An IPSec-Based Key Management Algorithm for Mobile IP Networks

Neng-Chung Wang[1], Jong-Shin Chen[2], Yung-Fa Huang[2], and Tzu-Wei Chan[3]
[1]Department of Computer Science and Information Engineering
National United University, Miao-Li 360, Taiwan, R.O.C.
Email: ncwang@nuu.edu.tw
[2]Graduate Institute of Networking and Communication Engineering
Chaoyang University of Technology, Taichung 413, Taiwan, R.O.C.
Email: jschen26@mail.cyut.edu.tw; yfahuang@mail.cyut.edu.tw
[3]Department of Computer Science and Information Engineering
Chaoyang University of Technology, Taichung 413, Taiwan, R.O.C.
Email: s9167610@mail.cyut.edu.tw

Abstract: - The Mobile IP network environment for users is very vulnerable to malicious attacks, such as denial-of-service, man-in-the-middle, and other types of attacks. For protection, the IETF standard Mobile IP protocol is modified with IP security (IPSec) primitives, which control the packet flow from a mobile host through multiple security gateways. In addition, IPSec uses strong cryptographic authentication and encryption algorithms to protect the integrity and confidentiality of IP traffic. In this paper, we proposed a key management algorithm for Mobile IP networks based on IPSec. The proposed scheme includes two parts: a wired network and a wireless network. In the wired network part, the proposed scheme produce two keys in each security gateway, transfers a packet with an encrypted key and receives a packet with a decrypted key. In the wireless network part, we use AH to arrive at wireless segment packet security. By the proposed scheme, we can enhance the security of Mobile IP networks.

Key-Words: - Key management, IPSec, Mobile IP, Network security, Private key, Public key.

1 Introduction

The Mobile IP network environment for users is very vulnerable to malicious attacks. IP packets can be easily captured and can be modified and replaced in transit without the destination hosts being able to detect the modifications.

In the wireless networks (for example, Mobile IP, GSM, and 3G), the wireless link is more vulnerable to the attacks, and the mobile devices (for example, Notebook, PDA or mobile phone) are computing-capacity-limited and power-limited. These characteristics raise new challenges in designing the authentication scheme for wireless network [6]. Anonymity and un-traceability is to protect the privacy of the identity of the sender. Also, a user should not be wrongly charged due to any billing errors or any security breaches of any service point. On the opposite, when a malicious user tries to repudiate services, the service provider should provide evidence to convince users the services.

In Mobile IP networks, each mobile node has a fixed IP home address belonging to the home network. The home network is unique to a given mobile node, having its prefix matching the home address of the mobile node. While roaming away, the mobile nodes receive packets addressed to their home address and forwarded to their present location by a fixed node residing in the home network called home agent. A home network can host a large number of mobile nodes. While these nodes are away, one single home agent must forward IP datagrams, maintain caches and manage registration messages for all the roaming nodes.

IP mobility working on OSI layer 3 [1] is intended to provide Internet connectivity to mobile hosts when they are away from their home network and on a visiting network. The Internet Engineer Task Force (IETF) formed the IETF Mobile Working Group to draw up a standard of mobility support for IPv4, called Mobile IP [14].

IP security (IPSec), a protocol suite defined by IETF, enables systems to select required security protocol. The selected protocols choose the cryptographic algorithms that are to be used, and generate and put in place any cryptographic keys that are necessary to provide the requested services. IPSec provides connectionless data integrity, authentication, data confidentiality, anti-replay protection, data origin authentication, and limited traffic flow confidentiality. In [5], Johnson et al.

proposed a security support in Mobile IP networks. Mobility has become the most imperative demand in recent spreading networking systems. For IPSec-based VPN users, Mobile IP developed by IETF is considered as the best solution for mobility management protocols [19].

In this paper, we proposed a new scheme to solve security problems in a Mobile IP environment. The proposed architecture is based on the IPSec-based VPN proposed by the IETF for mobile users. For IPSec-based VPN users, Mobile IP developed by the IETF is considered as the best solution for mobility management protocols. The proposed scheme consists of two parts: a wired network and a wireless network. In both networks, we use IPSec to enhance the security of our scheme. IPSec offers these services at the network layer, the layer in the TCP/IP protocol stack that contains the IP protocol. We change the way of one key in tradition as the method of two keys. In Mobile IP environment the agent that the packet must pass by is too many. So that very easy were invaded by the hacker or the password is cracked. Two keys absolutely can increase the safety.

The rest of the paper is organized as follows. In Section 2, we give an overview of Mobile IP and IPSec. We present the proposed IPSec-based key management algorithm for Mobile IP networks in Section 3. In Section 4, we compare IPSec-based Mobile IP with traditional Mobile IP. We give the conclusions in Section 5.

2 Overview of Mobile IP and IP Security (IPSec)

In this section, we give an overview of the Mobile IP and IP security protocol and describe them in some detail.

2.1 Main Component of Mobile IP

The basic concept of Mobile IP is as follows. Each MN must have a home address in its home network. When visiting any network away from home, each MN gets a temporary local address, called care-of address (CoA) [18]. On the visited network, the MN registers with its home agent so that the MN's current IP address can be tracked. Based on this concept, the functional components of Mobile IP are as follows [18]:

(1) Mobile node (MN): A host that changes its point of attachment from one network to another is called a mobile node (MN).
(2) Home agent (HA): A router on an MN's home network is called the home agent (HA), which maintains current location information on the MN and on tunnel datagrams.
(3) Foreign agent (FA): A router on an MN's visited network is called the foreign agent (FA), which provides routing services to the MN while the MN is registered with the HA.
(4) Correspondent node (CN): A peer with which a mobile node communicates is called the correspondent Node (CN). A CN may be either mobile or stationary.

2.2 Basic Operations of Mobile IP

Fig. 1 shows the operations of the Mobile IP protocol [16]. With Mobile IP, a mobile node (MN) has a home agent (HA) that is a router attached to the network to which the node belongs. When the HA is out of range, the MN can connect to a foreign agent (FA) that communicates with the HA to help keep track of the MN. The MN must then be able to have an IP address that associates it with its attachment to a particular network. The FA assigns a care-of address (CoA) that is used for communicating with the MN while the MN is on the visited network. The MN can send and receive packets from any type of node on the network. When communication is taking place between an MN and another node, the node that the MN is communicating with is referred to as the correspondent node (CN).

In the following, we briefly investigate the basic operations of standard Mobile IP. There are five main operations in the standard Mobile IP proposals. The five operations are mobile agent discovery, registration, tunneling, binding update, and foreign agent smooth handoffs.

(1) Mobile agent discovery: Mobile agents advertise their presence via agent advertisement messages. MNs determine if they are still linked to the home network using the source IP address in the advertisement message.
(2) Registration: The process by which an MN requests routing services from an FA on a foreign network, informs its HA of its current CoA, renews a registration which is due to expire, and deregisters with the HA when it returns to its home network. The registration process consists of an exchange of a registration request message and a registration reply message between an MN and its HA, possibly involving an FA.

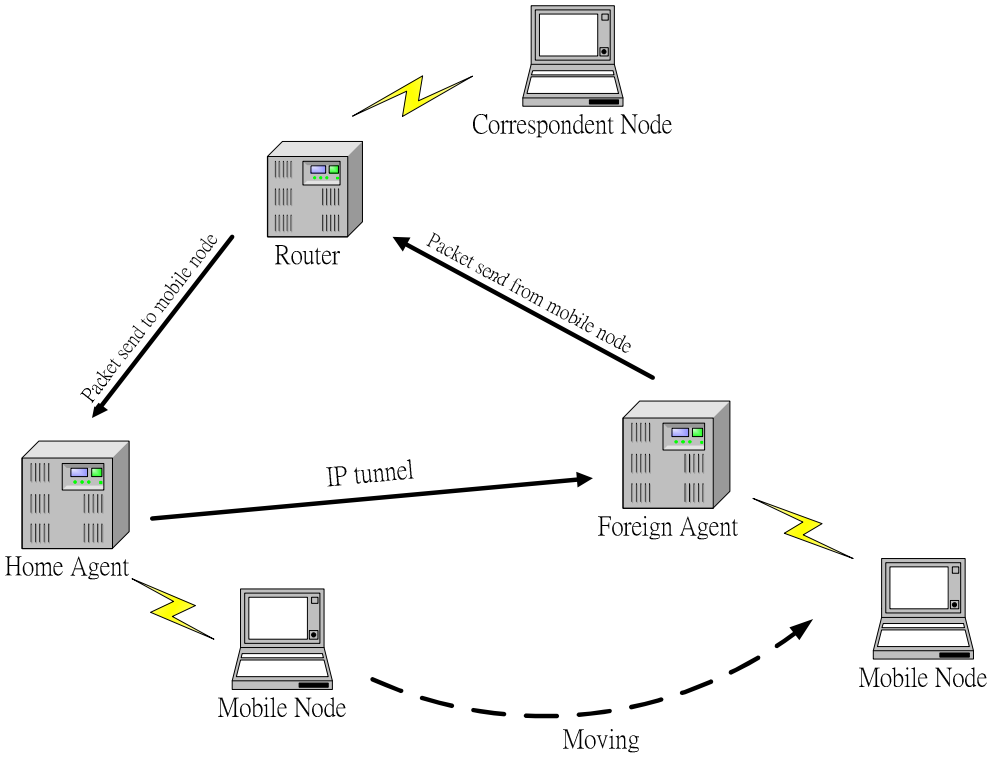

Fig. 1. Operation of the Mobile IP protocol.

(3) Tunneling: The mechanism by which the HA forwards the packets to the MNs. Using this mechanism, the IP packets are placed within the payload part of new IP packets, and the destination address of the encapsulating IP header is set to the MN's CoA.
(4) Binding update: In the absence of any binding cache entry, the packets destined to an MN will be routed to the MN's home link in the same way that any other IP packet would be, and then will be tunneled to the MN's current CoA by the MN's HA. If the CN had a binding cache entry for the MN, it would be able to send packets directly to the MN without the services of the HA.
(5) Foreign agent smooth handoffs: This operation is useful for defining a smooth handoff mechanism when an MN moves from one foreign network to another. During registration with the new FA, the MN requests the new FA to send a binding update message to the previous FA. This node will then be able to re-tunnel the packets destined to the MN.

2.3 Overview of IP Security (IPSec)

IPSec is a protocol suite defined by the IETF to secure IP packet exchanges [12]. Many researches have focus on the IPSec application systems [3, 11, 15]. the IPSec is designed to provide high-quality, interoperable, cryptographic-based security for Ipv4 and Ipv6 datagrams through the use of cryptographic key management protocols [2], such as the Internet Key Exchange (IKE) protocol [4]. Two new security headers are defined in IPSec: an authentication header (AH) [7] and an encapsulating security payload (ESP) [8]. The primary difference between AH and ESP authentication is the extent of coverage. ESP does not authenticate any IP header fields in the outer IP header. AH can provide better integrity check. It protects predictable fields in the outer IP header. In IPSec, AH provides data integrity and authentication using the hashing algorithms Message Digest Algorithm 5 (MD5) and Security Hash Algorithm (SHA-1) [13]. The ESP header provides integrity, authentication, and confidentiality to each IP packet. By using the MD5 and SHA-1 algorithms, ESP provides encryption algorithms like Digital Encryption Standard (DES) and Triple Digital Encryption Standard (3DES) [10].

IPSec was designed to prevent the spoofing of IP addresses, and any form of tampering with and replaying of IP datagrams, and to provide confidentiality and other security services for IP datagrams. IPSec offers these services at the network layer level, the layer in the TCP/IP protocol stack that contains the IP protocol. IPSec enables systems to select the required security protocols, chooses the cryptographic algorithms that are to be used with the selected protocols, and generate and

put in place any cryptographic keys that are necessary to provide the requested services.

3 An IPSec-Based Key Management Algorithm

In Mobile IP, there are home and foreign agents running on a wired network. These mobile agents (MAs) periodically broadcast Mobile IP advertisements on wireless networks. Whenever an MN migrates from one subnet to another (foreign) subnet, it starts receiving Mobile IP advertisements from the corresponding foreign agent.

An MN is any type of device that can be attached to the Internet. It can be a wireless laptop, a personal digital assistant (PDA), or an Internet-enabled mobile phone [12]. In the proposed scheme, an IPSec protection model is used to replace the Mobile IP model. IPSec is a standard mechanism for providing secure communications over the Internet [10].

Fig. 2 shows the packet format encrypted with a public key on a wired network. The proposed scheme transfers a packet with an encrypted key and receives a packet with a decrypted key. Hacker most easily invades wired networks. This scheme at each agent all the new IP header of the needle does to encrypt. That can increase and the safety of the packet, but can not increase and made the loading too much.

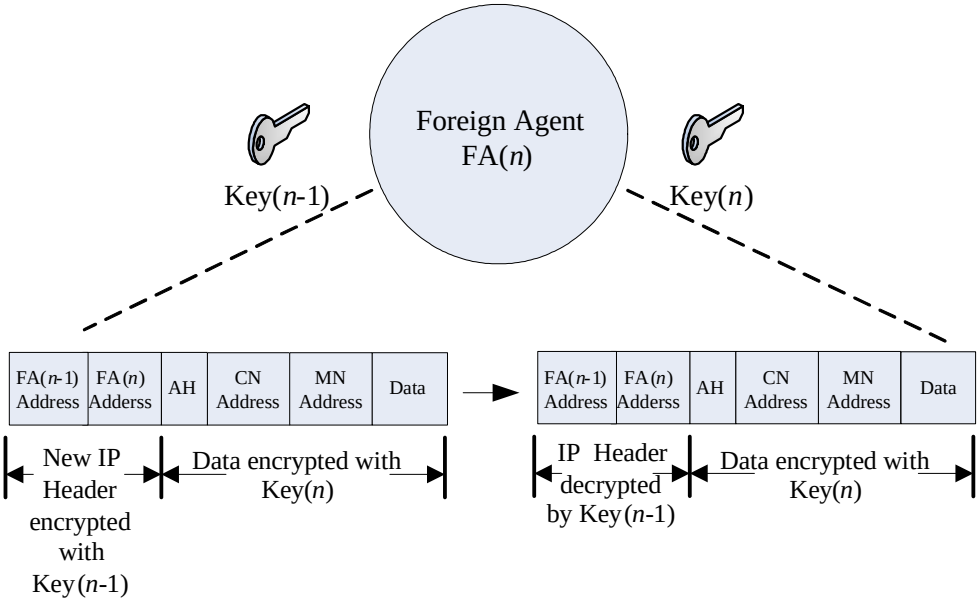

Fig. 2. Packet format encrypted with a public key on the wired network.

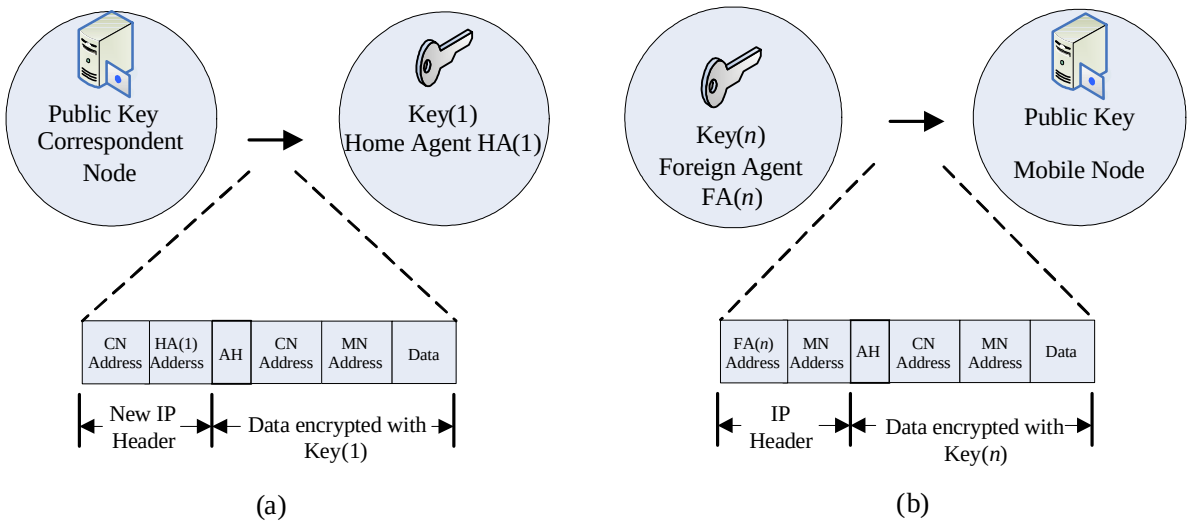

Fig. 3. Packet format encrypted with AH on the wireless network. (a) CN→HA. (b) FA→MN.

As shown in Fig. 3, we use AH to arrive at wireless segment packet security in wireless networks. In the proposed scheme, we describe how we use Key(i-1) of gateway i to decrypt a received packet. Then we use Key(i) of gateway i to encrypt a transferred packet. In the following, we will present the operations on a wired and a wireless network, respectively.

3.1 Operations on the Wired Network

In the following, we describe the method of operation of our proposed scheme on a wired network. Fig. 4 shows the packet format encrypted with a public key. We will first describe the basic ideas of the routing process and then proceed to describe the data transfer process. We will then describe the data reception process using the IPSec-based security method.

(1) Route Discovery Process

We assume that parameter "n" represents a count of hops from the HA to the FA. To allow for practical deployment requires that we "over-load" existing header fields in a manner that will have minimal impact on existing users. We describe our proposed encoding below. We can adopt any reasonable encoding that comes to light. Fig. 5 shows our choice for using the padding field. Five bits are sufficient to represent 31 hops, which is more than almost all Internet paths [16]. In the common case, the only modification to the packet is to increment its padding field.

The route discovery process is described as follows:

Step 1: First, we assume that parameter "n" represents the number of hops from the HA to the FA. Parameter "k" represents every gateway's number. Each agent stores k in each gateway register.

Step 2: The FA produces or obtains a random security key and stores it in Key(k). Key(k) is used later in the routing process to decrypt a packet. The process will record the parameter "k" into the packet.

Step 3: If gateway k receives the request message, this means this path has already arrived at the last agent. If gateway k does not receive the request message, the routing process stops. The packet will be transmitted to the last agent.

Step 4: When this packet is transferred to the last agent, this packet will store Key(k) and Key(k-1) to the register of gateway k, where k>1. When the routing process is finished, every agent (HA or FA) will obtain two keys.

This scheme mainly produces the public key which passes every FA, and saves the public key in the register in each agent (HA or FA). The route discovery procedure is shown in Algorithm 1.

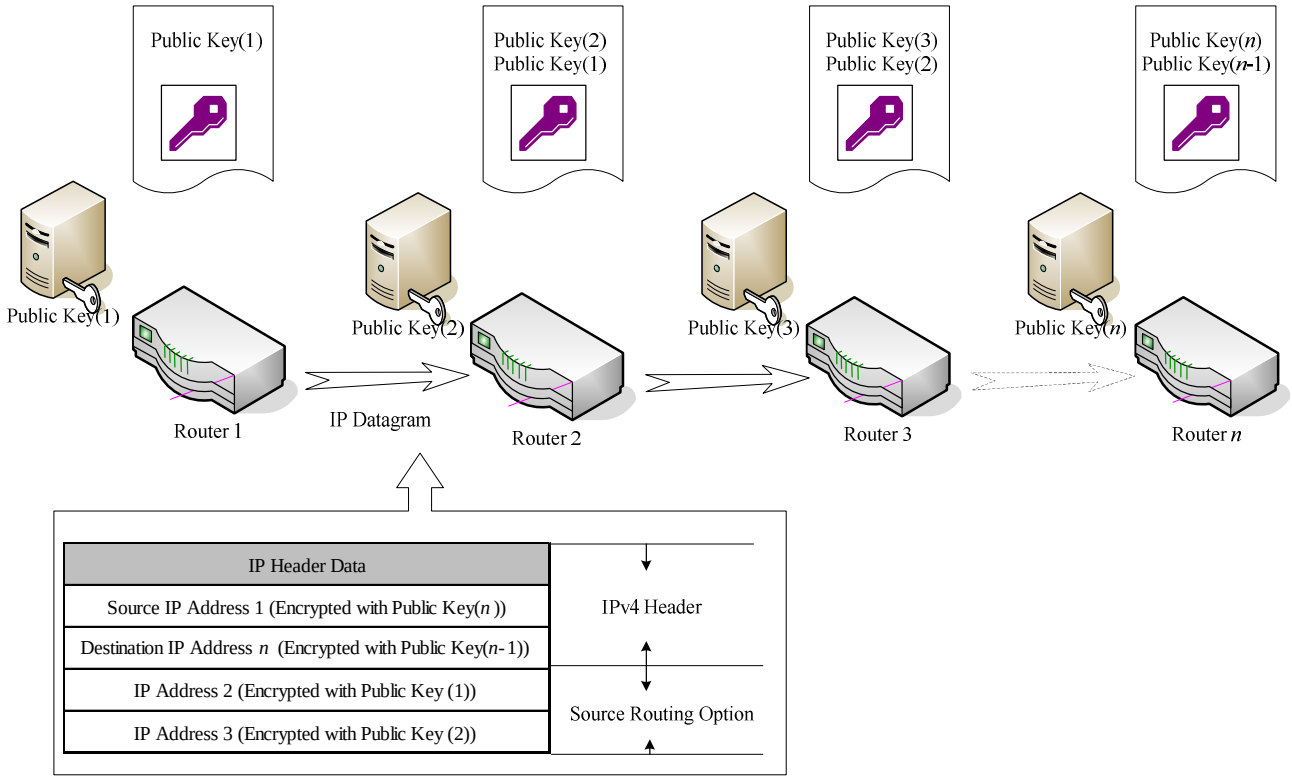

Fig. 4. Packet format encrypted with a public key.

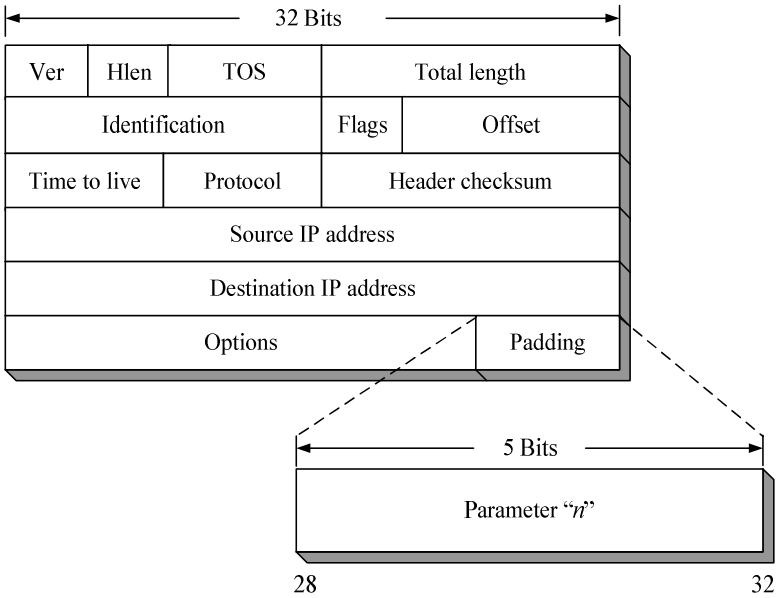

Fig. 5. Encoding parameter "*n*" into the IP padding field.

Algorithm 1: Route discovery process
Begin
Assume *n* is the number of gateway (HA or FA) nodes
Assume *k* is the number of last gateway nodes
If the packet is at the home agent
n = 1
Else
n = *n* + 1
k = *n*
Store *k* in gateway register
Endif
Assign a public key to Key(*n*) in gateway *n*
Record *n* into the packet
If gateway *n* receives the request message
k = *n*
Store Key(*k*) and Key(*k*-1) in the gateway register
k = *k* – 1
Endif
End

(2) Data Transfer Process
A CN delivers packets to the MN through the HA to FA(*n*). In this case, each mobile agent has two keys: one is Key(*k*) and the other is Key(*k*-1), where *k*>1. Key(*k*) is used to encrypt Mobile IP packets, and Key(*k*-1) is used to decrypt the received packets.

The data transfer procedure is given in Algorithm 2.

Algorithm 2: Data transfer process
Begin
Assume *n* is the number of gateway (HA or FA) nodes
Assume *k* is the number of last gateway nodes
If the packet is at the home agent
n = 1
Else
Get Key(*n*-1) from gateway *n*
Decrypt the IP header using Key(*n*-1)
Endif
Get Key(*n*) from gateway *n*
Encrypt the IP header using Key(*n*)
If gateway *n* receives the request message
k = *n*
Get Key(*n*-1) from gateway *n*
Decrypt the IP header using Key(*n*-1)
Else
n = *n* + 1
Endif
End

(3) Data Reception Process
Packets are delivered to the HA through FA(*n*). Key(*k*) is used to encrypt the Mobile IP packets, and Key(*k*-1) is used to decrypt the received packets, where *k*>1. For instance, when a packet is delivered to FA(*k*-1), FA(*k*-1) will decrypt the received packets with Key(*k*-1), and use Key(*k*) to encrypt the packets, after which the packets are sent out.

The data reception process is given in Algorithm 3.

Algorithm 3: Data reception process
Begin

Assume n is the number of gateway (HA or FA) nodes
Assume k is the number of last gateway nodes
If the packet is at the last gateway node
    $n = k$
Else
    Get Key(n) from gateway n
    Decrypt the IP header with Key(n)
    $n = n - 1$
Endif
If the packet is at the home agent
    Get Key(n) from gateway n
    Decrypt the IP header with Key(n)
Else
    Get Key(n-1) from gateway n
    Encrypt the IP header with Key(n-1)
Endif
End

3.2 Operations on the Wireless Network

Wireless network security differs from general computer and network security in that air link is involved, and a wireless network is most concerned with the edges of the network. Good security should be an added feature in existing wireless communication devices. Users that do not need it should not have to pay for it. On the other hand, users that want very secure communication devices should have that option available to them at an acceptable cost. For example, users could be offered the use of compatible but specialized user equipment when better security is needed. This is already being done in some cellular systems for large-scale emergency communications where public safety officials are issued special cell phones that have good interference immunity and priority access to the cell tower.

IPSec provides security by implementing different security algorithms. IPSec adds two specific headers: an authentication header and an encapsulating security payload. The authentication protection in AH does not allow this mode of operation. The AH protocol was designed to improve the security of IP datagrams. The AH protocol provides connectionless integrity, data origin authentication, and an anti-replay protection service. However, AH does not provide any confidential services: it does not encrypt the packets it protects. AH's role is to provide strong cryptographic authentication for IP traffic to ensure that packets that are tampered with will be detected. We show a simple authentication header model for Mobile IP in Fig. 6. The two authentication algorithms in the IP Authentication Header and Encapsulating Security Payload are the HMAC-MD5 and HMAC-SHA-I algorithms [13, 17]. MD5 and SHA-I have many similar characteristics.

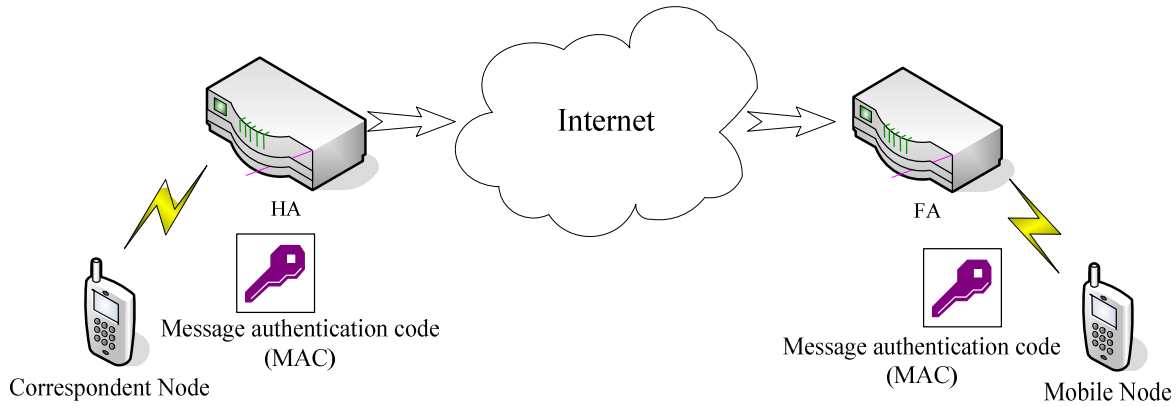

Fig. 6. A simple authentication header model for Mobile IP.

Encryption, key distribution, and PKI are closely related in building trust for businesses in the enterprise. Without this element of trust, MVPN would be a minor factor for corporate business transactions. The topics in this section not only basic encryption techniques but also a full packaging and implementation of such techniques to secure communications over an untrusted medium such as the Internet.

These secure communications protocols are prominently used in VPN today:

1. Secure electronic transaction (SET): Not yet widely supported, SET's origins from Vusa, MasterCard, Microsoft, Netscape, and others make it important for VPN. Designed for secure payments, SET supports DES and RC4 encryption and RSA for digital signatures, key distribution, and public key encryption of the bankcard numbers used.

2. Certificate Authorities (CAs): A CA, which is simply another server on a LAN attached to the Internet, provides the additional protection to conduct secure Internet cash transactions. CAs issue certificates to identify network users and systems. The CA verifies its certificates by digitally signing the certificates it issues. A public key inside the certificate indicates the certificate is legitimate and can be trusted. After a CA becomes a trusted source, it becomes the third party in a trust relationship, similar to a notary public. The other two parties are typically a client and a server that have chosen to communicate in a secure environment.
3. PKI Exchange (PKIX): A way to combine PKI with X.509 certificate uses over the Internet.
4. Simple PKI (SPKI): Another Internet initiative to simplify use of PKI and standardize the public key certificate format and associated key acquisition protocols.
5. Secure sockets layer (SSL): The most widely used Web site and Internet secure protocol. Invented by Netscape, SSL protects all TCP/IP applications and Web sites. SSL uses MD5 for message digests, and allows a variety of encryption techniques (DES, IDEA, RC2, RC4, or RSA).

In this case, we use AH to arrive at wireless segment packet security. Fig. 7 shows two methods in which the IPSec authentication services can be used. Fig. 7(a) shows typical IPv4 packets. In this case, the IP payload is a TCP segment; it could also be a data unit for any other protocol that uses IP, such as UDP or ICMP. For AH transport mode using IPv4, the AH is inserted after the original IP header and before the IP payload (e.g., TCP segment). This is shown in Fig. 7(b). For AH tunnel mode, the entire original IP packet is authenticated, and the AH is inserted between the original IP header and a new outer IP header. This is shown in Fig. 7(c).

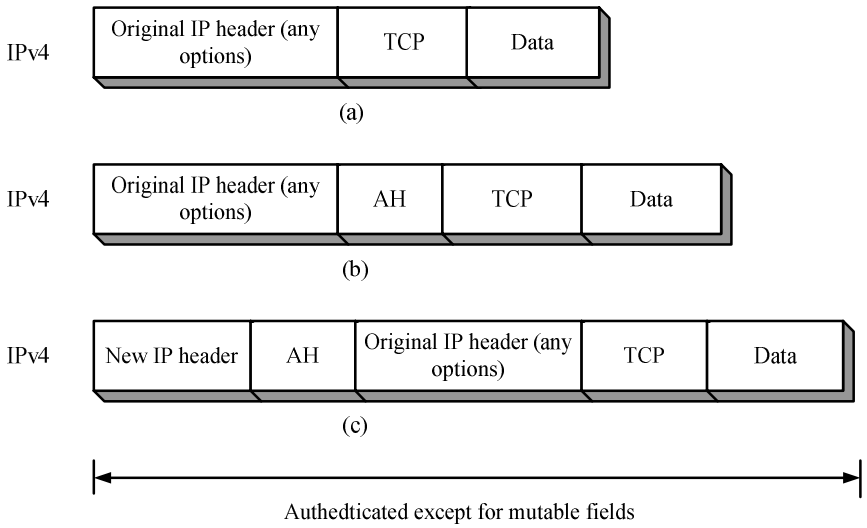

Fig. 7. The authenticated packet format except for mutable fields. (a) Before applying AH. (b) Transfer mode after applying AH. (c) Tunnel mode after applying AH.

4 The Comparisons between IPSec-Based Mobile IP and Traditional Mobile IP

The comparisons of IPSec-based Mobile IP and traditional Mobile IP networks are described as follows.

The IPSec-based Mobile IP networks works on the peer-to-peer mode and the use to operate on MVPN. Oppositely, the traditional Mobile IP networks works on the client/server mode. When it is used to implement MVPN, the compulsory tunnel style must be used and one MVPN device need to implement the access concentrator (AC) function while another need to implement the network server (NS) function. To make them symmetrical, both MVPN devices need to implement AC and NS functions. Obviously, it will increase the implementation overhead and the complexity of configuration and management operations.

Traditional Mobile IP does not provide any security mechanisms or only provides very weak security mechanisms. IPSec-based Mobile IP supports two security protocols: one is the IP

authentication header protocol which is used to provide data origin authentication, data integrity, and anti-replay protection; the other is the IP encapsulating security payload which provides data confidentiality, limited traffic flow confidentiality and optional data origin authentication, data integrity, and anti-reply protection. According to the security requirements, they can be used in speared or combined ways. In addition to the security protocols, IPSec also provides complete key management protocols, such as the Internet Key Exchange (ISAKMP/Oakley) protocol.

In an IPSec-based Mobile IP network, when we send a packet from the source to the second security gateway, a hacker can use a private key to unlock the next security gateway's IP address. This means the hacker can know the real address of the next hop. But that does not present a problem since the hacker still does not know what the packet's destination IP address is. In the proposed scheme, each security gateway has two keys. One is Key(i) and the other is Key(i-1). When a hacker invades a security gateway, he can only get the Key(i) of that security gateway. The hacker cannot decrypt the received packet. Therefore, the proposed method is safer than the traditional method.

5 Conclusions

With recent advances in wireless communication technology, mobile computing is an increasingly important area of research. End-to-end network security mechanisms, such as IPSec and the rich network services for wireless networks, are fundamentally conflicting mechanisms. In this paper, we proposed a key management algorithm for Mobile IP networks based on IPSec. The proposed scheme includes two parts: a wired network and a wireless network. In the wired network part, the proposed scheme produce two keys in each security gateway, transfers a packet with an encrypted key and receives a packet with a decrypted key. In the wireless network part, we use AH to arrive at wireless segment packet security. By the proposed scheme, we can enhance the security of Mobile IP networks.

Acknowledgments

This work was supported by the National Science Council of Republic of China under grants NSC-94-2213-E-324-025 and NSC-95-2221-E-239-052.

References:

[1] I. F. Akyildiz, J. Mcnair, S. M. H. Joseph, H. Uzunalioglu, and W. Wang, "Mobility Management in Next-Generation Wireless System," *Proceedings of the IEEE*, Vol. 87, No. 8, pp. 1347-1348, August 1999.

[2] R. Atkinson, "Security Architecture for the Internet Protocol," *RFC-1825*, August 1995.

[3] J. M. Diez, S. Bojanic, C. Carreras, and O. Nieto, "FPGA Implementation of Three IPSec Cryptographic Algorithms," *WSEAS Transactions on Systems*, Vol. 2, Issue 1, pp. 229-234, January 2003.

[4] D. Harkins and D. Carrel, "The Internet Key Exchange (IKE)," *RFC 2409*, Internet Society, Network Working Group, November 1998.

[5] D. Johnson, C. Perkins, and J. Arkko, "Mobility Support in IPv6," *RFC 3775*, June 2004.

[6] W. S. Juang, C. L. Lei, and C. Y. Chang, "Anonymous channel and authentication in wireless communications," *Computer Communications*, Vol. 22, pp. 1502-1511, May 1999.

[7] S. Kent and R. Atkinson, "IP Authentication Header (AH)," *RFC 2402*, Internet Society, Network Working Group, November 1998.

[8] S. Kent and R. Atkinson, "IP Encapsulating Security Payload (ESP)," *RFC 2406*, Internet Society, Network Working Group, November 1998.

[9] S. Kent and R. Atkinson, "Security Architecture for the Internet Protocol," *RFC 2401*, Internet Society, Network Working Group, November 1998.

[10] D. Khatavkar, E. R. Hixon, and R. Pendse, "Quantizing the Throughput Reduction of IPSec with Mobile IP," *Proceedings of the 45th Midwest Symposium on Circuits and Systems* (MWSCAS-2002), pp. 505-508, August 2002.

[11] J. Lim, M. Han, and K. Kim, "Application of IKE Protocol for IPSec VPN Into Embedded System," *WSEAS Transactions on Communications*, Vol. 4, Issue 9, pp. 876-880, September 2005.

[12] M. L. Maknavicius and F. Dupont, "Inter-Domain Security for Mobile IPv6," *Proceedings of the Second European Conference on Universal Multiservice Networks* (ECUMN 2002), Evry, France, pp. 238-245, April 2002.

[13] H. E. Michail, A. P. Kakarountas, A. Milidonis, and C.E. Goutis, "Efficient Implementation of the Keyed-Hash Message Authentication Code (HMAC) using the SHA-1 Hash Function,"

Proceedings of the IEEE International Conference on Electronics, Circuits and Systems (ICECS 2004), pp. 567-570, December 2004.

[14] C. E. Perkins, "IP Mobility Support," *RFC 2002*, Mobile IP Working Group, October 1996.

[15] C.-W. Tan, M. Benz, and A. Schill, "A 10 Gbit/s IPSec Gateway Implementation," *WSEAS Transactions on Communications*, Vol. 3, Issue 1, pp. 205-211, January 2004.

[16] W. Theilmann and K. Rothermel, "Dynamic Distance Maps of the Internet," *Proceedings of the IEEE INFOCOM*, vol. 1, pp. 275–284, Mar. 2000.

[17] S. Vaarala and E. Klovning, "Mobile IPv4 Traversal across IPSec-Based VPN Gateways," *RFC 5265*, Network Working Group, June 2008.

[18] I.-W. Wu, W.-S. Chen, H.-E. Liao, and F.-F. Young, "A Seamless Handoff Approach of Mobile IP Protocol for Mobile Wireless Data Networks," *IEEE Transactions on Consumer Electronics*, Vol. 48, No. 2, pp. 335-344, May 2002.

[19] R. Younglove, "Virtual Private Network - How They Work", Computing & Control Engineering Journal, December 2000.