스마트그리드 보안기술 동향분석 및 대응방안

유성민, 김남균, 김윤기
KT 융합기술원

요 약

에너지에 대한 수요가 급증하게 되면서 에너지의 효율적인 운영관리가 대두되기 시작하였다. 따라서 기존 전력 및 신재생에너지 기술에 ICT 기술이 융합된 스마트그리드 기술이 전 세계적으로 각광받기 시작하였다. 스마트그리드 기술은 사용자와 공급자에게 양방향 정보교환을 통하여 더욱 합리적인 의사결정이 가능하게 하였으며, 이러한 의사결정은 에너지의 효율적인 공급과 효율적인 사용으로 인한 에너지 낭비제거 그리고 에너지 신뢰성을 향상시킬 수 있다. 그러나 이러한 장점에도 불구하고 스마트그리드의 경우 ICT 기반의 네트워크를 통하여 정보를 공유를 하고 있기 때문에 사이버 침투에 취약하다는 약점이 있다. 그래서 이러한 약점을 보완하기 위하여 보안과 관련한 연구도 활발히 진행되어야 한다. 이번 본 고에서는 스마트그리드 보안 취약점과 그에 따른 사례들을 살펴보고 이에 대한 대응방안에 대하여 간략히 기술하고자 한다.

Ⅰ. 서 론

지난 1월 금융개인정보 유출 사건은, 금융의 보안의 취약성뿐만 아니라 국내 보안의 취약점을 드러내는 계기라 할 수 있다. 비록 눈에 보일만한 직접적인 피해는 없지만 3개 카드사 가입 고객의 정보 1억 건이 되는 정보가 유출되었다. 현재 정부는 금융개인정보 유출사건 재 방지를 위하여 관련 보안정책 및 개선방안을 검토 중에 있다.

만일 보안의 취약성으로 인하여 단순히 개인정보 유출에서 끝나는 것이 아니라 영화에 나올법한 관련 시스템 해킹으로 대형 미사일이 어떤 지역을 공격을 하는 불상사 혹은 단순한 시스템의 해킹으로 도시가 마비가 되어 버린다면 어떻게 되어 버릴까? 지금까지 이러한 상황들을 영화에서만 보아왔다면 가까운 미래에는 적국으로부터 이러한 공격이 충분히 가능하다. 그 이유는, ICT 및 네트워크 기술의 발달로 인하여, 우리의 삶에 밀접하게 연관되고 있기 때문이다.

그리고 이러한 대표적인 위험이 존재하는 사례가 기존 전력망에 ICT 기술이 융합된 스마트그리드 기술이라 할 수 있다[1].

스마트그리드 기술은 기존의 전력망에 ICT 기술이 적용 되어 기존의 불안정한 전력의 안전성을 높일 뿐만 아니라 에너지효율성을 향상 시킬 수 있다. 여기에 적용된 기술들은 AMI, 스마트미터기술, HAN (Home Network Area), 클라우드 컴퓨팅등 통신 기술들이 있다[2][3][4]. 비록 이러한 기술이 전력망의 안정성을 높여 줄 수는 있겠으나 위에 언급된 ICT 인프라 기술에 사이버 및 물리공격을 통하여 네트워크 및 ICT에 큰 혼란을 초래 할 수 있다[5][6].

스마트그리드 기술의 경우 전력 공급 및 수요상황 예측뿐만 아니라 원격으로 관제도 가능하기 때문에 자칫 네트워크를 통한 사이버 해킹에 의하여 정전상황이 발생할 수 있다. 뿐만 아니라 가정용 AMI의 경우 건물의 에너지 사용정보 제공뿐만 아니라 시스템적으로 제어까지 가능하다. 따라서 악의적으로 이러한 시스템을 해킹할 시 건물사용자의 정보뿐만 아니라 건물의 설비사용 및 일반가정에 큰 혼란을 야기 할 수 있다. 다시 말하여 단순한 시스템의 해킹으로 국가전체를 마비시킬 수 있다.

따라서 국가 에너지 효율화 및 신성장 동력으로서[7], 스마트그리드 사업의 육성도 중요하지만 보안이 뒷받침되어야 한다. 그렇기 때문에 스마트그리드 보안관련 연구는 매우 중요하다.

본 고에서는 스마트그리드 보안취약점에 대하여 살펴보고 이에 대한 대응방안에 대하여 논의 하고자 한다. 본 고의 구성은 다음과 같다. 제 2장에서는 스마트그리드 기술에 대하여 간략히 살펴보도록 하겠다. 그런 다음 보안에 대한 위협이 될 만한 소지 및 사례들을 살펴보도록 하겠다. 그런 다음 스마트그리드 위협에 대한 대응방안에 대하여 간략히 설명하고 결론부분에서는 추가적으로 보안기술의 연구방향에 대하여 언급하면서 본 고를 마무리 하도록 하겠다.

Ⅱ. 본 론

1. 스마트그리드 정의

스마트그리드 기술에 대한 정의는 명확하지 않고 각 나라, 기관별 정의는 약간 다르지만 그 맥락은 비슷하다[8][9]. 일반적으로 스마트그리드 기술은, 기존의 '발전-송전-배전-판매'의 단일 단계로 구성되어 기존의 전력망에 ICT 기술이 결합된 지능형 전력기술로, 공급자와 소비자가 양방향으로 실시간 에너지 사용정보를 교환함으로써 에너지 효율을 최적화 시켜주는 기술로 정의된다 〈그림 1〉참조[10]. 그러나 앞서 언급되었듯이 대체적으로 스마트그리드에 대한 기술정의는 비슷하나 각 기관별로 다르다. 미국의 경우, 에너지 독립 및 안보법에서 미래의 증가할 에너지 수요를 완화 시키고 전력 전송과 분배에 있어 신뢰성과 기반시설보호를 유지 할 수 있도록 구조화된 지능형 국가 전송 분배 시스템으로 정의된다[6]. 반면 유럽의 경우, 지속가능하고, 효율적이며, 안전한 전기 공급을 효율적으로 전송하기 위하여 연결된 모든 이용 관계자들의 행위를 지능적으로 통합 할 수 있는 지능형 네트워크로 정의하고 있다[11]. 이러한 스마트그리드 기술은 기존 전력망에 ICT 기술 융합정의 이외에도 그린기술과 ICT 기술이 융합된 그린 ICT 기술로 정의된다 [12]. 그린 ICT 기술로 정의되는 스마트그리드 기술은, 덴마크과학기술 및 혁신부에 따르면 환경친화 적이며 지속가능한 ICT 기술로도 정의된다[13].

그린기술 및 기존 전력망에서 ICT기술이 융합된 기술로 정의되는 스마트그리드는, IT산업뿐만 아니라 유관산업 (통신, 가전, 건설, 자동차, 에너지등)에도 시너지 기회를 제공하고 이러한 산업들을 촉진시켜 경제 활성화에 큰 기여 할 것으로 조사된다. 국내 스마트그리드 산업의 경제적 파급효과에 대한 연구에 따르면, 2010년-2020년까지 총 생산유발액은 약 77조원 총부가가치 유발액은 약 24조원 그리고 총 고용유발이원은 약 31만명에 이를 정도로 경제 활성화에 큰 기여를 할 것으로 전망된다[14][15].

다시 말하여, 스마트그리드 기술은 전력 공급의 안정성, 공급-수요 불균형해소 문제해결, 효율적인 에너지관리로 인한 에너지효율화 그리고 에너지 절감을 통한 저탄소 국가 실현뿐만 아니라 경제성장동력으로서 스마트그리드 기술은 매우 유망하다 할 수 있다. 참고로 스마트그리드 세계 시장은 연평균 8% 성장하여 2020년에 400조원에 이를 것으로 전망되었다[16]. 그러므로 전 세계적으로 각광받는 스마트그리드 기술에 대한 시장 경쟁력 확보하고자 선진국 및 중국은 스마트그리드에 대한 기술에 적극 투자하고 있다 [17]-[20]. 비록 이러한 스마트그리드에 대한 기술이 발전하여 국가 정책에 큰 긍정적인 혜택을 불러온다 할지라도 보안에 대한 접목되지 않는다면 전력망의 융합에 의한 해킹공격에 노출되어 심각한 피해를 야기할 수 있다[21]. 따라서 이러한 심각한 피해를 막기 위해서는 스마트그리드에 대한 기술개발과 동시에 보안에 대한 방안도 같이 이루어져야 한다. 이러한 주제에 관하여서는 5장에서 다루도록 하겠다.

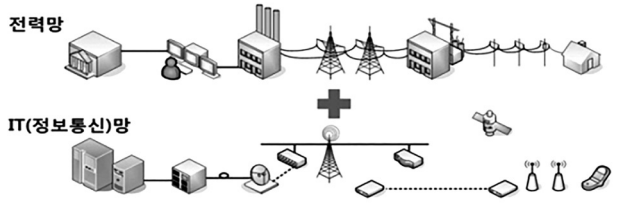

그림 1. 스마트그리드 개념도

2. 스마트그리드 기술 구성요소

2.1 스마트미터기

스마트미터기 (혹은 디지털미터기)는 분전반 및 배전반에 설치되어 에너지 사용량을 측정하는 기기이다[22]. 참고로 스마트미터기와 디지털미터기의 차이는 에너지 사용량을 에너지 요금으로 환산하여 주느냐 않느냐 이다. 스마트미터기의 경우 에너지사용량을 바탕으로 에너지사용요금으로 환산하여 주지만 디지털미터기는 단순히 에너지 사용량만 측정하여 준다. 과거에 스마트미터기는 단순히 에너지 사용량을 실시간으로 측정하여 스마트디스플레이에 에너지 사용량을 실시간으로 표출하는 기능만 가지고 있었다. 그러나 현재의 경우 실시간 에너지사용량 정보표출뿐만 아니라 과거 데이터 분석 및 통계분석까지 다양한 서비스를 제공하는 역할까지 담당 하고 있다[23][24].

2.2 AMI (Advanced Metering Infrastructure)

AMI 시스템은 자동검침 (AMR: Automated Meter Reading)에서 발전된 양방향 원격검침시스템으로서 에너지 사용량을 원격으로 검침하는 시스템이다[25]. 이러한 시스템은 스마트그리드 실현에 있어서 핵심 구축 시스템으로서 전력을 공급하는 에너지 설비와 에너지 사용 정보를 수집 분석하여 정보통신 설비를 총칭하는 의미로 사용되며, 현재 미국, 유럽과 같은 선진국에 도입이 되어 사용되고 있다. AMI 시스템에는 스마트미터기 양방향 통신을 기반으로 하고 있기 때문에 원격제어가 가능하며, 실시간으로 소비자들의 에너지 사용량을 체크하고 있기 때문에 수요예측 및 부하관리에도 활용이 가능하다.

이러한 AMI 시스템은 에너지 공급자와 소비자에게 양방향 통

신을 제공하여 서로에게 합리적인 정보를 제공함으로 인하여 에너지 사용량을 효율적으로 제어하여 에너지의 소모량 및 비용을 줄일 수 있다[26]. 뿐만 아니라 기술이 좀더 고도화 될 시 수요에 따른 에너지요금이 변화하는 RTP (Real Time Pricing) 요금제를 제공함으로서 에너지시장에 참여하는 수요반응 (DR: Demand Response)을 유도하여 에너지 관리의 효율화를 꾀할 수 있다[27][28].

2.3 HAN (Home Area Network)

정보가전을 포함한 가정의 전력기기를 유무선통신을 통해 관리하는 역할을 담당하고 있는 기술로서 AMI의 양방향통신 기술에 핵심요소 이다[29][30]. HAN은 네트워크에 기술에 따라서 다양한 네트워크 형태로 이루어 질 수 있는데, 이더넷, 무선랜, Zigbee, 전력선 통신 등 다양한 기술이 HAN을 구축하는 데에 사용될 수 있다[31].

2.4 MDMS (Meter Data Management System)

MDMS는, "HAN과 Smart Meter와 같은 AMI기반 인프라를 통해 수많은 수요 측 데이터를 수집, 취득하고 이들 데이터를 처리, 가공, 분석하여 가치 있는 정보로 변환시켜 요금서비스 및 다양한 부가서비스 창출에 활용되는 소프트웨어 인프라" 이다[32]. MDMS는, 미터기와 통신장비와 같은 하드웨어 및 소프트웨어로 이루어진 AMI의 로그정보들을 저장하게 된다[31], [32]. 이러한 정보를 통하여 MDMS는 '데이터수신,"데이터 보급 및 전달,' '데이터관리' 그리고 '데이터저장'과 같은 4개의 기능을 수행하게 된다[32].

2.5 EMS (Energy Management System)

국내의 경우 BEMS (Building Energy Management System)라고 지칭되는 EMS 는 AMI, 데이터정보를 가시화하는 GUI (Graphic User Interface) 및 MDMS 등으로 구성되는 에너지 관리시스템을 말한다. EMS의 경우 건물에 적용되면 BEMS라고 지칭되며 가정에 적용되어 나온 시스템을 HEMS (Home Energy Management System)로 지칭된다. EMS는, 건물 내&외부환경과 에너지 사용량 데이터를 분석하여 쾌적한 실내환경을 유지하면서 에너지 성능을 높이기 위하여 도입된 시스템을 말한다[33][34]. EMS는 대체적으로 에너지수요예측, 에너지정보가시화, 지능형건물설비 자동화 등 건물 및 가정의 에너지 관리서비스를 수행한다[35].

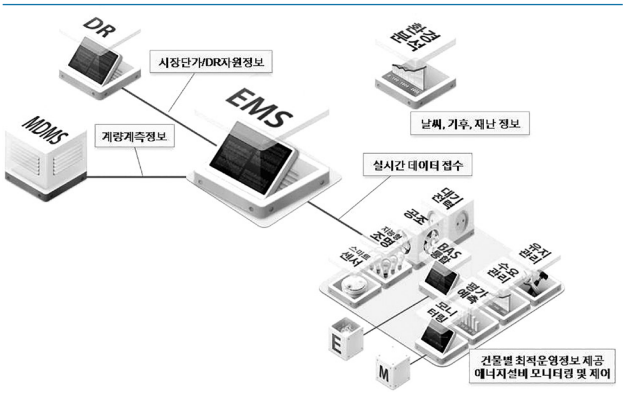

그림 2. EMS 구성도

3. 스마트그리드 보안위협 요소

3.1 펌웨어조작

보안대상 아래에 없는 기기들 혹은 보안이 허술한 기기들은 일차적으로 펌웨어 조작의 위험성에 노출될 가능성이 크다. 만일 펌웨어가 손상되게 된다면 기기들의 정상적인 동작에 지장이 생기게 되며 기기들의 정보를 송수신 하는 데에 많은 어려움이 뒤 따를 수 있다. 더군다나, "보안기능을 갖는 모든 기기들은 암호화를 위하여 암호키를 펌웨어 형태로 내장하게 된다. 그러므로 펌웨어를 해독함으로써 장치에 설정되어 있는 암호키를 알아내어 모든 정보가 유출될 수 있는 위험이 존재한다[22].

3.2 램공격

전력 (혹은 에너지) 사용량 데이터 표출하고 한국전력과 데이터 송수신 역할을 담당하는 스마트미터기의 경우[23], 해당기기의 램 공격위험에 노출되어 있다[21][24]. 참고로 램 공격이란, 해커가 주사기를 이용해 계량기의 메모리 칩의 각 측면에 바늘을 삽입하여 메모리 칩의 전기신호를 가로채는 것을 말한다. 이러한 램 공격을 통하여 해커들은 그러한 신호를 분석 함으로서 스마트미터기의 프로그램을 조정 및 정보를 분석하여 정보유출 및 정보왜곡을 시킬 수 있다[29]. 실제로 사용자가 램의 공격을 당하게 된다면 왜곡된 에너지 사용정보 및 사용요금 정보를 전달 받을 수 있다. 뿐만 아니라 사용자의 에너지 사용정보를 분석하여 사용자가 언제 집을 비우게 되는 시점추론이 가능하기 때문에 사용자는 본인의 거주지에 안전에도 위협요소가 될 수 있다.

3.3 네트워크 공격

해커가 만일 스마트미터기의 프로그래밍 해킹을 통하여 접속

을 하였다면, "전력망에 부착된 웜(Worm)이나 다른 악성코드"에 노출될 위험이 있다[29]. 만일 이러한 악성코드에 노출되면, 에너지 사용정보 및 제어정보의 위/변조를 일으킬 수 있으며 건물사용자에게 에너지 효율정보에 큰 혼란을 야기시킬 수 있다. 피해 범위의 경우 해커가 어떤 프로그래밍을 해킹하였느냐에 따라 달라질 수 있다. 다시 말하여 스마트미터기는 건물 내부에서 에너지 사용정보를 네트워크를 통하여 송수신을 하며 그리고 과금 정보 및 에너지 효율화를 위해서 에너지사용량정보 센터 서버와도 송수신을 하게 된다. 이 때 해커가 건물 내부의 네트워크 망을 해킹하게 된다면 개인 한 가정의 문제로 끝날 수 있지만 만일 데이터 서버와 송수신 하는 네트워크가 해킹 당하게 된다면 서버에서 관리하고 있는 데이터 정보유출뿐만 아니라 서버의 관리 대상이 되는 스마트미터기들의 모든 오작동의 원인이 되어 피해가 크다. 따라서 서버와 스마트미터기의 네트워크 망의 보안의 경우 각별한 주의가 요구된다.

3.4 서비스 중지 공격

해커는 스마트그리드의 구성장치에 대해서 컴퓨팅 자원을 고갈시키는 공격을 통하여 사용자에게 정상적인 동작이 불가능하게 끔 공격을 할 수 있다. 이러한 공격은 노드 간에 세션을 하이재킹 하여 메시지를 집중 전송함으로써 가능하다. 현재 네트워크에서 가능한 모든 종류의 서비스 중지 공격은 외부통신과 연결이 되어 있는 스마트그리드 전력망의 모든 노드에 대해서 가능하다고 할 수 있다[31].

한국형 스마트그리드에서의 보안 위협 및 보안 요구사항 원고에 따르면, 스마트그리드 기술이 적용된 AMI의 장치들에 다음과 같은 두 가지 사항으로 인하여 서비스 중지공격을 쉽게 받을 수 있다. 첫 번째의 경우 AMI 장치 구성들은 임베디드 시스템 기본의 필드 장치로서 거의 대부분 제한된 메모리를 가지고 있기 때문에 간단한 트래픽의 증가만으로도 정상적인 서비스 활동을 할 수 없는 경우가 많이 있다. 뿐만 아니라 HAN은 외부통신과 연결되어 있는 개방된 망으로서 외부에서 쉽게 접근할 수 있기 때문에 이러한 위험에 노출되어 있다[31].

비록 이러한 공격이 쉽게 노출이 되어 있지만 AMI의 경우 각 가정마다 보급이 되어 운영되고 있기 때문에 이러한 공격의 파급효과가 해당 노드에만 한정되어 있기 때문에 피해 정도는 낮다고 할 수 있다. 그러나 AMI의 상위에 존재하는 AMI 헤드엔드, HAN 및 MDMS의 경우에도 외부에 노출될 가능성이 있으며 외부공격을 당하였을 경우 하부의 모든 AMI 미터에 피해를 줄 수 있다[31].

4. 스마트그리드 보안 위협사례

앞 장에서는 스마트그리드의 보안 위협요소에 대하여 살펴보았다. 앞 장에 언급되었듯이 해커들은 다양한 경로를 통하여 스마트그리드 네트워크 망 혹은 일반가정의 네트워크 망을 공격할 수 있다. 비록 현재까지 스마트그리드 기술적용개발은 진행중에 있으며 아직까지 개발 완료단계가 아닌 상태이다. 그러나 기존 전력망 침투 및 스마트그리드 네트워크 보안침투 사례가 이미 발생하여 국가 기반 시설 및 사회에 큰 혼돈을 야기시키고 있다. 본 장에서는 이러한 대표적인 몇몇 사례들에 관하여 살펴보도록 하겠다.

그 중 대표적인 사례가 악성코드 (스틱스넷)을 통한 전력망 제어 시스템 공격이라 할 수 있다. 스틱스넷은 전력 제어시스템을 공격하는 악성코드 프로그램으로서 국가의 주요기반 시설에 혼란을 주는 목적으로 개발되었다. 이러한 공격의 대표적인 사례로서 2010년 07월 이란의 우라늄 농축 시설을 공격하여 원심분리기를 감염시킨 사례와 중국의 1,000개의 주요산업 시설에 스틱스넷을 감염시킨 사례들이 있다[36][37].

또 하나의 대표적인 사례로 미국의 사이버스파이를 들 수 있다. 2009년 4월 미국의 전력망에 악성코드가 발견되었는데 확인결과 중국과 러시아 등 해외의 사이버 스파이들이 미국의 전력 시설망에 해킹하여 악성코드로 심어 둔 것으로 밝혀졌다[36]. 이러한 시스템들은 미국 전체주의 전력 공급을 차단 할 수 있다는 사실이 밝혀지면서 큰 충격을 주었다. 즉 스마트그리드 전력 및 네트워크 망의 공격은 단순한 피해로 그치는 것이 아닌 국가에 큰 재앙을 초래 할 수 있기 때문에 이에 대한 보안 강구 필요하다. 따라서 다음 장에서는 스마트그리드 보안 대책방안에 대한 주제를 다뤄보도록 하겠다.

5. 스마트그리드 보안 취약점 대처방안

5.1 스마트그리드 보안요구 사항

스마트그리드 보안위협에 대비하기 위하여서는 다음과 같은 6가지 측면에서 대비가 이루어져야 한다: 기밀성, 무결성, 가용성, 사용자인증, 부인방지 및 접근제어[29][38]. 보안요구사항에 대한 아래의 〈표 1〉에 정리하였다. 스마트그리드 전력망의 안정적인 공급, 네트워크의 안정적인 운영 및 사용자 정보의 침해를 방지하기 위해서는 6가지 사항이 보안에 필수적으로 이루어져야 한다.

표 1. 보안 필수 구성요소

보안요소	보안요소 정의
기밀성	권한이 없는 사용자가 정보를 읽을 수 없도록 암호화를 통하여 방지하는 것을 의미하며, 스마트전자제품에서 데이터 수집 시 요구 됨
무결성	송신자가 전송한 원래의 메시지의 내용이 변경되지 않는 것을 의미하며, 스마트그리드 무선 센서의 보안 취약성 방지
가용성	권한이 부여된 사용자가 서비스에 접근을 보장하는 것을 의미하며, 서비스 거부공격의 방지가 주요관건
인증	사용자 및 기기들이 서비스 접근에 인증되었는지 여부를 판단하는 기능
부인방지	전자서명이나 공개키 등을 이용하여 송수신 사실을 부인 할 수 없도록 하는 것을 의미 함
접근제어	사용자 및 기기의 특성에 따라 서비스 접근가능성을 차등 부여하여 접근 통제하는 것을 말함

5.2 스마트그리드 보안 취약점 보완방안

네트워크 및 스마트 인프라의 비약적인 발달로 인하여 국가간의 물리적인 공격이 뿐만 아니라 사이버 상의 공격이 가능하게 되었다. 그리고 앞으로 물리적 공격보다는 사이버 상의 공격이 국가의 피해를 입히는 가장 효율적인 방법이 될 것으로 예측된다. 따라서 앞으로의 국가 경쟁력은 시장을 창출 할 수 있는 기술산업의 경쟁력도 중요하지만 사이버상의 공격을 대비하기 위한 보안 기술 확보 및 보안인력이 국가 경쟁력에 매우 중요할 것으로 예상된다. 특히 국가의 가장 중요한 기반시설 전력부문의 경우 스마트그리드 기술의 대두와 함께 전력보안뿐만 아니라 정보통신 보안도 함께 대응할 수 있는 인력이 필요하다. 그 이유는, 정보통신과 전력망 인력구성 자체를 일원 함으로써 스마트그리드 기술만에 대한 전문인력을 확충하여 국가의 중요 기반시설에 대한 보완이 강화되어야 하기 때문이다[21].

또한 스마트미터 및 네트워크 망의 경우 해커가 물리적으로 램 공격과 같은 사이버 공격이 가능하기 때문에 물리적인 공격에도 대응할 방안을 모색하여야 한다. 따라서 스마트미터 및 기타 AMI 관련 기기들의 경우 제 3자가 침투하지 못하도록 스마트미터기 및 AMI 설치장소를 비 공개된 구역 및 접근을 차단할 수 있는 기기 암호화를 하는 등의 대책방안이 필요하다.

해커의 경우 사이버 침투를 위하여 여러 차례 공격 및 시도를 가하여 취약부분을 노릴 것이다. 따라서 스마트그리드의 통신 및 전력망 안정성 확보를 위하여 별도의 사이버보안센터를 구축하여 모의침투를 통하여 취약점을 계속 보완하여 나갈 필요가 있다. 뿐만 아니라 스마트그리드가 사이버 침투공격에 당하였을 시에도 피해규모를 줄이기 위하여 별도의 대책 안을 마련해두어야 한다.

끝으로, 스마트그리드 기술의 경우 AMI, 네트워크 망, 데이터베이스 등등 여러기기들로 구성되어 있다. 따라서 이러한 이유로 해커들의 침투경로가 다양하다고 할 수 있으며, 이러한 공격들을 미리 사전에 방지하기란 현실적으로 불가능하다. 따라서 스마트그리드의 피해사항 및 여러가지 요소들을 고려하여 보안의 중요도에 따라 위험유형을 정리하고 가장 피해가 크거나 위험유형이 큰 사이버 침투 및 중요도가 높은 기기들을 중점적으로 고려하여 보안 대처 방안을 세워 둘 필요가 있다. 예를 들어 개인 에너지 사용량 정보를 담고 있는 서버의 경우 매우 중요하기 때문에 별도로 중점적으로 관리할 필요가 있다.

Ⅲ. 결 론

지금까지 본고에서는 스마트그리드에 대한 보안에 대하여 다루어 기술하였다. 스마트그리드 기술은 국가의 비용효율성, 신성장 동력 그리고 지구온난화를 대처가 가능하여 각광받고 있다. 그러나 스마트그리드 기술의 경우 ICT 기술이 융합된 새로운 기술이기 때문에 기존 전력망에 존재하지 않는 위험이 존재한다. 이러한 위험은 공격 유형에 따라 국가 전체에 피해를 줄 수 있기 때문에 정부는 이에 대응방안을 모색하여야 한다. 따라서 본 고에서는 스마트그리드 기술에 대한 정의를 먼저 살펴본 뒤, 스마트그리드 기술의 취약점 및 해외 사례들을 살펴보았다. 그리고 난 뒤 스마트그리드의 사이버 침투대응 방안에 대하여 거시적으로 살펴보았다. 비록 본 고에서는 이러한 주제를 단순히 거시적인 차원에서만 살펴보았지만, 앞으로 스마트그리드 사이버 침투를 줄이기 위해서는 정부는 기술적으로 정책적으로 모색방안에 관한 연구를 진행하여야 한다.

참 고 문 헌

[1] C. G. Park and S. J. Kim, “Smart Grid technology trend and market trend analysis”, Dongyang brief,, No. 2011-2014, June 2011.

[2] International Agency Environment, “The World Outlook 2011,” 2011.

[3] Vincent J Forte and Je.. Member of IEEE, “Smart Grid at National Grid,” Innovative Smart Grid Tchnologies, 2010.

[4] SungMin Rue, Haeju Jung, Daekyo Jung, Namkyun Kim, Hyunsook Kim and Yoonkee Kim, “kt BAS

Integration Technology davelopment based on ICT," Journal of Korea Institute of Next Generation Computing, vol. 10, no. 1, Feb. 2014.

[5] S. Massoud Amin and Bruce F. Wollenberg, "Toward a S,art Grid: Power Delivery for the 21st Century," IEEE Power Energy Magazine, Vol.3, Issue . 5, pp. 33-41, Sep. 2005.

[6] European Technology Platform, "Smart Grid Start egic Deployment Document for Europe's Electricity Networks of the Future," Apr. 2009.

[7] You Jin Kim, Byung Sun Cho and Jim Bo Sun, "The Economic Impact of the Smart Grid Industry by using Input-Output Analysis", Journal of KICS, Vol. 35, No. 8, Aug. 2010.

[8]Sung-Ho Lee and Yong-Hwan Cho, "Trends of Smmart Grid and Importance of Security" 2012 Korea Entertainment Industry Association Spring Confrence, 129-132, Apr. 2012.

[9] Fred Sissine, "Energy Independence and Security Act of 2007: A Summary of Major Provisions,"CRS Report for Congress, Dec. 2007.

[10]C.G Park and SJ. Kim, "Smart Grid technology trend and market trend analysis," Dongyang brief, No. 2011-4, June. 2011.

[11] Department of Energy, "The Smart Grid: An introduction," Apr. 2009.

[12] Young Ho Shim, Ki Youn Kim, Ji Yeon Cho, Jin Kyung Park and Bong Gyou Lee, "Strategic Priority of Green ICT Policy in Korea: Applying Analytic Hierarchy Process, World of Academy Science," Engineering and Technology 58, 2009.

[13] Danish Ministry of Science Technology and Innovation (MSTI), "Action Plan for Green IT in Denmark," 2007.

[14] Yoo Jin Kim, Byun Seo Cho and Jin Bo Sun, "The Economic Impact of the Smart Grid Industry by using Input-Output Analysis,"Journal of KICS, Vol. 35, No. 8, Aug. 2010.

[15] Myung-Kyu Lee and Sun-Hyung Kim, "Analysis of Smart Grid Technologies and Domestic and Foreign Policy Trends", Journal of Korea Institue of Information Technology, Vol. 11, No. 8, pp. 181-187, Aug. 2013.

[16] David Groarke, Zach Pollock and Ben Kellison, "Global Smart Grid Technologies and Growth Markets 2013-2020", GTM research, July. 2013.

[17] Mihye Lee and Jinkwon Lee, "Smart Grid Market Trend and Forecast", Korea Eximbank, Industrial Risk report, Vol. 2012-G-09, Dec. 2012.

[18] Taisiya Kim, Soo Kyung Park, Bong Gyou Lee, "What is Appropriate Strategy for Smart Grid Business: A case study of Test Bed in Korea" Ubiquitous Information Technologies and Applications (CUTE), 2010 Proceedings of the 5thInternationalConferenceon, Dec. 2010.

[19] Namhoon Kim, "Review of smart grid trend and market analysis", Hana Institute of Finance, Volume 18, Sep. 2010.

[20] Jerry Li, "From Strong to Smart: the Chinese Smart Grid and its relation with the Globe," AEPN (Asia Energy Platform), Sep. 2009.

[21] Woo-seok Seo and Moon-seog Jun, "A Direction of Convergence and Security of Smart Grid and Information Communication Network,"Journal of Korean institute of electronic communication sciences, Vol. 5, No. 5, Oct. 2010.

[22] Daekyo Jung, SungMin Rue, Yoonkee Kim and Byung-deok Chung, "Korea Micro Enery Grid Technology: The use case of the First-town in Sejong," 2013 15th Asia-pacific Network Operations and Management Symposium, Sep. 2013.

[23] Tom Hargreaves, Michael Nye and Jacquelin Burgess, "Making energy visible: A qualitative field study of how householders interact with feedback from smart energy monitors," Energy Policy 38, pp. 6111-6119, July. 2010.

[24] McDaniel, Patrick, and Stephen McLaughlin, "Security and privacy challenges in the smart grid," Security & Privacy, IEEE, vol.7, issue.3, pp 75-77, June. 2009.

[25] Il-Kweon Yang, Seung0Hwan Choi and Sang-Ho Lee, "An Efficient AMI Simulator Design adapted in Smart Grid," Journal of Korean Institute of Electrical Engineers, Vol. 62, No. 10, pp. 1368-1375, Oct. 2013.

[26] J.J. Lee, "The Structure of AMI," Information and Communications Magazine, Vol. 27, No. 11, pp. 17-22, Apr. 2010.
[27] Pierluigi Siano, "Demand Response and smart grids: A survey," Renewable and Sustainable Energy Reviews 30 (2014), pp. 461-478, Jan. 2014.
[28] Albadi, M. H., and E. F. El-Saadany, "Demand response in electricity markets: An overview," 2007 IEEE Power Engineering Society General Meeting, 2007.
[29] Jeong-Hoon Yi and Dae-Woo Park,"A study of Security Issues and Security Technology Policy ofr Smart Grid Infrastructures," the 2010 Korean Institute of Electrical Engineers Spring Conference, pp. 75-77, Apr. 2010.
[30] Do-Eun Oh, Sin-Jae Kang, Young-il Kim and Seung-Hwan Choi,"A Study on Home Area Network Service based on AMI," the 2011 Korean Institute of Electrical Engineers Summer Conference, pp. 1985-1986, June. 2011.
[31] Seok-won Hong, Myeong-ho Lee and Cheol-hwal Lee "Security risks and security requirement in the Korean Smart Grid,"the Korean Institute of Information Scientists and Engineers, Vol. 30, No. 1, Jan. 2012.
[32] Nam-Joon Jung, Il-Kwon Yang. Jae-Ju Song and Seong-Whan Choi,"Specification Analysis for Management of Meter Data based on AMI," the 2010 Korean Institute of Electrical Engineers Summer Conference, pp. 1896-1897, June. 2010.
[33] HyunJoon Moon, "BEMS (Building Energy Management System) recent trend of research," The Magazine of the Society of Air-Conditioning and Refrigerating Engineers of Korea, vol. 42, no. 9, pp. 54-63, Sep. 2013.
[34] JiPyo Hong, GaYoung Cho, SunWoo Lee, MyoungSouk Yoe and KwangWoo Kim, "A Study on Application Status and Improvement Direction of the Building Energy Management Systems (BEMS) in Korea," Korean Institute of Architectural Sustainable Environments and Building Systems Fall 2008 Conference, pp. 194-197, Oct. 2008.
[35] Si-O Seo, Seung-Young Baek, Doyeop Keum, Seungwan Tyu and Choong-Ho Cho "A Tutorial: Information and Communications-based Intelligent Building Energy Monitoring and Efficient Systems," KSII Transactions on Internet and Information Systems, vol. 7, no. 11, Nov. 2013.
[36] Kyo-il Jung, Han-nah Park, Boo-Keum Jung, Jong-soo Jang and Myeong-Ae Jung,"Smart Grid's Stability and Security Issues," the Korean Institute of Information Security and Cryptology, Vol. 22, No. 5, pp. 54-61, Aug. 2012.
[37] Nicolas Falliere, Liam O. Murchu and Eric Chien,"W32. Stuxnet Dossier," Symantec Security Response, Version. 1.4, Feb. 2011.
[38] Nauman Zafar, Edin Arnautovic, Ali Diabat and Davor Svetinovic,"System Security Requirements Analysis: A Smart Grid Case Study," Systems Engineering, Vol. 17, No. 1, pp. 77-88, Mar. 2014.

약 력

2014년 성균관 국정관리 대학원 석사
2013년~2014년 LG 화학연구소 근무
2012년~현재 kt 융합기술원 근무
관심분야: 스마트그리드, 네트워크 보안, R&D 융합

유 성 민

2003년 광주대 법학 학사
1990년~현재 kt 융합기술원 근무
관심분야: 스마트그리드, 네트워크 보안, R&D 융합

김 남 균

1989년 경북대 컴퓨터전자공학 석사
1989년~현재 kt 융합기술원 근무 (팀장)
관심분야: 스마트그리드, BEMS,네트워크 보안, R&D 융합

김 윤 기