The Journal of the Convergence on Culture Technology (JCCT)
Vol. 3, No. 4, pp.185-189, November 30, 2017. pISSN 2384-0358, eISSN 2384-0366

http://dx.doi.org/10.17703/JCCT.2017.3.4.185
JCCT 2017-11-25

LoRa 기반 IoT 보안대책에 대한 연구

A Study on IoT Security Technology using LoRa

정용식*, 차재상**

Youngseek Chung*, Jaesang Cha**

요 약 사물인터넷(IoT) 기술의 급속한 성장에 따라 우리는 공간의 제약을 받지 않고 사람과 사물, 사물과 사물을 서로 네트워크로 연결하여 정보를 주고받을 수 있게 되었다. 최근에는 이를 효과적으로 구현하기 위한 저전력 광역 통신방식인 LPWA(Low Power Wide Area) 네트워크 기술이 점점 인기를 얻고 있다. 본 논문에서는 LPWA 기술 중 하나인 LoRa 기술에 대해서 알아보고 LoRa를 기반으로 하는 IoT 시스템에서 보안위협을 최소화하기 위한 IoT 보안 기술을 제안한다.

주요어 : 사물인터넷, 사물인터넷 보안, LoRa

Abstract According to the rapid growth of Internet of Things (IoT) technology, we are able to connect between human and objects and between objects through network, allowing transmission and reception of information beyond the limits of space. These days, Low Power Wide Area (LPWA) technologies becomes popular more and more, to implement IoT infrastructure effectively. In this paper, this study aims to analyze LoRa, one of LPWA technologies, and suggest IoT security technology using LoRa to minimize threats to security

Key Words : IoT, IoT Security, LoRa

Ⅰ. 서 론

IoT(Internet of Things) 기술은 사람과 사물, 사물과 사물의 연결을 통해 우리 주변에 있는 모든 것들을 서로 연결시키는 기술로 많은 관련 사업에 영향을 미치면서 ICT 산업 분야의 새로운 성장 동력으로 주목받고 있는데, 글로벌 시장조사 기관인 가트너, ABI리서치 등은 2020년에 250억 개 이상의 사물들이 상호 연결될 것으로 전망하고 있으며, ICT 업체인 시스코에서는 500억 개 이상의 사물들이 상호 연결될 것으로 전망하고 있다[1].

우리 주변에서 쉽게 볼 수 있는 IoT 기술은 사람이나 사물에 부착된 다양한 센서를 통하여 위치, 동작, 환경, 온/습도, 신체 측정 등 다양한 데이터를 수집, 분석하여 유용한 정보를 도출하고 있으며, 센서에서 수집한 정보를 기반으로 IoT 기기들을 제어하고 명령을 내리면서 기존과는 다른 사용 편의성과 사용자 경험을 제공하고 있다. 이렇게 IoT 기술의 기본이 되는 센서들을 통해서 데이터를 수집하는 경우에는 적은 전력을 사용하는 센서들이 소량의 데이터를 일정한 주기에 따

*정회원, 서울과학기술대학교 정보통신미디어공학전공
**정회원, 서울과학기술대학교 전자IT미디어공학과
접수일: 2017년 9월 4일, 수정완료일: 2017년 9월 19일
게재확정일: 2017년 10월 23일

Received: 4 September, 2017 / Revised: 19 September, 2017
Accepted: 23 October, 2017
* Corresponding Author: chajs@seoultech.ac.kr
Dept. of Electronics and IT Media Eng,
Seoul National University of Science and Technology

라서 통신을 하게 되는데 3G/4G 등의 이동통신이나 Wi-Fi 등을 사용하는 경우에는 상대적으로 전력 소모가 크거나 고비용을 수반하게 된다. 따라서 IoT 시대에 맞춰서 센서 네트워크 구성에 최적화된 저전력 광역 통신을 지원하는 LPWA(Low Power Wide Area) 기술이 최근 표준화와 함께 확산되고 있다[2][3].

그러나 다양한 종류의 수많은 사물들이 서로 연결되어 정보를 주고받는 IoT 환경을 고려하면 IoT의 보안 위협은 현실에 있는 사람과 사물에 대한 신체적, 물질적 손실로 그대로 다가올 수 있기에 IoT 제품은 이를 보호하기 위한 보안 기술과 대책을 사전에 준비하여야 한다.

이에 본 논문은 LPWA 기술 중에서 전국망이 구축된 LoRa기반으로 IoT 서비스를 구축할 때 안전한 서비스를 제공하기 위한 보안 체계에 대하여 살펴본다. 1장의 서론에 이어 2장에서는 LoRa 기술에 대해서 살펴보고, 3장에서는 LoRa를 기반으로 구축하는 IoT 보안 기술에 대해서 설명하였으며, 4장에서는 결론을 내리고 본 논문의 끝을 맺는다.

II. LoRa 기술

1. LoRaWAN

LoRa는 복수의 네트워크상에서 다양한 어플리케이션들을 단일 네트워크 인프라에 연동하는 기술로, Chirp spread spectrum 기반 변조 방식을 이용하여 높은 감도로 견고한 네트워크 링크를 구성하여 네트워크 효율을 증가시키는 반면 간섭을 제거할 수 있도록 구성되어 있다. 또한 수백bps 이하의 낮은 데이터 전송률을 사용하여 Wi-Fi, Zigbee, Bluetooth 등 이동통신에 비하여 도달 거리가 길고 소규모 기기에서도 동작이 가능하여 배터리 기반의 센서들과 저전력 어플리케이션에 최적화된 기술이다. LoRa의 통신 가능거리는 도심지역에서는 2~15km, 지하에서는 1~2km, 실내는 2~3km이며, 대역폭은 125kHz, 최대 송신 전력은 14dBm로, 주파수 ISM 밴드에서 동작하고 전송속도는 낮은 대역 확산 방식으로 설계되어 있다[4]. 그림 1은 LoRaWAN의 Network Architecture를 보여준다.

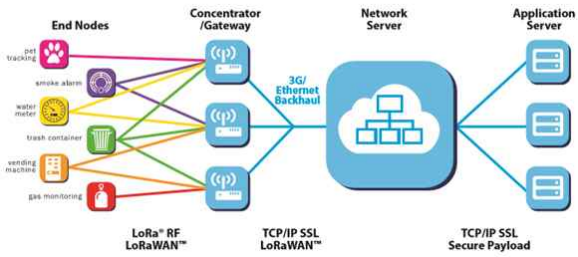

그림 1. LoRa 네트워크 아키텍처[5]
Fig 1. LoRa Network Architecture[5]

LoRaWAN은 각 단말들이 여러 게이트웨이를 통해서 네트워크 서버에 접속하고, 네트워크 서버를 통해서 해당 서비스를 제공하는 어플리케이션 서버로 전달되는 구성을 가진다. LoRaWAN 프로토콜의 스타형 토폴로지는 망형 네트워크와 비교할 때 상대적으로 전력 소모가 적고 여러 어플리케이션이 동시에 실행할 수 있도록 한다[2][4].

2. LoRa Network Layer

LoRa Network Layer는 Physical Layer, MAC Layer, Application Layer로 구성되며, 이 중에서 Physical Layer 통신 알고리즘은 “Semtech”사에서 특허를 가지고 있어서 단말과 기지국에 들어가는 모뎀칩은 “Semtech”사에서 전량 공급하고 있으며, LoRaWAN 기술은 전 세계 통신사업자, 네트워크 장비제조사, IT기업들이 결성한 “LoRa Alliance”에서 기술 규격을 제정하고 있다[6]. 그림2는 Lora의 Network Layer를 보여주고 있다.

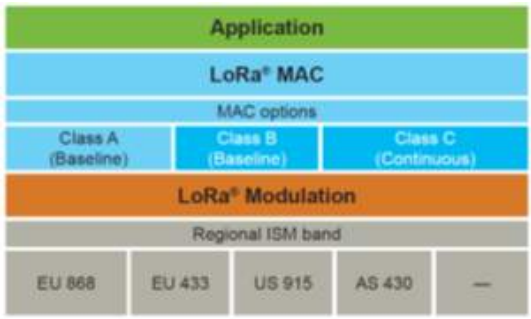

그림 2. LoRa 네트워크 레이어[5]
Fig 2. LoRa Network Layers[5]

LoRa의 MAC Layer는 전력방식과 응답특성에 따라 선택 할 수 있는 class A/B/C의 3가지 방식으로 구성된다[7][8][9].

Class A는 단말의 저전력 특성을 극대화하기 위해 단말이 주도하는 상향 통신에 최적화 되어 있다. 단말은 송신할 데이터가 있는 경우에만 상향 데이터를 발생하고, 상향 데이터를 수신하고 일정시간 후에 미리 정의된 채널로 하향 데이터를 송신하도록 되어 있다. 따라서 Class A는 단말이 상향 데이터를 보내지 않으면 기지국에서 하향 데이터를 보낼 수 없다는 단점을 가진다.

Class B는 하향 데이터가 제한되는 Class A의 단점을 보완한 방식으로, 하향 데이터를 송신하는 별도의 창을 준비하여 예정된 시각에 단말의 상향 데이터 전송과 무관하게 기지국이 하향 데이터를 단말에 전송할 수 있으며, 단말과 게이트웨이의 동기를 위해서 비컨을 사용하여 주기적으로 하향 데이터 유무를 확인한다.

Class C는 전원이 계속 공급되는 단말에 적합한 방식으로, 상향/하향 데이터 송수신 창을 항상 열어둔 상태로 송신하지 않는 순간에는 늘 수신이 가능하도록 구성되어 있다.

3. LoRaWAN Security

LoRa 단말과 게이트는 IP Address가 아닌 EUI-64 기반의 ID 체계를 사용하기 때문에 DDoS, 스미싱, 스캐닝, 바이러스 등 기존에 널리 알려진 IP 기반의 공격에 상대적으로 안전하다[10]. 그림 3은 LoRa 네트워크 상에서의 데이터 흐름에 따른 암호화 구간을 보여주고 있다.

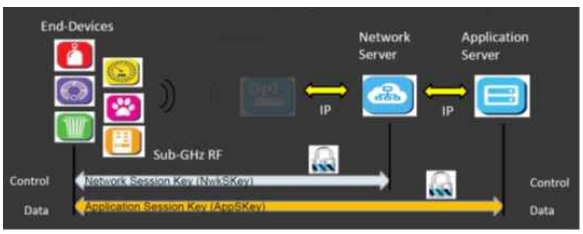

그림 3. LoRa 논리적 데이터 흐름[9]
Fig 3. LoRa Logical Data Flow[9]

LoRaWAN은 단말 인증 및 데이터 무결성 확보를 위한 Network Session Key와 중간 단계에서의 데이터 보호를 위한 Application Session Key를 사용하여 AES 128bit방식의 이중 암호화를 독립적인 보안 계층에 적용하고 있다[9].

III. 3장 LoRa 기반 IoT 보안대책

LoRa IoT 보안 체계를 다음과 같이 LoRa 단말, LoRa 서비스, LoRa Network로 분류하여 제시하였다.

1. LoRa 단말 보안 대책

LoRa 단말은 LoRa서비스와 연동되어 동시에 개발하는 경우도 있으나 일반적으로 서비스 운영과 단말 제작은 담당부서와 관리주체가 다른 경우가 일반적이어서 보안 대책을 구분하여 제시하였다.

1) Secure Boot 기술

LoRa 단말의 Firmware 변조 공격을 차단하기 위해서 Secure Boot를 적용하여 임의로 변조된 Firmware는 동작하지 못하도록 제한할 수 있어야 하며, 전자서명 기반의 H/W Secure Boot는 부트로더에 적용되는 제조사의 public key가 변조되지 않도록 보호해야 하고, S/W Secure Boot는 Firmware 리버싱 엔지니어링을 통해서 Firmware의 Checksum /Hash value 까지 노출될 가능성도 고려해야 한다.

2) Key 관리 보호 기술

LoRa 단말 제작 시 LoRa 네트워크 사업자나 LoRa 서비스 제공자가 발행하여 제공하는 Application ID, Application Key에 대해서 전달 시점부터 단말 설치 시점까지 제조사 내부적으로 외부에 유출되지 않도록 암호화 저장 및 접근 통제를 수행하여야 한다. 추가적으로 단말에 저장되는 Device ID, Application ID, 암호화 세션 Key 등은 유출 시 단말 복제가 가능하므로 보안이 중요한 분야에서는 H/W 모듈을 통한 키 관리를 고려해야 한다.

3) 데이터 보호 기술

LoRa 단말 정보 및 암호화 Key 외에도 센서 등을 통해서 단말이 수집하고 저장하는 민감한 데이터에 대해서는 보호조치를 수립하여야 한다. 서버 전송 후에는 민감 데이터를 삭제하도록 하고 민감한 데이터를 단말 내에 저장 할 경우에는 암호화 저장을 고려한다.

4) 디버깅 차단 기술

단말 제작 시 디버깅 용도로 주로 사용하는 JTAG

나 UART 기능을 통해서 내부 주요 정보가 노출되거나 로그인을 통한 shell 실행 등이 가능하므로, 개발 이후 정식 배포되는 단말은 로그 및 디버깅 포트 차단 또는 외부에서의 메모리 접근 차단 기술을 적용하여야 한다.

5) 시큐어 코딩

LoRa 모듈 개발 시 외부에서의 악의적인 공격 데이터가 입력될 가능성을 고려하여 입력값에 대한 검증, Buffer overflow 방지 등 시큐어 코딩 기법을 적용하여 S/W 레벨에서 취약점을 차단하여야 한다.

2. LoRa 서비스 보안 대책

LoRa 서비스는 단말 데이터를 수집하고 서비스를 제공하는 핵심으로 다음과 같이 보안 체계를 수립하여야 한다.

1) 접근 통제 및 권한 관리

가장 흔하게 발생하는 보안사고 유형의 하나는 업무 담당자의 실수에 의한 것으로 LoRa 어플리케이션 서버에 대해서 접근통제 및 권한관리 기술을 적용하여 담당자 외에는 접근할 수 없도록 하고, 담당자도 역할에 따라서 권한을 제한하여야 한다.

2) 데이터 보호 및 Key 관리 기술

LoRa 단말이 보내는 데이터는 Application Session Key로 암호화되어 LoRa 어플리케이션 서버에서만 복호화해서 데이터를 볼 수 있다. 단말과 네트워크 단에서 암호화로 보호된 데이터가 서버에 평문으로 저장되어 쉽게 유출 될 수 있으므로, 민감하거나 주요한 데이터에 대해서는 서버에서도 암호화하여 저장하도록 하고 암호화 Key에 대해서는 유출되지 않도록 관리하여야 한다.

3) 시큐어 코딩

LoRa 단말과 동일하게 서버 모듈 개발에 대해서도 시큐어 코딩 기법을 적용하여 S/W 레벨에서 취약점을 차단하여야 한다.

3. LoRa Network 보안 대책

LoRa 기반의 단말들은 일반적인 IoT 단말들이 사용하는 IP Address가 아닌 EUI-64 기반의 ID 체계를 사용하기 때문에 LoRa 단말과 LoRa 게이트웨이 구간에 대해서는 기존 IP 기반의 공격에 대해서 상대적으로 안전하다고 할 수 있으나, LoRa 게이트웨이 서버가 Network 사업자 내부망으로 연결되는 구간에 대해서는 보안 체계를 수립하여야 한다.

1) 네트워크 접근 통제 및 보호 기술

외부에 LoRa 게이트웨이가 IP Address를 통해서 직접 접속하도록 오픈되어 있으면, DDoS, 오과금 유발 등 서비스에 대한 공격 목표가 될 수 있기에 외부 접속을 차단하고 보호 기술을 적용하여야 한다.

2) 서버 접근 통제 및 권한 관리

LoRa 게이트웨이와 네트워크 서버 등 내부에서 관리하는 서버에 대해서는 접근통제 기술을 적용하여 업무 담당자 외에는 접속할 수 없도록 각 서버에 대한 접근통제 및 권한관리를 적용하여야 한다.

Ⅳ. 결 론

본 논문에서는 저전력 광역 통신망 기술인 LoRa 기반의 IoT 보안 기술에 대해서 살펴보았다. IoT 보안 기술은 우리 자신과 우리 주변의 사물에 센서를 부착하여 다양한 데이터를 수집하고 명령을 내릴 수 있기에 반드시 고려해야 할 부분이 보안이다. IoT 서비스 전반에 걸쳐서 IoT 단말, 네트워크, 서비스 등 어느 한 곳의 보안 취약점을 통해서 나와 내 주변의 민감한 데이터가 노출되거나 잘못된 IoT 단말의 제어를 통해서 사이버 상의 위협이 현실에 발생할 가능성이 있기 때문이다. 지금까지는 해커나 운영자의 실수 등에 의한 보안사고가 인터넷에 있는 서버들과 내 PC에서만 발생하였지만, 이제 IoT 환경에서 내 가정에 있는 다양한 센서와 IoT 단말들, 그리고 내가 몸에 착용하고 있는 IoT 센서와 단말에서 직접적인 보안사고가 발생한다면 그 피해가 훨씬 더 크고 심각할 것이다.

본 논문에서 제시한 보안 체계에 대해 LoRa 기반으로 IoT 단말을 개발하고 IoT 서비스를 운영할 때 참고가 될 것으로 사료되며, LoRa 기반의 IoT 보안 체계를 통해서 안전한 IoT 환경이 구축되고 다양한 LoRa 기반의 IoT 서비스가 활성화되기를 바란다.

References

[1] Korea Internet&Security Agency, “Study on Security Enhancement for IoT Device and Service” 2015
[2] Ha Jaewoo, Bang Joosun, Een-Kee Hong, “Comparison Study of IoT Supporting Technology”, The Korean Institute of Communications and Information Sciences(KICS), Vol.60, p1161-1162, June 2016.
[3] Byoungsup Shim, Kyungjoo Lim, Hyoseoung Kim, Yuegen yun, Seokjun Choi, “AMI System Based on LoRa IOT”, The Korean Institute of Communications and Information Sciences(KICS), p1302-1303, June 2017.
[4] S.Y. Kim, S.K. Park, H.D. Choi, “Wide Range IoT Technology and Standardization based on LPWA”, Electronics and Telecommunications Trends, Vol.34, No.2, p95-106, April 2016.
[5] LoRa Alliance, “A technical overview of LoRa and LoRaWAN”, November 2015.
[6] Deuk-Ryung Ko, “Low Power Wide Area technology Trends for Internet of Small Things”, OSIA S&TR Journal, Vol.29, No.3, September 2016.
[7] Shenghao Sun, JunHwan Huh, Dong Hyun Kim, Jong Deok Kim, “Analysis of LoRa Technology and Suggestions of Application in Practice”, Korea Computer Congress(KCC), p306-308, December 2016.
[8] Orange, “LoRa Device Developer Guide”, April 2016.
[9] LoRa Alliance, “ LoRaWAN101 - A Technical Introduction”, LoRa-Alliance.org
[10] Yu-Jin Kim, Nu-Ri Lee, Seong-Eun Shin, Seung-Yeon Song, Da-Young Jung, Young-Hyun Chang, Hyung-Nam Moon, “A Study on the Exposures and Threats for Internet of Things(IoT) IP“, The Journal of the Convergence on Culture Technology (JCCT), Vol. 2, No.4, pp.77-82, November 2016.

※ 이 논문은 2017년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (No. 2017-0-00218, LiFi 및 CamCom 기반 VLC 응용기술 국제표준화 연구)