Securing Mobile IP Registration Messages in Residential Networks

Young-bai Kim, Seung-jo Han*

Abstract— **Residential network is the hybrid technology of wireless, Ethernet, Bluetooth and RF to the internet via broadband connection at home to facilitate the convenient, safe and pleasant daily lives of home user with various home network services regardless of device, time and place. For ubiquitous development more devices will be wireless and most of them will be roaming. Since these roaming devices carry private information of daily life of residential users, the interaction among the roaming devices of residential network must be secure. This paper presents to secure registration of roaming devices using IP Security (IPSec) Protocol Suite without the need to trust foreign agents.**

Index Terms— Residential Networks, Roaming Device, IPSec, Mobile

I. INTRODUCTION

Residential network is not an entirely new network system but the integrated technology of wired and wireless network for a variety of purposes - from connecting multiple personal computers for printer, file and Internet connection sharing, to networking home entertainment systems and home automation [1]. This kind of integrated technology has been developed for providing comfortable and safe life of residential users. Figure 1 depicts the general residential network model which integrates powerline, Ethernet, wireless and phoneline technologies at the residential gateway which is connected to the outside world via internet through broadband internet connection. However, more and more devices are wireless because of the ability to control or access networked devices from anywhere in the residence. Emerging wireless home networking technologies in these devices include the 802.11 wireless LAN standard and low cost technologies such as Bluetooth and Home RF. If security mechanisms are not properly implemented in such hybrid networks, the wireless part could provide an entry point for malicious entities [2].

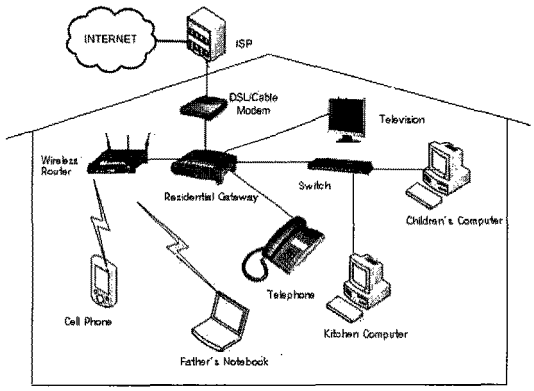

Fig. 1. General Residential Network Model.

Currently, there is a worldwide trend towards ubiquitous home. For ubiquitous home, multi-home roaming enables a device to move from one residence to another [3]. While roaming, attackers can spoof packets transmitted over wireless links, hence mobile users must be authenticated safely. Moreover residential network is subjected to various attacks of internet since it is connected to internet. A natural way to provide security to Mobile IP users and internet attacks is to use the IP Security protocol suite. The IPSec tunnel provides authentication, integrity, and privacy of each IP packet. Since wireless sector is hugely insecure zone of residential network, we propose to secure the mobile IP registration messages for roaming residential mobile nodes into foreign networks using IPSec. We have proposed the simple steps involved in securing Mobile IP registration messages when a residential mobile node moves to foreign networks.

In this paper, we propose to use an IPSec tunnel to protect the Mobile IP tunnel between residential gateway and mobile node, which traverse the insecure parts of the internet. In our work there is no need of foreign network be trusted in the process of Mobile IP registration. The trusted entity in the residential network that provides this capability is secure residential gateway (SRG). All registration packets over the Internet are authenticated and encrypted by IPSec. The IPSec tunneling mechanism provides authentication, integrity and replay protection of all IP packets sent during Mobile IP registration.

This paper is organized as follows; section 2 focuses on security implementation of Mobile IP using IPSec. Section 3 describes the proposed protocol used to secure

Manuscript received December 24, 2009; revised January 15, 2010; accepted January 29, 2010.

Young-bai Kim is with the Department of Information and Communication, Chosun University, Gwang-ju, 501-759, Korea (Email: newromeo12@naver.com)

Seung-jo Han is with the Department of Information and Communication, Chosun University, Gwang-ju, 501-759, Korea (Email: sjbhan@chosun.ac.kr)

*Corresponding author: Seung-jo Han

mobile registration messages between the roaming mobile SMN and the home agent in residential network. Section 4 performs the analysis of proposed protocol in terms of security. Finally it concludes with future works in section 5.

II. SECURITY IMPLEMENTATION

When we implement IPSec in any network, it is important to explore what sort of network entities should be enabled with IP sec to secure the whole network because a secret key should be shared between those entities to create IPSec tunnel. As mentioned in [4] it is generally relatively easy to install a shared secret between mobile node and its home agent, because these systems belong to the same residential network. A much more difficult task is to install a secret key between a mobile node and foreign networks. Foreign networks may or may not employ IP layer security. Furthermore, home network might not trust the foreign network to be involved in securing the roaming mobile node as explained in [4]. So in this paper we do not involve foreign agents in foreign residential networks for security establishment to reduce the security association overhead to residential network's home agent. Only the home agent and mobile nodes need to have IPSec. Residential gateway, which is the heart of the residential network connected to the outside world, can also act as home agent for mobile IP operations. So both mobile IP operations and IP sec is handled in residential network by residential gateway. Since this gateway is intended to use for security of residential network, we term it as Secure Residential Gateway. Residential mobile node maintains a single security association between itself and the residential gateway despite the location of mobile node. Unlike the proposed protocol in [5] the foreign agent is only responsible for agent discovery and relaying packets to SRG. Hence roaming mobile is always protected hence it is termed as secure mobile node (SMN) in our proposed protocol. This implementation allows IPSec to operate in a seamless manner when mobile node roams. The SRG and SMN are both responsible for encryption, decryption operation of IPSec and also encapsulation and encapsulation operations of Mobile IP for secure Mobile IP Communication.

III. PROPOSED PROTOCOL

When SMN visits a foreign residential network, it waits for an advertisement from or sends a solicitation message to the foreign agent informing its presence. The mobile node hence obtains a care-of-address (CoA) from foreign agent. Then it has to inform the home agent in residential network, i.e. SRG about the new IP address according to mobile IP concept. To send the registration message securely over the insecure zone of internet and wireless we have proposed to run IPSec tunnel mode between SRG and its SMN. So SRG sets up an SA (Security Association) for each SMN in its network. To achieve this, SMN and SRG share a security association to authenticate the registration information. So SMN sends an encrypted registration request with care-of address info using UDP securely as follows.

Registration Request

$MSG_{MR} = <IP_M, IP_R, LT, n_1, (K_{MR}, n_1, IP_M)K_{MR}>$

Where,

M	The Mobile Node
R	The Residential Gateway of M
K_{AB}	Shared secret key between A and B
IP_A	The IP address of device A
N_i	Nonce i
MSG_{AB}	A message sent from entity A to entity B
<...>	Contents of the message
LT	Lifetime
()X	The contents of the parentheses are encrypted by the key X
P_A	Public key of A

Mobile forwards this encrypted to the foreign agent and the foreign agent extracts the IP address of residential gateway where it has to transfer the encrypted packet. The foreign agent here is only used for forwarding packets. It is not involved for security purposes of the registration messages and also for communication between roaming devise and the residential gateway. The foreign agent here is only involved for forwarding packets between mobile node and the secure residential gateway and also for ending agent solicitation messages to let the mobile node know that it has visited different network.

After the secure residential gateway receives the registration request from the foreign agent, it decrypts the encrypted registration information and confirms that the request is from its own mobile node as the secret key is only shared between the residential gateway and mobile node. Then it sends the registration as follows with a session key so use by the mobile node after the registration during that particular session.

Registration Reply

$MSG_{RM} = <(K_{MR}, n_2, SK_{MR})K_{MR}>$

Where,

SK_{AB} Session Key between A and B

The foreign agent upon receiving the registration reply from the secure residential gateway forwards to the

destined mobile node and mobile node encapsulates the packet with shared secret key and confirms the registration process is complete. It extracts the session key sent by the residential gateway in encrypted message and uses that key for the secure communication with residential gateway during that session. Hence the communication between the mobile node and the residential gateway is secured. The step involved in proposed protocol is depicted in the figure 2.

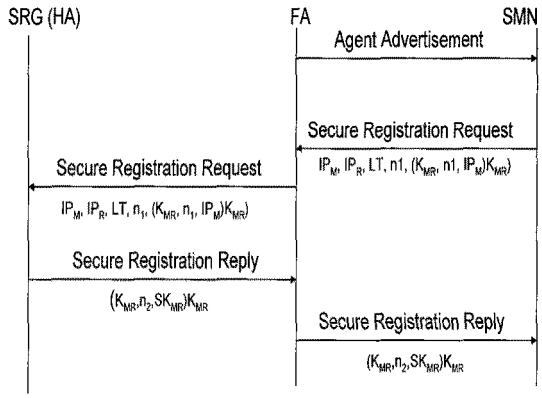

Fig. 2. Message Flow chart of proposed protocol.

IV. SECURITY ANALYSIS OF PROPOSED SCHEME

As we have focused on securing mobile communication integrating IPSec with Mobile IP, the security benefits of the proposed protocol are briefly described below.

Scalable Security

This protocol does not require any security relationships between the residential network and any other foreign networks. So it can easily be extended to cover any number of networks. Hence this protocol seems to be scalable for residential devices roaming in any networks.

Efficiency

The protocol seems to be efficient in the sense that only two messages between the mobile node and residential gateway are involved and thus only the least amount of delay is incurred while establishing a connection at a new network. Furthermore, it exposes the network to the minimal increase in traffic.

Key Management

No secret keys are needed to be installed between the residential gateway and each foreign agent. Thus, key management becomes easier as compared to shared secret key management.

Integrity

Every registration message is encrypted and hence the resulting cipher text cannot be altered by any hackers. This ensures the integrity of messages reaching any destination.

Confidentiality

The proposed protocol sends the secret session key to the SMN to be shared and encrypted by their respective keys during a session. Hence this protocol maintains confidentiality too.

Authentication after Registration

The protocol authenticates not only during registration but also after registration since this protocol generates a new session key every time a new registration occurs. This session key acts as a shared authentication secret between the SMN and its SRG during session lifetime.

V. SIMULATION

Simulation of roaming mobile device of residential network into foreign network was performed using OPNET modeler version 14.5 [6] as shown in figure 2. We performed the simulation configuring IPSec in SMN and SRG in order to secure Mobile IP Communication from SMN to Residential Network. It is assumed that the residential network is secure inside. So we focused in securing communication over the wireless and the internet while the SMN moves from residential network to foreign network. As residential network communication is assumed to be communication between residential devices we assumed CN is at home network and SMN roams from home network to foreign network. In residential network the devices may be mobile or wired. We chose CN as wired device which connected to residential gateway through wired connection which communicates with the SMN since SMN is at home and roams to different network as depicted in Fig. 2. The simulation was run for 10 minutes where the mobile node which was communicating with CN roamed into foreign network at around 7 minutes and 15 seconds.

The Foreign Agent in foreign network here is used for broadcasting advertisement messages periodically, assign CoA to roaming SMNs in its network and forward the messages sent by SMN and SRG. After getting CoA, MN forwards Secure Registration Request to SRG using KMR without having trust to FA. The foreign agent forwards the secure IP Registration Request packets received from SMN to SRG. SRG encapsulates the encapsulated packets using KMR and based on the information retrieved it sends the Registration Reply encrypted with

KMR. The FA again forwards the Secure Registration Reply to SMN. Using the SKMR sent by SRG, both SRG and SMN can communicate securely over wireless links and internet.

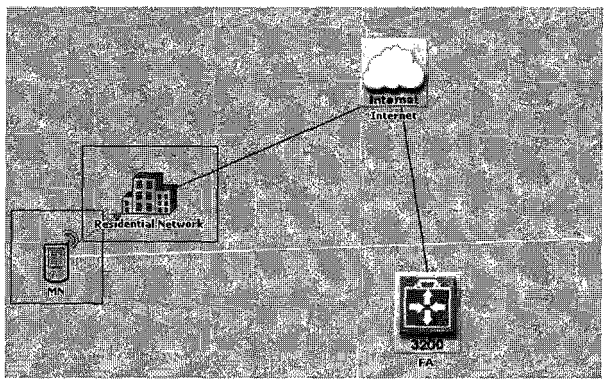

Fig. 3. Simulation set up for roaming mobile node of residential network.

The simulation parameters set for security of residential network communication were set as shown in table 1 below. RSA encrypted nonces are used to prevent form replay attacks. Both AH and ESP are used in bundle for authentication, encryption and confidentiality of data packets. The SA is maintained in both directions of tunnels.

TABLE I
Simulation parameters

Authentication Algorithm	HMAC-MD5
Authentication Method	RSA Encrypted Nonces
Encryption Algorithm	3DES
IP Sec Protocol	Bundle(AH+ESP)
SA Direction	Bidirectional
IKE Mode	Auto-negotiate

VI. RESULTS

As we implemented IPSec in SRG and SMN for secure Mobile IP Communication, we performed some analysis over WLAN properties like WLAN delay, load, MAC delay and throughput of both the Mobile IP entities.

SMN delay

The WLAN delay slightly increased upon registration after 7 minutes and 15 seconds and remained constant during Mobile IP Communication. Hence Securing the Mobile IP registration Messages introduces some delay due to encryption and encapsulation as shown in figure 3.

SMN load

WLAN load increased slowly upon registration and remained almost constant of 800 bits per second after the registration as shown in figure 3.

SMN MAC delay

The MAC delay was much affected due to Mobile IP and IPSec processes due to change in agents as SMN roamed to foreign network as shown in figure 3. Once the registration is completed the MAC delay decreased smoothly as shown in figure.

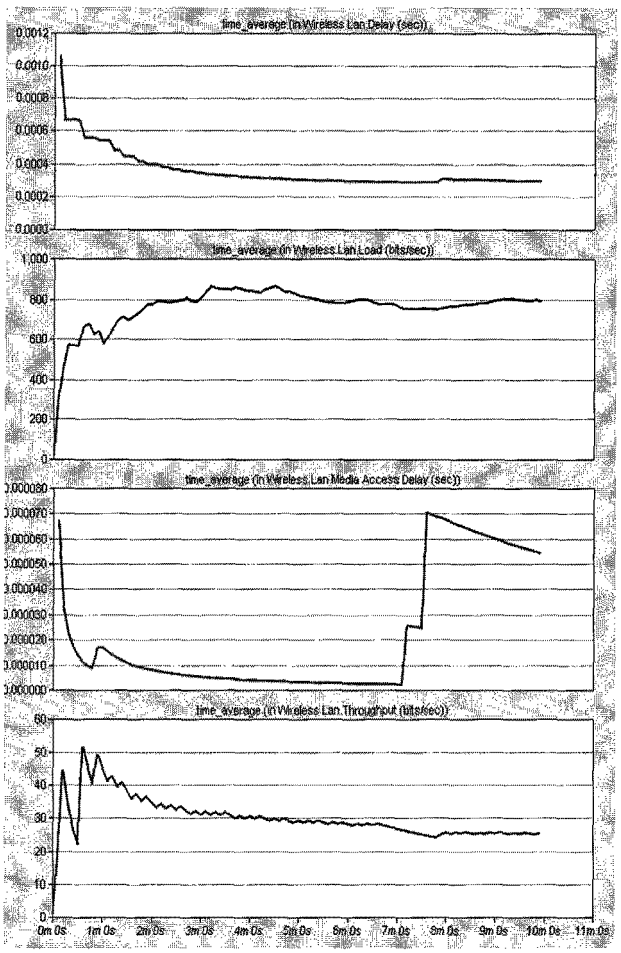

Fig. 4. WLAN Delay, Load, MAC delay and throughput of SMN.

SMN throughput

The throughput in SMN decreased before and during registration request as it has to wait for responses from FA for getting CoA and registration reply from SRG. Once the registration process is complete, the throughput remained almost constant of around 26 bits per second as depicted in figure 3.

SRG Delay

As depicted in figure 4, WLAN delay in SRG increased by 0.5 ms during registration request from MN as depicted in figure 4 as SRG has to wait while SMN finds FA, gets CoA and sends secure Registration Request Message with encryption and encapsulation processes of Mobile IP and IPSec. SRG incurred around 0.1 ms for IPSec and Mobile IP encapsulation and also for decryption of secure Registration Request packets. The WLAN delay also increased in SRG by 0.4 ms during registration reply from SRG for decision to accept or reject registration request from SMN and send the encrypted registration reply with IPSec and Mobile IP encapsulations. Hence the total WLAN delay during Registration process is 1 ms.

SRG Load

However WLAN load has no effect on adding security to Mobile IP packets in SRG as shown in figure 4 since SRG is powerful; device in residential network with high processing power.

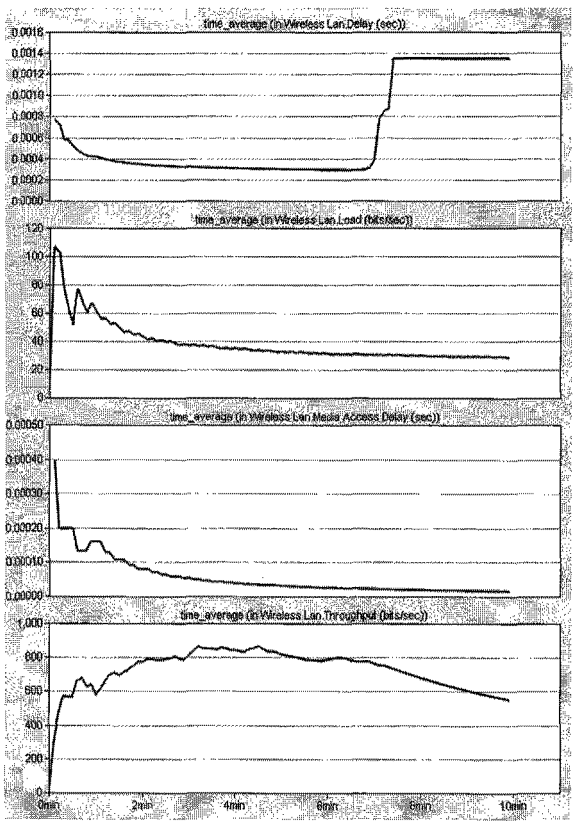

Fig. 5. WLAN Delay, Load, MAC delay and through put of SRG

SRG MAC Delay

The MAC delay also has no effect on adding security to Mobile IP packets in SRg as shown in figure 4 since SRG itself is the Access Point and is connected to the internet by PPP links via wired connection.

SRG Throughput

SRG does not seem to have effect of IPSec over Mobile IP during and after Mobile IP registration as SRG is a very powerful and efficient device with high processing power.

VII. CONCLUSION AND FUTURE WORKS

In this paper we have proposed a manageable authentication protocol that assured authentication not only during registration but also during any subsequent exchange of messages. Though this kind of protocol seem to add overhead to the residential gateway as it is involved in both mobile IP and IPSec operations with all the roaming mobile nodes, it won't affect much. Because it is the most powerful device being the heart of home network with several advanced features enabled in it along with integration of several technologies available at home. In future we would like to simulate the proposed protocol with a number of roaming mobile devices to perform deeper analysis.

ACKNOWLEDGMENT

This study was supported by research funds from Chosun University, 2009.

REFERENCES

[1] Prashant Krishnamurthy, Joseph Kabara, Tanapat Anusas-amornkul "Security in wireless residential networks" on the proceedings of IEEE Transactions on Consumer Electronics, Vol. 48, No. 1, february 2002, pp. 157-166

[2] Prashant Krishnamurthy and Joseph Kabara, "Security Architecture for Wireless Residential Networks" on the preceedings of VTC 2000, pp. 1960-1966

[3] Kyo-il Chung, "Security Framework for Remote Access to Home Network" on the proceedings of 2006 International Conference on Hybrid Information Technology (ICHIT'06) ,Vol. 1, pp.7

[4] MelbourneBarton, Derek Atkins, John Lee, Sanjai Narain, Deidra Ritcherson, Kemal E. Tepe and k. Daniel Wong, "Integration of IP mobility and Security for Secure wireless communication", Communications, 2002, ICC 2002, IEEE International Conference, Volume 2, pp. 1045-1049

[5] Dr. Muid Mufti. Aasis Khanum, "Design and Implementation of a Secure Mobile IP Protocol" on the proceedings of the Networking and Communication Conference, 2004. INCC 2004. International, 11-13 June 2004, pp. 53- 57

[6] Official site of Network Simulator OPNET, http://www.opnet.com

Young-bai Kim

1994. Graduate chief executive officer course of Korea University. 1996. Graduated public administration information communication broadcast course of Seoul National University 2008. A master coeducational in Dept. information and communication of Chosun University. 2009. A adjunct professor in Chosun University and Sunghwa University

Seung-jo Han

1982. A master coeducational in Dept. electronics of Chosun University. 1994 A doctor coeducational in Dept. arithmetic electronic of Chungbuk National University. 1986 ~ 1987 A visiting professor in University of New Orleans. 1995 ~ 1996 A visiting professor in University of Texas. 2000 ~ 2002 A visiting professor in University of California, Berkeley. 1998. A professor in Dept. information communication electronic of Chosun University.