgment as shown in the example above.

The Binding Update has to be sent from the Mobile node to the Home Agent and this process is called Binding Update with the Home Agent or Home Agent Registration. Binding Update signals also have to be sent from the Mobile node to the Correspondent node and this is called Binding Update with Correspondent node.

1.2 The Current Problem

The Mobile IPv6 still has some issues that not solved yet . However, the biggest issue is the security vulnerability within Mobile IPv6, because without proper security, the protocol will be useless.

There are two solutions for securing Mobile IPv6's Binding Updates. The first solution concerns securing the Binding Update signals between the Mobile node and its Home Agent by the use of IPSec (RFC3776, 2004).

The second solution, concerns the securing of the Binding Update signals between the Mobile node and its Correspondent node, which is more complex due to the absence of a pre-relationship between the Mobile node and its Correspondent node. The Mobile IP group has designed and documented (RFC3775, 2004) the protocol Return Routability. The next section gives a brief explanation about the two mechanisms, Return Routability and IPSec. Figure 1.8 shows the current security protocols used to secure the Mobile IPv6 protocol.

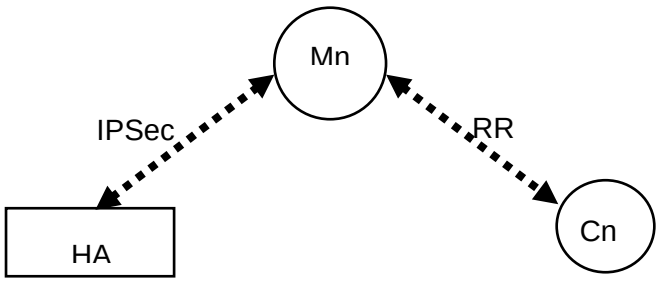

Figure 1.8: Security Protocols Used to Secure Binding Signals in Mobile IPv6

- **Return Routability (RR)**

The Return Routability protocol enables the Correspondent node to obtain assurance that the Mobile node is in fact addressable at its claimed Care of Address as well as at its home address. In other words, this lets the Mobile node prove that it is addressable by both addresses which are the original one (Home of Address) and the new one (Care of Address).

Only with this assurance is the Correspondent node able to accept Binding Updates from the Mobile node, which causes the Correspondent node to direct that Mobile node's data traffic to its claimed Care of Address.

During Return Routability the two nodes, mobile and correspondent, should exchange keys that have to be used for encryption purposes and also for the authentication. The problem in Return Routability (Wafaa and Sureswaran, 2003) is that there are some locations near the Correspondent node, which allow the attacker to sniff the keys and convince the Correspondent node to believe that the attacker is the original Mobile node. There is some research on improving the performance of Return Routability when there is more than one Mobile node communicating with the same Correspondent node (Feng et al., 2005) but such improvement still face this type of attack because the messages still have to be sent in plain text.

- **Internet Protocol Security (IPSec)**

IPSec (Cisco, 2006) is a general purpose protocol used to secure packets in the IP layer. IPSec contains a lot of options and policies, which are stored in the Security Policy Database (SPD). Options such as the keys, the algorithms of encryption and authentication and the parameters associated with each algorithm need to be decided before each session of communication for each IP's data traffic occurs.

IPSec also has a Security Association Database (SAD), where the negotiated algorithms with the key between the two nodes with their identities are stored. IPSec Security Association (SA) is unidirectional. When establishing secure communications for bidirectional communication between two nodes, one needs to configure security associations for each direction.

IPSec has two mechanisms, Authentication Header (AH) (RFC2402, 1998), which is used for authentication and an Encapsulation Security Payload (ESP) (RFC2406, 1980), which is used for encryption.

In Mobile IPv6, IPSec is used to secure the Binding Update signals between the Home Agent and the Mobile node (RFC3776, 2004). Both AH and ESP are needed to achieve the authentication and the integrity of the Binding Update signals. Each mechanism has its own tunnelling and algorithm. Manual configuration is needed to set the keys and algorithms for the Security Association Database with the Home of Address as the identity for the Mobile node. IPSec is considered a battery taxing protocol for mobile devices.

1.3 The Proposed Solution

A Certification Authority (CA) is a trusted third party organization or company that issues digital certificates to users. A digital certificate is an electronic document binding together some pieces of information, such as a user's identity and public key. Digital certificates are used with applications such as emails or online Banking due to the non-repudiation (high authentication) that is provided to the other party. The other party should only verify the certificate by checking the signer.

Two major types of certificates exist: end-entity certificate and CA certificate. An end – entity certificate is issued by a Certification Authority to an entity that does not in turn issue certificates to another entity. A CA certificate is issued by a Certification Authority to an entity that is also a Certification Authority and so may issue an end-entity certificate. Certificates can be issued to users as well as routers and nodes. Certificates based on users' identity is described in many publications, however, certificates for routers and nodes still remain a new field of research.

The focus of this thesis is on a CA certificate which allows the design of a Router Certification Authority protocol. In this case, the Certification Authority issues a certificate for routers who in turn issues sub-certificates to the end nodes. This protocol (Wafaa and Azman, 2006) allows the generation, renewal, and revocation of the router certificate as well as the generation, renewal, and revocation of the node sub-certificate. Such a protocol is novel and has never been designed before.

This new protocol eliminates the need for Return Routability within the Mobile IPv6 environment (see Figure 1.9). This is done while still ensuring an even higher level of security than that provided by Return Routability (with or without IPSec).

This new protocol can prevent attacks faced by Mobile IPv6 like the Man-In-The-Middle attack. Other security attacks like Replay Attack, Simple Denial of Service and Spoofing of IPv6 addresses can also be avoided in Mobile IPv6 using the new protocol. Chapter 3 explains this in more detail.

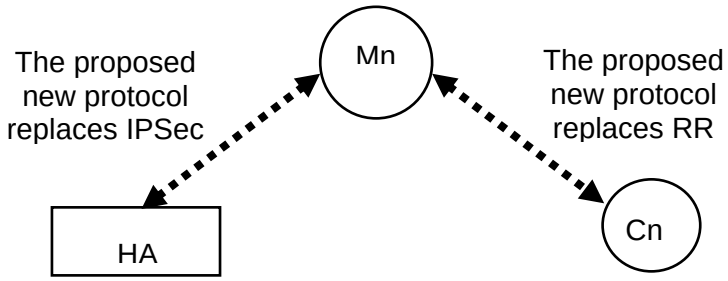

Figure 1.9: Our Protocol Used to Secure Mobile IPv6 Signals

1.4 Thesis Contribution

The contributions of the thesis are:

- An CA router certificate protocol which allows the generation, renewal, and revocation of the router certificate as well as the generation, renewal, and revocation of the node sub-certificate
- Constructing a new format of Router Certificate which is the extension of the Certificates X.509v3.
- Using the CA router certificate protocol to create a more secure environment within Mobile IPv6

1.5 Thesis Overview

This thesis is organized into six related chapters. **Chapter 1** presents the background of this thesis. It starts by presenting an introduction of IPv6, it then goes to give a brief description of the concept of mobility, followed by the reasons as to why

Mobile IPv6 is preferred over Mobile IPv4. After that, how Mobile IPv6 works are described. The importance of Binding Update signals, which are needed to achieve the mobility in IPv6, have been outlined. An overview of the current problem in the mobile IPv6 security protocol is also described. Then the last section introduces the proposed idea as well as the thesis contribution.

Chapter 2 gives an overview of the problem in the current protocol and then discusses the alternative solutions proposed by other researchers.

Chapter 3 is the core of the thesis which presents the design of the new protocol named CARC. This chapter gives a detailed description of the new protocol. This includes the design details for the generation of the router's certificate and the node sub-certificate as well as the renewal and revocation processes. The chapter also describes the possibility of the attacks in each process and how they can be avoided. Implementation of the first version of CARC was done. However, simulation results led to the second and final (improved) version of CARC that is presented in the second last section. Last section discuss the operation of CARC within Mobile IPv6 and its advantages

Chapter 4 discusses the security protocol verifier (Murphy) as well as the description of CARC simulation and formal verification is given in this chapter. Some of the verification scenarios are given in full detail.

Chapter 5 is the summary of the verification results and its discussions.

Chapter 6 is the conclusion and an outline of possible future work to continue and enhance the proposed research within this thesis.

CHAPTER TWO
LITERATURE REVIEW

This chapter analyses all the attacks that exploit the Mobile IPv6 signals, explains in detail the current security protocols used in Mobile IPv6 and their problems and then describes alternative solutions proposed to replace the current security protocols within Mobile IPv6.

2.1 Attacks That Exploit Mobile IPv6 Signals

Mobile IPv6 signals are usually referred to as Binding Update signals in Mobile IPv6 literature. This thesis will use both names alternatively. The Binding Update signal is an association of the Mobile node's Home of Address (HoA) and Care of Address (CoA) for a specific lifetime (t). The Mobile node has to send these signals to the Home Agent and then to the correspondent node after each movement. These signals are vulnerable to many attacks. Attacks that exploit the Binding Update signals in Mobile IPv6 can be classified into two types as listed below and explained in our work (Wafaa and Sureswaran, 2003). Figure 2.1 shows all the attacks:

1- Attacks when Binding Update signals are not authenticated or secured
2- Attacks when Binding Update signals are authenticated and secured

2.1.1 Attacks when Binding Update Signals are not Authenticated or Secured

If Binding Update signals are not authenticated and secured, then the attacker can send spoofed Binding Update, which can result in one of the following attacks:

1- Attack against secrecy and integrity

2- Attack using HoA to send unwanted data to any host

3- Attack using CoA to send unwanted data to any host

The explanation for the attacks is in the next sections.

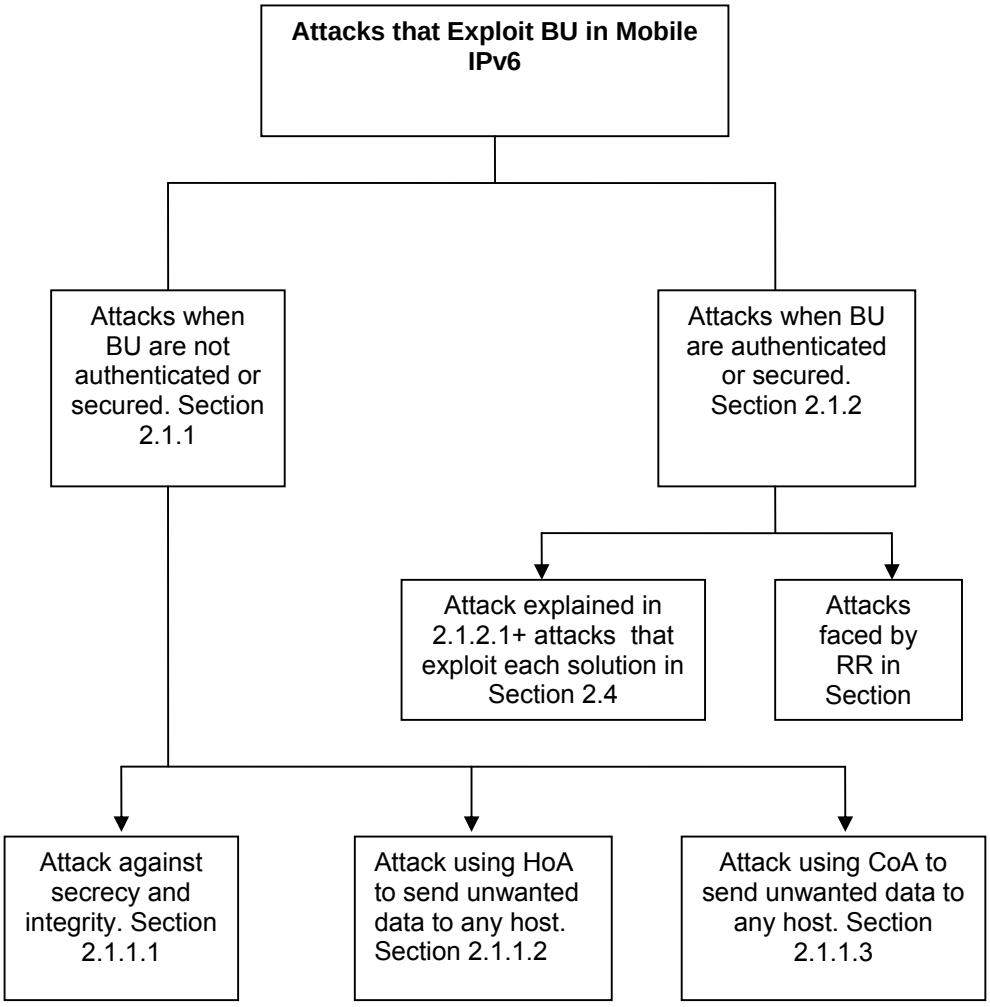

Figure 2.1: Attacks that Exploit BU in Mobile IPv6

2.1.1.1 Attack Against Secrecy and Integrity

An attacker sends a spoofed Binding Update to the Correspondent node as shown in Figure 2.2. An attacker can capture the data intended for the Mobile node and by pretending to be the Mobile node can hijack the connection with the Correspondent node, or establish new spoofed connections. Consequently, the attacker is able to see and modify the packets sent between the Correspondent node and the Mobile node.

These attacks are possible when the Mobile node and the Correspondent node support Route Optimization (RO) and the attacker knows their IP addresses. Strong encryption and integrity protection can prevent all sorts of attacks against data secrecy and integrity.

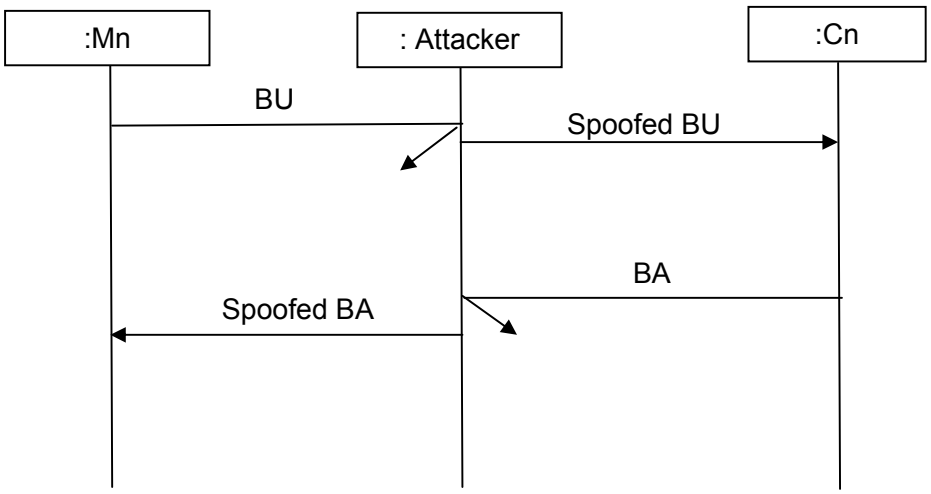

Figure 2.2: Attack Against Secrecy and Integrity

[1] Mn → Cn (captured by attacker): BU

[2] Attacker →Cn: spoofed BU

[3] Cn→ Mn (Captured by attacker): BA

[4] Attacker → Mn: spoofed BA

2.1.1.2 Attack Using HoA to Send Unwanted Data to Any Host

When the Binding Update signal is not authenticated, the attacker can choose any arbitrary address as its Home of Address (HoA) and thus target any Internet node. What happens is that an attacker claims to be a Mobile node with the HoA address similar to the target IP address. Then the attacker sends a Binding Update with its real IP as CoA and the target IP address as HoA as shown in Figure 2.3. The attacker then waits for the Binding Updates to expire, which will cause the Correspondent node to redirect the data traffic to the target IP address. The attacker can keep the stream alive by spoofing acknowledgements. Strong authentication for the identity of the machine and the association with its home address can prevent this type of attack.

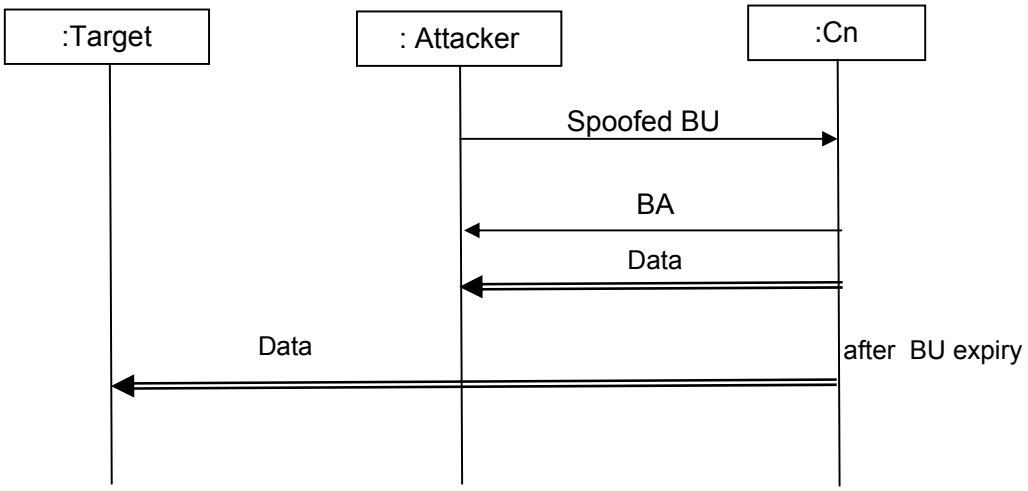

Figure 2.3: Attack Using HoA to Send Unwanted Data to Any Host

[1] Attacker (fake Mn) → Cn : spoofed BU [Target address as attacker's HoA, Attacker's CoA, t]

[2] Cn →Attacker: BA

2.1.1.3 Attack Using CoA to Send Unwanted Data to Any Host

This is similar to the type of the attack mentioned above only that in this sort of attack an attacker can choose any arbitrary address as its Care of Address (CoA) and thus target any Internet node. An attacker claims to be a Mobile node with the CoA similar to the target IP address.

Ingress filtering in the attacker's local network can control the problem but not solve it. Ingress filtering prevents the spoofing of source addresses but the attack is still possible if the attacker in the same network of the targeted address. An attacker can also target one or more IP addresses within the network by using this attack and the above one in tandem. Strong authentication of real IPv6 addresses is needed to mitigate this type of attack.

2.1.2 Attacks when Binding Update Signals are Authenticated and Secured

This type of attack usually is related to a particular security protocol like the attacks that exploit the Return Routability protocol which are explained in section 2.3.1 and also related to the attacks that exploit the security solutions, which are explained in section 2.4. However Replay Attack should be considered in any security solution proposed for Mobile IPv6. The next section explains the Replay attack in Mobile IPv6. Other attacks will be explained in section 2.3.1 and 2.4.

2.1.2.1 Replay Attack in Mobile IPv6

Any protocol that authenticates Binding Update signals will have to consider Replay Attack (WIKIPEDIA, 2007c), that is, an attacker may be able to replay recent authenticated Binding Updates to the Correspondent node and, that way, direct packets to the Mobile

node's previous location. What happens is that an attacker can capture the packets and impersonate the Mobile node if it reserves the Mobile node's previous address after the Mobile node has moved away and then replays the previous Binding Update to redirect packets back to the previous location as shown in Figure 2.4. The attack is a concern if the Mobile node is moving so frequently that it sends the next Binding Update before the previous Binding Update has expired.

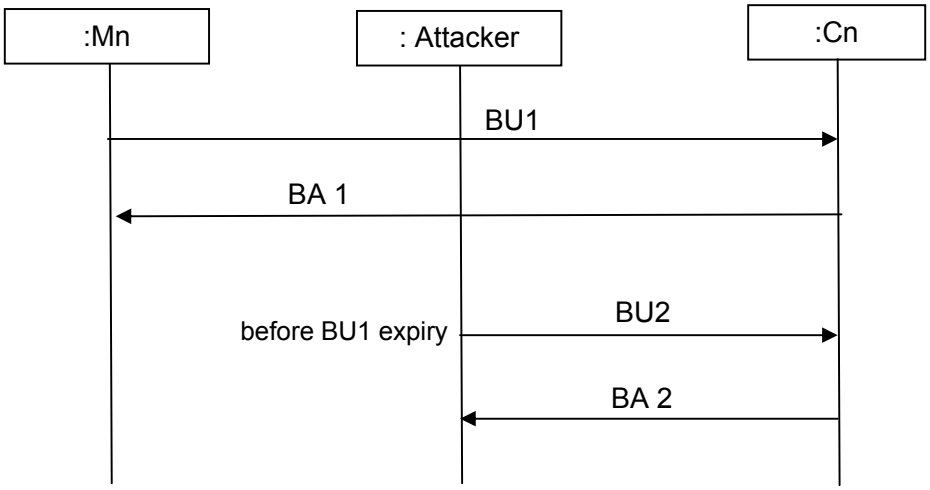

Figure 2.4: Replay Attack

[1] Mn → Cn: BU1 (Binding with the Mobile node's current CoA)

[2] Cn → Mn: BA 1

[3] Attacker → Cn: BU2 (Binding with the Mobile node's previous CoA)

[4] Cn →Attacker: BA1

Because of these attacks, the Mobile IP group has to design security protocols to secure the Binding Update signals. These security protocols are explained in the next section.