디지털산업정보학회 논문지 제12권 제1호-2016년 3월
http://dx.doi.org/10.17662/ksdim.2016.12.1.035

IoT 환경에서 안전한 통신을 위한 세션 키 기반 접근 제어 기법의 설계 및 평가

진 병 욱*·정 동 욱**·차 시 호***·전 문 석****

Design and Estimation of a Session Key based Access Control Scheme for Secure Communications in IoT Environments

Jin Byungwook · Jung Dongwoog · Cha Siho · Jun Moonseog

〈Abstract〉

Internet of Things (IoT) services are widely used in appliances of daily life and industries. IoT services also provide various conveniences to users and are expected to affect value added of all industries and national competitiveness. However, a variety of security threats are increased in IoT environments and lowers reliability of IoT devices and services that make some obstacles for commercialization. The attacks arising in IoT environments are making industrial and normal life accidents unlike existing information leak and monetary damages, and can expand damage scale of leakage of personal information and privacy more than existing them. To solve these problems, we design a session key based access control scheme for secure communications in IoT environments. The proposed scheme reinforces message security by generating session key between device and access control network system. We analyzed the stability of the proposed access scheme in terms of data forgery and corruption, unauthorized access, information disclosure, privacy violations, and denial of service attacks. And we also evaluated the proposed scheme in terms of permission settings, privacy indemnity, data confidentiality and integrity, authentication, and access control.

Key Words : Internet of Things, Key Generation, Access Control, Session Key

Ⅰ. 서론

사물인터넷(IoT, Internet of Things)은 사물이 통신의 주체로 참여하여 인터넷에 연결하는 기술을 의미하고 사물들로부터 효율적이고 다양한 서비스를 제공받을 수 있도록 해준다. 이러한 IoT 기술은 차량, 홈서비스, 의료서비스, 에너지 분야 등 다양한 분야와 결합하여 상호운영이 가능한 융합서비스분야가 가능하도록 지원되고 있다[1]. 이로 인하여 사용자들은 다양한 편의적인 서비스를 전폭적으로 제공받을 수 있지만, 이에 따른 보안위협의 사례가 갈수록 증가하고 있다. 따라서 IoT 환경의 신뢰성을 높이기 위해서는 보안위협을 극복할 수 있는 보안기술이 요구되고 있

* 숭실대학교 컴퓨터학과 박사수료
** 한화탈레스 전술통신팀 선임연구원
*** 청운대학교 멀티미디어학과 교수(교신저자)
**** 숭실대학교 컴퓨터학과 교수

다. 국외의 H사의 자료에 의하면 IoT 장비들의 패스워드 관리 및 인증 암복호화 기술에서 거의 70%이상의 취약점이 노출되어 이에 따른 위험성에 직면하고 있다. 또한 개인정보 유출 및 금전적인 피해도 발생하고 있다[2-3]. IoT 기술은 사용자의 환경과 매우 밀착되어 있기 때문에, 사회적 재회나 인명사고가 발생하는 심각한 문제를 야기하고 있다[2, 4].

따라서 본 논문에서는 IoT 디바이스와 사용자를 식별 후 세션 키를 생성하여 이를 기반으로 안전한 메시지를 통신하는 새로운 프로토콜을 설계하고자 한다.

본 논문의 구성은 다음과 같다. 2장에서는 IoT 정의 및 서비스 활용사례와 보안위협에 대해서 기술하고, 3장에서는 제안시스템의 설계, 디바이스 식별 및 SSL 채널 설립 절차와 메시지 통신에 대해서 기술한다. 4장에서는 본 논문에서 제안한 프로토콜의 효율성을 검증하기 위하여, IoT 환경에서 발생하는 보안위협에 대하여 안전성 분석 및 보안성을 평가하였다. 그리고 5장의 결론에서는 제안한 프로토콜의 향후 연구 방향에 관하여 논의하였다.

Ⅱ. 관련연구

2.1 IoT 서비스 활용사례 및 보안 요구사항

사물 인터넷(IoT)은 기존의 통신 환경이 사람과 사물 간에 언제(Anytime), 어디서나(Anyplace) 정보를 제공하는 것뿐만 아니라, 어느 것이나(Anything)라는 개념을 추가함으로써 사물 대 사물뿐만 아니라 사람과 사물의 영역까지 확대하여 통신을 수행할 수 있도록 제공하는 기술이다[3-5]. IoT 환경의 Anything은 실제적인 공간뿐만 아니라 가상공간에서도 식별하는 정보를 포함하고 있다.

국내외 IoT 활용 사례를 살펴보면 스마트 폰 기술과 융합하여 사용자들로부터 편의성을 제공하고 있으며, 국가기관에서도 전폭적으로 투자하고 있고 기업들에서도 기술력 향상을 위해 노력하고 있다. 현재는 주로 스마트홈(Smart-Home)과 스마트카(Smart-Car) 중심으로 서비스가 확대되어지고 있으며 비 IT 산업으로 연결하여 다양한 서비스가 생겨나고 있다[6, 8].

국외의 애플(Apple)과 시스코(Cisco)사는 스마트 환경에서 사용자 삶의 질을 향상시키기 위한 IoT 서비스가 개발되고 있으며, 국내에서는 LG 전자와 삼성 전자는 스마트 폰을 활용한 스마트홈 서비스, SKT사는 스마트카와 스마트팜 서비스를 활용하여 가전과 비가전을 연동하여 사용자들에게 효율성을 제공하고 있다[7].

IoT는 디바이스, 네트워크, 플랫폼/서비스 영역에서 보안 위협 및 취약점이 발생하므로 다음과 같은 보안 요구사항을 명시하고 있다. 디바이스 영역에서는 저사양 디바이스 기반의 경량 암호기술과 신뢰성을 보장하는 관리 기술이 요구된다. 네트워크 영역에서는 이기종의 통신 환경에서 상호 운용성 기반의 보안 기술과 모니터링 기술이 필요하다. 마지막으로 플랫폼/서비스 영역에서는 IoT 디바이스를 사용하는 사용자의 식별 정보 및 필터링 기술과 상호간의 인증, 키 제어, 신뢰성 관리에 대한 연구가 요구된다.

2.2 IoT 보안위협

IoT는 다양한 기술요소의 집합체로 단말, 네트워크, 애플리케이션이 다양하게 융합되고 있다. 이로 인하여 다양한 보안위협이 발생하고 있다. 예를 들어서 기존의 유무선통신 환경에서 나타날 수 있는 위협들을 상속되고 있으며, 기술적, 관리적인 측면에서도 아래와 같은 신규 및 변종 보안위협들이 발생하고 있다[4].

- 단말 분실 및 물리적 파괴 : IoT 서비스를 제공하기 위해서 개방된 장소에 설치될 때 악의적인 사용자에 접근에 의해서 물리적 파괴가 발생할 수 있다. 또한 사용자의 부주의로 디바이스가 분실될 때 정보유출과 같은 사고가 발생할 수 있다[5, 9].
- 무선신호 교란 : 이동통신망, 위성망, RF, Zigbee 등의 활용하여 무선네트워크를 통하여 IoT 서비스를 제공한다. 그러나 공격자는 무선인터페이스를 기반의 전파차단 장치를 활용하여 방해할 수 있으며, 허가되지 않은 무선교란 장치를 사용하여 DoS 공격을 수행할 수 있다[5].
- 정보유출 : IoT 환경에서 서비스를 수행할 때 유무선 통신기술 기반으로 데이터를 송수신한다. 이 때 기존에 발생하는 보안위협인 스니핑(Sniffing), 불법도청 공격기법을 통하여 중요정보, DB를 탈취한다. 이러한 정보를 악용하여 프라이버시 침해 등의 2차 피해를 발생할 수 있다[3].
- 데이터 위·변조 : 공격자는 비인가 된 단말기에 접근하여 데이터 통신과정에서 스니핑, 맨인더미들어택 (MMA or MITM : Man In The Middle Attack) 등과 같은 공격을 통하여 데이터를 위·변조할 수 있다[9].

Ⅲ. IoT 환경에서 안전한 통신을 위한 세션 키 기반 접근 제어 기법 설계

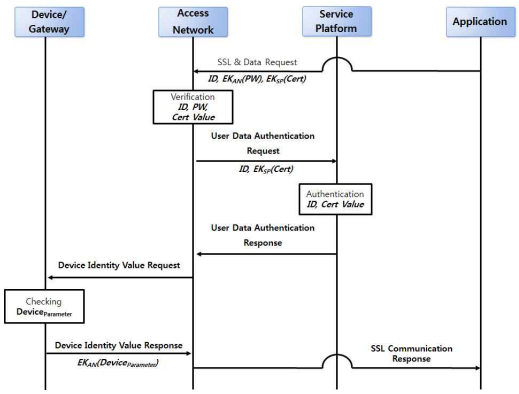
3.1 제안시스템 설계

본 논문에서는 사용자가 애플리케이션을 사용하여 액세스 네트워크에 접속한 다음 디바이스/게이트웨이에서 수집된 데이터를 전송받는 프로토콜을 제안한다. 디바이스/게이트웨이에서 수신된 데이터를 안전하게 받기 위해서 디바이스와 액세스 네트워크간의 인증과정을 수행한다. 이후 디바이스에서 생성한 난수 값을 사용하여 해쉬 알고리즘을 통한 해쉬 값을 생성하고, 액세스 네트워크의 파라미터 값을 조합하여 연산 작업을 수행한 후 세션 키를 생성한다. 생성한 세션 키를 기반으로 암호화를 수행하여 디바이스/게이트웨이와 액세스 네트워크간의 데이터를 전송한다. 이를 위하여 본 논문은 다음과 같은 두 가지 사항을 가정하고 있다.

1. 디바이스/게이트웨이를 설정하기 전에 액세스 네트워크로부터 시리얼 번호를 등록을 한다.
2. 디바이스/게이트웨이와 액세스 네트워크는 세션 키 생성 알고리즘을 공유하고 있다.

3.2 디바이스 식별 및 SSL 채널 설립 절차

<그림 1>은 본 논문에서 제안한 IoT 환경에서 안전한 통신을 위한 세션 키 기반 접근 제어 기법의 디바이스 식별 및 SSL 채널 설립 과정을 보인 것이다.



<그림 1> 디바이스 식별 및 SSL 채널 설립 과정

<그림 1>에서 보인 것과 같이 디바이스 식별 및 SSL 채널 설립 과정은 다음과 같은 절차에 따라 수행된다.

1. 사용자는 애플리케이션을 사용하여 액세스 네트워크에 SSL 통신 및 디바이스의 데이터를 요청한다.

$$ID, Ek_{AN}PW, Ek_{SP}(cert)$$

2. 액세스 네트워크는 애플리케이션으로 송신된 ID, PW, Cert Value를 검증을 한다.
3. 액세스 네트워크는 서비스 플랫폼으로부터 ID, Cert value를 송신하여 사용자의 데이터 인증을 요청한다.

$$ID, Ek_{SP}(cert)$$

4. 서비스 플랫폼은 사용자의 ID, Cert Value에 대한 인증 작업을 수행하고 액세스 네트워크로부터 사용자 데이터 인증 응답 메시지를 전송한다.
5. 액세스 네트워크는 디바이스로부터 식별 값을 요청한 다음, 디바이스를 위한 $Device_{Parameter}$를 생성한 후 이를 암호화 하여 액세스 네트워크로 전송한다.

$$EK_{AN}(Device_{Parameter})$$

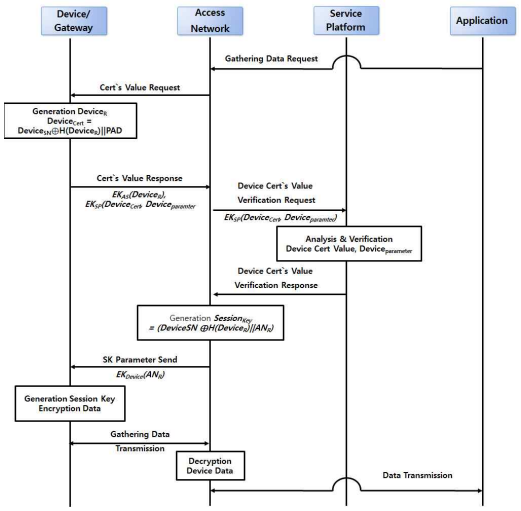
6. 액세스 네트워크는 애플리케이션으로부터 SSL 통신 채널을 설립하기 위한 요청 메시지를 전송한다.

3.3 메시지 통신 설계

<그림 2>는 IoT 환경에서 안전한 통신을 위한 세션 키 기반 접근 제어 기법의 메시지 통신 과정이다.

<그림 2>에서 보인 것과 같이 메시지 통신 과정은 다음과 같은 절차에 따라 수행된다.

1. 사용자는 애플리케이션을 활용하여 액세스 네트워크로부터 수집한 데이터를 요청한다.
2. 액세스 네트워크는 디바이스/게이트웨이로 Cert Value 요청 메시지를 전송한다. 디바이스는 난수



<그림 2> 메시지 통신 과정

를 생성한 후 해쉬 값을 생성하여 액세스 네트워크로 응답 메시지를 전송한다.

$$Device_{cert} = (Device_{SN} \oplus Hash(Device_R) \| PAD),$$
$$EK_{AS}(Device_R),$$
$$EK_{SP}(Device_{Cert}, Device_{Parameter})$$

3. 액세스 네트워크는 디바이스/게이트웨이에서 수신된 데이터를 서비스 플랫폼으로 검증 요청 메시지를 전송한다.

$$EK_{SP}(Device_{Cert}, Device_{Parameter})$$

4. 서비스 플랫폼에서는 디바이스/게이트웨이의 Cert Value, Device Info를 분석하고 검증한 후 액세스 네트워크로 검증 메시지를 전송한다.
5. 액세스 네트워크에서는 세션 키를 생성한 후 디바이스/게이트웨이에 관한 정보를 등록한다. 이후 세션 키를 생성한다.

$$Session\,Key = (Device_{SN} \oplus Hash(Device_R) \| AN_R)\, EK_{Device}(AN_R)$$

6. 디바이스/게이트웨이에서는 세션 키 파라미터를

수신한 후 세션 키를 생성한 다음 이를 기반으로 데이터를 암호화 하여 액세스 네트워크로 전송한다.

$$EK_{Device}(AN_R),$$

7. 액세스 네트워크에서는 디바이로부터 수신된 데이터를 복호화한 후 애플리케이션에게 SSL 통신이 설립된 채널을 통하여 데이터를 전송한다.

Ⅳ. 안정성 분석 및 보안평가

4.1 안전성 분석

본 논문에서 제안한 IoT 환경에서 안전한 통신을 위한 세션 키 기반 접근 제어 기법에 대한 안전성 분석은 2.2절에서 기술한 내용을 기반으로 데이터 변조, 비 인가된 접근, 정보 유출, 프라이버시 침해, 서비스 거부 공격 등과 같은 보안위협 및 취약점에서 분석한다.

- 데이터 위변조 : IoT 기술이 사용자로부터 상용화 되면서 센서로 부터 수집된 데이터 수집에 따른 위변조 위협이 존재할 수 있다. 이를 해결하기 위하여 디바이스를 식별한 후 SSL 채널을 설립함으로써 데이터의 보안을 강화할 수 있다.
- 비 인가된 접근 : 악의적인 사용자로부터 접근을 막기 위해 본 논문에서는 액세스 네트워크에서 ID, PW을 확인한 후 $Ek_{SP}(cert)$을 서비스 플랫폼으로 발송함으로써 Cert Value를 복호화하고 검증함으로써 비인가 된 접근에 안전할 수 있다.
- 정보 유출 : 최근 들어 IoT 관련 해킹 및 정보유출 사례가 발생하고 있다. 정보 유출을 막기 위해 서비스 플랫폼에서는 디바이스와 사용자 권한에 알맞은 세션 키를 생성한 후 등록한다. 세션 키는 디바이스의 $Device_{SN}$, AN_R, $Hash(Device_R)$ 연산으로 디바이스의 접근 출처 및 사용자의 인증 값을 확인함으로써 유출에 대한 피해를 막을 수 있다.
- 프라이버시 침해 : IoT 환경의 인터페이스는 디바이스와 사용자간의 상호작용을 촉진하고 프라이버시 보호에 대한 책임이 있어야 한다. 제안한 프로토콜에서는 서비스 플랫폼의 ID와 Cert Value에 대한 인증 작업을 수행하고 수신된 데이터를 검증함으로써 프라이버시 보호에 대해 안전할 수 있다.
- 서비스 거부 공격 : 메시지 통신 프로토콜 절차에서 검증요청 메시지 확인과 세션 키 파라미터를 수행함으로써 안전하게 수집된 메시지를 사용자로부터 안전하게 통신할 수 있으며, 디바이스 식별 및 채널 설립 절차에서 $Device_{Parameter}$를 생성한 후 이를 암호화 하여 액세스 네트워크로 전송하는 과정을 통하여 서비스 거부 공격에 안전하다.

4.2 보안성 평가

본 절에서는 앞에서 기술한 보안 요구사항을 참고하여 기존 시스템과 제안 프로토콜의 보안성을 평가하였다. <표 1>은 보안성 평가에 대한 내용을 보인 것이다.

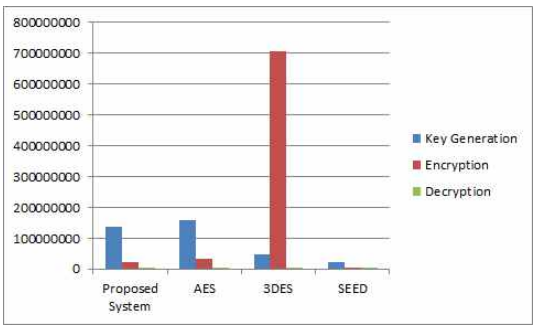
<표 1> 보안성 분석[4]

	기존 시스템	제안된 프로토콜
권한설정	△	○
프라이버시 보장	○	◎
데이터 기밀성 및 부결성	○	◎
인증	○	◎
접근통제	△	○

본 논문에서 제안된 프로토콜에서는 사용자의 Cert Value와 $Device_{SN}$을 활용한 세션 키를 사용하여 권한 설정과 데이터의 기밀성 및 무결성을 지원하도

록 설계하였으며, $Device_{Parameter}$를 확인하여 비 인가된 디바이스의 접근을 통제함으로써 프라이버시 보장이 제공하도록 설계하였다. 또한 액세스 네트워크에서 사용자의 ID와 PW뿐만 아니라 서비스 플랫폼에서 Cert Value를 검증함으로써 사용자 인증도 효과적으로 수행하도록 하였다. 마지막으로 디바이스의 $Devce_{SN}$, $Device_R$과 액세스 네트워크의 AN_R을 검증함으로써 상호 인증을 통하여 접근 통제 기능을 강화하였다.

또한 제안 프로토콜에서 생성된 세션 키의 효율성을 분석하기 위해서 기존의 대칭키 암호화 방식인 AES, 3DES, SEED의 암호화, 복호화, 키 생성의 수행시간에 대해서 분석하였다. 기존 암호화 수행방식과 제안된 암호 기법의 비교 분석은 <그림 3>과 같다.



<그림 3> 기존 암호화 수행방식과 제안된 암호기법의 비교분석

제안된 암호기번의 성능평가를 위한 수행 환경은 Inter(R) Core(TM)2 Quad CPU Q9400 @ 2. 66 Hz 2. 66GHz, 4.00GB와 Windows 7 Enterprise OS으로 구성하였으며, Eclipse IDE for Java Developers를 활용하였다. 제안된 프로토콜의 세션 키는 SHA-128 기반의 해쉬 함수를 수행해서 생성된 $Device_R$과 $Device_{SN}$을 Xor 연산 후 값과 연접한 값으로 기존에 사용되는 AES 대비 대략 13%의 향상성을 확인할 수 있었다.

Ⅴ. 결론

본 논문에서는 IoT 환경에서 세션 키를 생성하여 안전한 통신을 수행하기 위한 접근 제어 기법을 설계하였다. 디바이스 식별 및 SSL 채널 설립 단계에서 사용자 인증을 수행하고 $Device_{Parameter}$를 검증한다. 이후 해쉬 함수를 사용하여 $Device_{Cert}$를 검증한 후 디바이스와 액세스 네트워크의 난수 값을 생성하여 세션 키를 생성함으로서 메시지를 안전하게 통신하도록 설계하였다. 제안된 프로토콜을 IoT 환경에서 발생하는 데이터 위변조, 정보 유출, 프라이버시 침해, 서비스 거부와 같은 보안 위협에 대해서 안전성을 분석하였으며, 보안 요구사항을 기반으로 기존 시스템과의 보안성을 분석함으로써 그 타당성을 평가였고 기존에 암호화 방식은 AES보다 대략 13%의 향상된 효율성을 확인 할 수 있었다.

향후 연구계획으로는 IoT 기술을 활용하여 ICT 환경에서 적용되고 있는 분야에 따른 연구가 필요하다. 그리고 각각의 기관 및 기업에서도 효과적으로 적용할 수 있는 보안 정책 수립이 필요하다.

참고문헌

[1] 미래창조과학부 2013년도 업무보고 자료(과학기술과 ICT를 통한 창조경제와 국민행복 실현,) 2013.

[2] ITU, “ITU Internet Reports 2005, Internet of Thing,” ITU, 2005.

[3] ITU-T Y. 2060, “Overview of the Internet of Things,” ITU, 2012.

[4] EPoSS, “Internet of Things in 2020, A Roadmap for the Future,” EPoSS, 2008.

[5] 진병욱, 전문석, “IoT환경에서 안전한 데이터 송

신을 위한 키 생성 프로토콜 설계," 디지털산업정보학회 학술발표집, 2014.

[6] 임철수, "IoT 서비스 활용사례 분석 및 산업 활성화 이슈," 한국차세대컴퓨팅학회논문지, Vol. 11 No. 6, 2015, pp. 41-50.

[7] 정종수, 김재석, 김상철, 신규상, 마평수, 박승민, "M2M 지능형 사물 플랫폼 동향," 정보통신산업진흥원, 주간기술동향 통권 1455호, 2010.

[8] ITU-T Y. 2060, "Overview of the Internet of Things," ITU, 2012.

[9] 진병욱, 박재표, 이근왕, 전문석, "M2M 환경에서 신원기반 암호기법을 활용한 인증기법에 관한 연구," 한국산학기술학회논문지, 제14권, 제4호, 2013, pp. 1926-1934.

■ 저자소개 ■

진 병 욱
Jin Byungwook

2011년 3월~현재 숭실대학교 컴퓨터학과 박사수료
2011년 2월 숭실대학교 대학원 컴퓨터학과 (공학석사)
2010년 2월 청운대학교 멀티미디어학과 (문학사)

관심분야 : IoT, 인증 시스템, 접근제어
E-mail : quddnr4511@naver.com

정 동 욱
Jung Dongwoog

2008년 2월~현재 한화탈레스 선임연구원
2008년 2월 서울대학교 전기컴퓨터공학부 (공학석사)
2005년 8월 서울대학교 전기컴퓨터공학부 (공학사)

관심분야 : IoT, Artificial Intelligence, Software Engineering
E-mail : dongwoogjeong@gmail.com

차 시 호
Cha Siho

2009년 3월~현재 청운대학교 멀티미디어학과 교수
1997년 7월~2000년 2월 대우통신 종합연구소 선임연구원
2004년 2월 광운대학교 대학원 컴퓨터과학과 (공학박사)
1997년 8월 광운대학교 대학원 전산계산학과 (이학석사)

관심분야 : 네트워크 관리, 차량통신 네트워크, 무선 센서 네트워크, IoT
E-mail : shcha@chungwoon.ac.kr

전 문 석
Jun Moonseog

1991년 3월~현재 숭실대학교 컴퓨터학과 정교수
1991년 2월 New Mexico State University Physical Science Lab. 책임연구원
1989년 2월 University of Maryland Computer Science 박사

관심분야 : 정보보호, 암호학, 네트워크 보안
E-mail : mjun@ssu.ac.kr

논문접수일: 2016년 2월 27일
수 정 일: 2016년 3월 14일
게재확정일: 2016년 3월 17일