JKSCI

한국컴퓨터정보학회논문지
Journal of The Korea Society of Computer and Information
Vol. 25 No. 7, pp. 85-92, July 2020
https://doi.org/10.9708/jksci.2020.25.07.085

An Vulnerability Analysis and Countermeasures for Security in Outdoor Risk Management System based on IoT Technology

Sung-Hyun Jee*

*Professor, Dept. of Information Security, Baewha Women's University, Seoul, Korea

[Abstract]

Following the development of Internet of Things (IoT) technology, the scope of application of IoT technology is expanding to industrial safety areas that detect and prevent possible risks in outdoor environments in advance, away from improving the convenience of living in indoor environments. Although this expansion of IoT service provides many advantages, it also causes security problems such as data leakage and modulation, so research on security response strategies is being actively carried out. In this paper, the IoT-based road construction risk management system in outdoor environment is proposed as a research subject. As a result of investigating the security vulnerabilities of the low-power wide-area (LPWA, BLE) communication protocol applied to the research targets, the security vulnerabilities were identified in terms of confidentiality, integrity, and availability, which are the three major elements of information security, and countermeasures for each vulnerability were proposed. This study is meaningful in investigating and analyzing possible vulnerabilities in the operation of the IoT-based risk management system and proposing practical security guidelines for each vulnerability.

▸ **Key words**: IoT, LPWA, outdoor risk management system, vulnerability analysis, countermeasure

[요 약]

사물인터넷(Internet of Things: IoT) 기술 발전에 따라서, IoT기술의 적용범위는 실내 환경의 생활 편의성 개선에서 벗어나 실외 환경에서의 발생가능한 위험을 사전에 감지·예방하는 산업안전 분야로 확대되고 있다. 이러한 IoT서비스 확대는 많은 장점을 제공함에도 데이터 유출과 변조 등의 보안 문제도 함께 발생시키므로 이에 따른 보안 대응전략 연구도 활발히 진행되고 있다. 본 논문에서는 실외환경에서의 IoT기반 도로건설 위험방지시스템을 연구대상으로 IoT 보안관리 가이드라인을 제안한다. 연구대상에 적용한 저전력-광역(LPWA, BLE) 통신프로토콜의 보안취약점을 조사한 결과, 정보보안의 3대 요소인 기밀성, 무결성, 가용성 측면에서 보안취약점을 확인하여 이를 최소화할 수 있도록 취약점 별 대응방안을 제안하였다. 본 연구는 기 구현된 실외환경에서의 IoT기반 도로건설 위험방지시스템 운영에서 발생할 수 있는 취약점 조사·분석과 취약점별 실질적인 보안지침을 제안하는데 연구의 의의가 있다.

▸ **주제어**: IoT(Internet of Things), LPWA. 도로건설 위험방지시스템, 보안취약점 분석, 대응전략

• First Author: Sung-Hyun Jee, Corresponding Author: Sung-Hyun Jee
*Sung-Hyun Jee (sunny6205@baewha.ac.kr), Dept. of Information Security, Baewha Women's University
• Received: 2020. 07. 20, Revised: 2020. 07. 28, Accepted: 2020. 07. 28.

http://www.ksci.re.kr pISSN:1598-849X | eISSN:2383-9945

I. Introduction

최근 사물인터넷(Internet of Things: IoT)기술 발전에 따라서, IoT기술의 적용범위도 실내 환경의 생활 편의성에서 벗어나 실외 환경에서 발생가능한 위험을 사전 감지하는 산업안전 분야로 점차 확대되고 있다[1]. 대표적인 IoT 기반 산업안전 연구사례로 건설현장에서 작업자 위치 및 안전사고 등 실시간정보 공유를 위한 블루투스비콘 기반 재난대응시스템을 제안하였다[2,3]. 다른 산업안전 분야 연구사례로 실외환경에서 스마트기기를 휴대하지 않은 현장작업자를 대상으로 재난대응시스템을 구현하여 비콘서비스 한계를 극복하였다[4,5]. 그러나 IoT서비스 확대에 따라 보안 문제가 커짐에 따라 기술적 대응연구도 병행 추진되어야 한다[6,7].

본 논문에서는 IoT기반 도로건설 위험방지시스템 대상으로 보안취약점 조사와 대응전략을 도출함으로써, 실외환경에 적합한 IoT보안 가이드라인을 수립하고자 한다.

II. Application Cases of Outdoor IoT Support

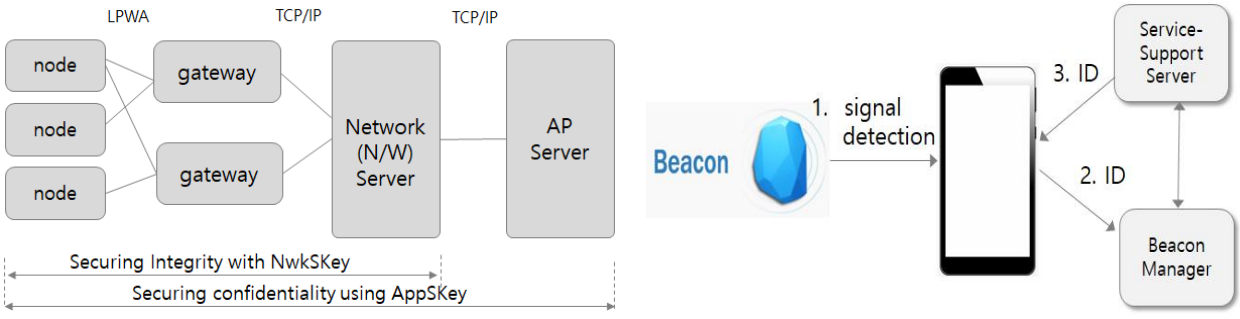
1. Related researches

실외환경에서 IoT서비스를 위한 선결과제는 데이터보안, 저전력소모, 광역 통신거리, 낮은 관리비용 등이 있다. 본 단원에서는 실외환경에 적합한 IoT기반 저전력-광역 통신프로토콜과 통신과정을 조사한다[8,9]. 더불어 실외환경에서 IoT기반 안전관리 서비스 제공을 위한 도로건설 위험방지시스템 구성도 조사한다[4,5].

WiFi나 LTE와 같은 모바일 통신기술은 고속·대용량 서비스 장점을 가지나, 전원이 공급되지 않는 야외지역에서 베터리에 의존하는 통신에는 적용하기 어렵다. 이에 따라서, 배터리 소모특성에 최적화되고 넓은 영역에 대한 통신서비스인 저전력-광역(LPWA: Low Power Wide Area) 통신기술 연구가 활발히 진행되고 있다[8,9]. LoRaWAN, NB-IOT, Sigfox 등 LPWA 네트워크 기술은 그림 1(a)와 같은 아키텍쳐로 LPWA 네트워크 구성요소 간 통신서비스를 진행하고 있다[7]. LPWA 네트워크 기술 가운데 보편적으로 사용하는 LoRaWAN 프로토콜은 그림 1(a)와 같이 구성된다 디바이스(노드)는 저전력 무선통신(LoRa RF)으로 하나 이상의 게이트웨이들과 통신하고, 게이트웨이는 수신한 데이터를 N/W서버에게 전송한다. 그림 1(a)은 LoRa 네트워크 프로토콜에 따른 패킷 송수신 과정을 보여준다. LoRa네트워크의 모든 메세지는 암호화세션키(AppSKey)를 이용한 AES128 암호화알고리즘으로 기밀성(confidentiality)을 지원하고, 인증세션키(NwSKey)를 적용한 4바이트 MIC(Message Integrity Code)으로 무결성(integrity)을 지원한다[8,9]

블루투스 4.0버전인 BLE(Bluetooth Low Energy)는 저전력 무선 통신을 목표로 하는 기술이다. 블루투스 비콘은 주기적으로 사용자 정보(ID)와 수신신호의 세기값을 블루투스 신호로 송신한다. 사용자가 신호 도달영역 내로 진입하면 스마트폰 앱에서 블루투스비콘의 신호를 수신하여 서비스지원서버로 사용자정보를 전달하며, 서비스지원서버는 개별 사용자 정보를 인식한 뒤 적절한 서비스 정보를 사용자의 스마트폰 앱으로 송신하여 서비스가 이루어진다. 저전력 블루투스 통신기술은 백화점내 고객대상 쿠폰발송, 상점내 상품정보 제공, 전시관내 전시물 안내 등 활용되고 있다[10~13]. 그림 1(b)는 BLE기반 통신서비스 절차를 보여준다.

실외환경에서 저전력-광역 IoT인프라 구축은 저전력-광역 통신기술의 특성에 맞는 최적화된 무선 컨넥티비티 선정이 중요하다. 따라서 LPWA 및 BLE 기술은 기존 셀룰러 망과 연동하여 상호 장점을 채택한 보완기술로 가능하며 특수 작업환경(예: 도로공사현장) 특성에 적합하도록 융합형 네트워크 설계에 적용되고 있다[4,5,9].



(a) LoRa Network Architecture (b) BLE-based communication flow chart

Fig. 1. Protocol for Support of Outdoor IoT Service

2. IoT-based road construction risk management system in outdoor environment

IoT기반 도로공사현장 위험관리시스템은 장시간 저전력 환경 하에서 도로 상의 교통정보 수집과 전송과 더불어 스마트기기를 휴대하지 않은 현장 작업자에게도 위험상황을 자동으로 알릴 수 있도록 구현하였다[4,5].

도로공사현장 위험관리시나리오는 다음과 같다. ① 공사현장 전방에 설치하는 안전표지판에 별도 통신장비(비콘, 센서, LPWA)를 설치하여 차량이 공사현장으로 근접 시 차량속도, 근접정보를 실시간 수집한다. ② 차량이 공사현장 위험구간까지 근접할 경우, 운전자와 작업자에게 즉시 위험문자를 전송한다. ③ 동시에 작업장 내부 경광등과 경고스피커를 통하여 위험경고음을 발생시켜 작업자가 현장에서 대피할 수 있도록 한다.

그림 2의 도로공사현장 안전관리시스템은 위험관리시나리오를 구현하였다(안전표지판⇒IoT안전표지판, 위험정보 수집·알림(스피커)⇒게이트웨이/스마트폰/서버, 관리자(본부 상황실)⇒서버·빅데이터 분석모듈). 통신망은 LPWA와 BLE기술을 융합하여 구성한다. IoT안전표지판에 설치된 LPWA모듈은 센서를 통해 수집된 위험정보를 주변 IoT안전표지판과 네트워크 서버로 전달한다. IoT안전표지판에 설치된 비콘은 스마트폰을 보유한 운전자 및 작업자의 앱과 클라우드서버를 연계하여 현장 위험정보를 운전자와 작업자에게 실시간 전송한다.

제안시스템의 작업흐름도는 그림 3과 같다. 공사현장 전방에 위치하는 IoT안전표지판의 라이더센서가 차량을 감지하면 거리를 측정한다. 만약 차량이 위험구간에 접근한 경우 동시에 네트워크 서버는 IoT안전표지판의 LPWA 모듈 간 통신을 통하여 위험정보를 전달받는다. 네트워크 서버는 공사장 내에 설치되어 있는 경고모듈(경광등, 경고스피커)을 이용하여 작업자에게 위험정보를 전달한다. 또한 네트워크 서버는 센서로부터 수집된 각종 정보를 클라우드 서버에 전송한다.

3. Implications

IoT서비스를 적용한 도로건설 위험방지시스템은 다양한 객체와 통신기술 간 융합을 통하여 서비스 적용범위를 확대하였다. 그러나 LPWA, BLE기반 통신 등 통신기술의 융·복합화가 확대됨에 따라서 발생 가능한 보안취약의 위협도 증가하여 장비(구성요소) 간 정보 송수신 과정에서 여러 유형의 기밀성, 무결성, 가용성 위협에 노출될 수 있다. 본 연구는 구현한 IoT기반 도로건설 위험방지시스템의 장치 간 통신과정에서 발생할 수 있는 다양한 보안취약점을 조사하여 취약점 별로 실질적인 대응방안을 제안하는데 연구의 의의가 있다.

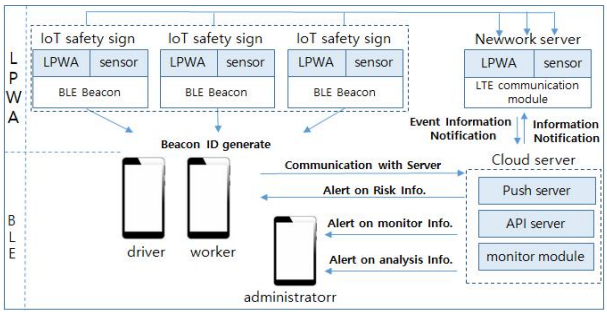


Fig. 2. risk management in road construction

III. Vulnerability analysis

도로건설 위험방지시스템은 장비(구성요소)간 통신과정에서 데이터 기밀성, 무결성, 가용성 침해를 발생시킬 수 있다. 공격자는 노드~네트워크(N/W) 서버, 네트워크(N/W)서버~어플리케이션(AP) 서버 간에 교환하는 데이터를 수집·분석 과정을 통하여 취약점을 발견할 수 있다. 이 장에서는 연구 대상의 통신 과정에서 발생 가능한 취약점과 공격유형을 분석한다.

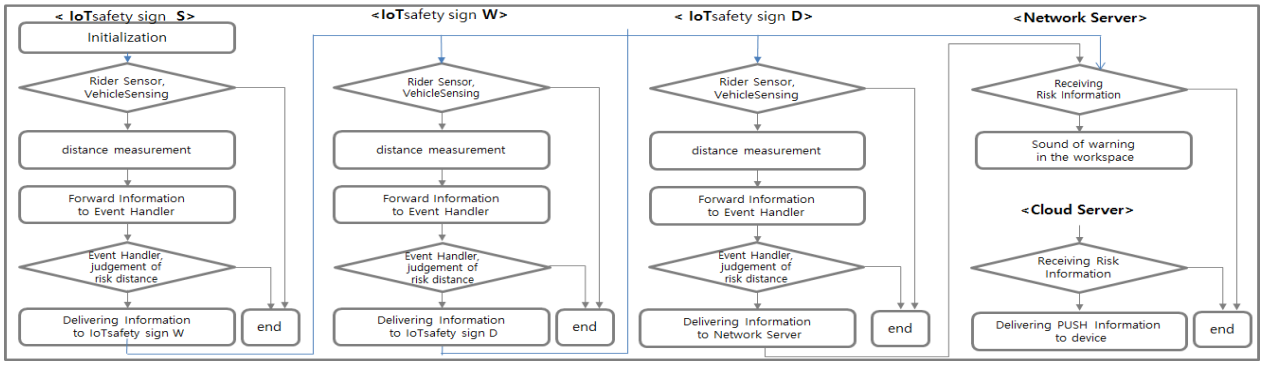
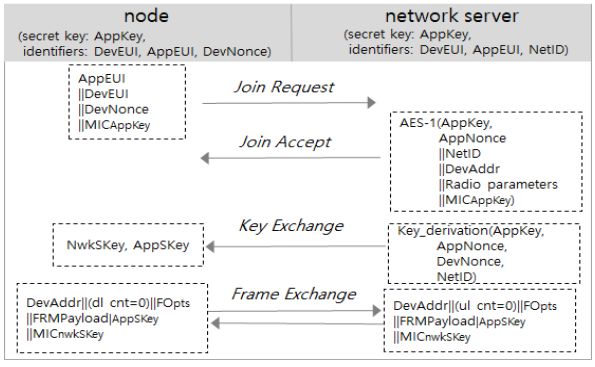


Fig. 3. LPWA Communication Flow on IoT Safety Sign

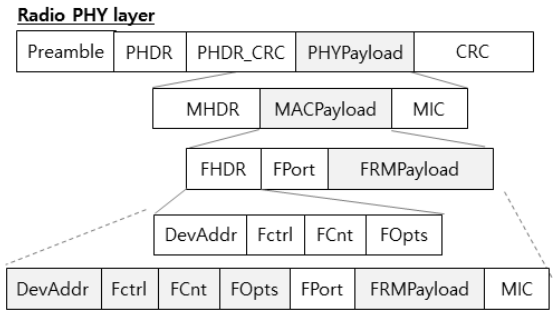
1. Low-Power Wid-Area Protocol&BLE

LPWA통신에서 노드와 N/W서버는 128비트 비밀키(AppKey)를 공유한다. 통신 시작을 희망하는 노드는 OTAA (Over-The-Air-Activation) 방식에 따라 N/W서버로 join-Request 메시지(4바이트 MIC(Message Integrity Code) 포함)를 전달한다. N/W서버는 전달받은 join-Request 메시지로 MIC값을 재계산하여 유효하다고 판정되면 join-Accept 메세지를 전송한다. 또한, N/W서버는 자신이 생성한 의사(psuedo-random) 코드인 AppNonce, NetID와 노드부터 수신한 보안파라메타 DevNonce를 이용하여 두 개의 128비트 암호화세션키 AppSKey과 인증세션키 NwSKey를 생성한다. LoRa네트워크에서 송·수신되는 모든 메세지에는 암호화세션키를 이용한 CTR기반 AES128 암호화알고리즘이 적용되고 인증세션키를 이용한 4바이트 MIC가 생성된다. 그림 4(a)는 노드와 N/W서버 간의 통신 처리절차를 보여준다. 또한 그림 4(b)는 노드와 N/W서버 간 정보 교환을 위한 메시지 포맷 구조를 보여 준다. 메시지포맷은 통신에 필요한 보안파라메타들, 암호화된 프레임페이로드(FRMPayload) 및 메시지인증값(MIC)으로 구성된다[14,15].

BLE 프로토콜 스팩은 HCI(Host Controller Interface)를 기준으로 호스트 컨트롤러 프로토콜과 호스트 프로토콜로 나뉘게 된다. 호스트 컨트롤러 프로토콜은 블루투스 모듈에 해당하며 베이스밴드(baseband), LMP(Link manager Protocol) 등 기능이 펌웨어(firmware) 형태로 모듈 내부에 포함된다. 호스트 프로토콜은 블루투스 모듈과 연결되고 어플리케이션 제어프로토콜(L2CAP, RFCOMM, SDP 등)로 구성된다. 블루투스 v4.0기반 비콘은 ① 소량(21바이트) 패킷, ② 주기적인 신호, ③ 페어링 불필요, ④ 저전력 소모, ⑤ 도달거리 최대 50m, ⑥ 소형, ⑦ 저비용 운영이 가능한 특징을 가진다[12,13].



(a) LPWA communication flow



(b) LPWA message format structure

Fig. 4. LPWA Communication Protocol

2. Vulnerability analysis

2.1 confidentiality threat

LPWA통신은 AES128-CTR알고리즘 암호화로 데이터 기밀성을 유지한다. 그림 5는 프레임페이로드(FRMPayload)의 암호화 절차를 보여준다. 공격자는 암호화세션키를 알지 못해도 메시지포맷 구조, 메시지복호화 절차, 암호화에 사용되는 키스트림(S_i)과 카운터블럭(A_i), 보안파라메타 특성을 분석하여 보안취약점을 발견할 수 있다. 이 단원은 기밀성을 침해할 수 있는 프레임복호화 시도와 bit Flipping 공격 발생가능성을 분석한다.

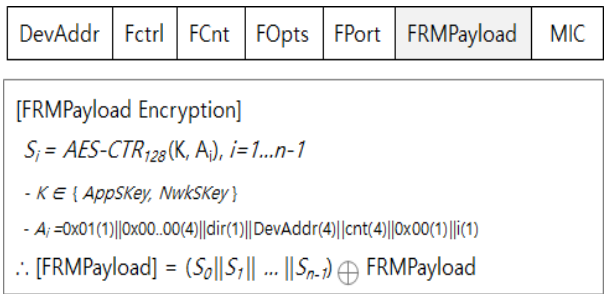


Fig. 5. cryptographic procedure of FRMPayload

2.1.1 decryption attempt

메세지 암호화를 위하여 키스트림 S_i 생성은 중요하다. 키스트림 생성에 필요한 카운터블럭(A_i)은 dir, DevAddr, cnt 및 비트 값들로 구성되는데, 여기서 카운터 cnt가 매회 1씩 증가(또는 감소)하는 것을 제외하면 나머지 값은 N/W서버에서 생성한 고정 값이므로 공격자가 카운터 값을 예측한다면 A_i값의 재사용(replay)을 시도할 수 있다. 만약 공격자가 서로 다른 세션에서 동일한 키스트림 S_t을 중복 사용하는 프레임 재생공격을 한다고 가정하자. 만약 세션 S_{old} 시 전송되는 프레임은 키스트림 S_t(t 시점의 카운터블럭 A_t적용)와 평문 P를 XOR연산으로 생성한 암호화된 페이로드 $C_t^{S_{old}} = P \oplus S^{S_{old_t}}$를 포함한다. 이때 다른

세션 S_{new}동안 전송되는 프레임에 키스트림 S_t(t 시점의 카운터블럭 A_t적용)과 XOR연산으로 생성된 암호화된 페이로드 $C_t^{S_{new}} = P' \oplus S^{S_{new_t}}$가 있고 A_t값의 재사용으로 키스트림 $S_t^{S_{old_t}} = S_t^{S_{new_t}}$ 일 때,

$$C_t^{S_{old}} \oplus C_t^{S_{new}} = (P \oplus S_t^{S_{old}}) \oplus (P' \oplus S_t^{S_{new}}) = P \oplus P'$$

두 암호문의 XOR 결과($C_t^{S_{old}} \oplus C_t^{S_{new}}$)는 두 평문의 XOR 결과($P \oplus P'$)와 동일하다. 만약 평문 P 또는 P'의 일부분을 안다면 $P \oplus P'$ 분석을 통하여 최종적으로 평문 P과 P'을 부분 또는 전체적으로 밝혀내는 복호화를 가능케 할 수 있다. 또한, 일부 평문을 안다면 암호문과 XOR 연산을 역이용하여 키스트림도 알아낼 수 있다.

2.1.2 Bit Flipping attack

공격자가 메시지 구조를 알고 있을 경우, 프레임페이로드 내 일부 비트를 플립핑(flipping)함으로써 데이터 변형이 가능하다. 이는 암호화세션키를 몰라도 가능하다. 프레임페이로드는 평문 P을 키스트림 S과 XOR연산으로 생성되므로 프레임페이로드 내 일부 비트의 프립핑만으로 정보 변조가 가능하다. 이때, N/W서버가 메세지 무결성 확인(변조 확인) 없이, 복호화를 실행하면 변조된 코드의 실행으로 공격자가 의도한 공격이 발생할 수 있다.

공격자가 키스트림 S_i 재사용 공격을 시도하는 이유는 키스트림 생성에 사용되는 보안파라메타 값을 확보할 수 있기 때문이다. 즉, DevNonce는 짧고 의사-랜덤 값으로 암호화 없이 join Request 메시지에 포함되어 전송하므로 스니핑 방식으로 확보 가능하다. 또한, N/W서버에서 생성하는 AppNonce는 3바이트 의사-랜덤 값이고 DevAddr는 고정 상수 값이므로 지속적인 메세지 수집·분석과 brute-forced 공격 시도를 통하여 취득할 수 있다.

2.2 Integrity threat

LPWA통신은 그림 6과 같이 CMAC(메세지인증체크)과 인증세션키 NwkSKey을 적용한 4바이트 MIC을 이용하여 데이터 무결성을 인증(authentication)한다.

DevAddr	Fctrl	FCnt	FOpts	FPort	FRMPayload	MIC

[Message Signification]

cmac = AES-CMAC(*NwkSKey*, B_0 | HDR | FRMPayload)

- B_0=0x49 | 4*0x00 | Dir | DevAddr | FcntUP or FCntDown | 0x00 | len(msg)
- HDR= DevAddr | Fctrl | FCnt | Fopts | FPort

MIC = *cmac* [0..3]

Fig. 6. Generation of Message Integrity Code

2.2.1 brute-forced attack

LPWA 통신 네트워크에서 교환되는 메세지는 메세지서명(MIC)을 적용하여 정보 무결성을 보증한다. 그러나 MIC는 4바이트(32비트)로 길지 않은 비트집합이므로 공격자는 brute-forced 공격을 통하여 2^{32}회 이내 일치 값을 찾으면 무결성 침해의 위협을 받을 수 있다.

2.2.2 message modulation in areas without certification

노드와 N/W서버 간의 LPWA통신은 MIC 메시지인증체크를 통하여 데이터 무결성을 확보한다. 그러나 N/W서버만이 인증을 검증할 수 있는 인증세션키 NwksKey를 보유하고 AP서버는 프레임 암·복호화에 사용하는 암호화세션키 만을 보유한다. 따라서 AP서버는 노드와 데이터 교환 시에 변조가 발생해도 이를 검증할 수 없다. 공격자는 프레임페이로드 내 일부 비트를 플리핑함으로 데이터의 변형이 가능하다. 그러나 AP서버는 복호화 메시지의 무결성 검증장치를 가지지 못하므로 변조된 메세지를 수신하더라도 변조 여부를 알 수 없다.

2.3 Availability threat

노드와 N/W서버 간 가용성 확보는 365일 무중단 서비스의 필수요소이다. 노드와 N/W서버는 새로운 세션을 시작하기 위하여 job Request와 job Accept 메세지를 교환하면서 보안파라메타 및 세션키(AppSKey, NwkSKey)공유가 필요하다. 이때 공격자가 노드와 N/W 서버 간 데이터 교환 과정에서 중간자공격(MITM Attack, Man In The Middle)을 시도할 경우 가용성 침해가 발생할 수 있다. 그림 7은 노드와 N/W서버와의 메시지 교환과정에서 공격자가 중간자공격을 시도하는 과정을 보여준다.

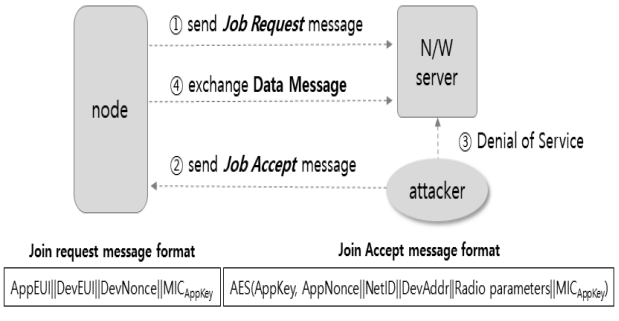


Fig. 7. MITM Attack during LPWA Communication

2.3.1 join Accept replay attack

공격자는 N/W서버에서 이전에 사용한 join Accept 메세지를 수집하여 재생공격(replay attack) 시 사용할 수 있다. 재생공격이 가능한 것은 노드가 자신이 전송한 join

request 메세지와 공격자가 전송한 join Accept 메세지 간 연계성을 확인할 수 없기 때문이다.

공격자로 인하여 발생가능한 통신흐름은 다음과 같다: ① 공격자는 N/W서버가 특정 노드에게 보내는 join Accept 메세지를 지속적으로 수집한다. ② 만약 해당 노드가 새로운 세션을 시작하기 위하여 N/W서버에 join Request 메세지를 전송할 때, 공격자는 이를 파악하여(N/W서버가 join Accept 메세지를 전송하기 전에) 사전에 수집한 join Accept 메세지를 재전송하는 중간자 공격을 실시한다. ③ 노드는 공격자로부터 전송받은 join Accept 메세지를 이용하여 세션키를 생성하고 암호화 메세지를 생성·전송한다. ④ N/W서버는 전송받은 암호화 메세지가 자신과 동일한 세션키를 적용하지 않은 메세지임을 검증하고 무시(ignore)한다. ⑤ 노드와 공격자 및 N/W서버가 동일한 상황을 반복하면서 통신 미연계 상황을 발생시킨다. 이와 같은 상황으로 인하여, 노드는 join Accept 재생공격으로 인한 통신 과다로 서비스 지연, 전력소모 등 문제를 발생시킨다.

2.3.2 join message harvest

N/W서버는 공격자에 의한 재생공격을 막기 위하여 전에 사용된 DevNonce값이 포함된 join request 메세지는 무시한다. 따라서 노드는 join request 메세지를 생성할 때마다 새로운 DevNonce 값을 생성한다. 만약 공격자가 사전에 수집한 Job Request 메시지를 N/W서버로 반복 송신하다면 N/W서버는 계속 무시한다. 노드는 그때마다 새로운 join request 메세지를 생성하여 N/W서버로 전송한다. 공격자는 스니핑을 통하여join request 메세지를 수집할 수 있다.

2.3.3 teardrop attack

메시지 전송에서 프레임카운터(FCnt) 값은 메시지 내에서 암호화되지 않은 상태로 전달된다. 노드가 동일한 N/W서버로 프레임을 전송한다면 프레임을 구성하는 보안 파라메타 DevAddr, Fctrl이 동일하다. 여기서 유일하게 변화되는 값은 카운터(FCnt)이다. 만약, 노드나 N/W서버가 카운터값을 체계적으로 관리하지 않을 경우, 공격자는 프레임 재생공격을 할 수 있다.

공격자는 전송중인 프레임을 가로채어 FCnt 값을 변조할 수도 있다. N/W서버는 수신한 프레임내 FCnt 값이 {0··MAX_FCnt} 범위 내에 존재하는 지 확인한다. 이때 Fcnt 초기값은 0이고 MAX_FCnt=2^{14}이다. 만약 공격자가 변조한 FCnt값이 2^{14}+1과 같이 큰 값 또는 매우 작은 값을 대입할 경우, N/W서버는 카운터 값을 비교하여 유효하지 않다고 판단하므로 수신한 메세지를 버린다. 이 공격은 패킷 재전송과 재조합 등 통신 과부하를 발생시켜서 최종적으로 서비스 중단을 발생시킬 수 있다.

프레임카운트(FCnt) 사용

DevAddr	Fctrl	FCnt	FOpts	FPort	FRMPayload	MIC

2.3.4 DoS attack

공격자는 join Accept 재생공격과 join message harvest 공격을 반복적으로 발생시켜서 N/W서버와의 통신연계를 방해한다. 이와 같은 서비스거부공격은 노드 측면에서 공격자로부터 받은 join Accept 메세지와 자신이 전송한 join Request 메시지 간 연계성 여부 및 N/W서버와 동일한 세션키를 공유하였는 지 검증을 할 수 없으므로 가능하다. 노드는 별도 검증 없이 공격자에게 전달받은 job Accept 메시지 내 보안파라메타를 이용한 메세지 암호화 등 유효하지 않은 작업을 반복한다.

DoS 공격은 게이트웨이~N/W서버 간 통신과정에서발생할 수 있다. 이때 장비 간 통신은 TCP/IP 통신으로 진행된다. 공격자가 N/W서버로 DoS공격을 지속적으로 실행하면 이는 N/W서버와 노드 간 통신단절을 초래한다.

2.3.5 BDoS

블루투스기반 비콘은 블루투스 자체로 2.45GHZ 내 많은 채널로 나누어져 있지만 지속적인 전파 간섭 및 교란신호 공격으로 서비스 오동작을 발생시킬 수 있다.

2.3.6 Spoofing

비콘 서비스는 MAC주소, IP주소 등 네트워크 통신과 관련된 정보를 변경하여 통신 흐름을 왜곡시켜서 장비 간 통신 연결이 되지 않는 상황을 만들 수 있다.

IV. Countermeasures

실외 환경의 IoT 기반 도로건설 위험방지시스템에서 조사된 보안취약점과 공격유형은 <표 1>과 같다. 본 단원은 시스템 내 장비(구성요소) 간 통신과정에서 확인된 보안취약점과 이를 최소화하기 위한 대응전략을 제안한다.

1. Confidentiality enhancement

① 보안파라메타 관리체계 강화

데이터 기밀성 침해는 공격자가 특정 노드나 N/W서버에서 사용한 보안파라메타를 재사용할 때 발생할 수 있다. 기밀성 침해 예방은 보안파라메타 값을 재사용을 할 수 없도록 관리하고 사용여부를 탐지하는 것이다. 이를 위해서는 노드와 N/W서버 별로 보안파라메타 생성·관리체계가

적용되어야 하며 공격자가 재사용하는 기회를 갖지 않도록 충분히 큰 비트수로 구성하여야 한다.

② 키스트림 관리강화

메세지 암호화를 위하여 키스트림 S_i 생성은 중요하다. S_i 생성에 필요한 카운터블럭(A_i)은 dir, DevAddr, cnt 및 비트 값들로 구성되는데, cnt을 제외한 값들은 N/W서버에서 고정 값이므로 공격자가 카운터 값을 예측한다면 A_i값의 재사용을 시도할 수 있다. 따라서 생성함수에 변화를 주거나 큰 크기의 비트수 구성이 필요하다.

③ 메세지 선 인증-후 복호화 절차 준수

Bit Flipping 공격은 N/W서버가 수신한 메세지의 MIC 체크를 검증한 후 프레임페이로드 복호화를 실행함으로써 프레임페이로드 변조를 확인할 수 있다. 만약 N/W서버는 메시지인증체크를 통한 변조를 확인하기 전에 메시지 복호화를 실행하면 변조된 정보를 실행시킬 수 있다. 그러므로 수신메시지는 <1단계> MIC체크를 통한 변조확인, <2단계> 변조되지 않은 경우 페이로드 복호화를 유지하여야 한다.

2. Integrity Enhancement

① MIC(메세지인증체크) 비트크기 확대

LPWA 통신 네트워크에서 무결성 보증을 위한 MIC(4바이트)는 brute-forced 공격을 통하여 2^{32}회 이내 일치값을 찾으면 무결성 침해의 위협을 받을 수 있다. brute-forced 공격에 대한 회피방법으로 MIC크기를 충분히 크게 하여 공격이 성공하지 못하도록 한다.

② 인증 미적용 영역 제거

노드와 AP서버 간의 메시지 교환 시, AP서버에는 노드로부터 수신한 메시지의 무결성 여부를 확인할 수 있는 무결성 검증장치가 없다. 그러므로 무결성 검증영역을 확대 적용할 수 있도록 AP서버에도 메시지 인증체계를 적용함으로써 무결성에 취약한 영역을 제거해야 한다.

3. Availability Enhancement

① join Request~join Accept 매칭 검증

노드는 송신한 join Request 메시지와 수신한 join Accept 메시지 간 연계성을 확인할 수 없다. 이러한 취약점으로 인해 join Accept, join message harvest 공격에 노출되므로 취약점제거 방법은 join Request-join Accept 간 연계성을 검증하는 것이다. 연계성검증 방법으로 join Request에 포함된 보안파라메타(DevNonce, DevEUI)와 join Accept 내 AppNonce을 이용한 계산 값을 산출하여 일치 여부를 상호 검증하는 기능을 고려할 수 있다.

② 화이트리스팅(유효하지 않은 IP주소 필터링)

게이트웨이에서 N/W서버로의 통신은 TCP/IP 통신으로 진행된다. 공격자가 N/W서버로 DoS공격을 지속적으로 실시하면 서비스 중단이 발생한다. 해결방안은 네트워크 내의 검증된 IP주소(노드)와의 통신이 가능한 화이트리스팅 IP주소활용(whitelisting IP address)을 추천한다. 리스팅에 속하지 않는 IP주소기반 통신을 필터링함으로써 불명확한 기기에서의 접근을 사전에 차단할 수 있다.

V. Conclusions

IoT인프라의 서비스 적용분야 확대와 함께 데이터 보안 문제점도 빈번하게 발생하고 있다. 본 논문에서는 실외환경의 IoT기반 도로건설 위험방지시스템을 연구대상으로 발생

Table 1. Type of attack by Communication Interval

Communication Interval / Attack Type	LPWA IoT security sign-IoT security sign	LPWA IoT security sign-N/W server	TCP/IP N/W server - AP server	BLE IoT security sign (Beacon)-Cell Phone	vulnerability type		
					C	I	A
Bit Flipping attack	○	○			○	○	
brute forced attack	○	○	○			○	
join Accept attack	○	○					○
join message harvest	○	○					○
frame replay attack	○	○			○		○
DoS attack	○	○	○	○	○		○
spuffing attack				○			○

※ C: Confidentiality, I: Integrity, A: Availability

가능한 보안취약점을 조사하고 보안취약점 별 기술적 대응 전략을 도출함으로써 IoT보안가이드라인을 제안하였다.

연구대상의 보안취약점 분석결과, 기밀성 침해로 인한 프레임복호화 시도·bit Flipping 공격, 무결성 침해로 인한 brute-forced 공격·미인증영역 내 메세지 변조, 가용성 침해로 인한 join Accept·join message harvest·DoS 공격 등의 발생가능성을 확인하였고 취약점 별로 실질적인 대응방안을 제안하였다. 향후 연구방향은 제안한 IoT보안 대응전략에 대한 학술적 검증 및 구현에 집중함으로써, 이를 통한 IoT보안표준화 분야에 주력할 예정이다.

ACKNOWLEDGEMENT

This work was financially supported by Baewha Women's University.

REFERENCES

[1] Boon-Do Jeong, Mi-Seon Hong "A Study on the Activation of IoT Industry Strategy and Policy in the 4th Industrial Revolution," International Commerce and Information Review, Vol. 21, No. 1, pp. 341-360, Mar. 2019.

[2] Song, J.H., Jang, Y.G. and Jeon, H.S., "Construction Method of Disaster Prevention/Prediction and Site Management System on Construction Site", Proceedings of Korea Society of Surveying, Geodesy, Photogrammetry, and Cartography, pp.325-327. Apr. 2015.

[3] Sang-Won Choi, "Development and Its Characterization of a worker's Safety Activity Detection Apparatus Using Smart Phone," Journal of the Korean Society of Safety, Vol. 30, No. 3, pp. 20-25, Jun. 2015

[4] Seungsoo Lee, Jeong-Min Han, Yun-Cheol Kim "Design of Safety Management System Using Smart Safety Signs," The 2018 Conference of The korean institute of communications and Information Sciences, p. 1508 - 1509. Jun. 2018.

[5] Seung-Soo Lee, Yun-cheol Kim, Sung-Hyun Jee, "Design and Implementation of Road Construction Risk Management System based on LPWA and Bluetooth Beacon," The Journal of The Korea Society of Computer and Information, Vol. 23 No. 12, pp. 145-151, Dec. 2018.

[6] Mijoo Kim, Woong Go, Sungtaek Oh, Jaehyuk Lee, Kim Hong-Geun, SoonTai Park "A Study on the types of IoT attacks by collecting IoT device vulnerabilities and exploits," The Journal of Korea Institute Of Information Security And Cryptology, Vol. 29, No. 6, pp. 81-88, Dec. 2019.

[7] Yoon-Su Jeong, Yong-Ho Yon "A Privacy Approach Model for Multi-Access to IoT Users based on Society 5.0," The Journal of Convergence for Information Technology, Vol. 10. No. 4, pp. 18-24, 2020.

[8] Woong Cho, "LoRa for LPWA network: overview and its performance enhancement technologies," The Journal of the Korea Institute of Electronic Communication Science, Vol. 14, No. 2. pp. 283~288. Mar. 2019.

[9] Pham Minh Trung, Vinayagam MariappanVinayagam Mariappan, Jae Sang Cha, "A Study on IoT/LPWA-based Low Power Solar Panel Monitoring System for Smart City," The Journal of The Korea Institute of Intelligent Transport Systems, Vol. 18, No. 1. pp. 74~82 Feb. 2019.

[10] Jihoo Jung, Jieun Baek, Yosoon Choi, "Analysis of Features and Applications of Bluetooth Beacon Technology for Utilization in the Mining and Construction Industries," TUNNEL&UNDERG ROUND SPACE Vol. 26, No. 3, pp. 143-153, http:// dx.doi.org/ 10.7474/TUS.2016.26.3.143, 2016.

[11] Kim, Yun Cheol, "Design and Implementation of the Beacon -based Safety Management System for Construction Industries", Advanced Science Letters, Vol. 23, No 10, pp. 9808-9811(4), Oct. 2017.

[12] Mingyuan Zhang, Tianzhuo Cao and Xuefeng Zhao, "Applying Sensor-Based Technology to Improve Construction Safety Management," The Journal of Sensors, Sensors doi: 10.3390/ s17081841, https:// www.mdpi.com/journal/sensors, Aug. 2017.

[13] Jung Yoon Ham, Dong Min Jang, Gyoung Bae Kim, Soon Jo Lee, Jung Hyun Cho, Je O Song, "Astudy onworking space safety management services using bluetooth low energy beacon," The Conference of The korean institute of communications and Information Sciences, P366~P367. 2017.

[14] Gildas Avoine, Loïc Ferreira, "Rescuing LoRaWAN 1.0,", Financial Cryptography and Data Security: 22nd International Conference, pp. 253~271. Mar. 2018.

[15] Emekcan Aras, Gowri Sankar Ramachandran, Piers Lawrence, Danny Hughes, "Exploring the Security Vulnerabilities of LoRa," The conference of 2017 3rd IEEE International Conference on Cybernetics (CYBCONF), Jun. 2017.

Authors

Sung-Hyun Jee received the B.S., M.S. and Ph.D. degrees in Computer Science from Chungbuk National University, Korea, in 1993, 1995 and 2000, respectively She also completed post-doctoral course at University of Missouri in USA for 2001-2003. Dr. Jee joined the faculty of the Department of Smart IT at Baewha women's University, Seoul, Korea, in 2014. She is currently a Professor in the Department of Information Security, Baewha women's University. She is interested in IoT Integration, internet and mobile computing, and IOT security.