사물 인터넷망의 기술 동향 및 정보보호 패러다임의 변화 분석

김정태

목원대학교

Analyses of Paradigm of Information Security and Trend of Technology in Internet of Things(IoT)

Jung Tae Kim

Mokwon University

E-mail : jtkim3050@mokwon.ac.kr

요 약

본 논문에서는 융합 기술의 발전으로 사물 인터넷을 매개체로 하여 기존의 통신망에서의 응용 기술들이 통합되어 발전되고 있다. 융합 기술로의 발전으로 인하여 기존의 통신망에서의 데이터 보호를 위한 기존의 정보보호 기술로는 사물 인터넷망의 데이터를 보호할 수 있다. 따라서 본 논문에서는 사물 인터넷망에서의 정보보호 기술의 동향 및 요구사항을 분석하여 융합 분야에서 필수적인 사항을 제안한다.

키워드

사물 인터넷, 정보보호, 융합기술, 보안, 저전력

Ⅰ. 서 론

최근의 기술적인 발전으로 기존의 인터넷망에서의 사물들이 연결되어지고 있는 추세이다. 이에 기본이 되는 사물 인터넷(IoT)의 제품과 서비스가 확산되면서 이에 따른 통신망과 사물에서의 침해사고 발생에 따른 경제적 피해는 물론 국민의 생명까지 위협하고 있는 현실에 도래하게 되었다. 이에 대한 대응 체계가 부재하며, 현재의 전 산업분야에서 제품 개발과 서비스의 설계단계 과정부터 보안을 내재하고, 체계적인 사이버 위협으로부터 대응할 수 있는 체계 구축 등이 IoT 보안에 필수불가결하다. 이러한 현상은 사물 인터넷망에서의 디바이스의 초경량, 저전력 특성을 갖는 이기종 기기간의 상호연결이 심화되면서, 기존의 보안기술로는 현재의 IoT 환경에 그대로 적용하기에는 많은 어려움이 발생한다. 따라서, 초경량 및 저전력 디바이스, 이기종간의 네트워크 연동 및 다중 사용자 이용 환경 등을 고려한 새로운 개념의 IoT 보안 기술이 필요하다. 선진국인 미국 및 EU 등은 글로벌 ICT 기업을 중심으로 IoT 보안을 미래 성장을 위한 핵심 경쟁력으로 인식하고, 연구개발에 대한 투자를 확대하고 있는 실정이다 [1].

Ⅱ. 핵심 보안 기술 동향

주요 핵심 IoT 보안 개발의 주요 사항은 디바이스의 소형화 기술, IoT 디바이스의 MCU, 메모리 등의 제한적인 요소, CPU 성능, 전력 상태 등을 고려한 경량 및 저전력 암호모듈 등의 기술 개발이 선행되어져야 한다. 경박단소를 위한 SoC(System on Chip) 및 IoT 보안 운영체제 기술 개발 등이 핵심개발로 대두되고 있다. 단기적으로는 기존의 암호기술을 경량화 시켜 하드웨어를 줄이고 저전력화 하는데 주안점을 두고 있으며 중장기적으로 경량·저전력을 갖춘 신규 암호 SW모듈을 개발하여 IoT 기기 및 네트워크 플랫폼에 적용하는 연구를 진행 중에 있다. 국내의 경우, 경량 및 저전력화를 위한 기존 암호는 AES, ARIA, SEED 등을 개발하였고, 신규 개발 경량암호로는 LEA, PRESENT 등을 연구 중에 있다. 또한 하드웨어(HW) 기반의 경량 및 저전력 암호 SW 모듈을 개발하여, 신체 부착형 웨어러블 기기 및 초소형 센서 등에 대한 위변조 및 부채널공격을 방지하는 보안 SoC 개발에 역점을 두고 있다. 이러한 기기 및 디바이스의 핵심 자원인 운

영체제 및 개인정보 등에 대한 비인가 접근차단 및 SW 위·변조 방지기능, 경량·저전력 암호모듈 등이 내재된 보안 기술이 필수불가결하다. 다음은 주요 개발해야 할 대표적인 연구 주제이다 [2].

가. 운영체제(Secure OS) 개발

모듈형 보안 운영체제를 개발하여 스마트의료, 스마트 카 등 인간의 안전과 직결되는 IoT 기기의 센서 및 게이트웨이 등에 재구성하여 우선 적용

나. 네크워크 기술

- 이기종 기기가 상호 연결된 사물 네트워크 환경에서 실시간 이상 징후를 탐지 및 대응하는 보안 기술 개발

- 신뢰/비신뢰 기기 및 이종 네트워크 간 상호 연결성과 보안 통신을 제공하는 IoT 보안 게이트웨이 개발

III. 보안 요구 사항 분석

사물 인터넷 망을 연결하는 센서 등 다양한 형태의 성능이 서로 다른 IoT 기기별 맞춤형 디바이스 보안 기술이 필요하다. 특히, CPU의 성능, 메모리 크기, 소비전력 등의 제약을 갖는 IoT 기기에서는 기존의 암호기술을 사용할 수 없으므로, 기기의 성능과 보안 강도를 고려한 경량 및 저전력의 암호 기술이 필요하다. 특히, 악성코드의 감염 및 외부 해킹으로 인한 운영체제 위·변조 방지와 디바이스의 정지 혹은 오작동을 방지하는 기술 필요하다. 또한, IoT 기기의 탈취·도난·해킹 등을 통한 불법 복제 및 중요 데이터 유출을 방지하기 위한 하드웨어 보안 기술이 특히 필요하다. 다음은 사물 인터넷망에서 요구되어 지는 보안 사항을 요약한 것이다.

가. 이기종의 기기가 상호 연결된 IoT 네트워크를 대상으로 하는 해킹 및 악성코드 공격 등을 탐지·차단하기 위한 네트워크 보안 기술 필요

나. 통신방식(ZigBee, Bluetooth, WiFi 등) 및 보안 특성(암호, 인증방식 등)이 서로 다른 기기·센서가 상호 연결된 네트워크

다. 서로 다른 기능을 수행하는 IoT 기기 간의 통합 네트워킹에 요구되는 단말 상호간 인증, 보안통신 및 접속제어 기능 필요

라. IoT 네트워크에 접속한 기기와 보안기능이 상이한 게이트웨이로 구성된 IoT 서비스 환경에서 통합 해킹공격 탐지·대응

마. 악성코드에 감염된 사물봇에 의한 트래픽 폭증 공격(DDoS)을 방지하기 위한 네트워크 모니

바. IoT 서비스 구성 요소(기기, 사용자, 서비스)간 상호 인증, 접근 제어 및 프라이버시(위치, ID, 데이터) 보호 기능 제공 필요

사. 위장 사물, 기능이 변조된 사물 등의 서비스 비인가 접속을 차단하기 위한 기기 간 인증, 키 관리 및 접근제어 기능 필요

아. IoT 환경에서 데이터 수집 분석에 의한 프라이버시 침해(개인식별, 추적)를 방지하기 위한 기술 필요

자. IoT 서비스 특성(홈·가전, 의료, 교통 등)과 동작환경(임베디드, 웨어러블, 모바일 등)에 특화된 보안 플랫폼의 개발이 필요

다음은 현재 사물 인터넷의 보안 기술을 위한 요구 조건을 도식한 그림이다 [3].

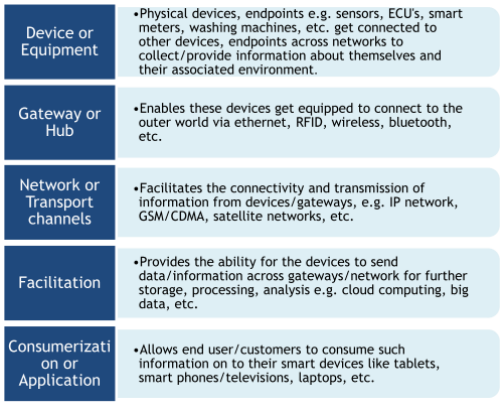

그림 1. 사물 인터넷망을 위한 보안 요구 사항

IV. 결 론

본 논문에서는 사물 인터넷망에서 발생될 수 있는 보안성에 대한 문제를 해석하였다. 현재의 기술로는 사물 인터넷망에서의 디바이스 및 기기 간의 하드웨어적인 제한 요소로 기존의 알고리즘을 사용할 수 없다. 따라서 본 논문에서는 이를 해결하기 위한 선행 조건을 분석하였다.

Acknowledgement

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (grant number: 2010-0024133)

참고문헌

[1] X.L. Jia, Q.Y. Feng, C.Z. Ma, “An efficient anti-collision protocol for RFID tag identification,” IEEE Communications Letters, vol.14, no.11, pp.1014-1016, 2010.

[2] M. Zorzi, A. Gluhak, S. Lange, and A. Bassi, “From today’s INTRAnet of things to a future INTERnet of things: A wireless- and mobilityrelated view,”IEEE Wireless Commun., vol. 17, no. 6, pp. 44.51, 2010.

[3] Ajit Jha & Sunil M C, "Security considerations for Internet of Things ", L&T Technology Services, 2015