情 報 保 護 學 會 誌
第22卷 第5號, 2012. 8

스마트그리드의 안전성과 보안 이슈

정 교 일*, 박 한 나**, 정 부 금***, 장 종 수****, 정 명 애*****

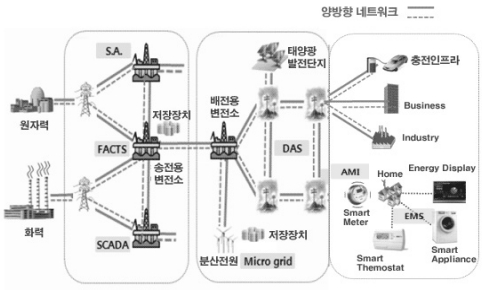
요 약

최근의 전력난, 일본 후쿠시마 원전사태 등은 전력생산이 상대적으로 적은 나라에게는 큰 부담이 아닐 수 없다. 이러한 배경에서 스마트그리드라는 지능형 전력망의 개념이 도입되었고, 우리나라도 녹색성장에 힘입어 적극 추진하고 있다. 그러나, 스마트그리드에도 소규모 분산 전원공격, 양방향 통신 프로토콜 공격, 배전망 관리센서 공격, 보안에 취약한 스마트 미터에 대한 공격 등의 사이버공격이 이루어지고 있어 전력 공급은 물론 전체 시스템에 타격을 줄 수 있다. 본 논문에서는 이러한 보안 체계에 대한 요구 사항을 정리하고, 안전성이 보장하기 위하여 필요한 이슈를 제기하고자 한다.

Ⅰ. 서 론

수년 전부터 우리나라도 전력 수요가 급증하여 해마다 전력 사용을 효율화하고, 심지어는 전력난 대비 훈련도 하는 지경에 이르렀다. 올해도 예외가 아니라서 7월 23일 기온이 32℃를 상회하면서 예비 전력이 6%정도로 급격히 낮아졌다. 또, 2011년 3월, 일본의 원자력발전소 사고는 발전 설비에 대한 의구심을 갖게 하였으며, 실제로 발전소 건설기간 등을 고려한다면 우리의 전력 공급시스템에 획기적 전환이 요구된다. 때맞추어 정부는 2012년 7월 18일 2016년까지 스마트 계량기 1,000만대, 20만㎾h급 에너지 저장장치(ESS, Energy Storage System), 전기차 충전기 15만기를 보급할 예정이라고 한다. 또한 7개 광역경제권별로 스마트그리드를 구현할 거점도시를 구축한다고 발표했다. 지식경제부는 '지능형 전력망 기본계획'을 발표하고, 스마트그리드 구축을 통한 제2기 국민발전소 건설을 적극 지원한다고 밝혔다[1].

여기에서 지능형 전력망 즉, 스마트그리드는 [그림 1]과 같이 전력생산에서부터 송전 및 배전, 전력소비자까지 광범위하게 광대역 통신망을 통해 데이터 전송이 이루어지는 시스템으로 공급자와 소비자가 양방향으로 실시간 전력정보를 교환함으로써 에너지효율을 최적화하는 차세대 전력망으로, 선진국을 중심으로 전략산업으로 추진 중이다.



〔그림 1〕 스마트그리드의 양방향 통합에너지 관리시스템
(출처: 지능형전략망협회 홈페이지)

그러나 스마트그리드에 대하여 그 동안 나타났던 사이버 공격으로 미루어보면, 소규모 분산 전원공격, 양방향 통신 프로토콜 공격, 배전망 관리센서 공격, 보안에 취약한 스마트 미터에 대한 공격 등이 가능하다. 사이버 테러 공격자는 일단 공격 거점을 확보하게 되면 연계된 네트워크를 통해서 전력거래 관련 시스템을 포함한 스

본 논문은 지식경제부 산업융합원천기술개발사업(10041066)으로 지원된 연구결과입니다.
* 한국전자통신연구원 융합기술원천연구팀 (kyoil@etri.re.kr)
** 한국전자통신연구원 생체정보연구팀 (hnpark@etri.re.kr)
*** 한국전자통신연구원 가상사설클라우드연구팀 (bgjung@etri.re.kr)
**** 한국전자통신연구원 네트워크시스템보안연구팀 (jsjang@etri.re.kr)
***** 한국전자통신연구원 융합기술미래기술연구부 (machung@etri.re.kr)

마트그리드 전체 전력망을 공격할 수 있어 그렇지 않아도 전력난에 허덕이는 우리에게 커다란 타격이 아닐 수 없다.

본 논문의 구성은 Ⅱ장에서 최근의 스마트그리드 개발 동향에 대하여 소개하고, Ⅲ장에서 스마트그리드에 대한 각종 위협과 사례를, Ⅳ장에서는 스마트그리드의 주요 보안 요구사항과 안전성 강화를 위한 보안 이슈를 제시하고, 마지막으로 결론을 맺는다.

Ⅱ. 스마트그리드와 보안기술 개발 동향

차세대 성장 동력인 스마트그리드의 시장을 예측하기 위해서는 세계 인구증가와 이에 따른 전력설비시장에 대한 예측이 필요할 것이다. 세계 인구는 2000년 61억명에서 2030년 81억명으로 약 20억명의 증가를 예상하고 있고, 이를 바탕으로 현재의 전력 수요 제외계층과 신규 인구로 인한 새로운 전력서비스 고객을 감안하여 추정해보면 2030년까지 증가는 23억명 이상이 될 것으로 예상하고 있다.

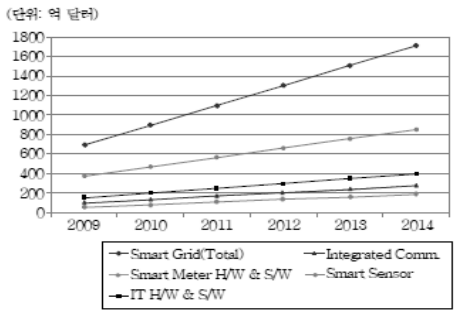
또한, 전력 환경 변화로 인한 전력 수요는 2004년 14,000TWh에서 2030년 28,000TWh로 두 배가 될 것으로 예상한다. 이러한 전력 수요의 증가에 따라 WEO는 2030년까지 전력부분의 신규 투자규모는 약 11.3조 달러에 달할 것으로 예상하고 있으며, 국제에너지기구(IEA)에 따르면 이중 스마트그리드관련 세계 시장규모는 2030년 2조 9880억달러 수준이라고 발표하였다[2,3].

스마트그리드 시장은 [그림 2]와 같이 통합 커뮤니케이션, 스마트미터 하드웨어 및 소프트웨어, 스마트 센서/디바이스, 그리고 IT 하드웨어 및 소프트웨어로 구분할 수 있으며, 전체 시장규모는 2009년 전체 693억 달러에서 2014년 1,714억 달러로 연평균 약 16%로 성장할 것으로 예상된다[2].

2.1 외국의 개발 동향

2.1.1 미국

미국은 전력산업 현대화를 목표로 IT를 비롯한 융합형 신기술을 개발하고 강력한 법·제도, R&D의 연계를 추진 중이다. 전력시설 노후화로 인한 대규모 정전사태 이후 EPACT05 (Energy Policy Act of 2005)와 EISA07 (Energy Independence and Security Act of 2007) 법안 등을 마련하여 산학연관 참여한 다양한 지능형 전력망 프로그램 추진하고 있으며, 미국 전력중앙연구소(EPRI)의 인텔리그리드, GridWise 등 10여 개가 넘는 기관에서 전력시스템의 지능화 및 선진화 구축사업에 참여하고 있다. 특히, 2009년 2월 일명 경기부양법으로 불리는 미국회복 재투자법(ARRA : American Recovery & Reinvestment Act of 2009)에서 387억 달러가 에너지 관련 예산으로 할당되어 있으며, 그중 45억 달러가 스마트그리드 관련 연구개발, 실증 및 보급 등의 투자예산이다.



〔그림 2〕 스마트그리드 기술의 세계 시장규모

이중 EISA07 에서 스마트그리드 사이버 보안 기술을 스마트그리드의 필수 기술로 정의하였으며, NIST (National Institute of Standards and Technology)로 하여금 스마트그리드 보안표준을 포함하여 스마트그리드의 상호운용성을 위한 표준을 제정하도록 하였다. 2009년 4월 미국은 중국 러시아 해커의AMI의 보안 프로파일을 비롯하여 스마트그리드 사이버 보안 가이드라인, 스마트그리드 사이버 보안 테스트 가이드 개발 등을 추진 중이다. 이 가이드라인은 스마트그리드 논리적 아키텍처 분석, 스마트그리드의 인터페이스에 적용 가능한 사이버 보안 통제사항, 암호 및 키관리 문제, 프라이버시 보호, 스마트그리드 보안 연구 개발 이슈 등을 정리했다.

그리고 국가 기반시설 전반에 활용되는 제어시스템의 보안성 제고 관련하여 에너지부 산하 6개의 국립연구소에서 17개의 NSTB(National SCADA Test Bed)를 구축 및 운영하고 있는데 주요 활동으로는 국가 제어시스템 보안정책 수립에 기술적 지원, 국가 제어시스템 보안강화, 제어시스템 침입탐지 및 대응기술 역량 고취, 에너지 분야 사이버 보안성 강화를 위한 차세대 기술 연구개발 등이 있다. INL(Idaho National Laboratory)

에서 SCADA/EMS 관련 38개 벤더들의 제어시스템들에 대해 취약성 평가를 완료한 상태이다[5].

2.1.2 유럽

EU차원에서 지능형 전력망 프로젝트를 추진하고 있으며, 각국의 신재생에너지 중심의 분산형 전원의 보급 확대, 환경 보전, EU 국가간 전력거래에 초점을 맞추고 있다. 그리고, 전통적으로 태양광・풍력 등 신재생에너지의 확산에 가장 적극적이지만, 지능형 전력망 기술 및 에너지 저장 장치 보급으로 태양에너지 발전의 비중을 현재의 1%이하 수준에서 '20년까지 12%로 상향 추진할 예정이다.

범유럽 연구개발 프로그램(FP7)에서 IT기반 에너지 효율화 과제를 포함하여 적극 추진하여 '13년까지 110만 가구에 AMI (Advanced Metering Infrastructure, 스마트미터, 스마트 계량기) 서비스를 적용할 것으로 전망하며, '30년까지 지능형 전력망 분야에 1 Trillion 유로를 투자할 계획이다. 현재 유럽의 스마트미터 보급 수준은 전체 가정의 6%수준으로 2012년 까지 30~40%로 확대할 계획에 있다.

영국의 경우 70~90억 파운드를 투입해 2020년까지 매년 260만 가구씩, 향후 10년에 걸쳐 2,600만 전체 가구에 가스 전기 스마트미터를 설치 추진할 예정이다. 스페인은 2013년까지 2,200만대의 기존 계량기를 스마트미터로 교체하는 작업을 실시할 예정이다.

독일 역시 Meregio(Minimum Emission Region)라고 알려진 스마트그리드 프로젝트를 시범 운영 중에 있으며, 네덜란드는 인공섬을 조성하여 조력, 태양광, 연료전지를 기반으로 하는 스마트시티를 건설 중에 있다.

한편, EU의 19개 전력회사가 모여 진행중인 스마트미터 표준화 프로젝트인 OPENmeter 는 보안 요구사항을 포함하는 스마트 미터 요구사항을 2009년 발표했다. OpenMeter 에서는 스마트 미터의 보안 위협을 허가되지 않은 자에 의한 정보의 접근 및 수정, 공격자에 의한 설정 변경과 전류 차단기 및 가스 밸브 등의 의도적인 차단, 서비스 거부공격, 개인 프라이버시 정보의 노출로 정의하고 있으며, 이를 보호하기 위한 보안 요구사항으로서는 AMI 전체적으로 기기인증, 접근제어, 데이터 기밀성・무결성, 인증서 사용 등을 요구하고 AMI 보안기술로는 안전성 등이 이미 검증되어 널리 사용되고 있는 기존 IT 보안 표준 기술사용을 제안하고 있다.

독일에서는 스마트그리드 추진에 있어 사이버보안을 중요한 요구사항으로 제시하고, 향후 보안을 강제적 요구사항으로 진행할 예정이며, 스마트 미터와 게이트웨이 영역에 보안기술을 적용하는 것부터 기술 개발을 시작하고 있다. 독일 경제기술성의 위임에 따라 연방정보보안청 (BSI, Bundesamt für Sicherheitin der Informationstechnik)에서는 스마트 미터 게이트웨이의 보안기술 평가를 위해 보호 프로파일(PP, Protection Profile)을 개발하고 있으며, 이를 EU 표준으로 적용하는 것을 목적으로 하고 있다[4].

2.1.3 일본

'07년 12월 Cool Earth 정책을 수립(경제산업성), IT 분야를 비롯한 20개 분야의 주요 에너지 혁신 기술개발을 추진하고 있다. Cool Earth 에너지 혁신 기술계획의 핵심기술로 ITS, 고효율 IT기기 및 망, HEMS/BEMS 및 지역 EMS 등의 에너지 관리기술 채택하여 '50년까지 온실가스 감축 50% 달성을 위해 21개 핵심기술을 선정하였다. 그리고 일본의 전력중앙연구소는 안정된 운영으로 광역 정전위험의 최소화, 수요와 공급의 통합으로 에너지의 효율적인 이용과 보존 가능성, 다수의 분산전원의 보급과 효과적인 이용을 구현하고 정교한 자산관리 및 전력 장비를 이용하여 미래 사회요구에 대응하는 것을 목표로 일본형 지능형 전력망 TIPS[1]를 1단계가 2010년까지, 2020년도까지 2단계로 나뉘어 수행될 계획이다.

2.1.4 호주

최대 전력 공급지역인 빅토리아주 정부에서 AMI를 중심으로 지능형 전력망 추진을 위하여 ISG(Industry Strategy Group)를 설립하여 AMI 규격 제정하고, NSW주는 '17년까지 스마트미터를 전 가정에 공급을 추진하고 있다.

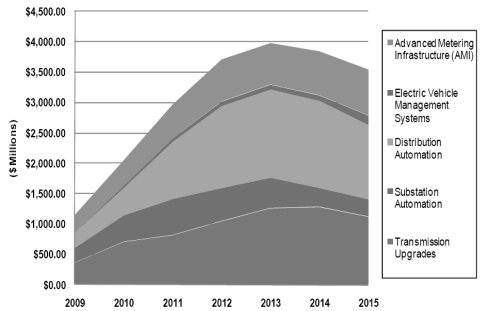
2.1.5 중국

빠른 경제성장을 위해, 꾸준히 전력분야에 투자하고

1) TIPS(Triple "I" Power Systems) : 지적(Intelligent), 상호영향적(Interactive), 통합적(Integrated)

있다. SGCC(State Grid Corporation of China)는 초고압 직류 송전과 교류 송전시스템을 건설하고 있으며, 정보기술과 자동차기술을 기반으로 스마트그리드를 구현하고 있다. 경제 분석가들은 중국이 스마트그리드에 약 6800억 위안을 2020년까지 총 4조 위안을 지출할 것으로 예상하고 있다.

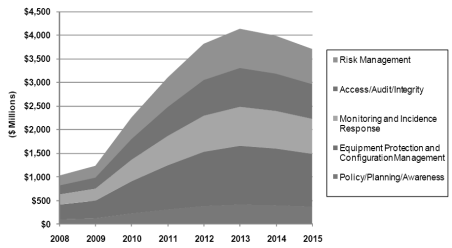
한편, 스마트그리드 사이버보안 투자예산은 전체 스마트그리드 투자금액의 15%에 해당될 것이라고 추정된다(출처 : Pike Research, Smart Grid Cyber Security Market, 2010). 지역적으로 보면, 북미 지역이 15%, 유럽이 12%, 아시아-태평양지역이 10%, 남미가 8%, 중동 및 아프리카가 8%등으로 예상하고 있다. 그리고 전 세계 스마트그리드 사이버 보안시장은 2009년~2015년 동안 20% CAGR (Compound Annual Growth Rate)로 성장할 것이라고 전망된다. 다음 [그림 3]에서 알 수 있듯이 2012년 스마트그리드 사이버보안시장은 35억달러로 추정되며, 2013년 41억 달러, 2015년에는 37억 달러로 예상하고 있다[3].



〔그림 3〕 전 세계 스마트그리드 사이버보안시장 규모
(출처: Pike Research, 2010)

스마트그리드는 전력망의 상태를 양방향 통신을 활용하게 되므로 시장의 성장에 따라 안전하고 신뢰성있는 통신기술에 대한 요구가 늘어날 것으로 전망된다. 즉, 시장 초기에는 주로 스마트미터나 센서장비의 유무선 통신에 대한 기술개발과 장비투자가 주를 이루게 되나, 시스템 확산에 따라 보안기술이 적용된 장비, 제품, 서버에 대한 수요가 급격히 증가할 것으로 전망하고 있다. 특히, 전력분야의 속성상 테러집단, 해커 등으로부터 안전한 스마트그리드의 운영을 보장하기 위한 요구가 증대할 것으로 보여 보안제품 및 서비스, 보안기술이 적용된 하드웨어에 대한 수요가 늘어날 것으로 전망하고 있다.

[그림 4]는 U. S. DHS/DOE CS categories 근거한 스마트그리드 보안기술 분야별 시장전망은 장비보호 및 구성관리(Equipment Protection and Configuration Management), 위험관리(Risk Management), 침해사고 모니터링 및 대응(Monitoring and Incident Response), 접근/감사/무결성, 정책/계획/상황인지 등의 순으로 시장점유율을 예상된다[3].



〔그림 4〕 U. S. DHS/DOE CS 분야에 근거한
스마트그리드 보안기술분야별 시장전망
(출처: Pike Research, 2010)

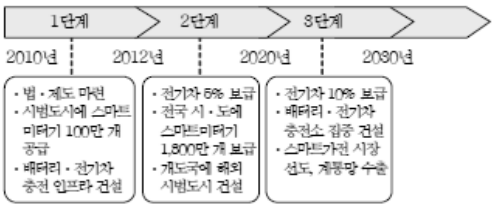
2.2 우리나라의 연구개발 동향

국내에서는 미국 등 해외 선진국가들 보다는 늦었지만 정부의 녹색성장정책과 맞물려 최근 빠른 속도로 진척되고 있다. 국토가 작은 것을 이점으로 2030년까지 전 국토에 걸쳐 지능형 전력 네트워크가 도입되는 세계 최초 국가단위의 지능형 전력네트워크 구축을 목표로 하고 있다. 녹색성장위원회의 로드맵을 요약하면 [그림 5]와 같고 2030년까지 녹색/품질요금제를 통해 에너지 사용량 15% 감소를 목표로 한다[2].

지식경제부는 '지능형 전력망 기본계획'을 발표하였는데, 2016년까지 스마트미터 1,000만대, 20만㎾h급 에너지 저장장치(ESS, Energy Storage System), 전기차 충전기 15만기를 보급한다. 또한 7개 광역 경제권별로 스마트 그리드를 구현할 거점도시를 구축한다고 발표했다.

이 계획에 따르면 상가와 빌딩에 스마트미터와 에너지 저장장치를 구축하고 지능형 수요관리를 실시해 실질적인 전기사용량 절감과 수요 분산을 유도한다는 방침이다. 올해에는 홈플러스, 이마트, 롯데마트, KT통신국, GS타워 및 포스코센터 등 467개소가 지능형 수요관리에 참가해 15,000여 가구가 사용할 수 있는 5만㎾의 전력이 절감될 것으로 지경부는 예상하면서 2016년

까지 지능형 수요관리 규모를 화력발전소 2기 규모인 120만㎾h까지 확대할 것이며, 계절과 시간대별로 전기요금을 다르게 적용하는 탄력요금제와 선택형 피크요금제 도입도 추진할 계획이라고 하였다[1].



〔그림 5〕 녹색성장위원회의 스마트 그리드 로드맵

한국전력은 2009년 8월 중으로 제주시에 스마트그리드 시범단지 조성을 시작하였다. 시범단지에는 풍력/태양광으로 생산된 전기의 송배전 시설, 분산 전원장치(배터리), 전기자동차 충전소, AMI 시스템 등 스마트그리드 관련한 많은 기술들이 도입될 계획이다. 대략 3천 가구를 대상으로 2012년까지 내구성과 안전성을 검증할 계획이다. 그 외에는 국책과제 중에 녹색 전력IT 10대 과제에 한전KDN, LS산전, 현대중공업, 효성 등의 기업체와 더불어 전력거래소, 전기연구원, 전력연구원, 한국전력 등의 공기업 및 연구소들도 참여하고 있다. 10대 과제는 전력의 송배전망 개선, 상태감시 및 관리 등의 시스템기술 등이 포함되어 있다.

지식경제부에서 전력산업융합원천기술개발사업의 일환으로 스마트그리드 보안체계 연구와 스마트그리드 DDoS 공격탐지 및 대응기술개발과제에 2013년까지 35억원을 지원하고 있으며, 스마트그리드 핵심보안기술개발을 위해 2015년까지 106억여원의 예산을 지원하는 것을 추진하고 있다. 한국스마트그리드사업단은 제주도에 스마트그리드 실증단지를 구성하여 운영하고 있으며, 실증단지 보안WG 및 보안센터 운영, 보안지침 및 보안가이드라인 제시, 각 운영센터별 보안대책 수립 및 이행 등을 통해 실증단지 보안대책을 다각도로 마련하고 있다[4].

Ⅲ. 스마트그리드에 대한 각종 위협과 사례

스마트그리드에서는 전력망에 통신망 기술이 접목되어 인터넷을 통하여 실시간으로 전력망을 감시, 통제, 변경할 수 있게 되므로 감청, 바이러스 감염, 사이버 공격, 해킹, DDoS 공격 등 모든 사이버 보안 위협에 노출되어 일반적인 IT 정보망에서의 단순한 정보유출을 넘어선 국가 기반시설 파괴 등의 거대한 재난상황으로 이어질 수 있다. 본 장에서는 독일, 미국 등 우수한 기술을 보유한 선진국들에도 직면했던 위협 사례들을 살펴본다.

3.1 스턱스넷(Stuxnet)

스턱스넷은 제어시스템을 공격하는 최초의 악성프로그램으로 한 국가의 주요 기간시설을 장악할 수 있는 사이버 무기로 작동된다. 전 세계적으로 사용되고 있는 독일 지멘스사의 산업자동화제어시스템을 공격 목표로 제작되어 원자력, 전기, 철강, 반도체 등 주요 산업 기반 시설의 제어시스템에 침투해 오작동을 일으키게 하여 시스템을 마비시킬 수 있다.

2010년 7월 이란의 우라늄 농축 시설을 공격하여 원심분리기를 감염시켰으며, 중국 1,000여개의 주요 산업 시설을 비롯해 전 세계 여러 국가에 감염이 확산되었다. 시만텍 보고서에 따르면 155개 국가 총 4만개의 스턱스넷 감염 IP가 조사되었으며, 이란 다음으로 한국이 감염 가능성이 높은 것으로 분석되었다[5].

3.2 미국 전력망 사이버 스파이

2009년 4월 미국의 전력망에 악성코드가 발견되었는데, 이는 중국과 러시아 등 해외의 사이버 스파이들이 미국의 전력 시설망에 침투해 시스템을 교란시키는데 이용할 소프트웨어를 심어둔 것으로 밝혀졌다. 악성코드를 이용하여 전기 공급을 차단할 수 있는 것이며, 이러한 시도는 특정 업체나 지역보다는 미국 전역을 대상으로 하고 있다. 또한, 인터넷을 통해 전기시설이나 원자력 발전소, 금융네트워크를 통제할 가능성이 우려되고 있으며 수도, 하수 등 다른 인프라 시스템도 위험에 누출될 수 있음을 시사한다. 사회 기반 시설이 점차 인터넷 기반의 통신에 의존하게 되면서 통제 시스템에 대한 스파이나 해커들에 의한 위협도 증가하고 있는 것이다[6].

3.3 스마트미터 사이버 공격

2009년 3월 CNN은 스마트 미터가 사이버 공격에 취약하다고 발표하였다. 차세대 전력망인 스마트그리드는

우리 모두에게 편리성을 주지만 위험성을 가지고 있는데 침투한 해커가 스마트그리드에 있는 수백만 개에 이르는 계량기의 동작을 멈추게 하여 대규모 정전 사태를 일으킬 수 있다는 것이다. 즉, 스마트미터를 통해서 스마트그리드 내부로 손쉽게 침투가 가능하여 대규모 스마트미터를 조작 가능하게 되어 전기수요 증감을 통한 전력망 불안정을 유도해서 대도시 정전 사태가 유발 가능함을 모의 해킹 실험을 통해서 그 위험성을 시사하였다[7].

Ⅳ. 스마트그리드에서의 안전성

4.1 보안 요구사항

스마트그리드는 공개된 통신망을 사용하는 것은 그만큼 여러 위험요인에 노출되어 있음을 의미함으로 안전한 스마트그리드 이용환경을 위해서는 반드시 높은 안정성과 신뢰성을 제공해야 한다. 따라서 여기에서는 스마트그리드에서의 보안요구사항을 정의하고자 한다.

4.1.1 기밀성(Confidentiality)

스마트그리드는 양방향 통신을 통해 에너지의 효율적인 관리가 이루어지기 때문에 전송되는 데이터의 내용을 권한이 없는 객체(unauthorized entity)에게 노출시켜서는 안 된다. 이를 위해 메시지 암호화가 필수적이며, 암호화와 함께 키 관리부분을 고려해야 한다. 크게 키는 마스터키(master key)와 세션키(session key)로 나눌 수 있으며 세션키는 마스터키를 통해 추출되므로 마스터키는 물리적인 공격까지 고려하여 보호해야 한다. 또한 세션키도 전방향 안정성(forward security) 등을 고려하여 각 세션마다 반드시 업데이트해야 한다. 기밀성은 시스템의 신뢰성과 밀접한 연관을 가지며 개인정보 유출과도 관련되므로 스마트그리드 환경에서 필수적으로 고려되어야 하는 요구사항이다.

4.1.2 가용성(Availability)

스마트그리드는 전력에너지 제공을 위한 인프라로 시스템의 성능 저하 또는 기능 마비가 되는 경우 국가적 재난을 초래할 수 있기 때문에 무엇보다도 가용성을 반드시 보장해야 한다. 스마트그리드 서비스가 공개된 망을 통해 이루어지기 때문에 특히 망의 허브 역할을 하는 AMI 등에 발생 가능한 여러 공격 (예를 들어, 서비스 거부 공격 등)을 방어할 수 있어야 한다. 또한 불가피하게 발생할 수 있는 자연재해 등 특정 상황에서 필수적으로 제공해야 하는 최소한의 기능과 자원들을 반드시 분류하고 별도의 안전조치를 취할 필요가 있다.

4.1.3 무결성(Integrity) 및 부인방지(non-reputation)

과금 정보 위·변조 등의 위협을 막기 위해 스마트그리드 내 모든 시스템들은 데이터의 내용 뿐 아니라 데이터 송신자 및 수신자, 작성자 등 통신망을 통해 전송되는 내용이 비권한자에 의해 변경되는 것을 탐지 및 검증할 수 있어야 한다. 이와 함께 시스템 운영상의 소프트웨어 업데이트 및 시스템 업그레이드가 발생하는 경우, 혹은 정전 및 피해 복구시에 데이터의 무결성을 보장함으로 시스템의 신뢰도를 높일 수 있다. 또한 데이터 소스 및 사용에 대한 증빙을 위해 부인방지도 반드시 필요하다.

4.1.4 사용자 및 기기 인증(Authentication)

다양하고 광범위한 환경을 가지는 스마트그리드는 반드시 사용자 대 기기, 기기 대 기기에 대한 상호인증이 필요하다. 스마트그리드를 구성하는 서버 및 기기들 간의 인증은 각 기기들 사이의 접근 및 권한통제 등 시스템 및 자원관리를 위해 고려되어야 하며, 특정 기능 및 데이터별로 인증을 지원할 수 있다. 사용자 대 기기의 경우 원격에서 사용되는 스마트그리드 환경에서 사용자를 확인하고, 해당 사용자에게 맞는 기능 지원 및 사용 허가, 과금 등을 위해 반드시 필요한 사항이다.

4.2 안전성 강화를 위한 보안 이슈

궁극적으로 안정된 전력을 공급하고, 댁내 스마트미터 설치와 운용으로 효율성을 높이며, 전기자동차의 보급 확대 등 스마트그리드의 이점과 함께 다양한 보안 요구사항을 구현하면서 국가에서는 안정된 운용과 사용자에게 편리함을 제공하게 될 것이다. 그렇지만, 앞에서도 나열하였듯이 새로운 보안 위협이 나타날 경우를 대

비하여 몇 가지 사항에 대하여 사전에 준비하고 대비한다면 보다 좋은 서비스를 제공하고, 받을 수 있을 것으로 보인다[8,9].

4.2.1 우리나라에 맞는 스마트그리드용 정보보호 가이드라인의 제정

'지능형전력망의 구축 및 이용촉진에 관한 법률(2011. 5. 24. 제정)'에 따라 시행계획을 수립할 때 우리나라의 지형적 특성, 전력소비 형태 등을 감안하여 망을 비롯하여 단말기까지의 모든 정보 및 흐름에 대한 정보보호 대책이 반드시 수립되어야 하며, 이때에 반드시 시행자에게 최소한 지켜야 할 가이드라인을 제정하여 각종 사이버 공경에 대응할 수 있어야 한다.

4.2.2 암호 · 인증 기술개발 및 체계 구축

스마트그리드에 적용되는 모든 기기는 반드시 국제표준을 준수하여야 한다. 그렇지만, 국내에 보급되는 스마트미터에는 관련기관에서 인정하는 암호 및 인증 체계를 사용하거나, 아니면 조속한 시일 내에 스마트그리드 전용 암호 및 인증 체계를 개발하여 적용하여야 한다. 특히 스마트미터의 물리적 제한이 있으므로 저전력의 소형 칩으로 구현해야한다. 또, 수많은 스마트미터 가입자에 대한 키관리 체계도 문제없이 운용될 수 있도록 준비하여야 한다. 아울러 전체 스마트그리드의 보안체계의 관제를 위한 시스템의 개발도 병행되어야 한다.

4.2.3 평가 체계의 확보

국제공통평가기준인 CC에서는 민간제품에 대하여 EAL5, SCADA 시스템과 같은 정교하고 중요시설에 대하여는 EAL7을 부여하는 바, 국내에서도 EAL5 이상의 평가 능력을 확보하여야 한다. 이를 위한 평가 전문기관의 선정, 평가 전문 인력의 확보 등도 수반되어야 한다.

4.2.4 전자결재

전기자동차를 활용하는 것도 스마트그리드의 새로운 도전일 것이다. 충전소에서 충전 비용의 결재를 위해서는 여러 방법이 가능할 것으로 보인다. 통상적인 신용카드를 활용한다면 현재의 결재 메커니즘을 그대로 사용할 수 있지만, 사용자의 댁내 스마트미터와의 연계를 할 경우에 대한 결재 전용 정보보호 체계의 수립과 현행 결재체계와의 연동도 고려해야 할 것이다.

Ⅴ. 결 론

2011년 일본 쓰나미와 함께 터진 후쿠시마 원전사고는 그렇지 않아도 부족한 전력공급을 더 어렵게 하였다. 그렇지만 부족한 전력의 안정된 공급을 위한 스마트그리드의 조기 정착을 위한 정부의 다각도의 노력은 더 서둘러서 추진했어야 할 사업일지도 모른다. IT발전과 함께 점차 지능화되는 전력시스템에 각종 사이버 공격이 나타나게 되면 어렵게 추진하였던 사업은 물론 우리 생활의 기반이 되는 전력 공급조차 위협받게 될 것이다.

본 논문에서는 스마트그리드 시스템에서 유기적이고, 적응적인 인증을 통해 보다 안전하고 효율적인 시스템의 구축이 되도록 몇 가지 문제를 제시하였다. 현재 진행중인 사업에 특정 암호 알고리즘에 대한 정의나 보안 시스템 구성에는 어려움이 있으나 본 논문에서 제시한 문제점들을 점차 해결하고 관련 기술들을 개발해야 할 것이다.

참고문헌

[1] http://news.imaso.co.kr/archives/8864, 2012. 7. 18.

[2] 도윤미, 김선진, 허태욱, 박노성, 김현학, 홍승기, 서정혜, 전종암, "스마트 그리드 기술 동향: 전력망과 정보통신의 융합기술," 전자통신동향분석, pp. 74-86, 2009. 10.

[3] 한국에너지기술평가원, "스마트그리드 보안기술 연구개발 상세기획보고서 : 전력계통/IT분과," 2010. 3.

[4] 서정택, "*스마트그리드 보안*," 스마트그리드 핵심기술교육, 한국스마트그리드협회, 2012. 6.

[5] Nicolas Falliere, Liam O. Murchu and Eric Chien, "W32. Stuxnet Dossier," Symantec Security Response, 2010. 9.

[6] Siobhan Gorman, "Electricity Grid in U.S. Penetrated By Spies," Wall Street Journal, 2009. 4. 8.

[7] Zoe Slocum, "Report: Smart-grid hankers could cause blackouts", CNN, 2009. 3.

[8] 서우석, 전문석, “스마트그리드(Smart Grid) 전력망과 정보통신망 융합보안방향,” pp. 477-486, 한국전자통신학회논문지 제5권 제5호, 2010. 10.
[9] 이철환, 홍석원, 이명호, 이태진, “한국형 스마트그리드를 위한 정보보호체계 및 대책,” pp. 71-89, Internet and Information Security 제2권 제1호, 2011. 5.

〈著者紹介〉

정 교 일 (Kyo-Il Chung)
종신회원
1981년 2월: 한양대학교 전자공학과 학사
1983년 8월: 한양대학교 대학원 전자계산학과 석사
1997년 8월: 한양대학교 대학원 전자공학과 박사
1980년 12월~1981년 11월: 엠-시스템즈 연구원
1981년 12월~현재: 한국자통신연구원 책임연구원
1991년 1월~현재: 한국정보보호학회 이사, 부회장
<관심분야> RFID/USN, 정보보호, IT-융합(국방, 유헬스, 방재 등)

박 한 나 (Han-na Park)
정회원
2008년 2월: 서울시립대 수학과 학사
2010년 2월: 고려대학교 정보보호학과 석사
2010년 9월~현재: 한국전자통신연구원, 연구원
<관심분야> RFID/USN, 정보보호, 유헬스, 프라이버시보호

정 부 금 (Boo-Geum Jung)
정회원
1986년 2월: 부산대학교 계산통계학과 학사
1991년 8월: 숙명여자대학교 전산학과 석사
1986년 1월~현재: 한국전자통신연구원 책임연구원
<관심분야> Security, 프라이버시보호, Internet Platform/Operating System/Distributed Network

장 종 수 (Jong-Soo Jang)
종신회원
1984년 2월: 경북대학교 전자공학과 학사
1986년 2월: 경북대학교 전자공학과 석사
2000년 2월: 충북대학교 컴퓨터공학과 박사
1989년 7월~현재: 한국전자통신연구원 책임연구원
2004년 1월~현재: 한국정보보호학회 이사, 부회장
2011년 12월~현재: 국가정보화전략위원회 정보화역기능전문위원
<관심분야> 정보보호, 영상보안, 네트워크관리

정 명 애 (Myung-Ae Chung)
1986년 2월: 이화여자대학교 물리화학과 학사
1988년 2월: 이화여자대학교 물리화학과 석사
1999년 7월: Clausthal 공대 고분자물리학 박사
2000년 5월~현재: 한국전자통신연구원 부장, 책임연구원
<관심분야> IT-융합(유헬스, 바이오 등)