ISSN 2234-4438
중소기업융합학회 논문지 제6권 제2호 pp. 37-44, 2016 DOI : http://dx.doi.org/10.22156/CS4SMB.2016.6.2.037

사물인터넷 통신기술에 내재된 보안위협과 대응 전략

문형진[1], 최광훈[1], 황윤철[2*]
[1]백석대학교 정보통신학부, [2]한국교통대학교 정보공학과

Countermeasure to Underlying Security Threats in IoT communication

Hyung-Jin Mun[1], Gwang-Houn Choi[1], Yooncheol Hwang[2*]
[1]Division of Information & Communication, Baekseok University
[2]Department of computer science and information Engineering, Korea National University of Transportation

요 약 현대 사회는 ICT 기술의 급속한 성장으로 모바일 기기의 대중화와 사회 전반이 네트워크화 됨으로써 사람과 사람, 사람과 사물, 사물과 사물 간에 언제 어디서든 연결할 수 있는 시대가 되었다. 또한 모든 전자기기가 인터넷에 연결됨으로써 사물의 특성이 더 지능화되고 자동화되면서 기기들의 연결을 통한 정보의 융합 및 가공이 가능해져 더 좋은 품질의 서비스가 제공되고 있다. 그러나 이런 기기들은 유·무선 네트워크를 통해 상호간에 정보를 전달하기 때문에 많은 보안 위협에 노출되어 있다. 따라서 본 논문에서는 사물인터넷 통신 관련 기술인 ZigBee, CoAP, MQTT, XMPP에 대해 분석하여 이런 통신기술들이 가지고 있는 보안 위협들을 도출하고, 사물인터넷을 구성하는 요소들이 가져야하는 보안요구사항을 제안한다. 그리고 사물인터넷에 존재하는 보안 위협에 대해 실제 사례들을 살펴보고 이에 대한 대응 전략을 제시하여 향후 사물인터넷을 보다 안전하게 사용할 수 있는 토대를 구축하는데 기여한다.

키워드 : MQTT, ZigBee, CoAP, XMPP, 사물인터넷

Abstract Due to the remarkable improvement of ICT, with the popularization of mobile devices and every sector of society connected by networks, an era, in which peer to peer, peer to thing, thing to thing can be connected to one another everywhere, has begun. As all the electronic devices are connected to Internet, they have become more intellectualized and automated, making convergence and process of information through the connection of the devices possible to provide a lot better services. However, those devices communicate mutually to send information and they are exposed to various security threats. Therefore, this study analyzes ZigBee, CoAP, MQTT, XMPP, which are communication-related technology of IoT, draws security threats they have, and suggests requirements that components of IoT should have. Plus, it examines real cases about security threats in IoT, and suggests a countermeasure so as to contribute to establishment of a basis for IoT to be used much more safely in the future.

Key Words : MQTT, CoAP, ZigBee, XMPP, Internet of Things

Received 2016-06-07 Revised 2016-06-14 Accepted 2016-06-17 Published 2016-06-30
*Corresponding author : Yooncheol Hwang (dolpin98@nate.com)

1. 서론

ICT 발달과 모바일 단말기 혁신으로 지금보다 더 많은 가전제품, 전자기기와 서비스가 네트워크로 연결되어 현재의 수준보다 더 나은 세상이 도래하고 있다.

사물인터넷(IoT)는 Internet of Things의 약자로 1999년 캐빈 애쉬튼(Kevin Ashton)에 의해 제안된 개념이다. IoT 개념의 출발은 RFID 태그를 통한 사물의 인식을 시발점으로 혁신적으로 발전해 왔다. 센서와 모바일 폰 등의 다양한 사물들이 네트워크를 통해 상호 연결되면서 혁신적인 발전이 이루어졌다[1].

CERP(Cluster of European ResearchProjects)에서 IoT를 향후 미래에 사용되는 인터넷의 통합적인 부분으로, 물리적 혹은 가상의 식별자를 소유한 표준 운용 통신, 서로 간의 운용 통신 프로토콜, 물리적 구조와 지능, 자동적 구성 기능과 활발한 세계적 네트워크 인프라로 정의한다[2].

하지만, IoT의 보안이슈는 산업시장을 위협 할 만큼 중요한 문제가 되었다. IoT 특성상 자원의 제한과 저전력 통신 기술을 적용함으로써 위협요소가 더 많아졌다. 사물인터넷 환경에서는 연결된 정보의 하이재킹을 통해 사용자의 정보가 공격자에 의해 수집 될 수 있다. 예를 들어, 사용자가 기계장치를 통해 외부에서 집안을 확인할 수 있는 CCTV 화면에 대한 하이재킹 등이 가능하다. CCTV 외에도 집이나 건물에 있는 IoT를 통한 많은 범죄 및 악용 가능성이 많아지고 있다.

본 논문의 구성은 다음과 같다. 2장에서는 IoT의 통신 보안기술에 대해 설명하고, 3장에서는 IoT에 대한 보안 요구사항 및 위협을 제시하고 4장에서는 위협사례 및 대응방안을 살펴본다. 마지막으로 5장에서는 논문의 결론과 함께 향후 연구방향을 제시한다.

2. 사물인터넷의 통신기술

2.1 ZigBee

ZigBee는 저가, 저전력 무선 메시 네트워크의 표준으로 개인 통신망을 구성하여 통신하기 위한 표준기술이다. ZigBee는 높은 수준의 보안에 속하는 HSM(High Security Mode)방식과 상대적으로 낮은 수준의 보안에 속하는 SSM(Standard Security Mode) 2가지 방식으로 나누어진다. ZigBee보안기술은 Open Trust Model 방식으로 작동한다. 서로 다른 ZigBee장치 간 통신의 무결성과 기밀성이 보장 된다면 신뢰할 수 있다. 하지만 통신 전 구간에 대해 암호화가 이루어지기 어렵기 때문에 비암호화 통신구간에 대한 별도의 대책을 필요하다[3,4].

Fig. 1에 명시된 것과 같이 ZigBee 네트워크에는 ZC(ZigBee Coordinator), ZR(ZigBee Router), ZED (ZigBee End Device)로 구성되어 있다. ZigBee 네트워크 내에 ZC는 하나만 존재하고, ZC내에 TC(Trust Center)가 존재한다. TC가 네트워크내의 모든 장치를 관리하고, 네트워크에 사용되는 키를 관리하고, 생성된 키는 암호화하여 전송한다[4]. 이 네트워크에 디바이스가 추가되기 위해서는 ZigBee 규격에 따라 SKKE(Symmetric -Key Key-Establishment) 프로토콜 이행을 통해 Link Key Network key를 확인하고, 라우터는 Network key 확인 후 Join을 허용하게 함으로서 권한이 없는 노드의 네트워크 참여를 차단한다[2,3,5,6].

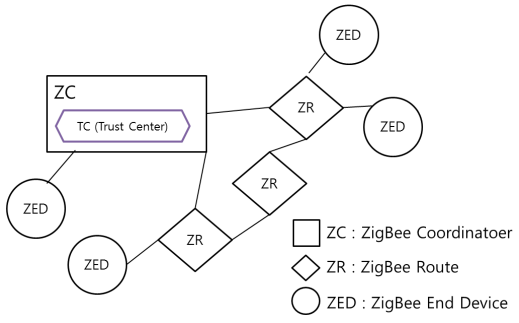

Fig. 1. ZigBee device and Trust Center

2.2 MQTT

1998년 IBM의 Dr. Andy Stanford-Clark과 EUROTECH의 Arlen Nipper에 의해 개발된 모바일용 양방향 통신규약인 MQTT(Message Queuing Telemetry Transport)는 경량적인 프로토콜이다[7]. 세계적인 비영리 컨소시엄인 OASIS(Organization for the Advancement of Structured Information Standards)에서 IoT를 위한 표준으로 MQTT를 채택하였다. 이는 인증이 되지 않은 네트워크 환경에서 보다 낮은 대역폭, 많은 대기시간, 한정된 자원을 가진 장치에 용이하다[7,8]. MQTT는 효율적인 통신을 위해 양방향 Pub/Sub 메시징 서비스로 Topic을 활용하여 통신한다. Clients (Publishers, Subscribers)들은 통신을 위해 Broker의 주소를 설정하고, TCP 기반으로 통신한다. MQTT가 HTTP보다 메시지 전달 및 수신

처리에 탁월한 성능으로 인해 현재에 Facebook Messenger 등에서 사용하고 있다[7].

2.3 CoAP

IETF의 CoRE그룹에서 보여준 CoAP 프로토콜은 REST 구조로 미래의 IoT 프로토콜로 활용 가능성이 높다. CoAP은 IoT 구성 요소들이 HTTP 프로토콜과 쉽게 통신이 되도록 연결이 용이하다[9]. 표준 인터넷 프로토콜에서 정의한 SOAP나 HTTP, FTP등은 기초 Payload의 길이가 길고, 혼잡한 흐름 통제 등의 문제로 인하여 IoT에 활용하는 네트워크 프로토콜로는 부적합하지만 CoAP는 향후의 IoT 부문에서 적합한 프로토콜이다. CoAP의 스택구조는 Fig. 2처럼 4단계로 구성된다[9]. CoAP는 UDP상에서 단순하며 낮은 오버헤드와 멀티캐스트을 수행한다. CoAP 표준은 사물 간 통신에서 데이터의 기밀성과 무결성을 위해 UDP기반 TLS 방식인 DTLS(Datagram Transport Layer Security)을 사용한다[10]. CoAP프로토콜은 DTLS handshake 이후에 세션을 구축하고, CoAP 메시지는 DTLS의 application data로 진송된다[11]. 키 값과 접근제어목록(ACL) 정보는 디바이스 권한설정 과정에서 제공된다. DTLS이 적용된 CoAP을 사용하는 Device의 보안모드는 Table 1과 같다[9-12].

Application
Request/Response Msg
DTLS
UDP

Fig. 2. Stack Structure of CoAP

2.4 XMPP

XMPP(eXtensible Messaging and Pressence Protocl)는 IETF(Internet Engineering Task Force)에서 제정한 XML 에 기반한 메시지 지향 미들웨어용 통신 프로토콜이다[13-15]. XMPP는 다른 사용자와 메시지와 상태정보를 실시간 통신하기 위한 XML 기반 오픈 표준 기술이다[15].

XMPP는 푸쉬 기술로 정보를 갱신할 때 HTTP기반의 Polling방식보다 자원소모가 적고 효율적이다.

구글은 XMPP 기술을 이용하여 googletalk 이라는 인스턴스메신저 서비스를 활용하고 있다[16]. XMPP는 누구나 XMPP서버를 구동할 수 있고, 개방형 표준기술이고, XMPP 서버를 XMPP 네트워크와 분리하여 보안기술을 적용할 수 있어 안전성이 확보할 수 있는 특징이 있다[16,17].

3. 사물인터넷의 통신기술

3.1 보안 요구사항

보안 요구사항으로 IoT 역시 기밀성, 무결성, 가용성의 보안 서비스가 요구된다. 추가적으로 Table 2에서 보듯이 IoT의 특성에 맞게 추가적인 보안 요구사항이 있다. 단말기 계층, 네트워크 계층, 응용 계층의 보편적인 측면과 단말기 등 특수한 경우에 맞는 요구사항이 있다[18].

3.1.1 네트워크 보안

무선 랜 기술은 데이터 링크계층에서 작동하는 IEEE 802.11 규격 기반의 고성능 무선통신으로 스마트 폰과 같은 모바일 단말기의 대중화로 많은 사용자들이 인터넷 서비스를 받고 있다. Wifi 의 데이터 패킷은 단말기와 AP사이 무선으로 전송될때 암호화되지 않을 경우 공격자로부터 무선 패킷 정보 유출 등의 스니핑, 데이터 위변조 등의 공격이 가능하다[19]. 사용자의 단말기와 AP 사이의 무선통신 과정에 안전한 인증과 보안 강한 프로토콜을 이용한 메시지 암호화가 필요하다. 초기에는 사용자 인증 프로토콜로 WEP(Wired Equivalent Privacy)를 사용하였지만 104 bit의 비교적 짧은 키의 길이와 RC4 알고리즘의 취약점으로 현재 사용되지 않고 있다. IEEE는 사용자의 인증으로 WPA(Wi-Fi Protected Access)와 WPA2를 권고한다[18,19].

Table 1. Security Mode of CoAP

Division	Description
NoSec Mode	Deactivated DTLS Mode, Different security mode like IPsec can be utilized
PreSharedKey Mode	Activated DTLS Mode, Authentication to be made with key value shared in advance
RawPublicKey Mode	Activated DTLS Mode, Use of asymmetric key, not certificate
Certificate Mode	Activated DTLS Mode, Use of X.509 standard certificate

Table 2. IoT Security Requirements

Division		Security Requirements
Common security	Device Layer	Setting of rights, Authentication, Integrity verification, Access control, Data confidentiality and Integrity protection
	Network Layer	Setting of rights, Authentication, Data and signal information confidentiality and Integrity protection
	Application Layer	Setting of rights, Authentication, Data confidentiality, Integrity, Privacy protection, Security audit implementation, Anti-virus installation
Special security	Security requirements for special situations such as mobile payment	

Table 3. Security Threats of the Internet of Things

Component	Security Threats
Applications	Forgery of Data, Infringement of data confidentiality, integrity, privacy, Access of unauthorized service or user, Rejection of service
Network	Wireless signal distortion, Forgery of Data, Infringement of confidentiality and integrity of signal data, Authentication disturbance, Rejection of service
Device	Infringement of confidentiality and integrity of device, Loss and theft, Physical breakdown, Cloning attack

3.1.2 단말 및 센서 보안

IoT 환경에서 다른 단말기기와 통신이 연결 될 때, 올바른 기기에서 전송된 데이터 여부 확인할 수 있어야 한다. 기계간의 인증절차는 기계 안에 탑재된 미들웨어 자체에서 실행되거나, 미들웨어가 없는 경우에는 다른 단말 게이트웨이에서 수행된다. 전반적으로 기기 인증방식에는 ID기반 인증, 인증서 기반 인증, SIM 인증 등이 있다.

- ID기반 인증은 일반적인 인증 방식으로 관리자와 기기 간 아이디와 패스워드 확인을 위한 어플리케이션이나 프로토콜을 요구하며, 계정 정보들은 사전에 공유되어 있다.
- 인증서기반 인증은 PKI 기반의 인증서를 많이 사용한다. 기기 확인을 위한 전자서명은 해시함수 SHA-2(256bit)나 암호알고리즘 RSA(2,048bit) 이상을 사용하는 것을 권고한다.
- SIM 방식은 단말에 사용된 UICC 또는 USIM 등을 활용한 인증으로, 이동통신망을 이용한 기기 간에 통신이 가능해지면서 국내 및 해외 여러 전문 기관에서 많은 연구가 진행되고 있다[20]. 국내에서는 여러 통신사가 참여해서 다양한 시범사업에 투자하고 있으며, 해외로는 2011년부터 세계이동통신사업자협회에서 Embedded SIM Project를 개최하여 3GPP, ETSI 등에서 대중화 작업을 진행하고 있다[18].

3.1.3 어플리케이션 보안

IoT 단말 미들웨어는 외부에서 반입되는 데이터가 단말의 운영체제 및 하드웨어 등을 동작하지 않도록 가상화같은 기술을 통해 운영체제와 논리적으로 완벽하게 분리가 되어야 한다. 또한 높은 단계의 응용 소프트웨어에게 전송받은 데이터가 의미가 있는지, 정상적인 기기로부터 전송받은 정보인지 확인하고 통신하는 동안에 데이터 무결성을 보장할 수 있도록 암호기술이나 해시함수 등의 매커니즘을 활용해야 한다[18].

3.2 사물인터넷의 보안 위협

서버와 단말에 불법적인 접근하여 IoT의 가용성을 침해한다. 또한 정보의 조작 및 정보를 탈취하여 기밀성과 무결성 공격, 사생활침해 등의 공격이 가능하다. IoT의 구성요소별 구체적인 보안 위협은 Table 3와 같다[18,21].

3.2.1 무선신호 교란

IoT 서비스는 대부분 무선네트워크 통신을 통해 이루어진다. 최근 GPS전파나 이동통신망을 비롯한 대부분의 무선 인터페이스를 대상으로 한 전파커트장비들이 등장하고 있으며, 허가 되지 않은, 불법적인 통신 혼란 장비를 사용 시 정상적인 IoT 서비스에 혼란을 야기할 수 있다[18].

3.2.2 단말분실 및 물리적 파괴

오픈된 공간에 설치된 센서 노드에 대한 허가되지 않은 자의 물리적 접근 및 파기, 또는 사용자가 소유한 스마트 폰, 모바일 기기 등 기기의 도난 및 분실로 인해 IoT

서비스가 정지될 수 있다. 또한 기기 분실할 경우 기기내에 저장된 개인정보 유출사고로 이어질 수 있다[18].

3.2.3 정보유출

IoT 서비스 환경에서 무선·유선통신 환경에 대량의 정보가 전송된다. 다양한 정보를 관리하고 있는 서버나 DB에 접근하여 스니핑이나 불법도청으로 정보를 유출한다. 예를 들어, 스마트미터의 전력 운용내역, U-Health 원격진료 등의 정보가 전송되는 과정에서 개인의 정보가 암호화되지 않는 평문으로 전송될 경우 프라이버시 침해 등의 2차 피해가 발생된다[2].

3.2.4 데이터의 위조와 변조

해커는 허가되지 않은 기기나 센서 등을 통한 데이터 발송 또는 유·무선 상에서 데이터를 탈취하여 위조 또는 변조한 뒤 허가된 기기 또는 허가된 사용자에게 데이터를 발송 할 수 있다[18]. IoT 기반의 스마트 그리드에서 실제로 데이터 위변조 공격이 일어나고 있다[22].

4. 사물인터넷 위협사례 및 대응전략

4.1 사물인터넷 보안 위협사례

IoT 의 특성상 높은 수준의 보안 솔루션을 도입하기 어렵고, 외부 해킹을 확인하기 어렵기 때문에 다양한 경로의 침투가 가능하여 계속적인 보안 위협사례들이 발생한다[23]

4.1.1 애플리케이션 관련 보안위협사례

2009년 미국의 중앙교통통제 시스템(central traffic control system)을 해킹하여 "전방에 공룡이 있으니 주의하십시오" 라는 메시지로 데이터 위·변조하여 교통 전광판에 표시한 사례가 있다[24,25].

4.1.2 네트워크 관련 보안 위협사례

IoT를 활용한 비닐하우스 제어 시스템은 스마트폰을 이용하여 운영하고 있다. 유럽에서 원격제어로 해킹하여 사료공급, 배수, 습도, 온도, 급수 등 농장시스템을 공격한 시도가 적발되었다[21].

2011년 미국 추수감사절 전날에 노스폴 토이(North Pole Toys)에서는 폐쇄된 망을 통해 제품을 배송하는 시스템에서 USB를 통한 웜으로 인해 배송에 문제가 발생하였다[26]. 또한 2010년 이란 핵발전소에 VirusBlokAda 악성코드가 발견되었는데 이는 폐쇄된 망에서 직원 노트북 및 USB를 통한 악성코드 전파 가능성을 보여 주었다[26].

2014년 SK브로드밴드 및 LG유플러스의 네트워크를 공격하여 일시적인 장애 사고가 발생하였다[23].

4.1.3 단말 관련 보안 위협사례

러시아는 중국에서 수입한 주전자와 다리미에서 초소형 마이크로칩이 내장된 것을 발견하였다. 이런 초소형 마이크로칩은 악성코드 혹은 스팸을 보안적용이 되지 않은 네트워크를 통하여 확산시킬 수 있으며, 도청을 통해 정보수집이나 정보 전송이 가능하다[27].

4.2 사물인터넷 보안의 대응전략

IoT 기반 융합 서비스의 활성화는 보안이 필수적인 요소이다. 보안이 제공되지 않을 경우 경제적 피해 뿐만 아니라 생명까지 위협할 수 있기 때문이다[28]. 정보보호와 프라이버시가 적용된 IoT 제품이나 서비스 설계, 경량화된 암호기술, 시큐어 코딩이나 제품인증 등을 통한 안전한 SW와 HW 개발이 요구된다[28].

IoT를 안전하게 사용하기 위해 사용하는 사용자의 사용시간, 사용위치 등 유저의 사용자의 사용패턴을 수집하고 분석하여 다른 사용정보의 접근이 의심되는 경우에는 Fig. 3 와 같이 서비스를 일시 중단 하는 기법이 필요하다.

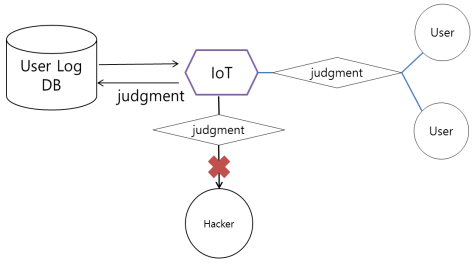

Fig. 3. Information-based services of the Internet of Things

IoT 보안은 디바이스, 앱, 네트워크, 서버를 범위로 하는 융합보안으로 IoT에 대한 위협과 공격은 하드웨어와 소프트웨어뿐만 아니라 서비스 영역을 포함한 전 영역에서 발생할 수 있다. 따라서 IoT 서비스 구조의 최전방에 위치한 사물 기기 대부분이 한정된 전력과 통신자원을

가지고 운영되기 때문에 사물간 통신 및 데이터 암호화, 소프트웨어 위변조 방지, 경량화 된 암호 알고리즘, 환경이 다른 기기와 네트워크에의 접근제어 및 통합관리, 게이트웨이 보안이 선결되어야 한다. 따라서 IoT 보안을 위해서는 웹을 통해 업데이트를 받는 단말기들이 안전한 시스템을 통해 다운받을 수 있도록 2중 인증 시스템(예를 들어 물리적 디바이스와 PIN을 결합한 인증)을 사용하고, IoT와 연결된 디바이스의 위치 데이터 전송 보안을 강화하고, 데이터 전송을 웹을 통해 수행한다면 반드시 암호화 기술을 사용해야하고 더불어 두 사람이 패스워드와 운영시스템을 같이 통제하는 방안을 통해 보안을 강화해야 한다. 그리고 불법 위조된 칩 혹은 디바이스 등이 보안 취약점을 야기할 수 있으므로, 제조업체 공급망에 대한 보안을 강화하여 악성 코드의 침입을 사전에 방지하고, 가급적 공개되지 않는 폐쇄망 사용을 권장하며 웹 어플리케이션 보안을 위해 안전한 웹 인터페이스, 인증, 안전한 네트워크 서비스, 운송 시스템 암호화, 안전한 클라우드 및 모바일 인터페이스, 보안 구성 통제, 안전한 소프트웨어 및 펌웨어와 적절한 물리적 보안 등과 같은 항목들을 표준화한다. 마지막으로 디바이스 보안 관리에 대한 가장 최신 정보는 미국의 국가표준기술연구소(NIST, National Institute of Standards and Technology)와 연방정보처리표준(FIPS, Federal Information Processing Standards) 등과 같은 연방정부 가이던스를 참고하여 그곳에서 제시하는 조치를 기반으로 정보 보호 및 주요 시스템 보안에 필요한 적절한 대책을 마련해야 한다.

5. 결론

휴대가 편리하고 다양한 기기들이 주변 사물들이 유·무선 네트워크로 연결되게 되어 언제 어디서나 사물과 사람의 소통을 원활하여 IoT가 많은 발전과 편의를 제공하고 있다. IoT의 급격한 발전으로 편의성을 보장하지만 IoT의 보안은 취약하다.

개발자들이 Application 개발 과정에서 보안과 관련된 사항 강화와 IoT 사용 시 인증하는 부분에서 전송하는 데이터의 암호사용, 외부의 어떠한 공격에 대한 즉각적인 점검 및 실시간 대응과 같이 전략적으로 보안함으로써 전체적인 보안을 향상시킬 수 있다면, IoT을 사용함에 있어서 보다 안정적이고 편리하게 사용할 수 있을 것이다. 이를 위해서는 IOT가 가지고 있는 3가지 보안주제인 단말, 네트워크, 서비스에 대한 보안 취약점을 지속적으로 파악하여 IoT 보안 위협을 최소화하는 연구가 필요하다.

REFERENCES

[1] M. J. Lee, “A Study on IoT Service for Game Development,” *Journal of digital Convergence*, Vol. 13, No. 2, pp. 291-297, Feb. 2015.

[2] H. N. Chin, S. C. Park and W. T. Choi, “Analysis of Network Security Technology for Internet of Things(IoT),” *Proceedings of the Korean Society For Internet Information Conference*, pp. 353-354, 2014.

[3] B. H. Kim, J. M. Lim and C. S. Park, “Analysis of ZigBee Security Mechanism,” *Journal of Security Engineering*, Vol. 9, No. 5, pp. 417-430, Oct. 2012.

[4] Y. J. Park, “Remote Temperature Control System using a Zigbee Communication,” *Journal of digital Convergence*, Vol. 14, No. 4, pp. 259-265, Aug. 2016.

[5] W. C. Park, M. S Lee, M. H. Yoon, S. D. Kim and S. H. Yang, “ZigBee End-to-End Security For Ubiquitous Home Network,” *IEMEK Journal of embedded systems and applications*, Vol. 2, No. 2, pp. 128-136, Jun. 2007.

[6] S. H. Lee and J. H. Kim, “Design of New Authentication Protocol for Mitigating Weakness in ZigBee Networks,” *Proceedings of the 18th JOINT Conference on Communications & Information*, pp. 90, 2008.

[7] H. Jung and C. W. Park, “Design and Implementation of MQTT Based Real-time HVAC Control Systems,” *Journal of the Korea Institute of Information and Communication Engineering*, Vol. 19, No. 5, pp. 1163-1172, May. 2015.

[8] S. H. Shim and H. B. Kim, “Internet of Things technology and MQTT,” *Journal of the Korea Institute Of Information Security And Cryptology*, Vol. 24, No. 6, pp. 37-47, Dec. 2014.

[9] H. W. Kim, “Security Issues in IoT Services,” *Communications of the Korean Institute of Information Scientists and Engineers*, Vol. 32, No. 6, pp. 37-41, Jun. 2014.

[10] Z. Shelby, K. Hartke and C. Bormann, “The Constrained Application Protocol,” IETF RFC7252, https://tools.ietf.org/html/rfc7252, 2014 6.

[11] IETF, “DTLS In Constrained Environments,” http://datatracker.ietf.org/wg/dice/, IETF RFC7252, 2016. 7.

[12] T. Xu, J. B. Wendt and M. Potkonjak, “Security of IoT systems: Desing Challenges and opportunities,” *Proceedings of 2014 IEEE/ACM International Conference on Computer-Aided Design*, pp. 417 - 423, 2014.

[13] XMPP, “History of XMPP,” http://xmpp.org/about/history.html, 2015. 12.

[14] XMPP, “Who’s XMPP?,” https://ko.wikipedia.org/wiki/XMPP. 2016. 5.

[15] D. K. Pyoun, L. Hao and H. K. Jung, “Android mobile phone information push system based on the XMPP protocol,” *Journal of the Korea Institute of Information and Communication Engineering*, Vol. 17, No. 3, pp. 561-566, Mar. 2013.

[16] S. M. Shin and H. B. KIM, “Sensor Network Security Technology To Analyze The Internet Experience,” *Review of Korea Institute of Information Security and Cryptology*, Vol. 24, No.4, pp. 56-65, Aug. 2014.

[17] W. J. Miller, “Big Data, and the Smart Grid,” XMPP, http://ewh.ieee.org/conf/sege/2013/William-Miller-Talk.pdf, 2013. 8.

[18] D. H. Kim , S. W. Youn and Y. P. Lee, “Security of IoT Service,” *Review of The Korean Institute of Communication Sciences*, Vol. 30, No. 8, pp. 53-59, Jul. 2013.

[19] W. Chang and Y. T. Shin, “A Study on the Network and Security for the Internet of Things,” *Proceedings of Korean Institute of Information Technology*, pp. 19-21, 2015.

[20] B. I. Jang and C. S. Kim, “A Study on the Security Technology for the Internet of Things,” *Journal of Security Engineering*, Vol. 11, No. 5, pp. 429-438, Oct. 2014.

[21] J. Y. Kim and S. M. Hwang, “Outlook and Challenges of Security System for the Activation of IoT,” *Proceedings of 2015 Conference of Korea Information Science Society*, pp. 1037-1039, 2015.

[22] Y. H. Jeon, “Internet of Things based smart grid security features and Issue Analysis,” *Review of The Korean Institute of Communication Sciences*, Vol. 24, No. 5, pp. 59-65. Oct. 2014.

[23] KISA, “Trend of Internet of Things security threats,” http://www.kisa.or.kr/uploadfile/201412/201412301124130506.pdf, 2014. 12.

[24] MoneyToday, “Is this for real? Unruly car and iron sending junk mails,” http://news.mt.co.kr/newsPrint.html?no=2014060909314198230, 2014. 6.

[25] Y. S. Ko, K. H. Park and C. S. Kim, “Problem Analysis and Countermeasures Research through Security Threat Cases of Physical Security Control Systems,” *Journal of Korea Multimedia Society*, Vol. 19, No. 1, pp. 51-59, Jan. 2016.

[26] Y. S. Kim, “Internet of Things era of cyber-physical systems Security Technology Trends,” *The Magazine of the IEEK*, Vol. 42, No. 8, pp. 16-25, Aug. 2015.

[27] DataNet, “The more convenient, the more security threats,” http://www.datanet.co.kr/news/articleView.html?idxno=69944, 2013.12.

[28] N. H. Kang, “Security Requirement of IoT convergence service,” *Review of The Korean Institute of Communication Sciences*, Vol. 32, No.12 pp. 45-50, Nov. 2015.

저 자 소 개

문 형 진(Hyung-Jin Mun) [정회원]

- 2008년 2월 : 충북대학교 전자계산학(이학박사)
- 2008년 3월 ~ 현재 : 백석대학교 강사

<관심분야> : 프라이버시 보호, 네트워크 및 웹보안

최 광 훈(Gwang-Houn Choi) [학생회원]

- 2012년 2월 : 구로고등학교 졸업
- 2012년 3월~현재 : 백석대학교 정보통신학부 정보보호학 재학

<관심분야> : 정보보호, 컴퓨터언어

황 윤 철(Yooncheol Hwang) [정회원]

- 2008년 2월 : 충북대학교 전자계산학(이학박사)
- 2000년 3월 ~ 현재 : 한국교통대학교(경기도 의왕) 외래교수

<관심분야> : 네트워크 및 웹보안, 침입방지시스템