디지털산업정보학회 논문지 제14권 제3호-2018년 9월
http://dx.doi.org/10.17662/ksdim.2018.14.3.011

스마트 디바이스 기반의 보안성 강화를 위한 접근제어 기법 설계

박 중 오*

A Design of Access Control Method for Security Enhance based Smart Device

Park Jungoh

〈Abstract〉

Smart devices refer to various devices and control equipment such as health care devices, imaging devices, motor devices and wearable devices that use wireless network communication (e.g., Wi-fi, Bluetooth, LTE). Commercial services using such devices are found in a wide range of fields, including home networks, health care and medical services, entertainment and toys. Studies on smart devices have also been actively undertaken by academia and industry alike, as the penetration rate of smartphones grew and the technological progress made with the fourth industrial revolution bring about great convenience for users.

While services offered through smart devices come with convenience, there is also various security threats that can lead to financial loss or even a loss of life in the case of terrorist attacks. As attacks that are committed through smart devices tend to pick up where attacks based on wireless internet left off, more research is needed on related security topics.

As such, this paper seeks to design an access control method for reinforced security for smart devices. After registering and authenticating the smart device from the user's smart phone and service provider, a safe communication protocol is designed. Then to secure the integrity and confidentiality of the communication data, a management process such as for device renewal or cancellation is designed. Safety and security of the existing systems against attacks are also evaluated. In doing so, an improved efficiency by approximately 44% compared to the encryption processing speed of the existing system was verified.

Key Words : Access Control, Smart Device, Security Enhance

Ⅰ. 서론

최근 스마트 디바이스를 활용한 다양한 서비스들이 사용자로부터 제공되고 있으며, 스마트폰과 연결을 통해서 스마트 홈, 웨어러블 기기, 자동차 산업등과 같은 응용서비스들이 급속히 확산되고 있다. 사물인터넷을 넘어서 만물 인터넷의 개념으로 스마트 디바이스 간 연동 및 연동을 통해 주변에 있는 데이터를 사용자로부터 전달하여 사용자의 생활밀첩형

* 성결대학교 파이데이아 학부 조교수

서비스가 제공되어 효율성 높은 편의성을 제공하고 있다[1,9].

스마트디바이스 및 스마트폰을 활용한 개인·기업에 대한 활용도가 높아지면서, 보안이슈가 끊임없이 발생하고 있다. 무선인터넷 기반의 서비스가 제공되어 지면서 기존의 발생한 보안위협 및 취약점을 포함하고 있으며, 신규 및 다양한 서비스에 대한 증가로 따른 새로운 위협사항이 증가하고 있다[2-3].

그러므로 본 논문에서는 스마트 디바이스 기반의 보안성 강화를 위한 접근 제어 기법을 설계하여 사용자로부터 안전한 서비스를 제공하도록 한다.

본 논문에 대한 구성은 다음과 같다. 2장은 관련 연구 항목으로 스마트 디바이스 정의 및 활용사례에 대한 내용을 서술한다. 3장은 제안부분으로 디바이스 등록 및 인증 절차, 메시지 통신 절차 프로토콜을 설계하며, 3.3 디바이스 해지 및 갱신 프로토콜에 대한 제안부분을 기술한다. 4장은 성능평가 부분으로 안전성 분석 및 보안성을 평가하며, 5장은 본 논문의 결론을 맺는다.

Ⅱ. 관련연구

2.1 스마트 디바이스 정의 및 활용사례

스마트 디바이스란 각종 무선 통신기술을 활용한 다양한 디바이스와 제어기기를 통칭하며, 웨어러블 기기, 스마트폰, 증강현실 서비스와 같은 다양한 형태의 제품들을 모두 포함하고 있다.

스마트 디바이스에서 수집된 데이터를 안전하게 전송함으로써, 사용자로부터 다양한 서비스를 제공하게 되며, 디바이스 서비스를 활용한 사용자로부터 개인적(Personal)이며, 보조 장치를 활용한 확장서비스를 가능하게 한다.

스마트폰 중심의 디바이스는 산업은 활발하게 변화되고 있으며, 스마트 디바이스 및 사물 인터넷의 대한 서비스 중심으로 국가 및 공공기관 및 기업에서도 활발하게 연구에 대한 투자를 진행하고 있어, 산업 특성이 급속도로 변화하고 있다[1,3,4].

2.2 스마트 디바이스를 활용한 사물인터넷 환경의 보안 위협 및 요구사항

본 절에서는 스마트 디바이스를 활용한 사물인터넷 환경의 보안 요구사항을 정의한다. 스마트 디바이스 활용한 대표적인 보안위협은 웹 인터페이스 취약점, 악성코드/Malware 공격위협, 서비스 장애, 물리적 디바이스 탈취, 데이터 유출이 있다[1,5].

프로토콜 변환 취약점 공격 : 사물인터넷 디바이스는 기능에 따른 성능에 인해 데이터 기밀성 및 무결성에 대한 위협, 악의적인 데이터 변조, 보안정책 위반, Injection 공격과 같은 보안 위협이 존재한다[1,6].

서비스 마비 : 스마트폰 디바이스를 활용한 사물인터넷 환경에서 게이트웨이의 디바이스 간 통신 데이터를 전송할 때 재밍공격 및 통신상에 취약점을 통해 서비스를 운영하지 못하는 공격기법이 발생한다[3,7].

악성코드 감염 : 악성코드/Malware 공격으로 인해 디바이스, 게이트웨이가 좀비화 되어 DDos 공격에 악용될 수 있으며. 데이터 유출과 같은 2차적인 피해가 발생할 수 있다. 그리고 또한 주변에 디바이스에 2차적인 악성코드 감염과 같은 피해를 발생할 수 있다[3,8].

웹 인터페이스 취약점 : 무선 인터넷환경에서 발생하는 취약점을 활용하여 관리자 권한 탈취, 접근제어 발생과 같은 피해가 발생한다[2,7].

위와 같은 보안위협을 방지하기 위해서 외부 공격에 대한 방어할 수 있는 접근제어 기법을 제공해야한다. 또한 디바이스에서 수집된 데이터를 안전하게 발생하기 위해서 데이터의 기밀성 및 무결성에 대한 보안성을 제공해야하며, 인가된 소프트웨어만이 통신기능을 수행할 수 있도록 보장해야한다. 연결된 데이터에 대한 인증 강화로 인한 신뢰성이 강화되어야 한다[6-9].

Ⅲ. 스마트 디바이스 기반의 보안성 강화를 위한 접근제어 기법 설계

본 장에서는 스마트 디바이스 기반의 보안성 강화를 위한 접근제어 기법에 대해서 서술한다. 사용자는 스마트폰을 활용하여 스마트 디바이스를 등록 및 인증과정을 수행한다. 이후 등록 및 인증 절차에서 생성한 데이터를 기반으로 메시지를 안전하게 전송한다. 그리고 디바이스 해지 및 갱신프로토콜을 설계하여 디바이스 관리적인 요소를 보완한다. 스마트 디바이스, 게이트웨이, 스마트 폰, 서비스 제공자, Certificate Authority으로 구성되어 있다. 제안한 논문의 설계한 프로토콜의 약어표는 <표 1>과 같다.

<표 1> 약어표

약어	설명
Epub-XX	xx의 공개키로 암호화
DeviceSN	디바이스의 Serial Number
DeviceCode	디바이스 코드값* * 디바이스의 패스워드와 시리얼 넘버를 XoR 연산 수행 한 식별값
DevicePW	디바이스의 패스워드
S-PhoneValue	스마트폰의 식별값
SPCode	서비스 제공자의 식별값
Hash	해쉬함수 수행
SignatureCode	서명값* * 서비스 제공자의 식별값과 스마트폰의 식별값, 타임스템프로 조합하여 연산한(XoR) 값
Timestamp	타임스템프
GatewayCode	게이트웨이 식별값
SignatureGateway	게이트웨이 서명값

3.1 디바이스 등록 및 인증 절차

디바이스 등록 및 인증 절차는 디바이스를 스마트폰을 통해 서비스 제공자로부터 등록 절차를 수행한다. 이후 상호간에 식별값을 요청 및 검증 후 등록과정을 완료한다. 디바이스 등록 및 인증 절차에 대한 설명은 <그림 1>과 같다.

1. 스마트 디바이스는 스마트 폰을 통해 등록 요청 메시지를 전송한다. 이후 서비스 제공자로 수신받은 메시지를 전송한다.

$$E_{Pub-Sp}(Device_{SN}) \quad (1)$$

2. 서비스 제공자는 수신한 메시지를 복호화하고, 이후 스마트폰을 거쳐서 디바이스로부터 인증값 요청 메시지를 전송한다.

3. 사용자는 메시지를 수신 후 디바이스에서 Password를 입력 후 디바이스 코드를 생성한다.

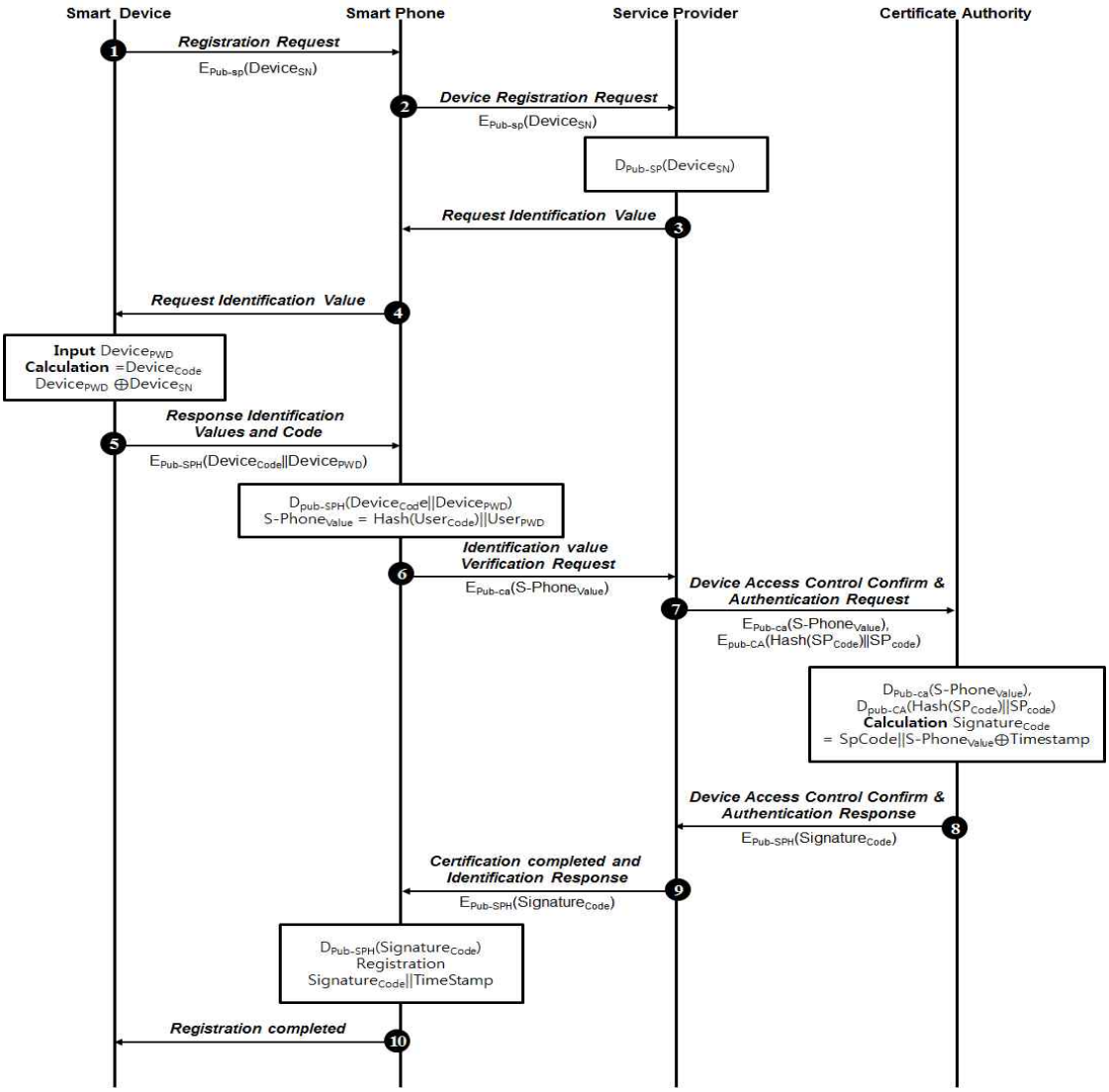
$$Device_{Code} = Device_{Pwd} \oplus Device_{SN} \quad (2)$$

4. 디바이스는 생성한 디바이스 코드와 패스워드를 포함한 메시지를 암호화 하여 스마트 폰으로 전송한다.

$$E_{Pub-SPH}(Device_{Code} || Device_{Pwd}) \quad (4)$$

5. 스마트폰은 수신한 메시지를 복호화 후 S-PhoneValue메시지를 생성 후 서비스 제공자로부터 전송한다.

$$E_{Pub-CA}(S-Phone_{Value}) \quad (5)$$



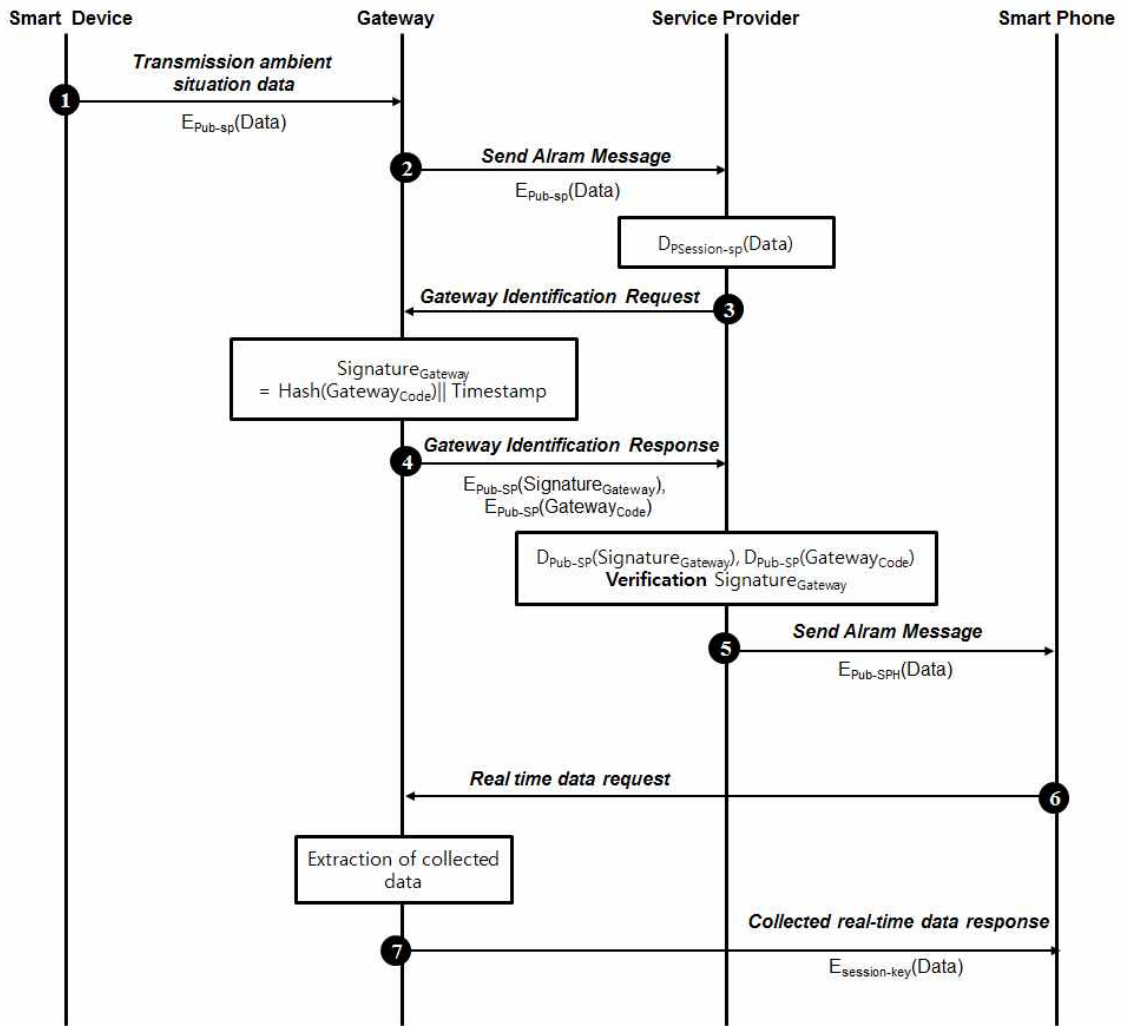
<그림 1> 디바이스 등록 및 인증 절차

6. 서비스 제공자는 Certificate Authority로부터 디바이스 접근제어 확인 및 인증 요청 메시지를 전송한다.

$$E_{Pub-CA}(S-Phone_{Value}), \quad E_{Pub-Ca}(Hash(Sp_{Code}||SP_{Code}) \tag{6}$$

7. Certificate Authority 수신한 메시지를 복호화 후 Signaturecode를 생성 후 서비스 제공자로 디바이스 접근제어 확인 및 인증 응답 메시지를 전송한다.

$$E_{Pub-SPH}(Signature_{Code}) \tag{7}$$



<그림 2> 메시지 통신 절차 프로토콜 설계

8. 서비스 제공자는 스마트 폰으로부터 인증값 확인 및 식별값 응답 메시지를 전송한다.

$$E_{Pub-SPH}(Signauture_{Code}) \quad (8)$$

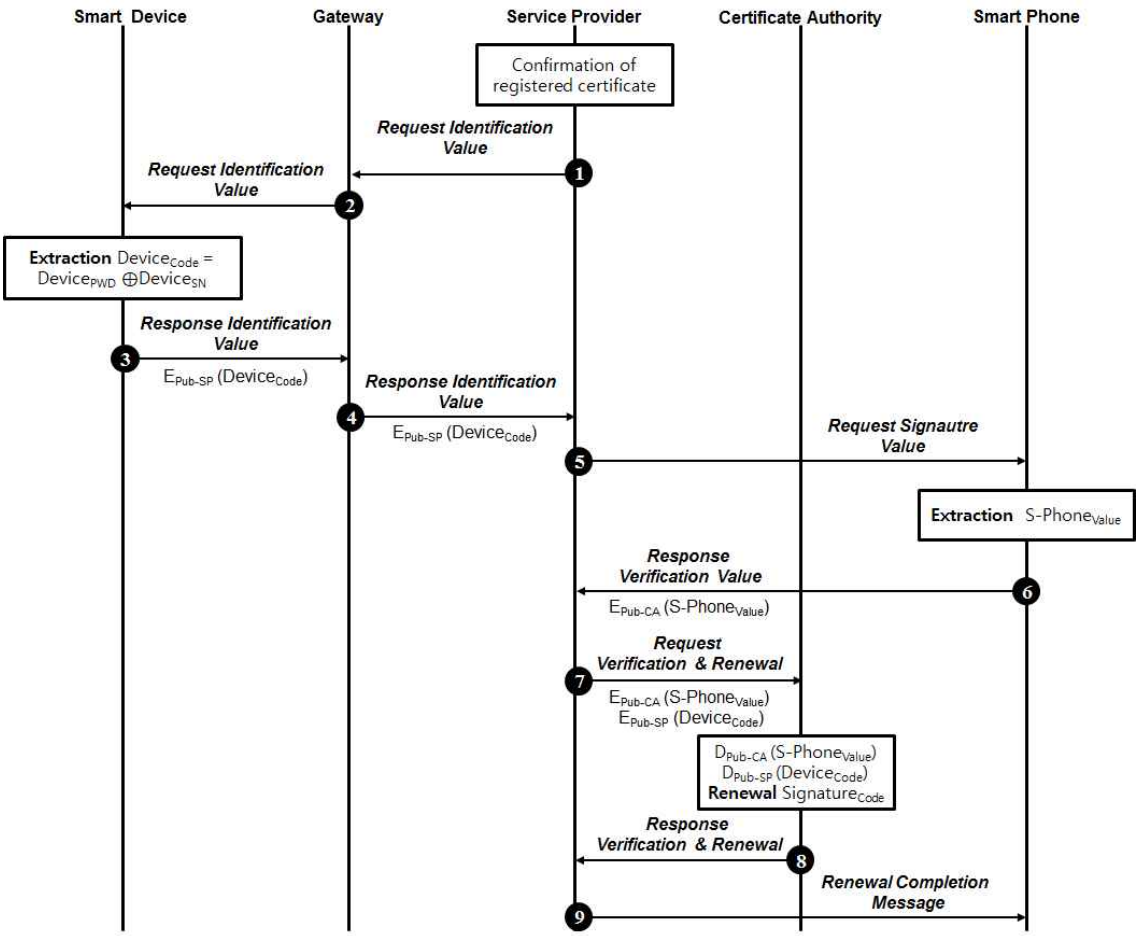
9. 스마트 폰은 수신한 메시지를 복호화 후 식별값을 등록 후 스마트 디바이스로부터 등록 완료 메시지를 전송한다.

3.2 메시지 통신 절차 프로토콜 설계

3.2절 등록 및 인증과정에서 생성한 식별값을 기반으로 메시지 통신 절차 프로토콜을 설계한다. 메시지 통신 과정에 대한 설명은 [그림 2]과 같다.

1. 스마트 디바이스는 게이트웨이로부터 주변 상황 메시지를 전송한다. 이후 게이트웨이는 수신한 메시지를 서비스 제공자로 전송한다.

$$E_{Pub-SP}(Data) \quad (9)$$



<그림 3> 디바이스 해지 및 갱신 프로토콜 절차

2. 서비스 제공자는 수신한 메시지를 복호화 후 게이트웨이로부터 식별값 요청 메시지를 전송한다.

3. 게이트웨이는 서명값을 생성 후 서비스 제공자로부터 식별값 응답 메시지를 전송한다.

$$E_{Pub-SP}(Signature_{Gateway}), \quad E_{Pub-SP}(Gateway_{Code}) \tag{10}$$

4. 서비스 제공자는 메시지를 복호화 후 서명값을 검증 한다. 이후 스마트 폰으로 스마트 디바이스에서 수신한 메시지를 전송한다.

$$E_{Pub-SPH}(DATA) \tag{11}$$

5. 스마트 폰에서 확인한 사용자는 게이트웨이로부터 실시간 데이터를 요청한다.

6. 게이트웨이는 수집한 실시간 데이터를 스마트 폰으로 세션키로 암호화 하여 데이터를 전송한다.

3.3 디바이스 해지 및 갱신 프로토콜

본 절에서는 등록된 디바이스의 해지, 갱신과 같은 관리체계에 관한 프로토콜을 설계한다. 디바이스 해지 및 갱신 프로토콜의 과정에 대한 설명은 [그림 3]와 같다.

1. 서비스 제공자는 등록된 식별값을 확인 후 게이트웨이로부터 식별값 요청 메시지를 전송한다. 이후 게이트웨이는 스마트 디바이스로부터 수신한 메시지를 전송한다.

2. 스마트 디바이스는 디바이스코드를 추출 후 게이트웨이로 전송한다. 이후 게이트웨이는 식별값을 서비스 제공자로부터 식별값 요청 메시지를 전송한다.

$$E_{Pub-SP}(Device_{Code}) \tag{12}$$

3. 서비스 제공자는 스마트폰으로부터 서명값 요청메시지를 전송한다.

4. 스마트폰은 서명값을 추출 후 서비스 제공자에게 식별값 응답 메시지를 전송한다.

$$E_{PUB-CA}(S-Phone_{Value}) \tag{13}$$

5. 서비스 제공자는 Certificate Authority에게 검증 및 갱신 요청 메시지를 전송한다.

$$E_{Pub-Ca}(S-Phone_{Value}), \quad E_{Pub-SP}(Device_{Code}) \tag{14}$$

6. Certificate Authority는 수신한 메시지를 복호화 후 서명값을 갱신한다. 이후 서비스 제공자로부터 검증 및 갱신 응답 메시지를 전송한다.

7. 서비스 제공자는 스마트폰으로부터 갱신완료 메시지를 전송한다.

Ⅳ. 성능평가

4.1 안전성 분석

중간자(Man-in-the-middle) 공격 위협 : 무선 네트워크 환경에서 중간자 공격의 빈도는 꾸준히 발생하고 있다. 인가된 무선 인터넷 중계기를 사용하더라도 해커는 중계기의 취약점을 이용한 공격을 시도하여 데이터를 가로 챌수 있다. 이러한 중간자(Man-in-the-middle) 공격의 위협에 대한 보안성을 강화하기 위해서 Certificate Authority에서 생성한 $Signature_{code}$를 전송하여 데이터를 암호화하여 안전하게 전송하다. 그리고 디바이스 해지 및 갱신 절차에서 그리고 DeviceCode, Signaturecode를 주기적으로 확인함으로써, 중간자 공격(Man-In-the middle Attack)은 실패하게 된다.

통신간 데이터의 기밀성 위협 : 수집된 정보를 사용자의 스마트폰으로 전송할 때 권한없는 사용자의 접근으로 인한 통신간 데이터 기밀성에 대한 취약점이 발생한다. 본 논문에서는 통신간의 전송하는 데이터의 취약점 조치 및 보안성 강화를 위해 등록 및 인증과정에서 생성한 DeviceCode, S-PhoneCode, SignartureCode와 같은 파라미터를 활용하여 데이터 위협에 대한 피해를 막을 수 있다. 데이터 기밀성 뿐만 아니라 무결성을 보장하기 위해서 게이트웨이의 Signatue 식별값을 검증함으로써, 안전한 통신을 수행하도록 하였다.

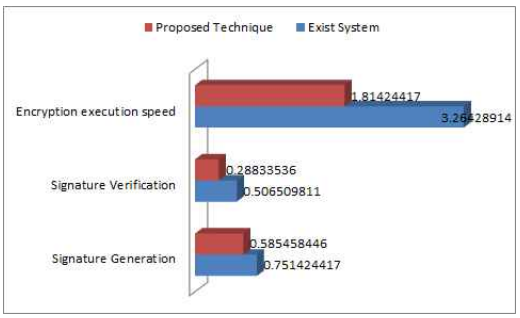
물리적 기기 위협 : 사용자의 부주의 및 도난등이 발생하여 디바이스에 대한 물리적 기기위협은 중대한 보안위협이 될 수 있다. PIN 그리고 비밀번호가 설정되지 않거나 암호화 강도가 낮은 데이터를 암호화를 수행하여 데이터를 전송하는 경우 데이터 관리를 취약할 수밖에 없다. 제안한 사항에서는 디바이스의 패스워드와 시리얼 넘버를 조합하여 Device 생성하여 안전한 데이터를 통신할 수 있도록 설계한다. 그리고 DeviceCode,S-PhoneValue 의 주기적인 확인을 통한 식별값을 검증함으로서, 디바이스의 보안성을 강화한다.

데이터 유출 : 스마트 디바이스를 활용한 무선 네트워크 환경에서 데이터 유출은 가장 우려되는 보안 위협으로 알려지고 있다. 해커의 악의적인 침해외로 사용자의 부주의로 발생하는 경우가 빈번하다. 본 논문에서는 스마트 디바이스로 부터 수집한 데이터의 유출의 피해를 막기 위해 메시지 통신 프로토콜 절차에서 Signature 값을 생성하여 서비스 제공자가 검증함으로써 데이터 위협을 방지할 수 있었다.

4.2 보안성 평가

본 절에서는 제안한 접근제어 기법과 기존 시스템의 보안성 평가를 수행한다. 제안한 접근제어 기법의 비교분석을 수행할 환경은 Intel(R) Core(TM) i7-4770 CPU @ 3.40 GHz, 3.40 GHz, RAM 8.00GB 64bit이며, Mysql 5.7.18, SQL developer, Eclipse Software를 사용하였다.

기존의 시스템에서 활용하고 있는 SSL/TLS기반의 메시지 통신 및 데이터 교환기법과 본 논문에서 제안한 기법에 대해서 비교분석을 수행하였다. 메시지의 무결성을 보장하기 위한 서명값 생성, 생성된 서명값에 대한 검증, 전체적인 암복호화 수행속도에 대해서 비교분석을 수행하였으며 결과는 <그림 4>와 같다.



<그림 4> 기존시스템과 제안기법과 비교분석

사물인터넷 게이트 보안 요구사항(TTAK.KO-12.0297)의 기반으로 기존의 시스템과의 비교분석을 수행하였다. 기존 시스템의 인증서 발급은 SSL/TLS 방식과 제안한 서명값 생성 및 검증과의 비교분석을 수행하였다. 그리고 암호화 수행속도는 PKI+AES와 제안한 암호화 통신 방식과의 비교분석하였다. 인증서 생성은 기존의 생성방식 대비 약 22%, 검증방식 대비 약 43%, 암호화 수행속도 대비 약 44%의 효율성의 속도증가 부분을 확인 할 수 있었다.

Ⅴ. 결론

본 논문에서 스마트 디바이스 기반의 보안성 강화를 위한 접근제어 기법을 설계하였다. 제안한 접근 제어 기법은 스마트 디바이스 등록 및 인증 절차를 수행하여 안전한 통신 프토콜을 설계하였다. 그리고 디바이스의 안전한 관리를 위해서 해지 및 갱신 프로토콜을 설계하여, 전송한 데이터에 대한 기밀성 및 무결성을 보안하였다.

제안한 접근제어 기법은 기존의 무선 네트워크 환경에서 발생하는 중간자 공격 위협, 통신간 데이터의 기밀성 위협, 물리적 기기 위협, 데이터 유출과 같은 취약점에 대해서 안전성을 분석하였다. 또한 기존의 사용하는 서명발급 및 검증, 통신 속도에 대한 효율성을 분석하여 보안성을 평가하였다.

4차 산업혁명에 따라서 스마트 디바이스 기반의 서비스가 급속도로 증가하고 있어, 본 논문에서 제안한 접근제어 뿐만 아니라 보안정책에 대한 연구가 필요하다. 그리고 스마트 디바이스에 대한 보안 위협 완화 및 보안성 강화에 대한 대응책이 요구되고 있다.

참고문헌

[1] 권혁찬, 정병호, “사물인터넷 게이트웨어 보안 요구사항,” TTAK.KO-12.0297, 2016.12.

[2] “스마트디바이스의 이해와 활용,” https://www.slideshare.net/mcstop81/ss-13459194

[3] “스마트 디바이스 산업의 정의,” http://kidia.or.kr/main/main.php?categoryid=02&menuid=01&groupid=00

[4] 강동호 외 6명, “스마트폰 보안 위협 및 대응 기술,” ETRI, Vol 25, No 3, 2010. 6

[5] 서승현, “스마트폰 보안 위협 및 대응 전략, TTA,” 2010.

[6] “2018년 주의해야 할 5대 모바일 보안 위협,” http://www.ciokorea.com/news/36874

[7] 산업연구원, “사물인터넷 시대 안전망, 융합보안 산업,” 2014.4.15.

[8] 정보통신기술진흥센터, 주요 ICT 분야의 중국 R&D 정책 현황 및 성과와 향후 전망, 2014.10.30.

[9] GSMA, “MOBILE INDUSTRY EMBRACES GSMA EMBEDDED SIM SPECIFICATION TO ACCELERATE GROWTH OF INTERNET OF THINGS,” 2014.10.

■ 저자소개 ■

박 중 오
(Park Jungoh)

2000년 7월 : 성결대학교 컴퓨터공학과 졸업
2003년 3월 : 명지대학교 전자계산교육 석사
2011년 8월 : 숭실대학교 컴퓨터공학 박사
2016년 3월 ~ 현재 : 성결대학교 파이데이아 학부 조교수

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

논문접수일 : 2018년 08월 22일
수 정 일 : 2018년 08월 28일
게재확정일 : 2018년 08월 29일