Secure Firewall Traversal in Mobile IP Network

Jung-Min Park[1], Min-Jung Jin[2], and Kijoon Chae[2]

[1] Intelligent System Control Research Center, KIST, Korea
pjm@amadeus.kist.re.kr
[2] Department of Computer Science and Engineering, Ewha Womans Univ., Korea
{mjjin,kjchae}@ewha.ac.kr

Abstract. With recent advances in wireless communication technology, mobile computing is an importance research area. Mobile IP is designed to provide IP services to roaming nodes. Mobile users take advantage of this protocol to obtain the services as if they were connected to their home network. In many cases mobile users is connected through a wireless link and is protected by corporation's firewall in virtual private network. In order to have a successful deployment of Mobile IP as an extension of a private network, security services should be provided as if the mobile node were attached to its home network. In this paper, we propose the security mechanism of combining Mobile IP and IPSec tunnels, which can provide secure traversal of firewall in a home network. The simulation results show that the proposed mechanism provides the secure and efficient communication.

1 Introduction

Mobility in IP networks is a significant issue due to the recent increase of many portable devices such as notebook and PDA and the development of wireless network interface. Many popular applications such as E-commerce and remote access require transmission of highly sensitive information, often over wireless links. Mobility implies higher security risk than static operation in fixed network, because the traffic may at times take unexpected network paths with unknown or unpredictable security characteristics. Technologies should be developed both IP security and mobility over wireless links.

Mobile IP has been designed with the IETF [1] to provide robust communication of mobile users as they roam from place to place [2][3][4]. With growth of public networks and the deployment of security protocols, enterprises around the world are trying to securely extend their network over the public backbones, establishing what are called Virtual Private Network (VPN). Practical applications of Mobile IP are likely to occur where a private network is extended over Internet. In many cases mobile users is connected through a wireless link and is protected by corporation's firewall in VPN. In order to have a successful deployment of Mobile IP as an extension of a private network, mobile users must be authenticated safely when roaming

P.M.A. Sloot et al. (Eds.): ICCS 2003, LNCS 2660, pp. 535–544, 2003.

from own network to another and only authorized users must be allowed the access to the private network. In Mobile IP, a tunnel is built up from a Home Agent (HA) to the Mobile Node's (MN's) Care-of-Address (CoA). Since this tunnel can be traverse the home network's firewall, the tunnel endpoints have to be administrated carefully with regard to security. Network operators are not likely to accept any tunnels through their firewalls. Additionally, the firewall has to inspect both outer and inner header of tunneled packets to ensure the packets are delivered only if their exact destination address is the home address of a registered MN, which may cause efficient problems. Since an MN abroad is logically still a part of its home network, security associations providing at least data origin authentication are necessary between each MN and a HA or a firewall in home network. Data encryption is required to keep confidential data transmitted to the MN as secure as it would be inside the home network. Another problem regarding Mobile IP and firewall is the use of topologically incorrect source addresses for packets sent by an MN. Few firewalls will allow such packets to exit a foreign network or to enter the MN's home network if the destination address is located there.

The IETF has also developed the suite of IPSec protocols [5] to provide capabilities to secure communications across the Internet at the network layer. With IPSec, security mechanisms are directly applied to IP packets. Additional headers are added to an IP packet to transport security related information and to identify protected packets.

In this paper we propose the secure tunneling mechanism of combining Mobile IP and IPSec tunnels, which can provide secure traversal of firewall in home network while mobile nodes are roaming abroad. This paper is organized as follows. Section 2 introduces the existing proposal for firewall over Mobile IP. Section 3 describes the our proposed mechanism. Section 4 presents our simulation environment and simulation scenarios and evaluates the simulation result. Finally, Section 5 summarizes and concludes this paper.

2 Related Works

Zao and Condell [8] describe the scheme to negotiate the use of IPSec on the Mobile IP tunnels and a procedure to establish these tunnels. IPSec is used to replace IP-in-IP tunneling, which is basic tunneling mechanism in Mobile IP. They defined the six possible unidirectional tunnels(HA-MN, HA-FA, MN-FA, and vice versa). The tunnel establishment has to be done by an appropriate protocol such as ISAKMP. The approach is required minimal overhead, but it is quite inflexible.

Binkley and Ricardson [9] propose a security model using IPSec for mobile user and networks providing access-points to these mobile nodes. They propose the bidirectional IPSec tunnels between a HA and a MN. Since they consider secure mobility problem as special case of ad-hoc network, it may be too complex in Mobile IP network.

Montenegro and Gupta [10] describe the scheme of combining Mobile IP and IPSec tunnels which can protect the home network when mobile nodes are roaming abroad. They propose to use SKIP for key management, authentication, and encryp-

tion. The approach seems to be easy and efficient to solve Mobile IP security problem, but all mobile nodes must support SKIP.

Mink et al. [11][12], propose the hierarchical mobility architecture FATIMA (Firewall-Aware Transparent Internet Mobility Architecture). In order to achieve the security, they define a special gateway in firewall and IPSec tunnels are established among those nodes. The approach is transparent to current Mobile IP and supports the micro-mobility. However, since all security-critical functionality is concentrated in FATIMA gateway, it causes a single point of failure. Moreover, the high cost in design and implementation of the architecture is additional disadvantages.

3 Proposed Secure Tunneling Mechanism

3.1 Secure Tunneling Mechanism

We describe the proposed secure tunneling mechanism. To simplify the security management we regard the firewall as screen-subnet firewall, where the private network and Internet are separated by de-militarized zone. Signaling between the mobile node and the firewall requires message authentication, integrity and replay protection, while mobile nodes roam foreign networks. We use an IPSec tunnel to protect the Mobile IP tunnel between firewall and MN, which traverse the insecure parts of the Internet, similar to the proposal by Montenegro and Gupta. Since all packets over the Internet are authenticated and encrypted by IPSec, the establishment of IPSec tunnel is able to implement a lightweight security in Mobile IP without additional security mechanism. Within the private network, we use the Mobile IP tunnel. Therefore, the traffic between HA and firewall is sent through IP-in-IP tunneling. The proposed tunneling mechanism provides authentication, integrity and replay protection of all IP packets sent during Mobile IP registration. Fig. 1 shows the proposed secure tunneling mechanism.

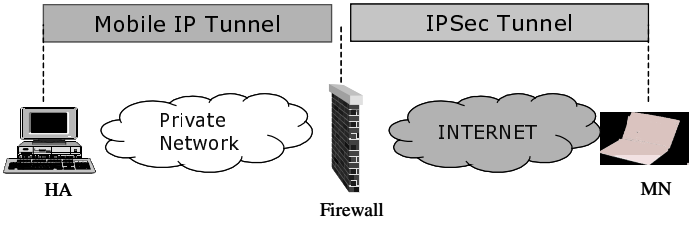

Fig. 1. Secure Tunneling Mechanism

We assume that MNs acquire their IP address from Dynamic Host Configuration Protocol(DHCP) [13] servers while MN is roaming abroad. DHCP allows to dynamically assign an IP address to a node and is a wide spread mechanism to reduce the administration overhead in dynamic changing network configuration. As regarding to the

practical implementation, the combination of Mobile IP with DHCP is used. Data transmission between the MN and the Correspondent Node(CN) takes place via the HA because of security reasons. It is also possible to communicate with the CN directly provided no security is needed. The encrypted and encapsulated Mobile IP packets are decrypted and decapsulated by the firewall and delivered to the HA. The HA finally decapsulates these Mobile IP packets and delivers them to the appropriate receivers.

3.2 Operation of Secure Tunneling Mechanism

When a MN moves new point of attachment, proposed tunneling mechanism operates as follows. When a MN enters new foreign network, the MN stops the old IPSec tunnels. The MN gets the co-located CoA from DHCP servers. Thereafter, bi-directional IPSec tunnel establishes between MN and firewall. Then, the MN registers at the HA and communicate with other CN. Fig. 2 shows the exchange of messages of proposed secure tunneling mechanism by time sequence.

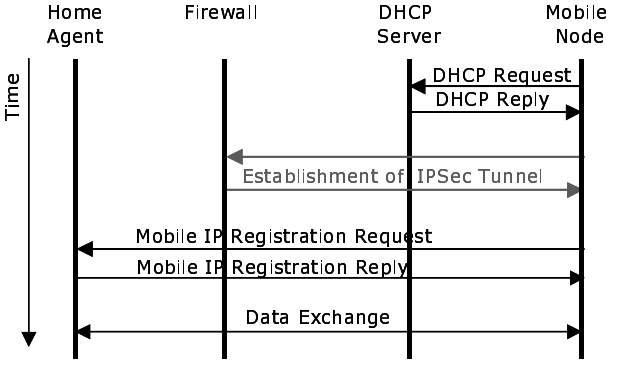

Fig. 2. Message Sequence Chart

4 Performance Evaluation

4.1 Simulation Environment

We analyze the performance of proposed mechanism through the simulation. In the following, we describe the four types of scenario for simulation and present the simulation results. Each scenario is simulated on Desktop PC with Intel Pentium IV 1G Hz CPU and run under Windows 2000 server operation system. In our simulation, we use the SDL(Specification and Description Language) which is standardized as ITU Recommendation Z.100. Because of SDL's suitability for real-time and stimuli-response

systems, it is well received in the telecommunication community and is used both in standards making and product development.

Fig. 3 shows our simulation network topology. In the simulation topology, the wired link bandwidth is 10 Mbps with 5 ms/km latency. The wireless side has 2 Mbps with 7 ms/km latency.

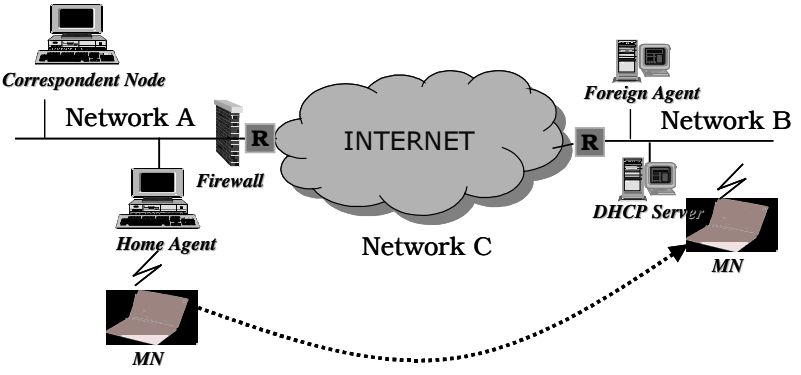

Fig. 3. Simulation Topology

Assumptions. We use the pre-established symmetric keys to eliminate the necessity of using asymmetric cryptography which represent more processing overhead for the system. We decide to use pre-negotiated security attributes between the HA and the MN and between the firewall and the MN for Mobile IP registration. Since all the security protocols simulated give various alternatives in terms of algorithms for the different security attributes, we have to decide the appropriate algorithms. For this purpose, we consider several aspects such as algorithm that have proven enough reliability, algorithm that comply with the basic requirement of the protocols, and computational time of cryptographic functions involved in the algorithm. We choose the HMAC-MD5 as the authentication algorithm to compute the keyed-hash and DES-CBC as the encryption algorithm.

4.2 Simulation Scenario

The simulation measures total latency involved in the necessary protocol operations. An important issue is the performance of authentication on the proposed tunneling mechanism. Our objectives focus on the performance impact of the registration procedure on the proposed secure tunneling scheme. To obtain the significant result, we describe the simulation scenarios, which take into account four different types of tunneling schemes and analyze this scenarios. The first one is basic routing mechanism, the second employs mobile IP tunneling, the third scenario employs the tunnel mode IPSec tunneling with AH, and the fourth use the tunnel mode IPSec tunneling with

ESP. Fig. 4 depicts the simulation environment and scenarios for the performance analysis.

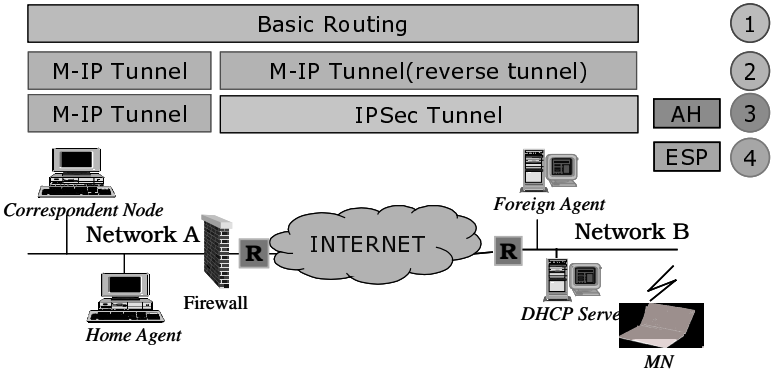

Fig. 4. Simulation Scenario

Scenario 1: Basic Routing. The first scenario is to measure the latency caused by raw data packet without tunneling and cryptographic operation.

Scenario 2: Mobile IP Tunneling. The second scenario is to measure the latency caused by Mobile IP tunneling. In this case, there are two kinds of tunnel. One is the Mobile IP tunnel between HA and firewall, the other is the reverse tunnel between firewall and MN. Since sending a packet from a MN located within a foreign network cannot be allowed by a firewall, we use reverse tunneling [14]. The basic authentication between the HA and the MN is represented in this scenario. The main reason of this stage of scenario is to get the least computational time for authentication compared with IPSec tunneling.

Scenario 3: IPSec Tunneling with AH. The third scenario is to measure the latency caused by the IPSec tunneling with AH protocol between firewall and MN for secure communication. The processing time of authentication is directly proportional to the type of security algorithm employed. Since there exist no uniform authentication standard in Mobile IP, we have measured the performance influence of authentication algorithm such as HMAC-MD5 and HMAC-SHA1.

Scenario 4: IPSec Tunneling with ESP. Compared with the previous scenario, this scenario provides the confidentiality as well as authentication. The scenario is to measure the latency when applying the IPSec tunnel with ESP protocol. This delay depends on the transported data in the ESP and security algorithm for authentication and encryption. The performance has been measured the total latency and the processing time of cryptographic function. In order to compare the influence of cryptographic function processing, we use the two kinds of hash algorithm such as HMAC-

MD5 and HMAC-SHA1 for authentication, and encryption algorithm such as DES-CBC and IDEA-CBC for encryption.

4.3 Simulation Result

We perform simulations of the scenarios described in section 4.2. Simulation measures the latency involved in the necessary protocol operations. Our objective focuses on the processing overhead of cryptographic operation produced by tunneling mechanism over Mobile IP network. Therefore, we measure the influence of cryptographic processing time in each node on the tunneling mechanism as well as total latency in each scenario. We evaluate the performance of Mobile IP registration using IPSec tunnel according to the following measures: total latency, time spent for cryptography computations, and time spent for message transmission.

Fig. 5 shows total latency of registration in each scenario. Total latency includes the message transmission delay, message generation time for registration request and reply, updating time in table, verification time for nonce or timestamps, and encryption/decryption time. In Fig. 5, the difference between Mobile IP tunneling(scenario 2) and IPSec AH tunneling(scenario 3) in total latency is not noticeable. But, there is a significant difference between IPSec AH tunneling(scenario 3) and IPSec ESP tunneling(scenario 4). Fig. 6 shows the time spent for registration in each node. Since a mobile node has limited resources, the processing time on MN is important. We can see that the processing time produced by a MN in case scenario takes shorter than any other. In the processing time on MN, IPSec AH tunneling is almost same as Mobile IP tunneling. IPSec ESP tunneling is three times longer than basic routing and is 1.7 times longer than IPSec AH tunneling. IPSec ESP tunneling has obvious effect on performance because of encapsualtion. In Fig. 5 and Fig. 6, we can conclude that IPSec AH tunneling is an efficient security mechanism to provide the security service such as authentication and integrity in firewall protected network, even though it doesn't provide the security service such as confidentiality.

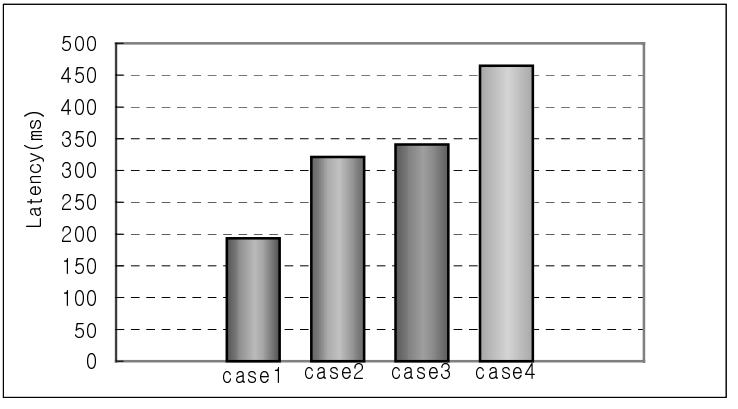

Fig. 5. Total Latency

Fig. 7 shows the cryptographic function processing time of each node according to each scenario. Fig. 8 shows the processing overhead of each node in scenario 3. Fig. 9 indicates the cryptographic processing overhead of each node according to cryptographic function in scenario 4. In Fig. 9, we can find that HMAC-MD5 for authentication algorithm and DES-CBC for encryption algorithm are appropriate.

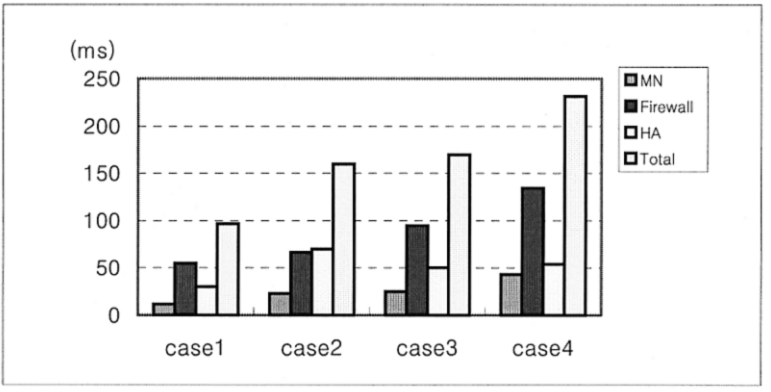

Fig. 6. Processing overhead for registration in each node

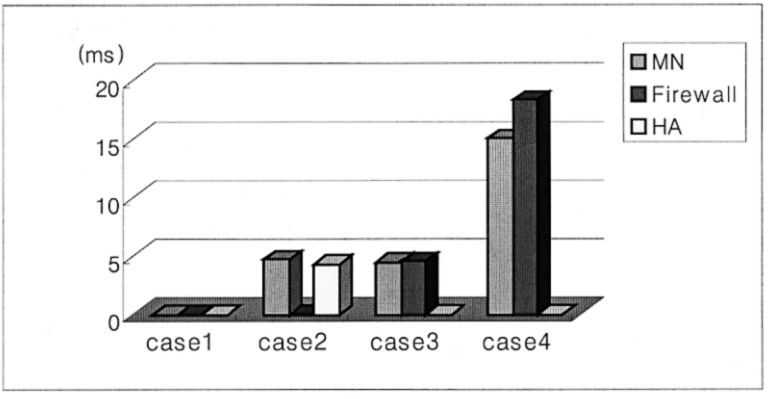

Fig. 7. Cryptographic processing overhead of each scenario

5 Conclusion

In this paper we have proposed the secure tunneling mechanism of combining Mobile IP and IPSec tunnels, which can provide secure traversal of firewall in home network while mobile nodes are roaming abroad. Additional functionality needs to be intro-

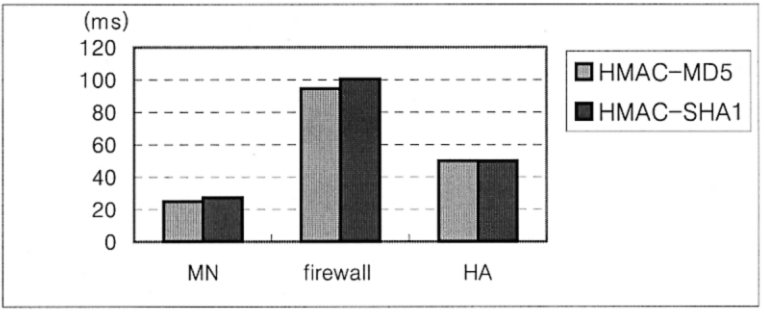

Fig. 8. Processing overhead in Scenario 3

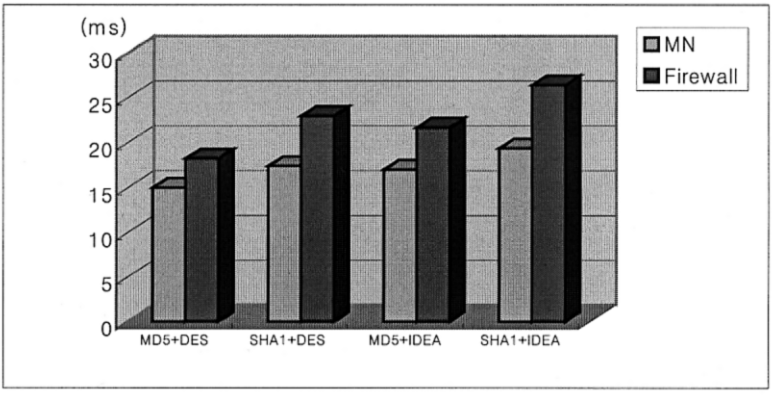

Fig. 9. Cryptographic processing overhead in scenario 4

duced only in the firewall and mobile node for IPSec tunnel whereas the rest of the Internet remains unchanged. The proposed mechanism can be efficiently managed since most function is concentrated in the home network's firewall. The Mobile IP for secure traversal of firewall in home network is transparent to the foreign network, which adds flexibility and efficiency for a network to host Mobile IP nodes and to provide the security services. In mobile networks, mobile nodes will require their security function such as authentication, confidentiality and integrity in a limited time. The proposed tunneling mechanism is not required significant processing overhead on mobile node for security. From simulation results, we may conclude that the proposed mechanism is reasonable performance toward the secure mobility. Our research will be extended to support firewall-protected foreign network and to minimize the delay in frequent handoff.

Acknowledgement. This work was supported in part by the University Research Program of Ministry of Information and Communication, 2002, Korea.

References

1. Internet Engineering Task Force, http://www.ietf.org
2. Perkins, C.: Mobile IP Design Principles and Practices. Addison-Wesley Wireless Communication Series (1997)
3. Perkins, C.: Mobile IP. IEEE Communications Magazine, May (1997)
4. Perkins, C.: IP Mobility Support for IPv4. RFC 3344, Aug. (2002)
5. Kent, S., Atkinson, R.: Security Architecture for the Internet Protocol. RFC 2401, Nov. (1998)
6. Kent, S., Atkinson, R.: IP Authentication Header. RFC 2402, Nov. (1998)
7. Kent, S., Atkinson, R.: IP Encapsulating Security Payload (ESP). RFC 2406, Nov. (1998)
8. Zao, J.K., Condell, M.: Use of IPSec in Mobile IP. Internet Draft Nov. (1997)
9. Binkley, J., Richardson, J.: Security Consideration for Mobility and Firewall. Internet Draft, Nov. (1998)
10. Montenegro, G., Gupta, V.: Sun's SKIP Firewall Traversal for Mobile IP. RFC 2356, (1998)
11. Mink, S., Pählke, F., Schäfer, G., Schiller, J.: FATIMA: A Firewall-Aware Transparent Internet Mobility Architecture. Proceedings of ISCC 2000, Antibes, France, (2000) 172–179
12. Mink, S., Pählke, F., Schäfer, G., Schiller, J.: Towards Secure Mobility Support for IP Networks. (2000) 555–562
13. Droms, R.: Dynamic Host Configuration Protocol. RFC 2131, Mar. (1997)
14. Montenegro, G.: Reverse Tunneling for Mobile IP. RFC 3024, Jan. (2001)