제36회 한국정보처리학회 추계학술발표대회 논문집 제18권 제2호 (2011. 11)

스마트그리드 장비의 보안 위협 요소

임용건, 박정규, 이근호
백석대학교 정보통신학부
E-mail:ddabia@nate.com, sunrise1987@nate.com, root1004@bu.ac.kr

Security threats of SmartGrid equipments

Yong-Gun Lim, Jung-Kyu Park, Keun-Ho Lee
Dept. of Information and Communication, Baekseok University

요 약

스마트 그리드는 기존의 전력망에 IT를 접목하여 전력 공급자와 소비자가 양방향으로 실시간 정보를 교환함으로써 에너지 효율을 최적화 하는 차세대 지능형 전력망이다. 지능형 전력망을 구축하기 위해 제품에 스마트 칩이 내장되어 있어 각 가정이나 빌딩마다 저장장치를 구비하여 저가 전기를 충전했다가 고가 시간대에 재사용하는 이러한 스마트그리드 홈서비스가 구축 될 것이다. 이러한 홈서비스에서 사용될 스마트그리드 장비의 보안 위협 요소를 알아보고 이에 대한 해결 대응 방안을 제시 한다.

1. 서론

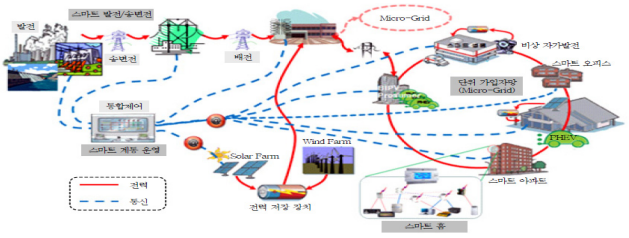
스마트 그리드는 기존의 전력망에 IT를 접목하여 전력 공급자와 소비자가 양방향으로 실시간 정보를 교환함으로써 에너지 효율을 최적화 하는 차세대 지능형 전력망이다.

기존의 단방향 전력망에 IT를 접목하여 전력 공급자와 소비자가 양방향으로 실시간 정보를 교환함으로써 에너지 효율을 최적화 한다. 전력 공급자는 전력 사용 현황을 실시간으로 파악하여 공급량을 조절할 수 있다. 전력 소비자는 전력 사용 현황을 실시간으로 파악함으로써 이에 맞게 요금이 비싼 시간대를 피하여 사용 시간과 사용량을 조절할 수 있으며, 태양광 발전이나 연료전기 전기자동차의 전기에너지 등 가정에서 생산 되는 전기를 판매할 수도 있게 된다. 또 자동조정 시스템으로 운영되므로 고장 요인을 사전에 감지하여 정전을 최소화 하고 기존 전력시스템과는 달리 다양한 전력 공급자와 소비자가 직접 연결되는 분산형 전원 체제로 전화되면서 풍량과 일조량 등에 따라 전력 생산이 불규칙한 한계를 지닌 신재생에너지 활용도가 증대된다.

스마트 그리드는 에너지 이용의 효율성을 높이는 것이 목적이다. 효율성을 높이기 위해선 자발적인 에너지 절약을 유도해야 한다. 수급 상황별 차등요금제를 적용하여 전력 수요를 분산시키고 소비자들에게 전기사용량과 요금을 실시간으로 보여줌으로써 자발적인 에너지 절약을 유도한다.

스마트 그리드는 신재생 에너지의 품질을 향상 시키고 활용도를 높여 줄 것이다. 전력변환장치가 신재생 에너지원의 초기 불안정한 획득 에너지에 대해 전압과 주파수 등이 고르고 안정적인 전기에너지로 변환시켜 준다. 여기에 저장장치가 결합하여 시간대별로 전기 공급을 일정하게 조정할 수 있다. 또한 바람세기를 감지해 바람이 세게 불면 풍력 발전기의 출력을 증가 시키는 대신 화력발전소의 출력을 감소시켜 전체 전력 공급을 일정하게 유지하는 등의 조정 기능이 가능하다.

스마트 그리드는 전력의 품질과 신뢰도가 향상 된다. 자기진단이 가능하고 시스템의 보호와 단독 운전이 가능하며 사고시 반자동으로 복구하고 자기 치유를 할 수 있다는 특징을 가진다. 고장요인을 사전에 감지함으로써 정전을 최소화 하고 전기의 품질을 높일 수 있다. 하지만 스마트그리드 기술을 접목한 장비들에는 항시 보안에 대한 위험이 있을 것이다. 지금껏 IT장비들에 보안이 위험성이 있듯이 스마트그리드 장비에도 보안에 대한 취약점이 있고 스마트그리드 장비에 대한 취약점 및 위협 요소 이에 대한 대응방안을 제시 할 것 이다[1,2].



(그림 1) 스마트그리드 구축 시스템

2. 스마트그리드 기술

스마트그리드의 핵심 기술로는 AMI 기술 ,수요반응 기술, 사용자 영역 네트워크 기술, 신재생 에너지 연계 기술 등으로 구성되며 이에 더불어 앞으로 안전하게 유지할 수 있는 보안 기술이 필요하게 된다.

<표 1> 현재전력망과 스마트 그리드 비교

전원 공급 방식	중앙 전원	분산 전원
비교 항목	현재 전력망	스마트 그리드
구조	방사형 구조	네트워크 구조
통신 방식	단방향 통신	양방향 통신
기술 기반	아날로그/전자기계적	디지털
사고시 복구	수동 복구	반자동 복구 및 자기 치유
설비 점검	수동 설비 점검	원격 설비 점검
제어 시스템	지역적인 제어 시스템	광범위한 제어 시스템
가격 정보	제한적인 가격 정보	모든 가격 정보 열람 가능
고객의 선택	고객의 제한적 선택 기능	고객의 다양한 선택 기능
자료:LS사전 자료 재구성		

-AMI(Advanced Metering Infrastructure) 기술

기존 원격검침(AMR)보다 기능이 향상된 개념으로, 아래와 같이 지능형 전력량계, 소비자 수요반응 기기, 지능형 전력정보 관리시스템, 지능형 전력서비스 네트워크 등 다음의 4가지 기술로 구성된다.

●스마트 미터: 양방향 통신을 지원하고 사용자에게 전력사용 정보를 제공, 수요반응을 통한 에너지 효율향상을 촉진.

●소비자 수요반응기기(수요반응):빌딩, 홈 등과 같은 소비자의 에너지 사용량, 요금제도, 예상요금 등 에너지에 대한 다양한 정보를 인지하고, 자발적으로 에너지절감 프로그램에 동참할 수 있도록 의사결정을 돕는 제품.

●지능형 전력 정보관리시스템(MDMS):수요 측의 대용량 전력자원을 통합관리하고 이의 효율적인 운영 .배분과 함께 신속하고 직관적인 그린에너지 정책 결정을 지원.

●지능형 전력 서비스네트워크(SUN):전력회사의 상위시스템과 전력량계, 고객을 연계하는 역할을 수행하며, 앞으로 스마트 그리드로 전력계통이 진화할 경우 AMI 구성요소를 포함해 스마트 그리드의 통신망으로 활용할 수 있는 스마트 전력통신 기술.

-수요반응(Demand Respond)시스템

전력 수요에 따라 가격을 실시간으로 결정해서 수요자에게 알려주고 수요자가 이를 근거로 전력 사용량을 효과적으로 조절하도록 해 주는 시스템이다.

수요자는 실시간 요금제 차등 요금제에 맞게 전력 소비형태를 바꾸게 된다. 수요 반응 시스템은 이러한 수요자의 반응에 따라 발전량을 제어하는 정보를 사업자에게 제공한다. 또한 수요자가 자신의 에너지를 직접 관리할 수 있고 전력 품질의 측정과 데이터 저장이 가능하며 수요자의 프로그램 설정에 따라 자동으로 부하를 제어하는 기능을 갖추게 된다.

-사용자 영역 네트워크 기술

AMI 기술과 수요반응 기술은 사용자 영역에서의 기기 상태 관리 및 제어로서 완성된다. 사용자 영역에서 스마트 미터는 스마트 그리드 최종단의 사용자의 에너지 관리 프로그램뿐만 아니라 사용자 영역 네트워크에서의 기기의 상태 관리 및 제어와 연계하는 게이트웨이 역할도 수행하게 된다. 일반 가정 영역에서는 전력회사가 소유한 스마트 미터와 같은 장비들은 물론 가전기기 제조회사나 사용자가 직접 구입한 다양한 스마트 그리드 장치들이 어울려서 동작 한다[3].

3.관련 연구

-스마트그리드 홈서비스

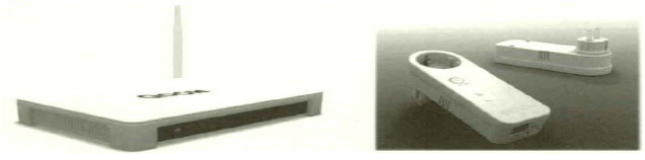
스마트그리드 홈서비스는 광범위한 스마트그리드 개념 중 가정에서 우선 필요한 전력/에너지 관련 서비스를 제공할 수 있다. KT에서 개발한 스마트그리드 홈서비스는 사용자가 가정 내 혹은 원격에서도 손쉽게 집안의 전력량을 모니터링하고 가전기기의 전원을 제어할 수 있는 서비스이다.

스마트그리드 홈서비스를 위한 장비인 스마트 박스와 태그에 대해 살펴보고 이들의 통신 방법에 대해서 살펴보고자 한다. 가정 내 에너지 관리 서비스를 위해 기기 별 전력사용량을 포함한 5종 미터(전력, 온수, 가스, 수도, 난방)의 사용량 정보를 스마트그리드 센터로 전송하고, 가정 내의 장치와 인터넷을 연결해 주는 스마트 박스를 개발하였다. 스마트 박스는 스마트 미터 및 스마트 태그 검침데이터 전송과 전력관리를 해줄 수 있는 홈 게이트웨이 역할을 수행한다. 스마트태그는 홈/빌딩 내에 가전기기 별로 설치되어 전력 사용량을 포함하여 전기, 가스, 난방, 수도, 온수, 5종 미터에 대한 사용량을 수집하여 스마트그리드 센터로 전달하며, 스마트태그에 연결된 기기의 전원을 제어할 수 있는 Actuator기능이 있다.

-스마트박스 스마트 태그

스마트 박스 장비는 유선 인프라를 활용한 스마트 홈 구현을 위한 장비로서 가입자 가정에 설치되어 홈 게이트웨이 기능과 스마트그리드를 위한 에너지 관리 기능을 제공하는 단말 장비이다. 스마트 박스는 가정 내 네트워크 단말 장비로서 홈 게이트웨이 기능, 고속PLC를 이용한 스마트 태그 원격 모니터링 및 제어기능, ZigBee 통신을 통한 스마트미터와의 연동기능 및 센터와의 연동기능을 제공한다.

스마트 태그는 연결된 가전기기의 실시간 소비전력량을 측정하여, 데이터를 스마트 박스를 통해 연결된 센터로 전송하고 연결된 전기기기의 전원 공급을 On/Off 제어할 수 있는 장치이다.



(그림 2) 스마트박스, 스마트태그

사용자는 현재 스마트 태그에 연결된 가전기기의 소비전력 및 전기요금 등을 스마트폰을 통해 실시간 확인할 수 있어, 전기사용의 절약과 관리를 효율적으로 할 수 있도록 유도한다.

-스마트 박스-태그 통신

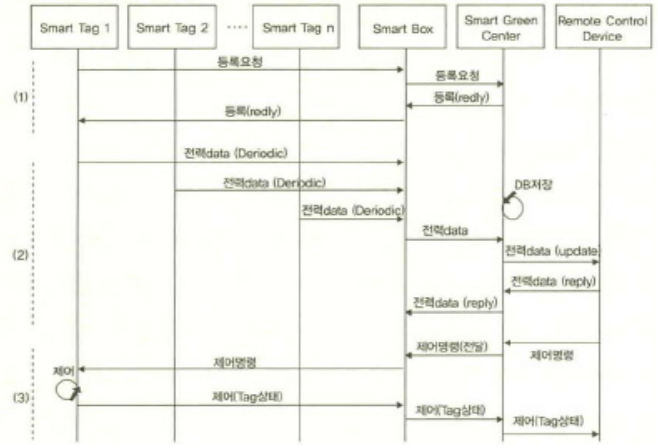
스마트 태그와 스마트 박스간의 데이터 통신은 스마트 미터와의 연동 및 전력 관리를 위해 저압 전자식 전력량계의 표준 프로토콜인 DLMS(IEC62056)을 채택하였다. 스마트 태그와 박스의 통신 방식은 1대의 박스와 다수의 태그간의 통신을 위해 PLC 기반의 HDLC(High-level Data Link Protocol)프로토콜 프레임을 갖는 통신 방식을 이용한다.

-스마트 박스-센터 통신

센터와 스마트 박스간의 통신 프로토콜은 Web서비스와 같은 방법을 사용하여 http/XML 형식의 메시지를 사용하였다. 스마트박스와 센터와의 접속을 TCP socket 방식을 이용 하였으며, 스마트 태그와 센터와의 연동을 위해선 IPC통신을 이용하였다.

-스마트그리드 홈서비스 주요 흐름도

스마트 센터는 스마트 박스로부터 주기적으로 전력정보를 수집해 DB에 저장한다. 사용자가 단말을 통해 전력 모니터링 서비스에 접속하면 해당 데이터 값을 DB로부터 전송한다.



(그림 3) 홈서비스 흐름도

- 전력 제어 서비스

스마트 태그에 연결되어 있는 가전기기의 전원을 원격으로 제어하는 서비스이다. 이 서비스를 통해 사용자는 단말을 통해 가정 내 스마트 태그와 연결된 가전기기의 전원 상태 및 사용량 현황을 알 수 있으며 전원 On/Off 제어가 가능하다. 사용자는 단말 화면을 통하여 가정 내에 등록된 스마트 태그들의 목록에서 태그별 사용량 확인 및 전력제어를 할 수 있다. 실시간 제어를 보장하기 위해 스마트 박스의 데이터를 주기적으로 스마트 센터에 전송하는 모니터링 서비스의 방식과 달리 전력 제어 서비스는 이벤트 드리븐 방식이다. 전력 제어 명령은 실시간적으로 스마트 태그까지 전달된다[7].

4.스마트그리드 장비의 보안 위험성

스마트그리드는 폐쇄망을 이용하던 전력인프라에서 벗어나 사용자에게 전력 이용현황을 보여주기 위해 인터넷망까지 연동해야 하기 때문에 사용자 개인정보가 쉽게 노출될 우려를 안고 있다. 특히 국가 전체 가구가 사용하게 될 스마트미터는 기기제어를 통해 가격신호 및 미터링 데이터 위조, 타인의 개인정보와 ID정보를 알아내 악용할 수 있고 나아가서는 스마트그리드 전체 네트워크에도 영향을 줄 수 있다. 이 때문에 외부공격에 의한 단전, 개인정보 유출, 전력사용 통제권 상실 등에 보안사고도 우려되는 상황이다. 스마트 미터의 보안 위험성을 말하자면,
프라이버시 및 데이터 보호관련 위험성, 커뮤니케이션 및 운영상의 위험성, 액세스 컨트롤 상의 위험성,
자산 관련 위험성, 물리적 환경 관련 위험성, HR 관련 위험성, IP 관련 위험성 등이 우려 된다.

<표 2> 분야별 보안 위협요소

	통신망	전력망	스마트 가정
특징	개방형 구조	폐쇄형 구조	통신망과 전력망의 접점
보호대상	유무선 통신망	발전소, 송/배전망	스마트미터, 스마트기기 홈네트워크
보안위협	DDoS공격,해킹/바이러스 위험	대규모 정전사태 송/배전 오작동	전력자기통제권상실,개인정보 유출

센터와 스마트 박스간의 통신 프로토콜은 Web서비스와 같은 방법을 사용하여 http/XML 형식의 메시지를 사용 한다 센터와 스마트 박스간의 통신은 기존의 사용자가 사용하던 Web서비스를 사용하기 때문에 기존의 해킹 및 바이러스들에 대한 위험성이 나타날 수 있으며 이로 인해 전력을 관리하는 스마트 센터에 까지 영향을 미쳐 정전 및 전력 서비스 거부 공격 DDos 공격의 피해를 입을 수 있으며 전력을 사용하고 있는 소비자들에게 피해가 일어 날 수 있다[8].

5. 결론

가정용 단말장비에 대한 이용자 인증 및 전력인증이 유무선 환경에서 동시에 수행됨에 따라 상호호환성 문제나 무선기술(와이파이) 보안취약성이 발생할 수 있다.

따라서 소비자 및 스마트기기 인증을 위한 인증시스템이 필요하고, 스마트기기에서의 과도한 개인정보 수집을 최소화할 수 있는 필터링 기술, 무선랜 보안기술(보안설정 강화)이 필요하다. 전력사용량을 측정해 해당 정보를 송수신할 수 있는 전자적 계량기인 스마트미터는 전력사용자의 외부통신망과 내부통신망 연결접점으로, 해킹이나 웜 바이러스, DDoS 등 공격 타깃이 될 가능성이 높다.

따라서 스마트미터 자체의 취약성을 보완해 외부공격에 대응할 수 있는 보안 칩이나 안티바이러스 연구 등이 필요하며, 통신구간 개인정보의 암호화 전송으로 개인정보 유출 가능성을 제거해야 한다. 스마트미터에 대한 접근통제를 위한 물리적 시건장치, 인증 및 로그관리 기술 등도 필요하다. 가정의 전력 사용정보를 제공에 이용되는 가정의 통신망과 전력사업자의 데이터 전송구간인 통신망(WAN) 구간은 전통적인 유무선 통신기술에 내재된 취약성과 해킹공격 등에 노출될 수 있다.

이를 위해 VPN 등을 통한 암호화 통신, 상황관제 및 통합 보안관리 체계 구축, 전력선 기반 통신의 셀간 위협 차단을 위한 기술 개발이 필요하다. 전력인프라 보안을 위해 송·배전 시스템의 취약성을 보완하기 위한 하드웨어 및 소프트웨어 보안성 평가가 필수적이며, 현재 정보통신기반시설을 추가해야 하고, 이를 위한 기반시설 취약성 분석, 평가기준을 마련해야 한다. 고객정보가 한곳으로 모이기 때문에 대량의 데이터관리 기술도 필요하다.

"이 논문은 2011년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임 (No.2011-0010457)"

참고문헌

[1] 이건희,서정택,이철원 "스마트그리드와 사이버 보안", 4월, 2010년

[2] 도윤미, 김선진, 허태욱, 박노성, 김현학, 홍승기, 서정해, 전종암, "전력망과 정보통신의 융합기술", 전자통신동향분석 제24권 제5호 2009년, 10월

[3] 이일우, 한동원, "IT기반의 스마트 그리드 기술", 한국정보기술학회지, 7(1), pp.25-30, 2009.

[4] U.S. Department of Commerce,"(Draft) NISTIR 7628,Smart Grid Cyber Security Strategy and Requirements," February 2010.

[5] Edward Chow, "Secure Smart Grids, University of Colorado at Colorado Springs," Freshmen Welcome '09, 2009.

[6] 이연섭, "스마트 그리드에서의 개인정보보호에 관한 연구", 동국대학교 국제정보대학원 석사학위논문, 2011

[7] 이근철, 오재영, 김윤기 "스마트그리드 홈 서비스"

[8] 디지털ITnet "국가 스마트그리드 보안 현황 과제"