

2018 춘계학술발표대회 논문집

일시 2018년 4월 27일(금) ~ 28일(토)

장소 제주대학교 아라캠퍼스 아라컨벤션홀

주최 사단법인 한국인터넷정보학회

주관 제주대학교

후원 네이버(주), (주)아이티센, (주)LGCNS,
(주)큐브시스템, LG히다씨(주), (주)워드바이스에세이리뷰



D-1-3 전해수생성기의 스케일제거 알림	133
권윤중(세명대)	
D-1-4 Wi-Fi 및 RFID 후방 산란을 이용한 모바일 RFID 판독기 및 CRFID 센서 태그 프로토콜	135
백승구, 이태진(성균관대)	
D-1-5 Fog Cloud Network 기반 데이터 처리 시스템 설계	137
손수락, 이병관(가톨릭관동대), 정은희(강원대)	
D-1-6 자율차량을 위한 OBDL(Optimized Back-propagation based Deep Learning) 알고리즘 설계 ...	139
정이나, 이병관, 손수락, 김경덕(가톨릭관동대)	
D-1-7 시각 장애인을 위한 경량화 된 스마트 지팡이	141
정재엽, 정진웅, 염상길, 추현승(성균관대)	
 D-2. IoT 2 / 인터넷교육및응용 (좌장: 서영균 교수(경북대))	
D-2-1 스마트폰 통제 IoT 플랫폼	145
원경필, 정진웅, 염상길, 추현승(성균관대)	
D-2-2 스마트시티 인프라 구축현황 분석 및 사이버보안 고려사항 연구	147
송진우, 김효빈, 홍기섭, 서정택(순천향대)	
D-2-3 ZigBee 프로토콜 취약점 및 보안 요구사항 분석	149
조정석, 곽진(아주대)	
D-2-4 정신 질환 환자를 위한 쉬운 런치 패드	151
장종권, 안효훈, 염상길, 추현승(성균관대)	
D-2-5 SIMD 기반의 IoT 디바이스 인증 프로토콜 설계에 관한 연구	153
최슬기, 곽진(아주대)	
D-2-6 개방형 교육 플랫폼 기반 학습 프로세스 마이닝 및 애널리틱스 기술 연구	155
김현아, 김광훈(경기대)	

ZigBee 프로토콜 취약점 및 보안 요구사항 분석

조정석*, 곽 진**

*아주대학교 컴퓨터공학과 정보보호응용및보증연구실

**아주대학교 사이버보안학과

e-mail : *jsjo.isaa@gmail.com, **security@ajou.ac.kr

ZigBee Protocol Vulnerability and Security Requirements Analysis

Jeong-Seok Jo*, Jin Kwak**

*ISAA Lab., Department of Computer Engineering, Ajou University

**Department of Cyber Security, Ajou University

요 약

IoT 제품에 활용되는 통신 프로토콜은 다양하다. 그 중 ZigBee는 IoT 환경에 맞추어 최소한이지만 안전한 보안 기능들이 적용되어 효율적으로 사용되고 있다. 하지만 최근 ZigBee 프로토콜의 취약점을 제시하고, 각 취약점들을 분석한 연구가 다수 진행되고 있다. 본 논문에서는 취약점을 제시한 다양한 연구를 분석하고 ZigBee 프로토콜의 보안 요구사항을 분석하여 ZigBee 프로토콜의 안전성을 향상시키고자 한다.

1. 서 론

최근 IoT 기기가 등장함에 따라 IoT 환경에 적합한 무선 네트워크 기술이 개발되었다. IoT 환경에서 사용하는 무선 네트워크는 디바이스의 인터넷 연결을 기반으로 통신하는 IP 프로토콜이 아닌 비 IP 디바이스 통신인 ZigBee, Z-wave 등을 활용한다[1].

비 IP 디바이스 통신 프로토콜 중 ZigBee의 취약점에 대한 연구가 활발히 진행되고 있다. ZigBee 프로토콜 또한 기존의 IP 프로토콜과 같이 보안을 위한 기능이 존재한다. 하지만 IoT 환경은 가용성을 위해 높은 수준의 보안 기능을 제공하지 않으므로 이에 대한 취약점이 존재할 수 있다.

본 논문의 구성은 다음과 같다. 2장에서 본 논문과 관련하여 ZigBee 프로토콜의 보안구조와 취약점에 대해 살펴보고, 3장에서 ZigBee 프로토콜의 보안 요구사항을 분석한다. 마지막으로 4장에서 결론을 맺는다.

2. 관련 연구

2.1 ZigBee 프로토콜 보안 구조

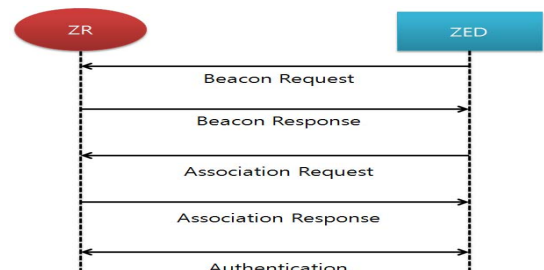
ZigBee 프로토콜의 구성요소로는 ZigBee Coordinator(ZC), ZigBee Router(ZR), ZigBee End Device(ZED)로 구성된다. ZC는 ZigBee 네트워크에서 하나만 존재하고 네트워크제어, 데이터 수집 등의 기능을 수행한다. ZR은 ZED의 데이터를 수집 및 전송하는 기능을 수행한다. ZED는 데이터를 전송하는 역할을 수행하고, ZC 또는 ZR과 통신한다. 이 중 키 관리를 담당하는 구성요소는 ZC이며, ZC에 존재하는 Trust Center(TC)가 ZigBee 네트워크의 전반적인 키 관리 역할을 수행한다[2].

ZigBee 프로토콜은 물리(PHY) 계층과 매체접근제어(MAC)

계층을 기반으로 구성되며, 두 계층 모두 IEEE 802.15.4 표준을 바탕으로 서비스를 제공한다. PHY 계층은 통신설정을 기준으로 데이터를 전송하는 역할을 수행하고 MAC 계층은 보안 서비스를 제공하는 역할을 수행한다.

ZigBee 프로토콜의 키 전달 과정에서 키를 확보할 수 있는 방법은 총 3가지이며, Key-transport, Key-establishment, Pre-installation 방법이다. ZigBee 프로토콜은 키 전달 과정에서의 취약점이 존재한다. ZigBee 프로토콜의 3가지 방식 중 Key-transport는 무선통신을 통하여 키를 전달 받는 방식이다. 해당 방식은 전달 과정에서 암호화가 수행되지 않으므로 키 노출이 가능하다. Key-establishment는 서로 신뢰성 확인을 위해 주고받은 정보들을 이용해 새로운 키를 만들어내는 방법이다. 마지막으로, Pre-installation은 미리 디바이스 안에 키를 입력해놓는 방식이다[3].

ZigBee 프로토콜에서 ZED가 네트워크에 연결되기 위해 ZR과 ZED의 인증과정을 거친다. 해당 과정은 비콘(Beacon)을 이용해 이루어진다. ZR과 ZED의 인증과정은 그림 1과 같다[2].



(그림 1) ZigBee 인증 과정

2.2 ZigBee 프로토콜 취약점 분석

□ 키 전달 과정 취약점

Pre-installation은 키가 미리 저장되어 있어 키 전달과정에서의 유출가능성이 적고, Key-establishment는 기존에 입력된 키를 이용해 새로운 키 생성을 위한 정보들을 암호화하여 보

본 연구는 과학기술정보통신부 및 정보통신기술진흥센터의 대학ICT연구센터육성 지원사업의 연구결과로 수행되었음 (IITP-2018-2015-0-00403)

내어 유출가능성이 적다. 하지만 Key-transport는 키 전송과정에서의 공격자의 개입이 있을 경우 키 유출 가능성이 존재한다[2].

□ ZigBee 프로토콜 인증 취약점 분석

ZigBee 프로토콜은 공격자가 ZC인 것처럼 위장하여 ZED의 연결을 유도하고 ZED가 송신하는 데이터들을 수신함으로써 ZED의 데이터손실을 발생시키는 공격이 가능하다. 해당 공격은 공격자가 ZigBee에서 사용하는 16개의 모든 채널을 도청하여 ZC의 채널을 파악한 뒤, 패킷의 일부분을 암호화하는 ZigBee 프로토콜의 취약점을 이용해 공격을 수행한다. 공격자가 사용가능한 정보들은 아래의 표 1과 같다. 공격자는 이러한 정보를 이용해 ZC인 것처럼 위장하여 ZED와의 성공적인 연결 프로세스를 수행한다. ZED가 ZC로 위장한 공격자와 연결된 후 데이터를 송신할 경우 정상적인 ZC로 데이터를 송신하지 않기 때문에 결과적으로 데이터 손실이 발생한다[4].

(표 1) ZC 위조를 위해 활용되는 정보

항목	내용
Sequence number	- ZC처럼 위장한 후 Beacon Response 전송에 사용
ZC의 MAC Address	- ACK 위조 시 사용
Beacon Reponse	- ZED와의 연결을 위해 사용 - 'Sequence number + 1'을 수행하여 전송
Association Reponse (ACK)	- ZC의 MAC Address 등의 획득한 네트워크 정보로 구성하여 전송

ZigBee 프로토콜 키 전달 과정에서의 취약점은 3번째 키 전달 과정인 Pre-installation을 통해 안전성을 보장할 수 있다. 3번째 키 전달 과정 적용을 통해 위의 공격 시나리오에 대한 대응 방안 제시가 가능하다.

ZC 인증을 위해 ZED와 ZC는 시도-응답을 수행한다. 시도-응답 수행을 위해 coordinator identity challenge, coordinator identity response 2가지의 메시지 타입이 요구된다. 이 값들은 페이로드로 사용될 랜덤한 N-byte의 값을 암호화한 결과 값으로 구성된다[4]. 우선 ZED가 coordinator identity challenge를 ZC에 전송하고, ZC는 해당 값을 복호화하고 간단한 비트 연산을 수행한 값을 암호화하여 coordinator identity response를 전송한다. ZED는 해당 값을 검증하여 ZC에 대한 인증을 수행한다. 결과 값 검증을 수행하여 실패할 경우, 해당 네트워크를 떠나고 새로운 ZC를 찾는다. 검증이 성공적으로 수행될 경우, 통신이 진행된다[4].

□ ZigBee 프로토콜 데이터 손실 취약점 분석

데이터 손실 방지를 위해 캐시를 활용한 방안이 제안된다. ZED는 데이터 손실 방지를 위해 적은 크기의 자유 메모리를 확보하고, 해당 메모리는 마지막으로 전송된 메시지 캐시 유지에 사용된다. 이러한 캐시는 가득 차게 될 경우, 앞서 수행한 시도-응답을 다시 수행하여 ZC에 대한 인증을 다시 수행하게 된다. 응답이 타당할 경우, 캐시를 비우고 아닐 경우 캐시를 유지하고 타당한 응답이 오는 ZC에 ZED는 연결을 하고 새 데이터 전송 전에 캐시의 모든 데이터 전송하는 방법을 통해 데이터 손실을 방지한다[4].

3. ZigBee 보안 요구사항 분석

□ ZigBee 프로토콜 키 전달 과정

키 전달 과정에서의 취약점 보안을 위해 ZC와 ZED의 개선된 키 전달 과정이 요구된다. 2.1절에서 언급된 키 전달 과정 중 Pre-installation이 가장 안전하지만 ZED가 개발되는 과정에서 키가 미리 설정되는 것 또한 위험할 수 있다. 회사 별로 설정되는 키 생산 방식이 공개되거나 키 생산 방식의 규칙이 존재하게 된다면 미라이 봇을 이용한 공격과 같은 원리처럼 공격자가 다량의 ZED를 확보하여 봇넷을 구성하는 것과 같은 Pre-installation 키 전달 방법의 새로운 문제가 발생하게 된다. 이러한 키 전달 방법 문제 방지를 위해 Pre-installation 적용 기기들의 안전한 키 생성이 보장되거나, 새로운 키 전달 과정이 연구되어야 한다.

□ ZigBee 프로토콜 인증

시도-응답을 이용한 인증방식 또한 취약점이 존재한다. 2.2절에서 언급된 대응방안 또한 시도-응답의 재전송 공격에 대한 취약점과 MAC 계층에서의 인증에 대한 문제점이 존재한다. 앞서 2.2절에서 언급된 시도-응답을 이용한 인증은 공격자가 해당 값을 이용해 재전송 공격을 수행할 경우 공격자의 ZC 위조를 방지할 수 없을 것이다. 그리고 시도-응답에서 사용되는 난수 생성에 대한 안전성 또한 IoT 기기의 제한된 환경에서 보장되어야 할 것이다. 또한 앞서 진행된 Pre-installation의 취약점을 이용해 공격자가 키를 가지고 있다면 공격은 더 쉽게 수행될 것이다. 이러한 취약점 대응을 위해 IoT 환경에서 주로 사용되는 ZigBee 프로토콜의 키 전달 과정과 인증 방식 개선이 요구된다.

4. 결론

본 논문을 통해 ZigBee 프로토콜의 키 전달 과정의 취약점과 데이터 손실의 취약점을 제시한 논문을 분석하여 ZigBee 프로토콜 개선의 필요성을 강조하였다.

ZigBee 프로토콜의 기본 키 전달 방식을 분석하고, 그에 대한 취약점을 제시하고 공격 가능성을 언급하였다.

또한 ZigBee 프로토콜의 취약점을 이용한 공격시나리오를 제시한 논문 분석을 통해 대응방안을 파악하였다. 그리고 대응방안에 대한 추가적인 취약점을 제시하였고, 앞서 언급한 키 전달 과정의 취약점과의 연관성을 통해 ZigBee 프로토콜의 보안의 관점에서 전반적인 개선점이 필요하다는 것을 파악할 수 있다.

향후 ZigBee 프로토콜에서의 인증 및 키 교환방식에 대한 개선방안을 연구할 예정이다.

참고문헌

- [1] 한국방송통신전파진흥원, “무선 센서 네트워크 기반 IoT를 위한 통신 기술”, 2014.
- [2] 김봉환, 임정미, 박창섭, “ZigBee 보안 메커니즘 분석”, 보안공학연구논문지, 제 9권 제 5호, 2012.
- [3] ZigBee Alliance “ZigBee Specification Document 053474r20”, 2012
- [4] Spencer Michaels, Kemal Akkaya, A. Selcuk Uluagac, “Inducing Data Loss in Zigbee Networks via Join/Association Handshake Spoofing”, CNS IEEE, 2016.