Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.25, NO.2, Apr. 2015 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2015.25.2.479

스마트홈 환경에서의 안전한 디바이스 관리를 위한 그룹키 관리 기법*

류 호 석,[1†] 곽 진[2‡]
[1]아주대학교 컴퓨터공학과 정보보호응용및보증연구실, [2]아주대학교 정보컴퓨터공학과

Group Key Management Method for Secure Device in Smart Home Environment*

Ho-seok Ryu,[1†] Jin Kwak[2‡]
[1]ISAA Lab., Department of Computer Engineering, Ajou University,
[2]Department of Information and Computer Engineering, Ajou University

요 약

IT 발전에 따라 스마트홈 서비스는 네트워크 기반의 스마트 디바이스를 통해 원격 서비스, 모니터링 서비스 등 다양한 서비스를 제공하고 있다. 그러나 스마트홈 환경에서는 악성 디바이스를 통한 데이터 위·변조, 불법 인증, 프라이버시 침해 등과 같은 보안 위협들이 존재한다. 이러한 보안 위협들에 대응하기 위한 스마트홈 환경에서의 보안에 대한 연구가 활발히 진행되고 있으나 디바이스 관리를 위한 연구는 초기 단계에 머물고 있으며, 스마트홈 환경에서의 그룹키 관리에 대한 연구가 부족한 실정이다. 따라서 본 논문에서는 스마트홈 환경에서 안전한 디바이스 관리를 위한 그룹키 관리 기법을 제안한다.

ABSTRACT

According to IT development, smart home services is providing remote service, monitoring service and other various services through smart home devices based on network. But, smart home environment exists security threats such as data falsification, illegal authentication and invasion of privacy through a malicious device. Smart home is studying to prevent these security threats, but the studies of smart home environment security are still in early stage of development and the studies of group key management method is lacking in smart home. In this paper, we propose the group key management method for secure device in smart home.

Keywords: Smart Home, Smart Device, Group Key, Internet of Things

I. 서 론

정보통신기술(ICT : Information Communication Technology)의 발달로 최근 스마트 디바이스 이용이 대중화됨에 따라 스마트 디바이스와 연동이 가능한 스마트홈, 스마트 헬스케어, 스마트 의료 등의 환경에서 스마트 디바이스에 대한 이용이 증가하고 있다[1].

스마트홈은 기존의 가정환경에서 정보통신기술을 융합하여 사용자와 가전기기가 실시간으로 정보와 데

접수일(2015년 2월 12일), 수정일(2015년 4월 6일), 게재확정일(2015년 4월 6일)
* 이 논문은 2014년도 정부(미래창조과학부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No.NRF-2014R1A2A1A11050818).
† 주저자, ryuhs@ajou.ac.kr
‡ 교신저자, security@ajou.ac.kr(Corresponding author)

이터를 송수신하는 지능형 가정환경을 의미한다. 이러한 스마트홈은 홈플랫폼 기술, 유무선 네트워크 기술, 스마트 디바이스 기술, 그린홈 기술로 나눌 수 있으며, 사용자가 스마트 디바이스 간의 유무선 네트워크 기술을 통해 실시간으로 디바이스를 제어할 수 있다[2,3]. 이러한 통신으로 사용자가 외부에서도 스마트홈에 접근하여 원격 검침 시스템, 냉·난방 시스템 제어, 조명 제어, 가전제품 제어 등의 서비스를 제공받을 수 있다[4].

하지만, 스마트홈 통신 구조는 스마트 디바이스가 네트워크 기능을 탑재한 만큼 기존의 통신 환경에서 존재하는 보안 위협들이 존재한다. 네트워크 기능을 통해 악성 디바이스가 접근할 경우 기존의 통신 환경에서의 데이터 위·변조, 불법 인증, 프라이버시 침해 등과 같은 보안 위협들이 존재할 뿐만 아니라 기술의 융합으로 새로운 보안 위협이 등장하고 있다. 또한 스마트홈의 특성으로 인해 2차 피해의 위험도 존재한다[5].

본 논문에서는 안전하고 효율적인 스마트홈 환경을 구축하기 위해 스마트홈 환경에 적합한 디바이스 관리를 위한 그룹키 관리 기법을 제안한다. 제안하는 기법은 스마트홈 환경에서 발생 가능한 공격으로부터 안전하고 효율적인 그룹키 관리 기법으로 사용자가 외부에서 통신하기 위한 해쉬 기반의 그룹키를 공유하게 된다. 따라서 본 논문에서는 스마트홈 환경에서의 안전한 통신을 구축하기 위해 보안 요구사항을 분석하고, 스마트홈 환경에 적합한 디바이스 관리 기법을 제안한다.

본 논문의 구성은 다음과 같다. 먼저 2장에서는 스마트홈 통신과 스마트홈 환경에서 제안된 인증 기법들을 분석하고 스마트홈 환경의 보안 요구사항을 분석한다. 다음으로 3장에서는 스마트홈 환경에서의 안전한 디바이스 관리를 위한 그룹키 관리 기법을 제안하고, 4장에서는 제안하는 프로토콜의 안전성과 효율성을 분석하고 마지막으로 5장에서 결론을 내린다.

II. 관련 연구

2.1 스마트홈 통신

스마트홈은 가전기기와 전자기기에 무선 네트워크가 탑재되면서 사용자에게 많은 서비스를 제공하고 있다. 스마트홈의 통신은 스마트홈 디바이스들 간의 유무선 네트워크를 통해 구성되어 있으며, 시간과 장소의 제약 없이 어디서나 스마트홈을 관리하고 서비스를 제공받을 수 있다. 모든 가전기기의 자동화와 스마트화로 스마트홈은 더욱 편리하고 유용한 서비스를 제공한다.

스마트홈의 유무선 네트워크 기술은 스마트간의 접속을 보장하고 제공하고 있다. 그중에서도 무선 네트워크 기술은 Wifi, 3G/4G/LTE, Bluetooth, Ethernet 등 고속화, 저전력 기술로 스마트홈 디바이스에 탑재되어 진화하고 있다. 스마트홈에서 디바이스 기술은 기존 가전기기와 센서 디바이스에 CPU, 유무선 네트워크 기술의 탑재로 스마트화됨으로써 사용자들에게 원격으로 스마트홈 서비스를 제공하고 있다. 이러한 스마트 디바이스와 네트워크 기술로 사용자가 외부에서 모바일 디바이스를 이용해 스마트홈 서비스를 제공받을 수 있다[6,7].

2.2 스마트홈 인증 기법

2.2.1 Mantoro 등의 연구

Mantoro 등의 연구[8]에서는 모바일 디바이스와 스마트홈 디바이스 사이의 안전한 통신을 제안하였다. 제안된 기법은 사용자가 공개키와 스마트홈 디바이스의 패스워드를 모바일 디바이스와 모든 스마트홈 디바이스에 할당하고 각 스마트홈 디바이스의 데이터베이스에 공개키와 패스워드를 저장하여 접근을 허용하는 시스템이다. 제안된 방식은 공개키로 암호화를 수행하여 중간자 공격에 안전한 시스템이다. 하지만 모든 스마트홈 디바이스의 패스워드와 공개키를 각 스마트홈 디바이스에 저장하고 있기 때문에 하나의 스마트홈 디바이스가 위험에 노출될 경우, 데이터 위·변조뿐만 아니라 전체 스마트홈 시스템의 위험을 초래할 수 있다. 또한 공개키 기반으로 스마트홈 디바이스를 인증함으로써 스마트홈 디바이스에는 부담될 뿐만 아니라 각 스마트홈 디바이스가 모든 패스워드와 공개키를 저장하고 있기 때문에 스마트홈 내의 스마트홈 디바이스가 증가할수록 효율성이 떨어지는 단점이 있다.

2.2.2 Shin 등의 연구

Shin 등의 연구[9]에서는 유비쿼터스 환경에서 그룹 통신을 위한 인증 기법에 제안하였다. 제안된

방식은 사용자가 세션을 연결하기 위해 티켓을 발급 받고 티켓으로 각 세션을 연결한다. 스마트 디바이스를 티켓을 통해 인증을 수행하여 스마트 디바이스의 연산을 최소화하여 효율적으로 인증을 수행한다. 하지만 디바이스의 무결성을 검증하는 과정이 없어 데이터의 위·변조와 재전송 공격이 가능하다. 이러한 경우 악성 디바이스가 접근한다면 스마트홈 시스템 전체의 위험을 초래할 수 있다. 또한 관리하는 그룹의 디바이스가 증가할수록 티켓의 수가 많아짐에 따라 효율성이 떨어질 수 있다.

2.2.3 Park의 연구

Park의 연구[10]는 유비쿼터스 환경에서 모바일 디바이스 인증 방식으로 공개키 기반 구조를 이용한 기법이다. 이 기법은 티켓을 발급 받기 위해 모바일 사용자가 서버에 등록하는 등록과정과 티켓을 발급받는 과정으로 이루어져 있다. 하나의 티켓을 통해 여러 서비스 서버에 제출함으로써 서비스를 제공받는다. 하지만 사용자 인증 메시지와 티켓을 전송하는 과정에서 공개키 알고리즘을 사용함으로써 모바일 디바이스에 많은 연산 오버헤드를 초래한다. 따라서 고속화, 저전력을 요구하는 환경에서는 효율성이 떨어지고 연산량에도 부담을 주는 단점이 있다.

2.3 보안 요구사항

스마트홈 환경에서는 데이터 위·변조, 불법 인증, 프라이버시 침해 등의 보안 위협이 존재하며, 이에 대응하는 보안 기법 연구가 필요하다. 따라서 본 절에서는 스마트홈 환경에서의 안전한 통신을 위한 보안 요구사항들을 분석한다[11].

2.3.1 데이터 기밀성

스마트홈 통신 환경에서는 개인정보 및 제어 메시지 등 프라이버시 침해가 가능한 민감 정보들이 네트워크를 통해 전송된다. 따라서 비인가된 제3자가 데이터의 내용을 알 수 없도록 통신 시, 데이터를 암호화하여 송·수신해야한다.

2.3.2 접근제어

스마트홈 통신 환경에서는 데이터에 대한 읽기 및 변경 등의 모든 접근권한이 구분되어야 한다. 허가되지 않은 디바이스의 접근시도를 사전에 차단하여 보안 위협들을 예방해야한다.

2.3.3 디바이스 무결성

스마트홈 디바이스는 네트워크로 접근이 가능하고 물리적인 접근이 가능하기 때문에 디바이스의 보호장치가 필요하다. 또한 공격자가 악성 소프트웨어를 삽입하고 악성코드를 통해 용도를 변경할 수 있다. 만약 무결성이 보장되지 않는 다면 스마트홈 시스템 전체가 악성코드에 감염되거나 스마트홈 시스템의 가용성이 손상될 수 있다. 따라서 스마트홈 디바이스의 무결성이 필요하다.

2.3.4 디바이스 인증

스마트홈 디바이스의 경우 보안을 고려하지 않고 사용되는 디바이스들이 많이 존재하며 무선 네트워크를 통해 인증되지 않은 스마트 디바이스들의 접근이 가능하다. 폐기 및 복제된 스마트홈 디바이스가 접근할 경우 악성코드를 삽입하거나 스마트홈 통신 환경을 오염 시키는 등 악의적으로 사용될 가능성이 있다. 또한 공격자가 정상적인 디바이스로 위장할 경우 사용자의 정상적인 사용이 불가능할 수 있다. 따라서 스마트홈 디바이스에 대한 인증이 제공되어야 한다.

III. 제안사항

본 장에서는 스마트홈 환경에서의 안전한 디바이스 관리를 위한 그룹키 관리 기법을 제안한다. 제안하는 그룹키 관리 기법은 새로운 스마트홈 디바이스를 스마트홈 서버에 등록하여 그룹키를 생성하는 가입 프로토콜과 사용자가 외부에서 스마트홈 디바이스와 통신하는 통신 프로토콜, 스마트홈 디바이스의 노후 및 고장으로 인해 디바이스를 교체 및 제거하는 탈퇴 프로토콜로 구성되어 있다.

제안하는 그룹키 관리 기법은 스마트홈 디바이스들을 인증하고 스마트홈 디바이스 간의 그룹키를 통해 통신하는 시스템을 제안한다.

3.1 표기법

제안하는 기법에서 사용하는 파라미터는 다음

Table 1. Notation

Notation	Description
$DeviceInfo$	The smart home device's information
$DeviceInfo'$	The smart home device's information authentication requested
PW	The smart home device's password
PW'	The smart home device's password authentication requested
GK_{Home}	The smart home's group key
$GK_{Home}{}'$	The new smart home's group key
$H(\cdot)$	Hash function
H_D	Hash value of smart home device's information
M	User message
$\oplus$	XOR operation
N	Random number
T_D	Time stamp of smart home device
$\triangle T$	Valid time interval for transmission delay

Table 1.과 같다.

3.2 가입 프로토콜

스마트홈 디바이스 가입 프로토콜은 새로운 스마트홈 디바이스를 스마트홈 서버에 등록하고 그룹키를 생성하기 위한 프로토콜이며 절차는 다음과 같다.

- **Step 1.** 사용자는 스마트홈 서버의 아이디와 패스워드를 통해 직접 접근하여 새로운 스마트홈 디바이스의 정보 $DeviceInfo$(고유 시리얼 번호 및 디바이스 정보)와 패스워드 PW를 입력한다.
- **Step 2.** 스마트홈 서버는 스마트홈 디바이스의 정보 $DeviceInfo$를 해쉬하여 H_D을 생성하고 저장한다.
- **Step 3.** 스마트홈 서버는 새로운 디바이스 정보 $DeviceInfo$와 기존의 디바이스 정보 $DeviceInfo_n$까지 XOR 연산하여 새로운 스마트홈 그룹키 $GK_{Home}{}'$를 생성한다.

$$H(DeviceInfo \oplus DeviceInfo_1 \oplus DeviceInfo_2 \cdots \oplus DeviceInfo_{n-1} \oplus DeviceInfo_n) = GK_{Home}{}'$$

- **Step 4.** 스마트홈 서버는 기존의 스마트홈 디바이스들에게 새로운 스마트홈 그룹키 $GK_{Home}{}'$를 기존의 스마트홈 그룹키 GK_{Home}로 암호화하여 전송한다.
- **Step 5.** 새로운 스마트홈 디바이스는 디바이스 정보의 해쉬 값으로 디바이스 정보 $DeviceInfo'$를 암호화한 값과 패스워드 PW'를 전송하여 스마트홈 서버에게 인증을 요청한다.
- **Step 6.** 스마트홈 서버는 저장된 스마트 디바이스의 $DeviceInfo$와 PW와 인증 요청된 $DeviceInfo'$와 PW'를 비교하여 디바이스를 인증한다.

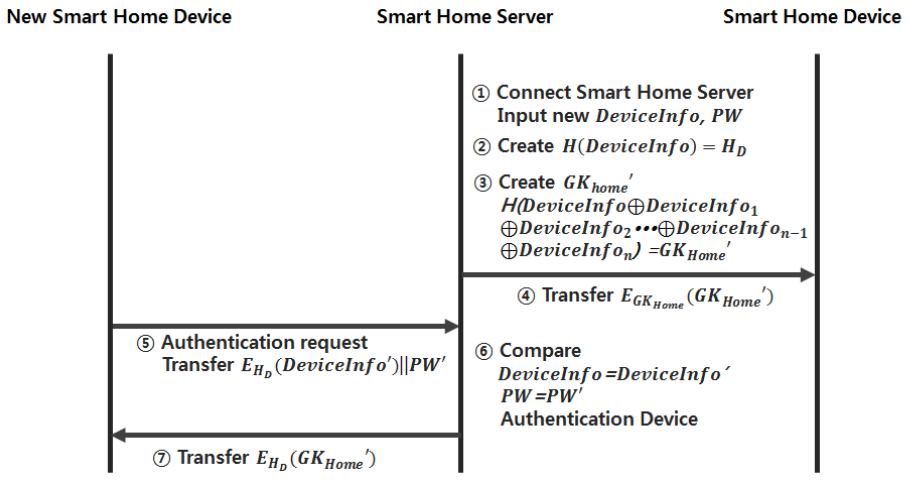


Fig. 1. Smart home device join protocol

- **Step 7.** 스마트홈 서버는 갱신된 스마트홈 그룹키 $GK_{Home}{}'$를 인증 요청한 스마트홈 디바이스 정보의 해쉬 값으로 암호화하여 전송한다.

3.3 통신 프로토콜

사용자가 외부에서 스마트홈에 접근하여 메시지를 전송하거나 데이터를 전송 받기 위해 세션을 연결하는 프로토콜이며 절차는 다음과 같다.

- **Step 1.** 사용자는 외부에서 등록된 모바일 디바이스를 이용하여 스마트홈 디바이스에 접근하기 위해 모바일 디바이스의 정보 $DeviceInfo'$와 사용자의 요청 메시지 M 그리고 재전송을 막기 위한 타임스탬프 값 T_D와 임의의 난수 값 N을 스마트홈 그룹키 GK_{Home}로 암호화하여 인증 패스워드 PW'와 연접하여 전송한다.
- **Step 2.** 스마트홈 서버는 T_D의 유효성을 체크하기 위해 T_D와 전송 받았을 때의 시간 $T_D{}'$간의 차이를 전송 지연시간의 임계값 $\triangle T$과 비교한다.

$$T_D{}' - T_D \leq \triangle T$$

- **Step 3.** 스마트홈 서버는 저장된 스마트 디바이스의 $DeviceInfo$와 PW와 인증 요청된 $DeviceInfo'$와 PW'를 비교하여 디바이스를 인증한다.
- **Step 4.** 임계값과 모바일 디바이스 정보 및 패스워드가 틀려 인증되지 않을 경우 통신을 해제하고, 인증된 경우 스마트홈 디바이스에 GK_{Home}로 암호화한 M과 임의의 난수 값 N을 전송한다.
- **Step 5.** 스마트홈 디바이스는 복호화하여 사용자 메시지 M을 확인한다.
- **Step 6.** 스마트홈 디바이스는 모바일 디바이스에게 임의의 난수 값 N을 전송하여 정당함을 확인 받는다.
- **Step 7.** 스마트홈 디바이스는 모바일 디바이스와 세션을 연결하고 사용자와 검증된 프로토콜인 SSL로 통신한다.

3.4 탈퇴 프로토콜

스마트홈 서비스를 제공하던 디바이스의 노후 및 고장으로 인해 서비스를 제공하지 못하여 교체 및 제거해야 할 경우 다음과 같은 프로토콜을 수행한다.

- **Step 1.** 스마트홈 서버는 탈퇴할 디바이스 정보 $DeviceInfo$와 패스워드 PW를 삭제한다.
- **Step 2.** 스마트홈 서버는 스마트홈 디바이스들의 정보 $DeviceInfo_n$까지를 XOR 연산하여 새로운 스마트홈 그룹키 $GK_{Home}{}'$를 생성한다.

$$H(DeviceInfo_1 \oplus DeviceInfo_2 \cdots \oplus DeviceInfo_{n-1} \oplus DeviceInfo_n) = GK_{Home}{}'$$

- **Step 3.** 스마트홈 서버는 스마트홈 디바이스들에게 새로운 스마트홈 그룹키 $GK_{Home}{}'$를 각 디바이스들의 해쉬 값 H_D으로 암호화하여 전송한다.

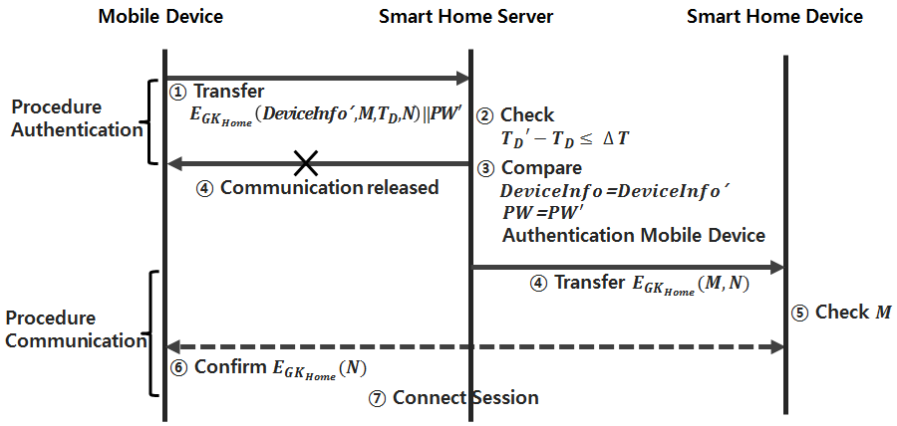


Fig. 2. Smart home device communication protocol

- **Step 4.** 스마트홈 디바이스는 기존의 스마트 홈 그룹키 GK_{Home}를 삭제하고 새로운 스마트 홈 그룹키 $GK_{Home}{}'$를 저장한다.
- **Step 5.** 스마트홈 서버는 기존의 그룹키 GK_{Home}를 삭제한다.

IV. 안전성 및 효율성

본 장에서는 제안하는 스마트홈 환경에 적합한 디바이스 관리 기법에 대해 안전성 및 효율성을 분석한다.

4.1 안전성

4.1.1 기밀성

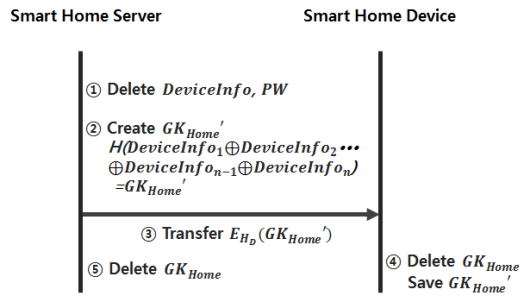
스마트홈 디바이스에는 개인정보 및 제어 메시지 등 프라이버시 침해가 가능한 민감 정보를 가지고 있기 때문에 기밀성을 보장되어야 한다. 본 논문에서 제안하는 디바이스 관리 기법은 디바이스 정보의 H 값을 통해 그룹키 GK_{Home}를 분배하기 때문에 스마트홈 서버에 등록되지 않은 디바이스일 경우 그룹키를 복호화 할 수 없고 하나의 스마트홈 디바이스 $DeviceInfo$가 유출되더라도 다른 디바이스 정보 $DeviceInfo_n$의 H_D 값을 알 수 없기 때문에 스마트홈 그룹키 GK_{Home}를 복호화 할 수 없다. 또한, 그룹키 GK_{Home}를 통해 데이터를 암호화하여 송·수신하기 때문에 데이터의 기밀성을 제공한다. 그러므로 제안하는 기법은 기밀성을 제공한다.

4.1.2 접근제어

스마트홈 통신 환경에서는 개인정보 및 민감 정보가 존재하기 때문에 허가되지 않은 디바이스에 대한 접근시도를 사전에 차단되어야 한다. 본 논문에서 제안하는 디바이스 관리 기법은 스마트홈 서버에 디바이스 정보 $DeviceInfo$를 통해 스마트홈 시스템으로 정상적인 접근이 가능한 디바이스인지 여부를 판단받는다. 그러므로 허가되지 않은 디바이스는 스마트홈 시스템에 접근할 수 없다.

4.1.3 디바이스 무결성

스마트홈 디바이스는 공격자가 악성 소프트웨어를



Fig, 3. Smart home device leave protocol

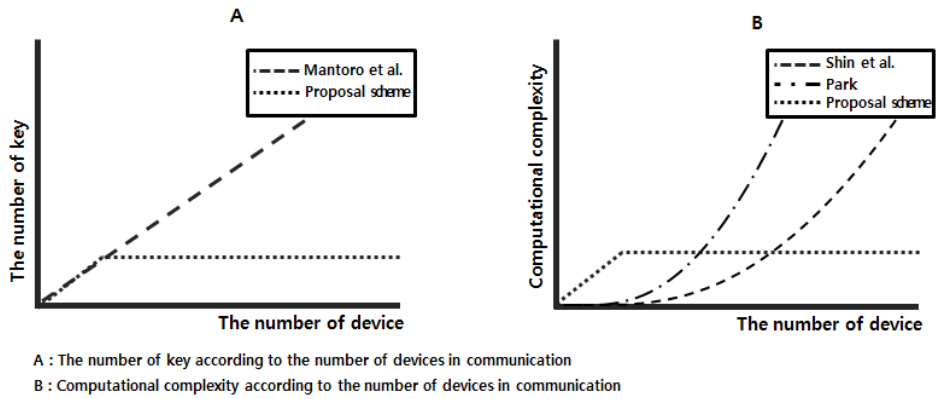
삽입하거나 악성코드로 디바이스의 용도를 변경하고 통신 네트워크를 감염시킬 수 있다. 본 논문에서 제안하는 스마트홈 디바이스 관리 기법은 스마트홈 디바이스 정보를 해쉬하여 해쉬 값 H_D을 저장함으로써 스마트홈에 추가되는 디바이스의 정보 또는 변경되는 디바이스 정보에 대해 무결성을 제공한다. 또한 스마트홈에 등록되지 않은 스마트 디바이스의 접근은 불가능하며, 하나의 스마트 디바이스의 정보를 획득하더라도 모든 스마트 디바이스의 해쉬 값 H_D을 알 수 없기 때문에 그룹키 GK_{Home}를 알 수 없다.

4.1.4 디바이스 인증

인증되지 않은 스마트 디바이스의 접근을 통해 악성코드를 삽입하고 악성메일을 보내는 좀비 스마트 디바이스 및 DDoS 공격을 발생시키는 좀비 스마트 디바이스들이 증가하고 있다. 본 논문에서 제안하는 시스템은 최초 등록 과정에서 각 디바이스들은 서버의 스마트홈의 그룹키 GK_{Home}를 나눠 갖고 저장함으로써 비인가 스마트 디바이스의 접근을 막을 수 있으며 디바이스에 대한 인증을 제공한다.

Table 2. Security comparisons between existing method and our proposal

Security	Mant-oro et al.	Shin et al.	Park	Prop-osed scheme
Confidentiality	O	O	O	O
Access control	O	O	O	O
Device Integrity	X	X	X	O
Device Authentication	O	O	O	O



Fig, 4. Efficiency comparisons between existing method and our Proposal

4.2 효율성

본 논문에서 제안하는 기법은 스마트홈 서버에서 생성한 하나의 그룹키 GK_{Home}를 기반으로 스마트홈 디바이스를 인증함으로써, 스마트 디바이스의 정보와 스마트 디바이스의 공개키를 각 디바이스가 저장하고 있는 Mantoro 등의 연구와는 달리 효율적이다. 또한 Shin 등의 연구는 그룹의 멤버가 증가할수록 티켓의 수가 증가하여 연산량이 많아지고, Park의 연구는 공개키 기반의 알고리즘을 사용함으로써 많은 연산 오버헤드를 초래한다. 하지만 본 논문에서 제안하는 기법은 스마트홈 서버가 하나의 그룹키 GK_{Home}를 생성함으로써 디바이스가 증가하여도 연산량은 같기 때문에 효율적이다. 따라서 본 논문에서 제안하는 기법은 Mantoro 등의 연구, Shin 등의 연구, Park의 연구보다 효율적이라 할 수 있다.

V. 결 론

IoT 기술의 발전으로 스마트홈 기술은 지속적으로 발전하며 스마트 디바이스 간의 자유로운 네트워크 통신을 통해 사용자에게 다양한 서비스를 제공하고 있다. 그러나 스마트 디바이스에 네트워크 기능이 탑재됨에 따라 기존 통신에서의 악성 스마트 디바이스 위장, 불법 인증, 프라이버시 침해 등 다양한 보안 위협뿐만 아니라 새로운 보안 위협이 발생하고 있다. 따라서 이러한 보안 위협들을 방지할 수 있는 안전한 통신을 위한 디바이스를 관리 기법이 필요하다.

본 논문에서는 스마트홈 환경에서 보안 요구사항들을 분석하였고, 스마트홈 환경에서의 안전한 디바이스 관리를 위한 그룹키 관리 기법을 제안하였다. 제안하는 스마트홈 그룹키 관리 기법은 각 디바이스들의 정보를 연산하고 해쉬하여 생성된 그룹키를 기반으로 악성 스마트 디바이스의 접근 및 인증을 차단할 수 있고, 스마트홈의 그룹키를 통해서만 통신함으로써 스마트홈에서의 안전한 통신을 할 것으로 기대한다. 또한 제안하는 그룹키 관리 기법은 저전력 기반의 경량화된 전력 시스템에서도 활용 가능하기 때문에 다양한 환경에 적용될 것으로 기대된다.

현재 스마트홈은 우리나라뿐만 아니라 외국에서도 스마트홈 관련 연구들이 활발하게 진행되고 있다. 스마트홈은 민감 정보를 가지고 있기 때문에 안전한 통신이 매우 중요한다. 이에 따라 본 논문에서 제안하는 스마트홈에서의 안전한 디바이스 관리를 위한 그룹키 관리 기법은 안전한 스마트홈 환경의 연구 및 개발에 도움이 될 것으로 기대한다.

References

[1] Ho-won Kim and Dong-kyu Kim, "IoT technology and security," Korea Institute of Information Security & Cryptology, 22(1), pp. 7 - 13, Feb. 2012

[2] Hwa-jeong Suh, Dong-gun Lee, Jong-seok Choe, and Ho-won Kim, "IoT security technology trends," The Korea Institute of Electromagnetic Engineering and Science, 24(4), pp. 27 - 35, July. 2013

[3] Raj, S.V., "Implementation of pervasive computing based high-secure smart

home system," Computational Intelligence & Computing Research (ICCIC), 2012 IEEE International Conference on, pp. 1-8, Dec. 2012.

〔4〕 Tae-woong Lee, Cheol-su Son, and Won-jung Kim, "The implement of intelligent home network system on smart phone," The Korea Institute of Electronic Communication Sciences, 6(4), pp. 505-509, Aug. 2011

〔5〕 A. Wright, "Cyber security for the power grid: cyber security issues & securing control systems," ACMCCS, Nov. 2009.

〔6〕 Kuba, M., Klatt, M., Ronge, K. and Weigel, R., "Automatic communication standard recognition in wireless smart home networks," Consumer Communications and Networking Conference (CCNC), 2012 IEEE, pp 270-274, Jan. 2012.

〔7〕 Seong-gu Sim, Ho-jin Park, and Jun-hee Park, "Smart home standardization construction and strategy," The Korea Institute of Information Scientists & Engineers, 30(8), pp. 19 - 25, Aug. 2012

〔8〕 Mantoro, T., Adnan, M.A.M., Ayu, and M.A., "Secured communication between mobile devices and smart home appliances," Advanced Computer Science Applications and Technologies (ACSAT), 2013 International Conference on, pp. 429-434, Dec. 2013.

〔9〕 Soo-bok Shin, Hong-jin Yeh, and Kang-seok Kim, "A ticket based authentication scheme for group communication," In Proceedings of The 2012 International Conference on Information Security and Assurance, pp. 152-155, Apr. 2012.

〔10〕 Jong-hyuk Park, "An authentication protocol offering service anonymity of mobile device in ubiquitous environment," The Journal of Supercomputing, vol 62, no 1, pp. 105-117, Oct. 2012.

〔11〕 Dong-hee Kim, Seok-woong, and Yong-pil Lee, "Security services for IoT," The Korea Institute of Communications and Information Sciences, 30(8), pp. 53-59, July. 2013.

〈저자소개〉

류 호 석 (Ho-seok Ryu) 학생회원
2014년 2월: 순천향대학교 정보보호학과(공학사)
2014년 2월~2015년 2월: 순천향대학교 정보보호학과 석사과정
2015년 3월~현재: 아주대학교 컴퓨터공학과 석사과정
〈관심분야〉 스마트홈 보안, 사물인터넷 보안, 응용시스템 보안, 디지털 포렌식

곽 진 (Jin Kwak) 종신회원
2000년 8월: 성균관대학교 학사
2003년 2월: 성균관대학교 석사
2006년 2월: 성균관대학교 박사
2006년 4월~2006년 11월: 일본 큐슈대학교 방문연구원
2006년 8월~2006년 11월: 일본 큐슈시스템정보기술연구소 특별연구원
2006년 11월~2007년 2월: 정보통신부 정보보호기획단 개인정보보호팀 통신사무관
2007년 1월~2009년 12월: 정보통신연구진흥원 주간기술동향 집필위원
2007년 1월~현재: 한국정보기술융합학회 이사
2007년 3월~2015년 2월: 순천향대학교 정보보호학과 교수
2008년 1월~현재: 한국정보보호학회 논문지편집위원
2008년 1월~현재: 한국정보보호학회 이사
2008년 4월~현재: 한국인터넷정보학회 논문지편집위원
2008년 12월~현재: 정보통신산업진흥원 기술평가위원
2009년 1월~2009년 12월: 순천향대학교 공과대학 교학부장
2009년 1월~2010년 12월: 순천향대학교 정보보호학과 학과장
2009년 5월~현재: TTA 표준화로드맵 기술표준기획전담반 위원
2010년 1월~2012년 12월: 순천향대학교 SCH BIT 창업보육센터장
2010년 3월~현재: 조달청 기술평가위원
2010년 5월~2010년 7월: 교육과학기술부 국가기술수준평가 위원
2011년 1월~현재: 한국정보처리학회 이사
2011년 1월~현재: JIPS 논문지 편집위원
2011년 2월~2012년 12월: 순천향대학교 중소기업산학협력센터 센터장
2011년 7월~현재: 지식경제부 지식경제기술혁신평가단 위원
2012년 ~현재: 한국암호포럼 운영위원
2012년 ~현재: 한국방송통신전파진흥원 평가위원
2013년 ~현재: 교육부 정책자문위원
2013년 ~현재: 금융보안연구원 보안기술 자문위원
2013년 ~현재: 금융감독원 인증방법평가위원
2015년 3월~현재: 아주대학교 정보컴퓨터공학과 교수
〈관심분야〉 자동차 보안, 암호프로토콜, 응용시스템 보안, 클라우드 컴퓨팅 보안, 개인정보보호, 정보보호제품평가