한국컴퓨터정보학회 하계학술대회 논문집 제19권 제2호 (2011. 6)

Smart Meter의 Gateway에 대한 접근제어와 취약점 분석

이재현°, 박대우*
°*호서대학교 벤처전문대학원 IT응용기술학과
e-mail: leejh9708@paran.com, prof1@paran.com

A Study on Access Control and Vulnerability Analysis about Smart Meter Gateway

Jae-Hyun Lee°, Dea-Woo Park*
°*Dept. of IT Application Technology, Hoseo Graduate School of Venture

● 요 약 ●

인류를 구할 8가지 기술 중 한가지로 스마트 그리드(Smart Grid)가 소개된 바 있다. 즉 에너지 사용의 효율성을 높여 전력량과 비용을 줄이고 전력 공급자와 소비자 간의 실시간 정보교환이 가능한 지능형 전력망이라 할 수 있다. 그러나 스마트 그리드의 취약점들로 인하여, Smart Meter가 해킹을 당해 정전으로 인한 대규모 피해가 예상 될 수 있다. 본 논문에서는 Smart Meter에 대한 취약점 분석을 실시하고, Smart Meter의 Gateway 보안을 위해서 접근제어와 인증을 통해, 사용자의 접근과 개폐에 대한 보안을 실시한다. 범죄가 발생했을 포렌식 자료를 통한 법적 책임에 관한 내용을 연구한다.

키워드: 지능형 전력망(Smart Grid), 스마트 계량기(Smart Meter), 게이트웨이(Gateway), 접근제어(Access Control)

I. 서론

이태리와 한국이 공동으로 스마트 그리드 선도국으로 지정된 이후 2010년 1월 25일 지식경제부는 「스마트 그리드 로드맵」을 확정하고, 세계 최초로 국가단위의 지능형 전력망 구축 비전을 발표하였다.

스마트 그리드 서비스가 제공되기 위해서는 먼저 망 내 통신의 환경적 특정을 파악해야 한다. 스마트 그리드에는 변전소 내, 제어센터 간, 고객 간 등 다양한 통신 환경이 존재하는데, 대부분의 통신 환경들은 인터넷 통신보다 보안성이 강화된 통신을 요구한다.

2003년 미국 북동부오 캐나다 남부지역의 8개 주에 걸쳐 대규모 정전사태로 공장운영이 중지되고, 뉴욕, 클리블랜드, 디트로이트, 토론토를 포함한 북동부 주요 산업 중심지역이 정전사태로 인해 미국, 캐나다 양국은 40~60억 달러에 이르는 피해규모가 발생한 것으로 보고되고 있다[1].

이와 같은 사태는 영화 다이하드 4에서 보여 주었던 내용이다. 즉 불법적인 해커가 스마트 그리드 전력망에 접근하여 해킹을 통해 대규모 정전 사태를 발생시키고, 국가의 전력 인프라를 마비시키는 것으로 묘사 되고 있다.

즉 스마트 그리드의 IP 네트워크상에서 제기되는 취약점으로 인해 해커의 불법적인 공격과 위협들이 문제가 되고, 스마트 그리드 전력망에서 Smart Meter의 구축 과정에서 계량기의 보안성 강화를 필요로 한다[2].

따라서 스마트그리드의 기능적인 안전성, 신뢰성 확보를 위해서는 사이버 보안 위협에 대해 대책 마련이 시급하다. 스마트 그리드에서 안정적인 접근제어와 동작을 위해서는 보안 인증과 접근제어가 뒷받침 되어야 한다.

본 논문에서는 1장에서는 스마트그리드의 문제점과 보안의 필요성에 대해서 살펴본다. 2장에서는 스마트그리드의 개념, 구조, 네트워크, 구현기술 미국의 전력 인프라 정책에 대해서 알아본다. 3장에서는 Smart Meter의 개념과 취약점에 대해서 분석하고 4장에서는 계량기, Gateway의 보안점에 대해 제시하고 5장에서는 결론과 향후 과제로 마무리한다.

II. 관련 연구

2.1 스마트 그리드 개념

스마트 그리드는 그림 1과 같이 현대화된 기술전력과 정보통신기술의 융·복합을 통하여 구현된 IT전력시스템 과 관리체계를 의미한다.

그림 1. 홈 스마트 그리드 적용
Fig. 1. Apply Smart Grid Home

이는 단순한 설비 관리의 고도화를 넘어서 통합 정보지식 플랫폼(consolidated knowledge platform)을 구축한다.

소비자에게 일방적으로 전기를 공급하는 공급자 위주의 단방향 구조에 IT 기술을 이용하여 사용자에게 전력을 제공한다. 기존의 전기 공급 위주에서 IT, 통신, 자동차, 가전, 건설, 에너지 등 다양한 업종을 에너지 차원에서 융합되고 있다[3].

스마트그리드가 구축되면 소비자는 IT 기술의 적용으로 전기 사용 요금과 사용량 정보를 실시간으로 알 수 있게 되고, 비용이 경제적인 시간대를 선택하여 전기를 사용할 수 있게 된다.

2.2 스마트 그리드의 구조와 네트워크

그림 2와 같이 스마트 그리드는 에너지 네트워크와 통신 네트워크가 합쳐진 지능형 전력망 네트워크이다.

조명, 경보시스템, 전화, 컴퓨터, 인터넷 연결, 그리고 가전제품과 오락 기계 등과, 플러그 접속식 하이브리드 전기자동차와 축전까지 정보처리 상호 운용성이 가능하다[4]. 표 1은 기존 전력망과 스마트 그리드 구조 비교이다[5].

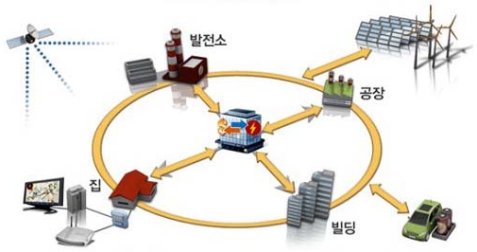

그림 2. 스마트 그리드 네트워크
Fig. 2. Smart Grid Network

표 1. 기존 전력망과 스마트 그리드 구조 비교
Table 1. Compared to the existing electricity grid and smart grid structure

항 목	기존 전력망	스마트 그리드
통제시스템	아날로그	디지털
발전	중앙집중형	분산형
송·배전	공급자 위주 (단방향)	수요공급 상호작용 (양방향)
전력공급원	중앙전원, 화석연료 위주	분산된 전원의 증가 (태양력, 풍력, 전기차)
고장진단	불가능	자가진단
고장제어	수동복구	반자동복구 및 자가 치유
설비점검	수동	원격
제어 시스템	국지적 제어	광범위한 제어
가격정보	제한적 (한 달에 한번 총액만)	실시간으로 모든 정보 열람
가격제	사실상 고정가격제	실시간 변동가격제
전력수요	급변(수요에 의존)	거의 일정(가격에 의존)
소비자 구매 선택	제한적	다양

2.3 스마트 그리드 구축 기술

스마트 그리드 분야는 전력과 IT기술을 융합하여 다양한 서비스를 가능하게 하는 AMI(Advanced Metering Infrastructure) 시스템과 발전, 송전 및 배전망의 전력계통 고도화, 신재생 에너지의 활용, 전기자동차 등 에너지 및 환경 관련하여 이슈가 되고 있는 기술들 중 전기와 관련된 직간접적으로 관계를 맺고 있다[6].

개방형 아키텍처, 강화되는 규제, 진화하는 표준 등으로 Smart Meter가 발전하고 있다.

2.3.1 개발형 표준

계량인프라는 미국 스마트 그리드 상호운영성 프레임워크 프로젝트(US Smart Grid Interoperability Framework project), 유럽 집행위의 스마트 그리드 표준, IEEEP 2030 스마트 그리드 표준과 같은 대규모의 개방형 표준화로 연결되고 있다.

2.3.2 IP(Internet Protocol) 전환

IP를 적용하면서 개방형 아키텍처로 개발되고 있다. 시스코, GE, 구글과 같은 기업들은 스마트 그리드 사업을 추진하면서 IP 적용범위를 확대하고 있다. 미국의 전력회사인 Duke는 시스코와 스마트 그리드 사업을 협력하면서 엔드 투 엔드 스마트 그리드 통신 아키텍처를 IP 기반에서 구축하고 있다. 또한 Smart Meter 시스템은 미국과 호주에서 IP 주소를 부여한 채 1,200만 개 이상이 보급 중이다.

2.3.4 홈 영역 네트워크(Home Area Network)

스마트 그리드 공급으로 Smart Meter가 보급되면서 세계적으로 약1억 대의 새로운 Smart Meter가 2015년까지 설치될 것으로 전망한다. 특히 가정 내의 에너지 관리 프로그램과 서비스를 위해 홈 영역 네트워크에 게이트웨이를 가질 것으로 보인다. ON World가 미국의 77개 유틸리티를 대상으로 한 설문조사에 따르면, 21%가 모든 Smart Meter에 홈 영역 네트워크 게이트웨이를 계획하고 있었다[7].

2.4 한국의 스마트 그리드 정책

한국은 2010년 주요 8개국(G8) 기후변화 주요국 회의에서 스마트 그리드 선도국가로 선정되었다[10]. 한국전력과 국책과제로 '스마트 그리드 실증단지 구축사업'을 추진 중이며 현재 기본설계를 완료하고 제주도를 실증단지 부지로 선정한 상태이다. 2010년에 본격적인 기술실증에 착수하여 2011년부터는 스마트 그리드 시범도시를 중심으로 대규모 보급을 개시하고 2020년까지는 소비자 측 지능화, 2030년까지는 전체 전력망지능화를 완료를 계획하고 있다.

III. Smart Meter 보안 취약점 분석

3.1 Smart Meter 분석

그림 3. 스마트 계량기
Fig. 3. Smart meter

가정에서 사용하는 Smart Meter는 전기와 가스사용 요금, 탄소 발생량을 실시간으로 모니터링 할 수 있는 계량기 및 데이터 전송시스템. 에너지 사용정보는 사용자의 휴대용 단말기 및 무선전화기, TV나 컴퓨터로도 전송이 가능하다. 그림 3은 Smart Meter이다.

- Smart Meter 공급업체는 가구마다 방문하는 계측 인력도 절감할 수 있게 되고 실시간 에너지 사용량 집계가 가능해 짐으로써 시간대별 에너지 수요를 보다 정확히 예측해 안정된 에너지 공급 및 시간대별(peak time/off-peak time) 혁신적인 가격 차별화 서비스를 제공 가능하다.
- 소비자는 Smart Meter를 이용하여 에너지 소비량이 많은 식기세척기와 같은 전기제품을 피크타임을 피해 사용함으로써 전기료를 절약하고 에너지 공급업체들은 일일 에너지 사용 변동폭을 줄일 수 있는 장점이 있다.
- 주택의 지붕 태양광패널이나 풍력발전을 통해 생산된 전력을 Smart Meter를 통해 스마트 전력망(Smart Grid)으로 다시 팔 수 있게 된다.

3.2 Smart Meter 취약점 분석(미국사례 중심)

해외 스마트 그리드는 각각의 로컬 네트워크가 확장하여 다른 로컬 네트워크와 다시 융합하여 전체 네트워크를 구성한다. 만약 이점을 이용해 해커가 스마트그리드로 연결된 계량기 한곳을 침투한다면 모든 Smart Meter를 조종할 수 있는 권한을 갖는 것과 같다.

2009년 3월에 미국 라스베이거스에서 열린 '블랙햇 보안 컨퍼런스'에서 Smart Meter의 취약성은 입증 됐다. 미국 전문 보안전문 회사인 IOActive는 자사의 연구 결과를 바탕으로 스마트 그리드 계량기에 커다란 보안 취약점이 존재한다고 보고하였다. 보고 내용은 Smart Meter의 프로토콜 변경, 버퍼 과다, 루트킷(rootkits), 코드 증식과 같은 보안 취약점들에 노출되어 있음을 확인하였다.

다른 보안회사인 InGuardian의 Wright는 Killerbee라는 공개 소스 해킹 툴을 이용해 ZigBee의 공개적인 암호화 키들의 교환을 통해 해킹하였다. ZigBee 프로토콜을 수신할 수 있는 무선기기를 이용하면 원격으로 특정인의 전원공급을 차단시키는 등 해킹을 할 수 있다.

이러한 Smart Meter의 취약점을 이용하여, 해커는 건물 전체의 모든 Smart Meter를 조종하면서, 전기 공급을 끊거나 전력회사에 한 번에 엄청난 양의 전기를 요구, 과부하를 일으킬 수 있다.

3.3 Gateway 취약점 분석

스마트 그리드에서 Smart Meter를 통한 Gateway는 Bluetooth, Zigbee, 전력선통신(PLC), RS-232, USB, FTTH, PSTN, VoIP 등 통신을 지원하는 장비이다. 초고속통신 및 네트워크 관련 통신 방식을 추진되고 있는 IT서비스 및 기술개발의 내용들이 전력 인프라의 물리적, 사이버 보안에 대한 취약점으로 사이버 공격에 대한 위험에 노출되어 있다.

Smart Meter를 통한 Gateway는 모든 근거리 관련 기술을 기반으로 한 기능들을 제공하고 있어 로컬 네트워크, 데이터 메시지 흐름 그리고 외부 IP호스트에서의 명령어 실행 등의 투명한 접근 및 제어를 가능하다.

따라서 Gateway를 기반으로 통신이 필요할 때는 웹 서버를 통해 게이트웨이의 관리 인터페이스와 직접적으로 연결하여 진행 할 수 있으며 스마트 그리드 전체 네트워크에 접속 할 수 있는 경로를 확보하여 불법적인 공격을 통한 피해를 유발 시킬 수 있다.

IV. Smart Meter 보안

4.1 Smart Meter의 보안

스마트 그리드에서 Smart Meter 데이터의 무결성 보장, 데이터의 보안 전송 디바이스 상호인증 등에 대한 표준이 확립되지 않았다.

따라서 계량기의 연동되는 기기들의 상호연관성을 관찰하고 대응할 수 있는 정보보호 기준이 제시되어야 하고, 권한관리, 접근제어, 암호화에 대한 표준이 마련되어적용되어 성능평가 후에 인증을 받아야 한다.

즉 전자서명, 스마트카드, 신분증명서 등을 이용해 전력망에 접속할 때, 인증을 받아야 서비스를 이용할 수 있도록 하여야 한다. 또한 스마트 그리드에서 개인의 프라이버시 정보와 해킹 및 보안 문제에 대한 사전 차단이 이루어져야 한다.

스마트 그리드에서 Smart Meter 보안을 위해서는 전력망 사용자에 대한 전사서명을 디지털 문서 인증 및 디지털 증거의 허용성 확보를 위해 PKI시스템을 활용하여 공인인증서와 디지털서명 등을 이용한 Smart Meter의 개폐 및 접근 제어를 실시하며, 만약 사이버 사고가 발생 할 시에 법적인 증거자료를 확보 할 수 있는 포렌식 증거 확보에 대한 포렌식 절차가 필요하고, 폴헨식 자료를 위한 실시간 감사 로그 기록의 저장과 저장된 자료의 이중 저장을 통해 무결성을 확보하는 포렌식 업무에 관한 표준도 제시되어야 한다.

4.2 Gateway 접근제어 및 인증보안

스마트 그리드에서 Smart Meter 데이터의 게이트웨이의 인터페이스에서 Zigbee가 내장된 장치와 게이트웨이 사이의 보안을 다루는 국제적인 보안 표준안이 제시되어야 하고, 이를 위해서 Work Group을 결성하여, 생산자와 학계, 각국의 표준기관들이 협의하여야 한다.

또한 Smart Meter와 Gateway의 접근제어 및 인증보안에 관한 제품 인증을 받을 때, 상호 인증을 통한 국제적인 기준과 호환성이 정의되고, 제품의 생산 유통 관리에 대한 국제 표준을 정해야 한다.

V. 결론

한국은 스마트 그리드의 선도 국가로서 Smart Meter에 대한 보안을 강화하기 위한 접근제어 및 인증체계의 표준이 확립되어야 한다. 특히 PC나 다름없는 Smart Meter와 Gateway의 접근제어 및 인증보안의 인증을 통해 보안성을 확보 하여야 한다.

따라서 본 논문에서는 스마트그리드의 스마트계량기 접근제어 및 인증의 필요성에 대해서 연구하였으며, 인가된 사용자만이 정보를 확인하고 접근할 수 있도록 통신보안에 대한 국제적인 표준화 체계가 필요함을 강조하였다.

향후 연구로는 스마트 그리드에 대한 실증단지를 구축하고 모의 해킹과 취약점 분석을 통해 안정성과 보안성을 강화한 스마트 그리드에 대한 보안 연구가 필요하다.

참고문헌

[1] 윤인하, “최근 미국 동부지역의 정전사태와 미국 전력산업의 문제점”, Asia-Pacific Review, 2003. 9.

[2] 오병민, “스마트 그리드 보안 위협 이미 나타나”, 보안뉴스, http://www.boannews.com, 2009. 11.

[3] 이일우, 한동원, “IT기반의 스마트그리드 기술”, 한국정보기술학회, 제 7권 제 1호, pp.25-30, 2009.

[4] 정영곤, 최현우, 염홍열, “스마트 그리드 보안 동향”, 정보보호학회지, 제 20권 제 4호, pp.66-79, 2010.

[5] 박남제, “스마트 그리드 환경에서의 개인정보 취약점 분석과 보호 방안”, 한국정보기술학회, 제 8권 제 9 호, pp.189~197, 2010.

[6] 강민구, 신호진, “ZigBee의 저전력화와 채널간섭 분석”, 인터넷정보학회, 제 11권 제 3호, pp.33~41, 2010.

[7] ZigBee Alliance, “Advanced Metering Infrastructure Market Requirements Document,” 2007.

[8] 김영명, 이영우, “스마트 그리드 서비스에 대한” 고객 수용도 분석”, 제 35권 제 9호, 2010.

[9] NDSL, “스마트 그리드 부문 기술 트랜드”, 글로벌동향브리핑(GTB), 2009.

[10] 한국스마트그리드협회, http://www.k-smartgrid.org