情 報 保 護 學 會 誌
第22卷 第5號, 2012. 8

스마트 그리드 통신망의 보안 특성, 고려사항, 구조, 설계 원칙과 연구동향에 관한 고찰

전 용 희*, 장 종 수**

요 약

여러 가지의 유·무선 통신망이 서로 연결되는 스마트 그리드 통신망은 현재 전력망에서는 존재하지 않는 취약성을 가질 것이다. 따라서 스마트 그리드 통신망에 대한 사이버 공격을 방지하고 대응하기 위하여 보안 기술이 개발단계 초기부터 고려될 필요가 있다. 본 논문에서는 국가적인 주요 인프라가 될 스마트 그리드 통신망에서의 보안 특성, 고려 사항, 구조, 설계 원칙과 연구동향에 대하여 제시하고자 한다.

Ⅰ. 서 론

기존 전력망에 정보기술(IT)을 융합하여 전력 공급자와 소비자가 양방향으로 실시간으로 정보를 교환함으로써 에너지 효율을 최적화하는 차세대 전력망이 스마트 그리드(smart grid)이다[1]. 스마트 그리드 역시 모든 IT 융합에서와 마찬가지로, 사이버 보안문제가 해결되어야 한다[2]. 미국 에너지 성(DOE: Department of Energy) Modern Grid Initiative 보고서에 의하면, 현대적인 스마트 그리드 통신망은 공격에 대한 저항성을 가질 것을 요구하고 있다[3]. 즉, 인간이 만들거나 자연적인 붕괴를 식별하고 대응하는 기술을 채택해야 하며, 실시간 통신으로 특정 영역을 고립시키거나 손상된 설비를 우회하여 전력 흐름을 변경 할 수 있도록 요구 한다.

스마트 그리드 통신망은 단일 통신망이 아닌, 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, RFID(Radio Frequency IDentification) 통신 같은 통합된 통신 형태가 될 것이다[3].

미국의 국가 하부구조 보호 계획(NIPP: National Infrastructure Protection Plan)에 의하면 사이버 보안은 다음과 같이 정의된다[3]:

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

스마트 그리드에 대한 위험 요소는 다음과 같다[2,3]:

- 복잡한 그리드에 따른 취약성이 발생할 수 있고, 잠재적인 공격 노출 및 비고의적 에러를 증가시킬 수 있다.
- 수많은 네트워크가 서로 연결됨에 따라 통상적인 취약성이 도입될 수 있다.
- 악성 소프트웨어 유입의 가능성이 증대됨에 따라, 통신 붕괴에 대한 취약성 및 서비스 거부(DoS: Denial of Service) 공격이나 소프트웨어 및 시스템 무결성이 침해될 수 있다.
- 잠재적인 공격을 위한 진입점과 경로의 수가 증가한다.
- 고객의 비밀성을 포함하여 데이터 기밀성의 침해가 가능하다.

미국 DOE에서도 현대적인 그리드를 도입하는데 해결해야 할 기술적인 장벽 중에 보안 기술을 명시하고 있다[4]. 특히 분산 에너지 자원 소유주, 독립 전력 생산자, 소비자의 수요 대응 및 자동화 검침 프로그램 등에

* 대구가톨릭대학교 IT공학부(yhjeon@cu.ac.kr)
** 한국전자통신연구원 사이버융합보안연구단(jsjang@etri.re.kr)

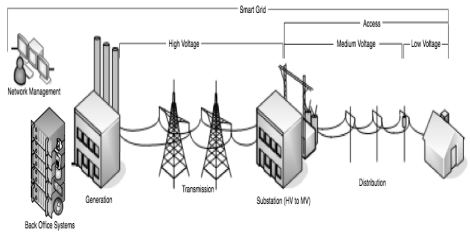
반드시 보안 기능이 구축되어야 하며, SCADA (Supervisory Control And Data Acquisition) 및 보호 계전기 시스템의 보안이 보장되어야 함을 명시하고 있다.

따라서 본 논문에서는 스마트 그리드와 같은 국가적인 주요 인프라를 보호하기 위한 보안 기술에 대하여 알아보고자 한다[5,6].

Ⅱ. 통신망 구조와 보안의 필요성

2.1 통신망의 구조와 요소

[그림 1]은 ITU-T의 스마트 그리드 일반적 모델을 보여준다[7]. 스마트 그리드는 공급자로부터 소비자까지 전력을 공급하는데 있어, 에너지를 절약하고, 비용을 절감하고, 신뢰성과 투명성을 제고하기 위하여 양방향 디지털 통신망을 사용한다.



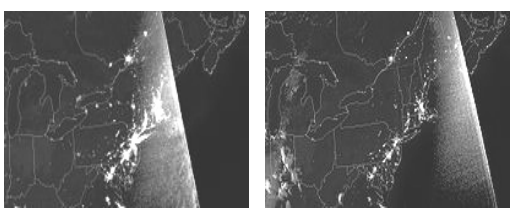
〔그림 1〕 스마트 그리드 통신망의 일반 구조

통신망은 아래와 같은 요소로 이루어진다[8].

- WAN(Wide Area Networks): 코어 네트워크/백본과 지역적인 MAN(Metropolitan Area Network)으로 이루어진다. 이 통신망은 SCADA/EMS, 고전압 전송선을 위한 보호 계전기, 발전소 자동화 및 배전 피더 자동화와 같은 전력 회사 하부구조의 안전하고 신뢰적인 운영을 위하여 필요하다.
- 유틸리티 LAN: 전력회사 운영과 기업 LAN들로 구성되며, 유무선 통신망을 통하여 WAN에 연결된다.
- Backhaul: WAN과 last mile 네트워크를 연결하는 통신망이다. 고객의 스마트 그리드 검침 데이터, 변전소 자동화 중요 파라미터 데이터 등을 모아서 전송한다.
- Last mile: 전력 분배 시스템 위에 있는 양방향 유무선 통신망이다. NAN(Neighborhood Area Network) 혹은 AMI(Advanced Metering Infrastructure)라고도 불린다.
- 고객 댁내(Customer Premise): HAN(Home Area Network), BAN(Business/building Area Network) 혹은 IAN(Industrial Area Network) 등으로 구성된다.

2.2 보안의 필요성

전력 계통의 통신 문제가 실제로 정전의 주요한 요인이 된 바가 있다. 2003년 8월 14일 미국 동북부의 정전 사고에서 제어시스템의 통신 지연이 주요한 요인이 되었다. 초기에 전력 장치 문제가 있었지만, 진행 중인 연속적인 실패(cascading failure)가 적절한 기간 내에 시스템 운용자에게 적절한 정보를 제공하지 못하는 주요 요인이 되었다. [그림 2]는 그 때 발생한 정전 사고 전후의 위성사진을 보여준다. 이 사고는 1999년 남부 브라질의 정전사고 이후 두 번째로 가장 넓게 발생한 정전사고로 기록되었다. 이 정전사고는 캐나다 온타리오 지역의 천만 명과 미국 8개 주에서 사천오백만 명에게 영향을 끼치고 사회 경제적 비용은 100억 달러에 이른 것으로 평가되었다[9].



(a) 정전 하루 전 밤 (b) 정전 당일 밤

〔그림 2〕 2003년 미국 동북부 정전 사고 위성사진[9]

광범위한 인터넷 기술을 포함하는 고도로 네트워크화 된 정보 하부구조 상의 통신과 복잡한 분산 응용을 요구하는 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.

스마트 그리드 보안 서비스가 방지하려고 하는 보안 사건의 몇 가지 예는 다음과 같다[3,10]:

- 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 여러 가지 자연적 소스와 같은 다양한 소스로부터 발생할 수 있다. 따라서 자연적 위협뿐만 아니라 악의적인 위협에 대하여 보호하기 위하여, 방어 전략을 세울 필요가 있다. 다음은 스마트 그리드에 대하여 가능한 위협을 보여주는 목록이다[11-13]:

- 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[13,14]:

- 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

Ⅲ. 스마트 그리드 통신망 보안 특성과 고려사항

3.1 스마트 그리드 통신망 보안 특성

스마트 그리드 통신망의 보안 특성은 기존 IT 시스템 보안과는 큰 차이가 있다. 예를 들어, 일반적으로 기존 IT 시스템의 보안 목적은 기밀성, 무결성, 가용성(CIA: Confidentiality, Integrity, Availability)의 순서를 따르나, 스마트 그리드에서는 그 순서가 AIC로 바뀐다.

[표 1]은 일반적인 정보 시스템과 스마트 그리드 시스템의 보안 특성의 차이점을 요약하여 보여준다[15-21].

〔표 1〕 정보 시스템과 스마트 그리드 시스템의 보안 특성 차이점

보안 특성	정보 시스템	스마트 그리드 시스템
앤티바이러스/모바일 코드	통상적 광범위한 사용	비통상적/효과적인 설치가 불가능
패치 응용	정기적 계획됨	드뭄, 비계획적 공급자 특정
변경 관리	정기적 계획됨	고도로 관리되고 복잡함
시간 민감 내용	일반적으로 지연 허용	지연 허용 안 됨
가용성	일반적으로 지연 허용	연속적 사용
보안 인식	개인 및 공공 부문에서 중간 정도	물리적 보안을 제외하고 열악
보안 시험/감사	좋은 보안 프로그램의 부분	정지에 대한 일시적 시험
물리 보안	안전	원격/무인 안전

NIST 사이버보안 워킹 그룹은 다른 그리드 시스템들 사이에 137개의 인터페이스를 식별하였다. 예를 들어, 모든 스마트 미터, 대부분의 센서, 발전소와 변전소의 주요 장비들이 통신 모듈을 가질 것이다. 이렇게 많은 다른 하드웨어와 소프트웨어 구성품들을 인터페이싱하는 것은 본질적으로 보안 취약성을 도입하기 쉽다[15].

3.2 스마트 그리드 통신망 보안 고려사항

NIST에서 기술하고 있는 AIC에 대한 사이버 보안 고려사항은 다음과 같다[13]:

1) 가용성: 전력 시스템 신뢰성을 위하여 가장 중요한 보안 목표이다. 가용성에 관련된 시간 지연은 아래와 같다.
   - 보호 계전기: 4ms 이하
   - 송전 광역 상황 인식 감지: 1초 이하
   - 변전소 및 피더 SCADA 데이터: 수초
   - 중요하지 않은 장비 및 가격 정보: 수분
   - 미터 리딩 등: 수 시간
2) 무결성: 전력 시스템 운영을 위한 무결성은 다음에 대한 보증을 포함한다.

- 인가 없는 데이터 변조 방지
- 데이터 소스의 인증
- 데이터 관련 타임스탬프는 알려지고 인증되어야 함.
- 데이터 품질이 알려지고 인증되어야 함.

3) 기밀성: 전력 시스템 신뢰성을 위하여 마지막으로 중요한 것이지만, 고객 정보에 대한 기밀성은 더 중요하다.
- 고객 정보의 프라이버시
- 전력 시장 정보
- 급여, 내부 전략 기획과 같은 일반 사내 정보

위와 같이 스마트 그리드의 보안 중요성은 AIC 순서가 되므로, 스마트 그리드 환경에 적합한 새로운 보안 솔루션이 필요하다고 할 수 있다.

[표 2]는 스마트 그리드의 응용별 보안 고려사항을 보여준다[7,13].

〔표 2〕 스마트 그리드의 응용별 보안 고려사항

응용	통신매체	프로토콜	가용성 (%)	보안 중요도
AMI	PLC, 무선, 광대역망	WiMAX, LTE, 802.15.4, 지그비	99-999.99	높음
전력수송	PLC, 무선	지그비, 802.15.4	99-99.99	비교적 높음
분산그리드 관리	광섬유, 무선, 위성, 이동통신	DNP3, IEC 61850, WiMAX, LTE 802.15.4	99-99.999	높음
지역간 통신	전화회선	IP	99.999	높음
분산 에너지 자원 및 저장	광섬유, 무선, 마이크로 웨이브, 위성	분산 그리드 관리와 같음	99-99.99	높음

위 표에서 802.15.4는 IEEE 802.15.4를 의미한다. 스마트 그리드에서 IP 프로토콜의 사용도 보안 취약성을 도입할 수 있다.

Ⅳ. AMI 보안 특성, 고려사항과 지그비 보안

4.1 AMI 보안 취약성과 특성

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[22].

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 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 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 [23-25]를 참조할 수 있다.

AMI에 대한 공격 방법은 아래와 같이 네 단계로 나누어진다[24]:

- 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.
- 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.

- 심층 분석: 초기 분석과정 동안 수집된 정보를 이용하여 시스템 기능과 잠재적인 취약성 영역을 식별하게 된다. 심층 분석 단계에서 사용될 수 있는 공격 벡터로는 fuzzing, firmware disassembly, 키 추출, 펌웨어 코드 분석, 결함 추적 및 열거, 시뮬레이션, power-glitching 공격, 클락-glitching 공격, 익스플로잇 개발, exploitation 등이 있다.
- 부당한 이용(exploitation): 심층 분석 단계 후, 공격 팀은 분석의 이용단계로 진입하며, 개발된 익스플로잇, 공격 도구와 다른 기법들이 시스템을 공격하기 위하여 사용된다.

4.2 AMI 보안 고려사항

AMI 보안을 위하여 AMI 컴포넌트에 대한 아래와 같은 제어 고려사항이 권고되고 있는데, 몇 가지만 간략하게 제시하면 아래와 같다[25]:

- 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.

AMI-SEC 태스크 포스에서는 높은 수준의 정보 보증, 가용성 및 보안을 제공하기 위하여 AMI 구현에 적용될 보안 고려사항을 제시하고 있다[23-25]. 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[25].

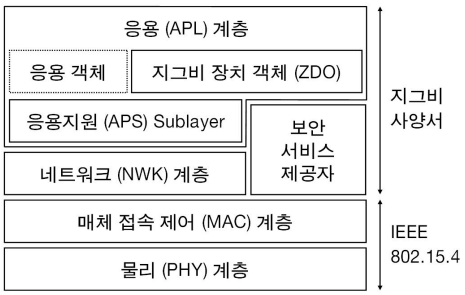
4.3 지그비(Zigbee) 보안

4.3.1 개요

AMI를 지원하기 위하여, 지그비 연합(Zigbee Alliance)에서는 Smart Energy Profile을 정의하고 재가하였다[26]. Zigbee Smart Energy는 용역회사에게 가정 내에서 에너지를 관리하기 위한 안전한 통신 메커니즘을 제공한다. 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 3]은 지그비 계층 구조를 보여준다.

지그비는 낮은 율 (low-rate)의 WPANs(wireless



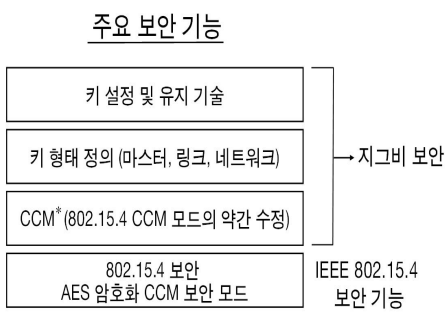
〔그림 3〕 지그비 계층 구조

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.

4.3.2 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



〔그림 4〕 지그비 주요 보안 기능

계층 무결성을 위하여, MAC 헤더를 포함하여 전체 MAC 프레임이 보호된다. 따라서 소스 주소도 인증될 수 있다[27].

[그림 4]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[27].

4.3.3 지그비 보안 고려사항

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 대

한 지침을 제공하여 있으며, 제시하고 있는 주요 보안 요구사항은 아래와 같다[26,27]:

- 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 안 된다.
- 계층 3의 패킷 보호를 위하여 IPSec을, 두 개의 IPv6 개체사이의 보안 연계(SA: security association)를 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.

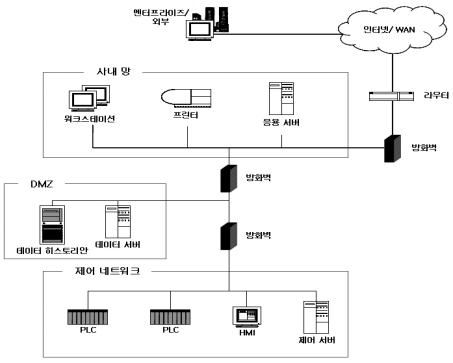
유비쿼터스 환경에서의 지그비 기술과 보안요구사항에 대하여는 [28]을 참조할 수 있다.

Ⅴ. 네트워크 보안 구조와 설계원칙[29-31]

5.1 스마트 그리드 심층-방어 보안 구조

[그림 5]는 사내 망과 산업제어시스템(ICS: Industrial Control System) 네트워크 사이에 한 쌍의 방화벽을 설치한 것을 보여준다. 데이터 서버와 같은 공통 서버는 MES(Manufacturing Execution System) 계층이라고 하는 DMZ-같은 네트워크 존 내의 방화벽 사이에 위치한다. 첫 번째 방화벽은 제어 네트워크나 공유 데이터 서버로 향하는 임의의 패킷들을 차단하고, 두 번째 방화벽은 침해된 서버로부터의 원하지 않는 트래픽이 제어 네트워크로 진입하는 것을 막아주고, 제어 네트워크 트래픽이 공유 서버에 영향을 미치는 것을 방지할 수 있다.

두 개의 다른 제조사로부터의 방화벽이 사용되는 경우 장점이 있다. 만약 어떤 조직에서 제어 그룹과 IT 그룹이 자신의 방화벽을 관리할 책임을 가진다면, 이 구조는 분명하게 분리된 장비 책임성을 가지도록 한다. 주요 단점은 비용 증가와 관리의 복잡성이다. 엄격한 보안 요구사항이나 분명한 관리 분리가 필요한 환경에 대하여, 이 구조는 몇 몇 강한 장점을 가진다.

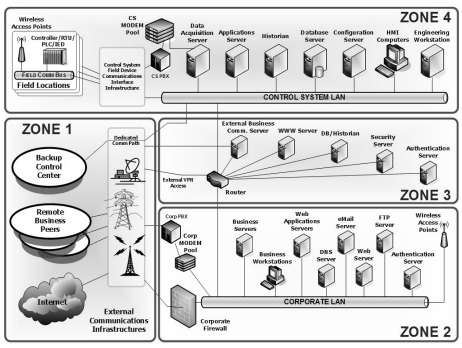


〔그림 5〕 사내 망과 제어 네트워크 사이의 방화벽 쌍

[그림 6]은 지역(zone)으로 구분된 보편적인 제어시스템의 구조를 보여준다. 스마트 그리드 통신망 보안을 위하여 이와 비슷한 심층-방어(Defense-in-Depth) 보안 구조가 가능 할 것으로 보여 여기에 소개한다. 이 zone들은 다음과 같이 구분되어 있다[20]:

- 지역 1: 인터넷, 피어 위치 및 백업 설비에 대한 외부 연결
- 지역 2: 사내 통신용 외부 연결
- 지역 3: 외부 서비스로부터의 제어 시스템 통신
- 지역 4: 프로세스-기반 혹은 SCADA 제어 시스템 운영

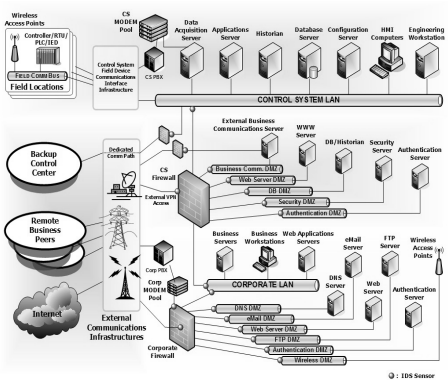
위의 지역 들은 각기 유일한 보안 요구사항을 가진다. 만약 스마트 그리드 시스템 운영 지역이 침해된다



〔그림 6〕 통상적인 구조에서의 지역[20]

면, 스마트 그리드 시스템 정보 자원의 조작은 치명적일 수 있다. 많은 부문에서 스마트 그리드 시스템에 대한 악성 공격은 실제적인 결과를 초래한다.

[그림 7]은 Control Systems Cyber Security: Defense in Depth Strategies 문서에 기술된 바와 같이 미국 국토안보부(DHS: Department of Homeland Security) CSSP(Control Systems Security Program) 권고 실제 위원회에 의하여 개발된 ICS 심층-방어 구조 전략을 보여준다.



〔그림 7〕 CSSP 권고 심층-방어 구조[20]

Control Systems Cyber Security: Defense in Depth Strategies 문서는 multi-tier 정보 구조를 유지하면서 제어 시스템 네트워크를 사용하는 조직을 위한 심층-방어 구조 전략을 개발하기 위한 지침 및 방향을 제공한다. 이 전략은 방화벽, DMZ의 사용과 ICS 구조 전체에 침입탐지 능력의 사용을 포함한다. 그림에서 여러 DMZ의 사용은 별도의 기능성에 대한 부가된 능력과 액세스 특권을 제공하고, 다른 운영 의무사항을 가진 네트워크들로 이루어진 대규모 구조를 보호하는데 매우 효과적인 것으로 증명되었다. 침입 탐지 설치는 다른 룰셋과 감시되는 각 도메인에 유일한 시그니처가 적용된다[20].

5.2 스마트 그리드 설계 원칙

5.2.1 개요

스마트 그리드 통신망 구조 설계는 일반적으로 Corporate Networks와 분리시키는 것이 권고된다. Corporate Networks에서 통상적으로 허용되는 인터넷 접근, FTP(File Transfer Protocol), 이메일 및 원격 접근 트래픽이 스마트 그리드에서는 허용되지 않아야 한다. 분리된 네트워크를 보유함으로써, 사내 망에 대한 보안과 성능이 그리드 네트워크에 영향을 미칠 수 없도록 해야 한다.

그러나 스마트 그리드와 Corporate Networks의 연결이 필요한 실제 상황이 발생할 수 있다. 만약 이런 연결이 이루어진다면, 이것이 심각한 보안 위험을 유발하기 때문에 설계 및 구현에서 주의가 요구된다. 두 네트워크가 연결되어야 한다면, 최소한의 연결을 허용하고 방화벽과 DMZ(De-Militarized Zone)를 통하는 것이 권고된다. DMZ는 방화벽에 직접 연결된 별도의 네트워크 세그먼트로써, 인터넷 접근 가능 서버와 네트워크 내의 서비스들을 보호하기 위한 버퍼 역할을 하는 네트워크 장치에 추가된 인터페이스를 의미한다.

5.2.2 방화벽

스마트 그리드 환경에서, 방화벽은 그리드 네트워크와 Corporate Networks 사이에 대부분 설치된다. 방화벽 구성이 적절하게 이루어진다면, 그리드 시스템 호스트 컴퓨터와 컨트롤러에 대한 불필요한 접근을 제한할 수 있고 보안을 증진시킬 수 있다.

방화벽은 프로세스 제어 장치에서 수행할 수 없는 다음과 같은 보안 정책을 실행해야 한다:

- 비보호 LAN과 보호된 그리드 네트워크상의 장치 사이에 특정 실행 통신망을 제외하고 모든 통신을 차단한다. 차단은 외향 및 내향 패킷 모두에 대하여 발생하며, 소스와 목적지 IP 주소 쌍, 서비스 및 포트 기반으로 이루어진다.
- 그리드 네트워크에 접근하는 모든 사용자의 보안 인증을 그리드 네트워크의 취약성에 따라 단순한 패스워드, 복잡한 패스워드, 복수-인자 인증 기술, 토큰, 바이오 메트릭 및 스마트카드 같은 특정한 방법을 사용하여 수행한다.
- 사용자의 업무 기능에 필요한 제어 네트워크상의 노드에만 접근을 제한적으로 허용함으로써, 고의적 혹은 우연적인 사고 가능성을 줄이도록 한다.
- 트래픽 감시, 분석 및 침입 탐지를 위한 정보흐름을 기록한다.
- 그리드에 적절한 운영 정책을 구현하도록 해야 한다.

그리드 환경에 방화벽을 설치할 때 다음과 같은 문제점이 존재 한다:

- 제어 시스템 통신에 지연 추가의 가능성
- 산업 응용에 적합한 규칙집합(rule set) 설계에서의 경험 부족

사이버 사고를 신속하게 탐지하고 대응하기 위하여 방화벽과 다른 보안 센서들의 실시간 감시가 필요하다.

5.2.3 그리드 네트워크의 논리적 분리

그리드 네트워크는 물리적으로 분리된 네트워크 장치 상에서 Corporate Networks로부터 최소한 논리적으로 분리되어야 한다. 연결이 필요할 때는 아래와 같은 원칙들이 지켜져야 한다:

- 그리드 네트워크와 Corporate Networks 사이에 문서화되고 최소한의 액세스 포인트만 있어야 한다.
- 그리드 네트워크와 Corporate Networks 사이의 상태(stateful) 방화벽은 분명하게 권한이 부여된 트래픽을 제외하고 모든 트래픽을 거부하도록 구성되어야 한다.
- 방화벽 규칙은 TCP와 UDP(User Datagram Protocol) 포트 필터링, ICMP(Internet Control Message Protocol) 유형 및 코드 필터링 이외에 적어도 소스와 목적지 필터링를 제공해야 한다.

그리드 네트워크와 Corporate Networks 사이의 통신을 하는 한 가지 바람직한 방법은 중간 DMZ 네트워크를 구현하는 것이다. 단지 Corporate Networks와 DMZ 사이에, 그리고 그리드 네트워크와 DMZ 사이에서 제한된 특정 통신만 발생하도록 하기 위하여, DMZ는 방화벽에 연결되어야 한다. Corporate Networks와 그리드 네트워크는 서로 직접 통신하지 않아야 한다.

5.3 지그비-기반 AMI 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 그리드 AMI에도 적용될 수 있다고 판단된다[22,26,27]:

- 심층 방어 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 상호연결 된다면, 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.

Ⅵ. 보안기술 연구 동향[30]

본 장에서는 [30]의 문헌 검토를 기반으로 스마트 그리드 보안에 대한 연구 범주를 프로세스 제어 시스템 보안, 스마트 미터 보안, 전력 시스템 상태 평가 보안, 스마트 그리드 통신 프로토콜 보안과 같이 4개로 분류

〔표 3〕 보안 연구 범주별 중요도

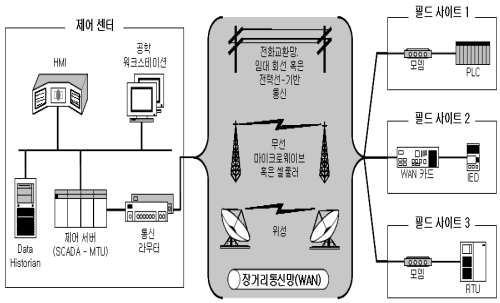
범주	중요도 표시
PCS 보안	A > I > C
스마트 미터 보안	I, C > A
전력 시스템 상태 평가 보안	A > I > C
스마트 그리드 통신 프로토콜 보안	기능에 따라 다름

* 범례. A: 가용성, I: 무결성, C: 기밀성

하여 각각에 대한 연구 동향을 소개한다[32-41]. 각 범주에 대한 보안의 중요도를 표시하면 [표 3]과 같다.

6.1 PCS 보안

프로세스 제어 시스템은 스마트 그리드에서 전력망을 감시하고 제어를 위하여 사용된다. 전통적으로 전력망은 외부망과의 연결을 가지지 않은 고립 통신망에서 운영되어 왔다. 그렇기 때문에 보통 보안 기능이 내장되어 있지 않다. 그러나 스마트 그리드에서는 외부 통신망과의 연결이 존재할 수 있기 때문에 보안이 문제가 된다. 전력망에서 가장 많이 사용되는 PCS는 SCADA 시스템이다. [그림 8]은 SCADA 시스템의 일반적 배치를 보여준다[31].



〔그림 8〕 SCADA 시스템의 일반적 배치

이와 같이, 전력 송배전망에서 지역적으로 분산된 SCADA 제어 기술을 사용한다. SCADA 시스템이 지역 원격 필드 제어 스테이션으로부터 데이터를 수집하여 전력 분배를 감시하고 제어하며 중앙 위치로부터의 명령을 내린다. 또한 물, 석유 및 가스 분배, 하수 처리 수집 시스템 등을 감시하고 제어하기 위하여 사용된다.

SCADA는 흔히 네트워크로 서로 연결된다. 이것은 전력 제어 센터와 발전 설비의 경우에 해당한다. 스마트 그리드 시스템에서 전송과 배전 명령과 생산 출력을 조정하기 위하여 SCADA 시스템과 통신 하여야 한다.

국내 주요 하부구조(Critical Infrastructure)도 물리적이고 또한 수많은 정보 통신 기술을 통하여 복잡하게 고도로 연결되어 있으며 상호 의존적이다. 한 하부구조에서의 사고가 연속적으로 증폭되어 다른 하부구조에 직·간접적으로 영향을 미칠 수 있다. 한 예로써, 전력 전송 SCADA 시스템에서 사용되는 마이크로웨이브 통신 네트워크의 붕괴로 연속적인 실패가 개시될 수 있다. 감시 및 제어 능력이 없어 대규모 발전 단위가 격리되고 전송 변전소에서의 전력 손실을 초래하는 이벤트가 발생할 수 있다. 이런 손실이 주요 불균형을 일으키고 전력 그리드를 통한 연속 실패를 야기 시킬 수 있다. 이것은 다시 대규모 정전 사태를 불러오고, 석유 및 가스 생산, 정유소 운영, 수 처리 시스템, 폐수 수집 시스템과 같은 전력에 의존하는 모든 산업에 심각한 영향을 미칠 수 있다.

PCS 보안에 대한 연구는 몇 개의 다른 이슈들을 포함하고 있고, PCS 보안 위험, 보안 평가 방법 그리고 침입탐지시스템(IDS) 등에 대하여 다루고 있다. 여러 저자들이 전력 시스템에서의 PCS 보안에 대하여 다루고 있다[30].

Watts는 [38]에서 실제 전력 시스템이 직면하고 있는 위험에 대한 검토를 수행하였다. PCS 보안에 대한 위험에 초점을 맞추고 있고 전력 시스템 보안 위험에 대한 상세하고 포괄적인 개요를 제공한다. 보안 완화 조치 목록도 구현 관심사와 함께 제공하고 있다. 이 작업에서는 전통적인 전력 시스템 보안 위험에 대하여 초점을 맞추고 있고, 스마트 그리드에 의하여 도입되는 새로운 보안 취약성에 대하여는 기술하지 않고 있다. 그러나 스마트 그리드에서도 확장하여 적용할 수 있을 것이다.

Jiaxi 등은 [32]에서 또한 여러 가지의 PCS 보안 위험에 대한 검토를 제시하고 있다. PCS 보안 위험에서의 작업은 시스템이 업데이트되거나 새로운 시스템이 설계될 때 어떤 기존의 보안 위험이 고려되도록 하기 위해서 필요하다. 이 논문은 SCADA 시스템의 취약성을 시스템, 시나리오와 접근 점의 세 가지 수준에서 체계적으로 평가하기 위하여 취약성 평가 프레임워크를 제안하고 있다.

침입탐지시스템(IDS)을 사용한 PCS 보안에 대한 작업도 수행되었다[33]. 기존의 대부분 PCS는 고립된 환경에서 운영되도록 설계되었기 때문에, 보안이 거의 고려되지 않았다. 그러나 스마트 그리드가 도입됨에 따라 PCS는 사내망(Corporate Networks)에 연결되어 조작될 수 있기 때문에 보안이 중요해진다. 사용된 IDS는 모델-기반 방법을 사용하고 시그니처 기반 방법과 보완적으로 사용된다. 그래서 알려진 공격뿐만 아니라 알려지지 않은 공격도 탐지할 수 있다고 제시하고 있다. 그러나 스마트 그리드는 매우 복잡한 시스템이기 때문에

모델-기반 방법이 문제가 될 수 있고, 정확한 모델의 설계가 어려운 것이 문제이다.

[32]에서는 또한 PCS 보안 평가 방법에 대한 연구결과도 제공하고 있다. 주로 PCS 보안 취약성을 평가하기 위한 수단 개발에 초점을 맞추고 있으며, 확률적인 평가와 통합적인 방법을 제시하고 있다.

6.2 스마트 미터 보안

스마트 미터(AMI) 보안 연구는 여러 가지 문제에 대하여 수행되고 있다. 일반적인 AMI의 취약성과 공격 방법론, AMI에서 사용되고 있는 MAC 프로토콜에 대한 취약성과 공격 방법, AMI 데이터의 비밀성 제공 등에 대한 연구가 주로 수행되고 있다. 기타 AMI 데이터 무결성에 대한 연구도 수행되었다[34]. 이 논문에서는 AMI 데이터의 정확성을 검증하는 한 가지 방법으로 별도의 전력 측정 장치를 사용하여 AMI로부터 수신한 전력 공급자 수치와 비교하는 방법을 제시한다. 전력 공급자로 보내는 계량치를 똑 같이 사용자 터미널에 전송하여 AMI 수치의 무결성을 검증하는 방법이다. 그러나 이 방법은 기밀성 문제를 야기 시킬 수 있는 것으로 보인다.

[35]에서는 스마트 미터 환경에 사용할 수 있는 명세서-기반 IDS를 제시하고 있다. 스마트 미터는 새로운 기술이고, 경험적 데이터가 부족하기 때문에 시그니처와 비정상-기반 시스템보다 더 높은 정확성을 제공할 수 있다는 것이다. 그러나 제한된 메모리와 계산력을 가지고 있는 스마트 미터에서 높은 오버헤드와 비용이 문제가 된다.

AMI 데이터는 소비자의 전력 사용 패턴에 대한 분석을 제공하기 때문에 비밀성(Privacy)이 문제가 된다. [36]에서는 AMI로부터 오는 다량의 데이터들을 익명화하는 방법을 기술하고 있다. 많은 사용자들로 부터의 빈번한 AMI 계량을 서로 연관시켜 개인의 식별을 막는 기술을 제시하고 있다. 두 개의 다른 식별자를 통하여, 하나는 빌링(요금청구)과 연관된 검침이고, 다른 식별자는 익명 검침을 위하여 사용된다. escrow는 그 두 개의 식별자 사이의 연관성을 아는 유일한 시스템이다. 이 시스템은 사용자의 집단 속에 개인의 신원을 숨기는 방법을 제공한다.

AMI 데이터의 비밀성에 대한 연구도 수행되었다. [37]에서는 소비자의 행위 패턴을 숨기기 위하여, 전기 에너지 흔적(시그너처)을 변환하는 방법을 제공한다. 전력 사용 시그너처는 냉장고, 세탁기, 전자 오븐 등의 전력 사용패턴을 보여주는 그림이다. 에너지 저장 장치로부터 전력 수요 부분을 offsetting 하여 소비자 가정 내의 전기 장치의 부하 시그너처를 숨기는 기능을 사용한다. 고객이 즉시 이용할 수 있는 다른 소스로 부터의 전력 스트림을 가져올 수 있는 배터리와 전력 스위치를 가정한다. 이 장치들을 이용하여, 전기 에너지 부하 시그너처의 모습을 변환하기 위하여 배터리로부터 임의양의 전력을 가져옴으로써 가정외부 네트워크로부터 소비자의 전기 에너지 시그너처는 감춰지게 되는 방법이다. 이렇게 함으로써 외부 관찰자에게 전력 사용 패턴을 난독하게 만든다. 이 시스템이 성공하기 위하여 배터리의 효율성이 중요하며, 재생 에너지 소스와도 통합의 가능성도 제시하고 있다.

이외에도 AMI 데이터의 비밀성에 대한 많은 연구가 수행되었다. NIST에서는 시스템이 아닌 데이터에 대하여 더욱 초점을 맞추고 있다[13,38]. AMI에 의하여 생성될 수 있는 가능한 비밀성 위험에 대한 검토도 제공하고 있다.

6.3 전력 시스템 상태 평가 보안

전력 시스템 상태 평가 보안은 스마트 그리드 사이버 보안 연구의 또 다른 범주에 속한다. 스마트 그리드는 전력 시스템의 실제적인 특성을 제어할 능력을 가지는데, 이것은 전력 그리드 내에서 스마트 그리드가 안정 상태(stable state)를 유지하도록 행해진다. 스마트 그리드는 전력 시스템의 정보를 가지고, 결정하고 조처를 취하기 위하여 현재 상태를 모델 하여야 한다. 상태 평가 모델은 PCS의 일부가 될 수 있다. 전력 시스템 상태 평가 모델의 보안은 전력 시스템을 유지하기 위하여 스마트 그리드에 의하여 사용되기 때문에 중요하다. 가용성이 제일 중요하고, 그 다음에 무결성이 중요하다. 기밀성은 실시간 시스템에 대하여 오버헤드를 부가하기 때문에 제일 중요하지 않은 목표이다.

[39]에서는 거짓 데이터 주입(false data injection) 공격에 대한 연구를 수행하였다. 이 공격은 상태 평가 모델에서 전력 시스템 상태를 변경하기 위하여 사용될 수 있다. 스마트 그리드 상에서의 거짓-데이터 주입 공격

의 영향을 보여주고, 공격의 영향을 전력 시장의 가격 조작에 의한 금전적 이득으로 측정한다. 이 연구는 금전적 이득을 위하여 이용될 수 있는 스마트 그리드의 가능한 공격의 하나를 보여주고 있다고 하겠다.

또한 이 논문에서는 상태 평가 모델에 대한 거짓-데이터 주입 공격을 발견하고 경감시키기 위한 연구를 수행하였다. 조작에 취약한 입력 소스 플로우를 식별하기 위하여 사용될 수 있는 보안 지수(security index)를 계산할 수 있는 연구와 거짓-데이터 주입 공격에 대하여 어떤 보안이 필요한지 식별하기 위한 알고리즘 생성에 대한 연구가 수행되었다. 이 알고리즘은 가장 이익이 되도록 암호화 입력 소스 통신을 어디에 설치해야 하는지 그 위치를 식별하기 위하여 사용될 수 있다.

기타 상태 평가 모델의 보안을 위하여 필요한 통신 채널 용량을 결정하기 위하여 통신 이론에 초점을 맞추고 있는 연구, 스마트 그리드 상태 평가를 침해할 수 있는 공격에 대한 연구를 수행하였다[30,40]. 관측될 수 없는 공격과 관측할 수 있는 공격의 두 가지 범주로 나누고, 관측할 수 없는 공격을 수행하는데 요구되는 가장 작은 수의 공격자들을 찾고, 관측할 수 있는 공격에 대한 대응 방법에 대한 연구를 수행하였다.

6.4 스마트 그리드 통신 프로토콜 보안

스마트 그리드 통신 프로토콜이 스마트 그리드 보안 연구의 다음 범주이다. 스마트 그리드가 제대로 동작하기 위하여 여러 다른 컴포넌트로부터의 통신에 의존한다. 각 컴포넌트들은 다른 통신 요구사항들을 가지고 있고, 매우 낮은 지연부터 높은 데이터 처리율까지 다르다. 그리고 각각은 그 나름대로의 보안 요구사항들을 가진다. 스마트 그리드는 다양한 연결 요구사항들을 만족하기 위하여 많은 통신 프로토콜들을 필요로 한다. 스마트 그리드 통신 프로토콜의 보안은 네트워크 통신이 스마트 그리드의 중추이기 때문에 중요하다.

[41]에서는 스마트 그리드 인증 프로토콜을 설계할 때 사용할 수 있는 설계 원칙의 집합에 대하여 제시하고 있다. 인터넷-기반 인증 프로토콜의 설계 원칙을 기반으로 스마트 그리드에서 중요한 보안 목적에 맞도록 수정하였다.

Ⅶ. 맺음말

2009년 7월 초에 발생한 7.7 DDoS 공격처럼, 만약 전력 인프라에 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. 따라서 본 논문에서는 스마트 그리드 도입에 따른 보안 기술의 특성, 고려사항, 구조, 설계 원칙과 연구 동향에 대하여 기술하였다.

기존의 IT 시스템은 “data를 처리하기 위하여 physics”를 이용하는 반면에, 스마트 그리드와 같은 제어시스템은 “physics를 처리하기 위하여 data”를 이용하는 근본적인 차이가 존재한다. 그러므로 기존 IT 시스템을 위한 보안 기술이 스마트 그리드 시스템의 보안을 위한 필요 메커니즘이 될 수는 있지만, 스마트 그리드 시스템의 심층-방어를 위하여 충분하지 않을 수 있다. 따라서 스마트 그리드 시스템의 보안 특성에 대한 충분한 이해를 바탕으로 국가 주요 정보 하부구조를 구성하고 있는 스마트 그리드 시스템 보안 기술 개발 및 구현에도 관심을 기울어야 할 것으로 생각된다.

참고사항

본 논문의 완성도를 위하여 그동안 저자가 발표하였든 논문 내용 중 일부를 이용하였음을 밝혀둡니다.

참고문헌

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

[2] 전용희, “지능형 전력망(Smart Grid)과 정보보호”, 정보보호학회지 제 19권 제4호, 한국정보보호학회, 2009년 8월.

[3] U.S. Department of Energy, National Energy Technology Lab., Modern Grid Initiative, http 검색 자료.

[4] DOE Office of Electricity Delivery and Energy Reliability, Barriers to achieving the modern grid, July 2007.

[5] 정수환, “융합보안 R&D 이슈 및 방향”, 정보보호

학회지 제 19권 제 3호, 한국정보보호학회, pp. 11-13, 2009년 6월.

[6] 전용희, 스마트 그리드의 취약성, 특성, 설계 원칙 및 보안 요구사항 분석, 정보보호학회지, 제 20 권, 제 3호, pp. 79-89, 2010. 6월.

[7] ITU-T Technical Paper, Series G for Smart Grid Applications, June 2010.

[8] NIST PAP 01, The Role of IP in AMI Networks for Smart Grid, Oct. 24, 2009.

[9] Northeast Blackout of 2003, Wikipedia, Retrieved in April, 12, 2011.

[10] Arvid Kjell, Guide to Increased Security in Process Control Systems for Critical Societal Functions, The Swedish forum for information sharing concerning information security-SCADA and Process control systems(FIDI-SC), Swedish Emergency Management Agency, Oct. 2008.

[11] 전용희, "산업제어시스템 정보보호: 개요", 정보보호학회지 제19권 제 5호, pp. 52-59, 한국정보보호학회, 2009년 10월.

[12] Patrick McDaniel and Stephen McLaughlin, Security and Privacy Challenges in the Smart Gird, Secure Systems, May/June, pp. 72-74, IEEE, 2009.

[13] NIST, NISTIR 7628, Guideline for Smart Grid Cyber Security: Vol. 1, Aug. 2010.

[14] Cisco White Paper, Security for the Smart Grid, 2009.

[15] NIST(National Institute of Standards and Technology), U.S. Department of Commerce, Special Pub. 800-82, Final Public Draft, Guide to Industrial Control Systems (ICS) Security, Sep. 2008.

[16] Wikipedia encyclopedia, Industrial Control Systems, May, 2009.

[17] Wikipedia encyclopedia, SCADA, July, 2009.

[18] 이철수, "산업제어시스템 정보보안 감리 프레임워크 연구", 정보보호학회논문지, 제 18권 제 1호, pp. 139-148, 한국정보보호학회, 2008년 2월.

[19] Alvaro A. Cardenas et al., "Research Challenges for the Security of Control Systems", Proceedings of the 3rd conference on Hot topics in Security, 2008.

[20] Homeland Security, Control Systems Security Center, Control Systems Cyber Security: Defense in Depth Strategies, May 2006.

[21] ISA 99, Security for Industrial Automation and Control Systems, 2009.

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

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

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

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

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

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

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

[29] Alcatel/Lucent, Smart Choices for the Smart Grid, Technology White Paper, Retrieved in Feb, 2011.

[30] Todd Baumeister, Literature Review on Smart Grid Cyber Security, University of Hawaii, Dec. 2010.

[31] 전용희, "산업제어시스템 보안을 위한 네트워크 설계 및 구조" 정보보호학회지 제 19권 제 5호, pp. 60-67, 한국정보보호학회, 2009년 10월.

[32] Y. Jiaxi, M. Anjia, and G. Zhizhong, Cyber Security Vulnerability Assessment of Power Industry, IEEE, 2006.

[33] A. Valdes and S. Cheung, "Intrusion Monitoring in Process Control Systems," in Proceedings of the 42nd Annual Hawaii International

Conference on System Sciences HICSS, pp. 1-7, 2009.

[34] D. P. Varodayan and G. X. Gao, “Redundant Metering for Integrity with Information Theoretic Confidentiality,” in 2010 First IEEE International Conference on Smart Grid Communications, pp. 345-349, 2010.

[35] R. Berthier, W. H. Sanders, and H. Khurana, “Intrusion Detection for Advanced Metering Data,” in 2010 First IEEE International Conf. on Smart Grid Communications, pp. 350-355, 2010.

[36] C. Efthymiou and G. Kalogridis, “Smart Grid Privacy via Anonymization of Smart Metering Data,” in 2010 First IEEE International Conf. on Smart Grid Communications, pp. 238-243, 2010.

[37] G. Kalogridis et al., “Privacy for Smart Meters: Towards Undetectable Appliance Load Signatures,” in 2010 First IEEE International Conf. on Smart Grid Communications, pp. 232-237, 2010.

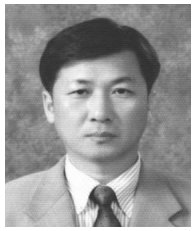
[38] D. Watts, “Security and Vulnerability in Electric Power Systems,” in 35th North American Power Symposium 2003, pp. 559-566.

[39] L. Xie, Y. Mo, and B. Sinopoli, “False Data Injection Attacks in Electrity Markets,” in 2010 First IEEE International Conf. on Smart Grid Communications, pp. 226-231, 2010.

[40] G. Dan and H. Sandberg, “Stealth Attacks and Protection Schemes for State Estimators in Power Systems”, in 2010 First IEEE International Conf. on Smart Grid Communications, pp. 214-219, 2010.

[41] H. Khurana et al., “Design Principles for Power Grid Cyber-Infrastructure Authentication Protocols,” In Hawaii International Conference on System Science, 2010.

〈著者紹介〉



전 용 희 (Yong-Hee Jeon)

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

장 종 수 (Jong-Soo Jang)

1984년: 경북대학교 전자공학과 학사
1986년: 경북대학교 대학원 전자공학과 석사
2000년: 충북대학교 대학원 컴퓨터공학과 박사
1989년 7월～현재: 한국전자통신연구원 사이버융합보안연구단 책임연구원
<관심분야> Network Security, 정책기반보안관리, 비정상트래픽탐지, 유해정보차단