情 報 保 護 學 會 誌
第20卷 第5號, 2010. 10

지그비 기반 AMI에서의 보안 특성 및 요구사항 분석

전 용 희*

요 약

AMI는 스마트 그리드 구축을 위한 핵심 기술로, 현재의 단방향·폐쇄적 에너지 공급에서 양방향 에너지 종합관리시스템 구축을 위한 기반 기술이다. 스마트 미터 및 AMI 구축을 통하여 전기요금에 대응하여 에너지를 절약하는 가전 기기 보급 및 부하 관리가 실현되고, 최대 전력의 감소를 통하여 추가적인 발전소 건설비용이 절약되게 된다. Zigbee는 AMI 통신 구현을 위한 표준 기술로 개발되고 있다. 본 논문에서는 Zigbee 기반 AMI 시스템에서 AMI 시스템의 보안 특성 및 보안 요구사항에 대한 분석 결과를 제시하고자 한다.

Ⅰ. 서 론

국내「지능형전력망 로드맵 추진위원회」자료에 의하면 스마트 그리드(smart grid)를 기존의 전력망에 정보기술(IT)을 접목하여, 전력공급자와 소비자가 양방향으로 실시간으로 정보를 교환, 에너지효율을 최적화하며 새로운 부가가치를 창출하는 차세대 전력망으로 정의하고 있다[1]. 한편, 미국 「에너지 독립 및 안보법」에 의하면, 스마트 그리드를 미래의 증가할 전력 수요를 해결할 수 있으면서 전력 전송과 분배에 있어 신뢰성과 기반시설 보호를 유지할 수 있도록 구조화된 국가전력 전송 분배 시스템으로 정의한다[2,3]. 이와 같이 스마트 그리드는 전력 인프라와 정보·통신 인프라가 융합된 고효율 차세대 전력망으로써, 스마트 그리드가 설치되면 발전-송전-배전-소비자에게 이르는 계층 구조의 전력망에서 다양한 주체들이 소비자이자 공급자인 네트워크 구조로 변화될 전망이다.

스마트 그리드의 특징 중에서 소비자들에게 가장 분명하게 나타나는 것은 에너지 소비 효율성을 위한 지능형 계량기(smart meter)일 것이다. 이 계량기를 통하여 첨두(peak) 혹은 비첨두(offpeak) 부하 기간 동안의 전력 생산 비용 차이를 반영하는 과금 체계가 가능하여진다. AMI(Advanced Metering Infrastructure)는 전기, 가스, 수도와 같은 여러 가지 유틸리티 자원의 사용과 관련한 데이터를 평가하기 위하여 사용되는 시스템의 집합체를 의미하며, 스마트 그리드에서는 부하 제어 및 수요 응답(demand response)을 사용하여 시스템 상의 첨두 요구를 감소시키고, 에너지 소비와 비용 감소를 유도하기 위한 동적 과금(dynamic pricing)을 가능하게 한다[4,5].

AMI 통신에는 BPL(Broadband over Power Line), WiFi, WiMax, 3G 셀룰라, TDMA/CDMA, VSAT(Very Small Aperture Terminal) 위성과 같은 여러 형태의 무선망 및 고속 인터넷 백본망, 전력선(PLC: Power Line Carrier) 통신, 공중 전화망, IEEE 802.15.4, 지그비, 6LoWPAN, IEEE 802.11 및 802.16을 포함한 라디오 주파수 통신 시스템을 포함한다.

AMI 시스템은 보다 큰 대규모의 스마트 그리드 이니셔티브로써 HAN(Home Area Network)과 NAN (Neighborhood Area Network)을 결합하는 시스템으로 구축되고 있다. HAN은 유틸리티 미터 혹은 관련 장치들과 인터페이싱하는 소비자-소유 장치를 나타내며, 반면 NAN은 동일 지역 위치 내에서 통신하는 유틸리티 장치들의 집합체를 의미한다. 수요 응답을 위한 AMI 네트워크는 통신 thermostat, 부하 스위치, 조명 시스템 및 미터에 대한 가정 내 디스플레이들을 연결하는

* 대구가톨릭대학교 컴퓨터정보통신공학부(yhjeon@cu.ac.kr)

HAN을 포함하며, NAN은 유틸리티 본부에 대한 back-haul을 위하여 수천 개의 가정 미터를 통합한 메시 구조를 이룬다[6].

본 논문에서는 특히, 이 두 네트워크 환경에서의 지그비-기반 AMI 시스템의 보안에 대하여 살펴보고자 한다[7].

Ⅱ. 스마트 그리드 보안의 필요성

스마트 그리드는 대체적으로 광범위한 인터넷 기술을 포함하는 고도로 네트워크화 된 정보 하부구조 상의 통신과 복잡한 분산 응용을 요구한다. 따라서 스마트 그리드 시스템에 대한 위협은 산업 스파이, 불만을 품은 종업원, 악성 침입자 및 시스템 복잡성, 인간 실수 및 사고, 장비 실패 및 자연 재해와 같은 자연적 소스와 같이 다양한 소스로부터 발생할 수 있다. 미국 에너지성(DOE: Department of Energy)에서도 현대적인 그리드를 도입하는데 해결해야 할 기술적인 장벽 중에 보안 기술을 명시하고 있다[8]. 특히 분산 에너지 자원 소유주, 독립 전력 생산자, 소비자의 수요 대응 및 자동화 검침 프로그램 등에 반드시 보안 기능이 구축되어야 하며, SCADA (Supervisory Control And Data Acquisition) 및 보호 계전기 시스템의 보안이 보장되어야 함을 명시하고 있다.

스마트 그리드 보안 서비스가 방지하려고 하는 보안 사건의 몇 가지 예는 다음과 같다[4]:

- 스마트 그리드의 안전성 공격
- 그리드의 물리적 재산 손상
- 서비스 거부(DoS)나 붕괴 공격
- 프라이버시 위반
- 장비 제어 하이재킹
- 물리적이고 논리적인 손상
- 운용자가 시스템을 붕괴하도록 하는 치명적 동작을 취하도록 상황 인식 전복
- 자동화 시스템이 허위 경보에 대하여 자원을 허비하도록 원인 제공
- 서비스 하이재킹
- 스마트 그리드 서비스나 지원 통신 메커니즘을 통한 종단 주거 사용자나 산업 네트워크 공격

이와 같이 스마트 그리드 시스템에 대한 위협은 산업 스파이, 불만을 품은 종업원, 악성 침입자 및 시스템 복잡성, 인간 실수 및 사고, 장비 실패 및 자연 재해와 같은 자연적 소스와 같이 다양한 소스로부터 발생할 수 있다. 자연적 위협뿐만 아니라 악의적인 위협에 대하여 보호하기 위하여, 방어 전략을 세울 필요가 있다. 다음은 스마트 그리드에 대하여 가능한 위협을 보여주는 목록이다[9]:

- 스파이웨어/멀웨어의 생성 및 배분 공격
- 좀비를 이용한 봇-넷(Bot-Net) 공격
- 스팸 메일 이용 공격
- 금전적인 이득을 위한 외부 공격
- 내부자 공격
- 피싱(Phishing)
- 기타 산업 스파이 활동 등.

이런 위협은 아래와 같은 요인에 의하여 점점 더 증대되고 있다[9]:

- MS 윈도우와 TCP/IP 같은 표준 프로토콜 및 기술의 채택
- 스마트 그리드와 Corporate 네트워크, WAN, 인터넷과 같은 시스템의 증가된 연결성
- 다른 시스템들의 통합에 따른 복잡성과 불안전한 연결
- 설계, 유지보수, 상호연결 및 통신에 관한 시스템 정보 공개

미국의 DOE 에너지 부문 계획에도 스마트 그리드의 효과적인 운용을 보장하는 사이버 보안의 역할에 대하여 문서화되어 있다. 미국의 국가 하부구조 보호 계획(NIPP: National Infrastructure Protection Plan)에 의하면 사이버 보안은 다음과 같이 정의된다[8]:

"기밀성, 무결성 및 가용성을 보증하기 위하여 전자 정보 및 통신 시스템과 서비스(그리고 그 속에 포함된 정보)에 대한 손상, 권한이 없는 사용 및 남용을 방지하고, 필요한 경우, 복구까지를 포함 한다".

그러므로 스마트 그리드와 같은 국가적인 주요 인프라를 보호하기 위한 보안 대책이 필요하며, 주요 보안 목표는 다음과 같이 제시될 수 있다[4]:

- 서비스 임무를 위협하는 악성 공격, 비고의적 사이버 및 물리적 재난 사건으로부터 스마트 그리드 서비스를 보호
- 스마트 그리드 서비스와 관련된 보안사건 방지
- 스마트 그리드 서비스의 무결성, 기밀성 및 가용성에서 신뢰 보증을 지원하기 위한 충분한 증거 제공

Ⅲ. AMI 보안 특성

3.1 AMI 개요

AMI는 현재의 단방향·폐쇄적 에너지 공급에서 양방향 에너지 종합관리시스템 구축을 위한 핵심 기반이다. 스마트 미터 및 AMI 구축을 통하여 전기요금에 반응하여 에너지를 절약하는 가전기기 보급 및 부하 관리가 실현되고, 최대 전력의 감소를 통하여 추가적인 발전소 건설비용이 절약되게 된다.

AMI 컴포넌트로는 통신 네트워크 장치, 예측 시스템, 헤드엔드, 미터, 미터 관리 시스템, 네트워크 관리 시스템, 요구 응답 분석 및 제어 시스템, 필드 도구/장치, 그리드 제어 센터, 미터 데이터 관리 시스템, 비전기미터, 제 3자 미터/서브미터 등으로 분류하고 있다[5].

또한 스마트 그리드에서 특정 제어 요구사항을 요구하는 특성에 대하여 장치, 응용 및 컴포넌트를 분석하기 위한 도구로 보안 도메인(Security Domain) 개념을 사용한다. 보안 도메인은 보안과 관련하여 상당히 일관된 집합의 제한 사항 및 기대를 부과할 수 있는 지역을 의미하며, 통신, 유틸리티 에지, 프레미스(Premise) 에지, 관리되는 네트워크, 자동화된 네트워크 및 유틸리티 엔터프라이즈 등으로 구분하고 있다[5].

AMI 보안을 위하여 AMI 컴포넌트에 대한 아래와 같은 제어 요구사항이 권고되고 있는데, 몇 가지만 간략하게 제시하고자 한다[5]:

- 공유 시스템 자원을 거쳐 권한이 부여되지 않은 혹은 의도되지 않은 정보 전달을 방지하여야 한다.
- DoS 공격에 대하여 보호되고, 영향을 제한하여야 한다.
- 우선순위에 의하여 자원의 사용을 제한하여야 한다.
- 보안 경계를 확립하고 경계 내에 존재하는 컴포넌트에 대한 의무적인 보안 요구사항을 명시해야 한다.
- AMI 시스템 설계 및 구현은 통신 정보의 무결성 및 기밀성을 보호해야 한다.
- 사용자(혹은 에이전트)와 컴포넌트 사이의 신뢰 통신 경로를 확립하여야 한다.
- 보호 정보와 운영 제한사항에 부합되는 암호적 보호 및 키 관리 하부구조를 선정하여야 한다.

3.2 AMI 통신 방식

현재 까지 Zigbee 방식, 고속 전력선 통신 방식 등을 적용하여 자동 계량기(AMR: Automatic Meter Reading)용 통신망이 보급되고 있으나, 다양한 유·무선 통신방식 등에 대한 검증 및 표준화 작업이 필요하다.

AMI 구축 기술로는 최근 국내외에서 Zigbee, PLC, Z-Wave 등에 대한 관심이 증대되고 있다[10].

PLC는 국내에서 기존의 매체를 이용할 수 있다는 점에서 다소 정책적인 측면에서 높은 관심을 보이고 있다. 그러나 기술적인 관점에서 주기적이며 안정적인 데이터 통신과 보안성과 같은 AMI 시스템의 주요 요구사항에 대해 중요한 취약점을 가지고 있다. 따라서 빈번하고 주기적인 통신과 높은 수준의 데이터 보안을 특별히 요구하지 않은 문단속 및 조명 조절과 같은 기본적인 홈네트워크 솔루션 제공에 적합하다는 분석이다.

Z-Wave는 최근 다양한 분야에서 중요한 무선 통신 기술로 검토되고 있으며, Z-Wave Alliance가 구성되어 여러 활동을 시작하고 있으나 업계의 포괄적인 참여가 저조하여 글로벌 표준으로 채택되기에는 일정 시간이 소요될 것으로 예상하고 있다. 기술관점에서 Z-Wave는 배터리 수명 면에서 Zigbee와 비교하여 성능이 좋은 편이나, 기술 차이는 근소한 것으로 분석되었다. 그러나 데이터 전송 속도, 통신 안정성 및 보안성과 같은 중요 항목에서는 Zigbee보다 떨어지는 것으로 분석되었다.

Zigbee는 PLC보다 다소 비용 측면에서 불리하지만, 많은 개발자 그룹이 Zigbee의 채택을 추진하고 있으며 단위 비용은 지속적으로 낮아질 것으로 분석되었다. 기술적 측면에서 Zigbee는 Z-Wave와 비교하여 배터리 효율성 측면만 제외하고 상당한 경쟁력을 가지는 것으로 보인다.

결론적으로 Zigbee가 AMI 기술로 상당히 유망한 것으로 평가할 수 있다.

3.3 AMI 보안 취약성

AMI 취약성은 크게 설계 혹은 구현상의 결함으로 나누어진다. 설계 결함은 시스템의 기초적인 구조 개념에 기인하는 취약성이다. 설계 보안 결함은 칩설계, 펌웨어

및 프로토콜 등과 같이 여러 레벨에서 발생할 수 있다. 예를 들어, 인증 과정 없이 미터의 핵심 요소에 대한 접근을 허용하는 통신 프로토콜은 설계 결함을 포함하는 것이다. 한편 구현 결함은 프로그래밍 실수에 의하여 발생되는 취약성이다. 이것에 대한 예로는 버퍼 오버 플로가 있다. 이런 유형의 결점을 식별하기 위한 분석과정은 매우 차이가 나기 때문에, 설계 및 구현 결함을 구분하는 것이 중요하다. 지적된 AMI의 가능한 취약점은 아래와 같다[6,7].

- 평문 트래픽: 미터와 수집 시스템 사이의 데이터 비밀성 문제
- 버스 스누핑: 임베디드 시스템 주변 장치 인터페이싱을 위한 버스 상의 데이터 노출
- 부적절한 암호: 약한 키 유도, 키 스트림 데이터의 부적절한 재사용, 재생 공격 보호 결여, 불안전한 암호 모드, 약한 무결성 보호, 불충분한 키 길이 등
- 직접 탬퍼링(direct tampering): 미터 장치의 악의적 변경 방지를 위한 손상-보호 메커니즘이 필요하다.
- 미터에 저장된 키 및 패스워드
- 암호 키 분배
- 불안전한 주요 인터페이스: 미터의 적외선 포트 네트워크 보안 주의 결여 등.
- 미터 인증 약점: 열악한 논스(nonce) 선택, 재생 공격 조건, 메모리 소모 DoS 취약성, 프로토콜 버전 협상 조작 등.
- NAN 인증 약점: NAN과 미터 장치의 상호 인증이 필요하다.
- 펌웨어 구현 결점, 트래픽 라우팅 결점, DoS 위협
- 정보 노출 위협 및 기타 사항

3.4 AMI 공격 방법론

AMI에 대한 공격 방법은 아래와 같이 네 단계로 나누어진다[6,7]:

- 정찰(reconnaissance): 이 단계에서 시스템에 대한 관련 정보를 수집한다. AMI 구성품의 특징과 의도되는 행위 등에 대하여 알기위하여 관련 문서를 수집하고, 미터 장치의 구성과 사용에 대한 정보 수집, 그리고 무선 주파수 특성에 대한 정보 등을 분석한다. 핵심 라디오 정보로는 주파수 스펙트럼, 변조, 채널 선택, 주파수 호핑 패턴 및 상위-레벨 프로토콜 등이 있다. 예를 들어, 지그비 구현에 대하여 다음과 같은 정보 집합이 가능하다:
  - 주파수 범위: 2.4GHz/ 868KHz/ 915KHz (802.15.4)
  - 변조: 2,4GHz: MSK, 868/915KHz: BPSK
  - 채널 선택: 수동: 16/10/1 채널
  - 채널 접속: CSMA-CA
  - 홉핑 패턴: 비적용
  - 상위-레벨 프로토콜: 지그비(보안-증진 프로파일)
- 초기 분석: 정찰 단계에서 수집된 정보를 사용하여 공격 목표 장치에 대한 초기 분석을 수행한다. 이 단계에서 손상 탐지 및 보고 방지 방법을 조사하고, NAN과 HAN으로부터의 무선 패킷을 포획하여 분석한다. 미터를 소유한 후, 모든 집적회로, 인터페이스, 버스 및 주변장치 등에 대한 철저한 문서화 작업을 한다. 이를 통하여 하드웨어 역공학을 시도할 수 있게 된다. 또한 이 단계에서 EEPROM 덤핑, 마이크로 컨트롤러 덤핑, 버스 스누핑 및 네트워크 스캐닝 등이 이루어질 수 있다.
- 심층 분석: 초기 분석과정 동안 수집된 정보를 이용하여 시스템 기능과 잠재적인 취약성 영역을 식별하게 된다. 심층 분석 단계에서 사용될 수 있는 공격 벡터는 다음과 같다.
  - fuzzing: 비정상적이고 임의적인 방법으로 애플리케이션과 상호작용하여 취약한 애플리케이션이 crash하거나 부정확하게 동작하도록 하는 것이다.
  - firmware disassembly: 이 과정을 통하여 목표 장치 운용에 대한 데이터와 상황에 대한 심층 분석을 하게 된다.
  - 키 추출: 펌웨어 혹은 EEPROM 데이터의 엔트로피 분석을 통하여 암호 키 위치가 식별될 수 있다.
  - 펌웨어 코드 분석: 펌웨어 취약성 분석을 통하여 다른 분석 및 공격을 제공하도록 이용될 수 있다.
  - 결함 추적 및 열거: 마이크로 컨트롤러 소프트웨어 결함 조건의 식별을 통하여 취약 코드 지역의 결정 분석에 이용될 수 있고, 실행 코드

를 주입하거나 유사한 악성 기능을 수행하기 위하여 신규 패킷이 생성될 수 있다.
- 시뮬레이션: 추출된 펌웨어를 가지고 미터 하드웨어를 모방할 수 있고, 통제된 환경에서 익스프로잇의 개발과 시험에 이용될 수 있다.
- power-glitching 공격: 이 공격을 통하여 시스템 마이크로 컨트롤러가 인증 실패 처리 루틴이나 다른 바람직하지 않은 명령어들을 생략하도록 조작하여, 미터나 NAN 자원에 대하여 적절한 인증 신용장 없이 접근을 허용하게 된다.
- 클락-glitching 공격: 클락 신호율을 조정하여 특정 명령어 실행을 생략하도록 조정할 수 있다. 이 기법을 통하여 공격자에게 시스템에 대한 더 많은 제어권을 부여할 수 있다.
- 익스플로잇 개발: 펌웨어 코드 분석 등으로부터 발견된 취약성을 기반으로, 변경되지 않은 미터를 조작하기 위한 익스플로잇을 개발할 수 있다. 이를 통하여 미터 DoS, 전력 서비스 종료나 개시, 서비스 이용 보고 조작 등을 할 수 있다.

• exploitation: 권한이 부여되지 않은 장치 인증, 펌웨어 악성 패칭 및 보고 데이터의 조작이 가능하다. 또한 수집자(collector)와 다른 제어 시스템 개체로 가장하여 power latch를 끄거나, 펌웨어 갱신 혹은 HAN 장치 공격 등과 같은 일을 수행하도록 제어 메시지를 강요할 수 있다.

3.5 AMI 시스템 보안 요구사항[7]

AMI-SEC 태스크 포스에서는 높은 수준의 정보 보증, 가용성 및 보안을 제공하기 위하여 AMI 구현에 적용될 보안 요구사항을 제시하고 있다[4]. 다음과 같이 지원하는 주요 가치 스트림에 일치하는 5개의 use case로 나누고 있다: billing, 고객, 분배 시스템, 설치 및 시스템

위와 같은 각 사용자 경우에 대한 보안 관심사를 기밀성, 무결성, 가용성 관점에서 제시하고 있다. 또한 견고하고 안전한 AMI 솔루션을 구현하고, 제시된 보안 요구사항을 AMI 구현에 적용하기 위하여 6 개의 보안 도메인 모델을 제시한다: 유틸리티 에지 서비스, Premise 에지 서비스, 통신 서비스, 관리 서비스, 자동화 서비스 및 비즈니스 서비스.

또한 시스템 보안 요구사항을 주요 보안 서비스, 지원 보안 서비스 및 보증으로 나누어 정의하고 있다. 주요 보안 서비스로는 기밀성과 비밀성, 무결성, 가용성, 식별, 인증, 권한 부여, 부인 봉쇄 및 계정 관점에서 제시하고 있다. 지원 보안 서비스로는 비정상 탐지 서비스, 경계 서비스, 암호 서비스, 통지 및 신호 서비스, 자원 관리 서비스와 신뢰 및 인증서 서비스를 기술하고 있다. 마지막으로 보증 부문에서는 개발 엄정(rigor), 조직적 엄정, 취급/운용 엄정, 계정성(accountability) 및 접근 제어에 대하여 기술하고 있다.

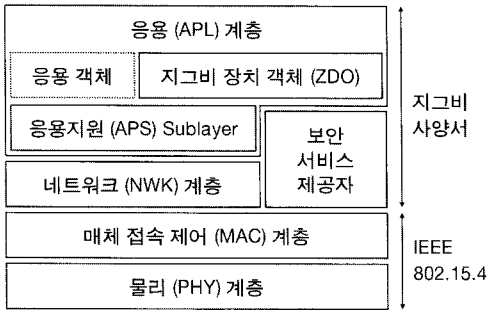
UCAIug 산하에서 운영중인 AMI-SEC 태스크 포스(Advanced Metering Infrastructure Security Task Force)에서는 AMI의 시스템 분석을 통한 AMI에서의 보안 요구사항, AMI 시스템 요소에 대한 사이버 보안 지침, 권고, 모범사례 등의 개발을 진행 중에 있으며, 이를 통하여 AMI와 관련된 산업계의 여러 이해 관계자들이 사이버 보안에 대한 논의의 초점을 공유할 수 있도록 하고 있다[4].

Ⅳ. Zigbee 보안

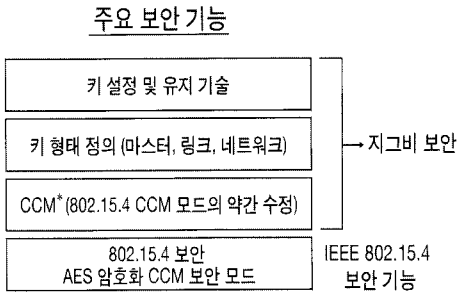
4.1 개요

AMI를 지원하기 위하여, 지그비 연합(Zigbee Alliance)에서는 Smart Energy Profile을 정의하고 재가하였다[11]. Zigbee Smart Energy는 용역회사에게 가정 내에서 에너지를 관리하기 위한 안전한 통신 메커니즘을 제공한다. 스마트 에너지 프로파일은 검침, 요구 응답 및 부하 제어, 가격, 문자 메시징 및 통지, 보안 및 지원 장치 목록을 정의한다. 좀 더 구체적으로, 프로파일은 어떤 장치들이 AMI 네트워크에 허용되는지(예를 들어, 게이트웨이, 전기, 수도 및 가스 미터, thermostat, 부하 제어 장치), 그리고 이 장치들 사이에 지원되어야 하는 의무적이고 선택적인 메시징을 정의하고 있다[11].

Zigbee 사양서는 2004년 처음 출판된 후 이제 실제 마켓에서 수용되기 시작하고 있는 글로벌 표준으로 성장하였다. 지그비는 낮은 데이터 율 기반, 저전력 메시 통신을 지원하는 무선 네트워킹 기술이다. IEEE 802.15.4는 물리 및 MAC(매체 접속 제어) 계층을 정의하고, 지그비는 네트워크 및 응용 계층을 정의한다.



〔그림 1〕 지그비 계층 구조



〔그림 2〕 지그비 주요 보안 기능

[그림 1] 은 지그비 계층 구조를 보여준다.

지그비는 낮은 율 (low-rate)의 WPANs (wireless personal area networks)를 위하여 IEEE 표준 802.15.4에서 정의하고 있는 물리 계층과 MAC 계층 상위에서 구축된다. 이 두 계층 위에 네트워크 계층, 응용 계층, ZDO(Zigbee device objects)와 Application Object로 구성된다. 코어에서 지그비는 메시(mesh) 네트워크 구조이다. 네트워크 계층에서는 스타 및 트리 형태, 그리고 일반 메시의 세 가지 형태의 토폴로지를 지원한다. 모든 네트워크는 한 개의 조정자(coordinator) 장치를 보유하며, 네트워크 생성 및 파라미터 제어와 기본 유지 보수 업무를 수행한다.

4.2 지그비 보안 특성

지그비 장치는 메모리 용량이 낮고, 작은 마이크로 컨트롤러 기반의 사용하기 쉬운 장치이다. 따라서 보안도 구현과 실행이 단순해야 하고, 키 저장 및 유지를 위한 오버헤드도 낮아야 한다.

지그비는 안전한 통신, 암호키의 설정 및 전송 보호, 프레임 암호화 및 장치 제어를 수행하기 위한 설비를 제공한다. 이것은 IEEE 802.15.4에서 정의된 기본 보안 프레임워크 상에서 구축된다. 이 부분의 구조는 대칭 키의 정확한 관리, 방법의 정확한 구현과 보안 정책에 의존한다.

지그비 보안 구조는 매체 접속제어(MAC), 네트워크 및 응용의 3 계층 프로토콜 스택에서 보안 메커니즘을 포함한다. MAC 계층은 자신의 보안 처리에 책임이 있으며, 상위 계층은 사용할 보안 레벨을 결정한다. MAC 계층 무결성을 위하여, MAC 헤더를 포함하여 전체 MAC 프레임이 보호된다. 따라서 소스 주소도 인증될 수 있다[12].

[그림 2] 는 지그비의 주요 보안 기능을 보여준다.

지그비 암호는 128 비트키와 AES 암호화 표준의 사용을 기반으로 한다. 암호화, 무결성 및 인증이 각 계층에서의 프레임을 안전하게 하기 위하여 적용될 수 있다. 키의 형태는 마스터, 링크 및 네트워크 키와 같은 형태가 있다. 네트워크 키가 지그비 네트워크의 모든 노드에서 공유되는 통상 키이다. 이 키는 외부 공격으로부터 인프라 및 응용 데이터를 보호한다. 지그비 표준은 키 갱신 목적으로 사용할 키 회전 형태의 대안적인 네트워크 키를 명시한다. 최소한 지그비 네트워크는 라우팅 메시지와 네트워크 합류(join) 요구와 같은 모든 네트워크 프레임을 보호하고 권한이 부여되지 않은 합류 및 불법 장치에 의한 지그비 네트워크의 사용을 방지하기 위하여 모든 장치들에 의한 네트워크 키의 사용을 필요로 한다. 링크 키는 두 통신 장치 사이에 사용되는 비밀 세션 키이다. 링크 키를 생성하기 위하여 마스터 키를 사용한다. 마스터 키는 두 장치 사이에 사용되는 장기간 보안의 기초를 제공하며, 링크 키는 두 장치 사이의 보안을 제공한다. 링크 및 네트워크 키는 주기적으로 갱신될 수 있다.

따라서, 기밀성을 보장하기 위한 기본적인 메커니즘은 키를 적절하게 보호하는 것이다. 키의 초기 설치 및 보안 정보 처리에 신뢰 관계가 필요하다. 지그비 네트워크와 같은 애드 혹(ad hoc) 네트워크는 외부 장치가 물리적으로 접근이 가능하고, 특정한 동작 조건을 미리 알 수 없기 때문에 보안을 특별히 고려하여야 한다. 보안 키 분배를 위하여 특별히 한 개의 장치를 신뢰 센터(trust center)로 지정해야 하며, 신뢰 센터는 네트워크 키를 유지하며 점대점 보안을 제공한다. 이 지그비 신뢰 센터(ZTC)가 신뢰 관리, 네트워크 관리 및 구성 관리

기능을 수행한다[12].

4.3 지그비 보안 요구사항

Smart Energy Profile 2.0에서는 보안 요구사항으로, 암호 알고리즘 및 키 크기 선택, 암호 강도, 키 설정, 신용장 메커니즘, 계층화된 패킷 보안, 네트워크 환경 보안, 응용 환경 보안, 식별, 인증, 권한부여, 감사, 관리행정, 인증서, 제안 암호 알고리즘 및 보안 정책 등에 대한 지침을 제공하여 있으며, 제시하고 있는 주요 보안 요구사항은 아래와 같다[7,11]:

암호 시스템은 최소한 128-비트의 암호 강도를 가질 수 있는 프리미티브를 사용 구축되어야 한다.

- 기밀성, 무결성, 부인봉쇄, 키 유도 및 디지털 서명용 프리미티브는 최소한 128-비트 암호 강도를 가져야 한다.
- 키 전달 스킴은 위의 암호 강도를 얻을 수 있는 인증된 키 전달 메커니즘이나 안전한 인증된 키 협상 스킴을 사용하여 설정된 키가 전송되는 기밀 메시지를 사용하여야 한다.
- 패킷 보호는 대칭 키의 사용을 권고한다.
- 대칭 키는 평문으로 전송되어서는 안된다.
- 계층 3의 패킷 보호를 위하여 IPSec을, 두 개의 IPv6 개체사이의 보안 연관(SA: security association)을 제공하기 위하여 IKE나 IKEv2의 사용을 권고하고 있다.
- 모든 네트워크 노드는 신뢰 네트워크에 대한 접근을 위하여 인증 키 협상 스킴을 사용해야 한다.
- 모든 물리적인 단위들은 식별값 혹은 장치 ID, 그리고 장치 ID에 대하여 장치 제조사를 binding하는 신용장을 가져야 한다.
- 장치들은 감사 로그를 제공해야 하고, 감사 로그 항목들은 타임스탬프 하도록 요구하고 있다.

유비쿼터스 환경에서의 지그비 기술과 보안요구사항에 대하여는 [13]을 참조할 수 있다.

4.4 보안 설계 원칙

프로세스 제어 시스템(PCS: Process Control System) 환경에 적용할 수 있는 지그비 표준에 기반한 안전한 LR-WPAN 솔루션을 만들고 설계하기 위하여 아래와 같은 보안 설계 원칙이 제시되고 있으며, 스마트 그리드에도 적용될 수 있다고 판단된다[12]:

- 심층 방어(Defense-in-Depth) 방법의 적용: 주요 임무 시스템 및 네트워크에 대한 접근을 제어하기 위하여 복수 계층의 보안 대책을 구현한다.
- 시스템의 모든 컴포넌트 분석 및 강화: 모든 유무선 네트워크, 서버, 종단 장치, 응용 소프트웨어 등의 각 요소가 보안 공격이나 구성 실패에 대하여 강화하기 위한 방법으로 분석되어야 한다.
- 다른 네트워크로부터 지그비 네트워크의 격리 및 분할: 가능하면 지그비 네트워크와 유선 네트워크는 직접 연결되지 않아야 한다. 두 네트워크 사이는 방화벽, 베스천(bastion) 호스트 혹은 보안 게이트웨이와 같은 장치에 의하여 분리함으로써, 트래픽 흐름을 더욱 효과적으로 고립, 분할 및 제어할 수 있는 보안 페리미터(perimeter)를 확립할 수 있다.
- 지그비 네트워크 입·출력 트래픽 제한: 만약 지그비 네트워크가 다른 기존 네트워크와 상호연결된다면, 최소한 소스와 목적지 주소, 서비스 포트 번호에 의하여 트래픽을 필터링해야 한다.
- 스택의 하위 계층에 802.15.4 보안 특징 실현: 지그비 보안 서비스 이외에, IEEE 802.15.4 표준에서 정의하고 있는 데로 MAC 계층에서 이용 가능한 보안을 실현해야 한다.
- 스택의 상위 계층에 지그비 보안 특징 실현: 네트워크 및 응용 계층에서, 암호, 인증 및 무결성 같은 지그비 표준이 정의한 보안 서비스를 실현해야 한다.
- 신뢰 센터의 보호를 최대화하는 기반의 보안 구조 개발: 신뢰 센터는 지그비 보안 구조의 핵심이기 때문에, 센터 컴포넌트를 안전하게 하기 위하여, 강한 보안 정책, 절차 및 기술적 통제 대책이 구현되어야 한다.

V. 결 론

2009년 7월 9일 이탈리아에서 개최된 G8 확대정상회의 기후변화 세션에서 '세계를 바꾸는 기술(전환적 기술)' 7개를 선정했는데, 이 중 스마트 그리드 기술 개발을 선도할 국가로 우리나라가 지정된바 있다. 우리나

라는 이미 지난 2009년 3월 세계 최초로 스마트 그리드 기술의 국가 단위 발전 로드맵을 작성한 바 있으며, 스마트 그리드 구축을 위한 로드맵을 올 1월에 수립한 바 있다[1].

전력망이 통신망에 융합되면서 정보통신 인프라에서 발생하고 있는 보안 문제가 전력망에서도 그대로 재현되고 있다. 따라서 전력 인프라에 대한 사이버 공격을 방지하고 대응하기 위하여 정보보호 기술이 개발단계 초기부터 고려될 필요가 있다. 만약 전력 인프라에 DDoS 공격과 같은 사이버 공격이 발생하면 국가적인 정전 사태와 같은 초유의 비상사태가 생길 지도 모른다. 따라서 국내에서도 정부와 산업체, 학계 및 연구소 등이 컨소시엄을 형성하여 점차 지능화·다양화되고 있는 사이버 공격에 대응할 수 있는 개발 전략을 수립하여야 할 것이다.

이를 위하여, 본 논문에서는 스마트 그리드, 특히 지그비-기반 AMI 시스템에서의 정보보호 기술의 필요성, 특성과 요구사항 등에 대하여 살펴보았다.

참 고 문 헌

[1] (재)한국스마트그리드사업단 스마트그리드구축 로드맵, 2010. 1.

[2] Amy Abel, "Smart Grid Provisions in H. R. 6, 110th Congress." CRS Report for Congress RL34288, 2008.

[3] 이경복, 박태형, 임종인, "정보보호정책 관점에서의 한국형 스마트 그리드 추진 방안에 관한 연구," 정보화정책 제 16권 제 4호(2009), pp.73~96.

[4] UCAIUG:AMI-SEC-ASAP, AMI System Security Requirements, V1.01, Dec. 2008.

[5] UCAIUG, Security Profile for Advanced Metering Infrastructure, Version 1.0, Dec. 2009.

[6] ASAP Red Team, Advanced Metering Infrastructure Attack Methodology, Ver. 1.0, Jan. 2009.

[7] 구본진, 장정숙, 이상철, 전용희, "Zigbee 기반 AMI 보안에 대한 연구," 2010년도 스마트그리드 연구회 학술대회 논문집, pp.39-41, 2010년 5월.

[8] DOE Office of Electricity Delivery and Energy Reliability, Integrated Communications, July 2007.

[9] 전용희. "산업제어시스템 정보보호: 개요," 정보보호학회지 제 19권 제 5호, pp. 52-59. 2009년 10월.

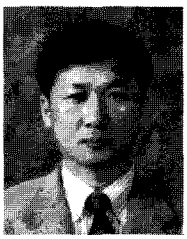
[10] 김선진, 서정해, 전종암, 표철식, "USN기반 AMI 서비스 및 기술동향: 전력 산업과 USN 산업의 융합기술," 전자통신동향분석, 제 23권 제 5호 pp.67-78, 2008.

[11] Zigbee Alliance, Zigbee Smart Energy Profile 2.0 Technical Requirements Document. Dec 2009.

[12] Ken Masica, Recommended Practice Guide, Securing Zigbee Wireless Networks in Process Control System Environments(Draft), Control Systems Security Program(CSSP), Homeland Security, April 2007.

[13] 김학범, "유비쿼터스 환경에서의 Zigbee 기술과 보안요구사항," 정보보호학회지 제 17권 제 1호, pp.79-88, 2007년 2월.

〈著者紹介〉



전 용 희 (Yong-Hee Jeon)
종신회원

1971년 3월~1978년 2월: 고려대학교 전기전자전파공학부, 학사
1985년 8월~1987년 8월: 미국 플로리다 공대 대학원 컴퓨터공학과
1987년 8월~1992년 12월: 미국 노스캐롤라이나주립 대학원 Elec. and Comp. Eng. 석사, 박사
1978년 1월~1978년 11월: 삼성중공업(주)
1978년 11월~1985년 7월: 한국전력기술(주)
1979년 6월~1980년 6월: 벨기에 벨가톰사 연수
1989년 1월~1989년 6월: 미국 노스캐롤라이나주립대 Dept of Elec. and Comp. Eng. TA
1989년 7월~1992년 9월: 미국 노스캐롤라이나주립대 부설 CCSP (Center For Comm. & Signal Processing) RA
1992년 10월~1994년 2월: 한국전자통신연구원 광대역통신망연구부 선임연구원
1994년 3월~현재: 대구가톨릭대학교 컴퓨터·정보통신공학부 교수
2001년 3월~2003년 2월: 대구가톨릭대학교 공과대학장 역임
2004년 2월~2005년 2월: 한국전자통신연구원 정보보호연구단 초빙연구원
2007년 1월~2007년 12월: 한국정보보호학회 학회지 편집위원장
2008년 1월~현재: 한국정보보호학회 부회장
2009년 1월~2010년 2월: 한국정보과학회 정보보호연구회 위원장
<관심분야> 네트워크 보안, 스마트 그리드 보안, IT 융·복합 보안, 통신망 성능분석