Journal of the Korea Academia-Industrial cooperation Society
Vol. 19, No. 10 pp. 661-667, 2018

https://doi.org/10.5762/KAIS.2018.19.10.661
ISSN 1975-4701 / eISSN 2288-4688

스마트 홈 환경에서 디바이스 상호 인증 및 키 관리 기법

민소연[1*], 이재승[2]
[1]서일대학교 정보통신공학과, [2]숭실대학교 컴퓨터공학과

Device Mutual Authentication and Key Management Techniques in a Smart Home Environment

So-Yeon Min[1*], Jae-Seung Lee[2]
[1]Dept. of Information and Communication Eng., Seoil University
[2]Dept. of Computer Science and Eng., Soongsil University

요 약 최근 무선 통신 기술과 센서 디바이스들의 발달로 스마트 홈 시장이 성장하고 있으며, 다양한 디바이스가 활용되고 있다. 이러한 사물인터넷 환경은 지능형 서비스를 위해 다양하고 방대한 양의 디바이스 정보를 수집하여 사용자 정보를 기반으로 서비스를 제공받으며, 다양한 디바이스를 제어해야 하고, 이기종 간의 통신을 제공해야 한다. 하지만, 이러한 성장과 함께, 스마트 홈 환경에서는 다양한 보안 위협이 발생하고 있다. 실제, 프루프 포인트와 HP에서는 스마트 홈 환경에서의 피해 사례 및 보안 취약점의 심각성에대해 경고하였으며, 다양한 환경에서의 침해 사례가 발표되었다. 그러므로, 본 논문에서는 스마트 홈 환경에서 발생할 수 있는 보안 문제를 해결하기 위해 스마트 홈에서 사용하는 스마트 노드들 간의 안전한 상호 인증 기법에 대해 연구를 수행하였다. 제안하는 논문의 경우 보안성 평가를 통해 스니핑, 스푸핑, 디바이스 상호 인증, 중간자 공격, 무결성 등 사물인터넷 환경과 센서 디바이스에서 발생할 수 있는 잘 알려진 취약점에 대해 난수와 수시로 갱신되는 세션키 및 비밀키를 이용하여 안전함을 검증하였다. 또한, 기존에 연구된 사물인터넷 보안 프로토콜과의 비교를 통해 보안성 및 키 관리 측면에서 우수함을 확인할 수 있었다.

Abstract Recently, the smart home market is growing due to the development of wireless communication technology and sensor devices, and various devices are being utilized. Such an IoT environment collects various vast amount of device information for intelligent services, receives services based on user information, controls various devices, and provides communication between different types of devices. However, with this growth, various security threats are occurring in the smart home environment. In fact, Proofpoint and HP warned about the cases of damage in a smart home environment and the severity of security vulnerabilities, and cases of infringement in various environments were announced. Therefore, in this paper, we have studied secure mutual authentication method between smart nodes used in smart home to solve security problems that may occur in smart home environment. In the case of the proposed thesis, security evaluations are performed using random numbers and frequently updated session keys and secret keys for well-known vulnerabilities that can occur in IoT environments and sensor devices such as sniffing, spoofing, device mutual authentication, And safety. In addition, it is confirmed that it is superior in security and key management through comparison with existing smart home security protocol.

Keywords : Smart Home, Smart Home Authentication, Smart Home Security, Device Authentication, IoT Security

본 논문은 2018년도 서일대학교 학술연구비에 의해 연구되었음
*Corresponding Author : So-Yeon Min(Seoil Univ.)
Tel: +82-2-490-7583 email: symin@seoil.ac.kr
Received September 17, 2018 Revised October 1, 2018
Accepted October 5, 2018 Published October 31, 2018

1. 서론

최근 통신 기술의 발전과 스마트 디바이스의 발달로 인해 스마트 디바이스 종류가 기하급수적으로 증가하고 있으며, 점점 스마트 디바이스를 통한 서비스와 개발영역이 확장되어, 전 세계 스마트 홈 시장이 급격히 성장하고 있다. 실제 시장 조사 기관 Strategy Analytic에 따르면 2012년 미국의 경우 스마트 홈 시장의 규모가 2011년 대비 55% 이상 증가하였으며, 연평균 19% 성장을 통해 오는 2019년 시장규모가 1150억 달러에 이를 것으로 예상하고 있다[1-2]. 또한, 유럽의 스마트 홈 시장 의 경우 2012년 전년 대비 82% 이상 상승하여 약 31억 달러의 규모를 달성하였으며, 연평균 성장률 26%이상의 성장률을 기록하고 있다. 이러한 스마트 홈 시장의 성장은 다양한 사업자 진영의 사업전개로 시장이 확산되고 있으며, 최근 스마트 홈 시장은 가전제품, 통신 및 보안 서비스, 모바일, 유틸리티 등 다양한 분야의 기업들이 적극적으로 참여하고 있는 상황에서, 급격한 성장세를 보이고 있는 사물인터넷과 M2M, 그리고 각종 센서와 웨어러블 디바이스, 동작 및 음성인식 기술 등이 융합되어, 다양한 주거 환경 서비스가 제공 될 수 있는 복합적인 디바이스 환경이 구축되고 있는 상황이다[3].

이렇듯 스마트 홈서비스 시장이 증대 되고 다양한 분야에서 활용되고 있지만, 이에 따른 보안 위협 또한 이슈되고 있다. 현재의 스마트 홈 환경의 경우 단순 환경 내에서 디바이스들이 네트워크에 연결된 수준이지만, 스마트 디바이스의 애플리케이션 개발 기술 및 기능의 발달로, 공급자 위주의 일방향식 서비스 제공구조에서 벗어날 것으로 전망하고 있으며, 이와 같이 생태계가 스마트 홈 환경에 적용 될 경우 스마트 디바이스와 함께 보안이 필수적으로 고려되어야 한다. 실제, 실리콘밸리 보안서비스업체 프루프 포인트는 지난해 발송된 전 세계 75만건 이상의 피싱·스팸 이메일이 스마트 홈 사물인터넷(IoT) 제품 해킹을 통한 것이었다고 발표하였으며, 2015년 2월 HP는 연구보고서를 통해 “스마트 홈 IoT 기기 대다수가 비밀번호 암호화, 인증 절차 등 보안에 취약하다”며 “스마트 홈 IT 기기를 사용하기 위해 개인정보를 제공해야 하기 때문에 사이버 범죄에 노출되기 쉽다”고 경고하였다[4-6].

따라서, 제안하는 논문은 스마트 홈 환경에서 발생 가능한 보안 문제를 해결하기 위해 스마트 홈에서 사용하는 스마트 노드와 원격 조종을 위한 스마트 디바이스 인증 기법을 제안 한다. 제안하는 인증 기법은 상호 인증을 통해 악의적인 사용자의 스마트 노드 접근을 방지하며, 스마트 노드 특성상 적용하기 어려운 SSL통신보다 경량화된 인증을 통해 디바이스 에너지 효율성 또한 고려하였다.

2. 관련 연구

2.1 Smart Home Network

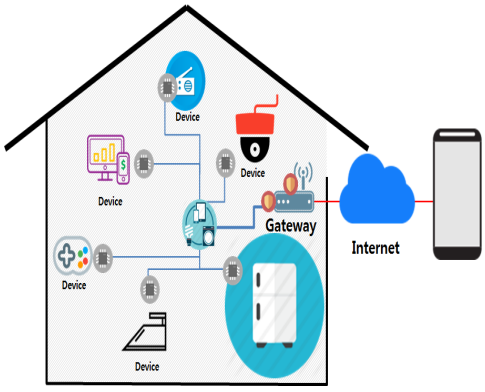

Fig. 1. SmartHome Network

스마트 홈 환경이란 사물인터넷의 발달로 홈 환경에서 디바이스들의 네트워크 연결을 통한 제어를 이용하여 가전제품의 에너지나 디바이스 상태 등을 관리하며, 제어를 함으로서 냉난방, 환기, 청소 등을 스마트 기기와 연동하여 제공해주는 솔루션과 서비스를 포함하는 개념이다. 이때, 사물인터넷의 경우 다양한 디바이스들이 생성한 정보를 공유하여 관리하는 컴퓨터 통신망을 나타내며, 이 중 스마트 홈은 가전제품과 조명 디바이스, 카메라 등은 물론 이고 스마트 자동차와 스마트교육 등을 포괄하고 있다. 즉, 우리의 주거환경에 정보통신기술을 융합하여 특별한 제약 없이 디바이스를 컨트롤하여 경제적 편의, 복지, 안전 등의 서비스를 받음으로서, 삶의 질을 한층 더 높게 만들어줄 수 있는 서비스가 스마트 홈 환경이다[7-9].

하지만, 이러한 스마트 홈 환경에서 디바이스의 취약점을 이용한 다양한 보안 사고가 발생하고 있다. 먼저, 러시아에서는 중국에서 제조된 다리미에서 해킹할 때 이용 되는 스파이 마이크로 칩이 탑재 된 사례가 있는데,

이러한 스파이 마이크로 칩은 보안되지 않은 무선 네트워크에 하여 다양한 보안 사고를 발생 시킬 수 있다. 일단 네트워크에 연결이 된다면, 해킹 프로그램, 악성코드 등을 유포 할 수 있으며, 도청되는 정보를 통해 정보를 수집하고, 이를 네트워크 통신을 이용하여 해커에게 전송하는 것이 가능하다. 실제로 이러한 스파이 마이크로 칩이 발견된 수량만 30여개에 달하고, 확인되지 않은 수량은 훨씬 더 많을 것으로 예상하고 있다. 이러한 시도는 호텔에서 자주 쓰이는 다리미나 전기 포트 등을 이용하여 세계 각국의 정치인이나 기업의 CEO 등을 타겟으로 한 공격으로 추측되고 있다. 또한, 다리미 와 전기 포트를 이용하여 네트워크 상에 존재하는 다양한 디바이스가 악성코드에 의해 감염되어 좀비PC가 만들어 졌다면, 좀비 PC를 이용한 서비스 거부 공격이나 해킹 등에 악용될 여지가 또한 존재한다[10-11].

또한, 미국의 보안업체 Proofpoint사에 의하면 2013년 말에서 2014년 초까지 약 75만 건의 스팸이나 악성코드, 피싱 프로그램 등이 전 세계의 홈 네트워크 환경의 디바이스와 라우터 등에 의해 발생 하였다. 이는 공격자들이 네트워크상에 연결된 집안의 다바이스 등을 해킹한 후, 제품에 탑재된 메일이나 송신 기능 등을 이용하여 악성 프로그램이 포함된 메일을 보냄으로서 발생하였다. 또한, 스마트 TV 카메라 기능을 이용하여 해킹한 후 집안 내부를 감시하거나, 마이크 기능을 통해 도청 또한 가능하다. 그리고, 사용자가 TV 홈쇼핑을 이용할 때, 신용카드 번호, 계좌번호, 위치정보 등의 수집함으로서 개인정보 유출의 피해가 발생할 수 있다. 이렇듯 현재 홈 네트워크 환경이 발전함에 따라, 이를 악용하는 다양한 사이버 공격이 발생하고 있다[12].

3. 제안 내용

본 논문에서는 스마트 홈 환경에서 이기종간 통신과 그린 IoT 시대에 맞춰 소형 디바이스들의 연산 량 및 에너지 효율성을 고려한 디바이스 인증 방법을 제안 하였다. 제안하는 기법은 에너지 효율성을 위해 스마트 홈 환경에서 에너지 활용에 제약이 없고 24시간 활용이 가능한 냉장고 등 대형 가전제품을 중간 역할을 하는 MD(Middle Device)로 활용 하여 배터리나 연산 량에 한계를 가지는 소형 디바이스들의 대리 역할을 할 수 있도록 인증 체계를 설계하였으며, 새로운 디바이스가 추가될 때도 안전한 인증 절차로 추가 될 수 있도록 설계하였다. 본 논문에서는 Home GW와 Service Provider 간에는 기존 공개키 시스템을 이용한 신뢰관계를 형성했다고 가정하고 진행한다.

Table 1. Proposed Notation

Notation	Meaning
ID_i	Device i ID
R_i , N_i	Device i Random Number
K_i, G_i	Key with Device i
E_i	Key I Encryption
PW	Password
S_i	Serial Number

3.1 신규 디바이스 추가 과정

스마트 홈 네트워크 환경에 새로운 디바이스가 추가되면, 디바이스는 서비스 제공을 위해 Home GW 에게 가입 요청을 위해 Service Provider 정보와 PIN Number, 랜덤한 수를 생성하여 $join\,Query$ $(ID_i, SP, E_s^i(P_i, R_i))$ 값을 Home GW에게 전송한다.

join Query를 수신한 Home GW는 요청 받은 디바이스의 검증을 위해 Service Provider에게 수신 받은 $E_s(P_i, R_i)$값과 함께 난수를 생성하여 $ID_g, E_s^g(ID_i, R_g, E_s(P_i, R_i)))$ 값을 전송한다.

Service Provider는 Home GW로부터 받은 값 $E_s^g(ID_i, R_g, E_s(P_i, R_i))$을 복호화하고, 디바이스가 암호화 하여 전송한 $E_s(P_i, R_i)$값을 복호화 하여 PIN Number를 확인 하여 검증한다.

디바이스를 검증한 Service Provider는 Home GW에게 검증 결과를 알리기 위해 ID_i, E_s^g, PW_i, E_s^i $(PW_i^g, R_s, P_i \oplus N_s))$ 값을 생성하여 전송한다.

Service Provider 로부터 값을 수신한 Home GW는 $E_s^i(PW_i^g, R_s, P_i \oplus N_s)$을 복호화 하고 $R_i' = R_g \oplus R_s$ 값을 계산한다.

이후, Home Device 와 통신을 하기 위한 키 값

$K_i^g = R_i' \oplus PW_i^g \| R_g$를 계산하고, $E_s^i(PW_i^g, R_s, P_i \oplus N_s)$값을 전송한다.

Home Device는 수신한 값 $E_s^i(PW_i^g, R_s, P_i \oplus N_s)$을 복호화 하여 $R_g' = R_i \oplus R_s$ 값을 계산하고 Home GW와 통신하기 위한 키 값 $K_i^g = R_i \oplus PW_i^g \| R_g'$를 계산한다.

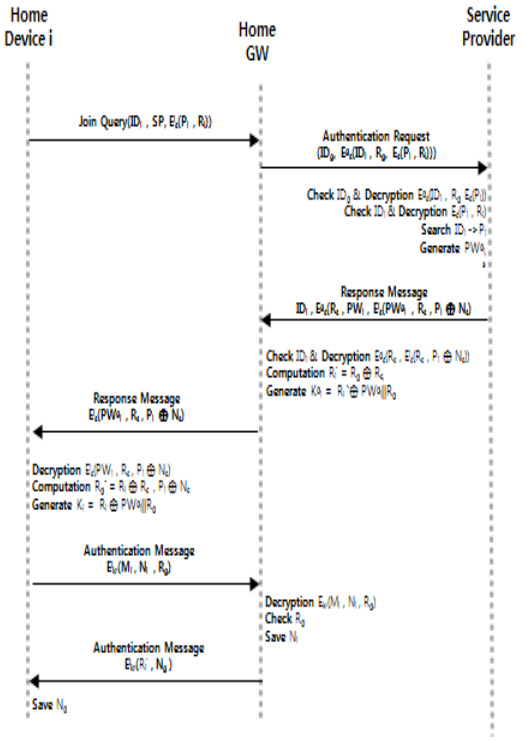

Fig. 2. Device Addition Protocol

Home Device 는 Home GW와의 인증을 위해 K_i^g로 암호화 한 값 $E_k^i(M_i, N_i, R_g)$를 전송하고 Home Device는 복호화 하여 R_g'값을 확인하고 N_i값을 저장한다. 이후, Home Device 가 검증할 수 있도록 $E_k^i(R_i', N_g)$값을 전송한다.

Home Device는 R_i'를 검증하고 이후 통신에 사용할 N_g값을 저장한다.

3.2 Middle Device 인증 과정

Middle Device는 주기적으로 새로 추가되는 디바이스를 고려하여 광고 메시지를 전송한다. 계산능력이나 배터리의 수명에 한계가 있는 소형 디바이스들은 수신된 광고 메시지 중 신호의 크기를 고려하여 Middle Device를 선정하고 $ID_i, E_k(R_i^2, N_i)$ 값을 포함하는 Join Query를 전송한다.

Middle Device는 Join Query를 보낸 디바이스의 인증을 위해 Home Device가 보낸 값에 자신의 ID와 이전 인증 과정에서 Home GW와 교환한 N값을 포함한 $ID_m, ID_i, E_k^m(N_m, E_k^i(R_i^2, N_i))$ 값을 전송한다.

값을 수신한 Home GW는 $E_k^m(N_m, E_k^i(R_i^2, N_i))$ 값을 복호화 하여 ID 와 매칭 되는 N값을 체크 한다. 이후 R_g^2과 G_i^m 값을 생성하고, $ID_i, E_s^g(R_g^2, N_i, E_s^i(R_g^2, N_m))$값을 전송한다. Middle Device는 $E_s^g(R_g^2, N_i, E_s^i(R_g^2, N_m))$값을 복호화 하고 R_g^2값을 이용하여 $R_i^{2\prime}$값과 G_i^m를 생성 한다. 다음으로 Home GW로부터 받은 $E_s^i(R_g^2, N_m)$값을 Home Device에게 전송한다.

$E_s^i(R_g^2, N_m)$ 값을 수신한 Home Device는 복호화 후 $R_m^{2\prime}$와 G_i^m를 계산하고, G_i^m를 새로운 키로 이용하여 $G_i^m(M_i, N_i^2, R_m^2)$값을 전송한다. 이를 수신한 Middle Device는 이전에 생성한 G_i^m값을 이용하여 복호화 후 $R_m^{2\prime}$값을 확인하고 검증하고, Home Device가 인증할 수 있도록 $G_i^m(R_i^2, N_g^2)$ 값을 전송한다.

이후, 인증에 활용했던 N값은 디바이스와 GW간 메커니즘에 의해 약속된 방법으로 값의 연접 및 해시 함수를 적용하여 업데이트 하며, 이후 인증에 활용 한다.

Middle Device와 인증 체계를 갖춘 디바이스는 이후 지속적인 데이터 수집된 자료의 저장이 필요할 경우 Middle Device에 의해 저장 및 전송하며, 실시간 통신이 필요할 경우에는 User Device와 직접 통신을 진행 한다.

3.3 User 접근 과정

User는 Service Provider가 제공하는 플랫폼으로 Home Device의 초기 정보를 제공 받으며, 이 정보를 통해 디바이스에 접속할 때, 인증 과정을 진행한다. 또한, 소형 디바이스의 경우 User의 요청에 따라 실시간 데이터를 원할 경우 직접 접근, 수집된 데이터의 경우

Middle Device에 접근하여 수신한다.

먼저, User가 요청 메시지와 함께 초기 정보로 제공받은 PW값을 전송하면, Home GW는 User ID를 포함하는 값 $ID_u, E_k^i(N_i^n, R_g^u, P^{2i})$를 전송 한다.

이를 수신한 디바이스는 $E_k^i(N_i^n, R_g^u, P^{2i})$값을 복호화 하고 N 값과 P 값을 체크하여 Home GW와 User의 유효성을 검증한다. 이후 R값을 이용하여 새로운 세션 키를 생성하고 응답 메시지를 전송한다. Home GW도 복호화를 이용해 N값을 검증하며, 세션 키 생성 후 응답 메시지를 전송한다. 이후, 생성된 세션 키를 이용하여 통신을 진행 한다.

Middle Device를 이용하는 경우도 거의 비슷하며, 인증에 활용되는 R값과 N값 그리고, PW값이 Middle Device에 맞춰 적용되어 진행 된다.

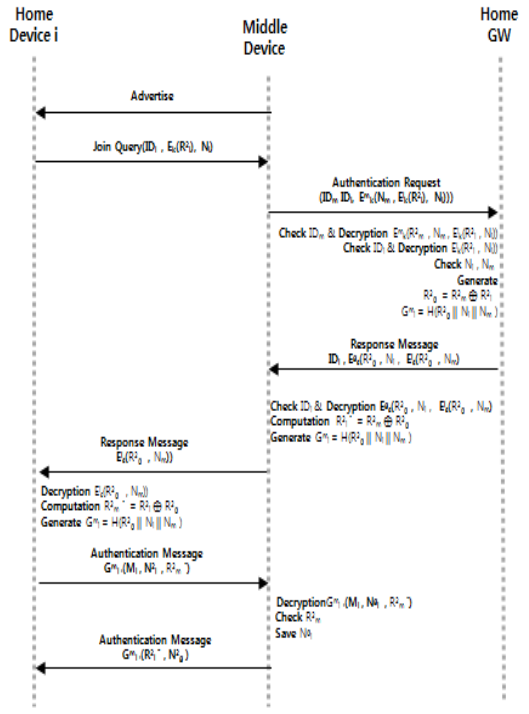

Fig. 3. Middle Device Authentication Protocol

4. 보안성 평가

4.1 보안성 비교 평가

본 절에서는 스마트 홈 환경에서 기기간 신규 디바이스 등록, 인증, 키 관리 등 스마트 홈 환경에서의 보안 취약점에 대해 파악하고 그에 대한 안전성을 평가 하며 기존 스마트 홈 환경에서 보안 기술을 적용한 인증 기술들과 비교 평가 한다.

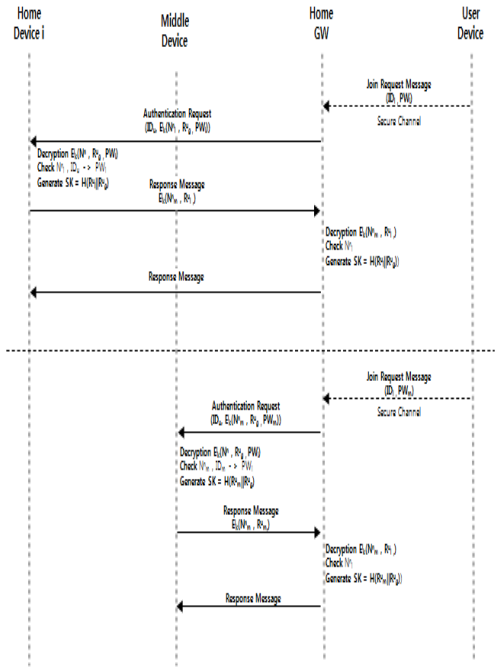

Fig. 4. User Device Access Protocol

Table 2. Security Analysis

	Zhu-Ma [13]	Wu[14]	Li[15]	Proposed
Mutual Authentication	X	X	O	O
Replay Attack	O	X	X	O
data integrity	O	O	X	O
Man in the Middle Attack	X	X	X	O
Sniffing	X	O	O	O
Spoofing	O	O	O	O

4.2 안전성 비교 분석

기존의 스마트 홈 환경에서 보안 프로토콜을 제안한

Zhu-Ma 스킴의 경우 재사용 공격과 데이터 무결성, 스푸핑 공격에 보안성을 갖췄으나, 디바이스간 상호 인증, 중간자 공격 등에 취약점을 가지고 있다. Wu 스킴의 경우 디바이스간 상호 인증, 재사용 공격, 중간자 공격에 취약점을 가지고 있으며, Li 스킴의 경우 재사용 공격, 데이터 무결성, 중간자 공격에 취약점을 가지고 있다.

제안하는 논문에서는 등록 단계에서 새로 추가되는 디바이스와 Service Provider 간 Serial Number를 이용하여 인증 과정을 진행하며, Home GW와 Service Provider 간에는 공개키 기반의 인증이 진행되었다고 가정하였다. 따라서, 추가된 디바이스는 Service Provider를 중계 역할로 활용하여 난수 R과 N을 통해 Home GW와 상호 인증이 가능하다.

또한, 비 인가된 유저가 각 노드 간 전송되어 지는 메시지를 탈취 및 재사용하는 재사용 공격의 경우, 인증 과정에서는 지속적으로 난수를 생성하기 때문에 기존의 메시지로 인증이 불가능 하며, 데이터 통신 과정의 메시지를 탈취하더라도 기존 세션 키가 아닌 새롭게 생성한 세션키 $R_i \oplus PW^g \| R_g$ 를 사용하기 때문에 이전 메시지의 재사용으로 인한 공격에 대하여 안전하다.

데이터 무결성의 경우 비 인가된 유저가 각 노드 간 전송되어 지는 메시지를 탈취한 후 원하는 형태 및 목적을 가지고 메시지를 위·변조하는 메시지를 전송하는 방식의 공격이지만, 메시지를 탈취한 당시의 세션키는 이미 갱신된 새로운 세션 키 $R_i \oplus PW^g \| R_g$를 사용하기 때문에 메시지의 위·변조로 인한 공격에 안전성을 가진다.

전송되는 데이터를 엿보는 스니핑의 경우 인증 절차에서 대칭 키 기반의 암호화가 진행되며, 각 노드 간 전송되어 지는 메시지의 경우 수시로 갱신되는 노드 간 비밀 키를 이용하여 암호화를 적용한 후 전송되기 때문에 공격자는 암호문만을 볼 수 있어 스니핑 공격에 대하여 안전하며, 스푸핑은 이미 디바이스들 간의 상호 인증 절차가 되어 있어, 스푸핑 공격을 하더라도 초기 디바이스 비밀 값을 추측할 수 없어 스푸핑 공격에 대하여 안전성을 가진다.

5. 결론

본 논문에서는 스마트 홈 환경과 환경에서 발생할 수 있는 보안 위협 사례들에 대해 살펴보고 다양한 보안 위협에 대응 가능하며, Middle Device를 이용하여 에너지 효율성을 고려한 인증 프로토콜을 제안 하였다. 현재, 통신 기술의 발전과 스마트 디바이스의 발달로 스마트 홈 서비스 시장이 증가하고 다양한 디바이스를 포함하는 스마트 홈서비스가 상용화 되고 있지만, 이에 대한 보안 적용 사항은 미비한 실정이며, 실제 다양한 리서치 기관을 통해 취약 사례 및 피해 사례가 나타나고 있음을 확인할 수 있었다. 따라서, 본 논문을 활용하여 기존 스마트 홈 환경에서 발생하는 다양한 보안 위협에 대응 가능하며, 그린 IoT 시대에 맞춰 에너지 효율성을 고려한 시스템을 적용할 수 있을 것으로 기대 된다.

References

[1] YOON, Seokung; PARK, Haeryong; YOO, Hyeong Seon. Security issues on smarthome in IoT environment. In: Computer science and its applications. Springer, Berlin, Heidelberg, pp. 691-696, 2015.
DOI: https://doi.org/10.1007/978-3-662-45402-2_97

[2] ROBLES, Rosslin John, et al. A review on security in smart home development. International Journal of Advanced Science and Technology, 2010.

[3] KOMNINOS, Nikos; PHILIPPOU, Eleni; PITSILLIDES, Andreas. Survey in smart grid and smart home security: Issues, challenges and countermeasures. IEEE Communications Surveys & Tutorials, 16.4: 1933-1954, 2014.
DOI: https://doi.org/10.1109/comst.2014.2320093

[4] FERNANDES, Earlence; JUNG, Jaeyeon; PRAKASH, Atul. Security analysis of emerging smart home applications. In: 2016 IEEE Symposium on Security and Privacy (SP). IEEE, pp. 636-654, 2016.
DOI: https://doi.org/10.1109/sp.2016.44

[5] SIVARAMAN, Vijay, et al. Network-level security and privacy control for smart-home IoT devices. In: Wireless and Mobile Computing, Networking and Communications (WiMob), 2015 IEEE 11th International Conference on. IEEE, pp. 163-167, 2015.
DOI: https://doi.org/10.1109/wimob.2015.7347956

[6] YE, Xiaojing; HUANG, Junwei. A framework for cloud-based smart home. In: Computer science and network technology (ICCSNT), 2011 international conference on. IEEE, pp. 894-897. 2011.
DOI: https://doi.org/10.1109/iccsnt.2011.6182105

[7] MOWAD, Mohamed Abd El-Latif; FATHY, Ahmed; HAFEZ, Ahmed. Smart home automated control system using android application and microcontroller. International Journal of Scientific & Engineering Research, 5.5: 935-939, 2014.

[8] SCHNEPS-SCHNEPPE, Manfred, et al. Wired Smart Home: energy metering, security, and emergency issues. In: Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2012 4th

International Congress on. IEEE, pp. 405-410, 2012.
DOI: https://doi.org/10.1109/icumt.2012.6459700

[9] MANTAS, Georgios; LYMBERO POULOS, Dimitrios; KOMNINOS, Nikos. Security in smart home environment. In: Wireless Technologies for Ambient Assisted Living and Healthcare: Systems and Applications. IGI Global, pp. 170-191, 2011.
DOI: https://doi.org/10.4018/978-1-61520-805-0.ch010

[10] FADELL, Anthony Michael, et al. Handling security services visitor at a smart-home. U.S. Patent Application No 14/587,835, 2015.

[11] JOSE, Arun Cyril; MALEKIAN, Reza. Smart home automation security. SmartCR, 5.4: 269-28, 2015.
DOI: https://doi.org/10.6029/smartcr.2015.04.004

[12] J.Zhu and J.Ma, A new authentication scheme with anonymity for wireless environments, IEEE Transactions on Communications, Vol. 50, No.1, pp.231-235, 2004.
DOI: https://doi.org/10.1109/tce.2004.1277867

[13] Farash, Mohammad Sabzinejad, Turkanović Muhamed, Kumari Saru, and Marko Hölbl. "An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the internet of things environment." Ad Hoc Networks 36 152-176, 2016.
DOI: https://doi.org/10.1016/j.adhoc.2015.05.014

[14] C.-C.Wu, W.-B.Lee, and W.-J.Tsaur,“ A secure authentication scheme with anonymity for wireless communications”, IEEE Communications Letters,Vol. 12, No.10, pp.722-723, 2008.
DOI: https://doi.org/10.1109/lcomm.2008.080283

[15] Qinghua Li and Guohong Cao, “Multicast Authentication in the Smart Grid With One-Time Signature”, IEEE Transactions on Smart Grid, 2(4), 2011.
DOI: https://doi.org/10.1109/tsg.2011.2138172

민 소 연(So-Yeon Min) **[종신회원]**

- 1994년 2월 : 숭실대학교 전자공학과 (공학사)
- 1996년 2월 : 숭실대학교 일반대학원 전자공학과 (공학석사)
- 2003년 2월 : 숭실대학교 일반대학원 전자공학과 (공학박사)
- 2005년 3월 ~ 현재 : 서일대학교 정보통신과 부교수

<관심분야>
통신 및 신호처리, 임베디드 시스템

이 재 승(Jae-Seung Lee) **[정회원]**

- 2013년 2월 : 평생교육진흥원 컴퓨터학과(공학사)
- 2015년 2월 : 숭실대학교 컴퓨터학과(공학석사)
- 2015년 3월 ~ 현재 : 숭실대학교 컴퓨터학과 박사수료

<관심분야>
시큐어코딩, Sensor Network, IoT Security