JOURNAL OF KOREA MULTIMEDIA SOCIETY, VOL. 9, NO. 6, JUNE 2006(pp. 735-741)

The Security Systems in the Wireless Home Networks

Su Jin Kim[†], Myungsoo Bae[††], Sae-Hong Cho[†††]

ABSTRACT

In the near future, the wireless home networks will connect several devices at home. Due to the broadcast nature of a wireless network, anyone can hear and capture communication. Thus, we need to protect our network from attacks outside the house. In this paper, we propose and implement a security system that provides different levels of the security services to heterogenous home devices. To reduce the communication cost and workload of the server, home devices send the encrypted messages directly instead of sending through the server. We implement our security system on laptops using JAVA and our security system achieves the better performance with the large number of devices and messages in a network. In order to prove that our security system is secure against various attacks, we analyze the security of our security system using attack trees.

Keywords: Security, Wireless Networks, Home Networks

1. INTRODUCTION

Nowadays, most of the home devices have embedded microprocessors in them and wireless LAN protocols. In the near future, home devices will have more computing power and communication capability due to the fast growth of the technologies. Therefore, the home devices will communicate with others through the wireless network, called as the wireless home network. In this paper, we define that a wireless home network is a collection of home devices controlled electronically and interconnected using wireless networks. The wireless home network contains a wide variety of devices, ranging from high definition television (HDTV) sets to toaster ovens [3]. One possible application for such wireless home network is home automation [5] which makes life more comfortable and efficient.

Due to the broadcast nature of the wireless network, neighbors can eavesdrop and modify information easily. Because the devices in this network transmit the personal and sensitive information, the security becomes more serious concern.

In this paper, we propose a server-based security system which provides the different security services to the various home devices based on their requirements and capabilities. The remainder of this paper is organized as follows: In Section 2 we discuss the related works. We overview our home security system in Section 3. In Section 4, we describe how a device communicates with other devices in our security system. In Section 5, we analyze the security of our security system by the attack tree. In order to analyze the performance, we compare the communication and computational cost of our security system with the existing system in Section 6. Finally, we conclude in Section 7.

2. RELATED WORK

A wireless home network consists of a wide

※ Corresponding Author : Sae-Hong Cho, Address : (136-792) 389 Samseon-dong 3-ga, Seongbuk-gu, Seoul, Korea, TEL : +82-2-760-4478, FAX : +82-2-760-4488, E-mail : chosh @hansung.ac.kr

Receipt date : May. 9, 2006, Approval date : June. 19, 2006

[†] Arizona State University, Department of Computer Science and Engineering
(E-mail : Su.Kim@asu.edu)

[††] Arizona State University, Department of Computer Science and Engineering
(E-mail : msbae@asu.edu)

[†††] Hansung University, Department of Multimedia Engineering

range of home devices which have different capability. With respect to security, home devices have different security requirements. Applying the same security mechanism for diverse devices is not efficient. Thus, we should support the different security policies for them.

Since home devices are expected to be inexpensive and small, they have limited resources which are not capable to perform complex encryption algorithms such as asymmetric cryptograph. Therefore, the wireless home networks need light-weight and energy-efficient algorithms and mechanisms.

Basically, the security for a home network requires three security issues [4]. First, a*uthentication* is required to separate communication between inside and outside the home network. Second, a*uthorization* verifies whether a device is allowed to do actions on other devices. Third, co*nfidentiality* is related to which devices are allowed to read the messages being transferred.

Some researchers have proposed solutions of the security problems in a wireless home network and home automation. Nakakita et al. have proposed the server-based security system for a wireless home network [2]. They assumed that there is one server which manages all devices connected to the wireless home network. The server uses two kinds of keys; a master key and shared network key. A master key is assigned to each device uniquely. The server encrypts a new shared network key with the master key of each device and distributes it periodically. The main problem is if a device or shared key is compromised, then the whole network becomes insecure. In this architecture, the frequent distribution makes the network and server busy.

Krishnamurthy et al. has introduced a classification of security services and security architecture based on it [1]. The proposed architecture uses the access point to mediate the communication·between devices. For communication, a device must first send a message to the access point. After the access point verifies the source device, it forwards the message to the destination. Because every message goes through the access point, there is also a bottleneck problem at the access point. There is a security weakness because the access point forwards a message without encryption and anyone can hear the communication.

3. OVERVIEW OF OUR HOME SECURITY SYSTEM

We assume there are several devices at a house which have microprocessors and wireless network capabilities such as IEEE 802.11x and Bluetooth. The server which manages all devices is secure completely. We also assume the encryption algorithm is very trustworthy. We propose a security system for the wireless home networks. We have three main goals to achieve in our paper. First, our security system divides devices into different security levels based on their requirements and capabilities. Second, we suggest efficient schemes to reduce workload of the server. Third, for secure communication, we encrypt all messages and assign a shared key to a pair of device. Thus, the communication is protected from outside and inside. Table 1 describes notations used in this paper.

Krisnamurthy et al. [1] suggested a classification of security services for a wireless home network as follows:

1) *No security*: Some devices such as toasters and refrigerators need no security.
2) *Moderate security*: Devices which need some

Table 1. Notations

ID_i	ID of device i
SL_i	the security level of device i
mk_i	the master key of device i
A | B	the concatenation of message A and B
$E_{mki}(A)$	the encryption of message A by the given encryption algorithm with mk_i
Dest	ID of the destination
sk_{ij}	the shared key between device i and j
TS	Time stamp

security to check identification such as switches on air-conditioning, but not encryption.

3) *Wireline equivalent security*: Devices in this category need authentication and encryption such as routine or cordless telephones.
4) *High security*: Devices such as desktops and cellular phones require higher security. They need very secure authentication and encryption.
5) *Ultra-high security*: The costly services, for example long distance call and video on demand, need the multiple levels of authentication and strong encryption.
6) *Critically high security*: For the surveillance cameras and security alarm, devices require strong security services so that nobody can break such a system.

We will follow this classification for our home security system. Each category can use different security policy. Thus, the length of keys, validity period of keys and other parameters of encryption algorithms depend on the security levels of devices.

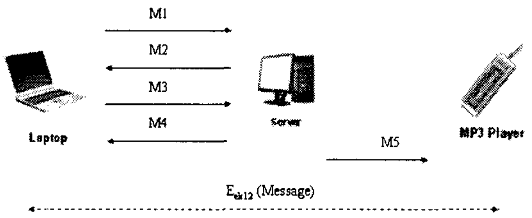
4. COMMUNICATION BETWEEN DEVICES

Our home security system uses two kinds of keys: the master key and the shared key. we assume that each device has been already registered at the server and obtained the unique master key. The master keys will be used to communicate with the server. For communication between devices, a shared key will be assigned to a pair of devices.

4.1 The Shared Key Establishment

Fig. 1 describes the example of communication between two devices, a laptop and MP3 player.

Suppose a laptop and MP3 player have been registered with ID_1, mk_1 and *high security* level, and ID_2, mk_2 and *wireline equivalent* security level respectively. When the laptop needs to communicate with the MP3 player, the laptop first generates a random number, R_1 and sends M1 to the server. The server decrypts M1 and generates a random number, R_2. Because other devices don't know mk_1, they can not generate correct R_1+1. The laptop decrypts M2 with mk_1 and compares R_1+1. If R_1+1 is correct, the laptop computes R_2+1 and replies M3. The server checks R_2+1. If it matches, the server assigns the shared key, sk_{12}, and distributes it to both devices. Since each message is encrypted with the master key of each device, the distribution is secure. M4 and M5 include the security level of another device for access control. After sk_{12} is distributed, all messages between the laptop and MP3 player will be encrypted with sk_{12} until sk_{12} will expire. After a shared key expires, a new shared key should be updated. Suppose Dev1 has a message to Dev2. First, Dev1 checks whether it has a valid share key or not. If Dev1 doesn't have it, Dev1 should request a new shared key.



M1: $E_{mk1}(ID_2 \mid R_1)$

M2: $E_{mk1}\,[(R_1+1) \mid R_2\,]$

M3: $E_{mk1}\,(R_2+1)$

M4: $E_{mk1}\,(ID_2 \mid SL_2 \mid sk_{12})$

M5: $E_{mk2}\,(ID_1 \mid SL_1 \mid sk_{12})$

Fig. 1. The example of the shared key establishment.

4.2 Access Control List

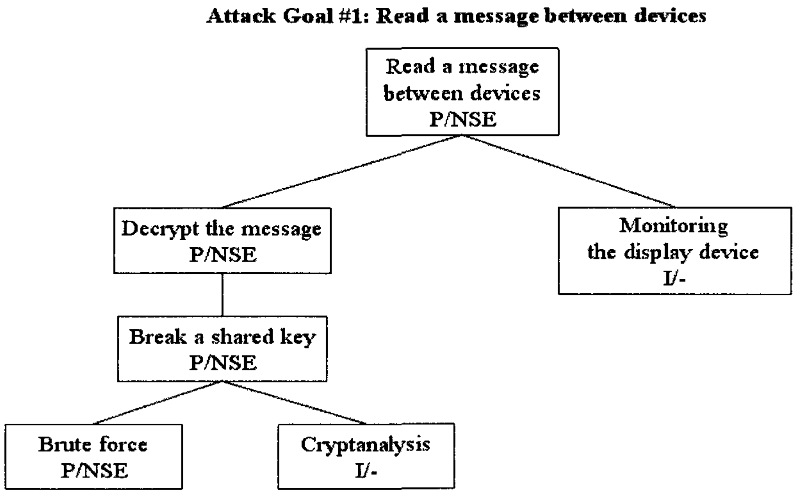
The existing architecture proposed by Krisnamurthy et al. allows a device to access other devices which have equal or lower security levels. The reason is that attacking a device with lower security level is much easier than one with higher security level. However, in some cases, we need to allow the device with the lower security level to access the device with higher security levels. For example, Alice is listening to music in the living room using her MP3 player. She wants to download music files from her PC in her room to the MP3 player with her. For this purpose, we use the access control list (ACL) which indicates who is allowed to do what with that resource [9]. For instance, MP3 player can read MP3 files, but can not write files or execute applications on the laptop.

5. SECURITY ANALYSIS

We use the attack tree to analyze the security of our security system. The attack tree provides a formal way to describe the security system in a tree structure [6]. The root is the goal of attacks and leaf nodes are ways to achieve that goal. Fig. 2 and 3 are attack trees against possible attacks in a wireless home network. All nodes in Fig. 2 and 3 are OR nodes which are alternative ways to achieve a goal. For each node, we assign two values; I (Impossible) or P (Possible), and NSE (No Special Equipment Needed) or SE (Special Equipment Needed).

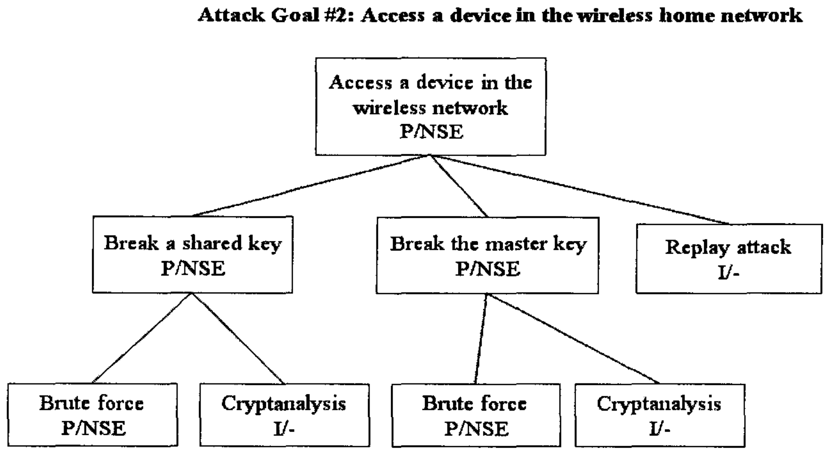
There are two possible attack goals in a wireless home network. First, Fig. 2 presents the attack trees against reading a message between devices. Monitoring display devices is impossible, but decrypting a message by a malicious node is possible. Cryptanalysis is not feasible due to assumptions of our system model. However, attackers can break a shared key using brute force. To prevent brute force, we restrict the use of a shared key within the validity period. Updating of shared keys will make a wireless home network more secure against brute force attacks.

Second, Fig. 3 describes the attack tree against accessing a device. Replay attack to get the access right is not feasible because of the mutual authentication. Therefore, there are two possible ways to attack a system in order to access a device. First, an attacker can try to break a shared key. If an attacker gets sk_{AB}, he can access device A and B using sk_{AB}. However, we already mentioned that the limitation of the key validity helps preventing the brute force attack. Breaking a master key can be the second possible attacking. If an attacker breaks the master key of device A, he can act as device A in order to request shared keys to the server. The server will recognize an attacker as device A and assign a shared key. Breaking a key using cryptanalysis is impossible due to our assumption. The brute force attack could be possible, therefore the master key should be long enough to prevent against the brute force attack.


Attack Goal #1: Read a message between devices
Read a message between devices P/NSE
Decrypt the message P/NSE
Monitoring the display device I/-
Break a shared key P/NSE
Brute force P/NSE
Cryptanalysis I/-

P: Possible, I: Impossible, NSE: No Special Equipment, SE: Special Equipment

Fig. 2. The attack tree against reading a message between devices.


Attack Goal #2: Access a device in the wireless home network
Access a device in the wireless network P/NSE
Break a shared key P/NSE
Break the master key P/NSE
Replay attack I/-
Brute force P/NSE
Cryptanalysis I/-
Brute force P/NSE
Cryptanalysis I/-

P: Possible, I: Impossible, NSE: No Special Equipment, SE: Special Equipment

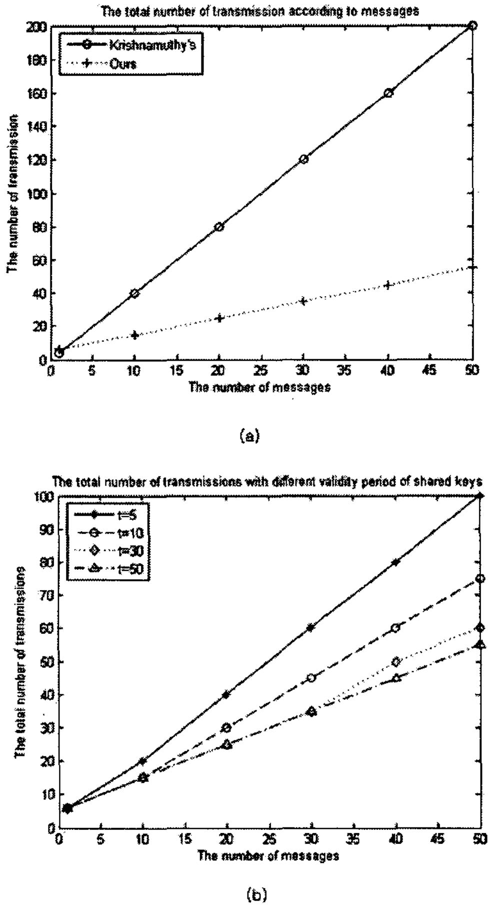
Fig. 3. The attack tree against accessing a device in a wireless home network.

6. PERFORMANCE ANALYSIS

6.1 Communication Cost

In this section, we compare the total number of messages. Since other existing architectures use a group key or one key for a whole network, we only compare our system with Krishnamuthy's architecture. For simplicity, we assume all transmissions are successfully done without any error or collision. We define that the number of transmission for one message includes authentication, key distribution, and transmission of an actual data.

Fig. 4 (a) shows the difference of the number of transmissions between Krishnamuthy's architecture and our security system. In this example, we assume shared keys would not expire. At the beginning of communication, the gap of the number of transmissions is small. However, as the number of messages increases, the total number of transmission decreases compared with Krishnamuthy's architecture. In our security system, shared keys will be updated to avoid exposure. Frequent updating a shared key provides better security, but it increases the total number of transmissions. Therefore, there is the trade-off between the security and communication cost. In Fig. 4 (b), a shared key is updated every t messages. We can



(a)

(b)

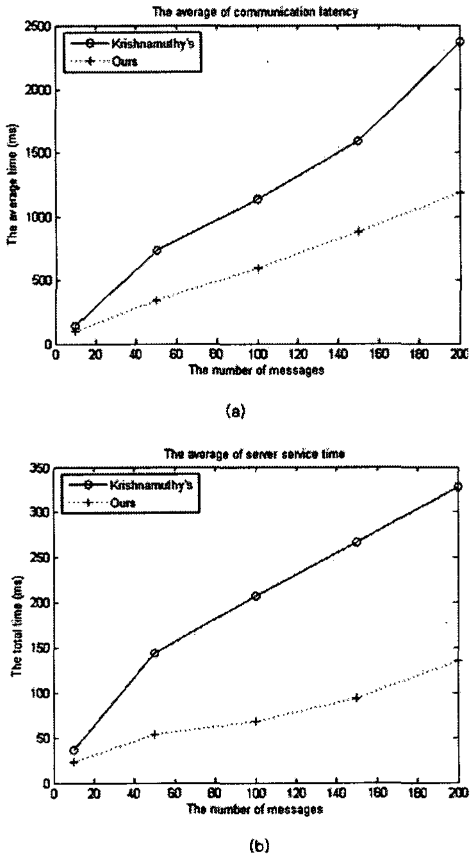
Fig. 4. (a): The comparison of the number of transmission, (b): The total number of transmissions according to different validity period of shared keys.

see that our security system takes at least 50% less transmissions than Krishnamuthy's architecture.

6.2 Computational Cost

To compare the computational cost, we have implemented our security system on laptops using JAVA and IEEE 802.11. For cryptography, we have chosen RC5 [7] because RC5 has small code size and suitable for the heterogeneity [8]. We used one server and 5 laptops assumed belong to different security levels as following: one laptop for "*Moderate security,*" two laptops for "*Wireline equivalent security,*" and two laptops for "*High security.*" We also assumed shared keys never expire.

We compare the average of communication latency and server service time of our security system with Krisnamurthy's architecture [1]. The average of communication latency is the average time from the start to send a request message to the end to complete transmission of actual data at a client. The server service time is the total time dedicated to process all steps for each system at the server. Figure 5 shows the results. The key length and validity period are 2 bytes and 300 ms for "*Moderate security*", 4 bytes and 200 ms for "*Wireline equivalent security*", and 8 bytes and 100 ms for "*High security*". When the number of messages is small, there is no big difference between two systems. However, as the total number of messages increases, the gap between results becomes much bigger. We expect our security system is much better than Krisnamurthy's architecture [1] when there are a lot of devices and messages in a network.



(a)

(b)

Fig. 5. (a): The average of communication latency, (b): The average of server service time.

7. CONCLUSION

We presented the efficient and secure home security system in a wireless home network. Due to the heterogeneity and limited resources of the home devices, our security system uses different levels of the security services depending on the security requirements and capabilities of the home devices.

In comparison to the existing architectures and systems, our security system has several advantages. First of all, the efficiency is one of the important issues due to the resource constraints in a wireless home network. We allowed a home device to communicate with other devices directly after getting shared keys from the server. As the total number of transmission was reduced in our security system, we reduced communication latency and the bottleneck on the server. When there are a lot of messages in a network, our security system is much better than Krisnamurthy's architecture [1].

In terms of security, our security system also provides better security by all encrypted messages and the mutual authentication. In additional, the devices with lower security level are allowed to access the devices with higher security level in our security system when they are permitted. In summary, our proposed security system provides better security in the more efficient way.

8. REFERENCES

[1] P. Krishnamurthy, J Kabara, and T. Anusasamornkul, "Security in Wireless Residential Networks," *IEEE Trans. On Consumer Electronics*, Vol. 48, No. 1, pp. 157-166, 2002.

[2] H. Nakakita, K. Yamaguchi, M. Hashimoto, T. Saito, and M. Sakurai, "A Study on Secure Wireless Networks Consisting on Home Appliances," *IEEE Trans. on Consumer Electronics*, Vol. 49, Issue 2, pp. 375-387, 2003.

[3] J. A. DiGirolamo, "Home networks - from toasters to HDTV," *Digest of Technical Papers in Intl. Conf. On Consumer Electronics*, pp. 82-83, 1996.

[4] Carl M. Ellison, "Home Network Security," *Intel Technology Journal*, Vol. 6, Issue 4, pp. 37-48, 2002.

[5] A. Wacker, T. Heiber, and H. Cermann, "A Key-Distribution Scheme for Wireless Home Automation Networks," *1st IEEE Intl. Consumer Communications and Networking Conf.*, pp. 47-52, 2004.

[6] B. Schneier, "Attack Trees: Modeling security threats," *Dr. Dobb's Journal*, Vol. 24, No. 12, pp. 21-29, 1999.

[7] R. L. Rivest, "The RC5 encryption algorithm," *Proc. 1st Workshop on Fast Software Encryption*, pp. 86-96, 1995.

[8] A. Perrrg, R. Szewczyk, V. Wen, D. Culler, and J. D. Tygar, "SPINS: Security Protocols for Sensor Networks," *Wireless Networks*, Vol. 8, Issue 5, pp. 521-534, 2001.

[9] C. Kaufman, R. Perlman, and M. Speciner, *Network Security: Private Communication in a Public World, Second Edition*, Prentice Hall, Upper Saddle River, New Jersey, 2002.

Su Jin Kim

1998 Sookmyung Women's University (BS, CS)
2000 Sookmyung Women's University (MS, CS)
2002-Present Arizona State University (Ph.D. Student, CSE)

Interesting Area : Security, Home Networks, Sensor Networks, Pervasive Computing, Ubiquitous Computing

Myungsoo Bae

1997 Eastern Michigan University (BS, CS)
1999 Arizona State University (MS, CSE)
2000-Present Arizona State University (Ph.D. Candidate, CSE)

Interesting Area : Computer Graphics, Computer-Aided Geometric Design (CAGD), Surface Matching, Virtual Reality, Face Recognition, Network

Sae-Hong Cho

1983 Yonsei Univ.
1991 California State Univ. (CS)
1996 Arizona State Univ. (MS, CSE)
1999 Arizona State Univ (Ph.D., CSE)
1999. 9 - 2002. 2 Daegu Univ.
2002. 3 - Present Dept. of Multimedia Engineering, Hansung Univ.

Interesting Area : Multimedia Application, Internet Ap-plication Program, Virtual Reality, Cyber Education, Game Application, Network