Mobile IPv4 Secure Access to Home Networks

A Thesis
Presented to
The Academic Faculty

by

Jin Tang

In Partial Fulfillment
of the Requirements for the Degree
Doctor of Philosophy

School of Electrical and Computer Engineering
Georgia Institute of Technology
August 2006

Mobile IPv4 Secure Access to Home Networks

Approved by:

Professor John A. Copeland, Advisor
School of Electrical and Computer Engineering
Georgia Institute of Technology

Professor Henry Owen
School of Electrical and Computer Engineering
Georgia Institute of Technology

Professor Chuanyi Ji
School of Electrical and Computer Engineering
Georgia Institute of Technology

Professor Raheem A. Beyah
Department of Computer Science
Georgia State University
Adjunct, School of Electrical and Computer Engineering
Georgia Institute of Technology

Professor Mustaque Ahamad
College of Computing
Georgia Institute of Technology

Date Approved: June 26, 2006

To my parents and sister,

for everything.

ACKNOWLEDGEMENTS

It is my pleasure to give my sincere thanks to all the people who have supported and helped me during the pursuit of my Ph.D. degree. Without their encouragement, I would not have completed this dissertation.

First of all, I would like to express my deep gratitude to my dissertation advisor, Dr. John A. Copeland, for his constant support, guidance, and encouragement through my Ph.D. study. Dr. Copeland has taught me how to not only do research but also lead a life. Under his kind help, I have improved my ability at various aspects. What I have learned from him will be very useful to my future career and life.

I would like to thank Dr. Henry Owen and Dr. Chuanyi Ji for serving on my dissertation proposal committee and defense committee. I would also like to acknowledge Dr. Mustaque Ahamad and Dr. Raheem Beyah for being on my dissertation defense committee and Dr. Yorai Wardi for being on my dissertation proposal committee. Their valuable and insightful suggestions have helped me to refine and improve my research work.

I would like to extend my appreciation to Dr. Siqing Zheng in University of Texas at Dallas and Dr. Jianhua Chen in Louisiana State University for their warm-hearted help. They motivated my interests in doing research.

I would also like to express my acknowledgement to the present and past members in Communications Systems Center. I am fortunate to know and work with them. Their friendship has accompanied me through these years. Special thanks to Dr. Kulsoom Abdullah and Chris Lee for their sincere help. Many thanks to Kathy Cheek for helping me in administrative affairs.

I am also grateful to all my friends in Georgia Institute of Technology. They have helped me to enjoy research as well as life.

Last but not least, I am deeply indebted to my parents and sister for their love, support, encouragement, sacrifices, and patience. No words can fully express my appreciation to

them. This thesis is dedicated to them.

TABLE OF CONTENTS

LIST OF FIGURES

SUMMARY

With the fast development of wireless networks and devices, Mobile IP is expected to be used widely so that mobile users can access the Internet anywhere, anytime without interruption. However, some problems, such as firewall traversal and use of private IP addresses, restrict use of Mobile IP. The objective of this thesis is to design original schemes that can enable a mobile node at abroad to access its home network as well as the Internet securely and that can help Mobile IP to be used widely and commercially. Our solutions are secure, efficient, and scalable. They can be implemented and maintained easily. In this thesis, we mainly consider Mobile IPv4, instead of Mobile IPv6. Three research topics are discussed. In each topic, the challenges are investigated and the new solutions are presented.

The first research topic solves the firewall traversal problems in Mobile IP. A mobile node cannot access its firewall-protected home network if it fails the authentication by the firewall. We propose that an IPsec tunnel be established between the firewall and the foreign agent for firewall traversal and that an IPsec transport security association be shared by the mobile node and a correspondent node for end-to-end security.

The second topic researches further on firewall traversal problems and investigates the way of establishing security associations among network entities. A new security model and a new key distribution method are developed. With the help of the security model and keys, the firewall and the relevant network entities set up IPsec security associations to achieve firewall traversal.

A mobile node from a private home network cannot communicate with other hosts with its private home address when it is visiting a public foreign network. A novel and useful solution is presented in the third research topic. We suggest that the mobile node use its Network Access Identifier (NAI) as its identification and obtain a public home address from its home agent. In addition, a new tunnel between the mobile node and its home agent is proposed.

CHAPTER I

INTRODUCTION

With the fast development of wireless networks and devices, more and more customers demand access to the Internet anywhere, anytime without interruption. In the Internet, an IP address is used to identify a network attachment point of a computer, and a tuple (*IP address, port number*) is employed to distinguish a connection. Whenever a mobile computer moves from a network attachment point to another, its IP address changes, and connections between the mobile computer and other hosts have to be stopped. For this reason, a mobile computer needs to have a stable IP address to maintain continuous communications with other hosts. However, a stable IP address means that a mobile computer cannot move from one network to another, that is, a stable IP address restricts the movement of a mobile computer. Many approaches [19, 37, 48] have been proposed to solve this mobility problem. Among them, Mobile IP [20, 41, 37, 38, 49], in which a mobile computer utilizes two IP addresses, successfully achieves seamless roaming. That is, in Mobile IP, although a mobile node's network attachment point changes because of movement, its permanent IP address keeps the same. Therefore, the connections between the mobile node and other hosts are not interrupted by the movement.

In this chapter, firstly we give an introduction to Mobile IP. Then we briefly describe the research objectives and the thesis outline.

1.1 Mobile IP Overview

Because the main task of Mobile IP is to correctly address packets to mobile computers, it is a routing protocol. Mobile IP is implemented on the network layer, so it is transparent to upper-layer applications. In Mobile IP, each mobile computer is completely administered by one network, and that network is called the mobile computer's *home network*. Other networks are called the mobile computer's *foreign networks*. Three new network entities are introduced as follows:

- Mobile Node (MN): a host that can change its network attachment point without changing its IP address. Thus a mobile node can communicate with other hosts without any interruption when it moves around different networks.
- Home Agent (HA): a router on a mobile node's home network that helps the mobile node's registration and packet delivery.
- Foreign Agent (FA): a router on a mobile node's foreign network that cooperates with the mobile node's home agent to finish registration and packet delivery.

An example of a Mobile IP scenario is shown in Figure 1. At least one home agent is located in a home network. It is optional that one or several foreign agents be deployed in a foreign network. Three mobile nodes, MN_1, MN_2, and MN_3 belong to the same home network. These mobile nodes may stay within the home network or visit foreign networks. They may exchange packets with other *correspondent nodes* (CN) that are located inside as well as outside the home network. While a mobile node works in the same way as other hosts when it stays at home, it works differently when it visits a foreign network. Specifically, when being away from home, a mobile node has to depend on the help of its home agent and a possible foreign agent to communicate with other correspondent nodes.

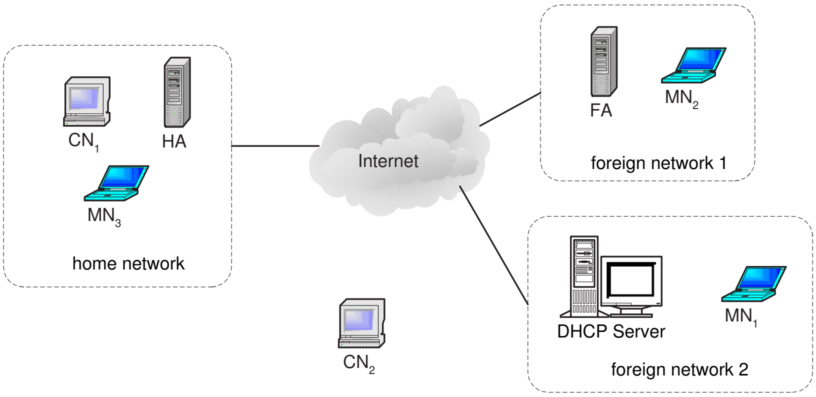


Figure 1: An example of a Mobile IP scenario.

In Mobile IP, to achieve mobility, each mobile node has two IP addresses. One is permanent and used for identification of a mobile node; hence this long-term IP address is called the mobile node's *home address.* The other IP address reflects the current location of a mobile node. That is, whenever the mobile node changes its point of network attachment, this address changes. Therefore, this address is temporary and used for routing. It is called the mobile node's *care-of address.* There are two types of care-of addresses. One is provided by a foreign agent and is called a *foreign agent care-of address.* The other is acquired by a mobile node itself through some external means and is called a *co-located care-of address.* For example, in Figure 1, the mobile node M_1 may get a co-located care-of address from a DHCP [12, 27] server and the mobile node M_2 may get a care-of address from a foreign agent.

In Mobile IP, it takes three steps for a mobile node to achieve seamless roaming, i.e., agent discovery, registration, and tunnelling. In other words, a mobile node finds mobile agents, registers with its home agent, and then communicates with other correspondent nodes. In the following, we explain these three steps in detail.

1.1.1 Agent Discovery

Both home agents and foreign agents are required to periodically broadcast *agent advertisement* messages.

A foreign agent uses agent advertisement messages to have its services and care-of addresses publicly known. Upon receipt of such a message, a mobile node compares this message with the previous agent advertisement message that it receives to detect whether it still stays within the same foreign network or already moves to another one. If the mobile node finds out that it is visiting a new foreign network, it needs to send a *registration request* message to its home agent.

While a foreign agent may claim to be too busy to serve mobile nodes, a home agent has to be available to its mobile nodes at any time. To avoid overload, usually there are several home agents in a home network, and each is in charge of almost an equal number of mobile nodes. With the help of an agent advertisement message broadcast by a home agent, a mobile node can determine whether it already has returned to its home network or is still visiting a foreign network. If the mobile node is back home, it is required to deregister with its home agent.

A mobile node is allowed to send an *agent solicitation* message if it does not want to wait for mobile agents' advertisement messages.

Since Mobile IP assumes that any agent that broadcasts its services is a mobility agent, it is unnecessary to put an authentication part into agent advertisement and solicitation messages. In the Internet, although some hackers may pretend to be mobility agents and attract mobile nodes to use their services, registration messages, which are explained in the following section, can protect mobile nodes against vulnerability.

1.1.2 Registration

When a mobile node receives an advertisement message broadcast by a mobility agent, it can determine its current location and decide whether it needs to send a *registration request* message to its home agent. Under the following conditions a mobile node should request a registration.

- When a mobile node just visits a new foreign network, it is required to inform its home agent of its current location and possibly to request services from a foreign agent.
- When a current registration time nearly expires, a mobile node should register to renew a binding.
- When a mobile node returns to its home network, it should deregister with its home agent so that its previous bindings can be deleted.

A mobile node may send a registration request to its home agent directly or through a foreign agent. Because a foreign agent is used in our research, we only discuss the latter case in the following.

The mobile node initiates a registration request and sends that to the foreign agent. The foreign agent plays a passive role in the registration procedure [41]. On receipt of a registration request message, the foreign agent checks its validity. If the message is invalid, the foreign agent discards it and sends a denial reply to the mobile node. Otherwise, the foreign agent finds the address of the home agent from the registration request message, puts that address as the destination, and then forwards the registration request message to the home agent.

The home agent plays a reactive role in the registration procedure [41]. If the home agent receives an invalid registration request relayed by the foreign agent, it rejects the registration request and returns a *registration reply* message indicating the reason for error. However, if the registration request satisfies the validity check, the home agent stores the current care-of address of the mobile node and updates the record of the mobile node's mobility bindings. Then the home agent is required to send a registration reply message back.

The foreign agent needs to check the validity of a registration reply message sent from the home agent. If the registration reply message does not pass the validity check, the foreign agent discards the reply message silently. At the same time, it sends a registration reply to the mobile node to notify it of the denial reason. But if the foreign agent receives a valid registration reply from the home agent, it modifies its visitor list for the successful registration of the mobile node and relays the reply message to the mobile node. Then the mobile node receives the reply message and completes registration.

Mobile IP uses the User Datagram Protocol (UDP) [44] instead of the Transmission Control Protocol (TCP) [45] for transporting registration messages. One reason for this choice is that Mobile IP does not need services provided by TCP, such as windowing, congestion control, or flow control. Another reason is that TCP performs poorly when packets are dropped as a result of high link error rates in wireless networks [4].

Since a mobile node is more vulnerable in wireless networks than in wired networks, it is very important to protect communications between a mobile node and its home agent against malicious users. Therefore, it is required for a mobile node to share a security association with its home agent in Mobile IP. With the security association, the mobile node and its home agent can authenticate registration messages exchanged between them.

Furthermore, if a mobile node shares a security association with a foreign agent, it can trust the services provided by the foreign agent. Similarly, if a home agent has shared a security association with a foreign agent, it can determine whether messages sent from the foreign agent have been modified by malicious users. However, because the administrative domain of a foreign agent is usually different from that of a mobile node and a home agent, in Mobile IP, it is optional for the foreign agent to have respective security associations with the mobile node and the home agent.

With respective security associations, a mobile node, a home agent, and a foreign agent may generate authentication extensions and append them to registration messages. In Mobile IP, there are three authentication extensions, i.e., the *mobile-home* authentication extension, the *mobile-foreign* authentication extension, and the *foreign-home* authentication extension. Based on the reasons explained above, the first authentication extension is required in all registration messages, and the other two are optional.

1.1.3 Tunneling

If a mobile node stays at its home network, the IP protocol is followed for packet delivery between the mobile node and other correspondent nodes. However, if a mobile node leaves its home, the Mobile IP protocol is used for transmitting packets. Because a foreign agent is deployed in our research, in the following we only introduce how data packets are delivered with the deployment of a foreign agent.

In Mobile IP, a *tunnel* is established from the address of the home agent to the care-of address of the mobile node for packet delivery. An IP packet is encapsulated at the entry point of the tunnel, i.e., the home agent, and then decapsulated at the exit point of the tunnel, i.e., the foreign agent. Both the home agent and the foreign agent are required to support tunneling packets using IP-in-IP encapsulation.

In IP-in-IP encapsulation, a new IP header is inserted before an original packet to form a new IP packet, shown in Figure 2. Therefore, the source address and the destination address of the new IP packet are used for routing from the entry point of the tunnel to the exit point.

A mobile node away from home may communicate with a correspondent node after registration. As shown in Figure 3, the home agent attracts packets destined for the mobile node. Then the home agent tunnels these packets to the foreign agent by encapsulating

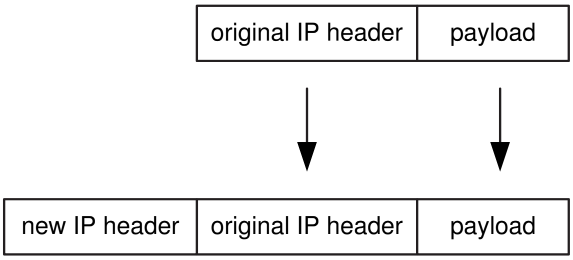


Figure 2: IP-in-IP encapsulation [37, 41].

them with new IP headers. In the new IP headers, the home agent's address is used as the source and the mobile node's care-of address as the destination. These packets exit from the tunnel at the foreign agent. In other words, once receiving the packets, the foreign agent removes the new IP headers added by the home agent. Then the foreign agent transmits the original packets to the mobile node.

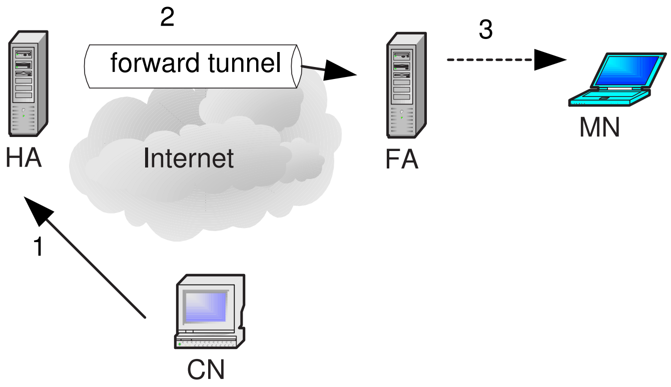


Figure 3: Packet delivery from a correspondent node to a mobile node [37, 41].

In the opposite direction, packet transmission may follow the IP routing, that is, the mobile node puts its home address as the source and sends packets directly to the correspondent node. However, because the mobile node is visiting a foreign network, the packets' source address, i.e., the mobile node's home address, is not topologically correct [34]. Currently, many routers check packets' source addresses besides destination addresses to prevent various attacks. They usually drop packets that do not have topologically correct source addresses because the routers doubt that these packets are from IP spoofing hosts. Therefore, a *reverse tunnel* [34] has been proposed to solve this problem. A reverse tunnel is established from the mobile node's care-of address to the home agent. Hence, a tunnel from the home agent to the mobile node's care-of address is also called a *forward tunnel.* It is assumed that the same configuration is used for both the forward tunnel and the reverse tunnel.

If a reverse tunnel is used, as shown in Figure 4, packets with the mobile node's home address as the source are put into the reverse tunnel by the foreign agent. Thus, in the encapsulated packets, the new source is the mobile node's care-of address and the new destination is the home agent's address. At the exit of the reverse tunnel, the home agent releases the packets and transmits them to the correspondent node.

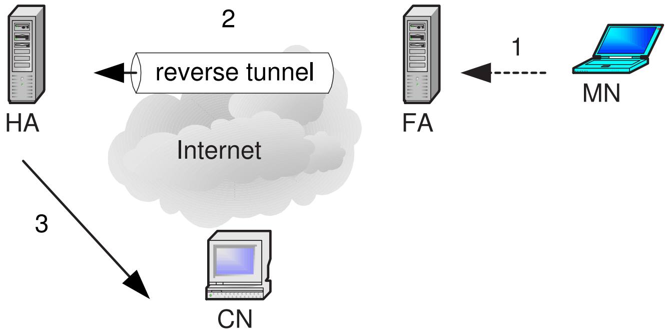


Figure 4: Packet delivery from a mobile node to a correspondent node with a reverse tunnel.

Some security problems might arise out of reverse tunnels. For example, if a foreign agent does not have respective security associations with a mobile node and a home agent, a malicious node might hijack the existing reverse tunnel and re-direct the tunnel to other nodes [34]. Therefore, the security associations shared between the foreign agent and the mobile node and those shared between the foreign agent and the home agent are very useful.

1.2 Research Objectives and Solutions

Although Mobile IP can provide seamless roaming services, some problems, such as firewall traversal, prevent Mobile IP from being used widely. The objective of this thesis is to develop original schemes that can enable a mobile node at abroad to access its home network as well as the Internet securely and that can help Mobile IP to be used widely and efficiently. Our solutions are intended to be implemented and maintained easily. In this thesis, we mainly discuss Mobile IPv4 [41], instead of Mobile IPv6 [20]. Three research topics are investigated. In the following, each topic is briefly explained.

1.2.1 Mobile IP Secure Firewall Traversal with the Deployment of Foreign Agents

If a mobile node's home network is firewall-protected, the mobile node at abroad cannot access its home network without successful authentication. Therefore, the home agent can neither know the current location of the mobile node nor tunnel packets to it. To some extent, the mobile node loses contact with its home agent and other correspondent nodes.

In our research, we consider the network scenario that, in Mobile IPv4, a mobile node away from its firewall-protected home network obtains a care-of address from a foreign agent. Our objective is to enable the mobile node to communicate with its home agent and other correspondent nodes that are located inside the home network behind the firewall. IPsec mechanisms [26] are applied on network entities. Specifically, an IPsec tunnel is established between the firewall and the foreign agent for firewall traversal, and a transport security association is shared between the mobile node and a correspondent node for end-to-end security. This approach can be extended to the network scenario in which foreign agents are deployed hierarchically.

Our solution is secure and scalable. The security association shared between the mobile node and a correspondent node does not need to be refreshed for the mobile node's handoffs.

1.2.2 Secure Firewall Traversal in the Mobile IP AAA System

Mobile IP is only a mobility technology. Mobile IP can be used commercially if it is combined with services of Authentication, Authorization, and Accounting (AAA) [13]. However, if a firewall is used to protect the home domain of a mobile node, the firewall prevents the mobile node from accessing the home domain without successful authentication. Thus the mobile node gets lost.

IPsec mechanisms can be used on network entities, similar to the first research topic explained in Section 1.2.1. Nevertheless, in the first research topic, the way of establishing security relationships is not investigated. In this research topic, a novel security model is proposed. The essential security associations shared by the network entities are illustrated in the security model. Moreover, a new key is suggested to be generated and a new method for key distribution is presented. The firewall and the relevant network entities use these essential security associations and these keys to set up IPsec security associations so that messages originally sent from the mobile node can pass through the firewall.

1.2.3 Mobile IP Use of Private Addresses in an RSIP Home Network

Because of a shortage of IP addresses and burden of routing overhead [46], many organizations apply private addresses in their internal networks. If the home network of a mobile node uses private addresses, the mobile node away from home does not have a public home address to uniquely identify itself in a public network. Thus, the mobile node cannot communicate with other correspondent nodes when it stays away from its home network.

In the network scenario that we discuss, the home network of a mobile node is a private network and the mobile node obtains its care-of address from a foreign agent in a public foreign network. Our approach can enable the mobile node to communicate with a correspondent node when it is at abroad. In more detail, the mobile node uses its Network Access Identifier (NAI) [1] to uniquely identify itself in a public network. When the mobile node enters a foreign network, if it does not have a public home address by that time, it puts its NAI and the IP address 0.0.0.0 to the registration request message and sends the message to the home agent. The home agent assigns a public home address to the mobile node. When the mobile node communicates with a correspondent node that is located inside the home network, to prevent private addresses from being accessed in the public network, an additional IP header is necessary to encapsulate an original data packet. If a firewall is used to protect the private home network, our scheme can also be extended to achieve for the mobile node to get access to its home network.

Our solution neither uses any private addresses in the public network nor brings any additional security holes.

1.3 Thesis Outline

The rest of this thesis includes four chapters.

Chapter 2 focuses on the solution to firewall traversal in Mobile IP. Because IPsec mechanisms are applied on network entities, an overview of IPsec is given. After the firewall traversal problems and related work are analyzed, the network scenario and assumptions used for our discussion are illustrated. We argue for the advantage and necessities of foreign agent deployment. Then, we present our firewall traversal solution in detail and extend the solution to the network scenario of hierarchical foreign agents. Analysis of our solution is also given in this chapter.

The approach to the firewall traversal in the Mobile IP AAA system is presented in Chapter 3. After the Mobile IP AAA system is introduced, challenges and related work are investigated. Then we go into details about our design, including the new security model, the key generation and distribution, and control message flow.

Chapter 4 gives the detailed scheme for using private addresses in Mobile IP. Because an Realm Specific IP (RSIP) [8] gateway is used in the network scenario for our discussion, an outline of RSIP is given. After we analyze the problems for use of private addresses in Mobile IP and related work, we specify the principles, objectives and considerations of our design protocols. The detailed communication procedures are illustrated with figures. We also extend our solution to the situation that a firewall is placed at the entrance of a private home network. Our solution is evaluated before the end of this chapter.

We summarize our research contributions in Chapter 5.

CHAPTER II

MOBILE IP SECURE FIREWALL TRAVERSAL WITH THE DEPLOYMENT OF FOREIGN AGENTS

2.1 Problems of Mobile IP Firewall Traversal

Nowadays, there are numerous attacks in the Internet. Since firewalls can monitor traffic to and from internal networks and only allow authorized traffic to pass, they are an effective tool to keep attacks outside internal networks and to minimize the danger [5, 52]. Thus many organizations install firewalls to protect their internal networks against attacks from the Internet. In Mobile IP, because mobile nodes roam over the Internet and use wireless links for communications, such characteristics provide more opportunities for hackers, and home networks are more vulnerable to attacks. So it seems that the deployment of firewalls is a good way to protect home networks. Contradictorily, firewalls bring problems to use of Mobile IP. Specifically, if a mobile node's home network is firewall-protected, when the mobile node is at abroad, it cannot contact its home agent unless it can be authenticated by the firewall successfully. Without access to its home agent, the mobile node cannot complete registrations. In other words, the home agent cannot know the current location of the mobile node and tunnel the packets destined for the mobile node, which leads that other correspondent nodes cannot communicate with the mobile node. Consequently the most significant advantage of Mobile IP, seamless roaming, is shadowed by intervention of firewalls.

2.2 Overview of IPsec

Because many approaches for solving the firewall traversal problems use IPsec, in this section we give an overview of IPsec.

IP security (IPsec) [26] is security mechanisms that are implemented on the network layer. Because IPsec authenticates and/or encrypts all traffic on the network layer, the security of upper-layer applications can be ensured. Since IPsec is below the transport layer, upper-layer applications are not affected by its implementation. IPsec is also transparent to end users, so end users do not need to learn IPsec mechanisms.

To achieve services of encryption and authentication in IPsec, a *security association* (SA) between a sender and a receiver is necessary. The SA is unidirectional. Therefore, to achieve a secure two-way communication between two hosts, two security associations are needed. Three parameters together can uniquely identify a security association. These parameters are *Security Parameters Index* (SPI), *IP Destination Address* and *Security Protocol Identifier* [23, 52]. Whenever one of these three parameters changes, a sender and a receiver have to re-negotiate the security associations between them. For example, if the receiver changes its IP address, a new security association is required to be re-established.

Two protocols, Authentication Header (AH) [24] and Encapsulating Security Payload (ESP) [25], are used to provide security services. The Authentication Header protocol uses a message authentication code (MAC) to support security services of authentication and data integrity. Thus, a sender and a receiver must share a secret key. With the help of the secret key, the receiver can authenticate the sender and detect modification of data packets. In addition, the Authentication Header protocol can guard against IP spoofing and replay attacks. The Encapsulating Security Payload protocol supports confidentiality besides the services provided by AH. Similar to AH, ESP also requires that a secret key be shared between a sender and a receiver. The sender uses this shared key to encrypt payload of data packets so that no one but the receiver can know the information contained in the data packets.

Both AH and ESP support two mode: transport mode and tunnel mode [23, 52]. Transport mode only protects data from upper-layers. That is, transport mode primarily gives protection for the payload of IP packets, and it does not ensure the security of IP header, as shown in Figure 5. Transport mode is generally used to achieve end-to-end security. AH in transport mode supports authentication for the payload of IP packets, and ESP in transport mode may encrypt the payload.

Different from transport mode, tunnel mode protects an entire packet. Firstly, an entire

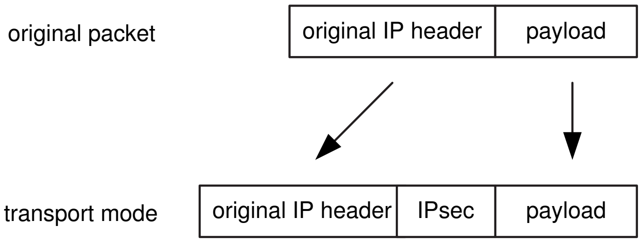


Figure 5: Packet formats of IPsec transport mode [23, 52].

packet, including the IP header and the payload, is authenticated and/or encrypted. Then, the entire packet is encapsulated with a new IP header, as shown in Figure 6. Because the original packet is encapsulated with a new IP header in tunnel mode, the packet overhead in tunnel mode is larger than that in transport mode.

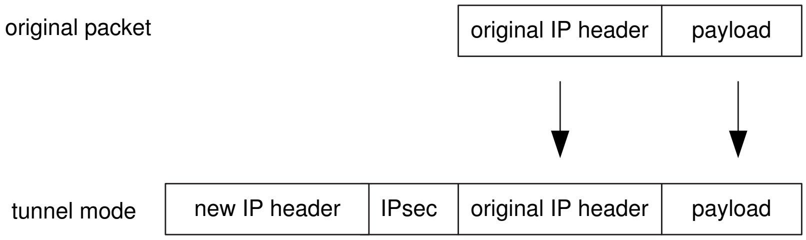
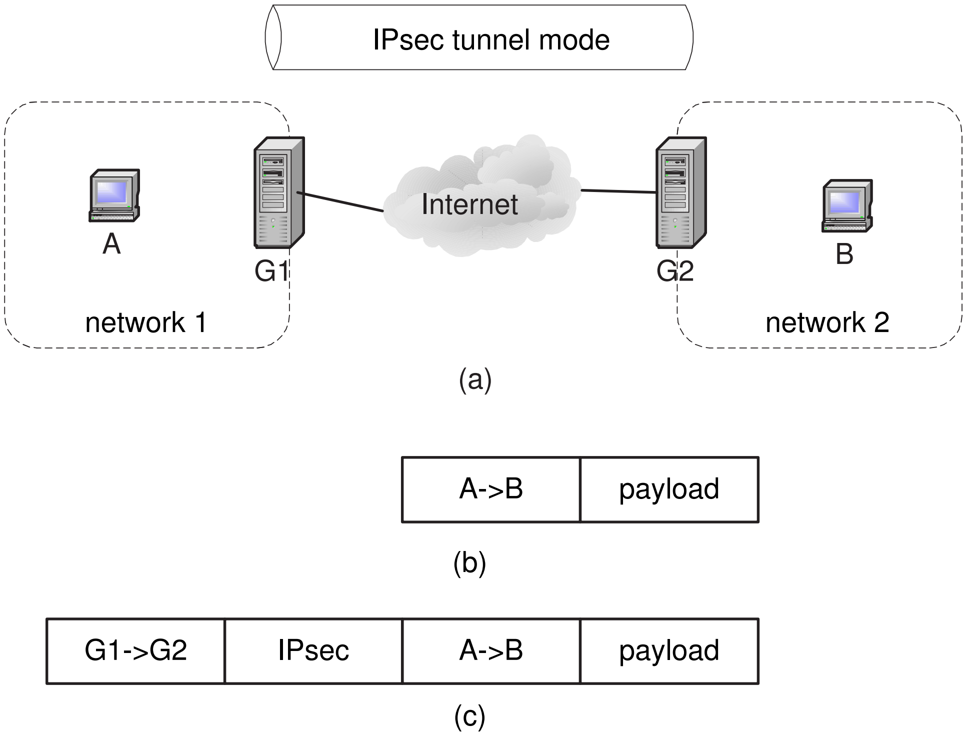


Figure 6: Packet formats of IPsec tunnel mode [23, 52].

In IPsec tunnel mode, the source and destination in a new IP header are two end points of a tunnel. When a packet traverses in this tunnel, no router along the path can examine the original packet. Usually gateways located between an internal network and the Internet are end points of a tunnel. Hosts behind the gateways may send unprotected packets. For example, in Figure 7(a), the gateways *G1* and *G2* are respectively located on the borders of two networks, and the Internet is between them. The hosts *A* and *B* are not installed security software to protect packets that they send. In order for the traffic exchanged between host *A* and host *B* to securely pass through the Internet, an IPsec tunnel is set up between the two gateways. In an original packet sent by the host *A*, the source address is the IP address of host *A* and the destination is the host *B* (Figure 7(b)). Before the gateway *G1* sends the packet, it uses IPsec mechanisms to protect the entire original packet . Then the gateway *G1* encapsulates the packet with a new IP header. Different from the original

IP header, the source in the new IP header is the address of the gateway *G1* and the destination is the gateway *G2* (Figure 7(c)). Because of the shared secret between the gateway *G1* and *G2*, the gateway *G2* can release the packet from the IPsec tunnel and deliver the original packet (Figure 7(b)) to the host *B*.



(a)

(b)

(c)

Figure 7: An example for use of IPsec tunnel mode: (a) network framework; (b) a packet sent by host *A*; (c) a packet sent by gateway *G1*.

2.3 Related Work

In recent years, the problems of firewall traversal by a mobile node have been investigated, and several solutions have been proposed.

Zao *et al.*[58, 57] point out that a firewall may also work as a mobility agent, that is, the functions of a firewall and a mobility agent may be combined together. Similarly, Mink *et al.* [32] propose that a gateway be inserted into a network's firewall and that this gateway use the security association shared between itself and the mobile node to authenticate the mobile node. Although these approaches [32, 58, 57] make perfect sense, there exist some practical problems. Currently many firewalls that have already been installed widely have no function of mobility agents. The cost is very high to upgrade these firewalls with mobility features. This kind of upgrade brings the issue of interoperability when technologies of mobility agents and firewalls are from different vendors [3]. Moreover, from the security point of view, it is suggested that firewalls run as few programs as possible to avoid security flaws [5]. As a result, there may be some potential security holes on firewalls if firewalls also act as mobility agents.

Because of characteristics of IPsec [26], many solutions [9, 14, 36, 55] focus on IPsec and employ it to solve the firewall traversal problems. In more detail, one IPsec tunnel is established between the mobile node's co-located care-of address and the firewall, and one Mobile IP tunnel is inserted inside the IPsec tunnel. The IPsec tunnel achieves data packets to pass through the firewall, and the Mobile IP tunnel helps data packets to transfer to and from the mobile node. Although it is very useful to apply IPsec mechanisms to network entities, these solutions [9, 14, 36, 55] still have some drawbacks. Firstly, all of them [9, 14, 36, 55] assume that the internal network is secure, hence only plaintext messages are transferred between the home agent and the firewall. However, it is well known that this assumption is not achievable in the real world because many hackers stay behind the firewall and attack the internal network. Therefore, it is not secure to use only plaintext messages in the internal network, especially for the security-sensitive messages. Secondly, since the IPsec tunnel terminates at the firewall, the firewall can read everything transferred between the two end users. In other words, no end-to-end security is achieved. Nowadays, end-to-end security becomes more and more important in many areas, such as e-commerce, where it is required that no third party know any secret information. Even worse, if the firewall is compromised, there may exist a potential "man-in-the-middle" threat and the firewall may modify messages exchanged between the end users. Thirdly, in these solutions [9, 14, 36, 55], the mobile node employs a co-located care-of address when it is away from home. In IPsec mechanisms, *IP Destination Address* is one of three parameters to identify a security association. As a result, whenever the mobile node obtains a new co-located care-of address, the IPsec tunnel security association has to be refreshed, which degrades the handoff performance [3]. Re-negotiation of security associations also costs power consumption and computation resources that are limited for a mobile node.

The basic reason that a security association needs to be refreshed during movement in above solutions [9, 14, 36, 55] is that IPsec mechanisms are applied after Mobile IP encapsulation [6]. The following solutions [56, 6] apply IPsec over Mobile IP to achieve no re-negotiation of security associations during handoffs, but they have some other disadvantages.

Vaarala and Klovning [56] proposes a new topology so that a mobile node can communicate with its firewall-protected home agent. In this topology there are two home agents. One is located in the internal network and is called *i-HA*. The other is located in the external network and is called *x-HA*. In order to detect itself location, the mobile node simultaneously sends two registration requests to i-HA and x-HA respectively. If the mobile node is within the internal network, it follows standard Mobile IP protocol. Otherwise, it registers its care-of address with the x-HA, establishes a VPN tunnel between itself and the firewall, and then registers the VPN tunnel inner address as its care-of address with the i-HA. As explained above, because another layer of Mobile IP is employed under IPsec, no re-negotiation for IPsec security associations is required whenever the mobile node obtains a new care-of address. Nevertheless, the solution of dual home agents may bring redirection attacks [56]. Like solutions in above proposals [9, 14, 36, 55], the IPsec tunnel still terminates at the firewall, instead of i-HA, accordingly, there is no end-to-end security between the mobile node and i-HA. In addition, the employment of an external home agent also has some shortcomings. Firstly, the total cost is increased. Secondly, the external home agent is under various attacks in the Internet and may be easily compromised because it is outside the firewall. Finally, the two separate registration requests sent from the mobile node to i-HA and x-HA increase network traffic load if the handoff is frequent.

Berioli and Trotta [6] also apply IPsec mechanisms after Mobile IP, that is, a Mobile IP tunnel encapsulates an IPsec tunnel. To achieve seamless handoffs, a mobile node uses its home address, not care-of address, for the IPsec tunnel establishment. However, this solution has some requirements on home network topology and firewall configuration [6]. In more detail, it requires the home agent be reachable directly from outside. Therefore, the home agent cannot be protected by the firewall and may be attacked by hackers. The firewall has to be configured particularly so that the traffic destined for the mobile node is forced to pass through the VPN gateway before the home agent. Furthermore, the Mobile IP data traffic is not protected by any security mechanism on network layer, thus redirection attacks are possible. Also there is no end-to-end security achievement in this solution.

2.4 Network Framework Model and Assumptions

The network framework shown in Figure 8 is used for our discussion. A firewall is used to protect a mobile node's home network from external attacks. The firewall is the only entry point to the home network so that all traffic must go through it, no matter whether the traffic is from outside to inside or vice versa. The firewall only allows packets with successful authentication to enter the home network and drops other unqualified packets. Although the home network is firewall-protected, we do not assume that the home network is secure, i.e., some hackers may stay behind the firewall. In the real world, normally there are some firewalls installed within the home network for better security protection, but we do not consider this case here for the simplicity reason.

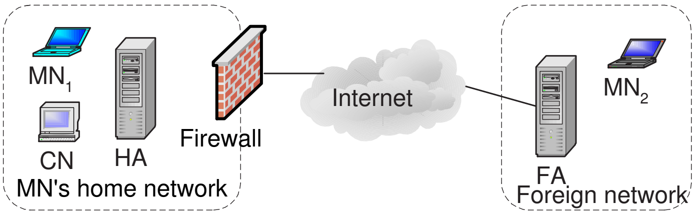


Figure 8: Network framework for firewall traversal in Mobile IP.

Unlike architectures in the solutions of [6] and [56], in our discussion, the home agent is located behind the firewall in order not to be exposed to various Internet attacks. Moreover, there is no external home agent. Different from the approaches in [32, 58, 57], in our scenario, the home agent and the firewall run on separate physical machines to avoid the potential security flaws and the interoperability problems that we point out in Section 2.3.

Correspondent nodes may be placed either inside or outside the mobile node's home network. Here we only consider the situation that the correspondent nodes are located behind the firewall of the home network. Because the mobile node and the correspondent node belong to the same network, it is natural to assume that they can be pre-configured to share a security association.

A mobile node can move freely and seamlessly within its home network as well as abroad. When the mobile node is at home, it can communicate with its home agent and other hosts behind the firewall directly. Nevertheless, when it enters a foreign network, unlike discussions in those solutions [9, 14, 36, 55], the mobile node obtains a care-of address from a foreign agent. In addition, we assume that the foreign agent is the default router of the mobile node.

If the foreign network is protected by a firewall as well, it is not reasonable to allow a mobile node to stay behind this firewall because the mobile node is an external node to the foreign network. The main function of a foreign agent is to relay messages to and from mobile nodes, that is, it always deals with external nodes. Therefore it is appropriate to place a foreign agent outside its network firewall. In a word, both the mobile node and the foreign agent should be located outside the firewall of the foreign network. So in our discussion, the firewall of the foreign network, if there is one, is omitted in Fig. 8. Certainly both the mobile node and the foreign agent are require installing some security software to protect themselves from attacks. For simplicity reason, the case of multiple firewalls is not considered here. As a result, in our scenario, when the mobile node is away from home, it only needs to traverse the firewall that protects its home network.

2.5 Deployment of Foreign Agents

As explained in Section 1.1, two different procedures for registration are defined in Mobile IP [41, 37]. One is that a mobile node obtains its care-of address from a foreign agent and sends the registration request to its home agent via the foreign agent. The other is that a mobile node acquires its care-of address from some external services such as Dynamic Host Configuration Protocol (DHCP) [12, 27] and registers this temporary address with its home agent directly. These two procedures are used in different environments. In our discussion, a foreign agent is used to relay messages for the mobile node because such deployment has some advantages and necessities.

The most direct benefit for using foreign agents is to save the number of IP addresses [41], that is, several mobile nodes can share one IP address. With the fast growth in the number of the mobile nodes, for the limited IPv4 address space, this benefit is significant. In addition, foreign agents are good for not only smooth handoffs to reduce packet losses but also regionalized registration to decrease network traffic [37].

In the real world, when mobile nodes enter a foreign network, they have to use resources of the foreign network to continue their network connectivity. The foreign network needs some mechanisms to protect its security and resources [40]. In more detail, the foreign network needs firstly to verify the identity of mobile nodes, then to authorize only legal users to access its network resources, and finally to send bills to those legal mobile nodes to collect payments. Consequently, it is necessary to employ a foreign agent to complete this important work.

On the other hand, a foreign agent is capable to accomplish this task. With the help of the authentication extensions in the registration messages, i.e., *mobile-home*, *mobile-foreign* and *foreign-home*, the foreign agent can successfully authenticate a mobile node and make an authorization decision. Because of the default router assumption described in Section 2.4, i.e., all traffic to and from a mobile node must pass through the foreign agent, the foreign agent can monitor the usage of network resources by the mobile node and calculate a bill. From the security point of view, if the foreign agent finds something abnormal, for example, the extraordinary usage of network resources by the mobile node, the foreign agent can disallow the mobile node to access the foreign network. Although the foreign agent can examine network traffic exchanged with the mobile node, in our solution, it cannot read any security-sensitive data. Hence the mobile node can still keep the information secret. Next we explain this point in more detail.

2.6 Firewall Traversal Solution

Because IPsec [26] is implemented on the network layer and it is transparent to applications, we use IPsec to solve the problems. There are two modes in IPsec, transport mode and tunnel mode. In this section, we show how we apply these two modes to achieve firewall traversal as well as end-to-end security. Two security protocols are provided in IPsec, Authentication Header (AH) [24] and Encapsulating Security Payload (ESP) [25]. We choose ESP for encryption and authentication services.

When a mobile node is away from home, it firstly registers the new care-of address with its home agent and then resumes data exchanges with a correspondent node. We explain our approach in detail according to this procedure. In each step, we describe cooperation of the network entities, i.e., the mobile node, the foreign agent, the home agent, the firewall and the correspondent node. We also illustrate packets transmitted among these entities. The shaded portion in the packet formats indicates encrypted data. Before the detail description of our solution, for the convenience, the abbreviations shown in the figures of the packet formats are listed as follows:

- MN: the home address of the mobile node;
- COA: the foreign agent care-of address of the mobile node;
- FA: the IP address of the foreign agent;
- HA: the IP address of the home agent;
- FW: the IP address of the firewall;
- CN: the IP address of the correspondent node.

2.6.1 Registration Procedure

As explained in Section 1.1.2, Mobile IP itself provides security protection for the registration messages to prevent malicious users from disrupting normal communications between a mobile node and its home agent [41, 37]. Particularly, in the registration messages, *Identification* field is used for prevention of replay attack, and three authentication extensions are used for origin authentication and data integrity. Among the authentication extensions, the *mobile-home* authentication extension is required, and the other two, i.e., the *mobile-foreign* authentication extension and the *foreign-home* authentication extension, are optional. Thus the registration messages provide themselves authentication services. Encryption provides confidentiality services. Since there is no security-sensitive data in the registration messages, it is not necessary to encrypt them. Optionally, the mobile node may encrypt the registration messages with the key shared between itself and the foreign agent to keep the registration messages from being read by other hosts but its foreign agent.

However, the mobile node cannot be authenticated by the firewall, therefore the registration request messages cannot pass through the firewall. IPsec security mechanisms are needed for firewall traversal. If the mobile node establishes an IPsec tunnel with the firewall, the foreign agent cannot process the registration messages, which breaks the requirement defined in Mobile IP [41]. As a result, it is appropriate to establish an IPsec tunnel between the foreign agent and the firewall (Fig. 9). Specifically, on receipt of the registration request (Fig. 10(a)) from the mobile node, the foreign agent processes it to form a new packet (Fig. 10(b)) and then puts that into the IPsec tunnel (Fig. 10(c)). The firewall decrypts and authenticates the packet (Fig. 10(c)). If the authentication is successful, the firewall relays the registration request (Fig. 10(b)) to the home agent. For the reverse direction, the procedure is just opposite (Fig. 11).

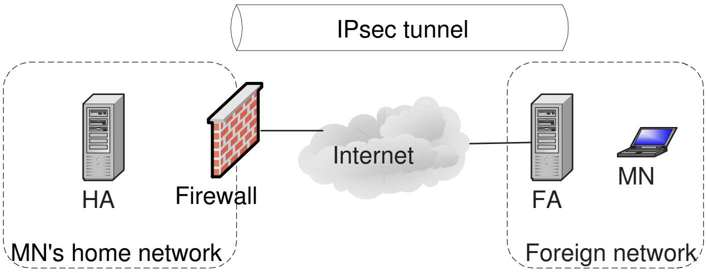


Figure 9: Establishment of an IPsec tunnel between the firewall and the foreign agent for registration.

2.6.2 Data Exchanges between the Mobile Node and the Correspondent Node

The mobile node can communicate with a correspondent node after registration. Although one IPsec tunnel has been already established between the foreign agent and the firewall during the registration period, it cannot achieve end-to-end security. Since transport mode protects upper-layer payload, we employ it to secure communication between the mobile

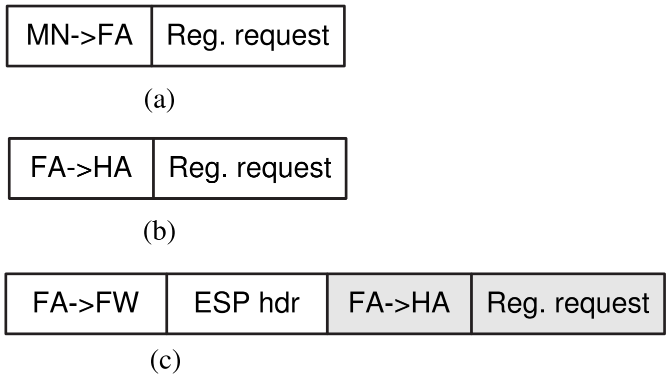


Figure 10: Pakcet formats for registration request: (a) request between the mobile node and foreign agent; (b) request processed by the foreign agent; (c) request between the foreign agent and the firewall.

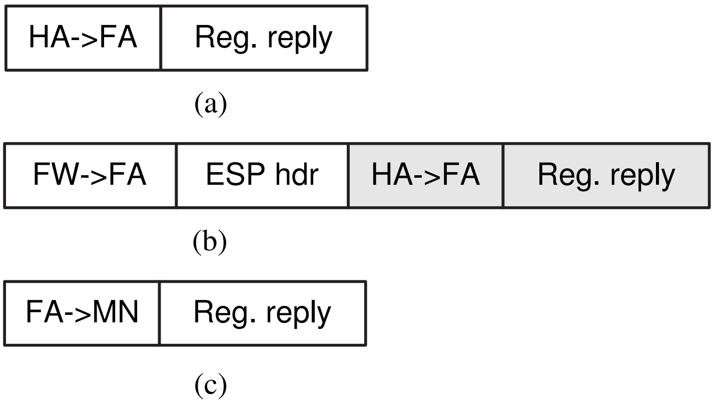


Figure 11: Packet formats for registration reply: (a) reply between the home agent and the firewall; (b) reply between the firewall and the foreign agent; (c) reply between the foreign agent and the mobile node.

node and the correspondent node. As our assumption written in Section 2.4, the mobile node and the correspondent node share security associations, so transport mode ESP can be used to encrypt data packets transferred between them. Briefly, in our solution, tunnel mode is applied between the firewall and the foreign agent for firewall traversal, and transport mode is used between the mobile node and the correspondent node for end-to-end security (Fig. 12).

For a packet sent from the correspondent node to the mobile node, it needs to traverse the forward tunnel as well as the IPsec tunnel (Figure 13). In more detail, when the correspondent node sends a packet to the mobile node, it encrypts the packet's payload

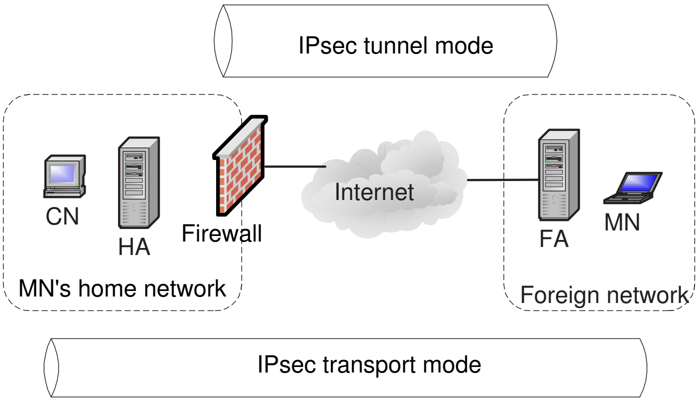


Figure 12: Security association establishment for Mobile IP data transfer.

according to the transport mode ESP (Fig. 14(a)). On the basis of Mobile IP [41, 37], the home agent intercepts the packet arriving for the mobile node. The packet is encapsulated with a new IP header and inserted to the Mobile IP forward tunnel (Fig. 14(b)). Because the packet's destination is outside the home network, the firewall puts it into the IPsec tunnel by encrypting the entire packet and then encapsulating it with another IP header (Fig. 14(c)). When the foreign agent receives the packet (Fig. 14(c)), firstly it strips off the outmost IP header, decrypts the remainder of the packet and gets the forward-tunneled packet (Fig. 14(b)). Then the foreign agent removes another IP header added by the home agent and recovers the original packet (Fig. 14(a)). The foreign agent cannot see any information contained in the packet's payload because it does not know the security association shared between the mobile node and the correspondent node. The original packet (Fig. 14(a)) is then forwarded to the mobile node.

As pointed out in Section 1.1, the mobile node can deliver data packets to the correspondent node directly or through a reverse tunnel [34].

We discuss the simpler case first, i.e., data delivery without a reverse tunnel. In this situation, only one tunnel, i.e., IPsec tunnel, is needed to pass through by a packet sent from the mobile node to the correspondent node, as shown in Figure 12. The entire transport-layer segment of a packet is encrypted by the mobile node (Fig. 15(a)). Because the packet needs to pass through the firewall, the foreign agent encrypts the packet and then encapsulates a new IP header whose destination address is the firewall (Fig. 15(b)). At the

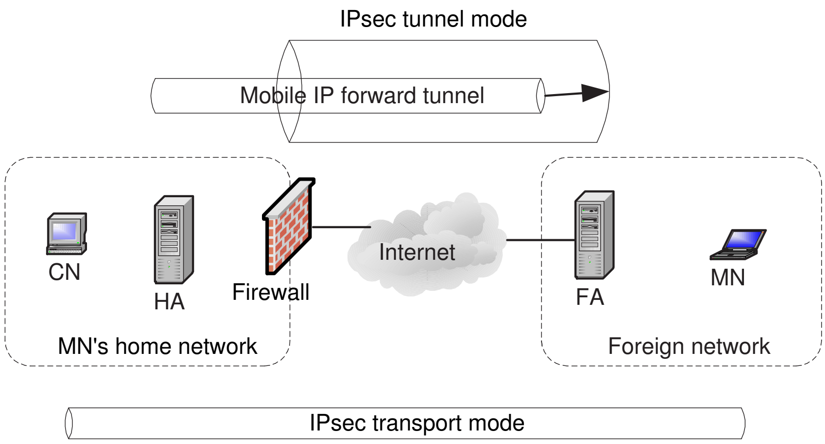


Figure 13: Packet delivery from a correspondent node to a mobile node.

CN->MN	ESP hdr	Upper Layer Payload

(a)

HA->COA	CN->MN	ESP hdr	Upper Layer Payload

(b)

FW->FA	ESP hdr	HA->COA	CN->MN	ESP hdr	Upper Layer Payload

(c)

Figure 14: Packet formats for data sent from a correspondent node to a mobile node: (a) packet sent by the correspondent node; (b) packet sent by the home agent; (c) packet sent by the firewall.

termination of the IPsec tunnel, the firewall processes the packet according to the security association shared with the foreign agent and recovers the inner packet (Fig. 15(a)). Then the inner packet (Fig. 15(a)) is received by the correspondent node.

MN->CN	ESP hdr	Upper Layer Payload

(a)

FA->FW	ESP hdr	MN->CN	ESP hdr	Upper Layer Payload

(b)

Figure 15: Packet formats for data sent from a mobile node to a correspondent node without a reverse tunnel: (a) packet sent by the mobile node; (b) packet sent by the foreign agent.

When the mobile node uses a reverse tunnel to transmit a data packet, the whole procedure is just opposite to that of packet delivery from the correspondent node to the mobile node (Figure 16). Particularly, the encrypted packet (Fig. 17(a)) enters the reverse tunnel and leaves for the home agent (Fig. 17(b)). The foreign agent secures the packet and tunnels it to the firewall (Fig. 17(c)). The firewall decapsulates the packet, reveals the reverse-tunneled packet (Fig. 17(b)) and then relays that to the home agent. After being removed another IP header used for reverse tunneling, the packet (Fig. 17(a)) is transferred to the correspondent node.

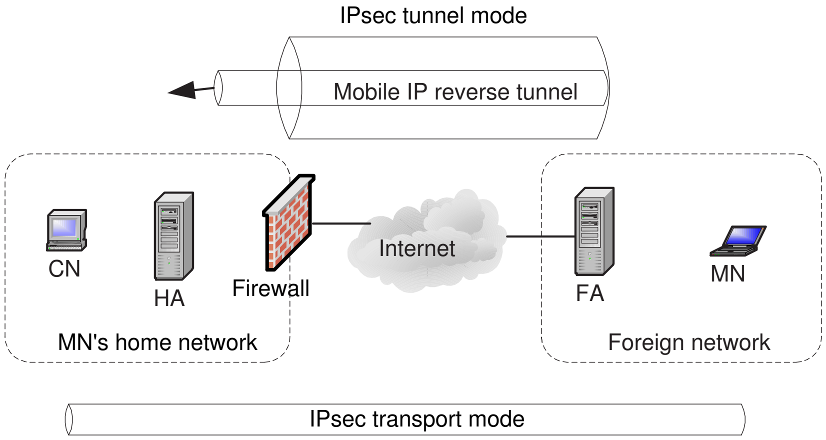


Figure 16: Packet delivery from a mobile node to a correspondent node with a reverse tunnel.

MN->CN	ESP hdr	Upper Layer Payload

(a)

COA->HA	MN->CN	ESP hdr	Upper Layer Payload

(b)

FA->FW	ESP hdr	COA->HA	MN->CN	ESP hdr	Upper Layer Payload

(c)

Figure 17: Packet formats for data sent from a mobile node to a correspondent node with a reverse tunnel: (a) packet sent by the mobile node; (b) packet sent from the care-of address; (c) packet sent by the foreign agent.

2.7 Firewall Traversal for Regional Registration

If a mobile node visits a foreign domain that is far from its home network, the registration delay may be long. To reduce the registration delay and the number of registration messages to the home network, regional registration [16] has been proposed. This situation is a special case in Mobile IP. In this section, first we introduce regional registration, then we discuss how to apply our solution explained in Section 2.6 to this special case.

2.7.1 Overview of Regional Registration

In regional registration, foreign agents are organized hierarchically in a foreign domain, as shown in Figure 18 [16]. One new network entities, *gateway foreign agent* (GFA), is introduced. A GFA is a foreign agent and its IP address is publicly routable. Typically the GFA is located at the top of the foreign agents' hierarchies. Two new registration messages, *regional registration request* and *regional registration reply*, are required when a mobile node changes its network attachment point within the same foreign domain. In the following, we briefly explain how a mobile node completes a home registration and a regional registration as well as data transfer.

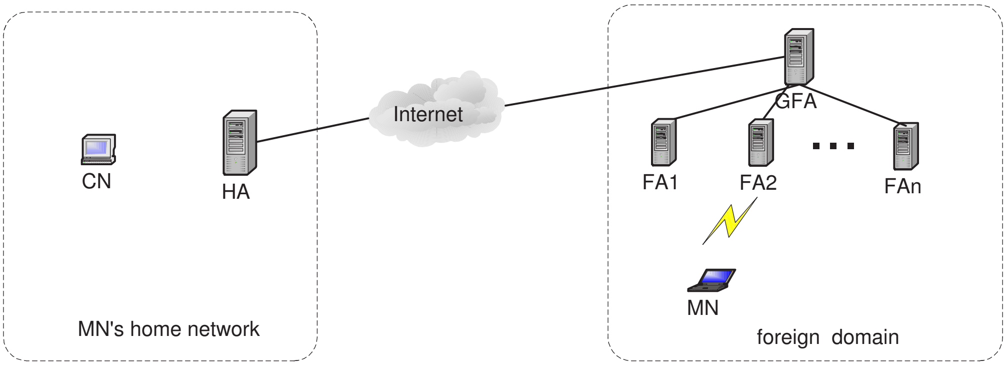


Figure 18: Hierarchical foreign agents in Mobile IP.

When a mobile node first enters a foreign domain, it is required to report its new care-of address to its home agent. From an agent advertisement message, the mobile node knows the GFA's address. It puts that address into *care-of address* field in a registration request message and then sends the request message to the closest foreign agent. The foreign agent processes the registration request message and forwards that to the GFA. The GFA records the address of the foreign agent that relays the request message. It is the GFA that relays the registration request message to the home agent. The home agent stores the GFA address as the mobile node's care-of address and sends a registration reply message to the GFA. When the GFA receives the registration reply message, it updates its visitor list and forwards the reply message to the foreign agent that relays the corresponding registration request message. Finally the reply message is delivered to the mobile node.

Because the GFA address is used as the mobile node's care-of address, it is not necessary to inform the home agent if the mobile node moves around several foreign networks that are supervised by the same GFA. Under this situation, the mobile node only needs to register locally. This is the reason that regional registration can reduce the number of signaling messages to the home network and reduce registration delay. In regional registration, security associations are shared between a mobile node and a GFA to provide authentication and integrity services.

When the mobile node changes foreign agents under the same GFA, it sends a regional registration request message. Upon receiving the regional registration request message, the foreign agent checks whether the mobile node is already in its visitor list. If the mobile node is a new visitor, the foreign agent passes the regional registration request to the GFA. The GFA stores the mobile node's new network attachment point and sends a regional registration reply message back. The regional registration reply message is delivered to the mobile node via the new foreign agent. The regional registration procedure is completed.

After a home registration or a regional registration, a mobile node may continue to communicate with other correspondent nodes. Packets sent from a correspondent node arrive at the GFA by passing through a forward tunnel. Then the packets are routed from the GFA to the mobile node via a foreign agent. Packets sent by the mobile node are transmitted to the GFA. Then the packets may be delivered to the correspondent node directly or through a reverse tunnel.

2.7.2 Firewall Traversal Solution for Regional Registration

The scenario that we discuss here is shown in Figure 19. The home network of a mobile node is protected by a firewall. The mobile node is visiting a foreign domain that supports regional registration. The mobile node faces the problems, i.e., how it can pass through the firewall and keep its packets securely. In the following we describe how our solution illustrated in Section 2.6 to be applied to the regional registration situation.

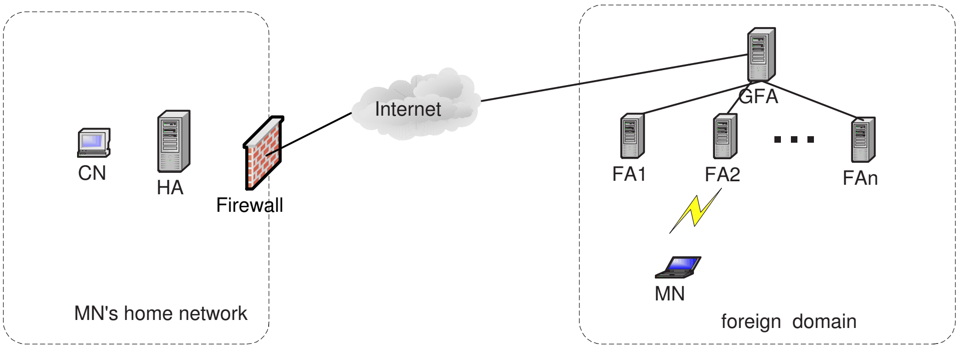


Figure 19: Regional registration scenario with a firewall protecting the home network.

Because all traffic exchanged between the mobile node's home network and the foreign domain must pass through the firewall and the GFA, we suggest that one IPsec tunnel be established between the firewall and the GFA. It is unnecessary to set up an IPsec tunnel between the firewall to each foreign agent. To achieve end-to-end security, the transport security associations are still required to be shared between the mobile node and the correspondent node. The solution is shown in Figure 20.

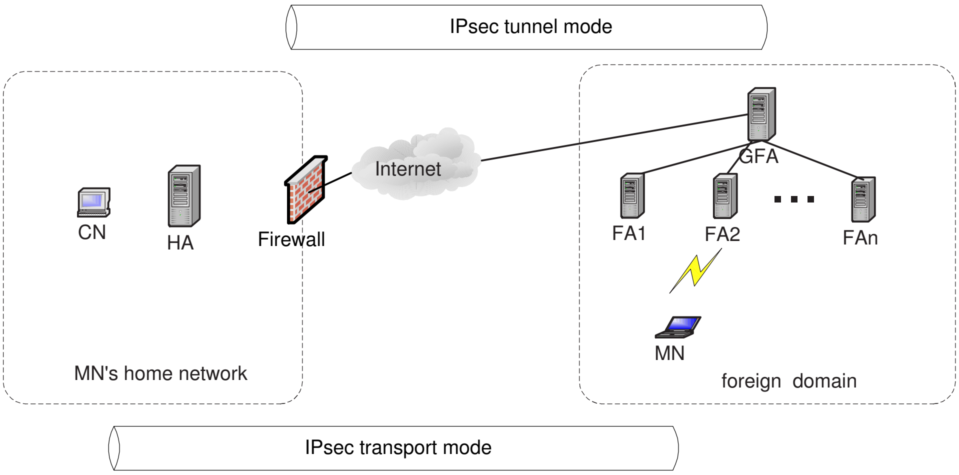


Figure 20: Firewall traversal solution for regional registration situation.

When the mobile node needs a home registration, a registration request message is sent by the mobile node and routed to the GFA. The GFA inserts the registration request to the IPsec tunnel. At the other end point of the tunnel, the firewall releases the request message and relays that to the home agent. The home agent stores the GFA's address as the mobile node's care-of address and sends a registration reply back. The reply message traverses the

IPsec tunnel and arrives at the GFA. Then the reply message is forwarded to the mobile node via the foreign agent to complete the home registration.

When the mobile node handoffs within the same foreign domain, regional registration messages are delivered among the mobile node, a foreign agent, and the GFA. Since no traffic is destined for the home network, the IPsec tunnel is not used for regional registration. In other words, the security associations shared between the firewall and the GFA are not affected by the mobile node's handoffs within the same foreign domain.

The mobile node may transmit data packets to other correspondent nodes after a home or regional registration. The solutions for each case are illustrated in Figure 21, 20 and 24, and the corresponding data packet formats are shown in Figure 22, 23 and 25. GFA is the abbreviation of the IP address of the gateway foreign agent. Other abbreviations are the same as those explained in Section 2.6. The shaded portion in the packet formats represents encrypted data.

Packets delivered from the correspondent node to the mobile node need to pass through the Mobile IP forward tunnel and the IPsec tunnel to arrive at the foreign domain (Figure 21). In more detail, the correspondent node uses the shared secret to encrypt the payload of a packet (Figure 22(a)). The packet is intercepted by the home agent and put into the forward tunnel that is established from the home agent to the mobile node's care-of address (Figure 22 (b)). Note that the mobile node's care-of address is the GFA's address, not a foreign agent's address. Then the packet is relayed to the firewall. Before being transmitted to the Internet, the packet is inserted to the IPsec tunnel (Figure 22(c)). It is the GFA that removes the packet from the IPsec tunnel (Figure 22(b)) and the forward tunnel (Figure 22(a)) sequentially. Finally the packet (Figure 22(a)) is routed to the mobile node through the foreign agent. Although there are many hosts along the way from the correspondent node to the mobile node, because of the transport security mechanisms, no host can know the information in the payload.

In the opposite direction, the mobile node uses the ESP transport mode security mechanisms to encrypt the payload of a packet (Figure 23 (a) and Figure 25(a)). The packet is transmitted to the GFA by a foreign agent. If a reverse tunnel is not used, the solution

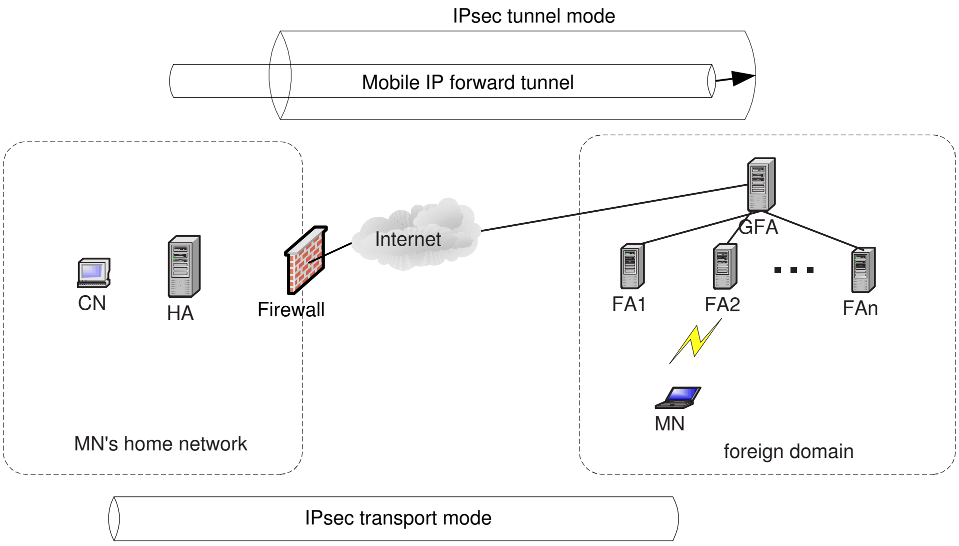


Figure 21: Packet delivery from a correspondent node to a mobile node in regional registration situation.

CN->MN	ESP hdr	Upper Layer Payload

(a)

HA->COA	CN->MN	ESP hdr	Upper Layer Payload

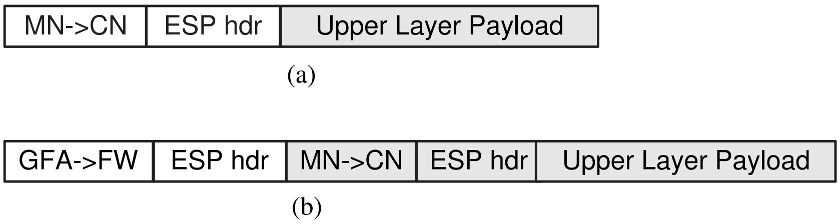
(b)

FW->GFA	ESP hdr	HA->COA	CN->MN	ESP hdr	Upper Layer Payload

(c)

Figure 22: Packet formats for data sent from a correspondent node to a mobile node in regional registration situation: (a) packet sent by the correspondent node; (b) packet sent by the home agent; (c) packet sent by the firewall.

scenario is quite simple, that is, it is the same as that shown in Figure 20. The packet enters the IPsec tunnel at the GFA (Figure 23(b)) and exits at the firewall (Figure 23(a)). The firewall directly transmits the packet to the correspondent node. However, the involvement of a reverse tunnel makes the solution scenario a bit complicated, as shown in Figure 24. Specifically, the packet is inserted into the reverse tunnel (Figure 25(b)) and then the IPsec tunnel (Figure 25(c)) by the GFA, instead of the foreign agent. The packet is released from the IPsec tunnel at the firewall (Figure 25(b)) and the reverse tunnel at the home agent (Figure 25(a)). In the end, the correspondent node receives the packet (Figure 25(a)) and decrypts it with the shared secret key.



(a)

(b)

Figure 23: Packet formats for data sent from a mobile node to a correspondent node without a reverse tunnel in regional registration situation: (a) packet sent by the mobile node; (b) packet sent by the GFA.

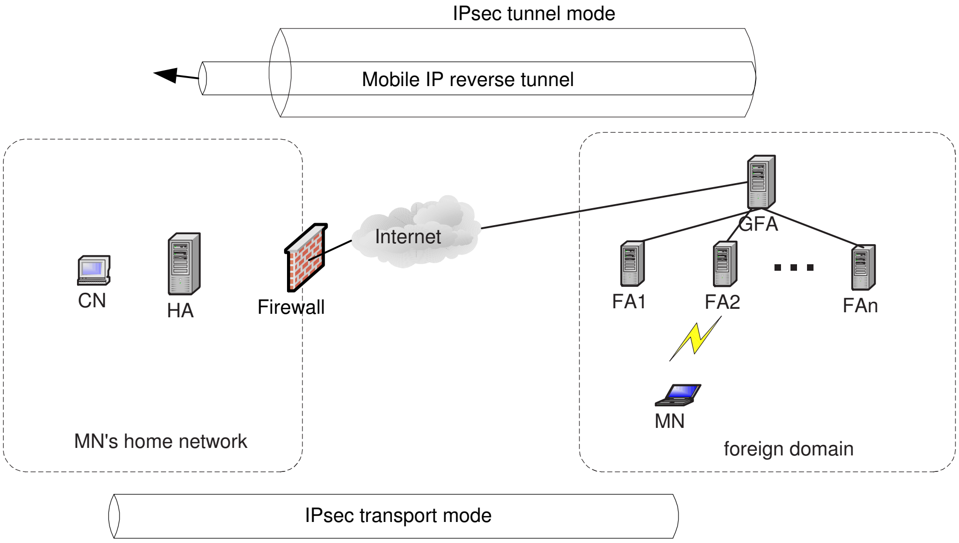


Figure 24: Packet delivery from a mobile node to a correspondent node with a reverse tunnel in regional registration situation.

Because the IPsec tunnel is set up between the firewall and the GFA, not between the firewall and each foreign agent, the IPsec tunnel does not need to be re-set up when the mobile node handoffs within the same foreign domain. Moreover, although the mobile node changes its network attachment point because of handoffs, its home address remains the same. The IPsec transport mode is set up between the correspondent node and the home address of the mobile node, that is, the mobile node's handoffs do not affect the IP destination addresses in the IPsec transport security association. It is known that an IPsec security association is uniquely identified by the triple (*SPI*, *IP destination address*, *security protocol identifier*) [23, 52]. In our solution, this triple is not changed no matter where the mobile node moves. In other words, the IPsec transport security associations

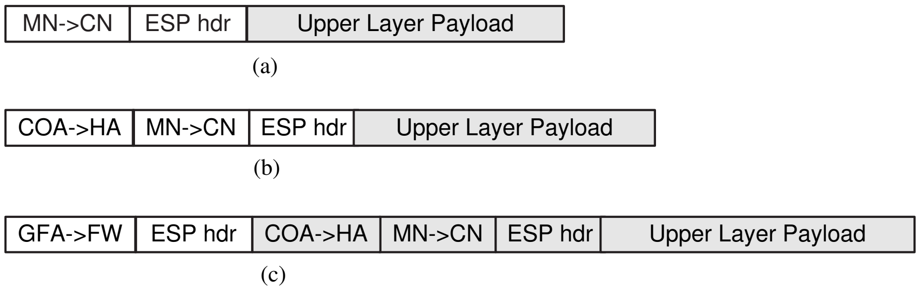


Figure 25: Packet formats for data sent from a mobile node to a correspondent node with a reverse tunnel in regional registration situation: (a) packet sent by the mobile node; (b) packet sent from the care-of address; (c) packet sent by the GFA.

shared between the correspondent node and the mobile node do not need to be refreshed for handoffs.

Briefly, when a mobile node is a new visitor to a foreign domain where foreign agents are deployed hierarchically, an IPsec tunnel is necessary to be set up between the firewall and the GFA. After that, no security association is required to be re-negotiated when the mobile node moves within the same foreign domain and communicates with a same correspondent node. Therefore, under this topology of foreign agents, the problem of security association re-negotiation caused by the mobile node's handoffs can be solved, and handoff performance is not degraded by security achievements.

2.8 Analysis

In this section we analyze our firewall traversal solution from four aspects, security, handoffs, packet overhead and scalability. We mainly discuss the solution explained in Section 2.6. Because regional registration is a special case in Mobile IP, the following analysis is also suitable to the solution described in Section 2.7.

2.8.1 Security

Our solution can fulfill the goal of Mobile IP security described by Zao *et al.* [58].

By means of an IPsec tunnel established between the firewall and the foreign agent, the mobile node can pass through the firewall successfully and move freely in the Internet without network connectivity loss. Additionally, Mobile IP itself achieves authentication services for registration messages, and transport mode operation implemented on the mobile node and the correspondent node provides confidentiality services and end-to-end security for data packets. That is, both registration and data transfer are secure.

For the home network, because of IPsec tunnel mode's characteristics and implementation on the firewall, our solution does not bring any new attacks to the home network when the mobile node is at abroad. For the foreign network, both the mobile node and the foreign agent are located outside the foreign network's firewall if the foreign network is also firewall-protected. Therefore the internal foreign network is not exposed to any new attacks caused by the visit of the mobile node. In a word, both the home and the foreign networks are safe from attacks when the mobile node is away from home. Moreover, the foreign agent can monitor IP header of the traffic to and from the mobile node and determine the mobile node's access according to some factors.

2.8.2 Handoffs

When a mobile node moves to another foreign network, the new foreign agent must build an IPsec tunnel with the firewall. Compared with mobile hosts on the wireless networks, the foreign agent and the firewall, which both usually are fixed hosts on the wired networks, have more power provision, faster computation speed, wider bandwidth and lower link error rate. As a result, they can establish an IPsec tunnel with much shorter time than mobile hosts. If an IPsec tunnel is established between the firewall and the mobile node's co-located care-of address, as mentioned in Section 2.3, due to the mobile node's capability, the re-negotiation of the security association lowers handoff performance noticeably [3].

On the other hand, as explained in Section 2.7, because the mobile node uses its home address, instead of its care-of address, in the transport security association, the security association does not need to be refreshed whenever the mobile node changes its network attachment point. In other words, the mobile node needs to do nothing about security implementation for handoffs except that already defined in Mobile IP [41]. Such characteristics can significantly save not only the mobile node's power consumption but also the handoff time.

For above two reasons, our solution performs well for a mobile node's handoffs.

2.8.3 Packet Overhead

Here we only discuss about packet overhead caused by employment of IPsec mechanisms. We do not consider the overhead brought by Mobile IP forward and reverse tunneling because these issues have already been written in [34, 41].

An ESP header specifies 4 bytes for *Security Parameters Index*, 4 bytes for *Sequence Number*, 8 bytes for *Initialization Vector*, 1 byte for *Pad Length* and 1 byte for *Next Header* [52]. In addition, we assume 7 bytes for *Padding* and 12 bytes for *Authentication Trailer* [56]. So there are 37 bytes for an ESP header.

For transport mode, an ESP header is inserted immediately after the original IP header of a data packet, it means that the overhead of 37 bytes is added. For tunnel mode, besides an ESP header, a data packet is encapsulated with a new IP header. The minimum size of a header in IPv4 is 20 bytes. Therefore the overhead for tunnel mode is an IP header plus an ESP header, i.e., 57 bytes. In our solution, because both IPsec transport mode and tunnel mode are applied, the total overhead added by IPsec mechanisms for a data packet is 94 bytes. Usually the Maximum Transmission Unit (MTU) is 1500 bytes in many networks. Under this condition, the overhead due to security implementation in our solution is 6.27%.

2.8.4 Scalability

Usually one home network may have a certain number of mobile nodes and these mobile nodes may visit different foreign networks at the same time. The firewall needs to set up IPsec tunnels to those foreign networks that the mobile nodes are visiting, one tunnel to one foreign agent. Correspondingly, one foreign network may have several mobile visitors simultaneously. The foreign agent requires establishing IPsec tunnels to the home networks that the visiting mobile nodes belong to, one tunnel to one home network. For example, in Figure 26, mobile nodes MN_{11}, MN_{12}, and MN_{13} are from *home network 1*, and mobile nodes MN_{21} and MN_{22} are from *home network 2*. Because both mobile nodes MN_{11} and MN_{22} are visiting *foreign network 2*, the *firewall 1* and *firewall 2* need to set up IPsec tunnels with *FA2* respectively. Both mobile nodes MN_{12} and MN_{13} are staying in *foreign* *network 3*, thus the *firewall 1* sets up one IPsec tunnel with *FA3*. Since there is only one mobile node, MN_{21}, inside *foreign network 1*, one IPsec tunnel is established between *firewall 2* and *FA1*. When all mobile nodes from the same home network leave the foreign network, the tunnel between these two networks can be removed.

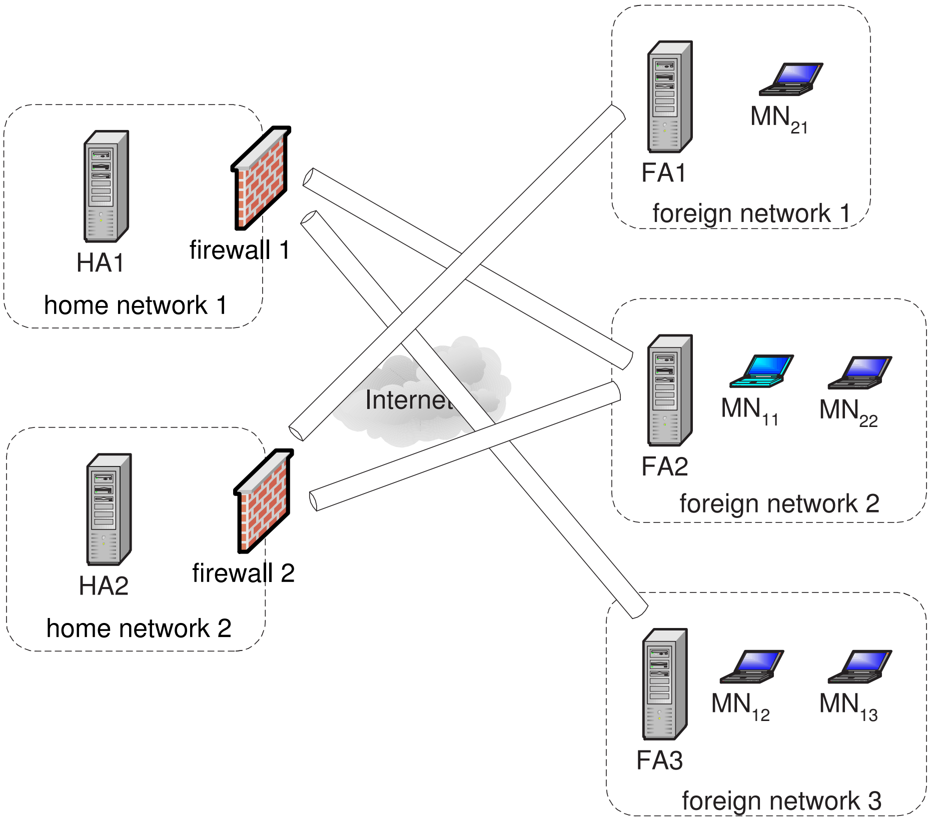


Figure 26: An example of scalability analysis for the firewall traversal solution.

A firewall and a foreign agent may use Internet Key Exchange (IKE) [17, 22] to create IPsec security associations. Each security association is independent, therefore, in theory, a firewall can establish as many IPsec tunnels with other hosts as it desires, so can a foreign agent. However, in practice, the capability of a foreign agent or a firewall, such as CPU speed, memory space, etc., restricts the number of IPsec tunnels that can be set up.

In section 2.4, we assume that a mobile node is pre-configured a security association with each correspondent node. However, if there are many correspondent nodes in the home network, in order to reduce such configuration burden on the mobile node, a special host may be set up in the home network. That is, before communicating with a correspondent node, the mobile node sends a request to the special host. Then the special host establishes a security association between the mobile node and the correspondent node. The home agent may also work as this special host. Certainly the mobile node and the correspondent node may use IKE to establish security associations as well.

In brief, our solution can work well in the scenario with a number of home networks, foreign networks and mobile nodes.

2.9 Conclusion

In this chapter we describe an approach so that in Mobile IPv4 a mobile node can securely access its firewall-protected home network as well as achieve end-to-end security with a correspondent node. A foreign agent is deployed in our scenario due to its advantages and necessities. IPsec security mechanisms are applied to accomplish the goal of Mobile IP security. In more detail, an IPsec tunnel is established between the firewall and the foreign agent for firewall traversal, and a transport security association is shared by the mobile node and the correspondent node for end-to-end security. In addition, this approach can also be applied to regional registration situation, that is, an IPsec tunnel is set up between the firewall and the gateway foreign agent for firewall traversal. In regional registration scenario, this solution can achieve that no security association needs to be refreshed if the mobile node moves within the same foreign domain. Our solution does not change any protocols and functions of network entities. Moreover, it is scalable. Therefore, our solution is useful in the real world.

CHAPTER III

SECURE FIREWALL TRAVERSAL IN THE MOBILE IP AAA SYSTEM

3.1 Overview of the Mobile IP AAA System

Mobile IP is only a mobility technology. It does not specify any information about authorization and usage when a mobile node roams in an administrative domain other than its home domain. When a mobile node moves from its home domain to a foreign administrative domain, it requires Internet services in order to continue its network connection. The service provider in that domain needs to authenticate the mobile node, to make an authorization decision and to maintain usage information. The services of Authentication, Authorization and Accounting (AAA) [2, 33] can meet these challenges. Therefore, the IETF Network Working Group suggests that Mobile IP work with the protocols of Authentication, Authorization and Accounting [13]. This approach can help Mobile IP to be applied commercially and broadly.

There are several AAA protocols. Among them, the RADIUS protocol [47] is the best-known [31]. However, because RADIUS is not suitable to large and complex networks, the DIAMETER protocol [10] is then designed to solve the problems appeared in RADIUS. Here, we only use general AAA concepts and services, and we do not discuss any specific AAA protocols.

In the Mobile IP AAA system, besides necessary mobility entities, two additional entities are involved. One is an AAA server in the home domain of a mobile node and is called a *home AAA server* (AAAH). The other is an AAA server in the foreign domain that the mobile node is visiting and is called a *foreign AAA server* (AAAF). In general, the home agent and the home AAA server of a mobile node are located inside the home domain, while at least one foreign AAA server and several foreign agents are placed within the foreign domain that the mobile node is visiting.

3.1.1 The Security Model

In order to achieve the services of authentication, authorization and accounting, security associations are necessary. We divide the security associations into two categories, *essential security associations* and *derived security associations*. The essential security associations must be pre-configured among the AAA servers and mobility entities while the derived security associations can be established with the help of the essential security associations and keys. Obviously, the essential security associations are important. Four essential security associations are required in the Mobile IP AAA system [40, 39, 13], as shown in Figure 27.

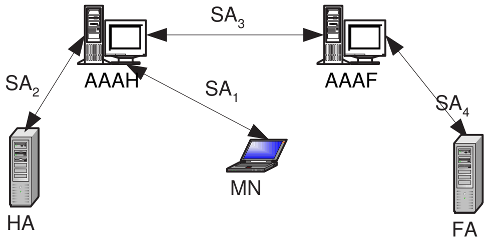


Figure 27: Trust model in the Mobile IP AAA system [40, 39].

The first security association, SA_1, is shared between a mobile node and its home AAA server. This significantly changes the security model of Mobile IP, which defines there is one pre-existing security association between the mobile node and its home agent [40]. The second security association, SA_2, is shared between the home AAA server and the home agent to reduce the burden of the mobile node, that is, the mobile node does not need to maintain an essential security association with its home agent. Although the home AAA server and the foreign AAA server are located in different administrative domains, they have to trust each other in order to rely on exchanged information. Therefore, one security association, SA_3, exists between them. Finally, because the foreign agent and the foreign AAA server belong to the same administrative domain, it is naturally to assume that they share a security association, SA_4. Based on these four essential security associations, mobility security associations between the mobile node and its home agent, and between the mobile node and the current foreign agent can be derived [42].

3.1.2 Registration Procedure

In the Mobile IP AAA system, when a mobile node just enters a foreign domain, it needs to send a registration request message to its home domain. After the registration, it can communicate with other correspondent nodes. Although the procedure of data routing in the Mobile IP AAA system is the same as that in Mobile IP, the procedure of registration is different.

There are two registration phases, initial registration and subsequent registration, in the Mobile IP AAA system. Compared with a subsequent registration, an initial registration is more important and time-consuming because it involves AAA servers and key distribution [40]. The message flow for the initial registration is shown in Figure 28 and Figure 29.

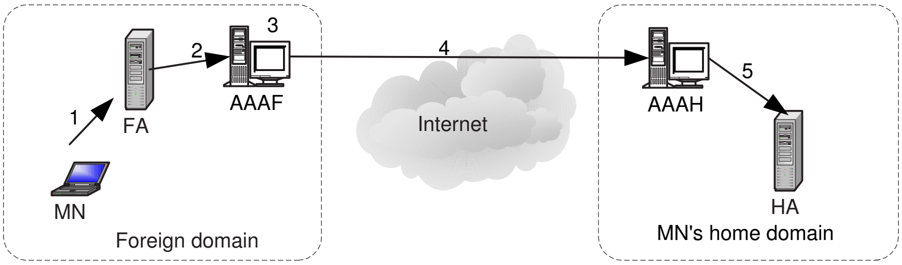


Figure 28: Initial registration request flow for the Mobile IP AAA system [39].

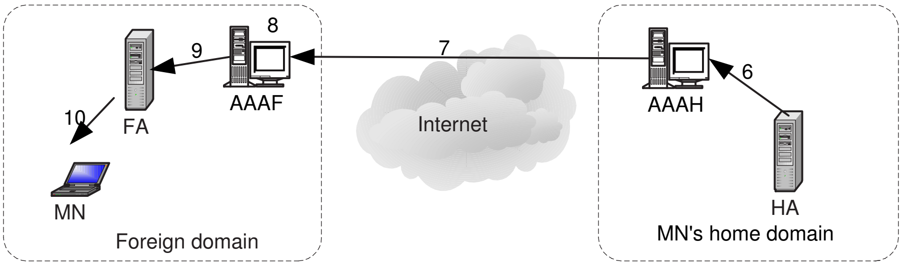


Figure 29: Initial registration reply flow for the Mobile IP AAA system [39].

In more detail, during an initial registration, a mobile node sends its credentials for authentication via a foreign agent. Because the foreign agent shares a security association, SA_4, with the foreign AAA server, it can consult the foreign AAA server securely for permission of resource allocation to the mobile node. If the foreign AAA server has enough information for verifying the mobile node, it notifies the foreign agent directly. Or else, the foreign AAA server has to deliver the mobile node's credentials to the home AAA server.

With the help of the essential security associations SA_1 and SA_3, the home AAA server can authenticate the foreign AAA server and the mobile node. If the authentication is successful, the home AAA server sends a registration reply back. Thus, the foreign AAA server authorizes the mobile node to use the network resources in the foreign domain. Meanwhile the home AAA server generates the following three keys:

- K_1: a key shared between the mobile node and the foreign agent;
- K_2: a key shared between the mobile node and the home agent;
- K_3: a key shared between the foreign agent and the home agent.

With the help of the essential security associations, the home AAA server can encrypt these keys and then securely deliver the keys K_1 and K_2 to the mobile node, the keys K_1 and K_3 to the foreign agent, and the keys K_2 and K_3 to the home agent. Only after the mobility entities get these keys, they can set up the derived security associations and proceed to subsequent registrations. A subsequent registration is a standard Mobile IP registration. Registration messages are transmitted only among the mobile node, the home agent and the foreign agent. Neither the home AAA server nor the foreign AAA server is involved during subsequent registration periods.

3.2 Challenges and Related Work

A firewall (FW) can be used to protect internal network resources, but it also brings challenges to the Mobile IP AAA system. Packets sent from untrusted external hosts are usually dropped by the firewall. Therefore, when a mobile node leaves its firewall-protected home domain and enters a foreign domain, the messages sent from the foreign domain cannot pass through the firewall that protects the home domain if they fail the authentication. In other words, the registration request messages cannot reach the home AAA server. Hence, the home AAA server neither knows that there are registration requests from the mobile node nor sends any replies and keys back. Due to no reply from the home AAA server, the foreign AAA server cannot allow the mobile node to access its network resources. Without the necessary keys generated by the home AAA server, the mobile node cannot establish the derived security associations with the home agent and the foreign agent to continue subsequent registrations. Additionally, from the home domain's point of view, because the home AAA server and the home agent do not receive any registration request messages from the mobile node, they cannot know the current location of the mobile node, that is, packets on the way to the mobile node cannot be tunnelled by the home agent to their correct destination. As a result, the objective of Mobile IP, seamless roaming, cannot be achieved due to the intervention of firewalls.

It is known that firewalls are used widely. As explained in Section 3.1, the combination of Mobile IP and AAA is inevitable. Therefore, it is important to solve the firewall traversal problems in the Mobile IP AAA system. In recent years, several solutions [9, 14, 36, 54, 55, 58] have been proposed to solve the firewall traversal problem in Mobile IP. IPsec mechanisms [26] are applied in these schemes. However, these proposals are only for Mobile IP without the involvement of AAA. Although the firewall problem in the Mobile IP AAA system is mentioned in [13] and [39], no detailed solution is given. Gustafson *et al.* give an approach to this problem, but they also point out that their solution is limited because both home AAA server and the home agent are globally reachable in their discussed layout [15].

In the following, we present our proposal to solve the firewall traversal problems in the Mobile IP AAA system. Our objective is that mobile users at abroad can securely have access to their home network resources and that meanwhile firewalls can also carry out their protection responsibilities. Our solution is intended to be practicable. Like [13] and [40], our approach does not involve any specific AAA protocols, such as DIAMETER [10] or RADIUS [47].

3.3 Network Architecture Model

The network architecture shown in Figure 30 is used for our discussion.

A firewall is deployed to protect the home administrative domain of a mobile node. The firewall can monitor all traffic to and from the home domain and only allow authorized traffic to pass [52].

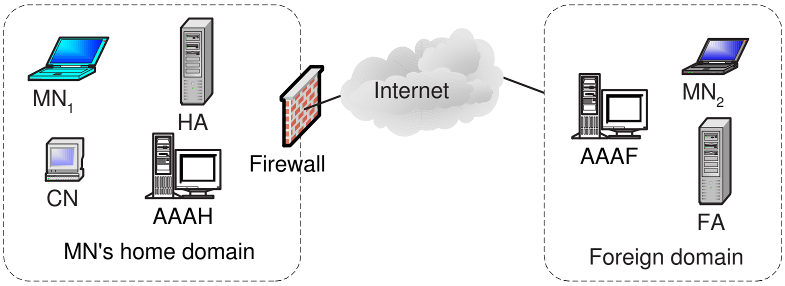


Figure 30: Network scenario for firewall traversal in the Mobile IP AAA system.

Both the home AAA server and the home agent of the mobile node are located inside the home domain. The home AAA server plays an important role in the Mobile IP AAA system. If the home AAA server is located outside the firewall, although it is simpler for the mobile node to send initial registration messages and receive keys, the home AAA server is exposed to various attacks from the Internet and installation of some security software is required for protection of the home AAA server. Normally the firewall can provide better protection than such security software. Hence, in our discussion, the home AAA server is located behind the firewall to reduce cost and avoid various attacks from the Internet. On the other hand, the security of the firewall is also crucial. It is known that firewalls only run as few programs as possible to prevent potential security holes [5]. Because the functions of the home AAA server are complicated, from the security point of view, we suggest that the home AAA server and the firewall run on separate physical machines. For the similar reasons, the home agent is also placed on an independent machine behind the firewall.

The mobile node can roam seamlessly in its home domain as well as in the foreign domain. In our discussion, the foreign administrative domain is not protected by a firewall, and one foreign AAA server is located inside. The mobile node obtains a care-of address from a foreign agent. The foreign agent is the default router of the mobile node, that is, all traffic to and from the mobile node must pass through the foreign agent.

In addition, brokers, which are centralized agents and used for scalability of security association establishment [40, 39], are omitted in Figure 30 because they do not affect our discussion.

3.4 The Security Model for Firewall Traversal

The key issue of the firewall traversal is that all traffic destined for the home administrative domain has to be authenticated by the firewall. In other words, the entities outside the firewall have to have some security relationships with the firewall so that messages sent from these entities can pass through the firewall. As explained in Section 3.1, these security relationships need to be based on the essential security associations and relevant keys. Therefore, in this section, we discuss whether any additional essential security associations and keys are necessary for the secure firewall traversal in the Mobile IP AAA system besides those that have already been described in Section 3.1. For simplicity and practicality, our objective is that the number of the additional essential security associations and keys is as few as possible. Moreover, we explain how the derived security associations can be set up between the firewall and the entities in the foreign domain.

3.4.1 The Essential Security Association between the Firewall and the Home AAA Server

During an initial registration, among the entities in the foreign domain, only the foreign AAA server sends a registration request message to the home domain. Before this request enters the home domain, the firewall intercepts it and needs to verify the identity of the foreign AAA server. In the Mobile IP AAA system, there is one essential security association, SA_3, shared between the home AAA server and the foreign AAA server, that is, the home AAA server trusts the foreign AAA server. The firewall should allow the messages sent from the foreign AAA server to enter the home domain so that the home AAA server and the foreign AAA server can communicate each other. Therefore, for the initial registration, we only need to discuss how to establish a security relationship between the firewall and the foreign AAA server.

Because of the essential security association SA_3, the home AAA server must have some information to authenticate the foreign AAA server, for example, the public key of the foreign AAA server. Thus the firewall can be pre-configured with such information and then use such information to verify the credentials of the foreign AAA server. In more detail, before the registration period, from the home AAA server, the firewall can obtain the public keys of the foreign AAA servers that the home AAA server trusts. With the help of the public keys, the firewall and the foreign AAA server can apply the IKE protocol [17, 22] to negotiate IPsec security associations and then establish an IPsec tunnel between each other, as shown in Figure 31. As a result, the messages sent from the foreign AAA server can pass through the firewall safely. Because the foreign AAA server is not involved during the subsequent registrations, the IPsec tunnel between the firewall and the foreign AAA server may be removed after the initial registration.

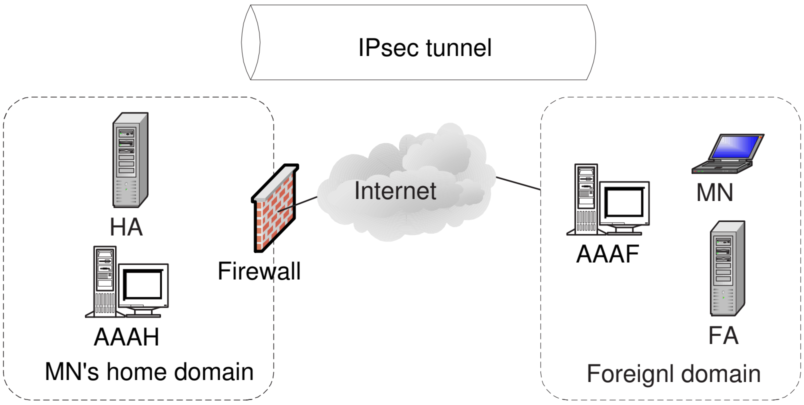


Figure 31: Establishment of an IPsec tunnel between the firewall and the foreign AAA server during an initial registration.

From above explanation, it is not necessary to have an essential security association shared between the firewall and the foreign AAA server. However, the reason that the firewall does not doubt the information obtained from the home AAA server is that the firewall trusts the home AAA server, which means that there must be one essential security association shared between the firewall and the home AAA server. We call this security association SA_5, as shown in Figure 32. Because the firewall and the home AAA server belong to the same administrative domain, the security association SA_5 can be implemented easily.

3.4.2 The Secret Key Shared between the Firewall and the Foreign Agent

After the initial registration, the mobility entities follow the Mobile IP protocol for the subsequent registrations. During the subsequent registrations, it is the foreign agent that

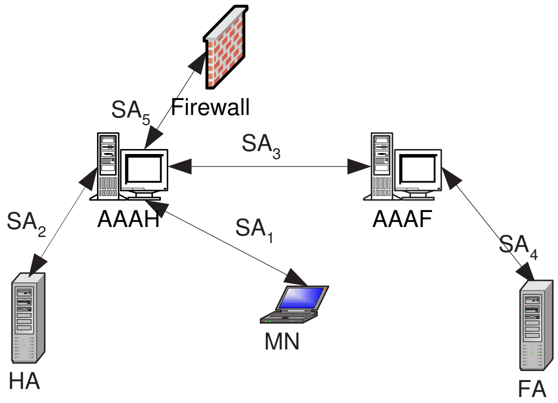


Figure 32: The security model for firewall traversal in the Mobile IP AAA system.

delivers messages originally submitted by the mobile node to the firewall. We can apply the approach proposed by Tang and Copeland [54] to accomplish our goal, that is, an IPsec tunnel is established between the firewall and the foreign agent for the firewall traversal, as shown in Figure 33.

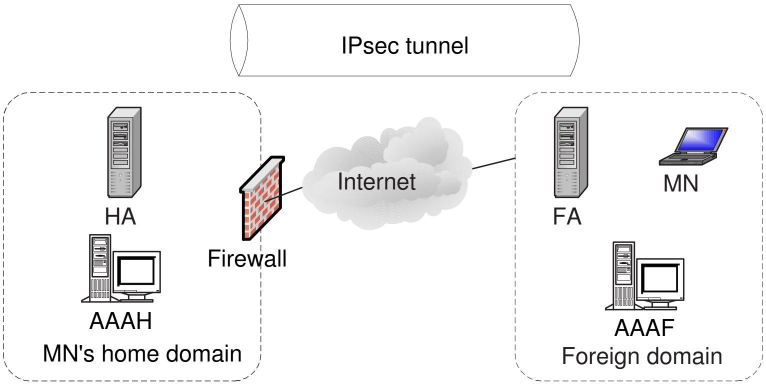


Figure 33: Establishment of an IPsec tunnel between the firewall and the foreign agent during a subsequent registration.

In order to establish an IPsec tunnel between the firewall and the foreign agent, one shared security relationship is required between them. However Tang and Copeland [54] do not mention how this shared security relationship is established. Here we propose that the home AAA server help the firewall and the foreign agent to share one security relationship. Specifically, during the initial registration, the home AAA server generates one additional key, K_4, and then distributes this key to the firewall and the foreign agent respectively. With the key K_4, the firewall and the foreign agent can use the IKE protocol [17, 22] to set up IPsec security associations.

Nevertheless, the key K_4 must be distributed securely to prevent from being seen by others, so the home AAA server has to encrypt this key before delivery. Because, as explained above, one essential security association, SA_5, is shared between the home AAA server and the firewall, the home AAA server can encrypt the key K_4 with the security association SA_5 and transmit that to the firewall. At the same time, the home AAA server can send this shared key along with the keys K_1 and K_3 to the foreign agent. A detailed description about the key distribution is given in Section 3.5.

3.4.3 Summary of the Security Model

Briefly, in order to solve the firewall traversal problems in the Mobile IP AAA system, we propose that one additional essential security association, SA_5, shared between the firewall and the home AAA server should be required. Therefore, as shown in Figure 32, there is a total of five essential security associations. During an initial registration, with the help of SA_5 and other essential security associations, one security association shared between the firewall and the foreign AAA server can be derived and thus one IPsec tunnel can be established between them. Furthermore, one additional key is necessary to be generated and distributed so that another IPsec tunnel can be set up between the firewall and the foreign agent during subsequent registrations. As a result, registration messages can securely pass through the firewall, and the mobile node can complete its registration.

3.5 Key Generation and Distribution

According to the security model described in Section 3.4, necessary keys for registration as well as for firewall traversal can be generated and distributed securely by the home AAA server. Figure 34 shows the key distribution based on our security model.

Before an initial registration, the home AAA server can transmit the public key of the foreign AAA server, denoted by P in Figure 34, to the firewall. Since the public key can be known to everyone, encryption of a public key is not necessary. The home AAA server may use the essential security association SA_5 to keep the integrity of the public key P, represented by $SA_5(P)$ in Figure 34. The delivery of the public key P from the home AAA

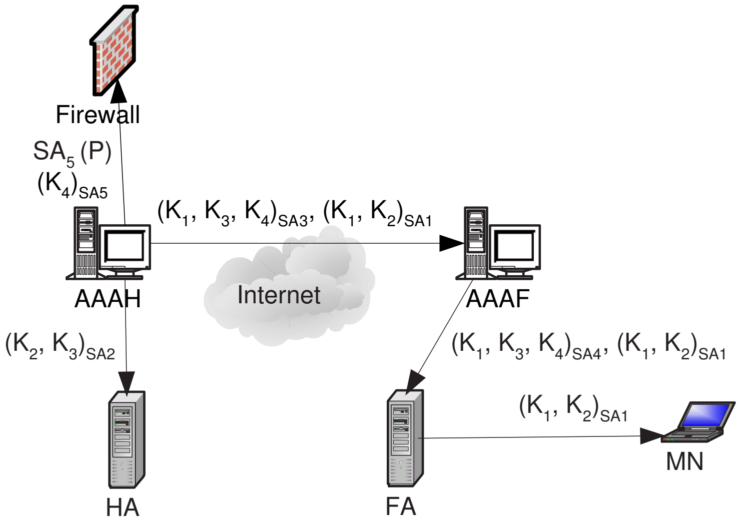


Figure 34: Key distribution for firewall traversal in the Mobile IP AAA system.

server to the firewall does not take any registration time because this transmission can be completed before the registration.

It is during the initial registration that the secret keys, i.e., K_1, K_2, K_3 and K_4, are generated and distributed by the home AAA server. Because encryption is required for secure delivery of secret keys, the home AAA server needs to encrypt these four secret keys with the appropriate essential security associations. In Figure 34, $(K)_{SA}$ means that the secret key K is encrypted with the security association SA. For the keys respectively destined for the home agent and the mobile node, the distribution procedure is the same as that described in [39], so it is not reiterated here. We mainly focus on the distribution procedure of the new secret key K_4.

The home AAA server encrypts the key K_4 with the essential security association SA_5 and sends that to the firewall. In the meantime, the home AAA server appends the key K_4 to the keys K_1 and K_3. Then it encrypts these three keys with the essential security association SA_3 and delivers that to the foreign AAA server. After being decrypted by the foreign AAA server, these three keys are encoded with the essential security association SA_4 and transmitted to the foreign agent. With the help of the key K_4, the foreign agent and the firewall can establish an IPsec tunnel. Because the key K_4 is delivered along with other keys, the distribution of the key K_4 does not cost any extra time.

In short, from the distribution procedure of the public key P and the secret key K_4, we can assert that our solution to the firewall traversal does not increase any extra delay for a registration period. In other words, in our approach, it still takes only one Internet round trip to complete an initial registration.

3.6 Control Message Flow

In this section we describe how the control messages flow among the AAA servers, the mobility entities and the firewall to achieve the firewall traversal as well as registration. Once a mobile node enters a foreign administrative domain, it needs to submit a registration request to the home AAA server so that necessary keys can be distributed to the relevant entities during an initial registration period. After that, the mobile node, the home agent and the foreign agent follow the standard Mobile IP protocol to complete subsequent registrations. In the following, we give the detail description about the control message flow according to this order.

3.6.1 Control Message Flow in an Initial Registration

Figure 35 shows the control message flow in an initial registration.

The mobile node sends a Mobile IP registration request along with the AAA key request to the foreign agent. After being processed by the foreign agent, the request is forwarded to the foreign AAA server. If the foreign AAA server has one shared essential security association with the home AAA server, the firewall must have been pre-configured with the public key of the foreign AAA server before the initial registration. Therefore, the foreign AAA server and the firewall can negotiate to set up an IPsec tunnel. Then the registration request is inserted into the IPsec tunnel by the foreign AAA server. Upon receipt of the registration request, the firewall decrypts and verifies it. If the authentication is successful, the registration request can enter the firewall and arrive at the home AAA server.

Once the home AAA server receives the registration request, it authenticates the mobile node's identity. If the home AAA server thinks that the mobile node's credentials are valid, it generates four secret keys, K_1, K_2, K_3, and K_4. The home AAA server encrypts the key K_4 with the security association SA_5 and sends that to the firewall. In the meantime, the

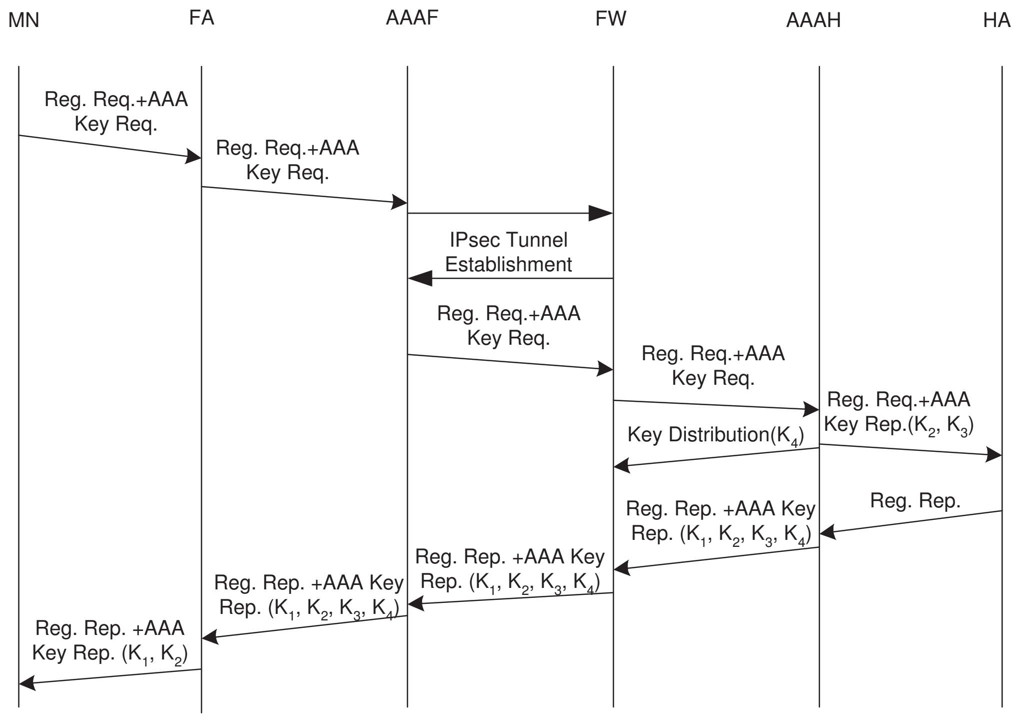

MN
FA
AAAF
FW
AAAH
HA
Reg. Req.+AAA Key Req.
Reg. Req.+AAA Key Req.
IPsec Tunnel Establishment
Reg. Req.+AAA Key Req.
Reg. Req.+AAA Key Req.
Reg. Req.+AAA Key Rep.(K2, K3)
Key Distribution(K4)
Reg. Rep.
Reg. Rep. +AAA Key Rep. (K1, K2, K3, K4)
Reg. Rep. +AAA Key Rep. (K1, K2, K3, K4)
Reg. Rep. +AAA Key Rep. (K1, K2, K3, K4)
Reg. Rep. +AAA Key Rep. (K1, K2)

Figure 35: Control message flow in an initial registration.

home AAA server delivers the registration request and the encrypted keys K_2 and K_3 to the home agent. After receiving the registration reply from the home agent, the home AAA server encodes the four keys with the appropriate essential security associations and sends out that along with the registration reply. The reply message goes through the IPsec tunnel from the firewall to the foreign AAA server. The foreign AAA server decrypts the keys K_1, K_3 and K_4 with the essential security association SA_3, re-encrypts them with the essential security association SA_4, and then sends that to the foreign agent. However, the foreign AAA server cannot know the key K_2 because the key K_2 is encrypted with the security association SA_1 shared by the home AAA server and the mobile node. The foreign agent uses the essential security association SA_4 to decrypt the keys K_1, K_3 and K_4. Meanwhile, the foreign agent relays the registration reply along with the encrypted keys K_1 and K_2 to the mobile node. Consequently the four keys are securely distributed.

3.6.2 Control Message Flow in a Subsequent Registration

After the keys are received by the relevant mobility entities during an initial registration, a subsequent registration just follows standard Mobile IP protocol. A subsequent registration does not involve any AAA servers. Figure 36 shows how the mobility entities and the firewall cooperate together to achieve the firewall traversal in a subsequent registration.

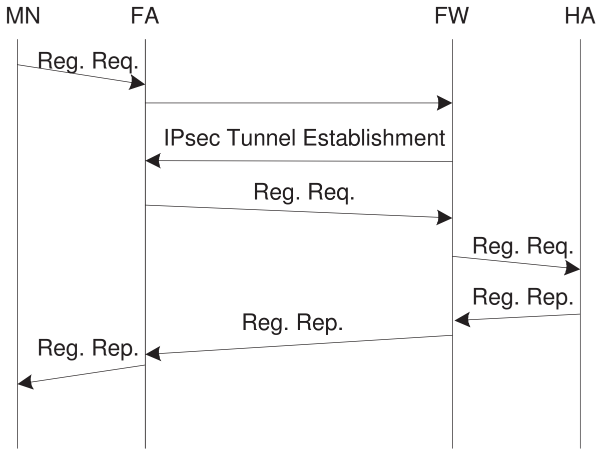


Figure 36: Control message flow in a subsequent registration.

Upon receipt of a registration request from the mobile node, the foreign agent can establish an IPsec tunnel with the firewall by using the shared key K_4. The registration request message passes through the IPsec tunnel and arrives at the firewall. The firewall verifies the registration request message with the help of the IPsec mechanisms and relays that to the home agent.

After processing the registration request, the home agent sends out a registration reply. Because the destination of the reply message is outside the home domain, the reply message enters the IPsec tunnel at the firewall and exits the tunnel at the foreign agent. The foreign agent needs to decapsulate and decrypt the reply message with the IPsec mechanisms. In the end, the mobile node receives the registration reply from the foreign agent.

After registration, the mobile node follows the Mobile IP protocol to communicate with other correspondent nodes. The mobile node may use the solution proposed by Tang and Copeland [54] to establish an IPsec transport security association with a correspondent node and to achieve secure communication.

3.7 Conclusion

In this chapter, we use the essential security associations and the relevant keys to solve the firewall traversal problem in the Mobile IP AAA system.

In our approach, one new essential security association, SA_5, shared by the firewall and the home AAA server is required. With the help of the security association SA_5 and other essential security associations, the firewall and the foreign AAA server can establish an IPsec tunnel so that messages sent from the foreign domain during an initial registration can pass through the firewall securely.

In addition, one new key, K_4, is necessary to be generated by the home AAA server during an initial registration. The key K_4 is encrypted with the appropriate security associations and delivered to the firewall and the foreign agent respectively. After getting this shared key K_4, the firewall and the foreign agent can set up an IPsec tunnel during the subsequent registrations. Thus, the mobile node can traverse the firewall and have access to its home domain.

Because the firewall and the home AAA server belong to the same administrative domain, the security association SA_5 can be configured and maintained easily. The generation and distribution of the key K_4 do not cost any extra time in the registration period. Moreover, because of IPsec mechanisms, the firewall still performs its tasks of home domain protection. That is, our solution does not bring any additional security holes. Therefore our solution to the firewall traversal problem in the Mobile IP AAA system is practicable and secure.

CHAPTER IV

MOBILE IP USE OF PRIVATE ADDRESSES IN AN RSIP HOME NETWORK

4.1 Introduction to Use of Private Addresses

Because the number of hosts in the Internet has grown fast, the IP address space will be exhausted and Internet Service Providers will be burdened with the amount of routing overhead [46]. On the other hand, many large organizations, for example, banks, most of time only exchange information within their internal networks. Therefore address allocation for private networks [46] has been proposed. While the use of private address space brings some advantages, such as conservation of the public IP address space and flexibility in network design for organizations, it also brings some problems to hosts that only have private addresses to get access to the Internet [46]. Specifically, because a private address is not globally unique and not valid outside a private network, a host with a private address cannot get access to public networks directly. Furthermore, routers in public networks usually reject packets that use private addresses [46], so a packet with private addresses cannot be delivered to a correct destination in public networks.

Network Address Translators (NAT) [51] are usually installed to map private addresses to public addresses so that hosts in a private network can get access to the external network transparently. There are two variations in traditional NAT, Basic Network Address Translation and Network Address Port Translation (NAPT) [51]. The function of basic NAT is translation of IP addresses, and the function of NAPT is translation of IP addresses as well as port numbers.

The advantage of NAT is that the address translation is transparent to hosts. However, since a NAT router always examines and changes the header information in the network layer, and possibly the transport layer, end-to-end packet integrity cannot be accomplished

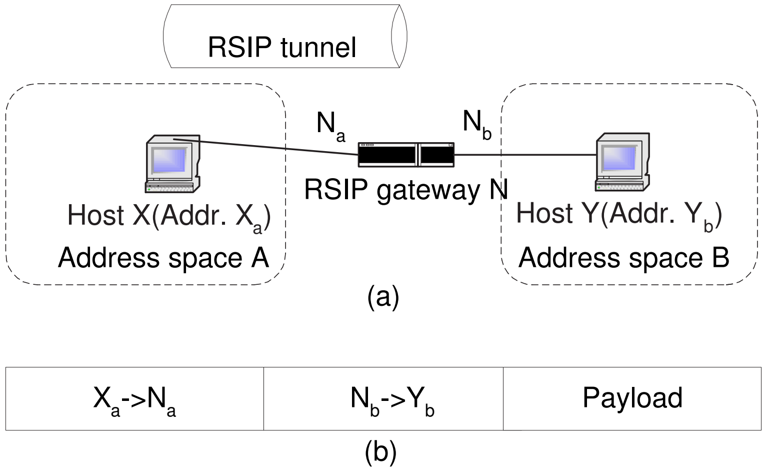
[51, 8]. Consequently, applications traversing a NAT router cannot be offered an end-to-end security. But if a NAT router is an end-point of an IPsec tunnel, it can provide security to packets transferring in the external realm [50].

Realm Specific IP (RSIP) [8] is viewed as an alternative to NAT. But it can maintain end-to-end packet integrity. We briefly explain RSIP in the next section.

4.2 Overview of Realm Specific IP (RSIP)

RSIP [8] is designed to be an application layer protocol [7]. It provides services that allow hosts in two different addressing realms to communicate each other [8]. For example, an RSIP gateway can help hosts in a private IPv4 network to exchange messages with a public network. Therefore, to some extent, RSIP is a way to lighten the address shortage burden on IPv4 networks. Furthermore, the deployment of RSIP is not limited to only IPv4 networks. RSIP can provide connectivity services between two different addressing realms, such as an IPv6 network and an IPv4 network, or a non-IP network and an IP network [8].

It is known that end-to-end integrity becomes more and more important nowadays. RSIP makes use of the tunnel concept to provide end-to-end integrity. In more detail, as shown in Figure 37(a), one RSIP gateway N is located between two address spaces A and B [8, 7, 35]. Thus the gateway N has two network interfaces, N_a for space A and a pool of addresses for space B. The hosts X and Y belong to spaces A and B respectively. An RSIP tunnel exists between the host X and the gateway N. When the host X wants to establish an end-to-end connection to the host Y, firstly it needs to request resources from the gateway N and obtains address assignment, for example, the address N_b. Then the gateway N binds the host X's information with the assigned address N_b so that it can correctly forward inbound traffic from Y to X. After that, the host X tunnels a packet, as shown in Figure 37(b), to the gateway N. When receiving the packet, the gateway N, which is the end point of the tunnel, removes the outer header and then delivers the decapsulated packet to the host Y. In the reverse direction, upon receipt of a packet from the host Y, according to the binding information, the gateway N encapsulates the packet with an outer header by using the address N_a as the source and the address X_a as the destination. The gateway N then submits the encapsulated packet to the host X. A network consisting of RSIP hosts inside and at least one RSIP gateway on the boundary is called an *RSIP network*.



X_a->N_a	N_b->Y_b	Payload

Figure 37: (a) RSIP architecture; (b) the format of a packet sent from the host X to the host Y through the RSIP gateway N [8, 7, 35].

4.3 Problems for Use of Private Addresses in Mobile IP

Due to a shortage of IP addresses and burden of routing overhead [46], currently many organizations apply private addresses in their internal networks. Nevertheless, the use of private addresses brings additional challenges to Mobile IP.

In Mobile IP, if the home network of a mobile node is a private network, the mobile node only has a private home address. When it stays in the home network and wants to get access to a public network, the mobile node only needs to request a public address from either a NAT router or an RSIP gateway that is located at the border of its home network. However, as we have explained in Section 4.1, because a private address is not unique in a public network, it can only be used within a private network. In other words, when a mobile node goes abroad, it is not allowed to use its private home address in a public network. Therefore, it is necessary for a mobile node to get a public home address when it is visiting a foreign network. According to Mobile IP [41], the mobile node cannot contact its home NAT router or RSIP gateway to get a public home address before it finishes the registration.

Where a mobile node can get a public home address is a problem.

Because a private address cannot uniquely represent a host in a public network, a mobile node needs some credentials to uniquely identify itself in a public network before it gets a public home address. Which credentials can be used is another problem.

If a mobile node uses a foreign agent to register with its home agent, because both the mobile node and the foreign agent are in the public network, neither of them should use the mobile node's private address in the IP header of registration messages. But the mobile node does not have a public home address by that time. Without a proper IP address to fill in the registration messages, the mobile node cannot complete the registration phase. In-complete registration leads to loss of contact with its home agent.

Additionally, during the data routing phase, a mobile node uses the private addresses to communicate with a correspondent node that is located inside the mobile node's home network. If such a packet is tunneled from the home agent to the foreign agent, the foreign agent would most likely be confused by the private addresses in the packet's IP header and then drop the packet after it decapsulates the packet from the Mobile IP forward tunnel.

Therefore, when a mobile node from a private home network visits a public network, it faces several problems of registration and data delivery.

4.4 Related Work

Several solutions have been proposed to solve the problems of a mobile node with a private address. From the mobile node's point of view, it may be assigned a private address by its home network, a foreign network, or both.

When a mobile node visits a foreign network that uses private address spaces, data traffic does not have any information of TCP/UDP port numbers that can be used to uniquely translate a public address into a private care-of address [28]. Levkowetz and Vaarala [28] apply MIP UDP tunneling so that a mobile node behind a NAT router in a foreign network can communicate with public networks. Specifically, a Mobile IP UDP tunnel is established during the registration period, and then data traffic goes through this tunnel from the home agent to the mobile node.

Since we mainly discuss the case that a mobile node has a private home address, we focus on the relevant approaches to this issue in the following.

As explained in Section 4.3, a mobile node needs some credentials to uniquely represent itself in a public network. Private IP Encapsulation (PIPE) is a method that a packet with private addresses in the IP header may be encapsulated within another IP packet [43]. The author argues that VPN-ID is unique globally and is used to identify a private network. In Malinen's solution, the combination of a mobile node's private home address and its home agent's address is employed as the mobile node's identification in public networks [30]. But both Petri [43] and Malinen [30] do not describe how the mobile node registers with its home agent.

If a mobile node uses a co-located care-of address, because the co-located care-of address is public, Gupta and Montenegro [14] suggest that the mobile node use this co-located care-of address to contact its home agent and to complete the registration. During communication with a correspondent node, if the mobile node uses a reverse tunnel, it can encapsulate its private home address with the public co-located care-of address so that a packet can be routed to the correspondent node. Only the home agent and the correspondent node inside the home network can see the private home addresses after the IP header containing the co-located care-of address is stripped off.

On the other hand, some solutions, such as [18, 21, 29], deploy a foreign agent in their scenarios. Although these proposals specify detail procedures for both registration and data delivery, there are several drawbacks. First of all, the use of private addresses in public networks violates the policy described in [46], though authors argue that the foreign agent can use MAC addresses to identify mobile nodes if private address collision happens. Secondly, the action of the foreign agent is changed. In Mobile IP, the foreign agent should play a passive role [41]. However, in [18, 21, 29], the foreign agent is active to request the home agent to assign a public address to a mobile node without notifying the mobile node. This action has some security problems. Because there is no required authentication for this request message, a hacker can easily pretend to be the foreign agent. Even worse, a hacker can use up the resources of public addresses in the home network. Thirdly, it is not secure that the home agent assigns a public address to a mobile node upon receipt of a request from a correspondent node. Since usually there is no security association between the home agent and a correspondent node, the resources of public addresses owned by the home agent can be exhausted by a hacker without any difficulty. Finally, the request of a public address for a mobile node during the data transfer period increases delay between two end users.

4.5 Network Scenario and Assumptions

The network scenario for our discussion is shown in Figure 38.

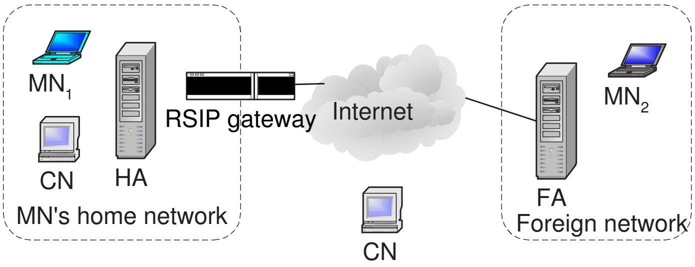


Figure 38: Network scenario for Mobile IP use of private addresses in an RSIP home network.

Unlike the scenario described in [28], we assume that the home network, not the foreign network, of a mobile node uses a private IP address space, that is, each host within the home network is assigned a private IP address. Furthermore, different from the network architecture explained in [18, 21, 29], one RSIP gateway, not a NAT router, is located at the border of the home network. The RSIP gateway has two network interfaces, one private address for the home network and a pool of public addresses for the external network. As far as we know, the research on the integration of RSIP and Mobile IP is under discussion [8], but there is no published paper on this research area as yet.

A home agent runs separately from the RSIP gateway. When a mobile node leaves its home, it needs to contact its home agent frequently from the public network. Hence, the home agent is required to communicate with the public network from time to time. It is inconvenient for the home agent to acquire a public address from the RSIP gateway whenever it needs to set up a new connection with the public network. On the other hand, since only a few home agents are located in the home network, it does not take many public addresses even if each home agent is assigned a public address. Therefore we assume that each home agent has a static public address in addition to a private address. We also allow the home agent to lease more than one public address from the RSIP gateway, which is permitted by the RSIP protocol [8].

A mobile node can move seamlessly in its home network as well as in a foreign network. The mobile node only has one private home address. It is pre-configured with both public and private addresses of its home agent. If the mobile node stays at home, it uses the home agent's private address as the destination for sending packets to its home agent. Otherwise, it uses the home agent's public address as the destination.

A correspondent node outside the home network has a public address. Nevertheless a correspondent node within the home network only has a private address. When both a correspondent node and a mobile node belong to the same home network, only private addresses are used for information exchange.

The foreign network in our discussion uses public address space, and the mobile node obtains a care-of address from the foreign agent, which is different from the network scenario illustrated in [14] and [28].

4.6 Design Principles and Objective

To be practical, our approach has to follow some basic principles.

Because a private address is not globally unique in the public network, use of private addresses in the public address space is ambiguous. As a result, packets with private addresses are usually dropped by routers in the public network and cannot be routed to the correct destination [46]. Additionally, from a security point of view, upon receipt of packets with private addresses, network entities in the public address space may believe that these packets are caused by an IP spoofing attack. Therefore, in our approach, no private addresses are allowed to be used in the public network.

Another principle is that no additional security issues arise from our design. The more complicated the design is, the more possible it is to have security holes. Thus our approach should modify the Mobile IP and RSIP protocols as little as possible. In particular, in order to comply with this principle, the following restrictions should be satisfied:

- No additional network entities, besides those that are necessary for the Mobile IP and RSIP protocols.
- No role change of the network entities. For example, the foreign agent plays a passive role and the home agent plays a reactive role in the Mobile IP registration procedure [41].
- No additional control messages exchanged among network entities.
- No change of security requirements. For example, it is still mandatory to authenticate registration messages exchanged between the home agent and the mobile node [41].

Briefly, our objective is to enable a mobile node with only a private home address to communicate with other hosts while the mobile node is visiting a public network. Additionally, the following two principles must be obeyed:

- no access to private addresses in the public address space;
- no additional security holes to those already existing in Mobile IP and RSIP.

4.7 Design Considerations

Because a private home address can neither uniquely identify a mobile node nor directly be used for communications in the public address space, what we need to solve is how the mobile node identifies itself and obtains an appropriate address in the public network. In the following, we explain the problems and the corresponding solutions in detail.

4.7.1 Identification of a Mobile Node

A major problem for use of private addresses in Mobile IP is that the private home address cannot be used to uniquely identify a mobile node in the public network. In other words, the mobile node needs some unique credentials in the public network. As mentioned in Section 4.4, Petri uses an identifier called *VPN-ID* to recognize a mobile node [43], and

Malinen employs the combination of a mobile node's private home address and its home agent's public address to distinguish the mobile node [30]. However, neither of them has been used widely. Currently the Network Access Identifier (NAI) [1] is used broadly. In our solution, we apply NAI to identify a mobile node in the public network.

4.7.2 Public Home Address Assignment to a Mobile Node

When a mobile node moves in the public network, it needs a public home address for communications with a correspondent node. The problem is which network entity can assign a public home address to the mobile node. According to the Mobile IP protocol [41], the mobile node is allowed to contact the foreign agent and the home agent during the registration period, so it can obtain the public home address only from either the foreign agent or the home agent.

If a public home address is assigned by the foreign agent, because the address prefix of the foreign network is different from that of the mobile node's home network, such assignment may cause confusion in network management. Also for the same reason, if the previous foreign agent assigns the public home address to the mobile node, when the mobile node moves to another foreign network, the new foreign agent may think that the mobile node is a hacker that is using an IP spoofing attack. Thus the new foreign agent may disallow the mobile node to access its network resources. Additionally, in Mobile IP, the authentication between the foreign agent and the mobile node is optional, not required [41]. So if there is no security association shared between the foreign agent and the mobile node, the foreign agent may not assign a public home address to the mobile node, or else the resources of public IP addresses in the foreign network can be used up easily by a hacker. In consequence, the assignment of a public home address to the mobile node cannot be performed by the foreign agent.

The other choice for address assignment is the home agent. In the following we explain why the home agent is capable of this task. Firstly and the most important, because a security association between the mobile node and the home agent is mandatory in Mobile IP [41], the home agent can verify the mobile node identity and protect the public address resources of the home network as well. If authentication is successful, because the RSIP protocol allows a host to lease more than one public address [8], the home agent can lease a public address from the RSIP gateway and then assign this address to the mobile node. The home agent inserts this public address in the registration reply message. With the help of *mobile-home* authentication extension appended to the registration reply message, this public home address assigned to the mobile node cannot be modified by hackers during packet delivery. Consequently, no new security problems arise from such assignment. Secondly, since the assignment of the mobile node's public home address is inserted in the registration message, neither additional control messages nor time delay is required. Finally, because the prefix of the assigned public home address is the same as that of the home network, it is convenient for network management. In short, it is a good choice to use the home agent to assign a public home address to the mobile node.

4.7.3 Source IP Address for the Registration Request Message

According to the principles described in Section 4.6, private IP addresses cannot be used in the public network. Therefore before the mobile node gets a public home address, it needs one appropriate IP address as the source address in order to deliver a registration request message from itself to the foreign agent. Mobile IP protocol specifies that 0.0.0.0 can be used as the source address if the mobile node does not know its IP address [41]. Although the case of a mobile node with an unknown IP address is different from that of a mobile node with a private home address, we can still apply this method. In other words, the address 0.0.0.0 can be used as the source IP address in the registration request message by the mobile node. As a result, the problem of source address for the registration request message can be solved without modification of Mobile IP protocol.

4.7.4 Address Issues for Data Transfer

After a mobile node finishes registration, it has a public home address and can communicate with a correspondent node. Depending on the location of the correspondent node, there are two cases, that is, the correspondent node is either inside or outside the home network.

If the correspondent node is located outside the home network, both the mobile node and the correspondent node use public IP addresses for communications, and the packets transferred between them follows the Mobile IP and RSIP protocols.

However, if the correspondent node is located inside the home network, as described in the Section 4.5, the private addresses are used between the correspondent node and the mobile node. When a packet sent from the correspondent node is intercepted by the home agent, in order to prevent private addresses from being accessed by the foreign agent in the public network, the home agent has to put one IP header outside the packet before it inserts this packet into the forward tunnel. Since this packet is delivered from the home agent to the mobile node, the home agent's public address may be used as the source and the mobile node's public home address may be used as the destination in the outer IP header. After that, the home agent puts the encapsulated packet into the forward tunnel.

In the opposite direction, similarly, a packet sent from the mobile node to the correspondent node also has to be encapsulated with an outer IP header to keep the foreign agent from accessing private addresses. Because the correspondent node does not have a public address and both the correspondent node and the home agent are located in the same network, the mobile node may use its own public home address as the source and its home agent's public address as the destination to encapsulate an original packet. Then this packet is routed to the home agent according to the Mobile IP and RSIP protocols. Finally this packet is decapsulated by the home agent and delivered to the correspondent node.

Therefore, for the case that the correspondent node is located inside the home network, it is necessary to build one tunnel between the public address of the home agent and that of the mobile node to keep private addresses from being accessed in the public network. We call this tunnel the *mobile-home tunnel*.

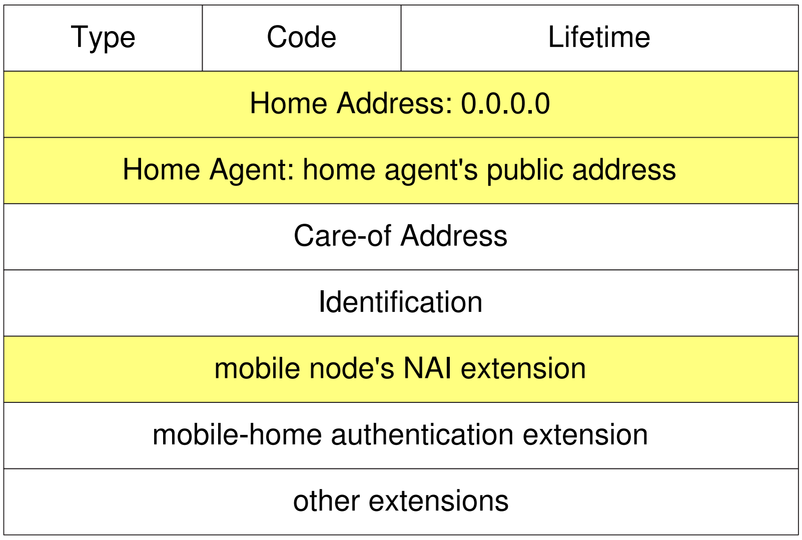
4.8 Procedures of Registration and Data Transfer

In this section, we apply the methods described above to achieve our objective. We present the whole procedures as well as the packet formats in detail. Because a mobile node first registers its care-of address and then communicates with a correspondent node when it visits a foreign network, our explanation is given according to this order.

4.8.1 Registration Procedure

When a mobile node visits a foreign network, it sends a registration request and then receives a registration reply. The format of a registration request and that of a registration reply are shown in Figure 39 and Figure 40 respectively, and our solutions are highlighted with the yellow color.

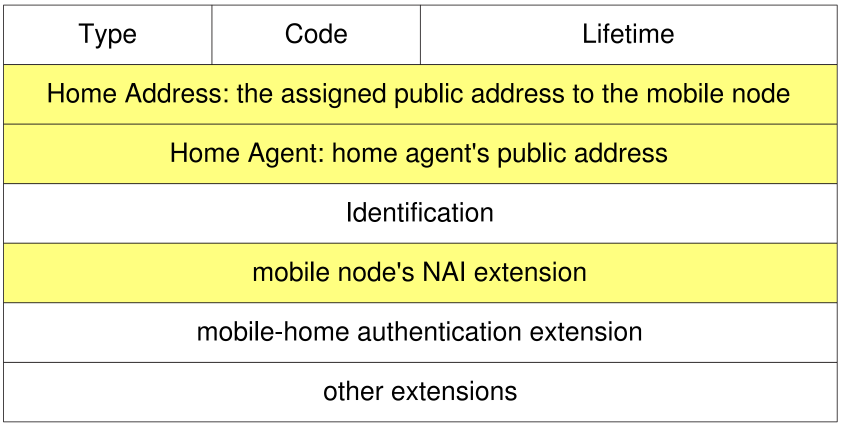
As explained in Section 4.7.3, because the mobile node only has a private home address, in the IP header of the packet that contains the registration request message as payload, the mobile node puts the IP address 0.0.0.0 as the source and the IP address of the foreign agent as the destination. In the registration request message, the mobile node fills in the *Home Address* field with 0.0.0.0 and the *Home Agent* field with the public address of the home agent. Since we use NAI to identify a mobile node in the public network, the mobile node also inserts its *NAI* extension before the *mobile-home* authentication extension. After being processed by the foreign agent, the registration request message is delivered to the home agent through the RSIP gateway.



Type	Code	Lifetime
Home Address: 0.0.0.0		
Home Agent: home agent's public address		
Care-of Address		
Identification		
mobile node's NAI extension		
mobile-home authentication extension		
other extensions		

Figure 39: Format of registration request message.

According to the mobile node's NAI extension, the home agent can recognize the mobile node. The home agent leases a public address from the RSIP gateway. Because this address will be the public home address of this mobile node, the home agent binds this address with the record of this mobile node together and then fills this address in the *Home Address* field of the registration reply message. The home agent puts its public address in the *Home Agent* field as well. Moreover, the mobile node's *NAI* extension and the *mobile-home* extension are required to the registration reply message [11]. On the receipt of the registration reply message, the mobile node obtains its public home address.



Type	Code	Lifetime
Home Address: the assigned public address to the mobile node		
Home Agent: home agent's public address		
Identification		
mobile node's NAI extension		
mobile-home authentication extension		
other extensions		

Figure 40: Format of registration reply message.

4.8.2 Data Transfer Procedure

A mobile node can communicate with a correspondent node after registration. In accordance with the location of a correspondent node, first we describe the procedure of communications between a mobile node and an external correspondent node, then we discuss that between a mobile node and an internal correspondent node. Moreover, for each case, there are two situations for packets sent from the mobile node to the correspondent node, i.e., direct delivery and use of a reverse tunnel.

The detailed data transfer procedures as well as the corresponding packet formats for each situation are shown in Figure 41 to Figure 46. The abbreviations shown in these figures are listed as follows:

- $HApub$: the public address of the home agent;
- $HApri$: the private address of the home agent;
- $MNpub$: the public home address of the mobile node;

- $MNpri$: the private home address of the mobile node;
- COA: the care-of address of the mobile node;
- CN: the address of the correspondent node;
- $Npri$: the private address of the RSIP gateway.

4.8.2.1 The Correspondent Node outside the Home Network

Because the correspondent node is located outside the home network, as explained in Section 4.7.4, public addresses are used in the packets transferred between the correspondent node and the mobile node.

When the correspondent node sends a data packet (Figure 41 (a)), it puts its IP address as the source and the mobile node's public home address as the destination (Figure 41 (b.1)). The packet is intercepted by the home agent after it passes through the RSIP gateway (Figure 41 (b.2)). The home agent follows the Mobile IP protocol and puts the packet into the forward tunnel. At the same time, according to the RSIP protocol, the home agent tunnels this packet to the RSIP gateway (Figure 41 (b.3)). The RSIP gateway decapsulates the packet and delivers it to the public network (Figure 41 (b.4)). Upon receipt of the packet, the foreign agent removes it from the forward tunnel and sends it to the mobile node (Figure 41 (b.5)).

In the opposite direction, if a reverse tunnel is not used, the packet format is quite simple. The mobile node just puts its public home address as the source and the correspondent node's address as the destination and then sends the packet (Figure 42).

However, the whole procedure is much complicated with use of a reverse tunnel (Figure 43 (a)). The original packet (Figure 43 (b.1)) is sent by the mobile node and inserted into the reverse tunnel by the foreign agent (Figure 43 (b.2)). The packet has to pass through the RSIP gateway before it reaches the home agent (Figure 43 (b.3)). The home agent decapsulates the packet from the RSIP tunnel and the reverse tunnel sequentially. Because the destination, i.e., the correspondent node, is outside the home network, the packet has to be inserted into the RSIP tunnel and sent to the correspondent node (Figure 43 (b.4)).

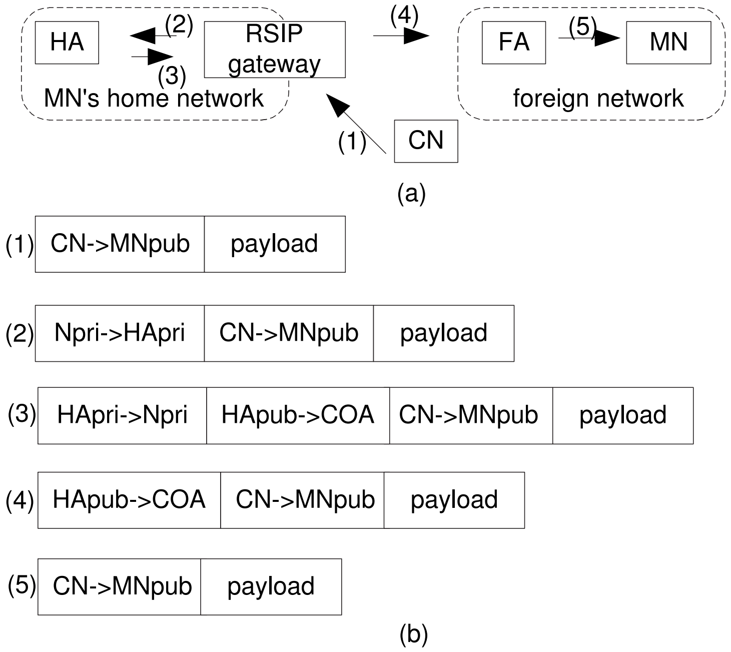


Figure 41: (a) Procedure of a packet delivered from an external correspondent node to a mobile node; (b) the corresponding packet formats.

After being decapsulated from the RSIP tunnel, the packet leaves for the correspondent node (Figure 43 (b.5)).

4.8.2.2 The Correspondent Node inside the Home Network

When the correspondent node is located inside the home network, as explained in Section 4.7.4, in order for the private addresses not to be accessed in the public network, one mobile-home tunnel is required.

An original packet (Figure 44 (b.1)) with the private addresses sent by the correspondent node is intercepted by the home agent (Figure 44 (a)). Because the mobile node has already moved outside the home network, the home agent has to put the packet through the mobile-home tunnel. Then the home agent puts the packet through the forward tunnel and the RSIP tunnel (Figure 44 (b.2)). The packet is decapsulated from the RSIP tunnel and transmitted to the public network by the RSIP gateway (Figure 44 (b.3)). On arrival at the foreign agent, the packet exits from the forward tunnel and leaves for the mobile node

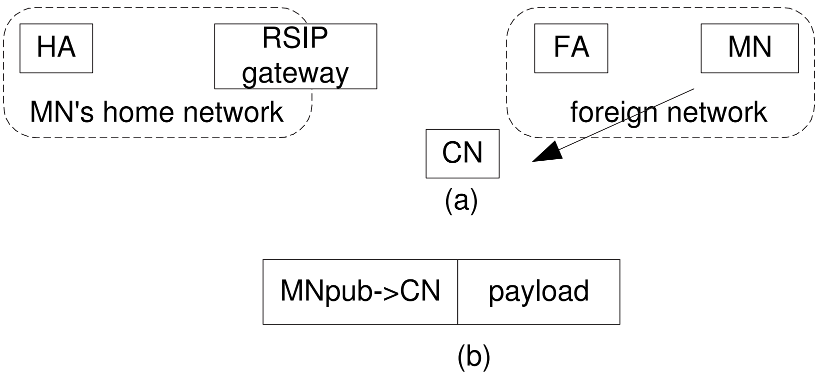


Figure 42: (a) Procedure of a packet delivered from a mobile node to an external correspondent node without a reverse tunnel; (b) the corresponding packet formats.

(Figure 44 (b.4)).

When the mobile node sends a data packet to the correspondent node (Figure 45 (a)), if a reverse tunnel is not used, the mobile node uses the public addresses to encapsulate the private addresses (Figure 45 (b.1)). At the entrance of the home network, the RSIP gateway tunnels the packet to the home agent (Figure 45 (b.2)). Then the home agent removes two IP headers, one from the RSIP tunnel and the other from the mobile-home tunnel. Finally the original packet (Figure 45 (b.3)) heads for the correspondent node.

However, if a reverse tunnel is used between the foreign agent and the home agent (Figure 46 (a)), after the packet is inserted into the mobile-home tunnel by the mobile node (Figure 46 (b.1)), it is put into the reverse tunnel by the foreign agent (Figure 46 (b.2)). On the arrival of the RSIP gateway, the packet is encapsulated with another IP header (Figure 46 (b.3)) and delivered to the home agent. Upon receipt of the packet, the home agent releases the packet from three tunnels, i.e., the RSIP tunnel, the reverse tunnel and the mobile-home tunnel. Finally the packet (Figure 46 (b.4)) is received by the correspondent node.

4.9 Solution to Mobile User Traversal of Firewall and RSIP Gateway

Usually a firewall and an RSIP gateway are installed in one machine and deployed on the entrance of a network, as shown in Figure 47. We use *FW/RSIP* to represent the

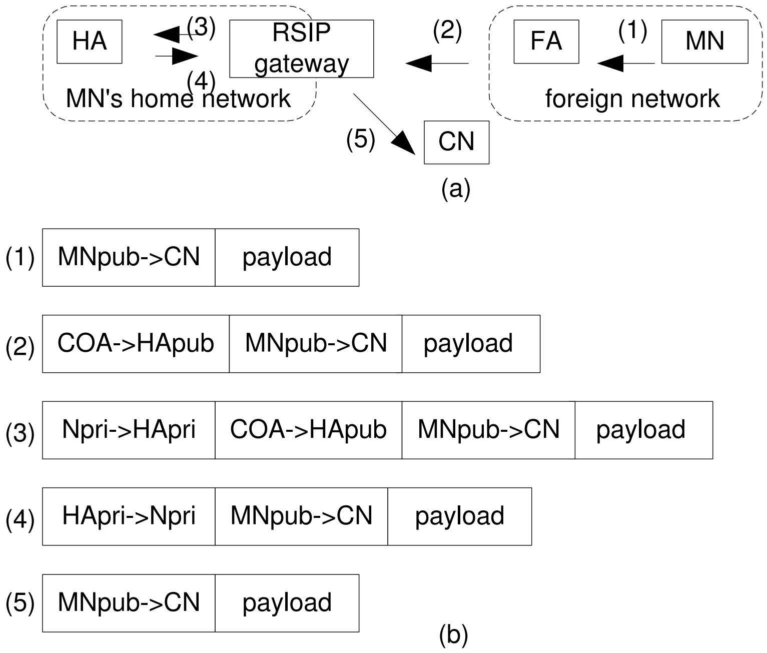


Figure 43: (a) Procedure of a packet delivered from a mobile node to an external correspondent node with a reverse tunnel; (b) the corresponding packet formats.

combination of a firewall and an RSIP gateway. In the network scenario shown in Figure 47, when a mobile node visits a foreign network, it faces the problems brought by the firewall as well as the RSIP gateway, which are respectively described in Section 2.1 and Section 4.3. Therefore, we combine the corresponding solutions proposed by Tang and Copeland [54, 53] to solve these problems. The new solution can enable a mobile node that only has a private home address to securely access its home network and communicate with other correspondent nodes. In the following, we give a description of this new solution. We still follow the order of registration and data transfer.

4.9.1 Registration Procedure

The registration procedure is shown in the Figure 48. In a registration request message, the mobile node puts the IP address 0.0.0.0 in the *Home Address* field and its NAI in the extension field. The format of the registration request message is the same as that shown in Figure 39. In order for the registration request message to pass through the firewall, the foreign agent sets up an IPsec tunnel with the FW/RSIP. After being de-tunneled by the

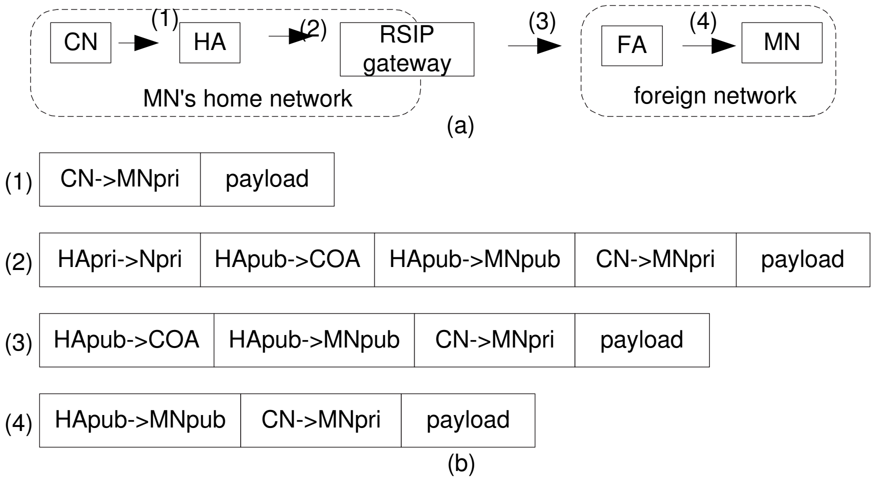

CN
(1)
HA
(2)
RSIP gateway
(3)
FA
(4)
MN
MN's home network
foreign network
(a)
(1) CN->MNpri | payload
(2) HApri->Npri | HApub->COA | HApub->MNpub | CN->MNpri | payload
(3) HApub->COA | HApub->MNpub | CN->MNpri | payload
(4) HApub->MNpub | CN->MNpri | payload
(b)

Figure 44: (a) Procedure of a packet delivered from an internal correspondent node to a mobile node; (b) the corresponding packet formats.

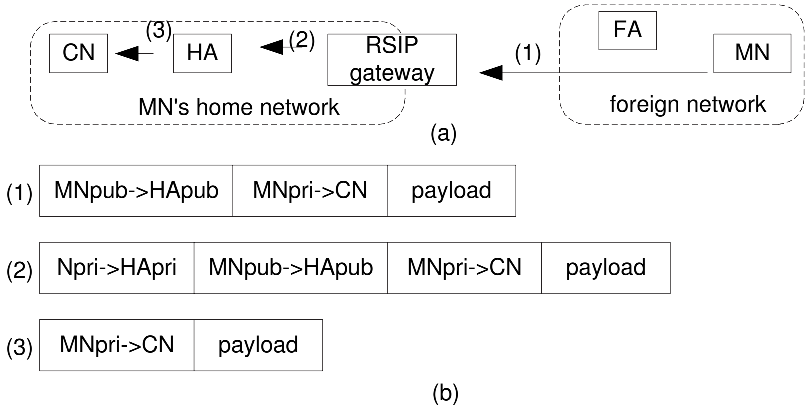

CN
(3)
HA
(2)
RSIP gateway
(1)
FA
MN
MN's home network
foreign network
(a)
(1) MNpub->HApub | MNpri->CN | payload
(2) Npri->HApri | MNpub->HApub | MNpri->CN | payload
(3) MNpri->CN | payload
(b)

Figure 45: (a) Procedure of a packet delivered from a mobile node to an internal correspondent node without a reverse tunnel; (b) the corresponding packet formats.

FW/RSIP, the registration request message is delivered to the home agent.

After verifying the registration request message, the home agent sends an *assign request* message [7] to the FW/RSIP to lease a public address for the mobile node. The home agent puts the assigned public address to the *Home Address* field in the registration reply message, as shown in the Figure 40. The registration reply message is inserted into the IPsec tunnel by the FW/RSIP for security reasons. The foreign agent removes the registration reply from the IPsec tunnel and transmits that to the mobile node. So far the mobile node gets the assigned public home address.

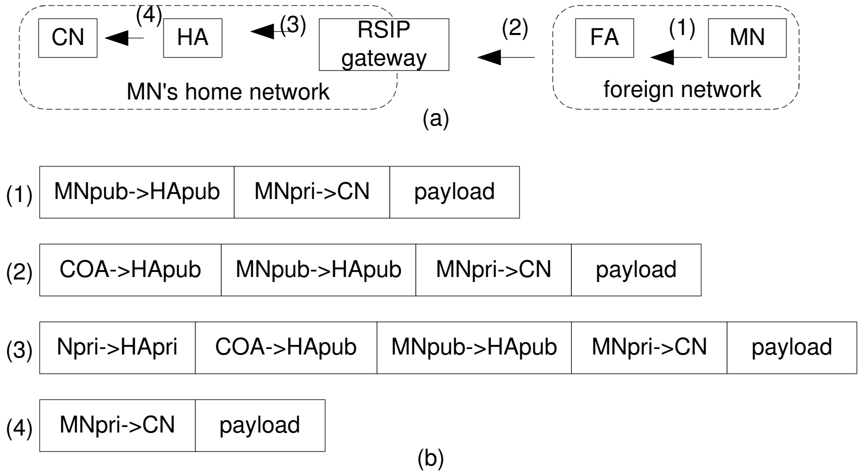

CN
(4)
HA
(3)
RSIP gateway
MN's home network
(2)
FA
(1)
MN
foreign network
(a)
(1) MNpub->HApub | MNpri->CN | payload
(2) COA->HApub | MNpub->HApub | MNpri->CN | payload
(3) Npri->HApri | COA->HApub | MNpub->HApub | MNpri->CN | payload
(4) MNpri->CN | payload
(b)

Figure 46: (a) Procedure of a packet delivered from a mobile node to an internal correspondent node with a reverse tunnel; (b) the corresponding packet formats.

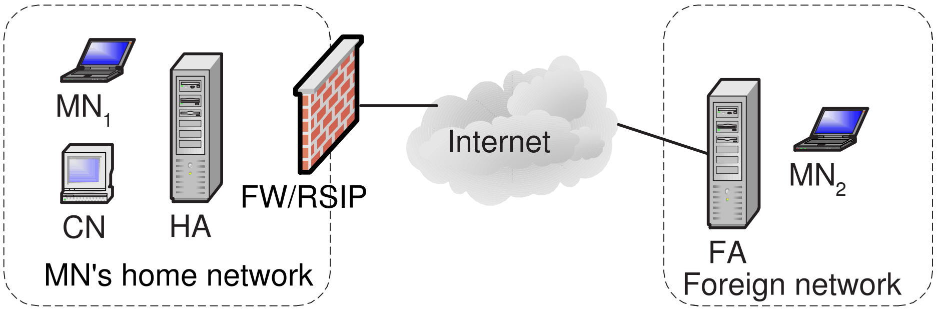


Figure 47: Network scenario for the combination of firewall and RSIP gateway.

4.9.2 Data Transfer Procedure

A mobile node may communicate with other correspondent nodes after registration. It is necessary and important for a mobile node that is visiting a foreign network to exchange information with a correspondent node that is located inside the home network. Moreover, the communication between these two nodes involves all mechanisms for firewall traversal and access to the private home network, which are described in Chapter 2 and Chapter 4. Therefore, in the following we detail the procedure and the corresponding packet formats for the communication between the mobile node and the internal correspondent node, shown in Figure 49, 50, and 51.

In our solution, the following tunnels may be used for data transfer:

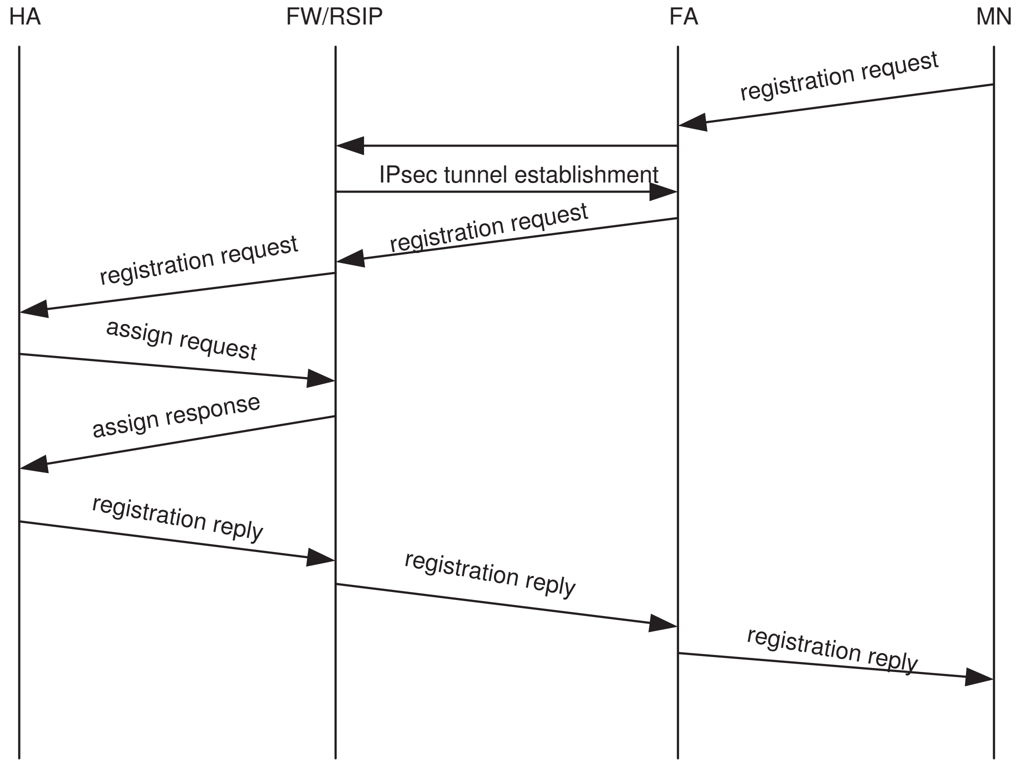


Figure 48: Control message flow in FW/RSIP network scenario.

- Mobile-home tunnel: a tunnel that is established between the public home address of the mobile node and the public address of the home agent.

- Mobile IP forward tunnel: a tunnel that is established from the public address of the home agent to the care-of address of the mobile node.

- Mobile IP reverse tunnel: a tunnel that is established from the care-of address of the mobile node to the public address of the home agent.

- RSIP tunnel: a tunnel that is established between the private address of the home agent and the private address of the FW/RSIP.

- IPsec tunnel: a tunnel that is established between the foreign agent and the public address of the FW/RSIP and uses IPsec mechanisms.

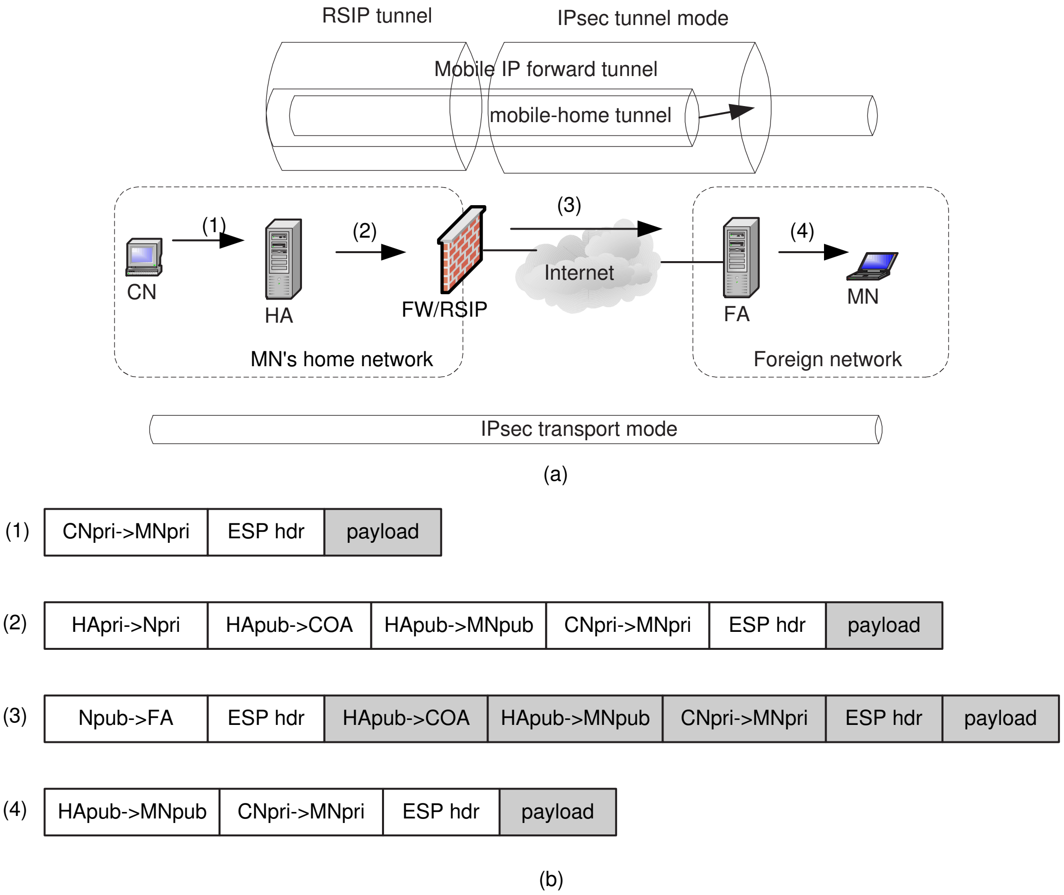
For packet formats shown in Figure 49, 50, and 51, besides the abbreviations listed in Section 4.8.2, $Npub$ and $Npri$ respectively represent the public address and the private address of the FW/RSIP. The shaded portion in the packet formats indicates encrypted data.

4.9.2.1 Packet Delivery from a Correspondent Node to a Mobile Node

The detail procedure for a packet delivery from a correspondent node to a mobile node is shown in Figure 49 (a) and the corresponding packet formats are shown in Figure 49 (b). Because both the mobile node and the correspondent node belong to the same network, they use their private addresses to communicate each other. After its payload is encrypted, a packet can be sent from the correspondent node to the mobile node (Figure 49 (b.1)). Based on the Mobile IP protocol [41], the packet is routed to the home agent. Because of the reason explained in Section 4.7.4 and the requirement of Mobile IP, the packet is put into the mobile-home tunnel and then the Mobile IP forward tunnel. The encapsulated packet passes through the RSIP tunnel and arrives at the FW/RSIP (Figure 49 (b.2)). The packet is de-tunnelled from the RSIP tunnel and put into the IPsec tunnel by the FW/RSIP (Figure 49 (b.3)) so that hosts in the Internet cannot know any information about the original packet. On arrival at the foreign agent, the packet is released from the IPsec tunnel and the Mobile IP forward tunnel (Figure 49 (b.4)). Then it is delivered to the mobile node. The mobile node firstly decapsulates the packet from the mobile-home tunnel. After that, it uses the secret shared with the correspondent node to decrypt the packet and gets the original packet.

4.9.2.2 Packet Delivery from a Mobile Node to a Correspondent Node

In the opposite direction, if no Mobile IP reverse tunnel is used, as shown in Figure 50 (a), a packet is encrypted and inserted into the mobile-home tunnel by a mobile node (Figure 50 (b.1)). Then the packet passes through the IPsec tunnel from the foreign agent to the FW/RSIP (Figure 50 (b.2)). After being released from the IPsec tunnel, the packet is inserted to the RSIP tunnel (Figure 50 (b.3)). The packet leaves for the correspondent node after it is de-tunnelled from the RSIP tunnel and the mobile-home tunnel (Figure 50 (b.4)). Because of the IPsec security mechanisms, only the correspondent node can successfully decrypt the payload of the packet.



(1) CNpri->MNpri | ESP hdr | payload

(2) HApri->Npri | HApub->COA | HApub->MNpub | CNpri->MNpri | ESP hdr | payload

(3) Npub->FA | ESP hdr | HApub->COA | HApub->MNpub | CNpri->MNpri | ESP hdr | payload

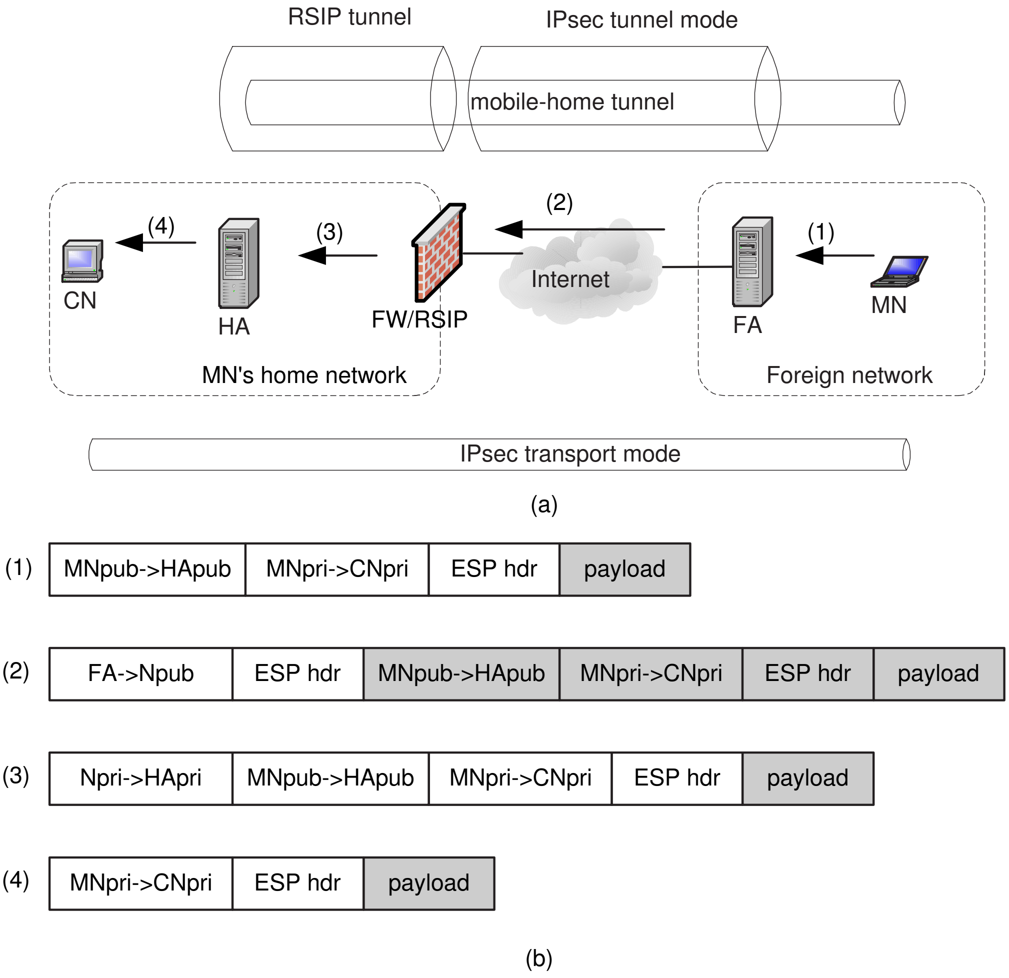
(4) HApub->MNpub | CNpri->MNpri | ESP hdr | payload

Figure 49: (a) Procedure of a packet delivery from an internal correspondent node to a mobile node in FW/RSIP network scenario; (b) the corresponding packet formats.

However, if a reverse tunnel is used (Figure 51 (a)), after being encrypted and inserted to the mobile-home tunnel (Figure 51 (b.1)), the packet enters the reverse tunnel before it enters the IPsec tunnel (Figure 51 (b.2)). The FW/RSIP releases the packet from the IPsec tunnel and lets it tunnel to the home agent (Figure 51 (b.3)). The home agent removes three outer IP headers from the packet and delivers it to the correspondent node (Figure 51 (b.4)). Because of the IP security mechanisms, no host along the way from the mobile node to the correspondent node can know the payload information of the packet.

4.10 Analysis

In this section, we mainly analyze the solution to private home network access, which is illustrated in Section 4.8, from four aspects, i.e., security, handoffs, packet overhead, and



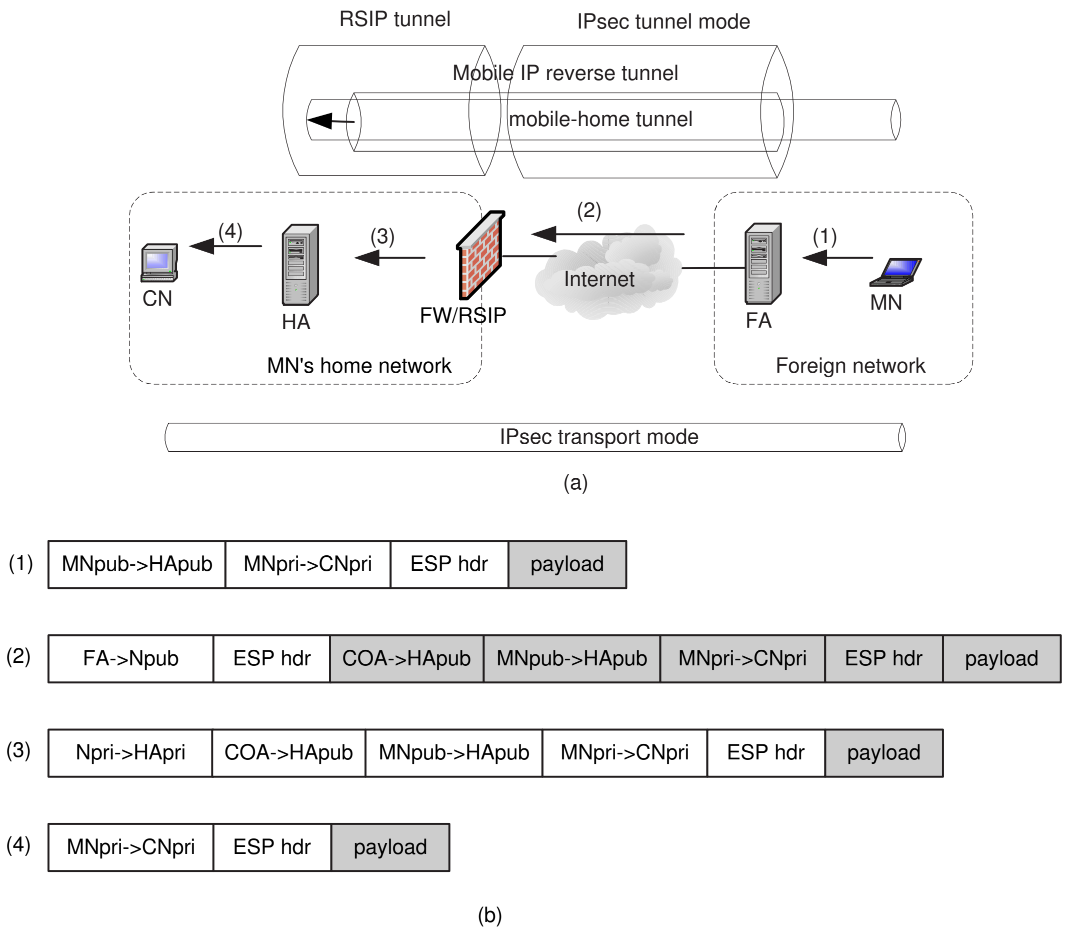
(1)	MNpub->HApub	MNpri->CNpri	ESP hdr	payload		
(2)	FA->Npub	ESP hdr	MNpub->HApub	MNpri->CNpri	ESP hdr	payload
(3)	Npri->HApri	MNpub->HApub	MNpri->CNpri	ESP hdr	payload	
(4)	MNpri->CNpri	ESP hdr	payload			

Figure 50: (a) Procedure of a packet delivery from a mobile node to an internal correspondent node without a reverse tunnel in FW/RSIP network scenario; (b) the corresponding packet formats.

scalability. Because the solution explained in Section 4.9 is just the combination of the firewall traversal solution [54] and the private home network access solution [53], which are described in Section 2.6 and Section 4.8 respectively, its analysis is the combination of Section 2.8 and this section.

4.10.1 Security

Because our solution follows the principles described in Section 4.6, our solution does not bring any additional security holes. In more detail, there is no new network entity in our solution. Unlike the methods proposed in [18, 21, 29], our solution does not change the



(a)

(1) MNpub->HApub | MNpri->CNpri | ESP hdr | payload

(2) FA->Npub | ESP hdr | COA->HApub | MNpub->HApub | MNpri->CNpri | ESP hdr | payload

(3) Npri->HApri | COA->HApub | MNpub->HApub | MNpri->CNpri | ESP hdr | payload

(4) MNpri->CNpri | ESP hdr | payload

(b)

Figure 51: (a) Procedure of a packet delivery from a mobile node to an internal correspondent node with a reverse tunnel in FW/RSIP network scenario; (b) the corresponding packet formats.

role of any network entities. For registration, our solution does not create any new control messages. All the control messages, such as registration request, registration reply, assign request, and assign response, that we use are defined in the Mobile IP protocol and the RSIP protocol. Although we modify the registration request and registration reply messages, the modifications are allowed by Mobile IP. For data transfer, we introduce a new mobile-home tunnel. Because the security association between a mobile node and its home agent is required, the mobile node and its home agent can apply security mechanisms to protect the mobile-home tunnel from being hijacked or redirected. Therefore, our solution is secure.

4.10.2 Handoffs

In our solution, after leaving its home network, the mobile node needs to request a public home address when it visits the first foreign network. After the mobile node gets a public home address, it does not need to request any home addresses when it stays abroad. Although a new mobile-home tunnel is proposed for data delivery, the two end-points, i.e., the public home address of the mobile node and the public address of the home agent, do not change for handoffs. Therefore, the mobile node only follows the Mobile IP protocol for handoffs. In other words, our solution has no influence on handoffs.

4.10.3 Packet Overhead

Although a Mobile IP forward tunnel, a Mobile IP reverse tunnel, and an RSIP tunnel bring some overhead to packets, we do not discuss that here. We only consider the packet overhead brought by our solution.

When a mobile node communicates with a correspondent node that is located outside the home network, data delivery follows the Mobile IP protocol and the RSIP protocol. However, when a mobile node communicates with a correspondent node that is located inside the home network, a mobile-home tunnel is necessary for data delivery. In other words, one additional IP header is required. The minimum size of an IPv4 header is 20 bytes. Suppose a packet size is 1500 bytes, which is the Maximum Transmission Unit (MTU) in many networks. Under the circumstances, the overhead of our solution is 1.33%.

4.10.4 Scalability

In our solution, whenever a mobile node leaves its home network, it needs a public home address. When a mobile node returns its home network, it puts its public home address back. The public address resources of the home network are limited. If the number of mobile nodes outside the home network is more than the number of available public addresses owned by the home network, some of the mobile nodes cannot communicate with other hosts. In other words, our solution is limited by the public address resources of the home network.

4.11 Conclusion

In this chapter, we present an approach that a mobile node with a private home address can communicate with a correspondent node when the mobile node stays outside its home network. In our scenario, an RSIP gateway is located at the border of the private home network, and a foreign agent that assigns a care-of address to the mobile node is placed in the public network. Our approach follows two principles, that is, no access to private addresses in the public network and no additional security issues. Our design consists of four parts. First, NAI is applied to identify the mobile node in the public network; second, the public home address of the mobile node is assigned by the home agent during the registration period; third, the IP address 0.0.0.0 is used as the source address for the registration request message; and finally, a mobile-home tunnel is required for data transfer when a correspondent node also belongs to the home network.

Our solution can be extended to solve the problems for the situation that the combination of firewall and RSIP gateway is located at the entrance of a mobile node's private home network. We combine our solution with the firewall traversal solution [54]. This new solution can enable a mobile node to pass through the firewall and to securely communicate with other hosts when the mobile node stays abroad.

Our solution is secure. It has no influence on handoffs and brings little packet overhead. But its scalability is limited by the public address resources of a mobile node's home network. Because our solution makes little modification of the Mobile IP and RSIP protocols, it is practicable .

CHAPTER V

CONCLUSIONS

In this thesis, the challenges that prevent Mobile IP from being widely used are investigated and the corresponding solutions are proposed. We mainly discuss how a mobile node can access its home network securely. We summarize the three research topics as follows.

5.1 Mobile IP Secure Firewall Traversal with the Deployment of Foreign Agents

The first research topic solves the firewall traversal problems in Mobile IP. When the home network of a mobile node is protected by a firewall, the mobile node cannot access the home network if it fails the authentication by the firewall. Thus use of Mobile IP is restricted by firewalls.

Our novel solution is presented in Chapter 2 to achieve firewall traversal in Mobile IP. Specifically, an IPsec tunnel is established between the firewall and the foreign agent for firewall traversal, and an IPsec transport security association is shared by the mobile node and a correspondent node for end-to-end security.

If a number of foreign agents are deployed hierarchically, an IPsec tunnel is set up between the firewall and a gateway foreign agent, instead of a foreign agent. Therefore, no security association needs to be refreshed if the mobile node moves within these hierarchical foreign agents, which means that handoff performance is not degraded by security achievements.

Furthermore, our solution is secure and scalable.

5.2 Secure Firewall Traversal in the Mobile IP AAA System

In the second research topic, which is described in Chapter 3, we research further on firewall traversal problems. For the situation that Mobile IP is combined with the services of

Authentication, Authorization, and Accounting (AAA), a new security model and a new key distribution method are developed so that a mobile node can pass through the firewall that protects the home domain of the mobile node.

In the new security model, a new essential security association shared between the home AAA server and the firewall is required. With this essential security association, the firewall can trust the home AAA server. From the home AAA server, the firewall gets some information about the foreign AAA server. The firewall uses such information to set up an IPsec tunnel with the foreign AAA server so that the mobile node's initial registration request message can traverse the firewall. Because the firewall and the home AAA server belong to the same administrative domain, it is easy to implement and maintain this new essential security association.

In addition, we propose that a new key be necessary for firewall traversal. This key is shared by the firewall and the foreign agent that is the default router of the mobile node. During an initial registration period, the home AAA server generates this new key, encrypts it with the appropriate essential security associations, and distributes it to the firewall and the foreign agent respectively. The firewall and the foreign agent use this key to set up IPsec tunnel for the mobile node's messages to pass through the firewall. Because this new key is delivered with other keys, its distribution does not cost extra time in the registration period.

Because of the easy implementation for the new essential security association and no extra distribution time for the new key, our proposal is practicable.

5.3 Mobile IP Use of Private Addresses in an RSIP Home Network

In Chapter 4, we mainly discuss the problems for use of private addresses in Mobile IP and design a secure and useful scheme. Our solution can achieve a mobile node with a private home address to access its home network as well as the Internet when it is away from home.

In a public network, a private home address cannot be used to uniquely identify a mobile node and to communicate with other correspondent nodes. Therefore, we suggest that Network Access Identifier (NAI) be used as a unique identification of the mobile node in a public network. The reason for the public home address assignment to a mobile node by its home agent is explained. The detailed formats for registration messages are presented. Specifically, the mobile node's NAI and IP address 0.0.0.0 are included in a registration request message. A registration reply message contains a public address that is assigned to the mobile node. In addition, to prevent private addresses from being accessed in a public network, we propose a tunnel should be established between the public home address of the mobile node and the public address of the home agent.

Furthermore, for the network scenario that a private home network is protected by a firewall, which is used widely, our approach can be extended to achieve a mobile node in such network scenario to securely get access to its home network.

The analysis shows that our solution is secure. It has no influence on a mobile node's handoffs and brings little packet overhead.

5.4 Summary

In conclusion, our original research can enable a mobile node to securely and efficiently access its home network as well as the Internet in Mobile IP. It brings no security holes to the home network or a foreign network. Our approach can be implemented and maintained easily. Therefore, our research can help Mobile IP to be used widely and commercially.

REFERENCES

[1] Aboba, B. and Beadles, M., "The network access identifier." RFC 2486, Jan. 1999.

[2] Aboba, B., Calhoun, P., Glass, S., and *et al.*, "Criteria for evaluating AAA protocols for network access." RFC 2989, Nov. 2000.

[3] Adrangi, F. and Levkowetz, H., "Problem statement: Mobile ipv4 traversal of virtual private network (VPN) gateways." RFC 4093, Aug. 2005.

[4] Balakrishnan, H., Seshan, S., Amir, E., and Katz, R. H., "Improving TCP/IP performance over wireless networks," in *Proc. 1st Annual International Conference on Mobile Computing and Networking*, pp. 2–11, Dec. 1995.

[5] Bellovin, S. and Cheswick, W., "Network firewalls," *IEEE Communications Magazine*, vol. 32, pp. 50–57, Sept. 1994.

[6] Berioli, M. and Trotta, F., "IP mobility support for IPsec-based virtual private networks: an architectural solution," in *Proc. GLOBECOM'03*, vol. 3, pp. 1532–1536, Dec. 2003.

[7] Borella, M., Grabelsky, D., Lo, J., and Taniguchi, K., "Realm specific IP: protocol specification." RFC 3103, Oct. 2001.

[8] Borella, M., Lo, J., Grabelsky, D., and Montenegro, G., "Realm specific IP: framework." RFC 3102, Oct. 2001.

[9] Braun, T. and Danzeisen, M., "Secure Mobile IP communication," in *Proc. 26 Annual IEEE Conference on Local Computer Networks*, pp. 586–593, Nov. 2001.

[10] Calhoun, P., Loughney, J., Guttman, E., Zorn, G., and Arkko, J., "Diameter base protocol." RFC 3588, Sept. 2003.

[11] Calhoun, P. and Perkins, C., "Mobile IP network access identifier extension for IPv4." RFC 2794, Mar. 2000.

[12] Droms, R., "Dynamic host configuration protocol." RFC 2131, Mar. 1997.

[13] Glass, S., Hiller, H., Jacobs, S., and Perkins, C., "Mobile IP authentication, authorization, and accounting requirements." RFC 2977, Oct. 2000.

[14] Gupta, V. and Montenegro, G., "Secure and mobile networking," *Mobile Networks and Applications*, vol. 3, pp. 381–390, Dec. 1998.

[15] Gustafson, U. and Forslow, J., "Network design with Mobile IP." INET 2001, June 2001. Available at http://www.isoc.org/inet2001/CD_proceedings/T40/inet_T40.htm, accessed on May 11, 2006.

[16] Gustafsson, E., Jonsson, A., and Perkins, C. E., "Mobile IPv4 regional registration." Internet draft, Nov. 2005. Available at http://www.ietf.org/internet-drafts/draft-ietf-mip4-reg-tunnel-01.txt, (work in progress), accessed on May 11, 2006.

[17] Hoffman, P., "Algorithms for internet key exchange version 1 (ikev1)." RFC 4109, May 2005.

[18] Idoue, A., Yokota, H., and Kato, T., "Mobile ip network supporting private ip addresses utilizing regional registration and nat function," in *Proc. 8th International Conference on Parallel and Distributed Systems*, pp. 141–146, June 2001.

[19] Ioannidis, J., Duchamp, D., and Jr., G. M., "IP-based protocols for mobile internetworking," in *Proc. SIGCOMM'91 Conference*, pp. 235–245, Sept. 1991.

[20] Johnson, D., Perkins, C., and Arkko, J., "Mobility support in IPv6." RFC 3775, June 2004.

[21] Kato, T., Idoue, A., and Yokota, H., "Mobile IP using private IP addresses," in *Proc. 6th IEEE Symposium on Computers and Communications*, pp. 491–497, July 2001.

[22] Kaufman, C., "Internet Key Exchange (IKEv2) Protocol." RFC 4306, Dec. 2005.

[23] Kaufman, C., Perlman, R., and Speciner, M., *Network Security: Private Communication in a Public World.* Prentice Hall Inc., second ed., 2002.

[24] Kent, S., "IP authentication header." RFC 4302, Dec. 2005.

[25] Kent, S., "IP encapsulating security payload (ESP)." RFC 4303, Dec. 2005.

[26] Kent, S. and Seo, K., "Security architecture for the Internet protocol." RFC 4301, Dec. 2005.

[27] Lemon, T. and Cheshire, S., "Encoding long options in the dynamic host configuration protocol (DHCPv4)." RFC 3396, Nov. 2002.

[28] Levkowetz, H. and Vaarala, S., "Mobile IP traversal of network address translation (NAT) devices." RFC 3519, Apr. 2003.

[29] Lim, H.-J., Jeong, J., and Chung, T. M., "Mobile IP using private IP address through stateful network address translation," in *Proc. 6th International Conference on Advanced Communication Technology*, vol. 2, pp. 765–769, 2004.

[30] Malinen, J., *Using private addresses with hierarchical Mobile IPv4.* MS thesis, Helsinki University of Technology, Finland, Mar. 2000. Available at http://dynamics.sourceforge.net/?page=publications/jkmaline_thesis.ps.gz, accessed on May 11, 2006.

[31] Metz, C., "AAA protocols: authentication, authorization, and accounting for the Internet," *IEEE Internet Computing*, vol. 3, pp. 75–79, Nov. 1999.

[32] Mink, S., Pahlke, F., Schafer, G., and Schiller, J., "FATIMA: a firewall-aware transparent internet mobility architecture," in *Proc. 5th IEEE Symposium on Computers and Communications*, pp. 172–179, July 2000.

[33] Mitton, D., Johns, M. S., Barkley, S., and *et al.*, "Authentication, Authorization, and Accounting: protocol evaluation." RFC 3127, June 2001.

[34] Montenegro, G., "Reverse tunneling for Mobile IP, revised." RFC 3024, Jan. 2001.

[35] Montenegro, G. and Borella, M., "RSIP support for end-to-end IPsec." RFC 3104, Oct. 2001.

[36] Montenegro, G. and Gupta, V., "Sun's SKIP firewall traversal for Mobile IP." RFC 2356, June 1998.

[37] Perkins, C., "Mobile IP," *IEEE Communications Magazine*, vol. 35, pp. 84–99, May 1997.

[38] Perkins, C., *Mobile IP: design principles and practices.* Addison-Wesley, 1998.

[39] Perkins, C., "Mobile IP and security issue: an overview," in *Proc. 1st IEEE/Popov Workshop on Internet Technologies and Services*, pp. 131–148, Oct. 1999.

[40] Perkins, C., "Mobile IP joins forces with AAA," *IEEE Personal Communications*, vol. 7, pp. 59–61, Aug. 2000.

[41] Perkins, C., "IP mobility support for IPv4." RFC 3344, Aug. 2002.

[42] Perkins, C. and Calhoun, P., "Authentication, Authorization, Accounting (AAA) registration keys for Mobile IPv4." RFC 3957, Mar. 2005.

[43] Petri, B., "Private IP encapsulation within IP (PIPE)." Internet draft, Jan. 2000. Available at http://mirrors.isc.org/pub/www.watersprings.org/pub/id/draft-petri-mobileip-pipe-00.txt, (expired), accessed on May 11, 2006.

[44] Postel, J., "User datagram protocol." RFC 768, Aug. 1980.

[45] Postel, J., "Transmission control protocol." RFC 793, Sept. 1981.

[46] Rekhter, Y., Moskowitz, B., and *et al.*, "Address allocation for private internets." RFC 1918, Feb. 1996.

[47] Rigney, C. and *et al.*, "Remote Authentication Dial In User Service (RADIUS)." RFC 2138, Apr. 1997.

[48] Snoeren, A. and Balakrishnan, H., "An end-to-end approach to host mobility," in *Proc. ACM/IEEE MobilCom'00*, pp. 155–166, Aug. 2000.

[49] Solomon, J., *Mobile IP: the Internet unplugged.* Prentice Hall Inc., 1997.

[50] Srisuresh, P., "Security model with tunnel-mode IPsec for NAT domains." RFC 2709, Oct. 1999.

[51] Srisuresh, P. and Egevang, K., "Traditional IP Network Address Translator (Traditional NAT)." RFC 3022, Jan. 2001.

[52] Stallings, W., *Network security essentials: applications and standards.* Prentice Hall Inc., 2000.

[53] Tang, J. and Copeland, J. A., "Mobile IP use of private addresses in an RSIP home network," in *Proc. 2006 IEEE Wireless Communications and Networking Conference.*

[54] Tang, J. and Copeland, J. A., "Mobile IPv4 secure firewall traversal with deployment of foreign agents," in *Proc. 2005 IEEE Wireless Communications and Networking Conference*, vol. 3, pp. 1533–1538, Mar. 2005.

[55] Tsuda, Y., Ishiyama, M., Fukumoto, A., and Inoue, A., "Design and implementation of network CryptoGate-IP-layer security and mobility support," in *Proc. 31 Hawaii International Conference on System Sciences*, vol. 7, pp. 681–690, Jan. 1998.

[56] Vaarala, S. and Klovning, E., "Mobile IPv4 traversal across IPsec-based VPN gateways." Internet draft, Nov. 2005. Available at http://ietf.org/internet-drafts/draft-ietf-mip4-vpn-problem-solution-02.txt, (work in progress), accessed on May 11, 2006.

[57] Zao, J., Kent, S., and *et al.*, "A public-key based secure Mobile IP," in *Proc. 3rd Annual ACM/IEEE MobiCom'97*, pp. 173–184, Sept. 1997.

[58] Zao, J., Kent, S., and *et al.*, "A public-key based secure Mobile IP," *Wireless Networks*, vol. 5, pp. 373–390, Oct. 1999.