Bluetooth, Zigbee를 응용한 Smart Grid 시스템의 인증 및 키 관리

장영현°, 표성배**, 송진영*, 박대우*
°배화여자대학 컴퓨터정보학과
*호서대학교 벤처전문대학원 IT응용기술학과
**인덕대학 컴퓨터소프트웨어과
e-mail: baewhaoa@paran.com, jedisong@naver.com, prof1@paran.com

Authentication and Key Management of Smart Grid System using Bluetooth and Zigbee

Young-Hyun Chang°, Jin-Young Song*, Dea-Woo Park*
°Dept. of, Computer Information, Baewha Women's University
*Dept. of IT Application Technology, Hoseo Graduate School of Venture
**Dept. of, Computer Software, Induk University

● 요 약 ●

Smart Grid는 전기 공급자와 수요자를 이어주는 전기 네트워크를 설치하여, 전기기기와 IT기술이 융합된 형태로 사용자내에서 Bluetooth, Zigbee를 이용한 전기기기를 통제하는 효율적인 에너지 네트워크의 일종이다. 하지만 Bluetooth, Zigbee는 인증과 키관리 문제가 있어 보안의 문제가 일어날 수 있다. 본 논문에서는 스마트 그리드에서 사용될 전기IT기기를 응용하여 제어하는 Bluetooth, Zigbee의 인증과 키관리, 키 생성 프로토콜을 통한 보안성 문제를 연구한다. 또한 Bluetooth, Zigbee에 대한 키 생성 프로토콜을 연구한다. 본 연구는 Smart Grid 시스템의 보안성과 안전성을 강화하여 Smart Grid 기술 발전에 기여할 것이다.

키워드: 지능형 전력망(Smart Grid), 보안성(Securability), 블루투스(Bluetooth), 지그비(Zigbee), 인증(Authentication), 키 관리(Key Management)

I. 서론

Smart Grid는 전기 공급자와 수요자를 이어주는 전기 네트워크를 설치하고 전기의 효율성을 개선시키기 위한 에너지 네트워크의 일종이다. Smart Grid에서는 중앙 집중형, 일방향인 전력 계통의 비효율성을 극복하기 위한 것으로, 분산 전원 시스템을 핵심 개념으로 한다.

Smart Grid에 사용되는 IT 전력기기에서 Bluetooth와 Zigbee는 전기안전을 위한 감시센서 정보전달을 맡고 있어서, 위험성은 더욱 커진다. 특히 WallPad, 지능형 계량기, 아울렛, 수배전반 센서를 통해 전기, 가스, 수도를 검침하려면, WiFi, WiMax, 3G, TDMA/CDMA, RFID, Bluetooth, Zigbee 통신과 같은 여러 형태의 무선망 및 고속 인터넷 백본망이 통합된 통신 형태로 Smart Grid의 전력망 안정성, 장비 상태 감시, 에너지 관리 정책 지원 등을 위한 센싱 및 측정 기술에 포함된 부품이다.

그러나 무선 통신 기술은 무선이라는 통신환경이기 때문에 유선에 비해 보안상으로 매우 취약한 면을 보이고 있다. Bluetooth, Zigbee 전력기기를 통한 취약점 등을 이용, 해킹하여 Bluetooth, Zigbee 전력기기의 권한을 획득[1]한 후 U-Home Gateway를 통하여 Smart Grid를 접속하여, 전력 인프라를 통한 국가 전체 전력 인프라 망을 공격 할 수 있는 가능성이 있다.

II. 관련 연구

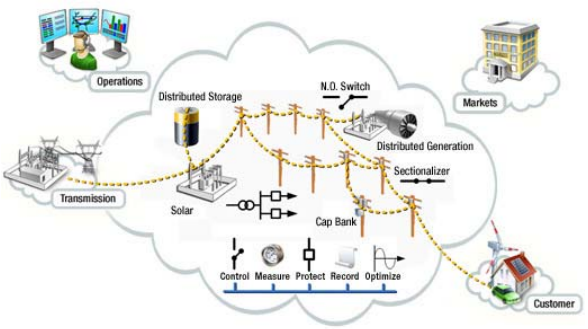

그림 1. Smart Grid 무선통신 개요도
Fig. 1 Smart Grid Wireless overview

2.1 Smart Grid 정의

Smart Grid는 기존 전력망에 IT기술을 접목해 전력 공급자와 소비자가 양방향으로 실시간 정보를 교환함으로써 에너지 효율을 최적화하고자 하는 차세대 전력망을 말한다. 신재생 에너지를 중심으로 하는 다양한 분산 전원이 도입되어 전력계통을 규모에 따라 분산적이고 독립적으로 운영할 수 있는 유연한 형태를 갖추게 되며, 각 계통에 센서, 미터들을 장착하여 소비자의 요구에 실시간으로 반응하는 지능화된 전력망이다.

전력 산업의 패러다임이 양에서 질로 공급 중심에서 수요 중심으로 중앙 집중에서 지역 분산으로 전기IT 기술로 변화하는 것을 의미한다. 미래의 전력망이 분산된 네트워크 구조를 가진다는 점에서 Smart Grid는 에너지 분야의 인터넷과 같은 역할을 수행한다고 볼 수 있다[1].

2.2 Zigbee의 특성

IEEE 802.15.4 ZigBee는 저속, 저가, 저 전력 소모를 필요로 하는 응용에 주안점을 둔 근거리 무선 통신 기술이다. 본 논문에서는 Ad Hoc 네트워크와 향후 Sensor네트워크에 활용 방안의 하나로 ZigBee와 RFID를 접목 시켰다. 이러한 아이디어는 작은 byte만으로도 충분한 통신을 할 수 있는 분야라면 어디에든 적용 가능할 것이다[3].

표 1에 ZigBee 특성을 설명하였다. ZigBee는 2.4GHz, 868MHz, 915 MHz의 주파수 대역을 사용하며 각각 250kbps, 20kbps, 40kbps의 데이터 전송률을 제공한다. ZigBee의 MAC 계층은 저전력 소모를 위한 방식들을 제공하고 있는데, Superframe 구조로 동작하는 방법, Data request frame을 사용하는 방법, backoff 횟수를 줄이는 방법, short address를 사용하는 방법 등으로 이를 실현하고 있다. PHY 계층은 간단한 구조로 되어 있다. 별도의 channel coding 기법을 사용하지 않고, Spreading과 PSK modulation만을 하여 전송하는 구조로 되어 있다. 따라서 근거리의 저속 무선 통신에 한정된 용도를 지녔지만, 낮은 가격으로 실현될 수 있다. PHY·MAC 계층에 대한 전 세계인 표준이 제정되자 ZigBee Alliance는 모든 새로운 무선 표준을 널리 보급하기 위해 네트워크, 보안, 애플리케이션 계층을 정의하는 작업을 진행하고 있다.

표 1. Zigbee 특성
Table. 1 Zigbee characteristics

구분	특성
데이터 전송률	868MHz : 20kbps, 915MHz : 40kbps, 2.4GHz : 250kbps
적용거리	10~75m
잠복 시간	Down to 15ms
주파수 대역	물리층 : 868/915MHz 및 2.4GHz
채널 수	868MHz : 1ch, 915MHz : 10ch, 2.4GHz : 16ch
채널 접속	CSMA-CA 및 slotted CSMA-CA
활용 온도 범위	−40 to +85℃

ZigBee Alliance는 Motorola, Honeywell, 삼성전자, Philips, Invensys, Mitsubishi Electric의 지원을 받고 있으며, 60여 이상의 회원사가 이곳에서 활동하고 있다. 이 무선 네트워크 표준화 단체는 상호 운용성 및 순응 테스트 표준을 제공하고, ZigBee 브랜드를 홍보하며, 기술의 진보를 위해 노력할 방침이다. ZigBee는 스타형 및 메시 토폴로지와의 조합을 가능하게 하는데, 이 조합은 클러스터 트리 네트워크라 불린다. 각 네트워크는 초기화, 노드 관리, 노드 정보 저장 기능을 제공하기 위해 코디네이터라고 불리는 FFD(full-function device)가 하나 이상 있어야 한다. 비용과 전력 소모를 최소화하기위해 나머지 노드는 배터리로 동작하는 간단한 RFD(reduced-function device)로 구성된다. ZigBee 네트워크는 몇몇 데이터 전송 시나리오에 적용된다. 무선센서 데이터 등의 주기적인 데이터의 경우 노드는 설정된 횟수만큼 깨어나 샘플링된 데이터를 코디네이터에 전송하고, 다시 절전 모드 상태가 된다. 그러므로 배터리 수명을 연장 시킬 수 있다.

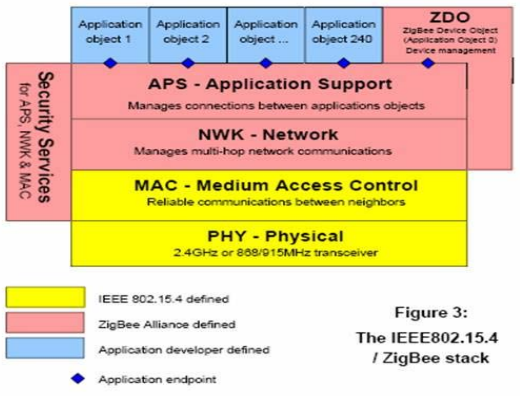

그림 2. Zigbee 프로토콜 계층구조
Fig. 2 Zigbee protocol hierarchy

2.3 Bluetooth의 특성

블루투스(Bluetooth)는 1994년 에릭슨이 최초로 개발한 개인 근거리 무선 통신(PANs)을 위한 산업 표준이다. IEEE 802.15.1 규격을 사용하는 Bluetooth는 PANs(Personal Area Networks)의 산업 표준이다. Bluetooth는 다양한 기기들이 안전하고 저렴한 비용으로 전 세계적으로 이용할 수 있는 라디오 주파수를 이용해 서로 통신할 수 있게 한다.

Bluetooth는 유선 USB를 대체하는 개념이며, 와이파이(Wi-Fi)는 이더넷(Ethernet)을 대체하는 개념이다. 암호화에는 SAFER(Secure And Fast Encryption Routine)+을 사용한다. 장치끼리 믿음직한 연결을 성립하려면 키워드를 이용한 페어링(paimg)이 이루어지는데, 이 과정이 없는 경우도 있다.

Bluetooth는 전 세계적으로 사용이 가능하며 허가가 필요 없는 무선 대역인 2.4GHz~2.5GHz 대역에서 운용되고 있으며 특징을 정리하면 다음과 같다[2].

- 1Mbps의 전송속도 (실제 723kbps)
- 대기상태 0.3mA, 송수신시 최대 30mA
- 전송거리 10M(2003년까지 100M까지 확장)

- 각 상태별 송신전력의 구분
- GFSK (Guassian Frequency Shift Keying) 변조방식
- FHSS (Frequency Hop Spread Spectrum) 사용

또한, Bluetooth는 자체적으로 보안 서비스를 제공해주고 있다. 이러한 보안 서비스는 각 장치에 적당한 보안 기능을 제공하며 주요 기능은 다음과 같다.

- 인증을 위한 Challenge-Response
- 암호화를 위한 스트림 암호
- 임의의 시간에 변경이 가능한 세션키의 생성

Bluetooth의 또 다른 특징의 하나는 하나의 작은 네트워크의 구성이 가능하다는 것이다. 이는 피코넷이라 불리우며 하나의 피코넷에는 2개에서 최대 7개까지의 슬레이브가 가능하다. 이러한 피코넷이 여러개가 모여 서로 연결되어 있을 때 이를 스카터넷(Scatternet)이라 한다. 결국 이러한 피코넷은 여러 통신장비를 하나의 통신 네트워크로 묶을 수 있다는 장점이 된다. 그림 1은 일반적인 Bluetooth 구조를 나타내는 그림이며 Bluetooth의 피코넷과 스카터넷의 관계를 잘 보여주고 있다.

III. Bluetooth 키 관리와 기기 인증을 통한 Smart Grid 시스템 보안

3.1 Bluetooth 키 관리

Bluetooth에서는 안전한 전송을 위해서 여러 종류의 키를 사용한다. 그 중 가장 중요한 요소는 Smart Grid에서 사용될 블루투스 기기간의 인증을 위해 사용되는 링크키이다. 이 링크키를 사용하여 암호키를 유도한다. Smart Grid에서 사용될 블루투스의 키 관리는 키-제어과정에서 다음 세 가지의 키를 사용한다.

첫 번째로 사용자 또는 Smart Grid 기기가 개인-식별번호를 등록한다. 개인-식별번호(Personal Identification Number, PIN)는 사용자가 선택하며 45비트로 구성되어야 한다.

두 번째로 Smart Grid 기기가 개인-링크키를 발생하고 두 번째 Smart Grid 기기와 인증 과정을 거친다. Smart Grid 블루투스 기기는 인증키(Authentication Key)로 불리는 네 가지의 서로 다른 종류의 링크키(Link Key) 중에서 하나를 사용한다. 네 가지는 임시 번호이거나 반영구적인 128비트의 불규칙한 번호이며, 전송 시마다 새롭게 생성된다.

마지막으로 Smart Grid 기기가 링크키로부터 개인 암호화키를 생성하고 두 번째 Smart Grid 기기와 인증하는 과정을 거친다. 개인용 인증키(Pricate Encryption Key)와 암호화키(Encryption Key)는 현재 사용되고 있는 링크키로부터 생성된다. 인증키는 암호화가 필요할 때마다 자동적으로 변경되며 8비트와 128비트 사이의 크기를 가진다.

3.1.1 Bluetooth 기기 인증

Smart Grid에서 Bluetooth의 인증 방식은 Challenge-Response 방식으로서 상대방의 식별 비밀키(대칭키)를 알고 있는지를 확인하기 위해 2-move 프로토콜을 사용한다.

이 프로토콜에서는 양쪽 Smart Grid Bluetooth 기기 모두 같은 키를 갖고 있는지를 확인하고 같은 키를 갖고 있을 때 인증이 성공하게 된다. 반면, 각 Smart Grid 기기가 키를 모른다면 연결은 취소된다. 인증 과정 중에 ACO (Authenticated Cipering Offset) 값을 생성하여 양쪽 Smart Grid 기기가 저장하는데, 이 ACO값은 후에 암호키를 생성하는데 사용된다. 인증이 실패되었을 경우 다시 인증을 시도하는 데는 대기시간(Waiting Time)이 소요된다.

IV. Zigbee 인증과 키 관리를 응용한 Smart Grid 시스템 보안

3.2 Zigbee 키 관리와 인증

Smart Grid에서 ZigBee는 보안 서비스 제공자 (Security Service Provider)는 NWK PIB (PAN Information Base)와 MAC PIB에게 Security Material 정보를 얻어와 네트워크 계층과 응용 지원 하부 계층에 보안 서비스를 제공한다. Smart Grid에서 ZigBee 보안 서비스는 128-bit AES의 대칭키 암호 알고리즘을 이용하여 두 노드 간의 비밀키 설정과 상호 인증을 수행한다. 각 비밀키는 MAC 계층, 네트워크 계층, 응용 계층에서의 데이터 프레임에 대한 Smart Grid 보안 기능을 제공하여 ZigBee 보안 메카니즘을 구성하게 된다. Smart Grid에서 ZigBee는 네트워크 키 (network key)와 링크키, 그리고 마스터키를 이용하여 인증 및 암호화를 수행하는데 Smart Grid 네트워크 키는 네트워크 레벨에서의 인증 및 암호화에, 링크키는 Smart Grid 디바이스 레벨에서의 인증 및 암호화에 사용된다. 그리고 마스터키는 Smart Grid 디바이스 간에 링크키를 유도하기 위한 신뢰성 있는 정보로, SKKE 프로토콜에서는 마스터키를 이용하여 Smart Grid 디바이스 상호간에 링크키를 생성하게 된다.

3.2.1 Zigbee 인증과 키 생성 프로토콜

Smart Grid에서 ZigBee 보안에서 새로운 디바이스가 PAN에게 조인하게 되면 PAN 코디네이터는 디바이스와 링크키를 생성하게 된 후, 마지막으로 Smart Grid 네트워크키를 전송하여 디바이스를 인증하게 된다. 링크키를 생성하기 위한 마스터키는 각 Smart Grid 디바이스에게 사전 분배하거나 네트워크에 조인한 Smart Grid 디바이스에게 직접 전송하는 2가지 방법이 존재한다. Smart Grid 디바이스와 PAN 코디네이터가 비컨 (beacon) 신호를 주고받은 후, Smart Grid 디바이스는 Association request command를 보내어 PAN에 조인을 요청한다. PAN코디네이터가 Association response command를 보내 Smart Grid 디바이스의 조인을 허가하면 PAN 코디네이터와 디바이스 간의 인증 및 키 생성 과정을 수행하게 된다. PAN 코디네이터는 Smart Grid 디바이

스에게 마스터키를 보내주고 SKKE 프로토콜을 진행하여 링크키를 생성한 후, 마지막으로 네트워크키를 보내어 Smart Grid 디바이스를 인증한다.

V. 결 론

Smart Grid의 보안성 문제를 해결하기 위해서 Bluetooth와 Zigbee를 응용한 전기IT기기를 통해서 Smart Grid 네트워크와 시스템을 제어를 할 수 있다.

본 논문은 Bluetooth와 Zigbee가 융합된 전기IT기기에 대한 인증과 키 관리 및 키 생성 프로토콜을 연구하여 전력망과 시스템에 대한 보안성을 강화시켰다.

향후 연구로는 전기IT기기인 Bluetooth와 Zigbee 통신 취약점을 이용한 Hacking 공격을 실행하여, 취약점을 발견하고 보안대책을 연구한다.

참고문헌

[1] 이일우, 박완기, 박광로, 손승원, “스마트 그리드 기술 동향”, 한국통신학회지, 26(9), 24-33쪽, 2009. 8.

[2] 김재완, 김병국, 엄두섭, “블루투스를 이용한 보안을 위한 무선 센서네트워크의 구현”, 한국정보처리학회 춘계학술발표대회, 11(1)

[3] 임송빈, 오영환, “스마트 그리드 네트워크에서 효과적인 Zigbee 인증 프로토콜에 관한 연구”, 한국통신학회논문지, 36(2), 184-194쪽