

IoT 환경에서 Z-WAVE 기반의 향상된 키 교환 프로토콜 연구

송경환*, 최슬기*, 송진희**, 전문석*
*송실대학교 컴퓨터학과
**신한대학교 IT 융합공학부
e-mail : mainevent34@ssu.ac.kr
seulgi.choi@ssu.ac.kr
jhsong@shinhan.ac.kr
mjun@ssu.ac.kr

A Study of Improved Key Exchange Protocol Based on Z-WAVE in IoT Environment

Kyung-Hwan Song*, Seulgi Choi*, Jin-Hee Song**, Moon-Seog Jun*
*Dept of Computer Science, Soongsil University
**School of IT Convergence Engineering, Shinhan University

요 약

IoT(Internet of Thing) 환경이 도래하면서 다양한 무선 통신 기술들이 사용되고 있다. 그 중에서 가장 많이 쓰이는 무선 통신 기술은 Z-WAVE 이다. Z-WAVE 는 저전력, 양방향 RF 등의 장점을 가지며, 세계 스마트 홈 시장에서 가장 폭 넓게 사용되는 기술이다. 이 기술을 채택한 연합을 Z-WAVE 연합이라고 하는데, 이 연합은 수백 개 이상의 제조사들과 1000 개 이상의 활성화 된 제품을 가지고 있다. 하지만 Z-WAVE 는 중간자 공격 등과 같은 보안성의 취약점을 가지고 있으며 아직까지 연구가 부족한 실정이다. 따라서 본 논문에서는 IoT 환경에서 Z-WAVE 기반의 향상된 키 교환 프로토콜 기법을 제안한다.

1. 서론

IoT 환경이 가정, 의료, 자동차 등의 생활 속으로 점차 확산되고 있다. IoT 는 스마트 홈, 스마트 카 등과 같은 환경과 같이 인간과 사물, 서비스 등 분산된 요소들 간에 인위적인 개입이 없이 상호 협력적으로 지능적 관계를 형성하는 사물 공간 연결망을 의미한다[1]. IoT 환경에는 다양한 통신 기술들이 쓰이지만 자주 쓰이는 기술 중 하나가 바로 WPAN(Wireless Personal Area Network)이다. WPAN 는 IEEE 802.15.3a(고속 UWB), 지그비(Zigbee), WiMedia, Z-WAVE 등의 기술이 있다. WPAN 기술 중 최근 주목 받고 있는 기술은 Z-WAVE 로 장점으로 저전력, 양방향 RF, 매쉬 네트워킹 기술 등의 장점을 가지고 있다[2]. 이러한 Z-WAVE 의 장점 때문에 많은 제조사들이 컨소시엄을 맺어 Z-WAVE 얼라이언스라는 컨소시엄을 설립하였다. 또한 스마트 홈 환경에서 Z-WAVE 제품이 1000 개 가까이 사용되어 향후에도 계속 전망이 높은 기술이다. 스마트 홈이란 사람들에게 편리한 주거 생활을 제공하는 것에 목적을 두고 있다. 스마트 홈은 지능형 주택으로 가정의 디바이스들을 네트워크를 통해 원격 모니터링 및 제어가 가능하게 한다[3]. 스마트 홈 환경에서 Z-WAVE 기술을 이용한 서비스 사례로는 미국 AT&T 사의 'Digital Life'가 있으며, 프랑스의 Orange 사

는 'Home Live' 서비스를 출시하였다[4]. 하지만 세계에서 가장 저명한 해킹 컨퍼런스인 'Black Hat USA(2013 년)' 과 DefCon 에서 Z-WAVE 무선 기술을 사용하는 스마트 홈 환경에서 취약점을 악용하는 것을 시연하였다. 이로 인해 많은 사람들이 Z-WAVE 기술이 안전하지 않다는 것을 인지하였다.

기존의 Z-WAVE 프로토콜은 컨트롤러와 슬레이브가 서로 인가된 디바이스인지 확인하는 부분이 부족한 취약점을 가지고 있다. 이로 인해 Z-WAVE 네트워크에 공격자가 인가된 디바이스로 가장하는 중간자 공격을 시도할 수 있다. 또한 중간자 공격을 통한 2차 피해도 생길 수 있다. 그러므로 본 논문에서는 컨트롤러와 슬레이브간 상호인증의 강화를 통한 중간자 공격 방지 프로토콜을 제안한다.

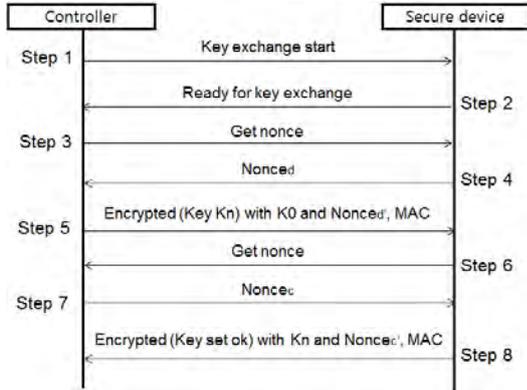
2. 관련 연구

2.1. Z-WAVE 프로토콜

Z-WAVE 프로토콜은 160 개 이상의 제조사들로 이루어진 컨소시엄인 Z-WAVE 얼라이언스에서 공통적으로 사용하는 프로토콜이다. 이 프로토콜은 스마트 홈, 스마트 의료와 같은 다양한 IoT 환경에서 적용된다. 하지만 아직까지 Z-WAVE 얼라이언스는 컨트롤러와 슬레이브간 Z-WAVE 통신의 보안 문서를 비공개

하였다. 그러나 2013 년 미국 라스베가스에서 열린 블랙햇 컨퍼런스에서 보안 컨설턴트 회사인 SensePost 에서 Behrang Fouldai 과 Sahand Ghanoun 이 Z-WAVE 프로토콜의 보안을 분석한 논문을 공개했다[4].

(그림 1)은 Z-WAVE 환경에서 컨트롤러와 슬레이브가 통신 패킷을 전송하기 전에 암호키를 교환하는 절차이다.



(그림 1) Z-Wave 키 교환 절차

먼저 Step1, 2 에서 컨트롤러와 슬레이브간 키 교환을 위한 준비를 한다. Step3, 4 와 Step6, 7 은 컨트롤러와 슬레이브가 nonce 를 서로 교환한다.

Step5 에서 컨트롤러는 임시키 K_0 을 사용하여 네트워크 키 K_n 을 암호화하여, $Nonce_a'$ 값과 메시지 인증 코드를 보낸다. Step8 에서 슬레이브는 컨트롤러에게 Key set ok 메시지를 K_n 키로 암호화하고 $Nonce_c'$ 값과 MAC 값을 함께 보내어 키 교환을 마친다.

하지만 위의 키 교환 프로토콜은 몇 가지 공격에 취약하다. 첫 번째는 중간자 공격으로 슬레이브는 임시키 K_0 을 사용하여 컨트롤러가 보낸 MAC 을 검증하지만, 인가된 컨트롤러인지에 대하여 검증하지 못한다. 두 번째는 키 복구 공격으로 Z-WAVE 환경에서 K_n 키를 전송할 때 기밀성이 결여되면 K_0 키는 잘 알려질 수 있는 문제점을 가진다[5].

컨트롤러와 슬레이브간 키 교환이 끝나면, 패킷을 교환하는 작업이 시작된다.

(그림 2)의 Step1, 2 에서 컨트롤러는 슬레이브에게 nonce 를 요청하고 슬레이브는 컨트롤러에게 $Nonce_a$ 를 송신한다. $Nonce_a$ 를 받은 컨트롤러는 자신도 $Nonce_c$ 를 생성하고 $Nonce_c$ 와 $Nonce_a$ 를 연접한 값인 초기 벡터(IV)를 계산한다. IV 는 nonce 값들로 이루어져 있기 때문에 암호문이 동일하지 않고 매번 달라 CBC 모드에 안전성에 중요한 역할을 한다. IV 를 생성한 컨트롤러는 IV 와 페이로드를 OFB(Output Feedback) 모드로 암호화 한 값인 ENC(P)를 생성한다. ENC(P)를 생성한 컨트롤러는 IV, SH(Security Header), SRC, DST, LEN, ENC(P)를 연접하여 K_m 키를 이용하여 MAC 을 생성한다.

Step3 에서 컨트롤러는 슬레이브에게 SH, IV, ENC(P), MAC 값을 연접해서 전송한다. 메시지를 수신한 슬레이브는 IV 의 마지막 8 바이트가 자신이 생성한

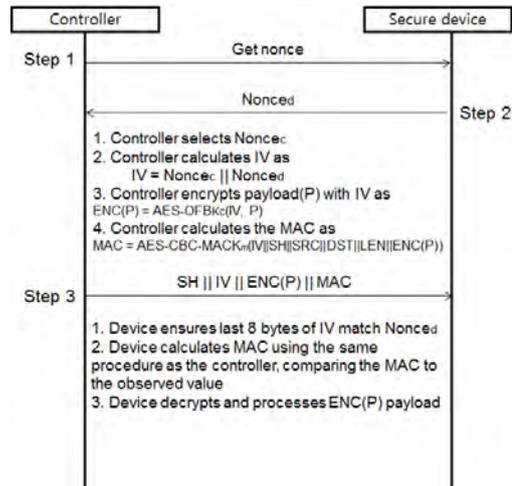
$Nonce_a$ 와 일치하는지 확인한다. IV 를 확인한 슬레이브는 컨트롤러처럼 MAC 을 계산하고 비교한다. 그 이후에 슬레이브는 수신한 데이터를 복호화하여 Z-WAVE 패킷 교환 절차가 끝나게 된다.

하지만 Z-WAVE 의 패킷 교환 프로토콜에서도 취약점이 존재한다. 그것은 바로 Z-WAVE 네트워크에서 사용하는 K_n 키에 있다. 컨트롤러와 슬레이브가 성공적으로 K_n 키를 교환한 후에, 두 장치 모두 프레임 암호화 키인 K_c 와 데이터 원천 인증 키인 K_m 를 다음과 같이 생성한다.

$$K_c = \text{AES-ECB}_{K_n}(\text{Password}_c)$$

$$K_m = \text{AES-ECB}_{K_n}(\text{Password}_m)$$

K_c 키는 ENC(P)를 암호화하고, K_m 키는 MAC 를 생성하는데 쓰인다. 하지만 공격자가 K_n 키를 알게 되면 자연스럽게 K_c , K_m 키를 알 수 있는 취약점이 있다. 또한 Step3 에서 SH, IV 를 암호화를 하지 않고 평문으로 전송하여 공격자에게 쉽게 노출된다.



(그림 2) Z-WAVE 패킷 교환 절차

2.2. 스마트 홈 표준화

최근 구글, 애플과 같은 글로벌 기업들이 IoT 산업에 많은 관심을 가지고 있으며 투자를 하고 있다. 글로벌 기업들이 IoT 산업에서 관심을 보이고 있는 부분은 단연 스마트 홈이다. 이 스마트 홈이 활성화 되기 위해서는 이기종간의 상호운용성을 지원하는 표준이 필요하다. 현재 국내에서는 RS485 통신 프로토콜을 기반으로 한 유선 스마트 홈 표준이 나온 상황이다. 무선 스마트 홈 표준은 올해 하반기에 나오며 16년 5월에 무선기반의 홈 네트워크 기기 제어 서비스 프로토콜 표준을 적용한다.

유선 스마트 홈 표준명은 지능형 홈 네트워크 기기 제어를 위한 RS-485 통신 프로토콜이다. 이 표준은 RS-485 통신 인터페이스에 연결되는 월 패드/홈 게이트웨이와 제어 기기간의 통신규격 및 메시지 기본 포맷을 제공한다. 또한 다양한 스마트 홈 서비스를 제공 하기 위한 데이터 통신 프로토콜을 정의한다.

(그림 3)은 RS-485 통신 프로토콜 구조도이다. (그림 3)에서 홈 게이트웨이는 홈 외부의 인터넷 망과 홈 내의 다양한 통신 방식을 가진 기기들의 상호연동을 보장한다. 표준적용 대상기기로는 가스밸브, 전등, 시스템 에어컨, 방범악장, 도어락, 보일러, 통합집진기, 실내환기 시스템, 온도조절기, 일출자단기, 커튼, 컴퓨터, 홈게이트웨이, 인터넷

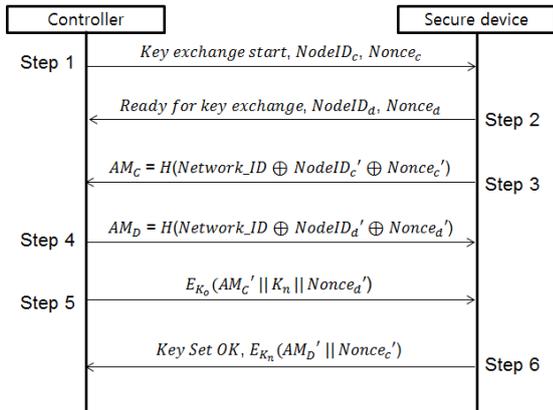


(그림 3) RS-485 통신 프로토콜 구조도

3. 제안 내용

3.1. Z-WAVE 환경의 키 교환 프로토콜

이 절에서 제안하는 프로토콜은 Z-WAVE 환경에서 컨트롤러와 슬레이브간 상호인증이다. 상호인증을 하는 목적은 컨트롤러와 슬레이브에서 발생할 수 있는 중간자 공격을 막기 위해서이다. (그림 4)는 컨트롤러와 슬레이브간 키 교환 절차이다.



(그림 4) 제안한 Z-Wave 키 교환 절차

Step1에서 컨트롤러는 슬레이브에게 키 교환을 요청하는 메시지와 자신이 가진 Node ID, 생성한 nonce 값을 송신하고 Step2에서 슬레이브는 이에 대하여 동일한 포맷으로 응답한다.

Step3에서 슬레이브는 먼저 컨트롤러에게 Z-WAVE 네트워크에서 고유로 사용되는 Network_ID와 수신한 Node ID와 nonce 값을 연결하여 해시한 AMc를 컨트롤러에게 송신한다. AMc를 수신한 컨트롤러는 자신도 동일한 방법으로 AMc'를 생성하고 같으면 슬레이브를 인증한다. Step4는 Step3과 동일한 원리로 컨트롤러가 슬레이브를 인증한다. 이렇게 하여 컨트롤러와 슬레이브가 상호인증을 수행한다.

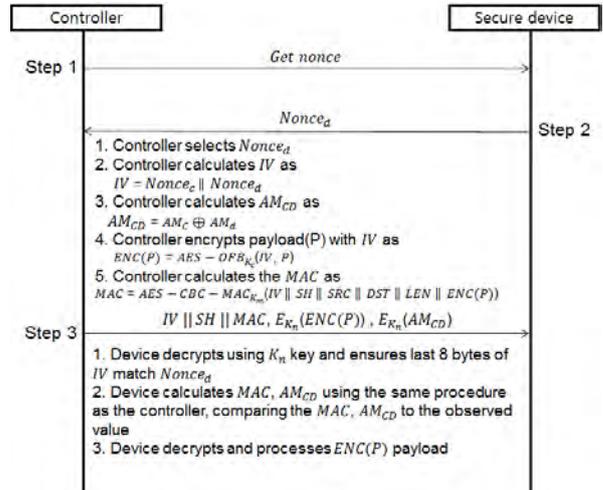
Step5는 컨트롤러와 슬레이브가 사전에 공유한 임시키 K0를 사용한다. 컨트롤러는 수신한 인증요소

AMc와 슬레이브의 nonce 값과 네트워크 키 Kn을 연결한 값을 암호화하여 슬레이브에게 송신한다. 메시지를 수신한 슬레이브는 K0로 복호화하고 먼저 AMc'와 Nonced' 값이 자신의 가진 값이 맞는지 확인하고 네트워크 키인 Kn을 사용한다.

Step6에서 슬레이브는 수신한 네트워크 키 Kn을 이용하여 키가 확립되었다는 Key Set OK 메시지와 인증요소 AMd'와 컨트롤러의 nonce 값을 연결해서 암호화한 메시지를 컨트롤러에게 송신한다. 컨트롤러와 슬레이브간 네트워크 키 Kn이 확립하면, 이 키를 이용하여 패킷을 암호화 해서 전송한다.

3.2. Z-WAVE 환경의 패킷 교환 프로토콜

이 절에서 제안하는 프로토콜은 기존의 Z-WAVE 환경보다 컨트롤러와 슬레이브가 안전하게 패킷을 교환하는 것이다. (그림 5)는 제안한 Z-WAVE 패킷 교환 프로토콜이다.



(그림 5) 제안한 Z-Wave 패킷 교환 절차

Step1, 2에서 슬레이브는 컨트롤러의 요청에 따라 nonce 값을 컨트롤러에게 송신한다. 맨 처음에 기존의 프로토콜과 동일하게 슬레이브는 자신의 nonce와 슬레이브의 nonce를 연결한 IV를 생성한다. 제안한 프로토콜에서는 키 교환 프로토콜에서 사용된 인증요소인 AMc와 AMd를 XOR 연산한 AMCD 값을 생성한다.

Step3에서 컨트롤러가 슬레이브에게 패킷을 보낼 때 IV, SH, MAC을 연결한 값과 네트워크 키인 Kn으로 각각 AMCD와 ENC(P)를 암호화해서 전송한다.

4. 보안성 분석

제안한 프로토콜은 표 1과 같은 보안성을 가진다. 기존의 프로토콜과 동일하게 컨트롤러와 슬레이브는 고유의 nonce 값을 사용하여 재생 공격을 방지한다. 하지만 제안한 키 교환 프로토콜에서는 Step3, Step4과 같은 절차로 컨트롤러와 슬레이브가 상호인증을 수행하였다. 기존 프로토콜은 상호 인증을 제공하지 않아 중간자 공격에 취약했지만 제안 프로토콜은 그

점을 보완하였다. 패킷 교환 프로토콜에서는 키 교환 프로토콜에서 사용한 인증요소인 AM_C 와 AM_D 를 XOR 연산한 값인 AM_{CD} 로 한번 더 인증을 수행하였다. 또한 기존의 프로토콜에서는 패킷을 보낼 때 평문으로 전송했지만 네트워크 키인 K_n 으로 암호화하여 전송해 보안을 강화하였다.

[6] 한국스마트홈산업협회, “스마트홈 업계, 공통 표준화 추진·적용 합의” 한국스마트홈산업협회, 2014.

<표 1> 기존 Z-WAVE 프로토콜과 제안한 프로토콜의 보안성 비교

보안성 항목	기존 프로토콜	제안 프로토콜
상호 인증	X	0
무결성	0	0
재생 공격	0	0
중간자 공격	X	0
기밀성	X	0

5. 결론

본 논문에서는 기존의 Z-WAVE 에서 컨트롤러와 슬레이브간 상호인증성의 부족으로 인한 중간자 공격에 취약한 점을 개선했다. 중간자 공격을 해결한 제안 방법은 먼저 컨트롤러와 슬레이브가 가진 고유의 값들을 교환한다. 이때 고유의 값은 Node ID 와 PRNG(pseudo random number generator)에서 생성한 nonce 이다. 이후에 수신한 각 값들을 XOR 연산을 하고 해시를 하여 다시 교환한다. 이후 똑같은 계산 방식으로 계산하여 값이 일치하면 인증을 한다.

Z-WAVE 기술은 현재 스마트 홈으로 미국, 유럽 등에서 널리 쓰이고 있다. 하지만 Z-WAVE 는 키 교환 및 패킷 교환 프로토콜에서 중간자 공격, 키 복구 공격 등의 문제점을 가지고 있고 새로운 보안 위협이 발생 할 수 있다. 따라서 컨트롤러와 슬레이브가 메시지를 송·수신할 때 인가된 디바이스인지 확인하는 기법이 필요하다. 향후 논문에서는 Z-WAVE 의 취약점 중 하나인 키 복구 공격을 해결하고 좀 더 경량화된 기법을 논의 할 것이다. 또한 무선 매쉬 네트워크를 기반으로 한 Z-WAVE 에서 효율적인 통신을 구현할 예정이며, 암호 성능의 정량적인 측면을 분석할 것이다.

참고문헌

[1] 이효은, “IoT 현황 및 주요 이슈.” 정보통신기술진흥센터, 2014.
 [2] 박현수, “통신사업자의 스마트 홈 서비스 동향.” 디지이코 보고서, 2014.
 [3] 한국스마트그리드사업단 국제협력팀, “주요국 Smart Grid 정책/시장 조사.” KOTRA Repository, KOTRA 자료, 2010.
 [4] Behrang Fouladi, Sahand Ghanoun, “Security Evaluation of Z-Wave_WP.” Black hat USA, 2013.
 [5] Joshua Wright, Johnny Cache, “Hacking Exposed Wireless, Third Edition: Wireless Security Secrets & Solutions.” Mc Graw Hill education, 2015.