J. Internet Comput. Serv.
ISSN 1598-0170 (Print) / ISSN 2287-1136 (Online)
http://www.jics.or.kr

Design and Implementation of a Secure Smart Home with a Residential Gateway

Sang-kon Kim[1] Tae-kon Kim[2*]

ABSTRACT

In this paper, we propose a secure smart home network model and a novel cryptographic protocol called the Smart Home Security Protocol (SHSP). Authentication, key distribution, and encryption functions are properly supported in order to make a smart home secure, and a residential gateway (RG) plays a central role in performing these functions. According to the characteristics of networks and attached devices, we classify smart homes into three different types of sub-networks and these networks are interconnected with one another by the RG. Depending on a sub-network, we use different types of secure schemes to reduce the burden of the process and the delay in devices while it provides proper security functions. The proposed secure smart home model is implemented and verified by using a variety of embedded system environments.

☞ keyword : Secure Smart Home, Cryptographic Protocol, Residential Gateway, Home Automation

1. Introduction

Due to the recent technological advances, lots of electronic devices with new features have become available in the consumer market. Particularly, various digital appliances with wired/wireless communication functions including the Internet of Things (IoT) begin to be utilized at home. These smart home appliances generate and share lots of information to improve the quality of residential life. People now desire to have a smart home network for remote device control, inter-device communication and information sharing. Smart home systems are evolving into a goal that can maximize the user's convenience beyond home automation [1]. In addition, advanced health and medical care services based on a smart home have been developing [2].

A smart home system is really a mixture of a wide variety of technologies: various home appliances, ranging from PC to a surveillance camera; various network solutions such as Ethernet (LAN), wireless LAN (Wi-Fi) and USB. What becomes a problem is that most of these network solutions are based on broadcast media. Although the broadcast media are cost effective and useful for message advertisement sometimes, they may be vulnerable to various types of information attacks. If appropriate security mechanisms are not supported, some home components could provide an entry point for malicious entities. A leak of messages from a network may reveal private information to any malicious person. Furthermore, when sensitive devices to security such as a gas valve controller or a door lock are connected through a home network, then high-level security mechanisms have to be considered.

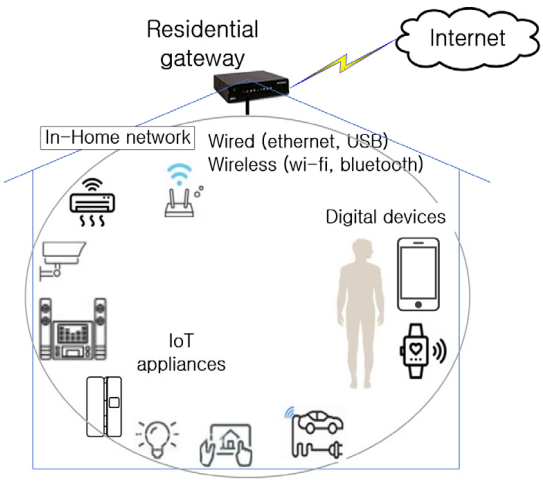
1.1 Smart home network architecture

The definition of a home network is gradually broadening with the advances in technology. Fig. 1 shows the reference architecture and there are various interfaces: Ethernet, Wi-Fi, Bluetooth and USB. The lighting system, security (surveillance) system, home appliances and home entertainment can be connected through Ethernet or Wi-Fi.

A residential gateway (RG) is often responsible for network access to a residential area. It provides overall control and management for a variety of devices through wired/wireless communication interfaces. It also offers transparent access to a diversity of services. In addition, a RG may be used to manage home security systems automatically or remotely. Recently, people can expect apps installed on a mobile phone instead of the above fixed RG. Although a smartphone guarantees excellent mobility, it is

[1, 2] Dept. of Electronics & Information Engineering, Korea University, Sejong, 30019, Korea
* Corresponding author: Tae-kon, Kim (taekonkim@korea.ac.kr)
[Received 03 November 2021, Reviewed 27 December 2021, Accepted 17 January 2022]

difficult to expect a sufficient role because of the power consumption and mobile cost. And it is also difficult to expect that it is fixed in a certain place and supplied with the wall power all the time.



(Figure 1) Architecture of a smart home network

1.2 Security services

To provide home network security, three kinds of security services usually have to be considered: *confidentiality*, *authentication* and *identification* [3]. Confidentiality or privacy is a security service that provides resistance to the security attack known as an interception. Interception is the most intuitive form of security attack where two communicating parties do not wish to reveal the contents of their transactions to a third party. In more rigid cases, the existence of the communication itself must not be exposed to unauthorized entities. Encrypting the messages and the identities of two parties is the most often used method of providing confidentiality. Message authentication service provides integrity of the message and it guarantees that a sender is who he or she claims to be (sender authentication). The corresponding attacks might be a modification of the message and impersonation of the sender's identity. Message authentication can be provided by attaching a digest of the message, which is encrypted by a key known only to the correspondents. Identification is another security service often used in transactions such as automatic teller machines. Mutual authentication is based on identification, in which a client must prove its identity to service, and the service must prove its identity to the client for any application traffic. A secret password or key is shared between the communicating entities. One of the entities challenges the other with a nonce (a random number), and the other entity responds by computing a one-way result using the nonce and the shared secret key. The challenger internally performs the same one-way computation and verifies the identity. In this way, the entities never reveal the shared secret to the outside world.

1.3 Security protocols for home networks

To provide most of the above security services, some sort of encryption and one-way functions are required. However, strong encryption in itself is insufficient. An opponent may exploit inherent weaknesses in underlying communications and security protocols. A security protocol is a set of cryptographic services and functions that prevent threats to reliability. A necessary foundation for network security is the ability to reliably authenticate communication partners and other network entities [4].

Including cryptographic authentication, security services require an efficient secure key generation and distribution capability. Currently, designs dealing with authentication in networks or distributed systems usually address the issues of authentication with key management. These designs typically assume that all network parties share a key with a commonly trusted entity. They can get pair-wise shared keys to carry out mutual authentication from the entity. These protocols are called *three party authentication protocols* [5].

On the other hand, *two-party authentication protocols* do not rely on a common trusted party. The protocols use usually either a public-key or shared-key cryptography system. With a public-key system, each party only has to know and verify the key of the other party, and there is no need to share secret keys. For example, the IPSec, SSL or TLS relies on two-party protocols based on public-key technology. However, these protocols are unsuitable for use in low-performance network devices due to their computational complexity. In [3], the *2-Party Authenticated Key Distribution Protocol* (2PAKDP) is proposed for

low-performance networks relying on a shared-key cryptography scheme.

In this paper, we propose a new cryptographic protocol called the Smart Home Security Protocol (SHSP) for authentication, key distribution and encryption.

2. Secure home network model

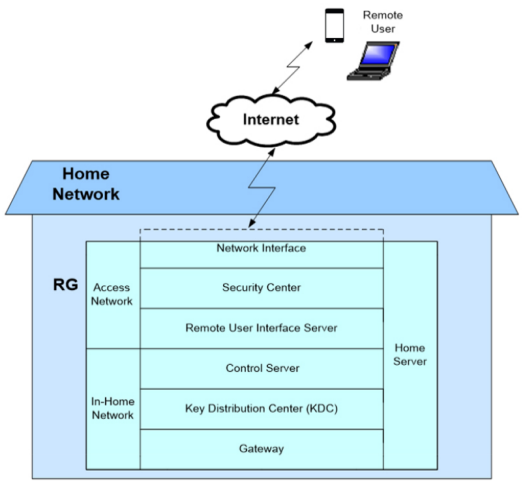
The secure home network model in the paper is simple but it is very efficient and useful for current network models. We classify a home network into three sub-network types depending on the performance characteristics and its components. These are class1, class2 and class3 sub-networks.

In case of class1 sub-network, devices have excellent processing resources and various network interfaces It can provide a public-key cryptographic system like SSL or TLS. There are PCs, Notebooks, PADs and so on. In class2 sub-network, devices have good processing power and a few network interfaces. It can provide a symmetric block cipher. There are digital TVs, audios, settops and so on. In class3 sub-network, devices have very limited processing capability and low-speed network interfaces. It can provide a symmetric stream chipper. There are door locks, air conditioners, gas valve controllers, and so on.

Now, we feel keenly the necessity of a central device that is able to give full connectivity, interoperability, network management, and security functions. A smart phone and PC system may be considered as a strong candidate due to their powerful resources. However, as we discussed, they are not suitable for a home network model because of power consumption and cost. So we introduce a residential gateway (RG) as a central device that has good resources, reliability, low power consumption and cost effectiveness. It can be always turned on and provide stable service in a fixed place.

The RG should also provide gateway, key distribution center (KDC), and control server features. As a home gateway, it offers an interconnection between two end-devices that use different communication medium. As a KDC, it provides identification, authentication, and key management functions for security. As a control server, it has a database for all controllable devices in-home network.

We assume that every message originated from each device passes through a RG before it reaches a destination device [6][7]. Under this assumption, a RG gives a connection between two end-devices that use different types of medium and network protocol. Moreover, it is possible to access a RG from outside the home through networks. In this situation, even if some devices hear others through the same physical medium and communication protocol, they ignore messages from others. They can communicate with others only through a RG.



(Figure 2) Functional block diagram of a RG

3. Security protocols review

Before delving into the proposing protocols, we explain the basic protocols: *2-party authentication protocol*, *2-party key distribution protocol*, *2-party authenticated key distribution protocol* and *3-party authenticated key distribution protocol*.

3.1 Terminology

We use the following symbols. The distribution of secret keys from a key distribution center (KDC) to its constituent principals (clients and servers) requires the use of secret channels. In the area of symmetric cryptography, this requires that each principal share at least one secret key with the KDC. In this paper, a master key is intended to denote this shared secret and a session key to denote a distributed secret key.

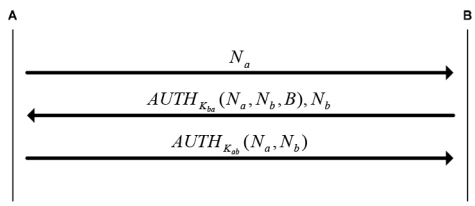
(Table 1) Terminology for security protocols

A,B,X,Y	Principals
K_x	Master key of X
$K_{x,y}$	Session key shared by X and Y
$E_k(M)$	Encryption of message M using key
$AUTH_k(M)$	One-way hash function of M using key
N_x	Nonce or challenge generated by or for X

3.2 2-party authentication and key distribution protocol

3.2.1 2-party authentication

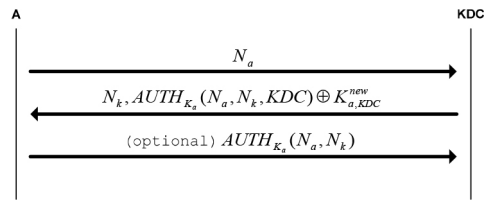
A family of simple 2-party authentication protocols was presented in [4]. The protocols are efficient in terms of message size and computation overhead, and minimal in use of cryptography. They were shown to be resistant to various kinds of attacks known as interleaving attacks. One of the 2-party authentication protocols (2PAP) is shown in Fig. 3 [4]. The variables N_a and N_b are used by each party to challenge the other to provide its identity. The $AUTH_{Kab}$ and $AUTH_{Kba}$ are used to show the authenticity of their parameter string, and the Hash function based massage authentication code (HMAC) is used. The number of exchanged messages is three, which is minimal for a challenge-based protocol. The use of challenges or nonces is robust by excluding state maintenance information such as synchronized clocks or counters.



(Figure 3) 2-party authentication protocol (2PAP)

3.2.2 2-party key distribution

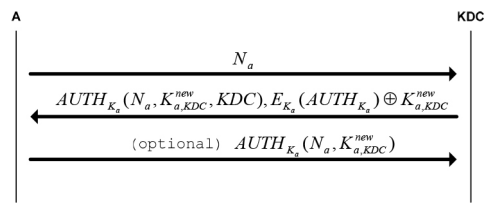
For each principal to obtain a session key from a KDC, a simple 2PKDP is constructed from the 2PAP in [7] as illustrated in Fig. 4. A 2PKDP consists of only two flows. It provides a simple key distribution method and only A and KDC can share $K_{a,KDC}^{new}$[8]. However, it is not secure in regard to key integrity. This means that an intruder can modify the key distribution and cause A to extract a key not issued by the KDC. In fact, the KDC may be unavailable and the intruder can forge the entire second flow. The 2PKDP constructs a protocol that copes with the above weak points while not compromising the minimality of the protocol.



(Figure 4) 2-party key distribution protocol (2PKDP)

3.2.3 2-party authenticated key distribution

2PKDP lacks two features: integrity of the new key and timeliness of the KDC's response. In [3], 2-party authenticated key distribution protocol (2PAKDP) was proposed and it is illustrated in Fig. 5. Its structure is similar to a 2PAP and the only difference is that the KDC's nonce (here, a newly generated session key, $K_{a,KDC}^{new}$) in flow 2 is hidden. The technique used to construct the message flow 2 is called braiding. A remark on a 2PAKDP is that, like its ancestors, a 2PKDP and 2PAP, it is a minimal protocol. Also, it requires only one additional (on top of 2PAP) block encryption operation in order to hide the key [7].

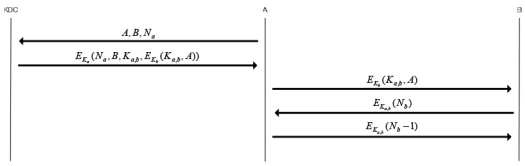


(Figure 5) 2-party authenticated key distribution protocol (2PAKDP)

3.3 3-party authentication and key distribution protocol

3.3.1 3-party authentication and key exchange

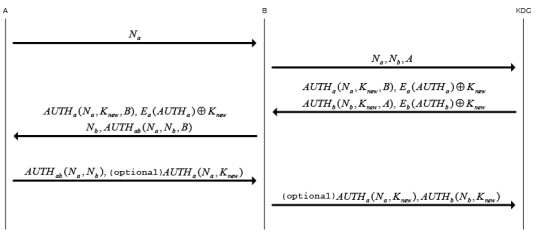
These kinds of protocols combine authentication with key exchanges to solve a general computer problem: *A* and *B* are on opposite ends of a network and want to talk securely. Each participant has to exchange a secret key and at the same time be sure that he/she is talking to the other and not to a malicious one. Most of the protocols assume that the KDC shares a different secret key (i.e., master key) with each participant, and that all of these keys are in place before the protocol begins. That is, the protocols are composed of two participants and a KDC: 3-party protocols. Lots of studies have been done since Needham and Schroeder's landmark paper [3].



(Figure 6) Needham-Schroeder's 3-party protocol

3.3.2 3-party authenticated key distribution

In [7], [9], and [10], the authors extended their 2PAKDP to 3-party authenticated key distribution protocols (3PAKDP), that is, A-B-K pull and K-A-B push models. Fig. 7 shows one of the A-B-K pull models (modification of Needham-Schroeder's 3-party protocol). A K-A-B push model is executed similarly.



(Figure 7) A-B-K 3-party authenticated key distribution protocol

4. Proposed protocol: SHSP

The discussed protocols previously are not appropriate in the proposing home network model due to the following reasons. First, they assume that a client *A* or *B* is either unable, unauthorized, or unwilling to contact the KDC, or it is simply willing to choose the other when it wants to contact the KDC. Second, they assume that a client *A* can communicate directly with client *B*. However, in an RG-based home network architecture, every message originated from each device passes through the RG. In this environment, it is unrealistic to adopt the discussed 3-party protocols directly.

Popular smart home networks consist of lots of devices with various performances. And this characteristic is consistent with the design purpose of a 2PAKDP, which is minimal, flexible and scalable authentication and key distribution protocols. In the following subsections, we design a novel 3-party protocol based on the 2PAKDP, which is an A-K-B model. We assume that the KDC's functions of authentication and key distribution can be integrated into the RG without severe loads.

4.1 Smart home security protocol (SHSP)

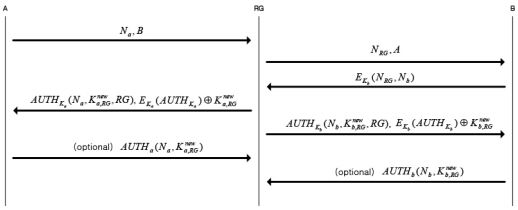
Let's suppose that entities *A* and *B* want to authenticate each other and subsequently engage in secure communication. Fig. 8 shows a practical SHSP in the home network.

1. *A* contacts RG in flow 1 letting RG know that A wants to communicate with B and challenging it to authenticate based on a nonce N_a.
2. RG informs *B* that it has some data from *A* and it needs to start a process of authentication and key distribution. Also, RG tries to authenticate *B* using a nonce N_{RG}.
3. Having received the message, *B* contacts RG in flow 3 challenging it to authenticate based on a nonce N_b. *B* would be authenticated by RG using a nonce N_{RG}.
4. RG replies to *A* in flow 4 with a newly generated key $K_{a,RG}^{new}$. The message follows the same syntax as in a 2PAKDP.
5. RG replies to *B* in flow 5 with a freshly-generated key

$K_{a,RG}^{new}$.

6. Having received the message, *A* extracts $K_{a,RG}^{new}$ and checks its integrity and freshness by re-computing the $AUTH_{Ka}$ expression. Here, the $AUTH_{Ka}$ denotes cryptographic one-way hash functions using *A*'s master key K_a. In flow 6, *A* can send an optional message for confirmation
7. Having received the message, *B* performs the same procedure as *A* in the previous step.

Actually, a SHSP, an A-K-B model, is composed of two instances of 2PAKDP and one additional indication flow (flow 2). It has a strong advantage compared to other 3-party protocols. A RG exists between two end devices so it can reduce unnecessary procedures.



(Figure 8) Smart home security protocol (SHSP)

4.2 Analysis

In this subsection, a SHSP is analyzed to prove its security. As we discussed, it is composed of 2PAKDP and indication flow. So, 2PAKDP is analyzed first, and then a SHSP is proved.

4.2.1 Analysis of 2PAKDP

4.2.1.1 Authentication

The first step is showing the equivalence of a 2PAKDP and 2PAP. The only difference between the two protocols is the nonce field of the second message. In a 2PAP, it is simply N_b while in a 2PAKDP it is a more complicated one, $E_{K_a}(AUTH_{K_a}) \oplus K_{a,KDC}^{new}$.

The purpose of this expression is to conceal the nonce, i.e. $K_{a,KTC}^{new}$ which is subsequently used as a key. $AUTH_{Ka}$ is also a nonce because it is a result of a strong one-way function. When E_{Ka} is a strong one-way hash function, (e.g., MD5) which produces a fixed-size digest of its input, different input values can be hashed into an identical digest.

4.2.1.2 Key distribution

Strong authentication is not sufficient for secure key distribution. For this purpose, a protocol has to satisfy non-disclosure, independence and integrity properties.

Disclosure of a key is possible only if an attacker is somehow able to obtain the $E_{Ka}(AUTH_{Ka})$ value. The adversary must either possess the encryption key or be able to elicit the desired value from one of the legitimate parties. The former is assumed to be impossible while the latter deserves a closer look. The adversary can try to obtain the desired value by interrogating *B* and pretending to be *A*. However, it is also impossible because of the freshness of the new key. An attacker gets a [plaintext, ciphertext] pair to break the device key. However, the encryption scheme is secure and it utilizes fresh values every time. They can not recognize a master key and the property of independence is proved. The integrity of the key is not the foremost problem as long as the key cannot be modified to a particular value selected by the attacker. And attacks of key modification require simultaneous modification of the authentication expression and attacks of this sort are not feasible with the 2PAKDP.

4.2.2 Analysis of SHSP

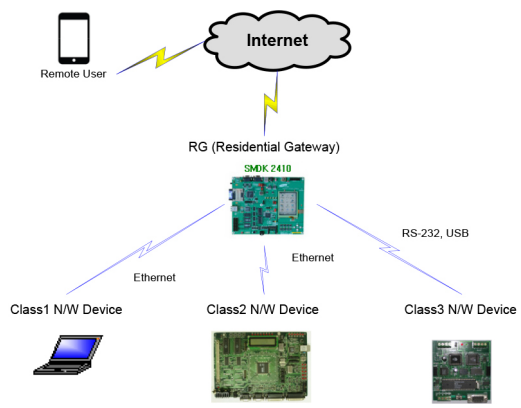
In a SHSP, a RG has the responsibility for distributing a fresh key to two parties. A SHSP satisfies the same conditions as a 2PAKDP with one added requirement. Neither party can alter the key being distributed. A SHSP is an A-K-B model and a RG is only able to generate, distribute, and manage the secret keys that are used. The proposed scheme is proved to be secure.

Additionally, we should consider any possible attack on a SHSP such as a replay attack and man in-the-middle attack. In fact, a 2PAKDP is already verified and the additional indication flow doesn't include any secret information. Even if an attacker gives a replay attack using indication flow, *B* would start the second 2PAKDP between *B* and the RG. As a result of that attack, *B* only gets a new session key and there is no disclosure of key. In this case,

if the RG manage keys properly, there wouldn't be any damage in the system. In the case of man in-the-middle attack, an attacker should know *B*'s master key, if not, it would be impossible.

5. Implementation and verification

We implement the proposing home network model using embedded systems in order to easily apply to real home networks. Fig. 9 shows the system configuration of our testbed.



(Figure 9) System configuration of the test bed

5.1 Implementation environment

We implement a remote user and class1 devices using PC systems, and a RG, class2 and class3 ones using the embedded systems.

5.1.1 Remote user system

We make an application program using OpenSSL on Linux O/S to communicate with the RG securely. The implemented PC system has an 866MHz processor and 256MB RAM.

5.1.2 Residential gateway

We implement home server and secure communication programs at the application layer on Linux O/S. And we use OSGi middleware and JVM(JAVA Virtual Machine) for a RG.

(Table 2) Implementation specification for the RG

H/W Spec.	SMDK2410 Evaluation Board - ARM920T RISC MICOM - 113MB ROM, 64MB RAM
Secure Comm.	SSL for remote user devices IDEA for class1 and class2 devices Stream cipher using multi-ASGs SHSP

5.1.3 Class1 in-home device

We apply IDEA symmetric block cipher and a SHSP for secure communication. In fact, most of them can provide SSL but it would introduce significant degradation of system performance. The implemented board has a 600MHz processor and 128 MB RAM.

5.1.4 Class2 in-home device

We apply IDEA block cipher and a SHSP for security. We don't use any O/S and optimally make a C code program to communicate with a RG securely.

(Table 3) Hardware specification of class 2 device

SNDS100 ARM7TDMI MICOM, 1MB ROM, 16MB RAM

5.1.5 Class3 in-home device

We apply stream cipher using ASG (alternating step generator) and a SHSP. We also make a C code program.

(Table 4) Hardware specification of class 3 device

80C320 25MHz 8-bit MICOM, 128KB ROM, 32KB RAM

5.2 Test results

Most Devices except a class3 would have an input system, so we utilize these four devices as command input systems and the destination ones can be controlled. We use two different test scenarios. One is a control of a class3

in-home device by a remote user device, and the other is a control of a class2 device by a class1.

In the first test case, a remote user will access the RG and change the state of a control point in a class3 in-home device. In this test, we implement a light controller and the state of the light is switched (turn on/off). If there is no delay, the response time of the overall operation is within 1 second and its operating procedure is as follows;

1) A user executes the remote user application program with appropriate certificates (password and IP address of target RG).
2) Using the permission of certificates, the program makes a SSL session between the remote user device and RG. The RG asks both an ID and password to authenticate a user.
3) Now, a remote user can access the RG legitimately and control a lamp at home.
4) The RG receives the command message and then checks whether the session key is valid or not. If not, the RG and end device would share a new session key using the SHSP.
5) Using the valid session key, the RG communicates with the end device securely.
6) The end device will control the lamp.

In the second test case, we assume that all of in-home devices are already registered at a RG and it knows the master key of each device. Someone who uses an in-home device should be a legitimate one because he/she already is at home. Therefore, we don't need to authenticate the user. According to the test scenario, a class1 device user accesses the RG and changes the value of a control register of a class2 device. The device is a TV in a room and it is controlled to adjust channels, volume and brightness. The response time is much faster than the previous one due to the use of intra-networks. The overall operating procedure is as follows;

1) A user puts a control command in the class1 in-home device. The user executes the application program for class1, selects a target device that is a class2, chooses the control register, and sets the value, successively. The command message is sent to the RG securely.
2) The RG receives the command message and checks whether a session key is valid or not. If not, the RG and the device would share a new session key using the SHSP.
3) Using the valid session key, the RG communicates with the device securely.
4) According to the command, the device is controlled and displays the adjustment on an LCD of the TV.

The home network model operates correctly within an appropriate response time in the test environment. So the proposed model is applicable to a real home network system.

6. Conclusion

In this paper, we propose a secure home network model and a smart home security protocol (SHSP). The standardization activity in the provision of a residential gateway is getting larger [6]. In the model, a RG plays a central role and it meets the international trends and standards. We classify the in-home networks into class1, class2, and class3 sub-networks and then apply suitable secure schemes to each of them separately. We design a much secure, effective and practical home network model. Moreover, we propose a minimal and optimal authenticated key distribution protocol. The proposing SHSP is a light, efficient and secure 3-party authenticated key distribution protocol for heterogeneous home networks. Through implementation and valid tests, the proposing secure smart home is verified to be secure and realistic with reasonable response time.

References

[1] W. Choi, J. Kim, S. Lee, E. Park, "Smart home and internet of things: A bibliometric study," *Journal of Cleaner Production*, vol. 301, 126908, June, 2021. https://doi.org/10.1016/j.jclepro.2021.126908

[2] X. Wang and Z. Jin, "An Overview of Mobile Cloud Computing for Pervasive Healthcare," in *IEEE Access*, vol. 7, pp. 66774-66792, May, 2019. https://doi.org/10.1109/ACCESS.2019.2917701

[3] P. Janson and G. Tsudik, “Secure and minimal protocols for authenticated key distribution,” *Computer Communications*, vol. 18, Issue 9, pp. 645-653, Sep., 1995. https://doi.org/10.1016/0140-3664(95)99807-O

[4] R. Bird, I. Gopal, A. Herzberg, P. Janson, S. Kutten, R. Molva, M. Yung, “Systematic design of a family of attack-resistant authentication protocols,” *IEEE Journal on Selected Areas in Communications*, Vol. 11, Issue 5, pp. 679-693. 1993. https://doi.org/10.1109/49.223869

[5] R. Needham, M. Schroeder, “Using encryption for authentication in large networks of computers,” *Comm. of the ACM*, Vol, 21, Issue 12, pp. 993-999. Dec., 1978. https://doi.org/10.1145/359657.359659

[6] Wacks, “Home systems standards: achievement and challenges,” *IEEE Communications Magazine*, Vol. 40, Issue 4, pp. 152-159, April 2002. https://doi.org/10.1109/35.995865

[7] P. Janson, G. Tsudik, M. Yung, “Scalability and flexibility in authentication services: The kryptoKnight approach,” Proceedings of INFOCOM ’97, *IEEE*, April, 1997. https://doi.org/10.1109/INFCOM.1997.644526

[8] T. Zahariadis, K. Pramataris, N. Zervos, “A comparison of competing broadband in-home technologies,” *Elect. and Comm. Eng. Journal*, Vol. 14, Issue 4, pp. 133-142, Aug., 2002. https://doi.org/10.1049/ecej:20020401

[9] R. Bird, I. Gopal, A. Herzberg, P. Janson, S. Kutten, R. Molva, M. Yung, “The KryptoKnight family of authentication and key distribution protocols,” *IEEE/ACM Trans. on Netw.*, March 1995.

[10] R. Bird, I. Gopal, A. Herzberg, P. Janson, S. Kutten, R. Molva, M. Yung, “The KryptoKnight family of light-weight protocols for authentication and key distribution,” *IEEE/ACM Trans. Netw.*, Vol. 3, Issue 1, pp. 31-41, 1995. https://doi.org/10.1109/90.365435

◐ Authors ◑

Sang-kon Kim (김 상 곤)

He received the Ph.D. degree in electrical and computer engineering from Seoul National University, Seoul, Korea, in 2008. He is currently an assistant professor of Electronics and Information Engineering in Korea University. His research interests include wired and wireless networks and communications, network and computer security, and e-health.

E-mail: paulka@korea.ac.kr

Tae-kon Kim (김 태 곤)

He received the Ph.D. degree in electrical engineering from the Pennsylvania State University, University Park, PA, in 2001. From 2001 to 2002, he was with Technology & Research Labs, Intel Corporation, Chandler, AZ. From 2003 to 2004, he was with Digital Media R&D center, Samsung Electronics, Suwon, Korea. Since 2005, he has been with Korea University, Korea, where he is an associate professor of Electronics and Information Engineering. His research interests include multimedia signal processing, wireless networks and communications, and e-health.

E-mail : taekonkim@korea.ac.kr