IoT 서비스를 위한 보안

김동희, 윤석웅, 이용필
한국인터넷진흥원

요 약

정보통신기술의 비약적인 발달은 오늘날 우리 주변의 사물들을 네트워크로 연결시켜주고 이들에 대한 정보를 언제, 어디서나 쉽게 접할 수 있는 사물인터넷(IoT) 시대의 도래를 촉진하고 있다. IoT 서비스는 스마트기기, 센서 등 다양한 단말 및 이기종 네트워크, 애플리케이션 등을 활용하기 때문에, 그만큼 발생할 수 있는 보안위협도 많을 것으로 예상된다. 본 고에서는 IoT의 주요 구성 및 기술요소들을 설명하고, 여기서 발생 가능한 보안위협들을 살펴본다. 아울러 IoT 환경에서 기본적으로 갖추어야 할 보안 요구사항들을 소개한다.

Ⅰ. 서 론

1991년 미국의 마크 와이저(Mark Weiser)는 사용자가 네트워크 또는 컴퓨터를 의식하지 않고 장소에 구애받지 않으며 자유롭게 네트워크에 접속할 수 있는 유비쿼터스 환경이 도래할 것이라고 주장하였다[1]. 오늘날 정보통신기술의 발달은 우리 주변 다양한 사물들의 지능화, 네트워크화를 촉진하고 있으며, 이들 간의 자유로운 통신 및 정보교환을 가능하게 하는 유비쿼터스 환경은 더 이상 먼 얘기가 아닌 현실이 되어가고 있다.

유비쿼터스 환경의 도래를 더욱 가속화시키는 ICT분야의 개념으로 사물지능통신(M2M) 또는 사물인터넷(IoT)이 새롭게 떠오르고 있다. 미국의 시장조사기관 가트너(Gartner)는 향후 10년간 유망할 것으로 예상하는 미래 IT분야로 IoT를 선정한 바

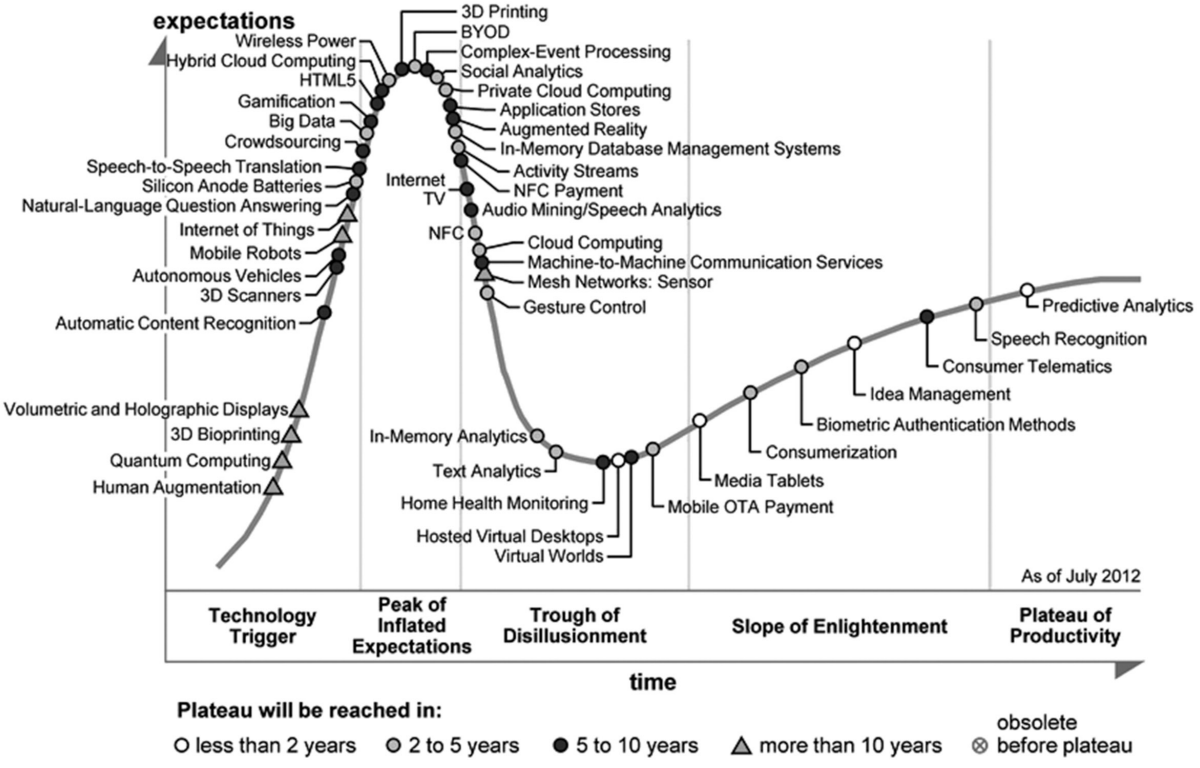

그림 1. 가트너의 미래기술 전망

있으며[2], 세계 이동통신 사업자 협회(GSMA)는 2020년까지 240억 개 이상의 기기들이 상호 연결되어, 통신사업자들이 1.2조 달러 규모의 신규 수익을 창출할 것으로 전망했다[3].

한국 IDC는 전세계 1,000억 개 이상의 센서와 태그 및 115억 대가 넘는 제품들이 네트워크를 통해 연계될 것으로 전망하였으며[4][5], ABI Research는 IoT 서비스와 관련된 단말의 출하량이 2015년까지 약 1억 150만대에 이를 것으로 전망하였다[4].

이렇게 IoT와 관련한 시장전망이 밝은 가운데, 우리나라에서는, 2009년 방송통신위원회에서 사물통신 기반조성 및 서비스 활성화를 위한 '사물통신 기반구축 기본계획(안)'을 마련한 바 있으며[6], 2013년 미래창조과학부를 중심으로 인터넷 신산업 육성을 위한 주요 추진과제로 IoT 서비스 확산을 위한 사물인터넷 기반의 신규 서비스 발굴 및 R&D 지원, IoT 시험환경 인프라 구축 확대 등을 추진 중이다[7]. 이외에도 정부 유관기관 및 학계, 민간분야에서 다양한 연구들이 수행되고 있다.

이처럼 IoT는 사람, 사물 간 자유로운 통신을 가능하게 해준다는 측면에서 새로운 서비스 및 시장창출을 견인할 것으로 기대된다. 하지만 IoT 플랫폼의 개방화, 다양한 이기종 단말/센서 및 유무선 네트워크 간의 연동 등으로 인한 새로운 보안취약점들이 등장할 것으로 예상된다. 따라서 IoT 서비스의 활성화를 위해서는 동 환경에서 발생할 수 있는 다양한 보안문제들이 해결되어야 할 것이다.

본 논문에서는 IoT 환경의 각 구성요소에서 발생할 수 있는 다양한 보안위협들을 정의하고, 이에 대한 보안대책을 제시한다. 논문의 구성은 다음과 같다. 2장에서는 IoT의 개념 및 구성요소에 대해 살펴보고, 3장에서 IoT 환경에서 나타날 수 있는 보안위협들을 도출한다. 4장에서는 IoT 서비스에서 요구하는 보안 요구사항들을 살펴보고 5장에서 결론을 맺는다.

Ⅱ. IoT의 개념 및 구성

1. 사물인터넷(IoT)의 개념

사물인터넷(Internet of Things, IoT)의 개념은 학계, 산업계 등에서 다양하게 정의되고 있다.

ITU(2005)는 ITU-T World Summit on the Information Society의 "ITU Internet Reports"를 통해 사물인터넷의 개념을 처음 제시하였다. 기존의 정보통신기술이 사람과 사물 간에 언제(Anytime), 어디서나(Anyplace) 정보를 주고 받을 수 있게 해주었다면, IoT는 〈그림 2〉와 같이 무엇(Anything)이라는 새로운 개념을 추가함으로써 사람-사물, 사람-사람, 사물-사물 간의 연결 및 통신을 가능하게 해주는 기술이라고 정의하고 있다[8][9]. 여기서 Anything이란, 물리적 공간의 특정 사물뿐 아니라, 가상 공간에서 식별 및 저장되어있는 정보도 포함한다.

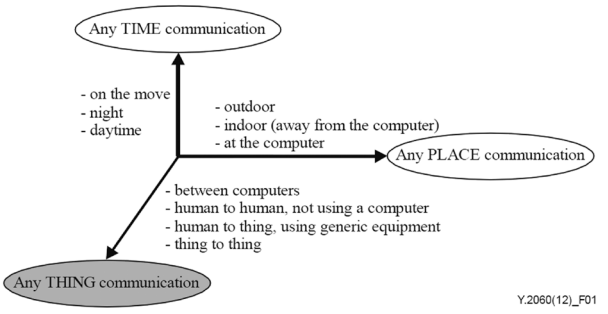

그림 2. IoT의 개념

EU(2008)[10]는 IoT를 고유의 식별자 및 가상의 인격을 가지고 지능화된 인터페이스를 통해 주변 환경요소들과 연결 및 통신할 수 있는 모든 사물이라고 명시하고 있다.

우리나라의 경우, 방송통신위원회(2009)(현 미래창조과학부)에서 IoT는 사물지능통신(M2M)과 유사한 개념으로 '사람 대 사물, 사물 대 사물 간 지능통신 서비스를 언제 어디서나 안전하고 편리하게 실시간으로 이용할 수 있는 미래 방송통신 융합 ICT 인프라'라고 정의하고 있다[6].

이처럼 국내 · 외에서 발표한 IoT의 다양한 정의들을 종합해 보면, IoT는 '사물의 지능화, 네트워크화를 통해 사람과 사물, 사물과 사물 간의 자유로운 데이터 통신 및 정보교환이 가능한 유 · 무형의 ICT 플랫폼'이라고 정의할 수 있을 것이다.

2. IoT 구성 요소

IoT의 개념을 통해 살펴보았듯이, IoT는 사람, 사물, 서비스를 상호 연결 및 소통시켜주는 역할을 수행한다. 〈그림 3〉은 ITU-T

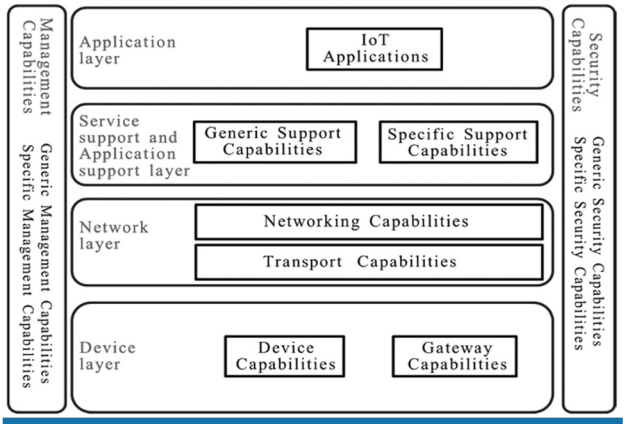

그림 3. ITU-T의 IoT 참조모델

에서 제시하고 있는 IoT 참조모델[9]로, 크게 사람이 소유하거나 우리 주변의 사물들에 부착된 단말/센서, 이들 간 통신이 가능하도록 하는 유 · 무선 네트워크, 전송된 정보의 처리, 분석 및 표현을 가능하게 해주는 애플리케이션으로 구분하고 있다.

2.1 단말

IoT 환경에서 단말은 특정 사물에 부착되어 해당 사물로부터 데이터를 추출하여 네트워크를 통해 타 단말 또는 이들을 관리하는 게이트웨이(Gateway)로 전송하는 역할을 수행한다. RFID, 센서노드, 스마트 기기 등이 해당되며, 게이트웨이는 다양한 이종 네트워크 프로토콜을 사용하여 송 · 수신되는 데이터를 처리할 수 있다.

2.2 유 · 무선 네트워크

사람, 단말 간 전송 데이터와 기기 인증정보, IoT 연결정보 등을 송수신하는 유 · 무선 통로의 역할을 수행한다. 3GPP, ETSI 등 표준에 기반한 네트워크를 사용하며, 기존 TCP/IP 기반의 유선망 뿐 아니라, ZigBee, Bluetooth, Wi-Fi, 2G/3G, LTE 등과 같은 무선통신도 지원한다.

2.3 애플리케이션

IoT 기술을 이용한 다양한 서비스를 제공하기 위한 애플리케이션들이 해당된다. 애플리케이션은 단말, 유무선 네트워크를 구성하는 장비 등에 탑재된 운영체제, 미들웨어 뿐 아니라 End User 단의 IoT 관리, 통제 프로그램 등도 포함한다.

IoT 단말은 비용, 크기 등으로 인해 가용 자원이 제한되어있기 때문에 기존의 웹 서비스와의 연동을 위한 TCP-HTTP 프로토콜 적용이 어렵다. 따라서 IoT 미들웨어는 경량화된 웹 아키텍처 REST(Representational state transfer) 기반의 CoAP(Constrained Application Protocol)를 지원한다[11]. CoAP는 UDP 기반으로 동작하며 신뢰성 문제를 CoAP 내부에서 해결하는 구조를 가지고 있다.

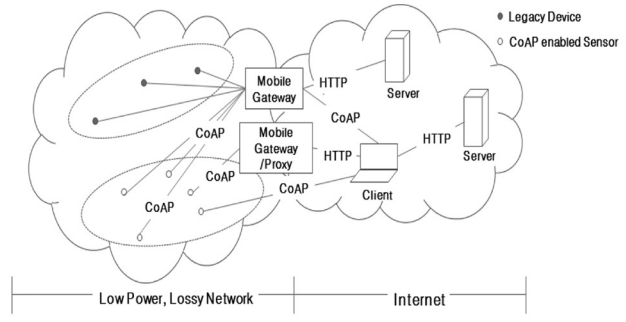

그림 4. CoAP 프로토콜

3. IoT 활용 분야

IoT는 교통, 홈/가전, 유통, 헬스케어 등 다양한 분야에서 활용되고 있다. EU FP7 프로젝트를 수행 중인 연구기관IERC는 IoT의 활용분야를 〈표 1〉과 같이 분류하고 있다[12].

표 1. IoT의 활용분야

구 분	세부 분야
도시	주차, 지능형 교통망, 가로등, 쓰레기 관리 등
환경	산불 예방, 대기/토지 오염 측정, 지진 감지 등
수질	수질 관리, 누수 탐지, 홍수 예방 등
에너지	수력/화력/태양열 발전설비 모니터링 등
보안/안전	물리적 접근통제, 방사능 오염도 및 유해가스 등 측정
물류/유통	물류/유통망 관리, NFC결제, 지능형 쇼핑 등
산업	실내공기 관리, 온도 모니터링, 실내측위 등
농경	골프코스 관리, 농작물 온 · 습도 관리, 기후변화 감지 등
축산	가축 건강 및 위치관리, 유해가스 측정 등
홈/가전	가정용 에너지/물 사용량 측정, 원격관리, 침입감지 등
건강	백신/의약품 관리, 자외선 측정, 운동량 측정, 독거노인 건강관리 등

Ⅲ. IoT 보안위협

IoT는 다양한 기술요소들의 집합체이다. 최근에는 IoT 플랫폼의 개방화를 통한 이기종 단말, 네트워크, 애플리케이션 간 연동이 가속화될 것으로 예상되는 가운데, 이로 인한 기술적, 관리적 측면의 다양한 보안위협들이 발생할 것으로 예상된다.

IoT 환경에서 발생할 수 있는 보안위협들은 기존의 정보통신 환경에서 나타날 수 있는 위협들을 상속한다. 흔히 정보보안의 3대 요소라고 할 수 있는 CIA, 즉 기밀성(Confidentiality), 무결성(Integrity), 가용성(Availability)을 침해함으로써 정상적인 서비스의 이용 및 제공을 방해하는 보안위협들이 나타날 수 있다. IoT의 각 구성요소에서 발생할 수 있는 보안위협들을 살펴보면 아래의 〈표 2〉와 같다.

표 2. IoT 구성요소별 보안위협

구 분	보안위협
단말	분실/도난, 물리적 파괴
네트워크	무선신호 교란, 정보유출, 데이터 위변조, 서비스거부
애플리케이션	정보유출, 데이터 위변조, 서비스거부

1. 단말 분실 및 물리적 파괴

IoT 서비스를 위해 개방된 장소에 설치된 센서노드에 대한 비

인가자의 물리적 접근 및 파손, 또는 사용자가 소유한 스마트폰, 스마트기기 등 단말의 분실 및 도난에 의한 통신기능 상실로 인해 IoT 서비스가 중단될 수 있다. 아울러 단말을 분실할 경우 정보유출 사고로도 이어질 수 있다.

2. 무선신호 교란(jamming)

IoT 서비스는 주로 무선네트워크 통신에 의해 수행된다. 최근 이동통신망, GPS, 전파(RF) 등 다양한 무선 인터페이스를 대상으로 한 전파 차단 장치들이 등장하고 있으며, 인가 받지 않은 불법 무선통신 교란 장비의 설치를 통해 정상적인 IoT 서비스를 방해할 수 있다.

3. 정보유출

IoT 서비스 환경에서의 정보유출은 크게 유·무선통신 구간에서의 스니핑, 불법도청 또는 정보를 저장하고 있는 서버, DB로의 비인가 접근을 통해 이루어질 수 있다. 예를 들어, U-Health원격진료, 스마트미터의 전력 사용내역 등의 전송과정에서 개인의 생체정보, 개인정보 등 중요정보가 암호화되지 않고 평문으로 저장 또는 전송되는 경우, 프라이버시 침해 등의 2차 피해를 야기할 수 있다.

4. 데이터 위·변조

공격자는 인증 받지 않은 단말/센서를 통한 데이터 전송 또는 유·무선 네트워크 상에서 데이터를 중간에 가로채어 위·변조한 뒤 정상적인 기기 또는 사람이 이를 송신한 것으로 위장할 수 있다.

5. 서비스 거부(Denial of Service)

사람 또는 사물에 부착된 단말/센서들은 정상적인 서비스 제공 여부 및 위치 확인 등을 위해 단말/센서 간 또는 이들을 관리하는 게이트웨이를 통해 원격지에서 수시로 연결요청을 수행한다. 공격자는 이를 악용하여 임의로 대량의 연결요청 및 확인 패킷을 지속적으로 전송하고 이를 단말/센서에서 처리하는데 필요한 자원을 소모시킬 수 있다. 또한 이러한 서비스거부 공격은 기기의 전력을 지속적으로 소모하여 서비스가 불가능하도록 유도할 수 있다.

Ⅳ. IoT 보안 요구사항

ITU는 IoT 서비스 참조모델을 통해 기본적으로 요구하는 보안수준을 정의하고 있다. IoT 보안 요구사항은 크게 일반(generic) 보안과 특별(specific) 보안으로 구분하고 있으며, 각각에 대한 주요 내용은 〈표 3〉과 같다[9].

표 3. IoT 보안 요구사항

구 분		보안 요구사항
일반 보안	단말 레이어	권한설정, 인증, 단말 무결성 검증, 접근통제, 데이터 기밀성 및 무결성 보장
	네트워크 레이어	권한설정, 인증, 데이터/신호정보의 기밀성 및 무결성 보장
	애플리케이션 레이어	권한설정, 인증, 데이터 기밀성, 무결성, 프라이버시 보장, 보안감사 수행, 안티바이러스 설치
특별 보안	모바일 결제 등 특수한 상황에 요구되는 보안 요구사항	

1. 단말/센서 보안

1.1 단말/센서 기기 인증

IoT 환경에서 타 기기와 통신이 이루어질 때, 올바른 기기에서 전송된 데이터인지 식별 및 인증할 수 있어야 한다. 기기 간 인증절차는 기기 내에 탑재된 미들웨어 자체에서 수행하거나, 미들웨어가 없는 경우에는 별도의 단말 게이트웨이를 통해 이루어질 수 있다[13]. 기기 인증방식으로는 ID/PW, 인증서, SIM 등이 이용된다.

ID/PW 방식의 경우, 가장 기본적인 인증 방식으로 관리자와 기기 간 ID/PW 인증을 위한 별도의 애플리케이션 및 프로토콜이 요구되며, 계정정보는 사전에 공유되어있어야 한다.

인증서 방식의 경우, PKI 기반의 기기인증서가 널리 이용되고 있다. 단말 인증을 위한 전자서명 생성 및 검증 알고리즘으로 RSA(2,048비트), 해쉬함수 SHA-2(256비트) 이상을 사용하는 것이 안전하다.

SIM 방식은 단말에 탑재된 USIM 또는 UICC 등을 활용한 인

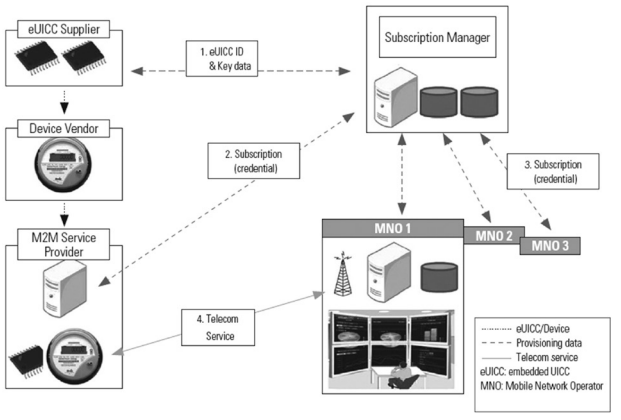

그림 5. Embedded SIM기반 기기인증 체계[14]

증기법으로, 최근 이동통신망을 통한 기기 간 통신이 가능해지면서 국내·외에서 활발한 연구가 진행되고 있다. 2011년부터 GSMA에서 Embedded SIM Project를 시작하여 ETSI, 3GPP 등에서 표준화 작업을 진행 중이며, 국내에서는 KT, SKT 등 이동통신사에서 참여하여 다양한 시범사업을 진행하고 있다.

1.2 물리적 접근통제

IoT 서비스에 이용되는 단말 및 센서는 원활한 통신을 수행할 수 있도록 외부에 노출되어있는 경우가 많다. 따라서 비인가자가 단말/센서로 접근하여 이를 물리적으로 파괴 또는 훼손시킬 경우 정상적인 서비스가 이루어질 수 없다. 따라서 IoT 서비스를 위한 단말/센서는 물리적인 접근이 불가능하도록 별도의 시건장치, 접근통제가 이루어지는 공간에 설치되어야 한다. 또한 각각의 단말/센서는 상황 인지(Context-Awareness) 기반으로 설계·구축되어야 향후 단말/센서 오동작 시 이를 파악하고 이에 신속하게 대응할 수 있다.

2. 네트워크 보안

앞서 설명한 바와 같이 IoT 환경에서의 네트워크 영역은 저전력, 고속통신을 위한 효율적인 통신을 수행할 수 있는 기술요소들이 활용되고 있다. 각각의 IoT 네트워크 기술요소들에 대한 보안 요구사항들을 살펴보면 다음과 같다.

2.1 RFID/USN

RFID(Radio Frequency IDentifier)는 ISO 18000-7 표준에 기반하여 사물에 부착된 태그를 통해 사물의 정보, 주변 환경정보를 수집, 처리, 저장 가능한 무선 네트워크 기술이다. 산업계에서 설립한 자발적 RFID 규격 단체인 EPCglobal에서 다양한 분야의 RFID 표준, 정보보호 및 프라이버시를 위한 기술 규격을 수립하고 있다.

USN은 이동단말이나 센서와 같은 장비에서 사용되는 CPU, 배터리의 용량이 매우 적기 때문에 사용자 단말을 집중적으로 공격해 보유자원을 급격히 소모시킨다면, 일반 사용자들은 서비스를 받을 수 없다. 또한 USN 무선망의 경우에는 중앙 집중형 보안 기능이 상대적으로 취약한 애드혹 네트워크 구조를 취하고 있으므로 이동형 단말기에 대한 통제가 어려워 사이버 공격에 대한 취약성이 늘어날 것으로 보인다. 센서 네트워크의 특성을 고려한 안전한 USN 플랫폼 설계가 필요하며, 센서 네트워크의 보안통신 및 관리 기술을 포함하여 USN 서비스를 구성함에 네트워크 보안과 데이터 보안을 동시에 고려해야 한다.

2.2 ZigBee

ZigBee는 네트워크 계층과 응용계층에서 동작하는 IEEE 802.15.4 표준 기반의 무선통신기술이다. ZigBee의 단말들은 다른 무선네트워크에서와 달리 적은 전력을 사용하여 센서 간 연동 및 통신이 가능하다는 장점이 있다. 하지만 단말 성능이 경량화된 만큼 보안 측면에서 높은 수준의 암호화 기술의 적용이 어렵다는 단점이 있다.

ZigBee는 낮은 수준의 보안을 위한 SSM(Standard Security Mode)과 높은 보안 수준을 제공하기 위한 HSM(High Security Mode) 방식이 있으며, 각각의 ZigBee 장치는 Open Trust Model 방식으로 동작하기 때문에 장치 자신에 대한 신뢰성을 보장한다. 따라서 각각의 ZigBee 장치 간 통신과정에서의 기밀성과 무결성이 보장된다면 신뢰를 담보할 수 있다[17]. ZigBee Alliance에서 제시한 스펙에 따르면, 각 장치 간 통신과정에 제공되는 기본적인 암호화 알고리즘은 AES-CCMP 방식이 있다. 하지만 모든 통신구간에 대한 암호화가 이루어지는 것은 아니기 때문에, 비암호화 구간에 대한 별도의 보안대책 마련이 요구된다.

2.3 무선랜(Wi-Fi)

무선랜 또는 와이파이(Wi-Fi)는 데이터 링크계층에서 동작하는 IEEE 802.11 표준 기반의 무선통신기술로, 최근 국내에서는 스마트폰, 태블릿PC 등의 보급과 함께 이용자 수가 급속히 증가하였다. 무선랜은 데이터 패킷이 사용자 단말과 AP 간 air interface구간에서 전송되기 때문에 해당 구간에 대한 암호화 통신이 이루어지지 않은 경우, 비인가자의 무선 패킷 스니핑, 정보유출 및 위·변조 등의 공격이 이루어질 수 있어 보안에 취약한 것으로 알려져 있다. 따라서 사용자 단말과 AP 간 무선통신 과정에 대한 적절한 인증 및 암호화가 이루어져야 한다.

IEEE 802.11 표준에서는 기본적으로 사용자 인증 프로토콜로 WEP(Wired Equivalent Privacy)를 명시하고 있으며, 여기서 사용되는 기본 암호화 알고리즘은 RC4이다. 하지만 WEP방식은 104비트의 짧은 키 길이와 RC4 알고리즘 자체의 취약점으로 인해 권고되고 있지 않고 있다. 이에 따라 IEEE 802.11i에서는 WEP의 단점을 보완한 사용자 인증방식으로WPA(Wi-Fi Protected Access)와 WPA2를 제안하였으며, 암호화 알고리즘은 TKIP(Temporal Key Integrity Protocol), AES-CCMP를 사용하도록 권고하고 있다.

2.4 모바일 네트워크(3G/LTE)

3G 이동통신 네트워크는 도입 초기에 음성 중심의 폐쇄된 환

경을 가진 네트워크 구조였으나 단말 환경이 피처폰 중심에서 스마트폰 등 스마트 디바이스 중심으로 바뀜에 따라 네트워크에 대한 접속 개방성을 통해 다양한 보안 위협에 노출되고 있다. 이러한 환경에서 최근에는 모바일 악성코드의 증가로 감염 단말의 악성 · 비정상 트래픽이 3G/4G망으로 유입되고 있고, 이로 인해 개인정보 또는 단말정보 유출, DDoS 공격 등 다수의 보안위협이 발생 가능하다.

그러나 3G/4G망에는 기존 인터넷 환경에서 이용하던 보안장비의 적용이 불가능하므로, 무선채널 형성이나 지속적 채널유지 시도 등 주요 공격에 대해 탐지 및 대응이 어려운 실정이다.

3. 애플리케이션 보안

IoT 서비스에서의 애플리케이션은 저전력의 경량화된 단말/센서에 최적화되어 운용되기 때문에 이에 적합한 보안 메커니즘이 적용되어야 할 것이다. IoT 애플리케이션 영역의 보안요구사항은 다음과 같다.

3.1 보안/인증 관리

IoT 단말 미들웨어는 외부로부터 유입되는 데이터로 인해 단말의 운영체제, 하드웨어 자원 등이 영향 받지 않도록 가상화 기술을 통해 운영체제와 논리적으로 완전한 격리가 이루어져야 한다. 또한 상위 응용 소프트웨어로부터 전달받은 데이터의 유효성 및 정당한 단말/센서로부터 수신한 데이터인지 여부를 식별하고, 통신과정에서의 무결성을 보장할 수 있도록 암호화, 해쉬 등의 매커니즘을 적용해야 한다.

3.2 자원(리소스) 관리

IoT 단말/센서의 자원은 매우 제한적이기 때문에, 공격자의 반복적인 통신연결, 처리 요청 등 서비스거부 공격에 취약하다. 따라서 미들웨어에서 단말/센서에서 발생하는 트랜잭션 및 자원에 대한 효율적인 분배 및 이와 관련된 로그정보 등을 관리서버로 전달할 수 있어야 한다.

Ⅴ. 결 론

스마트기기의 보급과 통신기술의 발전으로, IoT는 다양한 영역에서 널리 활용될 것이며, 이는 유비쿼터스 시대로의 진입을 더욱 가속시킬 것으로 전망된다. 하지만 IoT는 단말/센서, 네트워크, 애플리케이션과 같이 여러 분야의 정보통신기술이 접목된 만큼, 다양한 보안위협들이 나타날 것으로 예상된다.

본 고에서는 IoT 환경을 구성하는 단말/센서, 네트워크, 애플리케이션 영역별 주요 기술요소들을 살펴보았다. 아울러 각 영역별로 발생할 수 있는 보안위협들을 살펴보았다. IoT 서비스는 다양한 분야에서 다양한 기기 및 기술요소들이 활용되기 때문에 모든 보안위협을 사전에 완전히 예방하는 것은 쉽지 않겠지만, 본 논문에서 제시한 보안 요구사항들을 통해 안전한 IoT 환경 조성 및 활성화에 기여할 수 있을 것으로 기대한다.

참 고 문 헌

[1] Mark Weiser, "The Computer for the 21st Century", Scientific American, 1991.

[2] Gartner, "2012 Gartner's Hype Cycle for Emerging Technologies", 2012.8. (http://www.gartner.com/newsroom/id/2124315)

[3] Gigacom, "Internet of things will have 24 billion devices by 2020", 2011.10.13. (http://gigaom.com/2011/10/13/internet-of-things-will-have-24-billion-devices-by-2020/?utm_source=pulsenews&utm_medium=referral&utm_campaign=Feed%3A+OmMalik+%28GigaOM%3A+Tech%29/)

[4] 임용재 외 2, 미래인터넷의 진화방향: Internet of Things, PM Issue Report 2012-제2권 이슈1, 2012.

[5] IDC, Worldwide Smart Connected Device Shipments 2010-2016, 2012.3.28

[6] 사물통신 기반구축 기본계획(안), 방송통신위원회, 2009.

[7] 미래창조과학부 2013년도 업무보고 자료(과학기술과 ICT를 통한 창조경제와 국민행복 실현), 2013.4.18.

[8] "ITU Internet Reports 2005, Internet of Things", ITU, 2005.11.

[9] ITU-T Y.2060, Overview of the Internet of Things, 2012.6.

[10] "Internet of Things in 2020, A Roadmap for the Future", EPoSS, 2008.9.

[11] 박지예 외 1, "안전한 WEB of Things 응용을 위한 개체 인증 기술", 한국통신학회논문지 13-05 Vol.38B No.05, 2013.5.

[12] The Internet of Things 2012 New Horizons, IERC, 2012. (http://www.internet-of-things-research.eu/pdf/IERC_Cluster_Book_2012_WEB.pdf)

[13] M2M 단말 미들웨어 플랫폼, TTA 표준, 2012.12.21
[14] 조수현 외 5, "KT의 사물지능통신 기술 개발 현황", TTA Journal Vol.134, pp. 51-56, 2011.4.
[15] 김호원 외 1, "IoT 기술과 보안", 한국정보보호학회지 제22권 제1호, 2012.2.
[16] 김봉환 외 2, "ZigBee 보안 메커니즘 분석", 보안공학연구논문지 제9권 제5호, 2012.10.
[17] 이상원 외 2, "인증서 기반의 정보통신 기기인증서비스 표준화 추진전략", TTA 제6회 정보통신표준화 우수논문집, 2010.12.
[18] M2M 지능형 사물 플랫폼 동향, 주간기술동향 통권 1455호, 정보통신산업진흥원, 2010.7.21

약 력

김 동 희

2007년 단국대학교 경영정보학과 졸업
2009년 고려대학교 정보보호대학원 석사
2009년~현재 고려대학교 정보보호대학원 박사수료
2009년~현재 한국인터넷진흥원 인터넷침해대응센터 선임연구원
관심분야: 정보보호 정책, 무선네트워크 보안, 위험관리

윤 석 웅

1998년 인하대학교 자동화공학과 졸업
2003년 인하대학교 전자계산공학과 석사
2008년~2010년 인하대학교 정보공학과 박사수료
2006년~현재 한국인터넷진흥원 융합서비스보호팀 책임연구원
관심분야: 정보보호 정책, 신규 IT서비스 보안

이 용 필

1995년 서울대학교 경제학과
2003년 서울대학교 행정대학원 석사
2004년~2008년 서울대학교 행정대학원 박사수료
2003년~현재 한국인터넷진흥원 융합서비스보호팀 팀장
관심분야: 정보보호 정책, 기업 정보보호