Journal of Convergence for Information Technology
Vol. 10. No. 11, pp. 55-63, 2020
e-ISSN 2586-4440
DOI : https://doi.org/10.22156/CS4SMB.2020.10.11.055

사물인터넷 기반 디바이스 관리를 위한 안전한 통신 프로토콜 설계

박중오[1], 최도현[2*], 홍찬기[3]
[1]성결대학교 파이데이아학부 조교수, [2]숭실대학교 컴퓨터학과 학생, [3]가톨릭관동대학교 의료IT학과 교수

A Design of Secure Communication for Device Management Based on IoT

Jung-Oh Park[1], Do-Hyeon Choi[2*], Chan-Ki Hong[3]
[1]Assistant Professor, Division of Paideia, Sungkyul University,
[2]Student, Department of Computer Science, Soongsil University
[3]Professor, Department of Medical IT, Catholic Kwandong University

요 약 사물인터넷 기술은 신규 기술이 아닌 기존 산업 환경에 있는 기술을 응용하여 융합하는 분야다. 사물인터넷기술은 스마트 홈, 헬스케어, 건설, 자동차 등 타 산업과 융화된 다양한 응용서비스가 출시되고 있으며, 사물인터넷 기반기술을 이용하는 사용자로부터 업무 효율성 및 사용자 편의성도 확보할 수 있다. 그러나 사물인터넷 기반기술 환경에서 발생하는 보안위협은 기존 무선 네트워크 환경에서 발행하는 취약점을 계승하고 있으며, ICT융합환경과 접목되어 신규 및 변종 공격이 발생하여 이에 따른 피해가 발생하고 있다. 그러므로 사물인터넷 기술 기반의 환경에서는 사용자와 디바이스, 디바이스 와 디바이스 통신 환경에서 안전하게 메시지를 전송할 수 있는 연구가 필요하다. 본 논문에서는 사물인터넷 기반기술 환경에서 디바이스 관리를 위한 안전한 통신 프로토콜을 설계하도록 한다. 제안한 통신 프로토콜에 대해 사물인터넷 기술기반 환경에서 발생하는 공격기법에 대한 안전성 분석을 수행하였다. 그리고 기존 PKI-기반 인증서 발급시스템과 제안한 통신 프로토콜의 성능평가를 통해 통신절차에서 약 23%의 높은 효율성을 확인하였다. 또한 인증서 발급량에 따른 인증서 관리기법 대비 기존 발급시스템 대비 약 65%의 감소된 수치를 확인하였다.

주제어 : ICT융합, 인증서 관리, 자가인증, 통신 프로토콜, 해시트리

Abstract The IoT technology is a field that applies and converges the technologies in the existing industrial environment, instead of new technologies. The IoT technology is releasing various application services converged with other industries such as smart home, healthcare, construction, and automobile, and it is also possible to secure the work efficiency and convenience of users of IoT-based technologies. However, the security threats occurring in the IoT-based technology environment are succeeding to the vulnerability of the existing wireless network environment. And the occurrence of new and variant attacks in the combination with the ICT convergence environment, is causing damages. Thus, in the IoT technology-based environment, it would be necessary to have researches on the safe transmission of messages in the communication environment between user and device, and device and device. This thesis aims to design a safe communication protocol in the IoT-based technology environment. Regarding the suggested communication protocol, this thesis performed the safety analysis on the attack techniques occurring in the IoT technology-based environment. And through the performance evaluation of the existing PKI-based certificate issuance system and the suggested communication protocol, this thesis verified the high efficiency(about 23%) of communication procedure. Also, this thesis verified the reduced figure(about 65%) of the issued quantity of certificate compared to the existing issuance system and the certificate management technique.

Key Words : ICT Convergence, Managing Certificates, Self-Certification, Communication Protocol, Hashtree

*Corresponding Author : Do-Hyeon Choi(cdhgod0@ssu.ac.kr)
Received October 15, 2020
Revised November 6, 2020
Accepted November 20, 2020
Published November 28, 2020

1. 서론

사물인터넷기술이 타 산업과 융화되면서 발전되고, 신규 부가가치 사업들이 창출하고 있다. 보건, 의료, 교통, 제조업 등에서 IoT 기술이 융합되어 첨단관리 시스템이 구축되고, 이를 통해 사용자로부터 효율성 높은 편의성을 제공하고 있다[1]

그러나 IoT 기술이 융합된 환경은 안전한 보안대책이 요구되고 있다. IoT 기술은 기존 무선네트워크 환경에서 발생된 취약점을 계승하고 있으며, 신규 및 변종에 따른 공격기법이 발생하고 있다. 해커는 IoT 융합환경의 취약점을 이용하여 공격을 시도하고 있다. 대표적으로 디바이스를 대상으로 데이터 위·변조를 통한 정보유출, 서비스 거부 공격, 프라이버시 유출 피해가 발생하고 있다[2]. 그러므로 본 논문에서는 사물인터넷 기반 ICT 융합환경에서 디바이스 관리 및 안전한 통신을 수행하기 위해 자가인증 기법을 활용하여 통신 프로토콜을 설계하도록 한다.

본 논문은 5장으로 구성되어 있다. 2장에서는 자가인증 기법 연구, 사물인터넷 기반 ICT융합환경의 취약점 및 보안 요구사항에 따른 관련 연구를 수행한다. 3장에서는 디바이스 등록, 사용자 인증 및 통신 프로토콜을 설계한다. 4장에서는 안전성 분석, 보안성 및 효율성 평가를 수행한다. 5장은 결론으로 향후 경량화성 통신 프로토콜에 대한 연구 방향성을 제시하고 논문을 종결한다.

2. 관련연구

2.1 자가인증 기법

자가인증 기법은 객체의 내부적인 키 관리 시스템을 이용하지 않고 키와 파일이름을 매칭시키는 기술이 제안되어 처음 사용되었다. 대표적인 기술로서는 AIP(Accountable Internet Protocol)로 제3자에 대한 인증 없이 자신을 인증할 수 있는 자가인증기반 기술이 제안되었으며, 자가인증식별자, 객체 자신이름으로 적용되는 메커니즘 연구가 진행되고 있다[3].

콘텐츠 중심 네트워크환경에서 콘텐츠에 생성자, 이름, 생성자에 따른 공개키를 기반의 객체 식별을 위한 메커니즘 활용이 필요하고, 두 가지 제약조건이 요구된다[2,3].

첫 번째 자가인증을 수행하기 위해 DoS에 대한 대응방안이 마련되어야 하며, 적절하게 바인딩 되기 위해 키와 이름에 대한 연관성 검증이 필요하다. 두 번째는 자가인증을 통해 객체그룹에 대한 확장성이 보장되기 위해서는 객체에 따른 식별값 검증이 요구되고 있다[4-5].

대표적인 자가인증 기법인 AIP에 대한 특징은 객체의 주소를 활용하여 제3자의 도움 없이 상호간의 인증을 수행할 수 있는 프로토콜을 제공한다. 변조된 객체 및 사용자가 참여시 프로토콜 과정에서 네트워크 추적 기능을 제공함으로써 보안사고에 따른 책임을 전가할 수 있다[6].

2.2 사물인터넷 기반 ICT융합환경의 취약점 및 보안 요구사항

IoT기술과 타 산업환경과의 융합을 통해 다양한 응용서비스 생성되고 있으며, 사용자는 이에 따른 서비스를 제공받아 높은 편의성을 보장받고 있다. 하지만 해커의 공격으로 인해 서비스 침해가 발생 시 경제적 피해를 넘어 인명피해가 발생할 것이라 예측하고 있다. 그리고 사용자의 프라이버시 침해로 인한 정보유출이 사고가 생겨나고 있다[7,12]. 그러므로 IoT기반 융합서비스 활성화시 기하급수적으로 발생하는 디바이스 관리에 따른 보안체계 구축 및 대응방안 연구가 요구되고 있다[8].

IoT융합환경은 이기종 장비와의 연결, 기존의 무선네트워크 기술과 지능화된 플랫폼기반으로 서비스를 수행하고 있어, 서비스 수행환경에 따른 보안위협에 대한 요구사항이 설계되어야 한다[9]. 우선 IoT 디바이스 설계시 메시지 전송에 따른 정보보호와 프라이버시의 보장성이 확보되어야 한다[10,11]. 또한 IoT 디바이스에 따른 서비스를 접목하기 위해 보안 프로토콜을 준수하여 상호간에 안전한 통신이 수행되어야 한다[12]. 그리고 디바이스 하드웨어와 펌웨어에 따른 지속 모니터링과 업데이트가 수행하여 발생하는 데이터에 따른 무결성이 확보되어야 한다[13,14]. 마지막으로 침해사고 발생에 따른 분석 및 사고추적성이 확보되어야 한다[15]. 3장 제안부에서는 IoT융합환경의 취약점 및 보안 요구사항으로 기반으로 디바이스 관리를 위한 통신 프로토콜을 설계하도록 한다.

3. 디바이스 관리를 위한 통신 프로토콜 설계

본 장에서는 사물인터넷 기반 ICT융합환경에서 디바이스 관리를 위한 통신 프로토콜 설계에 대해서 서술한다. 각 절에서는 디바이스 등록 절차, 사용자 인증 및 통신 프로토콜에 대해서 설계한다. 제안한 통신 프로토콜에 대한 약어표는 Table 1과 같다.

Table 1. The abbreviation of a paper

Abbreviation	Description
$Device_{SN}$	Serial number of device
$Device_{CER}$	The authentication value of the
$Deoce_{Code}$	Code of device
$Device_{Sig}$	Signature value of device
H(Device)	Device authentication value hashed function value
$Device_{G-cer}$	Signature value of device group
$Device_{UUID}$	universally unique identifier of Device User
$Server_{M-Cer}$	Signed value of server
$User_{Cert}$	The user's authentication value
$User_{Info}$	User's Information
Ms_{Cert}	The authentication value of the Management Server
MS_{Sig}	Signed value of Management Server

3.1 디바이스 등록 절차

본 절에서는 제안한 인증절차 및 통실 프로토콜의 디바이스 등록 절차를 설계한다. 사용자는 신규 디바이스를 통해 인근 디바이스 그룹과의 가입을 수행한다. 이후 IoT 통신인프라 및 서비스 제공자에게 신규 디바이스 등록 절차를 수행한다. 디바이스 등록 절차는 아래 Fig. 1과 같다.

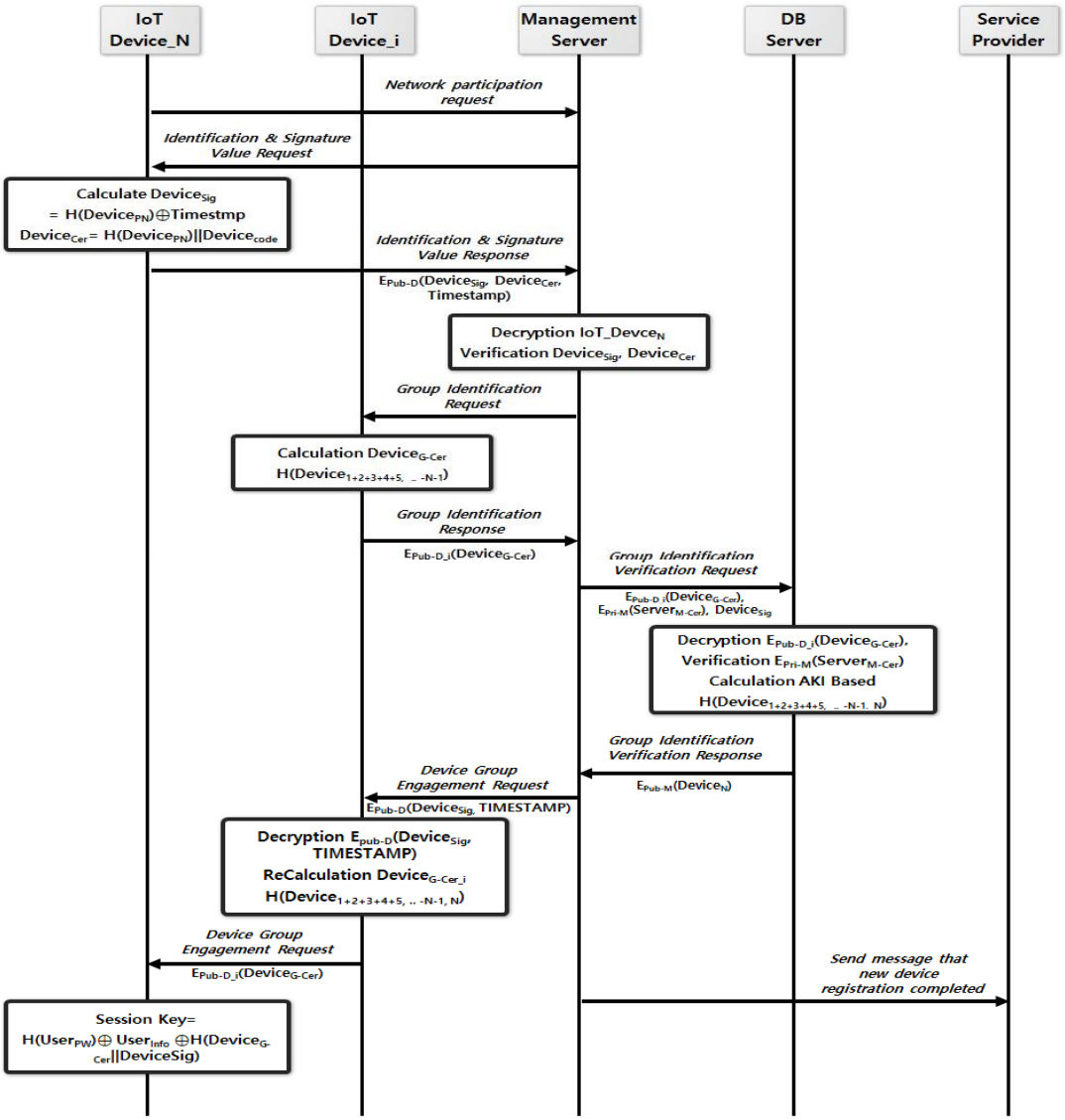

Fig. 1. Device Registration Procedure

1. 사용자는 IoT Device$_N$을 사용하여 IoT Device$_i$ 그룹가입 참여를 위해 네트워크 참여 요청 메시지를 Management Server로 전송한다.

2. Management Server는 그룹참여 요청한 신규 IoT Device$_N$으로부터 검증 및 서명값 요청 메시지를 전송한다.

3. 메시지를 수신 받은 신규 IoT DeviceN은 서명값 및 검증값을 생성 후 Management Server로 서명값 요청메시지를 회신한다.

$$Device_{Sig} = H(Device_{PN}) \oplus Time\,stamp$$
$$Device_{Cer} = H(Device_{PN}) \| Device_{code}$$
$$E_{Pub-D}(Device_{Sig}, Device_{Cer}, Time\,stamp)$$

4. Management Server는 수신된 메시지를 복호화 후 Device$_{sig}$, Device$_{Cer}$를 검증한다. 이후 그룹 IoT Device$_i$로부터 그룹 신원검증 요청 메시지를 전송한다.

5. IoT Devicei는 수신된 메시지를 확인 후 신원 검증 메시지 Device$_{G\text{-}cer}$를 생성한다.

$$H(Device_{1+2+3+4+5,..N-1)}$$

6. 이후 IoT Device_i는 Mamagement Server로 DB Server의 공개키를 활용하여 생성한 Device$_{G\text{-}cer}$를 전송한다.

$$E_{Pub-DB}(Device_{G-Cer})$$

7. Management Server는 자신의 개인키를 활용하여 ServerM$_{\text{-}Cer}$를 생성 후 이전에 검증받은 Device$_{Sig}$와 이전 서명값 Device$_{G\text{-}cer}$를 전송한다.

$$E_{Pub-DB}(Device_{G-Cer})$$
$$E_{Pri-M}(Server_{M-Cer}), Device_{Sig}$$

8. DB Server는 수신한 메시지를 복호화를 수행 후 Management Server의 Server$_{M\text{-}Cer}$메세지를 검증한다.

9. 이후 DB Server는 자가인증 기법을 활용하여 그룹서명값 Device$_{G\text{-}cer}$ 검증계산을 수행한다. 그리고 Management 서버로 검증수행 메시지 Device$_N$을 전송한다.

$$H(Device_{1+2+3+4+5,..N-1,N})$$

10. Management Server는 IoT *Device$_i$*로부터 암호화를 통한 신규 디바이스 참여 요청 메시지를 전송한다.

$$E_{Pub-D}(Device_{sig}, Time\,Stamp)$$

11. IoT *Device$_i$*는 수신된 메시지를 복호화 후 그룹 참여를 위해 재계산 및 Device$_{G\text{-}Cer_i}$를 생성한다.

$$Device_{G-cer-i} =$$
$$H(Device_{1+2+3+4+5,...N-1,N})$$

12. IoT Device$_i$는 재계산 및 검증을 완료 후 IoT DeviceN으로 그룹 참여 완료 메시지를 전송한다.

$$E_{Pub-D-i}(Device_{G-Cer})$$

13. Management Server는 Server Provider로 신규 디바이스 참여 확인 후 신규 디바이스 등록 완료 메시지를 전송한다.

14. 디바이스는 수신된 데이터를 확인 후 사용자의 데이터를 전송할 수 있는 세션키를 생성한다.

$$Session = H(User_{pw}) \oplus User_{info}$$
$$\oplus H(Device_{G-Cer}) \| Device_{Sig}$$

3.2 사용자 인증 및 메시지 전송 프로토콜 설계

본 절에서는 3.1절 디바이스 등록 절차에서 생성된 값을 기반으로 사용자 인증 및 메시지 전송 프로토콜을 설계한다. 우선 사용자는 등록된 디바이스를 통해 현재 데이터를 요청하고, IoT 통신 인프라를 통해 인증을 수행 후 안전하게 메시지를 전송한다. 사용자 인증 및 메시지 전송 프로토콜 과정은 아래 Fig. 2.와 같다.

1. 사용자는 등록된 IoT *Device$_i$*로 현재 상황의 수집된 데이터 요청 메시지를 전송한다.

$$E_{Pub-MS}(User_{info} \| Device_{UUID})$$
$$E_{Pri-U}(User_{Cert}), E_{Pub-D-i}(User_{Cert})$$

2. IoT Devicei는 수신된 메시지를 확인 후 Management Server로 검증 요청메시지를 전송한다.

$$E_{Pub-MS}(User_{info} \| Device_{UUID})$$
$$E_{Pri-U}(User_{Cert})$$

3. 검증 요청메시지를 수신 후 Management Server는 디바이스로부터 검증 요청 메시지를 전송한다.

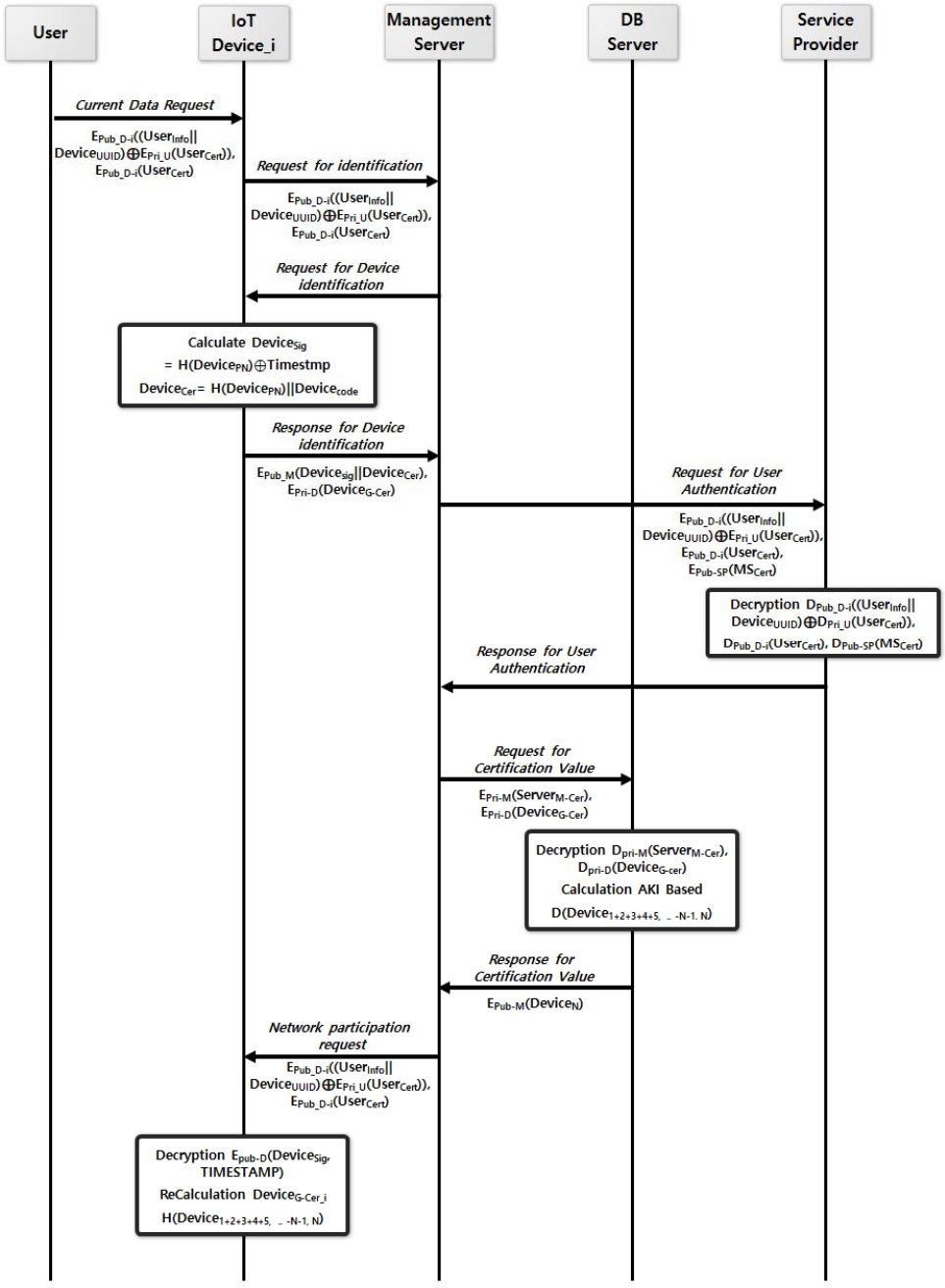

Fig. 2. User Authentication & Message Send Protocol

4. IoT Device$_i$는 사용자로부터 받은 인증값을 복호화 및 검증을 수행한다. 이후 $Device_{Sig}$를 생성한다. 그리고 디바이스의 단속 인증값을 생성 후 Management Server로 디바이스 신원 확인 응답메시지를 전송한다.

$$Device_{Sig} = H(Device_{PN}) \oplus Time\ Stamp$$

$$Device_{Cer} = H(Device_{PN}) \| Device_{Code}$$

$$E_{Pub-M}(Device_{Sig} \| Device_{Cer}),$$
$$E_{Pri}(Device_{G-Cer})$$

5. Management Server는 사용자 인증을 위해 Service Provider로 인증 요청 메시지를 전송한다.

$E_{Pub-SP}((User_{Info} \| Device_{UUID}) \oplus E_{Pri-Sp}(User_{cert})), E_{Pub-sp}(MS_{Cert})$

6. Server Provider는 수신한 메시지를 복호화 수행 후 인증과정을 수행 후 Management Server로부터 사용자 인증 응답 메시지를 전송한다.

7. Management Server는 수신한 메시지 인증서 검증을 수행하기 위해 DB Server로 인증서를 전송한다. DB Server는 메시지 복호화를 수행 후 검증을 수행한다. 이때 검증을 수행하기 위해서 3.1절에서 $Device_N$ 검증하는 자가인증 기법을 활용한다.

$H(Device_1 \| Device_2) = H(Device_{1+2})$
$H(Device_3 \| Device_4) = H(Device_{3+4})$
...
$H(Device_{N-1} \| Device_N) = H(Device_{N-1+N})$
$H(H(Device_{1+2}) \| H(Device_{3+4}))$
...
$H(H(Device_{N-3+N-2}) \| H(Device_{N-1+N}))$
$H(Device_{1+2+3+4+5,\ldots N-1,N})$

8. DB Server는 인증서 검증을 수행 후 Management Server로 계산한 인증서를 전송한다.

$E_{Pub-M}(H(Device_N))$

9. Management Server는 IoT $Device_i$로부터 신원 검증 완료 메시지를 전송한다.

$E_{Pri-D}(MS_{Sig}, TIMESTAMP)$

10. IoT *Devicei*는 수신한 메시지를 복호화 후 검증을 수행한다. 이후 사용자로부터 세션키를 활용하여 데이터를 전송하여 메시지 통신 절차를 마친다.

$E_{Pri-D}(MS_{Sig}, TIMESTAMP)$
$H(Device_{1+2+3+4+5,\ldots N-1,N})$

4. 성능평가

4.1 안전성 분석

본 논문에서 제안한 통신 프로토콜에 대해 IoT기반 융합환경에서 발생하는 공격기법에 대해서 안전성을 분석한다. 비 인가된 접근제어, 데이터 변조, 중간자 공격, 물리적 디바이스 탈취 등에 따른 대응방안을 분석하였다[11-13].

비인가 된 사용자 및 디바이스의 접근 : IoT 환경에서 대표적인 보인 이슈 중의 하나인 비인가 사용자 및 디바이스 접근을 차단하기 위해 본 논문에서는 디바이스 등록절차에 따른 $Device_{Sig}$값을 식별하고 이를 기반으로 생성된 $H(Device_{1+2+3+4+5,..N-1,N})$을 재계산을 수행하여 디바이스 및 사용자 검증을 수행하여 비인가 접근을 막을 수 있다.

데이터 변조에 대한 위협 : 공격자가 특정 디바이스에서 발생한 데이터를 탈취 후 변조하여 인증서 및 사용자 프라이버시 침해할 수 있다. 이러한 공격에 대응하기 위해 DB Server, IoT $Device_i$그룹에서 자가인증 기법을 수행하여 데이터, 메시지, 인증서 등 무결성 검증을 통해 대처할 수 있다.

중간자 공격(Man in the middle attack, MITM) : ICT 융합환경에서 기존의 무선네트워크 환경에서 발생하는 중간자 공격에 대한 취약점을 계승하고 있다. 제안한 통신프로토콜의 검증값(MS_{sig}, $User_{Cert}$, $Device_{G\text{-}Cer\text{-}i}$)을 통해 인증을 수행함으로써 중간자 공격이 실패한다.

디바이스 도난 및 분실 위협 : 디바이스 도난 및 물리적 탈취에 따른 위협을 막기 위해 본 논문에서는 사용자의 정보($User_{Info}$, $User_{Cert}$)와 디바이스 식별값($Device_{UUID}$)을 확인한다. 이후 디바이스 신원 확인 메시지($Device_{Cer}$) 및 사용자 인증을 Management Server에서 인증을 수행함으로써 탈취된 디바이스를 통해 메시지 유출을 막을 수 있다.

4.2 보안성 및 효율성 평가

본 절에서는 기존의 PKI 인증서 기반의 통신프로토콜과 제안한 통신프로토콜에 따른 효율성 평가를 수행하였다. 통신 수행과정에 따른 암호화 및 복호화 수행과정, 인증서 관리사항, 주요 공격에 대한 위협, 특징에 따른 보안성을 분석하였으며 결과는 아래 Table 2과 같다.

Table 2. Evaluation of Security of Proposed Communication Protocols with Existing PKI-based Communication Protocol

Sortation	Conventional PKI-based communication protocol	Proposed Communications Protocol
Encryption and Decryption Process	4E+4D+2C	4E+4D+2H
Certificate management	Issuing CA Subject Certificate	Self-certification-based certificate management
Typical Vulnerabilities and Major Attacks	Access to unauthorized users and devices Threats to Data Modulation Man in the middle attack	-
Certification Process Features	Certificate issued by authorized authority	Certification Management System Between Mutual Groups

제안한 시스템에서는 암호화 및 복호화 수행 시 인증서 발급이 아닌 자가인증 기반의 해시트리기법을 활용하여, 인증서 관리를 수행하였다 기존의 PKI-기반 통신 프로토콜의 인증서 발급 및 암복호화 수행과정은 4번의 암□복호화와 2번의 인증서 발급을 수행한다. 제안한 프로토콜을 인증서 발급과정을 대체하여 자가인증기반의 2번의 해시값 검증을 수행한다. 인증서 관리 측면에서는 신뢰된 제3자의 인증서 기반으로 객체의 검증을 수행한다. 제안한 프로토콜에서는 AKI기반 자가인증기법을 수행하여 취약점 대응 및 상호인증과정을 통해 객체를 서로 검증하였다.

관련연구 2절에서 언급된 정보보호와 프라이버시의 보장, 데이터 무결성 확보, 펌웨어 모니터링 및 업그레이드, 침해사고 발생에 따른 사고추적성 확보에 대해 보안성을 서술하였다. 우선 정보보호와 프라이버시의 보장성을 확보하기 위해 디바이스 인증서, 그룹인증서를 통한 메시지 검증절차를 강화하여 인가된 사용자로부터 메시지 전송되도록 설계되었다. 메시지 통신절차에 따른 검증값 확인절차를 통해 디바이스의 생성된 데이터와 물리적인 무결성을 확보하였다. 메시지 통신절차에 따른 검증값 확인절차를 통해 지속적인 모니터링 절차를 강화하였다. 그리고 침해 발생에 따른 주체 확인 검증 절차를 수행하기 위해 사용자 정보, 디바이스 소유에 따른 검증을 수행한다.

성능분석을 수행하기 위해서 Ubuntu 64bit 운영체제기반에서 Apache Tomcat 7.0.93을 활용하여 서버를 구축하였다. JAVA 기반 Eclipse 개발 킷을 통해 java.security library를 사용하여 위에서 언급된 PKI 기반 인증서 발급을 통한 통신 프로토콜과 제안한 프로토콜에 성능평가를 수행하였다. 비교분석 항목은 메시지 통신과정, 서명 및 검증 과정, 인증서 관리(인증서 추출 및 계산)이며 결과는 아래 Fig. 3과 같다.

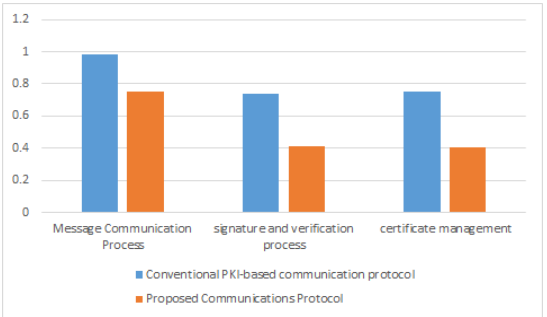

Fig. 3. Analyze the efficiency of existing systems and proposed protocols(Left : Conventional PKI-based communication protocol, Right :Proposed Communications Protocol)

제안한 통신 프로토콜은 공인된 인증서 발급 주체 없이 상호간 해시트리 기반의 자가인증을 수행하여 기존 시스템의 메시지 통신과정 대비 약 23%의 높은 효율성을 확인할 수 있었다. 그리고 서명 및 검증 과정, 인증서 관리 절차에서는 약 44%의 높은 효율성을 확인할 수 있었다.

그리고 기존 인증서 발급시스템(PKI, WPA2)와 제안한 시스템의 인증서 발급 시스템과의 성능 평가를 수행하기 위해 위의 언급된 개발환경에서 Openssl, EASY RSA, WPA2 AES, SHA-256을 활용하여 비교분석을 수행하였다.

PKI, WPA2의 인증서 발급 대비 약 74%, 65% 대비 높은 효율성을 확인할 수 있었다. 제안한 인증서 관리 시스템에서는 기존 인증서 관리 시스템의 제3자 기관 인증수행 과정이 없이 해시값(SHA-256)기반의 해쉬트리기반 인증서를 생성하여 상호간에 검증을 수행하며, 새로운 디바이스 추가를 위해 그룹 해쉬인증서를 검증한다.

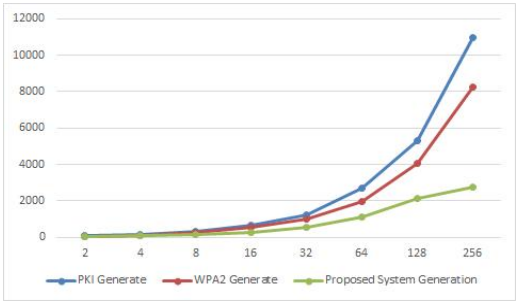

Fig. 4. Analysis of the amount of existing PKI-based certificates and the proposed amount of protocol certificates issued

5. 결론

본 논문에서는 사물인터넷 기반 ICT융합환경에서 디바이스 관리를 위한 통신 프로토콜을 연구하였다. IoT Device$_i$ 참여그룹을 통한 자가인증 기반 인증서 발급 및 검증 절차를 수행하였으며, 이를 기반으로 사용자가 IoT Device를 활용한 통신 프로토콜을 설계하였다.

제안한 시스템은 사물인터넷 기반 ICT융합환경에서 발생하는 대표적인 공격기법 중간자 공격기법과 데이터 변조의 위협, 비인가 된 사용자 및 디바이스의 접근, 디바이스 도난 및 분실 위협과 같은 취약점을 분석하였다. 그리고 기존 인증서관리시스템과 보안성 및 효율성 평가를 수행하여, 메시지 전송 프로토콜 대비 약 23%의 향상성을 확인할 수 있었으며, 기존 시스템 인증서 발급량 대비 관리 측면에서 약 65%의 효율성 증가를 확인할 수 있었다.

향후 본 논문에서 제안한 통신 프로토콜을 활용하여 다양한 융합환경에서 적응할 것으로 기대하고 있다. 하지만 통신 프로토콜 연구뿐만 아니라 안전하게 사용할 수 있는 보안정책 방안도 필요하다. 그리고 IoT 소형기기에서도 사용할 수 있는 경량화성 통신 프로토콜에 관한 연구가 요구되고 있다.

REFERENCES

[1] B. W. Jin, J. O. Park & M. S. Jun. (2017). A Study on Authentication Management and Communication Method using AKI Based Verification System in Smart Home Environment. *The Journal of The Institute of Internet, Broadcasting and Communication, 16(6),* 25-31, DOI : 10.7236/JIIBC.2016.16.6.25

[2] T. H Kim, J. H Hong & H. Y. Jung. (2015). Trend in Trustworthy Communication for the Next-Generation. *Electronics and Telecommunications Trends, 30(4),* 129-139.

[3] T. H. J. Kim et al. (2013). Accountable key infrastructure (AKI) a proposal for a public-key validation infrastructure. *In Proceedings of the 22nd international conference on World Wide Web* (pp. 679-690).

[4] Y. T. Kim. (2015.). Secure Messenger System using Attribute Based Encryption. *Journal of Security Engineering, 12(5),* 469-486,

[5] S. E. Ponta, H. Plate & A. Sabetta. (2018, September). Beyond metadata: Code-centric and usage-based analysis of known vulnerabilities in open-source software. *In 2018 IEEE International Conference on Software Maintenance and Evolution (ICSME)* (pp. 449-460). IEEE.

[6] Y. Yang, L. Wu, G. Yin, L. Li & H. Zhao. (2017). A survey on security and privacy issues in Internet-of-Things. *IEEE Internet of Things Journal, 4(5),* 1250-1258.
DOI : 10.1109/JIOT.2017.2694844

[7] K. H. Lee, (2013). A Security Threats in Wireless Charger Systems in M2M. *Journal of the Korea Convergence Society, 4(1),* 27-31.
DOI : 10.15207/JKCS.2013.4.1.027

[8] Malcolm Shore. (2017). *IoT Common Security Principle v1.0*, KISA.

[9] J. I. Lee. (2015). Convergent Case Study of Research and Education: Internet of Things Based Wireless Device Forming Research. *Journal of the Korea Convergence Society, 6(4),* 1-7,

[10] CoAP(Constrained Application Protocol), IETF(*Internet Engineering Task Force*, http://www.ietf.org)

[11] L. A. Tawalbeh, F. Muheidat, M. Tawalbeh & M. Quwaider. (2020). IoT Privacy and security: Challenges and solutions. *Applied Sciences, 10(12),* 4102.

[12] B. K. Rios & J. Butts. (2017). When IoT Attacks: understanding the safety risks associated with connected devices. *Proceedings of Black Hat USA.* https://www.blackhat.com/docs/us-17/wednesday/us-17-Rios-When-IoT-Attacks-Understanding-The-Safety-Risks-Associated-With-Connected-Devices.pdf

[13] D. Y. Kang & J. H. Hwang. (2019). A Study on Priority of Certification Criteria for IoT Security Certification Service. *The Journal of the Korea*

Contents Association, 19(7), 13-21.

[14] Y. An. (2016). A Strong Biometric-based Remote User Authentication Scheme for Telecare Medicine Information Systems with Session Key Agreement. *International Journal of Internet, Broadcasting and Communication, 8(3),* 41-49, DOI : 10.7236/IJIBC.2016.8.3.41

[15] Common Criteria Recognition Arrangement. (2017). Common Criteria for Information Technology Security Evaluation. *Part 1 : Introduction and general model*, CCMB-2017-04-001.

박 중 오(Park, Jung Oh) [정회원]

· 2000년 7월 : 성결대학교 컴퓨터공학과 졸업
· 2003년 3월 : 명지대학교 전자계산교육 석사
· 2011년 8월 : 숭실대학교 컴퓨터공학 박사

· 2016년 3월 ~ 현재 : 성결대학교 조교수
· 관심분야 : PKI, Network security, 암호학
· E-mail : pjo21@naver.com

최 도 현(Choi, Do Hyeon) [정회원]

· 2008년 2월 : 동서울대학교 컴퓨터소프트웨어학과 졸업
· 2010년 8월 : 숭실대학교 컴퓨터학과(공학석사)
· 2016년 3월 : 숭실대학교 컴퓨터학과(공학박사)

· 관심분야 : Mobile, Network Security, PKI, Virtualization
· E-Mail : cdhgod0@ssu.ac.kr

홍 찬 기(Chan-Ki Hong) [정회원]

· 1986년 : 중앙대학교 전자계산학과(이학사)
· 1988년 : 중앙대학교 대학원 전자계산학과 (공학석사)
· 1992년 : 중앙대학교 대학원 전자계산학과(공학박사)

· 1992년 3월~현재 : 가톨리관동대학교 의료IT학과 정교수
· 관심분야 : 정보보안, PKI, 블록체인
· E-Mail : chankih@cku.ac.kr