차세대 IoT 네트워크 보안 현황

권혁찬·정병호·김정녀 (한국전자통신연구원)

목차

1. 개 요

최근 몇 년 사이에 사물인터넷(IoT)이라는 키워드가 화두가 되고 있다. 시스코는 2020년에 네트워크에 연결된 디바이스 수를 50억 개로 추산하고 있다[1]. 이는 2020년 전 세계의 예상 인구인 76억의 약 6.5배인 수치이다. 가트너에서는 IoT로 창출되는 부가가치가 2020년까지 약 1조 9천억 달러에 이를 것으로 전망하고 있다. 시스코, 구글, 마이크로소프트 등에서는 IoT의 글로벌 경쟁력 확보를 위한 기술 개발에 박차를 가하고 있다.

IoT는 스마트홈, 스마트의료, 스마트카, 스마트에너지, 스마트팩토리 등 인류의 삶과 직결되는 다양한 서비스의 주축이 되는 기술로 관련 산업/서비스의 활성화 및 안전성을 답보하기 위해서 반드시 해결해야 할 문제는 바로 '보안'이다. 사람, 사물, 공간, 데이터 등 모든 것이 연결되는 IoT 환경에서의 보안위협은 경제적 피해뿐만 아니라 생명과 국가기반시설까지 위협할 수 있기 때문이다.

해외의 주요 기업들을 포함하여 국내외 다수의 업체가 IoT 보안기술 확보 경쟁에 뛰어 들고 있다. 대표적으로 시스코는 IoT 사업과 보안역량을 강화하기 위한 전담부서(IoT systems and software group, IoT security group)를 신설하여 운영하고 있다 시스코는 Fog Computing[2], IoE (Internet of Everything)[3] 등의 신 키워드를 발표하고 교통시스템 등에 IoT를 적용하기 위한 구체적인 계획을 수립하는 등 매우 발 빠르게 IoT 시대를 준비하고 있다. 또한 IoT 디바이스 보호를 위한 IoT 보안 플랫폼 등의 기술개발도 매우 활발히 진행하고 있다.

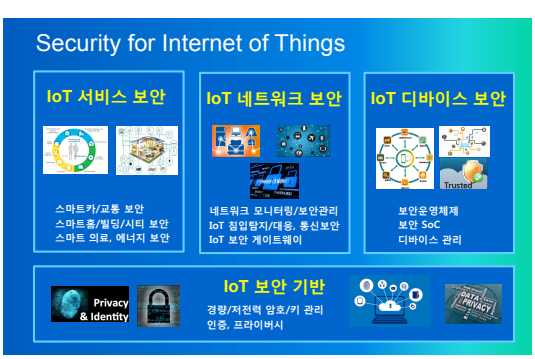
인텔은 보안 전문업체 McAfee를 인수하고 인텔의 IoT 게이트웨이[4]에 보안 솔루션을 탑재하여 일부 제품을 출시하기도 하였다. 버라이존은 클라우드 기반 IoT 디바이스 식별, 인증, 통신데이터 보호를 위한 보안 솔루션을 개발하였으며 GE(General Electric) 역시 보안업체 Wurldtech을

인수하여 정유시설, 전력망, 의료기기 용 보안솔루션 개발을 진행하고 있다[5].

IoT의 보안 영역은 (그림 1)과 같이 크게 디바이스 보안, 네트워크 보안, 서비스 보안 및 보안 기반기술로 분류할 수 있다. 디바이스 보안은 초경량/저전력 센서에서 게이트웨이 및 고성능 디바이스에 이르기까지 다양한 자원/성능을 갖는 디바이스에 특화된 보안 기술로 보안 운영체제, 보안 SoC, 디바이스 보안 플랫폼 등을 포함한다.

네트워크 보안은 하드웨어 자원, 통신방식, 보안구조가 상이한 네트워크간 연결/연동되는 환경에서 다양한 공격에 대응하며 종단간 통신 신뢰성을 제공하기 위한 기술이다. 서비스 보안 기술은 스마트홈, 스마트의료, 스마트카/교통, 스마트에너지 등 다양한 IoT 응용서비스의 보안요구사항을 충족시키기 위한 특화된 보안 기술이다. 그 외에 IoT 환경에 적용 가능한 경량 암호, 인증 플랫폼, 프라이버시 보호 등의 기반 기술도 있다.

본 기고문에서는 이 중 IoT 네트워크에 대한 보안 현황을 소개하고자 한다. 2장에서는 IoT 네트워크 현황을 소개하고 3장에서는 IoT 네트워크 보안 현황 및 전망을 분석하고 4장에서 결론을 맺는다.



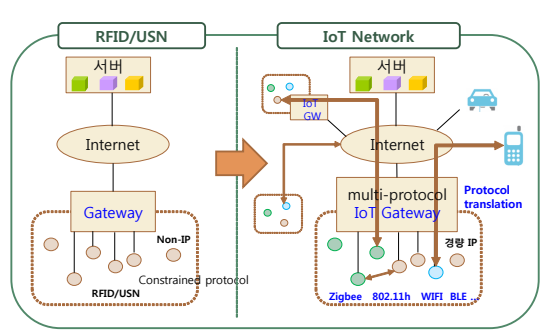
(그림 1) IoT 보안 기술 분류

2. IoT 네트워크 현황

2.1 특성

IoT 네트워크의 특성은 '초연결성'이라는 키워드로 요약할 수 있다. IoT 에서의 초연결성이란 하드웨어 자원, 통신방식, 보안구조가 상이한 네트워크 간 연결 및 연동되는 구조를 의미한다[5].

(그림 2)는 기존의 RFID/USN 네트워크와 IoT 네트워크의 구조를 비교하였다. 기존의 일반적인 RFID/USN 네트워크는 IP가 없는 센서들이 센싱한 정보를 게이트웨이가 수집하여 서버로 전달하는 구조를 갖는다. 센서 간 또는 센서와 게이트웨이 간의 통신은 ZigBee등 제한된 프로토콜을 사용한다. 반면 IoT 환경에서의 네트워크는 초경량 센서부터 스마트폰까지 다양한 성능을 가진 단말들이 ZigBee, 802.11h, Wi-Fi, BLE(Bluetooth low energy) 등 다양한 네트워크 프로토콜을 사용하여 연결하고 연동하는 특징을 갖는다. IoT 디바이스들이 IP 주소를 보유하는 것도 하나의 특징이다. 물론 non-IP 디바이스도 존재한다. IoT 보안 게이트웨이의 기능 확장도 하나의 특징이다. 네트워크 프로토콜 변환, 키관리/권한제어, 터널링, 그룹관리 등의 다양한 기능이 서버 단에서 IoT 게이트웨이 단으로 내려오고 있는 추세이다.



(그림 2) IoT 네트워크 특성

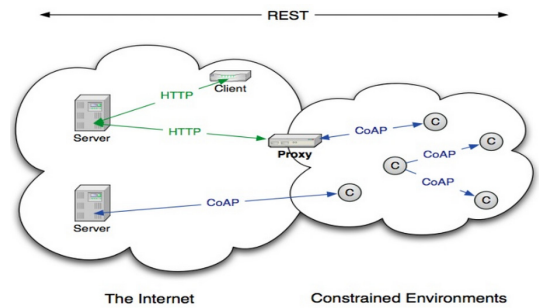
2.2 현황

<표 1> 에서는 일부 IoT 응용서비스에서 사용되는 저전력 사물 네트워크의 현황을 보여준다.

IoT에 사용되는 통신 프로토콜로는 Wi-Fi, Ethernet, Bluetooth, ZigBee, PLC, 3G/4G, IPv6 등 다양하며, 이는 기존에 존재하던 프로토콜들이다. IoT를 위한 신규 통신/네트워크 프로토콜로는 CoAP, MQTT, LwM2M(Light weight M2M) 등이 있다.

CoAP(Constrained application protocol)[6][7]은 IETF CoRE 워킹그룹에서 개발된 표준으로 응용계층에서 자원이 제약된 IoT 디바이스간 통신을 위한 경량의 통신 프로토콜이다. 4바이트의 압축 헤더를 가지며 UDP, SMS, TCP를 지원한다.

CoAP는 임베디드 웹 전송 프로토콜이며



(그림 3) CoAP의 구조

'coap://대한민국/주소/2층작은방/3번전구'와 같은 형태로 IoT 기기를 지정할 수 있다. (그림 3)은 CoAP의 기본 통신 구조를 보여준다.

MQTT(Message queueing telemetry transport)[8]는 TCP 상위에서 동작하는 프로토콜로 경량의 publish/subscribe 메시징 모델이다. MQTT 역시

〈표 1〉 IoT 네트워크 현황

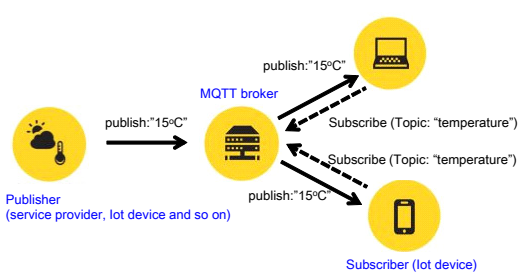
응용	사물네트워크	전력	대역폭(Hz)	기기수	속도(bps)	거리(m)
무선M2M/백홀/스마트그리드	802.11ah Wi-Fi	저전력	900M	8,100	200	1K
	Wi-Fi	고전력	2.4/5G	수십	G급	수십
핼쓰, 착용형 기기, 무선센서	블루투스	저전력	2.4G	8	700K	〈30
	BTLE	초저전력			1M	5-10
	Zigbee(메쉬)	초저전력		250	250K	〈300
스마트조명	Z-wave(메쉬)	초저전력	908M	232	40K	〈30
	DALI(버스)	저전력	-	64	1.2k	300-600
스마트에너지	wireless Mbus	저전력	433/868M	250	2.4K	300-1K
	EnOcean(메쉬)	초저전력	315/868M	1000	125K	〈300
	DASH7	초저전력	433	8	200K	〈2K
	PRIME	저전력(2W)	-	65,535	40-125K	〈1K
산업제어 (빌딩,공장 제어)	Wireless HART	초저전력	2.4G	〈30,000	250K	〈200
	ISA100.11a(메쉬)	초저전력	2.4G	무제한	250K	〈200
	HPGP(메쉬)	중전력(4W)	-	1,155	4M	〈100
	BACNet(이더넷)	고전력	-	Many	1-100M	10-150
	LONWorks	중전력	-	32,000	3.6-5.4K	〈130
	EtherCAT	고전력	-	65,535	100M	〈100
	PROFINET	중전력	-	Many	10M	〈100
	PROFIBUS	저전력	-	127	12M	〈1.2K
	CANOpen	저전력	-	〈2,000	1M	50

자원이 제약된 디바이스를 위한 프로토콜이며 토픽이라는 개념을 특징으로 한다. MQTT 동작을 위해서는 브로커가 필요하며 현재 Mosquitto, HiveMQ, TabbitMQ, ActiveMQ 등 다양한 open source MQTT 브로커가 존재한다[9]. 디바이스는 전달받기를 원하는 정보를 MQTT 브로커에게 등록하며 MQTT 브로커는 해당 정보를 주기적으로 등록한 디바이스로 push하는 방식으로 동작한다. MQTT는 Facebook massenger를 비롯하여 스마트홈, 파이프라인 모니터링 등의 응용에 사용되고 있으며 향후 다양한 IoT 서비스를 위한 통신 기술의 일부로 활용이 될 것으로 예상된다.

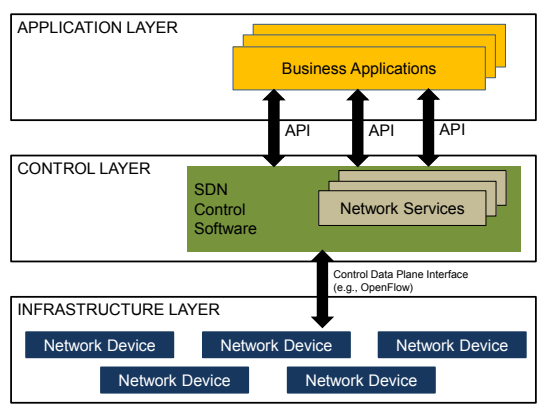
IoT 환경으로 진화하면서 폭증 트래픽 대응 및 다양한 서비스/응용에 따른 동적 네트워크 구성 등에 대한 요구가 증가함에 따라 소프트웨어 기반의 네트워킹 기술인 SDN(Softeare defined network)과 NFV(Network functions virtualization)에 대한 관심도 증가하고 있다. SDN은 기존 하드웨어 장비의 제어기능을 소프트웨어로 전환해 통합된 하드웨어 제어 시스템을 구축하는 기술이다[10].

SDN의 제어기능을 담당하는 SDN 컨트롤러는 빅스위치(BigSwitch), NEC, HP 등에서 출시하고 있으며 국외에서 Cisco, Juniper networks, 국내에서 Atto research, Kul cloud 등에서 개발을 진행하고 있다. 인텔, 파이오링크 등에서 SDN 스위치 장비를 출시하고 있으며 일부 제품에서는 기존 스위치 장비에 SDN을 위한 소프트웨어 에이전트를 탑재하여 활용하기도 한다. SDN의 표준은 ONF[11]에서 컨트롤러와 스위치 간의 통신을 위한 오픈플로우(openflow) 기술을 표준화하고 있으며 IEEE, ITU-T, OpenDaylight 등에서도 관련 표준화가 진행되고 있다.

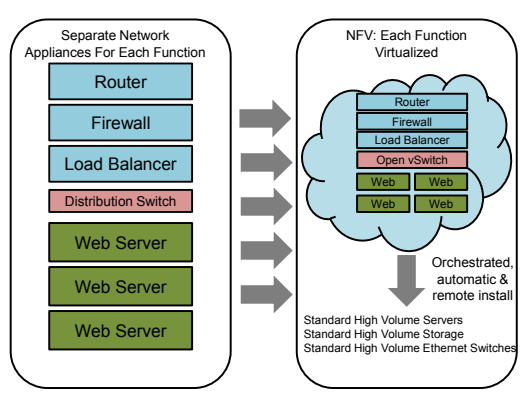
NFV는 네트워크 장비내의 여러 기능들을 분리시켜 소프트웨어적으로 제어 및 관리가 가능하도록 가상화 시키는 기술이다[12]. NFV에서 가상화하는 네트워크 기능은 라우팅 기능, 모바일 네트워크 노드 기능, VPN, DPI, QoS 모니터링, AAA, 정책 서버, 방화벽, 스팸 방지, 홈 라우터 셋탑박스 등 매우 다양한 기능을 포함한다. NFV의 표준화는 ETSI의 ISG에서 진행되고 있으며



(그림 4) MQTT publish/subscribe 모델



(그림 5) SDN 구조



(그림 6) NFV 구조

28개의 service provider를 포함하여 150개의 업체가 참여하고 있다. (그림 5)와 (그림 6)은 각각 SDN과 NFV의 구조를 보여준다.

3. IoT 네트워크 보안 현황

미국의 보안서비스업체 프루트포인트의 발표에 의하면 2013년말부터 2014년초까지 전 세계에서 75만건의 '피싱', '스팸'과 같은 악성메일이 가정에 설치된 라우터, TV, 냉장고 등을 통해 발송되었다고 한다. 2014년 BlackHat Asia에서는 차량의 제어네트워크에 침투하여 차를 마음대로 제어할 수 있는 20달러 회로 기판이 소개되기도 하였다. 2013년 11월에는 가정용 라우터, 셋톱박스, 감시카메라, 산업통제시스템 등의 다양한 디바이스를 감염시키는 새로운 형태의 리눅스 웜이 발견되기도 하였다. 이처럼 현재에도 IoT와 관련한 공격사례가 속속 보고되고 있으며 향후 그 위협은 더욱 증대될 것으로 예측된다.

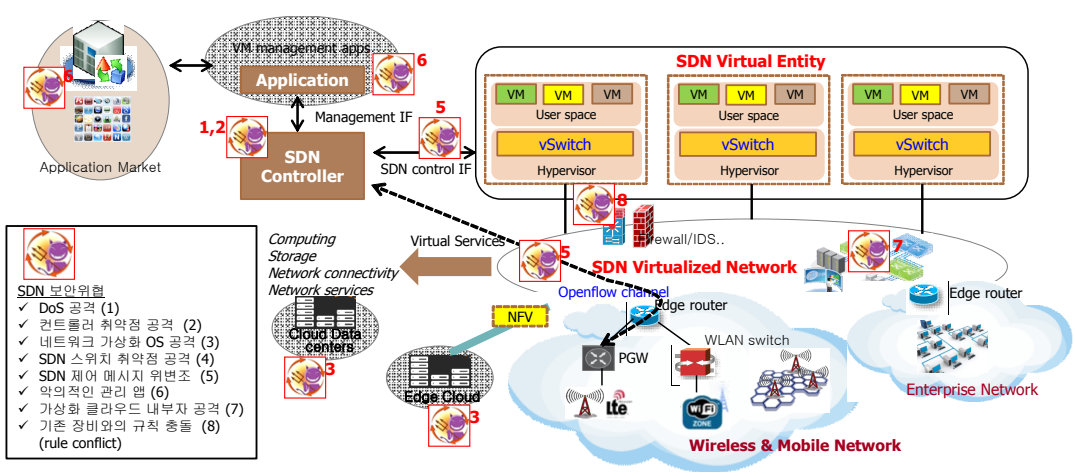
3.1 보안 취약성/위협

IoT 네트워크에서의 주요 보안 취약성/위협은 다음과 같다.

- 저사양 디바이스에 보안 적용의 어려움 및 이에 따른 보안위협이 네트워크로 전이
- 이기종 사물 네트워크간 연동·통신 과정에서 일정한 보안수준 유지의 어려움 및 보안정보가 변조되거나 유출
- IoT 디바이스, 네트워크 및 게이트웨이 해킹 및 크로스 네트워크 디바이스로 피해 확산
- 불법복제/위장기기를 통한 공격
- 악성코드에 감염된 IoT 디바이스들로 구성된 대단위 사물봇에 의한 트래픽 폭증 공격
- 방대한 IoT 디바이스에 대한 보안관리(보안패치, 모니터링 등) 취약점 증가

차세대 네트워크로 등장하고 있는 소프트웨어 정의 네트워크인 SDN, NFV 에서의 주요 보안 취약성/위협은 다음과 같다.

- SDN 컨트롤러 및 SDN 스위치의 취약점 분석을 통한 공격
- SDN 컨트롤러 공격을 통한 Single-point-of-failure 문제
- SDN 제어 메시지 위변조



(그림 7) SDN/NFV 보안위협

- 기존 장비와의 규칙 충돌 문제(rule conflict)
- 가상화 클라우드의 취약점 및 내부자 공격
- NFV로 구성된 네트워크에서 토폴로지 검증의 어려움
- NFV 이미지 위변조

현재, ETSI에서는 취약성과 위협에 대해 추가적으로 NFV 상에서 토폴로지 검증, secure boot, secure crash, 가상화된 test function을 통한 백-도어 문제 등에 대한 논의가 진행되고 있다[13]. (그림 7)은 SDN과 NFV 환경에서의 보안위협을 보여준다.

3.2 IoT 네트워크 보안 기술 개발 현황

본 절에서는 IoT 보안기술에 대한 산업계의 동향을 소개한다. 본 고에서는 IoT 보안 기술을 초연결보안, 보안관리, 침입탐지/대응, SDN/NFV 보안으로 분류하여 개발 현황을 기술한다. <표 2>에서는 주요 IoT 네트워크 보안 기술개발 현황을 분류별로 정리하였다.

초연결 보안 분야는 현재, IoT 보안 게이트웨이 기술에 대한 수요도 높으며 가장 활발히 개발되고 있다. CoAP, LwM2M 통신을 보호하는 DTLS(Datagram TLS)[14] 기술도 표준과 함께 기술개발이 진행되고 있다. 현재까지 IoT 게이트웨이의 보안 기능은 VPN이나 인증 정도로 제한되어 있는 상황이며 향후 다양한 디바이스, 통신방식 및 보안구조를 지원하며 디바이스의 보안관리 기능까지 제공하는 형태로 확장될 것으로 예상되며 스마트카, 스마트의료 등 서비스에 특화된 다양한 IoT 보안 게이트웨이가 개발/출시될 것으로 예상된다.

보안관리기술은 현재 자원제약없는 무선/모바

〈표 2〉 IoT 네트워크 보안기술 개발 현황

분류	국내	국외
초연결 보안	한국부품연구원에서 IoT 연결성을 지원하는 IoT 게이트웨이 및 디바이스 플랫폼 개발 – SSL 기반 암호화/인증 기술 적용 암호/인증이 포함된 상용 zigbee 센서용 프로토콜 개발 (레이디오펄스, KETI 등) DTLS개발 사례(ETRI) 및 PKI, IEEE1609.2 기반 차량통신 보안 기술 구현 사례 있음(펜타시큐리티)	퀄컴에서 개발한 IoT 연결성 플랫폼(AllJoyn)에 앱단위의 인증/암호 기능 제공 인텔, 어드밴텍, 유로텍, 프리스케일 등에서 다수의 IoT 게이트웨이가 출시 키분배/암호/인증이 포함된 zigbee(Atmel, TI, EM 등) 및 BLE(CSR, connectBlue, TI 등) 칩/솔루션 개발 취리히 대학은 X.509, TPM, DTLS를 이용하여 IoT 기기와 서버간 경량/저전력 상호인증 및 단대단 보안 기술 개발
보안관리	현재 상용제품들은 자원제약이 없는 무선/모바일 기기 보안관리 중심 (예: MDM 기술) SKT와 KETI에서 OneM2M의 기기관리 프로토콜 개발 중	표준화 중심. IPSO, OneM2M 등에서 IoT 디바이스 제어 및 보안관리 표준규격 개발 중 OneM2M은 M2M 디바이스, 게이트웨이, 서버로 구성된 네트워크 환경에서 인증, 암호통신, 원격신뢰관리, 키관리 등의 보안규격 개발 중
침입탐지/대응	WLAN 환경에서의 무선침입/해킹탐지 기술 중심 (ETRI, 삼성전자, 코닉글로리, 유넷시스템 등) 무선센서네트워크에서 센서에 탑재된 코드의 무결성 원격 검증 기법 연구 사례 (인하대학교)	WLAN 환경에서 무선침입/해킹탐지 기술 보유(AirTight, AirDefense, Cisco 등) 무선센서네트워크에서 센서탑재코드의 원격검증을 통한 이상 센서 탐기기법 연구 사례(미시건대, 카네기멜론대)
SDN/NFV 보안	기반기술은 일부보유 – SDN 콘크롤러(아토리서치, 나임네트워크, ETRI), SDN 스위치(파이오링크), NFV기반 LTE 코어(SKT/삼성전자) 등 보안 기술은 KAIST, 성균관대 등에서 연구 진행 중	주니퍼, 버라이존, HP, Checkpoint, vArmour, Radware 등에서 SDN/NFV 보안 기술개발 활발히 진행 중 주니퍼–IPv5, SDN, NFV, 클라우드 기반 보안 솔루션 개발 중. Checkpoint–Softeare defined protection 기술 개발, vArmour–Bigweitch 기반 보안 기술 개발

일 기기 중심이며 IoT 기기보안관리는 표준화 중심으로 보안 규격이 개발되고 있는 상황으로 아직까지는 관련 기술개발이 미진한 상황이다. 특히 경량/저전력 IoT 디바이스들을 모니터링하고 원격에서 보안패치/업그레이드를 지원하기 위한 기술에 대한 연구도 필요한 상황이다.

침입탐지/대응기술은 현재는 무선랜(WLAN) 환경에서의 기술이 주류를 이루고 있다. IoT 환경에서는 다양한 센서들이 포획되어 임의 조작이 가능하며 이에 대응하기 위해 WSN에서 원격으로 센서 내장 코드의 무결성을 검증하는 기법연구도 학계를 중심으로 연구된 사례가 있다[15]. 다양한 네트워크 포인트에서 봇넷 및 봇넷을 통한 폭증트래픽에 대응하기 위한 기술개발에 대한 요구도 점차 증가하고 있는 추세이다.

SDN/NFV 기반기술은 국내에서도 보유하여 일부 서비스에도 적용하고 있으나 보안 기술은 학계 중심의 초기단계로 연구가 진행되고 있다. 반면 국외에서는 주니퍼, 버라이존, Checkpoint, HP 등에서 SDN/NFV 연구가 매우 활발히 진행되고 있다.

4. 결 론

본 기고문에서는 IoT 네트워크에 대한 보안 현황을 소개하였다. IoT 시대를 대비하여 다양한 형태의 보안기술이 개발되고 있으며 일부 서비스에도 적용되고 있다. 현재는 주로 IoT 보안 게이트웨이, 경량 통신네트워크 보안, 인증, SDN/NFV 보안에 대한 기술개발이 주류를 이루고 있으며 기존의 WSN에서 적용되던 보안 기술을 확장하여 적용하기도 한다.

IoT를 기반으로 하는 스마트 카, 스마트 의료, 스마트 홈, 스마트 에너지, 스마트 팩토리 등의 서비스의 도입이 가시화되고 있으며 이러한 서비스에 특화된 보안기술 수요도 증가할 것으로 예측된다. 예를 들어 스마트 의료의 경우 디바이스 간 통신을 위한 IEEE11073 규격, 의료시스템 간 통신을 위한 HL7 규격에 특화된 통신 프로토콜 보안이 필요하며 스마트카의 경우 자동차 전용 근거리 무선통신 방식인 IEEE1609에 특화된 보안기술의 적용이 필요할 것이다.

향후에는 IoT의 초연결성 즉 하드웨어 자원, 통신방식, 보안구조가 상이한 네트워크간 연결 및 연동되는 환경 및 클라우드/빅데이터 기반의 분석서비스가 연동되는 환경을 고려한 종합적인 보안기술개발이 필요할 것으로 사료된다. 다양한 형태/기능의 IoT 보안게이트웨이에 대한 수요도 지속적으로 증가할 것으로 예상된다. 특히 현재의 IoT 게이트웨이 보안기술에 네트워크 프로토콜 변환, 키관리/권한제어, 터널링, 디바이스 및 그룹관리 등의 다양한 기능이 추가된 보다 고도화된 IoT 보안 게이트웨이가 등장할 것으로 예상된다.

참 고 문 헌

[1] Dave Evans, "The Internet of Things, How the Next Evolution of the Internet Is Changing Everything", White paper, CISCO, 2011.

[2] Cisco Fog computing, https://techradar.cisco.com/trends/Fog-Computing.

[3] Cisco Internet-of-everything(IoE), http://www.cisco.com/c/r/en/us/internet-of-everything-ioe/index.html.

[4] Intel IoT Gateway Product Brief, http://www.intel.com/content/www/us/en/embedded/design-tools/evaluation-platforms/gateway-solutions/iot-product-brief.html.

[5] “세계최고의 스마트 안심국가 실현을 위한 사물인터넷(IoT) 정보보호 로드맵”, 미래창조과학부,

2014.10.
[6] Z. Shelby,K. Hartke, C. Bormann, “The Constrained Application Protocol (CoAP)”, RFP7252, IETF, 2014.
[7] Zach Shelby, “CoAP: The Web of Things Protocol”, ARM IoT Tutorial, 2014. 3.
[8] MQTT, http://mqtt.org/
[9] MQTT community wiki, https://github.com/mqtt/mqtt.github.io/wiki.
[10] NIPA 동향보고서, "통신업계의 네트워크 가상화 기술(SDN/NFV)도입 동향, 해외ICT 정책동향“ , NIPA, 2014년 2호.
[11] Open network foundation(ONF), https://www.opennetworking.org/
[12] 이종화, “ETSI NFV 기술 표준화 동향”, Vol.151, TTA Journal, 2014 01/02.
[13] ETSI Draft, “Network functions virtualization(NFV); NFV security; problem statement”, ETSI GS NFV-SEC 001 v0.0.9, 2014.
[14] E. Rescorla,N. Modadugu, “Datagram Transport Layer Security Version 1.2”, RFP6347, IETF, 2012. 1.
[15] Tamer AbuHmed, Nandinbold Nyamaa, and DaeHun Nyang, “Software-Based Remote Code Attestation in Wireless Sensor Network”, IEEE "GLOBECOM" 2009.
[16] J.W. Ho, “Robust Detection of Malicious Nodes in Mobile Sensor Networks Using Software Attestation”, Int'l. Journal of Distributed Sensor Networks, 2013.
[17] Marcello Lioy, “Peer-to-Peer Technology: Driving Innovative User Experiences in Mobile”, AllJoyn, Presentation Slides.

저 자 약 력

권 혁 찬
이메일 : hckwon@etri.re.kr

- 2001년 충남대학교 컴퓨터과학과 이학박사
- 2001년~현재 한국전자통신연구원 ICT융합보안연구실 책임연구원
- 관심분야 : IoT 보안, 융합보안, 무선/모바일 보안, 콘텐츠 보호

정 병 호
이메일 : cbh@etri.re.kr

- 1988년~2000년 국방과학연구소 선임연구원
- 2000년~현재 한국전자통신연구원 ICT융합보안연구실장
- 관심분야 : 무선보안, IoT보안, 멀티미디어 보안 등

김 정 녀
이메일 : jnkim@etri.re.kr

- 1987년 전남대학교 전산통계학과 졸업
- 1996년 OSF/RI 공동연구 파견(미국)
- 2004년 충남대학교 컴퓨터공학과 석사, 박사
- 2005년 Univ. of California, Irvine Post-Doc.
- 1988년~현재 한국전자통신연구원 사이버보안시스템연구부장 책임연구원
- 2015년~현재 과학기술연합대학원대학교(UST) 정보보호공학과 교수
- 관심분야 : IoT 보안, 모바일 보안, 시스템·네트워크 보안, 보안 OS 등