디지털산업정보학회 논문지 제15권 제2호-2019년 6월
http://dx.doi.org/10.17662/ksdim.2019.15.2.043

무선 네트워크 환경에서 기기 관리 및 사용자 인증을 위한 안전한 통신 프레임워크 설계

박 중 오*

A Design of Secure Communication Framework for Device Management and User Authentication in Wireless Network Environment

Park JungOh

〈Abstract〉

The recent technological developments of smart devices, multiple services are provided to enhance the users' quality of life including smart city, smart energy, smart car, smart healthcare, smart home, and so on. Academia and industries try to provide the users with convenient services upon seamless technological research and developments. Also, whenever and wherever a variety of services can be used without any limitation on the place and time upon connecting with different types of devices. However, security weaknesses due to integrations of multiple technological elements have been detected resulting in the leakage of user information, account hacking, and privacy leakage, threats to people's lives by device operation have been raised. In this paper, safer communication framework is suggested by device control and user authentication in the mobile network environment. After implementations of registration and authentication processes by users and devices, safe communication protocol is designed based on this. Also, renewal process is designed according to the safe control of the device. In the performance evaluation, safety was analyzed on the attack of protocol change weakness occurred in the existing system, service halt, data leakage, illegal operation control of message, and so on, which confirmed the enhanced speed approximately by 8% and 23% in the communication and verification parts, respectively, compared to the existing system.

Key Words : Device Management, User Authentication, Wireless Network

Ⅰ. 서론

최근 무선 네트워크 환경의 급격한 발전으로 인하여 다양한 스마트 디바이스 생산되고 있으며, 이를 활용하여 사용자로부터 높은 편의성을 제공하고 있다. 대표적으로 스마트 홈, 스마트 시티, 스마트 에너지, 차량융합 환경 등을 제공하고 있다[1, 5].

* 성결대학교 파이데이아학부 조교수

그러나 다양한 스마트 디바이스를 노리는 공격은 급격히 발생하고 있으며, 사용자에 따른 DDoS, 사용자 계정탈취, 사생활 유출에 따른 보안위협이 발생하고 있다. 이로 인해 금전적인 피해와 더불어 기기조작을 통한 생명을 위협하는 보안위협이 발생할 수 있다[2-3].

그러므로 본 논문에서는 무선네트워크 환경에서 안전한 기기 관리 및 사용자 인증을 위한 통신 프레임워크를 설계한다. 그리고 무선 네트워크 환경에서 발생하는 취약점 및 공격기법에 대한 안전성을 분석하고, 기존 시스템 환경과의 효율성 비교분석을 수행한다.

본 논문의 구성은 다음과 같다. 2장에서는 무선 네트워크 디바이스 활용 사례와 보안요구사항에 대한 관련연구를 다룬다. 3장에서는 디바이스 등록 및 사용자 인증, 안전한 메시지 통신 프로토콜 설계, 디바이스 갱신 및 관리에 대한 제안부분을 설계한다. 4장에서는 제안한 통신 프레임워크에 대한 안전성 분석 및 효율성 평가를 수행한다. 마지막으로 5장에서는 향후 연구계획에 대한 결론을 제시한다.

Ⅱ. 관련연구

2.1 무선 네트워크 기반 디바이스 활용 사례

최근 무선 네트워크 환경의 발전과 더불어 IoT 디바이스의 빠른 확산으로 인하여 사용자로부터 편의성을 제공하는 서비스가 급격히 발전하고 있다. 기존 인터넷 기반 장비를 활용하여 인터넷을 극한적으로 사용했던 거와 달리 사람의 제어 및 조작으로 언제 어디에서나 장소 및 시간에 제한적이지 않게 사용하고 있다[4]. 무선 네트워크 기반 스마트 디바이스의 특징은 아래와 같이 설명한다.

스마트 디바이스 지능화 : 단순 데이터 측정이 아닌 원격조절을 통한 제어가 가능하며, 실시간 수집된 데이터에 따른 통계기능을 제공한다. 그리고 사용자의 최소한의 개입을 통하여 지능적인 통신을 수행한다[4-5].

외부 공격에 따른 취약점 : 단순 게이트웨이 및 Access Point의 취약점에 따른 보안위협이 아닌 스마트 디바이스에 대한 데이터 탈취로 수많은 공격기법이 존재한다[2, 5].

스마트 디바이스의 실시간 동작 시스템 : 디바이스 고유의 Real-time Operating System을 탑재한 실행체계로 펌웨어 업그레이드 및 커넥티드 디바이스에 대한 관리가 요구된다[2, 8].

2.2 무선 네트워크 환경의 보안 요구사항

본 절에서는 무선 네트워크 상 게이트웨이, 디바이스, 네트워크 보호 요구사항에 대해 설명한다. 우선 게이트웨이 공통 보안 요구사항은 아래와 같다.

웜, 바이러스와 같은 외부 해킹공격을 탐지하며 방어할 수 있는 기능을 제공해야 하며, 인터페이스를 제공하는데 있어 인증된 사용자만이 제어할 수 있는 접근제어 권한이 설정되어야 한다. 그리고 또한 디바이스의 플랫폼 무결성 검증 및 인가된 소프트웨어만 실행되어야 한다[2, 6].

게이트웨이에서 데이터 송수신에 따른 메시지를 안전하게 전송되어야하며, 데이터 위협에 대한 무결성 검증이 보장되어야 한다[2-3].

두 번째 사물인터넷 게이트웨이 서비스 제공자에 따른 보안 요구사항은 다음과 같이 설명한다.

이종 네트워크 프로토콜 간 데이터를 변환과정의 수행과정은 안전해야하며, 데이터 무결성이 보증되어야 한다. 또한 보안 정책이 일관적으로 적용되어 이기종 기기 간 데이터를 전송할 때 일관성이 유지되어야 한다[2-4].

사용자가 게이트웨이를 통한 기기를 제어할 때 접

근제어 정책관리 기능을 수행하여, 안전성 있는 서비스를 제공되어야 한다[3, 7-8].

네트워크 및 기기에 대한 관리기능을 수행하여 기기 관리에 따른 오작동, 조작, 트래픽 폭증과 같은 이상징후를 탐지할 수 있어야 한다. 마지막으로 게이트웨이는 자신의 영역의 기기에 대한 데이터를 사용자로부터 비밀키 설정, 식별값 관리, 접근제어에 따른 대행 기능을 제공해야 한다[7].

Ⅲ. 무선 네트워크 환경에서 안전한 기기 관리 및 사용자 인증을 위한 통신프레임워크 설계

본 장에서는 무선 네트워크 환경에서 안전한 기기 관리 및 사용자 인증을 위한 통신 프레임워크를 설계한다. 디바이스, 게이트웨이, 서비스 제공자, 인증센터, 사용자에 대해서 구성되어 있다. 기기 등록 및 인증 절차를 수행 후 안전한 통신프로토콜을 설계하였으며, 기기 관리에 대한 갱신 값 관리 프로토콜을 제안하였다. 아래 절에 대한 프로토콜에 대한 약어는 <표 1>과 같다.

<표 1> Abbreviation

Sign	Description
$Device_{IV}$	Identification value of the device
$Device_{\Pi NCODE}$	Pincode on device
$Device_{SN}$	Serial number of device
$Device_{nonce}$	Random number of devices
$User_{IV}$	User's identification
$User_{CV}$	Validation value of the user
$Gateway_{IV}$	Gateway's identification
AS_{CFV}	Identification value of the Center for Certification Center
SP_{CV}	Validation value from service provider
$Device_{Data}$	Data collected by the device
AS_{Nonce}	Random number of certification centers

3.1 기기 등록 및 사용자 인증 절차

사용자는 기기 등록 및 사용자 인증을 수행하기 위해서 게이트웨이를 통해 서비스 제공자로부터 신원확인 및 검증값을 전송한다. 이후 인증센터로부터 생성된 값을 기반으로 기기를 등록하고, 사용자 인증에 대한 완료 메시지를 수신 후 절차를 마친다. 아래의 <그림 1>은 기기 등록 및 사용자 인증 절차에 대한 제안한 프로세스이다.

1. 사용자는 기기등록을 수행히기 위해서 게이트웨이로부터 등록 요청 메시지를 전송한다.

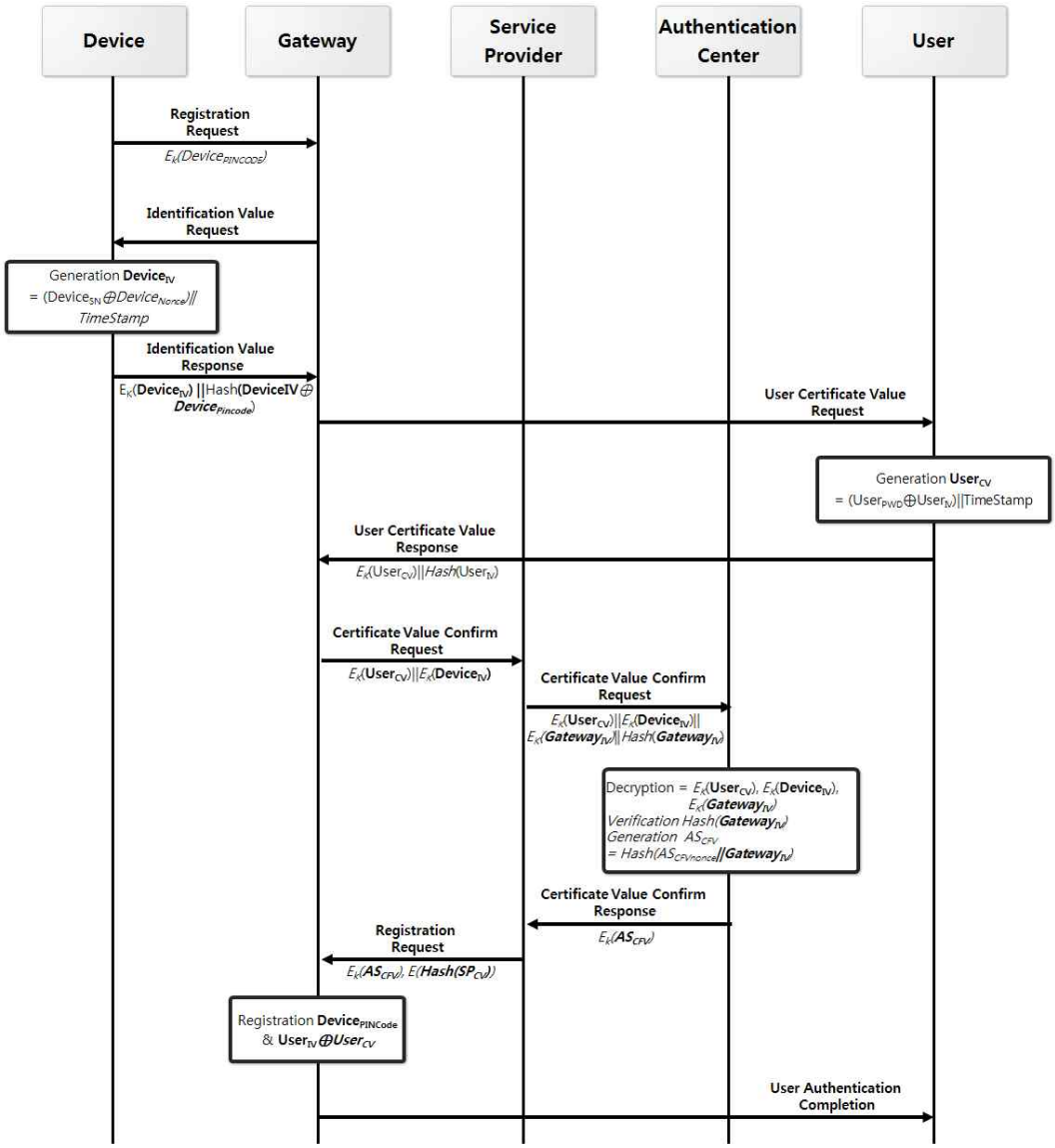
$$E_k(Device_{\Pi ncode})$$

2. 게이트웨이는 기기로부터 인증값을 요청하고 이후 기기에서 인증값을 생성 후 게이트웨이로부터 전송한다.

$$Device = \\ Device \oplus Device_{Nonce} \| Timestamp \\ E_k(Device_{IV}) \| \\ Hash(Device_{IV} \oplus Device_{\Pi ncode})$$

3. 식별값을 수신받은 게이트웨이는 사용자로부터 인증값을 요청한다.

4. 사용자는 인증값 요청에 대한 메시지를 수신 후 인증값을 생성하여 게이트웨이로부터 인증값 응답 메시지를 전송한다.



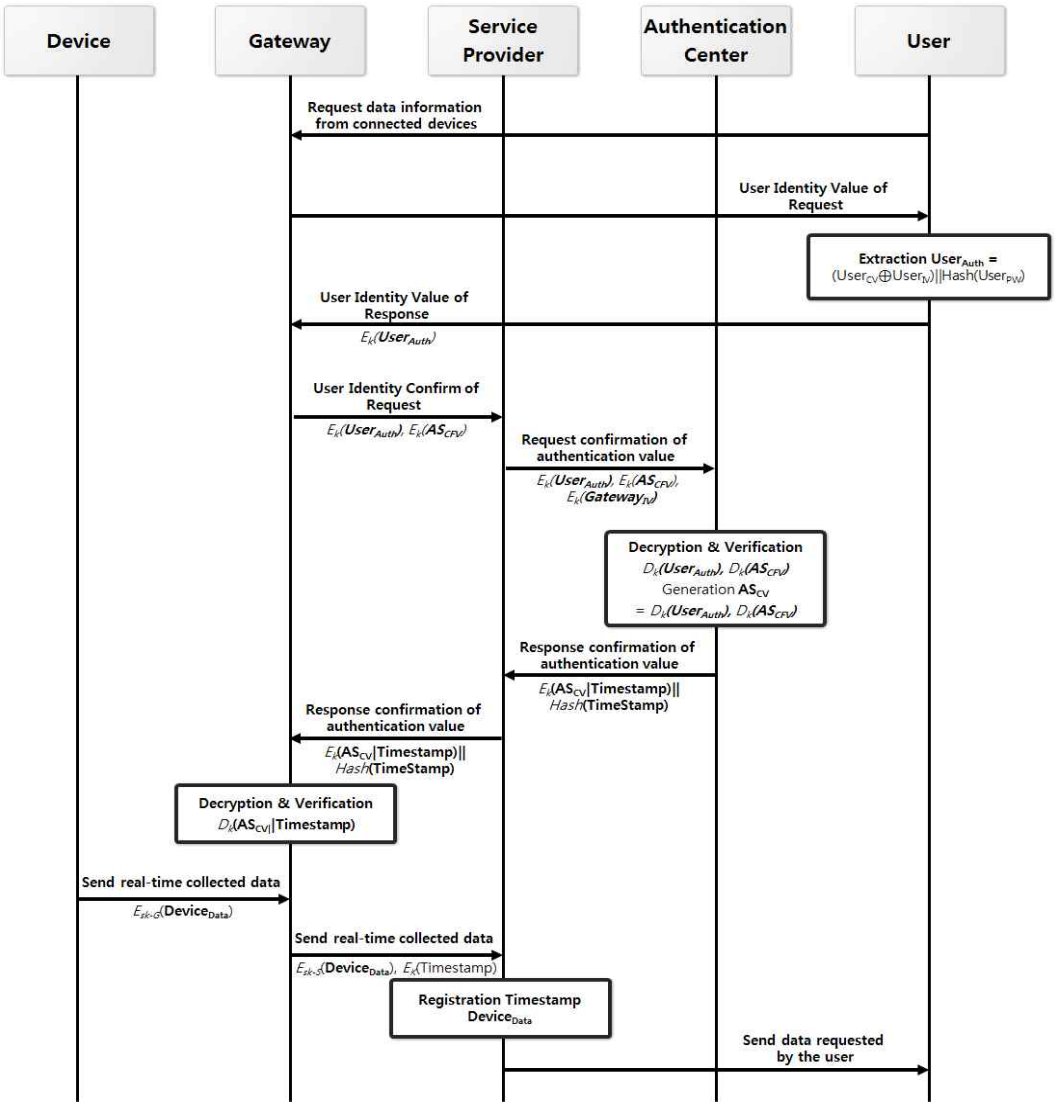
<그림 1> 기기 등록 및 사용자 인증 절차

$$User_{CV} = (User_{PWD} \oplus User_{IV}) \| Timestamp$$
$$E_k(User_{CV}) \| Hash(User_{IV})$$

5. 게이트웨이는 서비스 제공자로부터 신원값 검증 요청 메시지를 전송한다.

$$E_k(User_{CV}) \| E_k(Device_{IV})$$

6. 서비스 제공자는 자신의 식별값을 해쉬함수를 수행 후 수신된 값과 연접하여 검증값 요청 메시지를 인증센터로부터 전송한다.

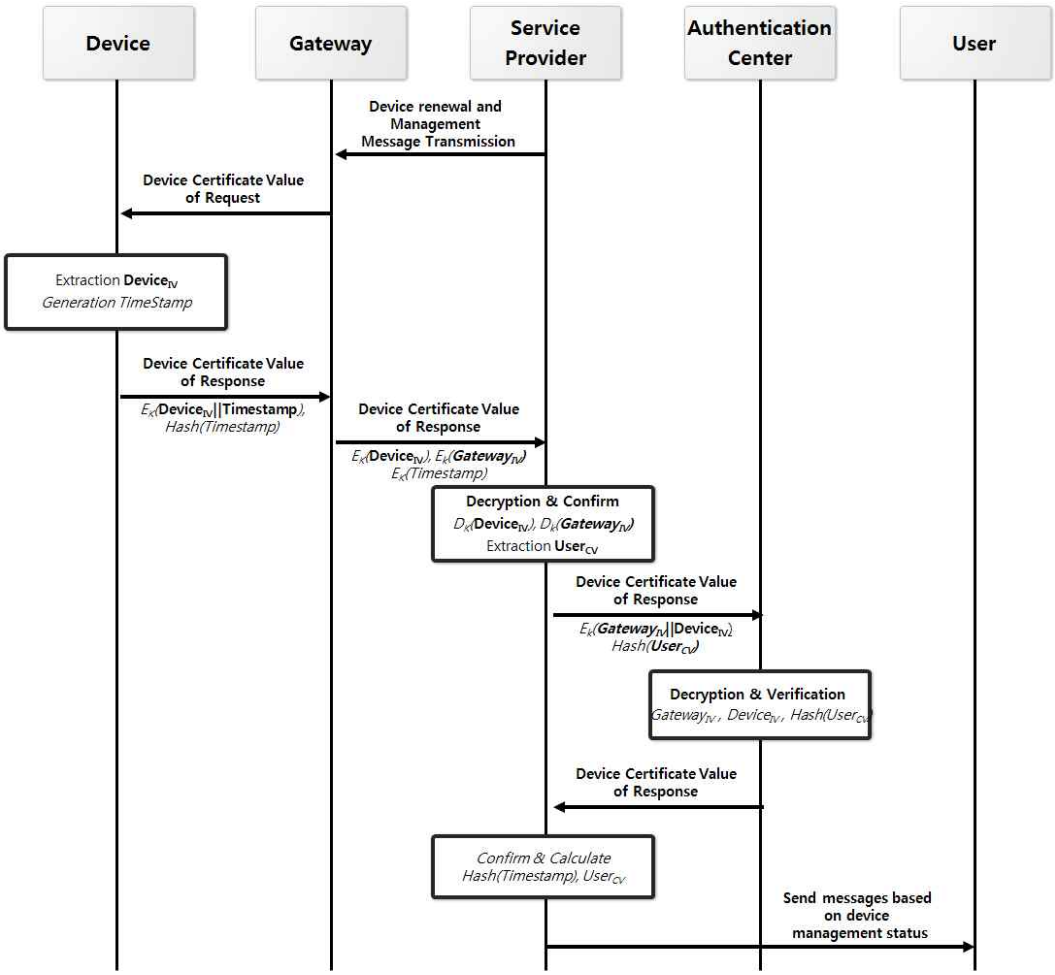


<그림 2> 안전한 메시지 통신 프로토콜 설계

$E_k(User_{CV})\|E_k(Device_{IV})\|$
$E_k(Gateway_{IV})\|Hash(Gateway_{IV})$ 을 전송한다.

7. 인증센터에서는 수신된 값에 대해서 복호화를 수행 후 해쉬함수를 통해 게이트웨이로부터 받은 식별값을 검증 한다. 이후 확인값을 생성 후 검증응답에 해당하는 메시지를 전송하여 올바른 메시지에 대한 확인값

AS_{CFV}
$= Hash(AS_{CFVNonce}\|Gateway_{IV})$
$E_k(AS_{CFV})$



<그림 3> 디바이스 갱신 및 관리 절차

8. 서비스 제공자는 게이트웨이로부터 등록 요청 메시지를 전송한다.

$$E_k(AS_{CFV}), E(Hash(SP_{CV}))$$

9. 게이트웨이에서는 디바이스에 대한 값 및 사용자로부터 인증된 값에 대해서 등록을 수행한다. 마지막으로 사용자로부터 인증이 완료된 메시지를 송신한다.

$$Registration\ Device_{nonce}$$
$$User_{IV} \oplus User_{CV}$$

3.2 안전한 메시지 통신 프로토콜 설계

사용자는 게이트웨이로부터 수집된 데이터를 안전하게 수신받기 위한 메시지 프로토콜을 제안한다. 앞 절에서 생성된 인증값을 기반으로 메시지를 전송하며, 데이터의 무결성 검증을 수행한다. 제안한 프로토콜은 아래 <그림 3>과 같다.

1. 사용자는 게이트웨이로부터 디바이스로부터 수집된 데이터를 요청한다.

2. 게이트웨이에서는 사용자로부터 신원확인 요청 메시지를 전송한다. 이후 사용자는 사용자 인증값을 추출하여 게이트웨이로부터 전송한다.

$$User_{Auth} = (User_{CV} \oplus User_{IV}) \| Hash(User_{PWD})$$
$$E_k(User_{Auth})$$

3. 게이트웨이는 서비스 제공자로부터 신원 확인 요청 메시지를 전송한다.

$$E_k(User_{Auth}), E_k(AS_{CFV})$$

4. 서비스 제공자는 인증센터로부터 인증값 확인 요청메시지를 전송한다. 이후 메시지를 받은 인증센터는 수신된 값에 대한 메시지에 대한 검증을 수행한다.

$$AS_{CV} = User_{Auth} \oplus AS_{CFV} \| AS_{nonce}$$

5. 사용자 인증센터에서는 서비스 제공자에게 인증값 검증에 대한 메시지를 전송한다.

$$E_k(AS_{CV} \| Timestamp) \| Hash(Timestamp)$$

6. 게이트웨이는 수신된 메시지에 대해 복호화 및 검증을 수행 후 게이트웨이로부터 수집된 데이터를 서비스 제공자로 세션키를 활용하여 전송한다.

$$E_{Sk-S}(Device_{Data}), E_k(Timestamp)$$

7. 서비스 제공자는 수신된 메시지를 복호화 후 서비스 제공망을 활용하여 수신된 메시지를 전송한다.

3.3 기기 인증값에 대한 갱신 및 관리 절차

1. 서비스 제공자는 게이트웨이로부터 등록된 디바이스에 대한 갱신 및 관리를 수행하기 위한 메시지를 전송한다.

2. 게이트웨이는 디바이스에 대해서 검증값 요청메시지를 전송한다. 이후 디바이스는 식별값을 추출 후 타임스탬프를 생성하여 게이트웨이로부터 응답메시지를 전송한다.

$$E_k(Device_{IV} \| Timestamp)$$
$$Hash(Timestamp)$$

3. 게이트웨이는 서비스 제공자로부터 검증값 확인 요청 메시지를 전송한다.

$$E_k(Device_{IV}), E_k(Gateway_{IV}),$$
$$E_k(Timestamp)$$

4. 서비스 제공자는 수신된 메시지를 복호화 후 사용자의 등록한 검증값을 추출한다. 이후 인증센터로부터 디바이스 인증값 요청메시지를 전송한다.

$$E_k(Gateway_{IV} \| Device_{IV})$$
$$Hash(User_{CV})$$

5. 수신받은 메시지를 복호화 및 검증 후 서비스 제공자로부터 응답요청메시지를 전송한다.

6. 서비스 제공자는 검증 및 계산 후 타임스탬프를 해쉬함수 수행하여 사용자로부터 등록된 기기에 대한 관리메시지를 전송한다.

Ⅳ. 성능평가

4.1 안전성 평가

본 절에서는 무선 네트워크 환경의 발생하는 프로토콜 변환 취약점 공격, 서비스 마비, 데이터 유출, 메시지 불법 동작 제어, 인터페이스 취약점, 물리적 탈취와 같은 공격에 대한 안전성 평가를 서술한다.

프로토콜 변환 취약점 공격 : 무선 네트워크 환경의 디바이스는 성능 제약으로 인한 고기능성 프로토콜의 전환하는 가정의 보안위협이 발생한다. 이를 해결하기 위해서 제안한 통신 프로토콜의 $Gateway_{IV}$와 AS_{CV}검증을 수행함으로써 프로토콜 변환 취약점을 보완할 수 있다.

서비스 마비 : 무선 네트워크 상의 대표적인 공격으로서 취약점을 이용한 jamming 공격을 통해 게이트웨이와 디바이스 사이의 통신을 불가능하게 하는 공격을 말한다. 이를 방지하기 위해서 서비스 제공자와 인증센터로부터 $User_{CV}$, $User_{Auth}$, ,$Device_{IV}$에 대한 검증을 수시로 갱신 및 관리를 수행함으로써 출처 불명의 디바이스에 대한 통신을 수행하지 못하도록 한다.

메시지 불법 동작 제어 : 통신상의 메시지를 가로채어 데이터를 변조하는 공격이 빈번히 발생하는데 이에 대한 공격을 해결하기 위해서 사용자 인증 및 기기 등록과정의 설계된 AS_{CFV}, SP_{CV}의 메시지 검증을 수행함으로써 데이터를 탈취하더라도 메시지에 대한 변조를 막을 수 있다.

인터페이스 취약점 : 사용자가 무선 네트워크 환경의 게이트웨이를 접근을 위한 인터페이스의 취약점을 활용하여 관리자 권한 탈취 등과 같이 피해가 발생할 수 있다. 이를 방지하기 위해 사용자 인증과정의 $User_{IV}$, $User_{CV}$, SP_{CV}에 대한 검증을 수행하며, 디바이스 갱신 및 관리 절차에서 $Gateway_{IV}$와 인증센터의 생성한 $Time\,stamp$를 검증을 수햄함으로써 인터페이스 취약점을 보완하였다.

디바이스 물리적 탈취 : 디바이스 접근을 통해 악의적인 사용자가 디바이스를 조작하여 게이트웨이 펌웨어 또는 물리적인 메모리 탈취를 통해 데이터를 획득할 수 있는 상황이 발생한다. 본 논문에서는 디바이스의 검증에 대한 인증값 $Device_{IIncode}$,$Device_{IV}$ m $Device_{Time\,stamp}$를 검증 후 이를 기반으로 통신함으로써 악의적인 사용자에 대한 탈취 후 데이터 조작이 실패한다.

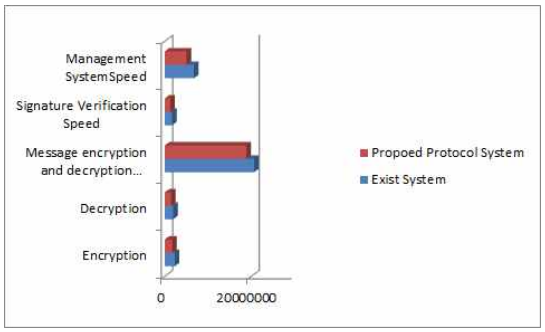
4.2 보안성 분석 및 효율성 평가

본 논문의 제안한 통신 프레임워크 상 프로토콜의 효율성을 분석하기 위해서 윈도우(Windows 10 Home Standard 64 bit) Intel(R) Core i7-4970(3.6GHz), 8.00 GB 환경에서 Java 기반의 암·복호화 성능을 비교분석 하였다. 기존 시스템의 활용한 암호화 프로토콜의 대한 성능분석과 제안한 통신프로토콜의 성능을 비교분석한 내용은 <표 2>와 같다.

<표 2> 기존 시스템과 제안한 프로토콜의 프로토콜 비교분석

	Exist System	Propoed Protocol System
Encryption	2321351	1744561
Decryption	1949935	1465431
Message encryption and decryption speed during communication	20647915	18892026
Signature Verification Speed	1699228	1277019
Management System Speed	6746680	5070322

(Number Point : nanosecond)



<그림 4> 기존 시스템과 제안한 프로토콜과의 비교분석

암호화, 복호화, 메시지 통신 프로토콜 과정, 서명 검증, 관리 시스템 절차에 따른 비교분석을 수행하였으며, 수치는 nanosecond로 표현하였다. 기존의 시스템 대비 암호화 및 복호화에서는 약 24%, 전체 통신 프로토콜 대비 약 8%, 검증 분석 및 관리 프로토콜 대비 약 23%의 높은 효율성을 확인 할 수 있었다.

Ⅴ. 결론

본 논문에서는 무선 네트워크 환경에서 안전한 기기 관리 및 사용자 인증을 통한 통신 프레임워크를 설계하였다. 디바이스 등록 및 사용자 인증 절차를 수행 후 이를 기반으로 안전한 통신 프로토콜을 제안하였다. 이후 디바이스 관리를 안전하게 수행하기 위한 갱신 및 관리 절차를 설계하여 사용자로부터 안전한 메시지를 전송을 수행하도록 하였다.

제안한 통신 프레임워크에 따른 성능 분석을 수행하기 위해서 무선 네트워크 환경뿐 만아니라 사물 인터넷 환경에서 발생하는 프로토콜 변환 취약점 공격, 서비스 마비, 데이터 유출, 메시지 불법 동작 제어, 인터페이스 취약점, 물리적 탈취와 같은 공격기법 및 취약점에 안전성 분석을 수행하였다. 그리고 기존 시스템과 제안한 통신 프로토콜과의 효율성 분석을 수행하여 기존 시스템 대비 암호화 성능 분석 약 24%, 통신 프로토콜 대비 약 8%, 검증 분석 및 관리 절차에 대한 23%의 높은 효율성을 확인 할 수 있었다.

마지막으로 제안한 통신 프레임워크를 다양한 환경에 접목하기 위한 꾸준한 연구가 필요하고, 신규 및 변종 공격에 대비하여 보다 안전하게 효율성 높은 서비스를 사용자로부터 제공하기 위한 보안정책이 요구된다.

참고문헌

[1] Security Requirements for the Smart Phone Security Management Product, TTA.Ko-12.0265, TTA, 2014.

[2] Security Requirements for IoT Gateway, TTAK.KO-12.0297, 2016.

[3] Keun-Ho Lee, “A Security Threats in Wireless Charger Systems in M2M”, Journal of the Korea Convergence Society, Vol. 4, No. 1, 2013, pp. 27-31.

[4] 임철수, “IoT 서비스 활용사례 분석 및 산업 활성화 이슈,” 한국차세대컴퓨팅학회, 한국차세대컴퓨팅학회논문지, 제11권, 제6호, 2015, pp. 41-50.

[5] 유재학,”사물 웹(WoT) 융합 기술 및 표준화 동향”, 정보통신산업진흥원, 주간기술동향, 2014.

[6] 류호석·곽진, 스마트홈에서의 보안 위협 및 보안 요구사항 분석, 한국인터넷정보학회 추계학술대회 논문집, 2014.

[7] D. Gessner, A. Olivereau, A. Salinas Segura, A. Serbanati, ‘Trustworthy Infrastructure Services for a Secure and Privacy-respecting Internet of Things,’ IEEE Conference on Trust, Security and Privacy, 2012.

[8] Internet of Things Architecture, www.iot-a.eu/public

■ 저자소개 ■

박 중 오
(Park, Jung Oh)

2011년 8월 숭실대학교 컴퓨터공학 박사
2016년 3월~현재
성결대학교 파이데이아학부
조교수

관심분야 : Network security, 암호학, PKI
E-mail : jopark02@sungkyul.ac.kr

논문접수일 : 2019년 5월 30일
수 정 일 : 2019년 6월 5일
게재확정일 : 2019년 6월 10일