

2018년 한국정보보호학회 하계학술대회

CISC-S'18

Conference on Information Security
and Cryptography 2018 Summer

2018. 6. 21일(목) ~ 6. 22일(금)
동신대학교 중앙도서관 1층 동강홀(전남 나주시)

- > 주 최 : 한국정보보호학회
- > 주 관 : 동신대학교
- > 후 원 : 국가정보원, 네이버, 교육부, 한국연구재단,
한국전력공사, 전력거래소,
한국인터넷진흥원, 국가보안기술연구소,
한전KPS(주), 한전KDN(주),
한국방송통신전파진흥원



한국정보보호학회

Korea Institute of Information Security & Cryptology

프로그램 일정표

날짜	시간	행사내용	비 고
6월 21일 (목)	11:30 ~ 13:00	등록 및 리셉션 (중앙도서관 1층)	
		세션 A - 정보전산센터	
	13:00 ~ 14:20	암호화폐/ 블록체인1 좌장:허준범 (고려대학교) 네트워크1 좌장:최대선 (공주대학교) 암호이론1 좌장:한동국 (국민대학교) IoT보안1 좌장:강승호 (동신대학교) 관리정책 교육1 좌장:김태희 (동신대학교) 컴퓨터보안1 좌장:이만희 (한남대학교) 개인정보보호 좌장:신상욱 (부경대학교) CPS보안 좌장:서정택 (순천향대학교)	
	14:20 ~ 14:30	Break Time	
		세션 B - 정보전산센터	
	14:30 ~ 16:10	암호화폐/ 블록체인2 좌장:임을규 (한양대학교) 네트워크2 좌장:김광조 (카이스트) 암호이론2 좌장:이동훈 (고려대학교) IoT보안2 좌장:이임영 (순천향대학교) 관리정책 교육2 좌장:이경현 (부경대학교) 취약점분석 좌장:박창섭 (단국대학교) 산업보안 좌장:오희국 (한양대학교) 악성코드 좌장:하재철 (호서대학교)	
	16:10 ~ 16:20	Break Time	
	16:20 ~ 16:50	초청강연 : Post Quantum Crypto 표준화 추진 현황 및 KISA의 역할(한국인터넷진흥원)	
	16:50 ~ 17:00	특별강연 : 연구 윤리 및 출판	
	17:00 ~ 17:30	중 앙 도서관 1층 동강홀 개회식 / 사회 : 운영위원장 이동휘 교수 개회사 동신대학교 김필식 총장 환영사 한국정보보호학회 홍만표 학회장 축 사 한국인터넷진흥원 김석환 원장 국가보안기술연구소 조현숙 소장 한국전력공사 김종갑 사장 우수논문 시상식 행안부 장관상, 한국인터넷진흥원장상, 한국전력공사사장상, 한국전자통신연구원장상, 국가보안연구소장상, 학회장상(암호분야 특별상), 학회장상, 여성과학자상	
	17:30 ~ 18:00	경품추천	
	18:00 ~ 20:00	이동	
		만찬 : 빚가람 호텔 만찬홀 (구:M-STAY Hotel) : 사회 서정택 교수	
6월 22일 (금)	10:00 ~ 10:30	등록 (정보전산센터 1층)	
		세션 C - 정보전산센터	
	10:30 ~ 11:50	암호화폐/ 블록체인3 좌장:유일선 (순천향대학교) 암호화폐/ 블록체인4 좌장:현상원 (조선대학교) 관리정책 교육3 좌장:김인식 (고려대학교) 관리정책 교육4 좌장:장항배 (중앙대학교) 컴퓨터보안2 좌장:서승현 (한양대학교) 여성과학자 + invited talk 좌장:심미나 (성결대학교) 기 타 좌장:이옥연 (국민대학교)	26개 논문 한국전력 공사 견학
	12:00 ~ 13:00	중식(교직원식당)	중식 (한전구내식당)
	13:00 ~ 14:30		한국전력거래소 견학
	14:30 ~ 16:00		한국인터넷 진흥원 견학
	16:00 ~ 16:30	KTX, SRT 나주역 이동 후 종료	

구두 발표 세션 A

6월 21일(목) 13:00-14:20 정보전산센터

208호	발표 논문
암호화폐/ 블록체인 1	블록체인 기반 분산형 키 관리 시스템의 설계 안형철, 김광조
	분기로 발생한 미확인 트랜잭션의 우선적인 처리기법 박승운, 오희국
	블록체인 기반 디지털증거 해시 관리 시스템 구현 정재완
	암호화폐 키 관리에 의한 보안 사고 및 대응방안 연구 김근영, 박준후, 오원찬, 류재철
좌장: 허준범 교수 (고려대학교)	
303호	발표 논문
네트워크 1	스마트 계약 언어에서 함수 호출의 안전성 향상을 위한 코드 재작성 기법 이수연, 정형근, 조은선
	6LoWPAN Neighbor Discovery 주소 등록 분석 및 취약점 평가 한상우, 박창섭
	웹 크롤링을 이용한 교통정보 수집 기법 박세진, 윤지원
	ZigBee 프로토콜에서의 향상된 인증 방안에 관한 연구 조정석, 광진
좌장: 최대선 교수 (공주대학교)	
304호	발표 논문
암호이론 1	진난수생성기에 대한 부채널 공격 및 난수성 분석 사례 조사 최낙준, 이지은, 김광조
	중첩된 무한 해시체인을 이용한 Lamport OTP 확장 신동진, 박창섭
	Linux OS 상에서의 커널 및 응용 LEA 암호모듈 구현 및 호출 분석 송행권
	Survey of Functional Encryption and its Functionality 윤현도, 권현수, 허준범
좌장: 한동국 교수 (국민대학교)	
305호	발표 논문
IoT보안 1	스마트 시계 활용 무자각 지속 인증 강화 연구 류권상, 옥도민, 최대선
	라즈베리 파이를 이용한 휴대용 영상감시시스템 개발 최경호, 김현진, 현부영, 김종민, 이동휘
	LR Guard: ARM TrustZone을 활용한 제어 흐름 보호 기법 설계 진홍주, 장혜린, 이동
	IoT 기반의 스마트 홈 보안 동향 박정인, 이가연, 윤현경, 엄홍열
좌장: 강승호 교수 (동신대학교)	

2018 한국정보보호학회 하계학술대회

A2 네트워크 1

Ⅱ 최 대 선 (공주대학교) Ⅱ

- 스마트 계약 언어에서 함수 호출의 안전성 향상을 위한 코드 재작성 기법
이수연, 정형근, 조은선
- 6LoWPAN Neighbor Discovery 주소 등록 분석 및 취약점 평가
한상우, 박창섭
- 웹 크롤링을 이용한 교통정보 수집 기법
박세진, 윤지원
- ZigBee 프로토콜에서의 향상된 인증 방안에 관한 연구
조정석, 곽 진

ZigBee 프로토콜에서의 향상된 인증 방안에 관한 연구

조정석*, 곽진**

*아주대학교 컴퓨터공학과 정보보호응용및보증연구실,

**아주대학교 사이버보안학과

Improved Authentication Method in ZigBee Protocol

Jeong-Seok Jo*, Jin Kwak**

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

**Department of Cyber Security, Ajou University

요약

다양한 IoT 통신 프로토콜들 중 ZigBee 프로토콜은 제한적인 IoT 환경에 맞추어 보안 서비스를 제공하고 있다. 하지만 최근 ZigBee 프로토콜의 취약점을 분석하고 제시하는 연구가 다수 진행되고 있다. 본 논문에서는 ZigBee 프로토콜의 인증 과정에서의 취약점을 분석하고 개선 사항을 제시함으로써 ZigBee 프로토콜의 인증 방식을 향상시키고자 한다.

I. 서론

최근 무선 네트워크 기반 IoT 기기들의 취약점에 대한 연구가 활발히 진행되고 있다. IoT 기기들이 무선 통신을 위해 사용하는 기술에는 Z-wave, ZigBee, KNX-RF, Bluetooth 등이 있으며, 이러한 기술들의 효과적인 활용을 위해 IEEE 802.15.4 표준이 제정되었다[1].

ZigBee는 IEEE 802.15.4의 물리(PHY), 매체 접근 제어(MAC) 계층의 기능을 기반으로 동작하며, ZigBee 표준에서 정의된 NWK(네트워크) 계층과 APL(애플리케이션) 계층을 더한 형태로 구성된다[2].

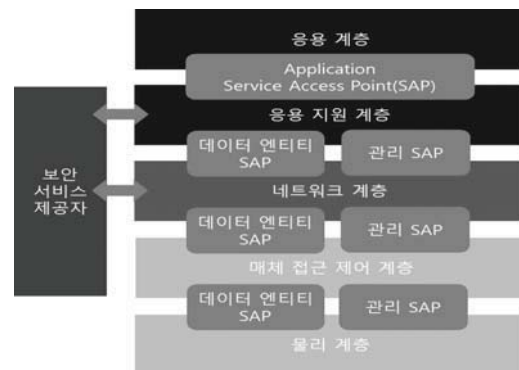
이러한 ZigBee 스택구조를 바탕으로 ZigBee 프로토콜의 인증 과정에서 Address Spoofing 취약점이 존재한다. 또한 ZigBee 프로토콜에서의 재인증을 위한 시도-응답 과정에서의 재전

송 취약점 또한 존재한다.

본 논문에서는 Address Spoofing의 피해를 줄이고, 인증의 효율성을 높일 수 있는 방법을 제시하고 기기 재인증 과정에서의 시도-응답 재전송공격 방지를 위한 시도-응답 과정을 제시하고자 한다.

II. 관련 연구

2.1 ZigBee 프로토콜 스택 구조



(그림 1) ZigBee 프로토콜 스택 구조

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

ZigBee 스택 구조는 (그림 1)과 같다. 해당 구조에서 ZigBee 프로토콜은 응용 계층, 네트워크 계층 그리고 보안 서비스 제공자가 함께 보안 서비스를 제공한다. 특히 해당 계층들에서 보안에 필요한 키들(마스터 키, 링크 키, 네트워크 키)에 관한 정보들이 저장되어 있다[2].

ZigBee 프로토콜은 ZigBee Coordinator(ZC), ZigBee Router(ZR), ZigBee End Device(ZED)로 구성된다. ZC는 ZigBee 네트워크에서 하나만 존재하고 네트워크제어의 기능을 수행한다. ZR은 ZED의 데이터를 수집 및 전송하는 기능을 수행한다. ZED는 데이터를 전송하는 역할을 수행하고, ZC 또는 ZR과 통신한다[3].

2.2 ZigBee 프로토콜 키 생성 및 인증 과정

ZigBee 프로토콜 키 생성 및 인증 과정은 (그림 2)와 같다. 해당 방식은 ZED가 미리 마스터 키를 가지고 있다고 가정한다. ZigBee에서는 SKKE(Symmetric-Key Key-Establishment) 프로토콜을 기반으로 키를 생성한다. 앞서 언급한 마스터 키와 랜덤하게 생성한 QEU, QEV 값들을 이용하여 링크 키를 생성한다. 생성한 링크 키를 이용해 인증을 수행한다. 인증 과정은 아래와 같다[4].

Step 1. Association Request(ZED→ZR)

ZED가 ZR에게 연결을 요청한다.

Step 2. Association Response(ZR→ZED)

ZR이 ZED의 연결 요청에 대한 응답을 전송한다.

Step 3. Update-Device(ZR→ZC)

기기 목록 갱신을 위해 ZC에게 Update-device 전송한다.

Step 4. SKKE-1(ZC→ZED)

생성한 임의의 값 QEU를 ZED에게 전송한다.

Step 5. SKKE-2(ZED→ZC)

SKKE-1를 수신한 뒤, 생성한 임의의 값 QEV를 ZC에게 전송한다.

Step 6. SKKE-3(ZC→ZED)

ZC는 확보한 QEV의 값으로 $MacTag_2$ 를 생성하여 전송한다.

$$MacData_2 = 03_{16} V || U || QEU || QEV$$

$$MacTag_2 = MAC_{MasterKey}(MacData_2)$$

Step 7. SKKE-4(ZED→ZC)

ZED는 $MacTag_1$ 을 구성하여 전송한다.

$$MacData_1 = 02_{16} V || U || QEU || QEV$$

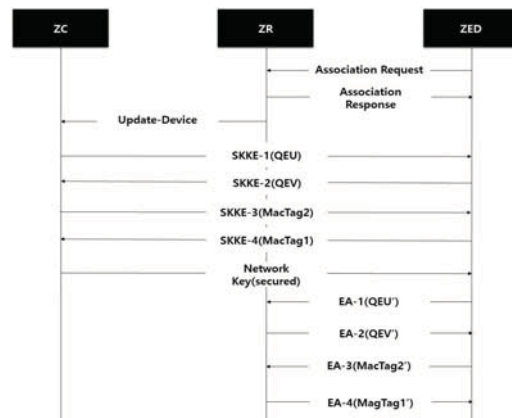
$$MacTag_1 = MAC_{MasterKey}(MacData_1)$$

Step 8. Network Key(secured)

$MacTag_1$, $MacTag_2$ 를 이용해 생성한 링크 키를 이용해 네트워크 키를 전송한다.

Step 9. EA-1 ~ EA-4

SKKE와의 동일한 원리로 ZR과 ZED의 인증을 수행한다.



(그림 2) ZigBee 프로토콜 인증 과정

2.3 시도-응답 인증 방식

시도-응답을 통한 인증 방식은 (그림 3)과 같다. 해당 방식은 난수와 대칭키를 이용하여 상호 인증을 수행하는 방식이다. 수행 과정은 아래와 같다[5].

Step 1. Challenge(ZC→ZED)

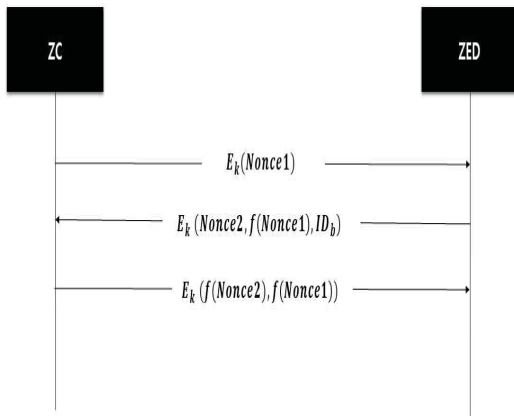
ZC가 ZED에게 생성한 난수를 암호화 ($E_k(Nonce1)$)하여 전송한다.

Step 2. Response(ZED→ZC)

ZED가 생성한 난수, 수신한 난수의 비트 연산 결과 값 그리고 ID를 ZC에게 암호화하여 전송한다. ($E_k(Nonce2, f(Nonce1), ID_B)$)

Step 3. 비트 연산 수행(ZC→ZED)

비트 연산 결과 값들을 암호화하여 전송한다. ($E_k(f(Nonce2), f(Nonce1))$)



(그림 3) 시도-응답 과정

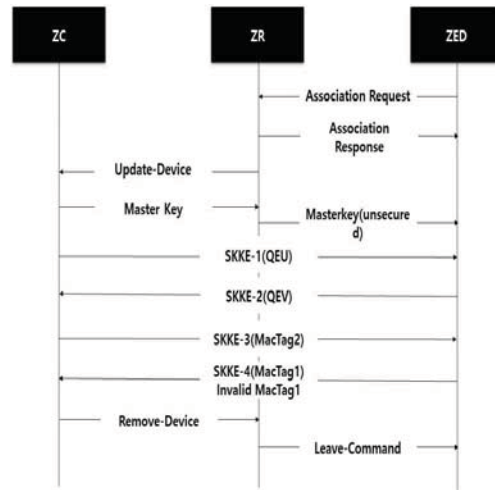
2.4 ZigBee 프로토콜 취약점

□ ZigBee 인증 과정 자원 고갈 취약점

우선 ZigBee의 인증 과정에서 ZC는 ZED가 마스터키 소유 여부를 알 수 없으므로 공격자가 Address Spoofing 공격을 이용해 자원 고갈이 발생할 수 있다. 공격 방식은 (그림 4)와 같다.

기존의 인증 방식으로 진행할 경우 SKKE-4의 프레임에서 ZED는 마스터 키를 모르기 때문에 정상적인 MacTag1를 구성할 수 없기 때문에 ZC는 SKKE-4 값에 대한 검증이 불가능하므로 Remove-Device 과정을 수행한다.

하지만 이러한 과정 또한 ZR-ZC의 자원 낭비를 초래한다. 그 결과, 자원 고갈 공격이 성립하게 된다.



(그림 4) ZigBee 자원 고갈 공격

□ 시도-응답 재전송 공격

ZigBee 프로토콜 기기 간 재인증 과정에서 시도-응답을 수행할 때 기존의 사용된 값들을 재전송하여 재인증을 수행할 수 있다.

III. 제안사항

3.1 ZigBee 프로토콜 인증 개선 방안

기존의 ZC, ZR, ZED의 인증 방식을 개선한 인증 방식은 (그림 5)와 같다. 해당 방식은 ZED가 미리 마스터 키를 가지고 있다고 가정한다.

Step 1. ~ Step 3.의 과정은 기존의 인증 과정과 동일하다.

Step 4. SKKE-1(ZC→ZED)

기존의 방식과 달리 생성한 QEU를 마스터 키로 암호화($E_{MK}(QEU)$)하여 ZED에게 전송한다.

Step 5. SKKE-2(ZED→ZC)

생성한 QEV와 SKKE-1에서 복호화하여 얻은 QEU 그리고 (QEU, QEV)를 이용하여 생성한 MacTag1을 전송한다.

Step 6. SKKE-3(ZC→ZED)

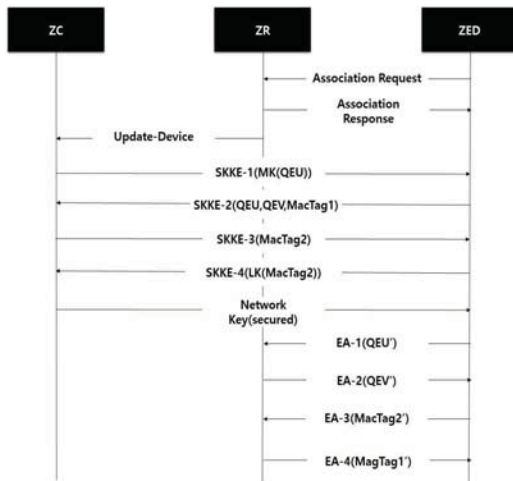
ZC는 확보한 QEV의 값으로 MacTag2를 생성하여 전송한다.

Step 7. SKKE-4(ZED→ZC)

ZED는 생성한 링크 키를 이용해 MacTag2를 암호화($E_{LK}(MacTag2)$)하여 전송한다.

Step 8. 의 과정은 기존의 인증 과정 Step 9. 과 동일하다.

위에 제시한 방안을 통해 앞서 제시한 취약점에 대한 대응이 가능하다. 우선, 지속적인 인증 시도를 통한 에너지 고갈 취약점에 대응하여 ZC, ZR의 에너지 효율을 증가시킬 수 있다. SKKE-2 과정에서 MacTag1 값과 QEU 값에 대한 검증을 통해 ZED에 대한 우선적인 검증이 가능하다. 또한 SKKE-4 과정을 통해 생성된 링크 키에 대한 검증이 가능하다.



(그림 5) ZigBee 인증 개선 방안

3.2 시도-응답 개선 방안

IoT 환경에서 인증을 위해 주로 수행하는 방법은 시도-응답이다. 하지만 기존의 시도-응답의 과정에서 공격자가 ZED로 위장했을 경우, 그에 대한 재인증을 위해 시도-응답을 수행할 경우 이전에 사용된 난수를 재전송하여 인증을 수행하는 공격이 수행 가능하다. 이에 대해본 절에서는 IoT 기기의 캐시를 이용하여 기존의 시도-응답 방안의 재전송 공격 방지를 위한 개선 방안을 제시한다. 시도-응답 개선방안은 (그림 6)과 같다.

개선된 시도-응답 수행 과정은 아래와 같다.

Step 1. Challenge(ZC→ZED)

ZC가 ZED에게 생성한 난수를 암호화($E_k(Nonce1)$)하여 전송한다.

Step 2. Response(ZED→ZC)

ZED가 생성한 난수, 수신한 난수의 비트 연산 결과 값 그리고 ID, TimeStamp값을 ZC에게 암호화하여 전송한다.

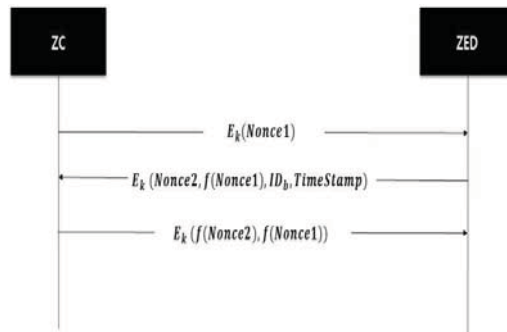
$(E_k(Nonce2, f(Nonce1), ID_B, TimeStamp))$

Step 3. 비트 연산 수행(ZC→ZED)

ZC는 수신한 값들을 점검하여 비트 연산 결과 값을 암호화하여 전송한다.

$E_k(f(Nonce2), f(Nonce1))$

해당 개선 사항을 통해 기가 간 재인증 취약점을 개선할 수 있다.



(그림 6) 시도-응답 개선 방안

3.3 개선 방안

제시한 개선 방안을 정리한 표는 [표 1]과 같다.

[표 1] 개선 사항

	기존 방식	개선 방안
ZigBee 자원 고갈 취약점	- SKKE-4에서의 마스터 키 검증을 통한 자원 효율 감소 - 링크 키 검증 수행하지 않음	- SKKE-1에서의 마스터 키 검증을 통한 자원 효율 향상 - SKKE-4를 통한 링크 키 검증 수행
시도-응답 재전송 공격	- 재전송 공격의 취약점 존재	- 타임스탬프를 활용한 재전송 공격 방지

IV.결론

본 논문을 통해 ZigBee 프로토콜의 인증 과정과 시도-응답 과정을 분석하고 각각의 취약점을 제시하여 프로토콜 개선의 필요성을 강조하였다.

ZigBee 프로토콜 인증 과정의 자원 고갈 취약점 개선을 위한 인증 과정을 제안하였다. 해당 개선 사항은 ZC는 ZED의 마스터 키와 링크 키 검증을 통해 ZED에 대한 인증이 가능하도록 제안하였다.

또한 시도-응답 개선 사항을 통해 시도-응답에 사용되는 값들의 재전송 여부 탐지를 위한 개선사항을 제안하였다.

향후 ZigBee 프로토콜에서의 인증 방식의 전반적인 개선방안을 연구할 예정이다.

[참고문헌]

- [1] Stefan Marksteiner, "An Overview of Wireless IoT Protocol Security in the Smart Home Domain", 2017
- [2] ZigBee Alliance, ZigBee Specification: ZigBee Document 053474r20, September, 2012.
- [3] 김봉환, 임정미, 박창섭, "ZigBee 보안 메커니즘 분석", 보안공학연구논문지, 제 9권 제 5호, 2012
- [4] Moazzam Khan, "The Cost of Security: Performance of ZigBee Key Exchange Mechanism in an 802.15.4 Beacon Enabled Cluster", 2007
- [5] Mohammad A. Alia, "Cryptography Based Authentication Methods", 2014