한국컴퓨터정보학회 하계학술대회 논문집 제19권 제2호 (2011. 6)

Smart Grid에서 사용되는 Smart Meter에 대한 공격 및 보안 방법 연구

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

A Study on Offensive and Security Method about Smart Meter in Smart Grid

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

● 요 약 ●

우리나라에서도 2010년 1월 25일 지식경제부의 “Smart Grid 로드맵” 확정으로 Smart Grid 사업이 진행 중이다. 그러나 정보통신 환경에서 발생하고 있는 다양한 공격에 대한 보안위협이 Smart Meter에서도 발생하고 있다. 따라서 본 논문에서는 Smart Grid에 사용되는 Smart Meter 공격을 분석하고 Smart Meter 방어 방안을 제시한다.

키워드: 지능형 전력망(Smart Grid), 스마트 계량기(Smart Meter), 보안 위협(Security Threat), 보안 방법(Security Method)

I. 서론

2010년 1월 25일 지식경제부는「Smart Grid 로드맵」을 확정하고, 세계 최초로 국가단위의 지능형 전력망 구축 비전을 발표하였다[1].

Smart Grid 서비스가 제공되기 위해서는 먼저 망 내 통신의 환경적 특정을 파악해야 한다. Smart Grid에는 변전소 내, 제어 센터 간, 고객 간 등 다양한 통신 환경이 존재하는데, 대부분의 통신 환경들은 인터넷 통신보다 보안성이 강화된 통신을 요구한다.

즉 Smart Grid의 IP 네트워크상에서 제기되는 취약점으로 인해 해커의 불법적인 공격과 위협들이 문제가 되고, Smart Grid 전력망에서 Smart Meter의 구축 과정에서 Smart Meter의 보안성 강화를 필요로 한다[2][3].

따라서 Smart Grid의 기능적인 안전성, 신뢰성 확보를 위해서는 사이버 보안 위협에 대해 대책 마련이 시급하다. Smart Grid에서 안정적인 접근제어와 동작을 위해서는 Smart Meter에 공격에 대한 방어가 뒷받침 되어야 한다.

II. 관련 연구

2.1 Smart Grid의 정의

Smart Grid는 그림 1과 같이 자동화된 송배전 기기들로 구성되어 있어 안정적이고 효율적인 에너지 소비 방식으로 운영되는 전력시스템으로 사고에 대한 자가복구 기능을 갖추고 있어 에너지 시장의 수요에 대응할 수 있다[4].

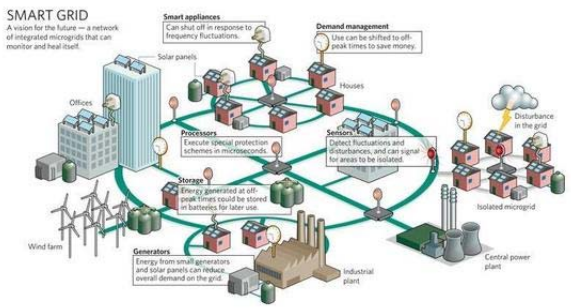

그림 1. Smart Grid 개념도
Fig. 1 Smart Grid Concept

2.1.1 Smart Grid 와 기존 전력망의 구조

표 1은 기존의 전력망과 Smart Grid의 차세대 전력망의 구조의 비교이다.

표 1. 기존 전력망과 스마트그리드 전력망의 구조 비교
Table. 1 Existing electricity grid and smart grid grid structure comparison

항 목	기존 전력망	Smart Grid 전력망
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

2.1.2 Smart Meter

Smart Grid 구축 기술 중 하나인 Smart Meter는 기존의 Smart Meter 공급자 위주의 방식을 벗어나 양방향으로 전기기기의 실시간 전력 소비를 모니터링 할 수 있는 서비스를 제공하고 있다. 그림 2는 기계식 계량기와 전자식 계량기이다[5][6].

그림 2. 기계식 계량기와 전자식 계량기
Fig. 2 Mechanical meters with electronic meters

III. Smart Meter 공격

3.1 Smart Meter의 취약점 및 공격 분석

3.1.1 램 공격

만약 계량기 기기의 외부보안과 내부보안을 제대로 갖추지 못하고 있다면, 해커들은 주사기를 이용해 계량기의 메모리칩의 각 측면에 바늘을 삽입하여 전기 신호를 가로채 관리자의 권한을 습득하여 내부의 프로그램을 변경과 계량기 안에 저장되어 있는 정보를 빼낼 수 있다.

3.1.2 무선 크래킹

보안전문회사 IOActive는 해커들이 네트워크상에서 상호 통신하는 계량기의 무선 네트워크 장치를 이용해 계량기에 침투할 수 있다고 경고한다. 공격자들은 SDR(Software Defined Radio)을 이용해 네트워크의 무선 통신을 해킹할 수 있고, 시간에 따라 계량기와 통신하는 방식을 변화시킬 수 있다. SDR이란 하드웨어 즉 단말기나 칩을 바꾸지 않고 소프트웨어 조작만으로도 셀루러, PCS, WiBro, 무선랜, 위성통신과 같은 다양한 무선 통신 서비스를 하나의 단말기에서 이용할 수 있게 하는 기술이다.

3.1.3 주파수 크래킹

램 공격과 유사한 기술이 Smart Meter의 무선 주파수를 조정할 수 있다. 이런 방식을 통해 전력망 자체를 공격할 수 있다. Smart Meter의 양방향 무선 칩은 계량기가 원격으로 정보를 읽고, 네트워크상의 명령을 받아들일 수 있는 기능을 갖고 있다. 그 침의 소프트웨어는 보안코드를 갖고 있는데, 계량기의 프로그래밍을 크래킹 한 해커가 네트워크에 침투하기 위해 그 보안코드를 활성화 할 수 있다[7].

IV. Smart Meter 공격에 대한 방어 및 보안

4.1 방어 및 보안 방법 분석

표 2. 계량기 공격에 대한 방어 대책
Tavle. 2 Meter defensive measures against attacks

공 격	방어 대책
램 공격	Smart Meter를 외부조작하려고 할 때 감지 센서를 통해 실시간으로 사용자에게 데이터를 전송함으로써 램 공격에 대한 보안이 가능하다.
무선 크래킹	무선 환경에서의 보안성 확보를 위해 Smart Meter에서 사용되는 통신표준의 장치/사용자 인증(Authentication)과 데이터 암호화(Encryption)를 통해 방어가 가능하다.
주파수 크래킹	크래킹에 방어 대책으로 무선 환경에서 전송되고 있는 주파수를 인증 서버를 이용하여 사용자의 유효성을 검사하고 네트워크 액세스를 제공함으로써 방어가 가능하다.

4.1.1 무결성 방어

Smart Meter에서 전달되는 데이터가 통신망 영역으로부터 중간에 변형되지 않도록 무결성을 보장하여야 한다.

통신에서 유·무선 통신 네트워크에서의 취약점을 방어하려면, 메시지를 변형이 되었는지의 여부를 알 수 있는 메시지의 인증 코드 값을 생성하게 된다. 또한 전력선 기반 통신에서의 셀 보안 취약점 에서도, 통신 메시지가 변경이 되지 않았다는 것을 보장하기 위해 메시지 인증 코드 값이 있어야 한다.

4.1.2 기밀성 방어

기밀성 보장을 위한 대표적인 보안 방법은 데이터 암호화이다. 암호화는 비밀키(security key)를 이용하여 원본 데이터를 특정 알고리즘에 따라 변형시킴으로써 비밀키를 가지고 있는 사람만이 암호를 풀어서 원본 데이터를 읽을 수 있도록 하는 방법이다.

Smart Meter 공격으로 인해 사용자 개인정보를 가로채려고 할

때 방어를 위해 사용자 데이터를 암호화하여 기밀성을 보장해 줌으로서 해결을 할 수 있다. Smart Meter에 저장된 개인정보를 암호화함으로서 Smart Meter에서의 프라이버시 문제를 해결 할 수 있다.

4.1.3 사용자 관리자 인증(authorization)

인증은 Smart Meter가 통신 네트워크상의 사용자나 장치들에 대한 접근과 제어를 할 때, 사용자는 고유의 신분증을 사용하여 서로가 누구인지, 신뢰할만한 대상인지를 판단하도록 하는 일종의 확인 과정이다.

통신에서 대상이 누구인지 확인하는 방법으로 인증이 사용되는데, Smart Meter에서도 인증을 사용하여 인가된 사용자와 그렇지 않은 사용자를 구분할 수 있도록 할 수 있다.

4.1.4 가용성 방어

가용성 방어는 Smart Meter가 정상적으로 작동하지 못하도록 하는 DoS공격으로부터 방지하는 것을 말한다. DoS 공격이란 전력IT기기가 작동 할 때 사용되는 CPU, 통신 대역폭 등의 시스템 자원을 의도적으로 소모시켜 해당 시스템을 마비시키거나 정상적인 동작이 불가능하도록 만드는 공격을 말한다.

스마트 제어 부분에서 서비스 거부 공격인 DDoS 공격을 받게 되면 전력망 내의 중요 시스템이 제어가 불가능한 상황이 되어 정상적인 동작을 못하게 되거나 관리자가 시스템에 접속할 수 없게 되어 치명적인 결과를 초래할 수 있다.

DDoS 공격을 방지할 수 있는 확실한 방법은 사설(전용선) 네트워크를 이용하면 외부와의 통신이 차단되기 때문에 적용할 수 있는 환경에 한계가 있다. 따라서 지능형 보안 DB 시스템을 구축하면 서비스 거부 공격을 조기 진단하고 방어하기 때문에 가용성 보장이 가능하게 된다.

4.1.5 Smart Meter 접근제어

Smart Meter 접근제어는 시스템에 접근 권한을 차등적으로 부여하는 방법이다. 접근제어를 위해서는 이미 인증된 대상에 적절한 권한부여(authorization)가 필요하다. 기반통신에서는 접근 제어를 위해 사용자별 권한부여 DB를 사용하게 된다.

스마트 제어 부분에서 전력 사용에 대한 통제권 보장을 위해 권한부여 DB를 사용하여 비정상적 전력 사용을 방지하고, 스마트미터기의 경우에는 스마트 미터기에 대한 접근통제를 위해 권한부여 DB를 사용하여 전력량을 조작하는 상황이 발생하지 않도록 한다. 서비스 제공자 분야에서는 권한부여 DB를 사용하여 허가되지 않은 곳에 전력을 전송하는 일이 없도록 할 수 있다.

V. 결론

한국은 Smart Grid의 선도 국가로서 저장된 만큼 현재 진행 중인 실증단지에서의 Smart Meter에 취약점에 대해 적극적으로 사전 방어 방안을 마련하여야 하며, Smart Meter에 대한 접근제어 및 인증을 강화하여 인가된 사용자만이 시스템을 통제 할 수 있도록 보안되어야 한다. 또한 Smart Meter 공격을 받았을 때 로그기록 등을 수집하여 대응할 수 있도록 포렌식 연구도 필요하다.

따라서 본 논문에서는 Smart Grid의 Smart Meter 공격에 대한 방어와 인가된 사용자만이 정보를 확인하고 접근할 수 있도록 통신보안에 대해 연구하였으며, Smart Meter에 대한 보안의 필요성을 강조하였다.

향후 연구로는 Smart Grid 실증단지에서 발생 가능성이 있는 취약점과 해킹방법 조사를 통한 Smart Grid 사전대응 연구가 필요하다.

참고문헌

[1] 엄찬왕, “Smart Grid 정책과 국가로드맵,” TTA 저널, 129, 2010. 5.

[2] 김명순, 김용수, “네트워크 통신에 기반한 향상된 스마트그리드 관리 시스템 구현,” 대한전자공학회 정기총회 및 추계종합학술대회, 2010.

[3] 손소현, “Smart Grid(Smart Grid)의 현재와 추진 정책 :전기계량기의 미래 모습, Smart Grid,” 기술과미래, 60(4), 64-67쪽, 2010. 1.

[4] 문승일, “스마트그리드 개념,” 정보와 통신 : 한국통신학회지, 27(4), 3-9쪽, 2010. 4.

[5] 최원석, “[산업기술] Smart Grid, 호주 녹색산업의 유망주,” KOTRA, 동향자료, 2009.

[6] 손소현, “Smart Grid(Smart Grid)의 현재와 추진 정책 :전기계량기의 미래 모습, Smart Grid,” 기술과미래, 60(4), 64-67쪽, 2010. 1.

[7] 정영곤, 최현우, 염홍열, “Smart Grid 보안 동향,” 정보보호학회지, 20(4), 66-79쪽, 2010. 8.