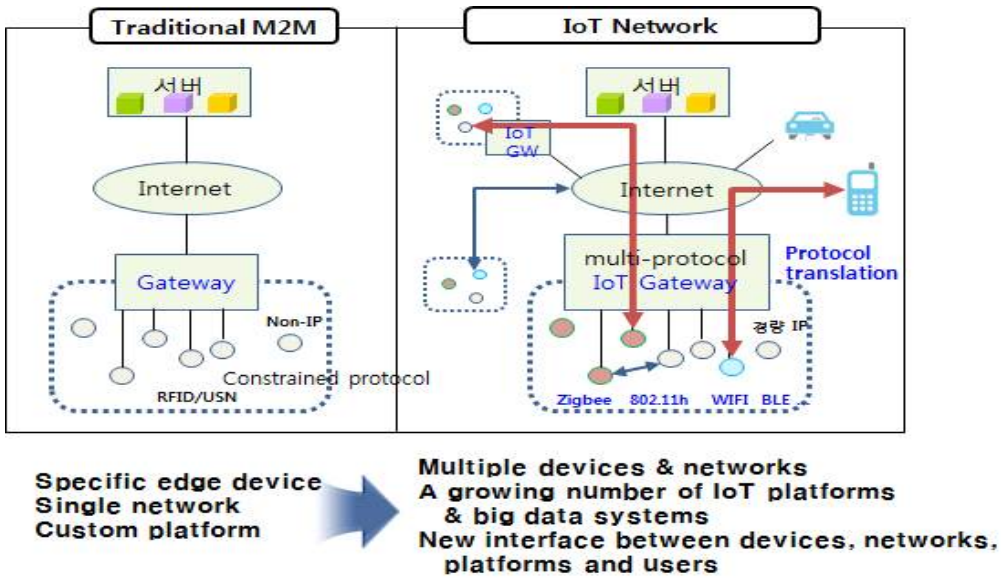
제목 : 사물인터넷 네트워크 보안

(작성자 : 한국전자통신연구원, 책임연구원, 권혁찬)

□ 개요

○ IoT 네트워크는 HW자원·통신방식·보안구조가 상이한 초연결성을 가지며, 사물봇의 광범위한 확산이 용이한 구조로 장치 간 동작의 신뢰성 확보가 필수

- IoT의 '초연결성'은 하드웨어 자원, 통신방식, 보안구조가 상이한 네트워크간 연결 및 연동되는 구조를 말함
- 기존의 RFID/USN과 비교할 때, IoT 게이트웨이의 기능 확장(초연결 지원), 다양한 기기가 다양한 네트워크를 통해 통신, 사물이 IP를 보유, 사물간 직접 통신 지원 등의 특징을 가짐

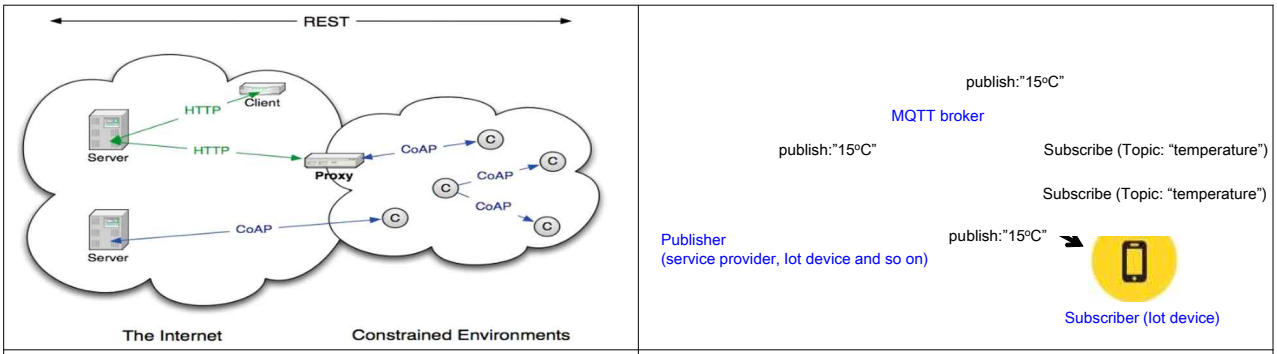


(그림 1) 사물인터넷 네트워크의 특성

○ IoT에 사용되는 통신 프로토콜로는 기존의 Wi-fi, Ethernet, Bluetooth, BLE, Zigbee, PLC, 3G/4G, IPv6 등과 IoT를 위한 신규 프로토콜인 CoAP, MQTT, LwM2M(Light weight M2M) 등이 있음

- CoAP(Constrained application protocol)은 IETF CoRE 워킹그룹에서

개발된 표준으로 응용계층에서 자원이 제약된 IoT 디바이스간 통신을 위한 경량 프로토콜이며, MQTT(Message queueing telemetry transport)는 TCP 상위에서 동작하는 프로토콜로 경량의 publish/subscribe 메시징 모델임



(a) CoAP 구조 (b) MQTT 기반 서비스 동작 사례

(그림 2) CoAP, MQTT 서비스 구조

○ IoT의 초연결성이라는 특성으로 인한 다양한 보안위협이 존재

* 주요 위협: 이기종 사물 네트워크 간 연동 통신과정에서 정보변조 및 유출 위협, T2T 기기, 네트워크 및 게이트웨이 해킹 공격 및 크로스 네트워크 기기로 피해 확산 위협, 대단위 사물봇에 의한 트래픽 폭증으로 인한 IoT 서비스 거부 공격 위협 등

□ 해외 동향

○ ARM, Intercede, Sollacia, Symantic 등 업체들을 중심으로 사물인터넷 보안 프로토콜 OTrP(Open Trust Protocol) 공동개발에 착수('16년)

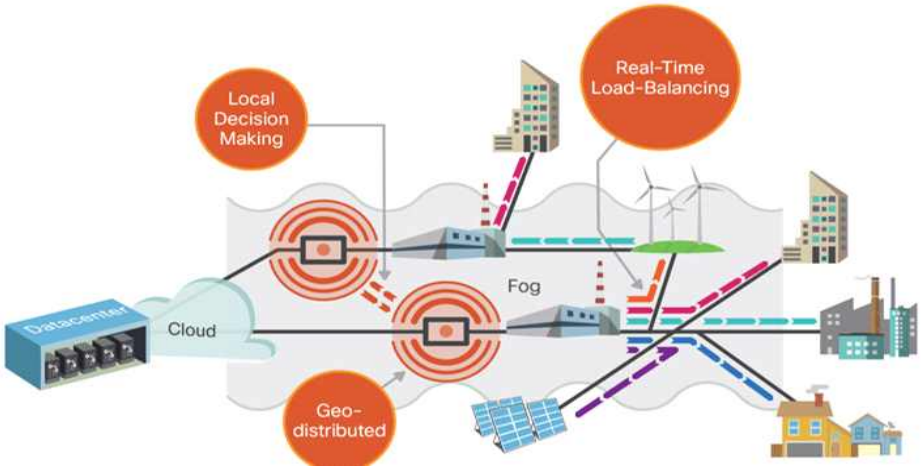
* Beanpod, Sequitur Labs, Sprint, Thundersoft, Trustkernel, Verimatrix 등의 업체들도 참여

* OrTP는 상호작용하는 기기간 신뢰성을 확보하기 위한 기술로, 상위 프로토콜로 ARM Trustzone 기반 Trusted Execution Environments 등의 솔루션과 연동됨

○ 시스코는 IoT 보안 강화를 위한 전담부서 신설 및 다양한 응용에 IoT 기술 적용/실증 추진 등 적극적인 행보를 보임

- IoT systems and software group, IoT security group 신설/운영
- IoE(Internet of Everything), Fog computing 등의 新키워드를 발표하고 교통시스템 등에 IoT를 적용/실증 추진

* Cisco의 Fog computing은 사물인터넷 네트워크에서 생성되는 정보를 클라우드로 올리지 않고 지상의 안개(Fog)와 같은 사물 네트워크 단에서 분석/결정/활용하는 구조



(그림 3) Cisco의 Fog computing 개념도 (출처: Cisco)

○ 인텔은 보안전문업체 McAfee를 인수하고 인텔의 IoT 게이트웨이에 보안 솔루션을 탑재하여 출시

○ 버라이존은 클라우드 기반 IoT 디바이스 식별, 인증, 통신데이터 보호를 위한 보안 솔루션을 개발하였고, GE(General electric) 역시 보안업체 Wurldtech을 인수하여 정유시설, 전력망, 의료기기 용 보안솔루션을 개발

○ 퀄컴에서 개발한 IoT 연결성 플랫폼 AllJoyn에 앱단위의 인증/암호 등 다양한 보안 솔루션 탑재

○ OneM2M은 M2M 디바이스, 게이트웨이, 서버로 구성된 네트워크 환경에서 인증, 암호통신, 원격신뢰관리, 키관리 등의 보안규격 개발 중

□ 국내 동향

○ 삼성전자는 2016년 4월 IoT 데이터를 수집, 분석할 수 있는 클라우드 서비스 '아틱 클라우드'를 공개함

- REST/HTTP, 웹소켓, MQTT, CoAP 등의 프로토콜로 기기와 클라

우드를 연결하며, TLS 및 인증서 기반으로 클라우드와 디바이스의 안전연결 기능 및 OAuth2 표준 적용을 통한 인증 기능 등을 제공

○ ETRI 등 다수의 기관에서 DTLS(Datagram TLS)를 개발하였으며, SKT, KETI 등에서 OneM2M 기기관리 보안 프로토콜 등을 개발한 사례가 있음

○ 펜타시큐리티, 현대오토에버 등에서 IEEE 1609.2 기반 차량간 통신 보안 기술을 개발하였으며, PKI 전문기업인 한국정보인증에서 CAMP 및 IEEE1609.2를 준용하는 차량 PKI 기술 개발 진행중

○ 개인 의료/헬스케어 기기간 연결성을 지원하기 위한 ISO/IEEE 11073 프로토콜에 보안 기능 내재화 연구가 ETRI에서 진행되었음

□ 사물인터넷 네트워크 주요 보안 이슈

○ 이기종 사물네트워크간 연동/통신 과정에서 정보변조/유출 가능성이 있음 → 초연결 종단간 신뢰통신 필요

○ 저전력 사물네트워크 지원 및 무선 해킹, 신호 위변도 등 이슈 → 저전력/경량 통신 보안, 호스트 기반의 IPS/IDS 등 필요

○ 대단위 사물봇에 의한 트래픽 폭증 공격 대책 필요 → 사물인터넷 상에서의 악성트래픽 탐지/대응, 분산 IPS 등 기술 필요

○ 대규모 사물보안 관리의 어려움 → IoT 네트워크, 기기의 보안상태 모니터링/관리 기술 및 사물 보안 업데이트/패치 기술 필요

○ IoT 게이트웨이의 기능 확대 → 초연결 지원뿐 아니라 도메인 보안관리, 침입방지, 접근제어, 키관리, 그룹관리 등의 기능 요구

(그림 4) 다양한 IoT 게이트웨이 플랫폼 제품들