Z-Wave환경에서 Diffie-Hellman을 이용하여 안전한 키교환 프로토콜 설계

박근일*, 이재승*, 김만식*, 유한나**, 강정호*
숭실대학교 컴퓨터학과*
KT융합연구소**
e-mail: higa_ps15@ssu.ac.kr
ljs0322@ssu.ac.kr
mansik@ssu.ac.kr
hanna.you@kt.com
kjh7848@naver.com

A Design of Secure Key Exchange Scheme Using Diffie-Hellman in Z-Wave Environment

Geunil Park*, Jae-Seung Lee*, Mansik Kim*, Hanna You**, Jungho Kang*
Department of Computer Science and Engineering, Soongsil University*
Convergence Laboratory, KT R&D center**

요 약

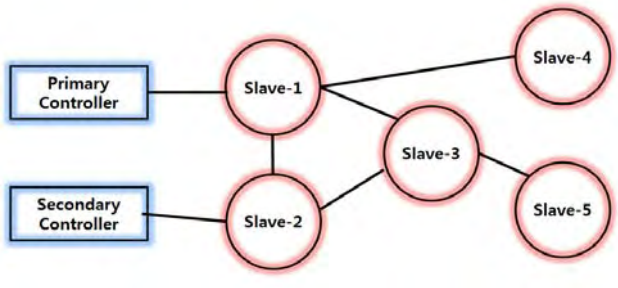
ICT기술이 빠르게 발전함으로써 헬스케어, 스마트홈, 스마트 씨티, 스마트카, 웨어러블과 같이 다양한 인간중심의 서비스가 개발되고 있다. 이러한 인간중심 서비스를 제공하기 위해 여러 센서들을 이용하여 작은 네트워크를 구현한다. 일반적으로 많은 무선 프로토콜 중 Z-Wave를 많이 사용한다. 센서들의 정보를 AES기반으로 암호화하여 Controller와 Device간 통신하는데 가장 효율적이지만 Z-Wave통신으로 데이터를 보내기위해 암호화 키를 생성할 때 사용되는 값이 평문으로 전송되기 때문에 보안위협이 존재한다. 따라서 이러한 보안 위협을해결하기 위해 Controller와 Device간 암호화 키를 생성할 시 Diffie-Hellman을 이용하여 보다 안전한 프로토콜을 제안한다.

1. 서론

오늘날 사회는 ICT(Information and Communication Technologies)의 발전과 가속화됨에 따라 IoT(Internet of Things) 또는 IoE(Ineternet of Everything)기반을 구현된 초연결 사회로 접어들었다. 초연결 사회는 사람과 사람, 사람과 사물, 사물과 사물이 네트워크로 연결된 사회를 의미하며 대표적으로 헬스케어, 웨어러블, 스마트 씨티, 스마트홈, 스마트카 등이 있다. 이러한 환경은 사물, 사람 등 모든 요소들이 연결되면서 여러 방면으로 새로운 서비스 가치 창출할 것으로 기대하고 있다. 초연결 사회 환경에서 사물간 연결하기 위해 BLE(Bluetooth Low Energy), ZigBee, Insteon, Weightless, Z-Wave, WiFi 등 대표인 무선 통신프로토콜을 사용하고 있으며 업체별 경쟁이 심화 되고 있다. 이 무선 통신프로토콜 중에서 Z-Wave는 다른 프로토콜에 비해 가정 자동화와 센서 네트워크와 같은 저전력, 저비용, 저대역폭을 요구하는 장치를 위해 설계되어 가장 많이 IoT 산업에 가장 폭 넓게 사용되는 RF(Radio Frequency)기술이다. Z-Wave 덴마크 소재의 Zensys와 Z-Wave Alliance에서 개발하고 있으며 삼성전자, LG전자, 마이크로소프트, 퀄컴, 인텔, GE, 시스코, 일렉트로눅스, 캐논, 하이얼 등 전 세계적으로 300개 이상의 기업이 참여하고 있다[1]. Z-Wave는 저전력, 양방향 RF, 매시 네트워킹 기술로 스마트홈에서 사용되는 센서와 장치를 제어하는데 아주 적합하지만 만약 악의적인 목적을 가진 공격자가 무선 환경에서 돌아다니는 데이터를 이용하여 홈 네트워크에 접근을 하고 제어를 할 수 있다면 해킹, 개인사생활 침해 등과 같은 큰 보안문제가 발생할 수 있다. 이러한 보안 문제를 해결하기 위해 본 논문에서는 비 대칭키의 Diffie-Hellman기법을 이용하여 Z-wave 키 교환 프로토콜을 제안한다.

2. 관련연구

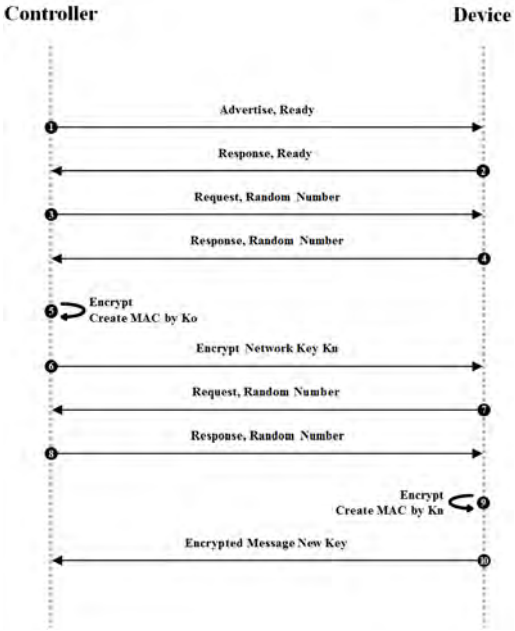
2.1 Z-Wave 네트워크



(그림 1) Z-Wave protocol layers

Z-Wave는 ZenSys가 주축이 된 Z-Wave Alliance에서 제정한 홈오토메이션 무선전송 방식이며, Z-Wave의 주목적은 무선 네트워크에서 하나 이상의 Node들과 Control Unit 사이에서 신뢰성 있는 통신을 제공하는 것이다.
Z-wave 네트워크는 Primary Controller, Secondary Controller, Slave들로 구성되어있다. Z-Wave 기술은 장치간의 통신을 위해 Controller와 Slave의 두 가지 장치를 정의하는데, Controller는 Slave에서 명령을 전송하며, Slave는 명령에 대한 응답 또는 수행한다. 이를 통해 Controller는 직접적으로 연결되어있지 않은 Slave와도 통신이 가능하다[2].

2.2 Z-Wave 키 교환

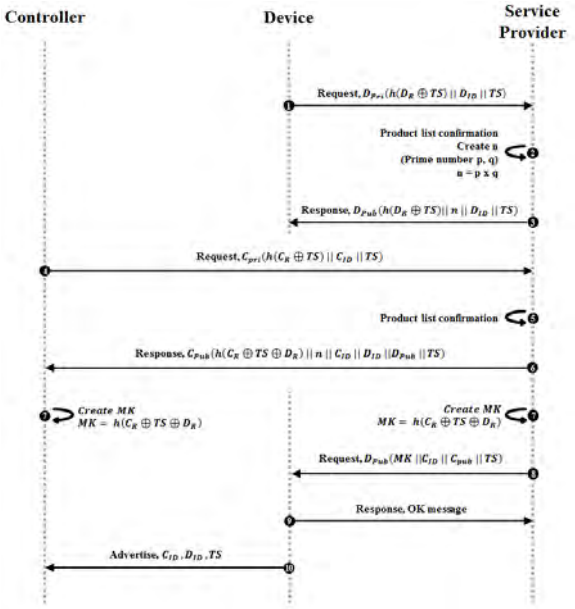


(그림 2) Z-Wave 키 교환

Z-wave네트워크에서 사용되는 키교환 프로토콜은 그림 2와 같다. Z-Wave의 암호화 방법은 AES-OFB에 기초하고 있으며 키를 교환하기 위해 Controller는 Device에게 준비신호를 요청한다[3]. 신호를 받은 Device는 준비되었음을 Controller에게 알리고 Controller는 Device에게 난수를 요청하여 받은 난수를 Ko로 네트워크 키 Kn을 암호화한 값과 연산을 통한 MAC값을 같이 보낸다. Device도 이와 같은 과정을 통해 MAC값과 Kn 값을 암호화 하여 보냄으로써 Controller와 Device는 같은 Kn값 공유한다.

3. 제안

기존 Z-wave네트워크는 무선네트워크를 이용하여 키교환이 이루어진다. 또한 AES암호화 알고리즘을 이용하기 때문에 무선통신환경에서 안전하게 데이터암호화 하여 전송할 수 있도록 한다. 하지만 처음부터 난수 값이 평문으로 보내지기 때문에 악의적인 공격자가 처음부터 sniffing을 시도하여 송수신된 데이터를 가지고 있다면 무작위의 대입을 통해 MAC을 계산 할 수 있고 실제로 송수신된 값과 비교하여 AES암호화 알고리즘에 사용되는 키를 구할 수 있다. 따라서 이 문제를 해결하기 위해 (그림 3)과 같이 Controller와 Device의 안전하게 키를 교환가능하게 하는 매커니즘 Service Provider를 이용한다. 또한 간단한



(그림 3) Diffie-Hellman을 이용한 키 교환

비 대칭키 분배 방법의 Diffie-Hellman을 이용하여 기존보다 안전하게 키를 교환하는 프로토콜을 제안하여 문제를 해결할수 있다.

4. 안전성 평가

Controller와 Device간 송수신 되는 명령어 또는 데이터는 인가된 대상에 의해서만 정보가 제공되어야 하고 비 인가적인 대상으로부터 차단되어야 한다. 본 논문에서 제안된 키 교환 프로토콜은 키 생성과정에서 발생할수 있는 보안문제를 해결하고자 비대칭키 분배방법의 Diffie-Hellmanq 방법을 사용한 안전한 키 교환을 제안하였다. 안전하게 키가 교환이 되면 Controller와 Device간에 송수신되는 모든 패킷들은 AES알고리즘으로 암호화하여 데이터를 안전하게 송수신할 수 있다.

5. 결론

Z-wave 기술은 스마트홈, 헬스케어, 스마트카, 웨어러블 디바이스 등 센서간 데이터 전송을 통해 사용자에게 서비스와 편의성을 제공되고 네트워크의 발달로 인해 모든 사물이 연결되는 통신환경으로 빠르게 진보하고 있다. 스마트홈, 헬스케어, 스마트카, 웨어러블 디바이스 등 사용자의 정보가 무선네트워크통신을 통해 전송이 된다. 하지만 인간중심 서비스에 사용되는 정보들은 민감하기 때문에 절

대로 기밀성, 무결성, 가용성이 침해되어서는 안된다. 주로 작은 센서들의 통신에서 사용되는 Z-Wave는 작은 무선 센서들간 통신하기에는 가장 효율적이고 적합한 기술임에도 불구하고 Device와 Controller간 키 교환방식이 평문으로 보내지기 때문에 사용자의 민감한 정보들을 악의적인 공격자가 해킹하여 탈취 및 위조, 변조, 불법적인 정보활용으로 인해 사용자의 신체적인 위협 또는 경제적인 피해를 유발하는 보안위협으로 이어질 수 있다. 본 논문에서는 Z-Wave를 이용한 무선 통신환경에서 보안위협이 Key 교환 과정이 취약하다는 것을 논점을 두고 있다. Z-Wave 통신은 Key교환 과정으로 인해 사용자의 데이터는 노출에 대한 보안 취약성이 존재한다. 따라서 Key교환 과정을 보안적인 요소를 추가하여 제안한 Diffie-Hellman을 이용하여 안전한 키교환 프로토콜을 제안함으로써 보다 안전한 키교환 과정을 통해 Z-Wave 네트워크를 구축할 수 있을 것으로 기대한다.

참고문헌

[1] Gomez, Carles, and Josep Paradells. "Wireless home automation networks: A survey of architectures and technologies." IEEE Communications Magazine 48.6 (2010).

[2] 금승우, et al. "홈 정보가전 연동 서비스를 위한 IoT 기술." 한국통신학회지 (정보와통신) 32.4 (2015): 36-43.

[3] Kahate, Atul. Cryptography and network security. Tata McGraw-Hill Education, 2013.