# 스마트그리드(Smart Grid) 전력망과 정보통신망 융합 보안 방향

서우석* · 전문석**

# A Direction of Convergence and Security of Smart Grid and Information Communication Network

Woo-seok Seo* · Moon-seog Jun**

요 약

본 논문은 스마트그리드 전력망과 정보통신망의 이원화된 별도의 망을 하나의 통신체제로 재구성하고 스마트그리드 융합 정보통신망을 구현하기 위한 보안 방향과 향후 사이버 공격으로부터 방어를 위한 네트워크를 3단계 주요 핵심 망으로 재구성 및 기존 정보통신망 구성 계층인 TCP/IP Layer 4계층과 전력망과의 계층적 분리를 통한 방어 방향을 제안하고 있다. 또한 현재 스마트그리드 전력망의 문제점과 취약성 그리고 3가지 보안 모델을 제안함으로써 연구와 실험을 위한 기반을 제안하고 있다. 미래지향적인 전력산업의 한 기술로써 발전 방향과 현황을 제시하고 본 논문을 통하여 TCP/IP Layer별 공격과 방어를 전력망과 융합하고 새로운 스마트그리드 전력통신망 기술과 시장의 발전방향 및 스마트그리드 향후 정보보안 과제를 알아보는데 의의가 있다.

ABSTRACT

This Study suggests security directions to reconstruct separate network of Smart Grid and information communication network as one communications system and implement Smart Grid integrated information communication network. In addition, it suggests prevention directions to prevent future cyber attacks by reorganizing network as the key three-stage network and separating TCP/IP four layers that consist of existing information communication network from Smart Grid. Moreover, it suggests the foundation for the study and the test by providing current problems of Smart Grid, weak points, and three security models. This study is meaningful to suggest development directions and situations as a technology of future-oriented electric industries, integrate attacks and preventions of TCP/IP Layers with Smart Grid, and seek for a new technology of Smart Grid and future tasks for Smart Grid information security.

키워드

TCP/IP Layer, Security, Policy, Smart Grid Device, Smart Grid Network, Concentration Center

* 숭실대학교 일반대학원 컴퓨터학과 (ssws2003@yahoo.co.kr)
** 교신저자 : 숭실대학교 일반대학원 컴퓨터학과(mjun@ssu.ac.kr)
접수일자 : 2010. 09. 01 심사(수정)일자 : 2010. 10. 01 게재확정일자 : 2010. 10. 15

## Ⅰ. 서 론

21세기 정보화 사회의 가장 큰 사회적 이슈인 전력 자원에 대한 효율적인 관리와 사용은 정보통신 정보 기술과 융합되어 전력 공급 및 수급을 위한 양방향성 그리고 중앙관제를 통한 적절하고 효율적인 전력 에너지 자원의 소비 효율 최적화를 구현하게 되었다. 또한, 전력망과 기존의 통신망 융합은 또 다른 정보화 사회의 한 기술로써 자리를 잡아가고 있으나, 통신망 기반에 존재하는 다양하고 치명적인 정보유출과 변조 등 많은 정보보호 문제점을 전력망에서도 공격을 방지하고 대응하기 위한 기술이 요구되어 졌으며, 전력망과 통신망을 융합하여 망을 구현함에 따라 개인의 프라이버시 정보 및 전력 통제 정보 등과 같은 주요 정보를 대상으로 하는 사이버공격을 통한 접근과 통제가 필요하게 되었다[1].

최근 다양한 보안에 대한 이슈와 새로운 공격기법에 의한 침해 사례가 다변화되고 단순히 차단 및 확인 등의 학습을 통해 정보를 데이터베이스화 하는 보안 시스템으로는 적극적이고 공격성이 강한 침해를 방어하기가 힘들어 짐에 따라 보안 시스템의 통합과 정책 다양화와 변화가 급격하게 이루어지고 있다. 이는 방어기법의 비약적인 발전과 기능의 다양화 및 최신 고도화된 방어기술에도 불구하고 종합적인 접근과 침해에 대한 종합 관제가 이루어지지 않고 있기 때문이다. 전력망에서 전력 효율화를 위해 제시되어진 디지털 전력 센서, 디지털 스마트 미터기, 분산전원 시스템, AMI(Advanced Metering Infrastructure)시스템, 종합 전력 제어시스템 역시 공중망에 노출되어진 통신망을 통해서 정보가 생성, 가공, 저장, 보존 등이 이루어지기 때문에 정보통신망에서 공격의 대상이 되는 정보와 동일하게 취약점을 갖는다[2][3].

따라서 본 논문에서는 정보통신망에서 보안 침해가 가능한 공격 등을 확인하고 스마트그리드를 통해 생성되어진 정보에 대한 공격기법과 현황 그리고 향후 취약점 개선을 위한 정보보호 기술에 대하여 알아보고자 한다. 본 논문의 구성은 다음과 같다. 2장에서는 스마트그리드 취약성 및 침해 가능 공격분석을 통해서 문제를 제시하고, 3장에서는 스마트그리드 정보 보안을 위한 기술현황이 기술되고, 4장에서는 전력망에서 스마트그리드 보안모델과 향후 정보보안 과제를 알아본다.

## Ⅱ. 관련연구

### 2.1. 개요

스마트그리드는 전력망을 기반으로 정보통신망 이용 기술과 다양한 솔루션을 적용하여, 전력 효율성을 극대화함으로써 전력 공급과 소비의 균형을 유지하는 기술이다. 또한, 융합된 기술을 통해 전력시장에서 전력공급자와 소비자가 양방향으로 전력관리와 운영으로 생성되어진 정보를 실시간으로 교환함으로써 에너지효율 최적화가 가능하도록 하는 차세대 전력망이다. 그 활용분야로는 녹색에너지 마이크로그리드, 송전망 이용 효율화를 위한 FACTS(Flexible AC Transmission System) 유연송전시스템, 글로벌 지역연계를 위한 HVDC(High Voltage Direct Current) 직류송전 시스템, 소비자 또는 전력망 사용자에게 다양한 품질 전력 공급 시스템, AMI(Advanced Metering Infrastructure) 기기와 그린 IT 기술과도 융화되어진 녹색성장을 위한 DC 직류전력공급 그리고 ASM(Advanced Smart Meter), 전기자동차 등과 같이 그 기술 활용분야는 매우 폭넓게 개발되어지고 있다[4][5].

또한, 해외의 스마트그리드의 경우도 전력망이라는 기술부문과 정책적인 방향이 결합되어 스마트그리드 분야의 활용도를 극대화하고 있다. 해외에서 스마트그리드 현황의 경우 미국은 GRID2030 계획을 수립하고 전력망을 백본, 중간본, 미세본으로 구성 및 구분해서 전력망에 인공지능 기술까지 융합하는 기술 및 정책 방향으로 진보하고 있으며, 원격검침 및 시간대별 전력요금 산정을 위한 전자식 전력량계 보급, 500KV급 초고압 송전로 증설 계획 등 다양한 방법을 도입하고 있다. 캐나다 및 유럽의 국가들도 스마트미터기 교체와 OPERA(Open PLC European Research Alliance) 프로젝트 등 빠르게 스마트그리드를 도입하고 생활에 적용하고 있다[6].

표 1과 같이 전력망의 특성이 IT와 접목된 스마트그리드는 다양한 변화와 분야에서 활용되어지고 있으나, 정보전송 라인인 전력망의 경우 기존 정보통신망을 활용 또는 일부 기술을 융합함으로써 정보를 생성, 관리하는 부문에서 정보통신망에서 발생 가능한 사이버 공격과 방어가 또 다른 이슈로 붉어지고 있다. 따라서 전력망에서 발생 가능한 정보보안상의 취약성과 공격 그리고 방어에 대해서 학술적인 부분에서 연구

되어져야 한다.

표 1. 전력망 .vs. 스마트그리드
Table 1. Grid .vs. Smart Grid

| 구분 | 전력망 | 스마트그리드 |
|---|---|---|
| 통신방향 | 단방향 | 양방향 |
| 전원방식 | 중앙집중[수직적] | 분산[수평적] |
| 구현구조 | 방사형 | 망[네트워크] |
| 전력흐름 | 단방향 | 양방향 |
| 구현기술 | 아날로그 | 디지털 |
| 설비운영 | 전력공급자 중심 | 공급자+수요자 |
| 리스크관리 | 수동 | 자동 |

## 2.2. 취약성

정보통신망과 유사한 전력 정보 생성과 전송을 하는 전력망의 경우 정보통신망이 기존에 가지고 있는 시스템 소프트웨어 또는 응용소프트웨어와 같은 소프트웨어적인 부분과 네트워크 및 데이터베이스, 하드웨어적인 부분에 이르기까지 취약성을 갖는다. 이는 전력망에서 생성되어진 정보가 정보통신망과의 융합 접점을 거쳐 상호 유기적인 정보의 흐름이 발생함에 따라 정보통신망과 전력망에서 취약점을 상호 비교 분석하는 부분이 필요하다. 망에 따른 취약점은 표 2와 같이 분류할 수 있다.

표 2. 정보통신망과 전력망의 취약점 분석
Table 2. Analysis on Weak Points of Information Communication Network and Smart Grid

| 구분 | 분류 | 통신망 취약점 | 세부 공격 유형(기법) |
|---|---|---|---|
| Hardware Control | Firmware | RAM(Random Access Memory), frequency | |
| | Malware | malicious software, malicious code | |
| Sofrware Control | Network | DoS[DDoS]<br>Sniffing<br>poofing<br>Hijacking (session) | Ping of Death<br>Syn Flooding Attack<br>Tear Drop Attack<br>Smurf Attack / Fraggle Attack<br>LAND Attack<br>Window, TCP/IP L2 base Attack / SARP, IP, DNS<br>Air Signal Sniffing, MAC Spoofing, WEP Crack, Session Hijacking & Man In the Middle Attack, Fake Access Point, Dos(Denial of Service) |
| | System | 계정과 패스워드 관리, 세션 관리, 접근제어, 권한 관리, 로그, 취약점 관리 | |

전력망 구현을 위한 정보흐름 경로에 따른 영역별 구성영역은 그림 1과 같이 총 3단계의 SGD(Smart Grid Device), SGN(Smart Grid Network), CC(Concentration Center)로 구성되어 진다. 영역 구분을 위한 기준은 실제 구현 프로세스별로 구분한 것이며, 따라서 3가지 주요 핵심 공격 가능 네트워크 영역을 대상으로 취약성과 방어기법 그리고 일반적인 현황을 연구한다[7][8][9].

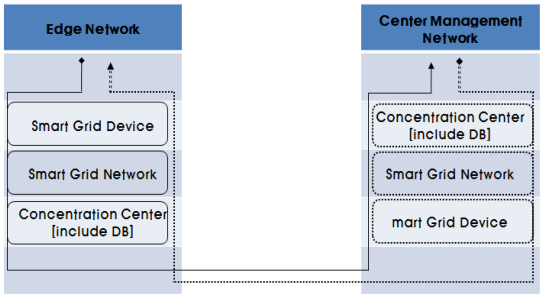


그림 1. 구성영역과 정보 흐름
Fig. 1 Configuration and Information Flow

### 2.2.1. SGD(Smart Grid Device)

전력망에 이용되어지는 Device의 경우는 세계적으로 공격대상으로 가장 많이 이용되어지고 있으며, 공격으로 인한 이슈가 되고 있는 스마트계량기의 램, 디지털 주파수, 멀웨어 그리고 팜웨어를 중심으로 공격이 이루어진다. 우선 스마트디바이스 중 특화되어진 Smart Edge Home Network에서 개인의 전력 사용량과 그 외의 다양한 전력정보를 CC(Concentration Center)를 거쳐 최종 전력정보 취합 및 관리와 운영을 위한 Center Management Network로 보내는 정보통신망에서 게이트웨이와 같은 역할 또는 Edge 네트워크 단말 장치인 스마트 계량기는 최근 세계적인 공격 추세가 램 공격으로 최종 공격의 형태가 나타난다. 이는 제3의 공격자가 해당 기기의 램을 직접 공격함으로써 계량기를 통해 생성되는 정보를 분석하고 분석되어진 정보를 기반으로 계량기를 인위적으로 조작함으로써 보안의 3요소인 기밀성, 무결성, 가용성 중 무결성을 침해한다. 또한, 정보통신망의 가장 핵심적인 기술로 진화되어진 무선통신 부문에서는 무선 주파수단에 주파수 교란을 통한 전력 정보의 차단, 계량기에 탑재되어진 관리 소프트웨어를 공격하는 멀웨어 바이러스나 트로이 목마와 같이 시스템에 해를 입히거나 시스템을 방해하기 위해 특별히 설계된 소프트웨어, 또는 데이터·컴퓨터·네트워크를 위험에 노출시킬 수 있는 코드 공격이 이루어진다[13]. Smart Sensor, RELAY, CAP BANK/E - BRIDGE, SWITCH/S - BRIDGE, 통합제어 센터 시스템에 대한 팜웨어 공격

이 존재한다. 그림 2에서는 Smart Grid Device의 전체적인 개요도를 나타낸다.

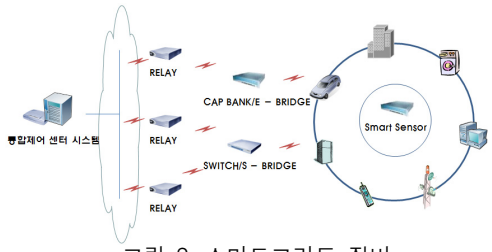


그림 2. 스마트그리드 장비
Fig. 2 Smart Grid Device

### 2.2.2. SGN(Smart Grid Network)

최초 전력망에서 개인의 전력정보를 생성하는 Smart Grid Sensor로부터 Smart Grid Device를 거쳐 최종 Concentration Center(CC)에 정보를 취합하기 위해 정보의 전송로는 Access Point, Ethernet, Code Division Multiple Access(CDMA), Group Special Mobile(GSM) 등을 이용하며, 그림 3은 Smart Grid의 정보 생성부터 최종 취합까지의 네트워크 연계도 및 구성을 나타낸다.

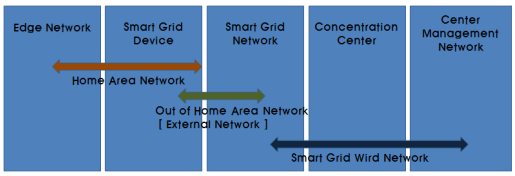


그림 3. 스마트그리드 네트워크
Fig. 3 Smart Grid Network

Edge 네트워크의 Smart Sensor가 취합한 전력정보를 전력망과 정보통신망이 융합되어 구성된 네트워크망을 통해서 단위 네트워크 형태의 Ethernet 또는 그 이상의 정보 전송 경로인 CDMA, AP, GSM, BPL, WiFi, WiMax, PLC, RFID 등을 통해서 Concentration Center에 취합되어진다[14]. 또한, 역 경로 역시 동일한 방식으로 구성되어지며, 정보통신망이 융합되어 있는 네트워크로써 보안부문에서 제3자가 가장 많은 공격을 감행하는 공격의 주된 대상이 된다. DoS, DDoS, Sniffing, Spoofing, Hijacking(session)이 공격 방법으로 제시된다. 이는 정보통신망이 가지고 있던 보안의 문제점을 전력망 또한 포함하고 있다는 결과로 별도의 전력망을 구성하지 않은 상태에서 기존의 정보통신 인프라를 융합, 활용함으로써 발생하는 보안 문제점이다. 따라서 보안부문에 대한 공격기법과 방어기법에 대한 현황제시와 향후 문제점 구분을 Home Area Network(HAN), Out of Home Area Network(External Network), Smart Grid Wird Network)으로 공격기법과 방어에 대한 방법을 제시한다.

### 2.2.3. CC(Concentration Center) - include DB

최종 Edge 네트워크에서 생성된 정보와 중앙에서 생성한 정보가 상호 공존하는 시스템을 구현한다. 정보의 중앙 집중화를 통해서 전체 전력망 관리 및 운영 그리고 생성된 데이터베이스를 학습하고 전력 사용량 등과 같은 개인의 정보를 기반으로 과금을 하는 등의 최종 리포팅과 모니터링을 한다.

자료의 운영과 전산환경의 세대별 구분으로 분석한다면, 과거 중앙 집중형의 관리에서는 정보와 자료 그리고 환경이 모두 성능이 우수하고 관리의 책임이 중앙에 있기를 원한 소비자의 요구사항과 클라이언트 전산장비가 서버에 비해 환경이 열악한 점이 중앙 집중화를 이끌어 냈으나, 이후 클라이언트들의 전산환경이 저가에 고속의 장비를 활용 가능한 시장 상황으로 변경됨으로 인해 다양한 콘텐츠와 서비스를 클라이언트에서 생성 또는 운영을 했다. 하지만 전력망인 Smart Grid의 경우는 중앙에서 전력망을 관리하고 특화되어진 서비스인 전력에 대한 소비자의 관리, 운영이 불가능함으로 그림 4와 같이 3세대 형태의 중앙으로 집중하는 형태를 요구한다. 따라서 제3자의 불법적인 접근의 가장 큰 최종 공격 대상이기도 하다.

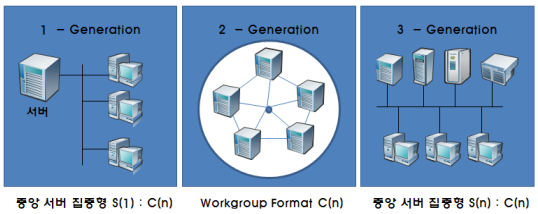


그림 4. 세대별 전산환경의 방향과 변화
Fig. 4 Directions of Computation Environment by Generations and the Changes

### 2.3. 침해 가능 공격분석4

스마트 계량기, 센서, 고도화된 통신네트워크와 전

력망에서 운용되면서, 정보보안, 네트워크 보호 등에 관한 다양한 리스크가 표 3과 같은 공격유형에 따라 높아지고 있다. 이러한 보안에 대한 위험요소들은 Edge Network으로부터 Center Management Network까지 취약성이 나타나고 기존 정보통신망, 전력망, 전력시스템 및 신규 구현 시스템 간 호환성과 상호 정보운용에 비약적인 기술 진보가 이루어지지 않고 또한 서로 다른 기반의 기술을 융합함으로써 취약점이 외부의 물리적, 사이버 공격으로 인해 전력망 손실 등이 더욱 크게 부각된다.

철저한 스마트그리드 운영을 위한 보안체계가 구축되어야 함에도 현재까지는 스마트 그리드에 대한 관심과 구현에 있어서 정보보안에 대한 기술 도입 및 구축 이전으로 치명적인 장애에 대한 유추만이 가능하다. 스마트그리드의 정의에 맞는 구현과 운영을 위한 구축이 필요하지만, 보안이 접목되어지지 않는 기술은 정보통신망과 전력망의 융합에 의한 불안정한 정보보호로 기술에 큰 문제점을 야기한다.

표 3. 공격유형
Table 3. Pattern for attack

| 구분 | 공격 유형 |
|---|---|
| 공격방법 | Remote Finger Printing / IP Scanner / Port Scanner / Third Party Effect |
| | Trinoo Attack / TNF Attack / Stacheldraht Attack / TFN2K Attack |
| | Remote Active Attack / Etc |
| | IP / E-mail / Web / ARP / DNS |
| | Syn Flooding Attack / Smurf Attack / UDP Flooding / Brute-Force Attack / Land Attack / Teardrop / Targa / NewTear / Nestea / Ping of Death / Inconsistent Fragmentation |
| | Hub Attack / Switch Jamming / ARP Redirect / ICMP Redirect / ICMP Router Advertisement |

## III. 스마트그리드 정보보안을 위한 기술현황

### 3.1. 보안 기술방향과 세부공격 및 방어 기법

스마트그리드 보안과정은 제시되어진 보안모델인 정보통신과 전력망 융합 보안, 클라우드 컴퓨팅(Cloud Computing)과 전력망 융합 보안, 인증을 통한 전력망 융합 보안의 3가지 제안방법 중 그림 5와 같이 기존에 구축되어 운영되어지고 있는 정보통신망과의 융합을 기반으로 하는 보안과정을 활용하고 기존에 존재하는 다양한 제3의 사이버 공격에 대한 공격기법과 방어기법이 공개되어진 기술을 활용한다[10][11].

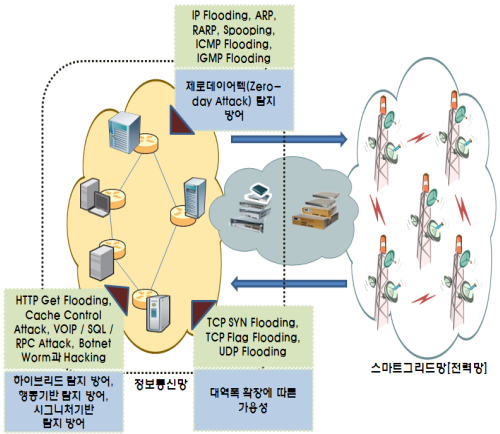


그림 5. 정보통신과 전력망 융합 네트워크
Fig. 5 Information & Communication and Smart Grid integrated Network

### 3.2. 국내외 스마트그리드 보안정책과 운영현황

스마트그리드에 관한 국가적 차원의 기술 도입과 구축 및 운영을 위한 방안이 정책적으로 국내뿐만 아니라 미국, 영국, 캐나다, 유럽, 일본 등에서 수많은 정책과 방향 등을 제시하고 이를 구현하기 위한 기술과 인력들을 확보하는데 주력을 다하고 있으나, 최근 가장 큰 문제점으로 이슈가 되어 지고 정보통신망과의 융합을 통한 기반 하에서 기존 사이버보안 문제점이 스마트그리드 구현을 위한 네트워크 망에서도 문제가 되는 것을 확인했다. 또한 공격의 대상이 되는 스마트그리드 기술의 향후 발전방향과 보안 분야에 대한 확실한 대처기법 제시가 중요시 되어졌다. 따라서 표 4와 같이 전력망 보안문제점과 정보통신망 보안문제점을 다각도로 분석하고 각 국가 간 상호 스마트그리드 개발과 구현을 위한 보안정책 방향들이 제시되고 있다[12].

표 4. 국내외 스마트그리드 보안정책 방향
Table 4. Directions for Domestic and Overseas Smart Grid Security Policies

| 구분 | 국가명 | 보안현황 |
|---|---|---|
| 국내 | 대한민국 | - 스마트미터 자체 취약성 보완 : 보안 Chip나 바이러스 연구<br>- 통신구간 : 생성 및 전송 정보의 암호화<br>- 상호 Edge 네트워크 및 CC와의 인증 및 로그관리 [예 : VPN]<br>- 중앙 통합 보안관리체계 구축<br>- 생성 및 관리되는 대량의 데이터관리 |
| 국외 | 미국 | - 취약점 클래스 개발(development of vulnerability classes)<br>- 보안 문제 세부 분류(구분), 보안 선택과 개발을 6개의 기능 우선 영역으로 분류<br>- 인터페이스 식별과 매석(identification and analysis of interfaces)<br>* 2009년 9월25일 미국 NIST는 "스마트그리드 사이버 보안 전략과 요구사항 (Smart Grid Cyber Security Strategy and Requirements)" 이라는 NIST IR 7628이라는 초안(Draft)을 발표 및 2010년 2차 발표 |
| | 유럽 | - 스마트그리드 비전 및 향후 연구개발 전략 : 5개 연구부분, 19개 세부과제 선정<br>. "운영, 복구, 방어 계획을 위한 아키텍처와 도구"<br>. 스마트그리드 장애 및 외부 공격 대응 방안<br>. 송, 배전 시스템의 사이버보안 및 복구 능력 향상 방법론 |

## IV. 스마트그리드 향후 정보보안 과제와 보안모델

### 4.1. 보안모델

#### 4.1.1. 정보통신과 전력망 융합 보안

기존에 존재하고 이미 운영되어지고 있는 정보통신망을 기준으로 공격방법과 방어기법 등을 소개한다. 즉, 스마트그리드의 전력망이 정보통신망과 융합되어짐에 따라 정보통신망에서 존재하는 모든 보안문제점이 전력망에도 이전되어 있다는 전제를 한 것이다. 표 5는 정보통신망의 TCP/IP Layer 4계층을 전력망의 네트워크와 비교하고 공격기법과 방어기법의 현황을 도식화한 것이다.

표 5. 정보통신과 전력망 융합 보안 현황
Table 5. Information & Communication and Smart Grid integrated Security Situations

| 분류 | 구성 | 정보통신 & 전력망 [TCP/IP Layer] | 공격기법 | 방어기법 |
|---|---|---|---|---|
| Edge Network | 정보통신망 + 전력망 | Application | HTTP Get Flooding, Cache Control Attack, VOIP / SQL / RPC Attack, Botnet Worm 과 Hacking | 하이브리드 탐지 방어, 행동기반 탐지 방어, 시그니처기반 탐지 방어 |
| Path Network | | Transport Internet | TCP SYN Flooding, TCP Flag Flooding, UDP Flooding | 대역폭 확장에 따른 가용성 |
| Center Network | | Network | IP Flooding, ARP, RARP, Spooping, ICMP Flooding, IGMP Flooding | 제로데이어택(Zero-day Attack) 탐지 방어 |

스마트그리드의 네트워크를 크게 Edge, Path, Center Network로 구분하고 이를 정보통신망의 TCP/IP Layer 4계층에 대칭시켜 기존에 존재하는 방어기법과 공격기법을 나타냈다. 모든 보안을 위한 카테고리는 목적과 쓰임에 따라 기술의 적용이 가능하지만 스마트그리드의 경우는 정보통신을 기반으로 구현하는 기술로써 기존의 문제점을 해결하고 스마트그리드만의 보안 문제점 방향과 과제를 이끌어 내야 한다. 따라서 정보통신망의 TCP/IP Layer 4계층을 통해 최종 CC로 정보가 집결됨을 착안하여, 기존 정보통신 Layer별 공격과 방어기법을 전력망과 계층별 대칭을 통한 기존 방어기법을 우선 적용 후 지속적인 학습데이터에 따라 방어기법을 적용한다. 방어기법으로는 IDS(Intrusion Detection System), IPS(Intrusion Prevention System), VPN(Virtual private network), ESM(Enterprise Security Management) 등과 같은 정보통신망에서 운영 중인 방어 시스템을 기반 솔루션으로 적용한다. 전력망 생성 정보 또는 통신망 생성 정보 역시 최종 CC로 집결을 위해서는 반드시 기존의 정보통신망 방어기법을 활용함에 착안하여, 기존 정보통신망 기술을 활용한다[13][14][15].

#### 4.1.2. 클라우드 컴퓨팅(Cloud Computing)과 전력망 융합 보안

다양한 IT분야에 대한 비용절감을 목적으로 스트리밍 콘텐츠, 웹자원, 전산장비의 리소스 등을 하나의 IT인프라 내에 구현함으로써 많은 IT 자원에 대한 운영과 관리 부문의 비용절감을 유도하는 것이 클라우드 컴퓨팅이다. 클라우드 컴퓨팅의 주요 특징을 전력망과 융합함으로써 보안부분과 녹색성장을 위한 기반을 구현한다. 그림 6은 정보통신망 내 클라우드 구현과 전력망과의 연결을 나타낸다. 클라우드 컴퓨팅의 특징으로는 서버, 스토리지, 운영체제와 관련 리소스에 대한 가상화 기술을 통해 물리적인 시스템 통합, 파일시스템의 무제한적인 용량과 다양한 파일시스템 운영 방식 그리고 온라인 무결성 검사와 복구, 구조적, 비구조적 데이터 처리 기능 등이 있다. 따라서 다양하고 가상적인 물리 자원 통합으로 전력망과 정보통신망과의 융합에 적용함으로써 다차원의 보안 기법과 방어기법을 1차원적으로 방어가 가능하고 또한 제2, 제3의 순차적이거나 반복적인 공격이 발

생해도 종합적으로 구현되어진 물리적 시스템을 연동함에 따라 방어가 가능하다. 다만, 클라우드 컴퓨팅의 발전 방향을 정보통신망 기반에서 전력망까지 포함하는 수준으로 폭을 넓혀야 하는 기술적인 문제점이 있다.

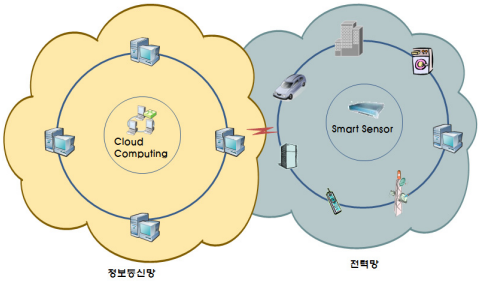


그림 6. 클라우드 컴퓨팅
Fig. 6 Cloud Computing

또한, 가상의 ESM 방어 시스템을 구현함으로써 침입자의 공격이 ESM의 종합보안통제권 내에서 보안 조치되고 이후 클라우딩을 적용하는 단계적 방어 시스템 적용이 다소 과거의 방어 기술임에는 틀림없지만, 전력망과의 통합 이후 발생할 보안 문제점을 정보통신망에서 발생했던 보안 침해로 판단 순차적인 기술적용이 필요하다.

#### 4.1.3. 인증을 통한 전력망 융합 보안

Smart Sensor가 위치한 Smart Home인 Edge Network에 중앙의 전력 관리 시스템과 제3자의 불법적인 접근과 생성된 전력정보의 위조와 변조를 차단하고자 상호 인식 가능한 인증을 사용한다. 스마트그리드 Edge단의 클라이언트(전력 사용자) 인증서를 CC단의 서버가 요구함으로써 서버의 보안을 높일 수 있다. 또한, 상용 CA(인증기관) 또는 스마트그리드 전력정보통신망 내 별도의 관리와 운영을 위한 내부 CA에서 클라이언트 인증서를 관리 및 발급함에 따라 제3자의 접근을 차단한다. 장비와 장비간의 정보에 별도의 공인인증과 같은 상호 암호화와 복호화 과정을 통해서 정보의 무결성을 보장하거나 또는 정보통신망 기준인 정보보호 보증 등급을 전력망의 장비에도 적용함으로써 전력망과 정보통신망의 융합되어진 망에서도 동일한 정보보호의 솔루션이 적용될 수 있도록 해야 한다. 또한, 스마트그리드 네트워크에서 전력망 쪽의 클라이언트와 중앙서버와의 인증 문제에 있어서 실시간 그리고 신속한 정보의 인증이 필요함에 따라 향후 인증절차 및 인증방법에 대한 개선 없이는 현재 운영되어지는 인증방법으로는 전력망과 통신망의 조화로운 인증체계를 구성 할 수 없다. 인증과 관련된 솔루션이 보다 전력망과 통신망의 이원화된 네트워크 구성에 맞게끔 개선되어짐이 중요한 과제이며, 또 한편으로는 표 6과 같이 장비에 대한 인증 솔루션의 등급 체계도 일부 새로운 등급체계로의 변화를 모색해야 한다.

표 6. 정보보안 제품에 따른 보안 등급 분류
Table 6. Division of Security Levels according to Information Security Products

| 구분 | 프로파일 | 보안등급 | 평가기준 | 적용방향 |
|---|---|---|---|---|
| 시스템 | 침입차단 시스템 | EAL4 | CC 3.1 | 전력망 보안 제품과 정보통신망 구현 장비의 보안 등급 및 기준에 표준화가 이루어져야 함 |
| | 침입탐지 시스템 | EAL3 | CC 3.1 | |
| 시스템 및 네트워크 | 등급기반접근통제 | EAL3 | CC 3.1 | |
| | 개방형 스마트카드 | EAL4+ | CC 3.1 | |
| | 지문인식 | EAL2 | CC 3.1 | |
| 네트워크 | 가상 사설망 | EAL3 | CC 3.1 | |
| | 스팸차단 | EAL2 | CC 3.1 | |
| | 침입차단 시스템 | EAL3 | CC 3.1 | |

### 4.2. 향후 정보보안 과제

#### 4.2.1. 보안 기반 확충

스마트그리드 기술과 방향은 수많은 인력과 장비로써 제안되어지고 있고 현실 속에서 구축되어 운영되고 있다. 또한, 많은 국가들이 서로 새로운 기술에 대한 선점을 위해 다소 무리한 물리적인 확장을 우선시하는 과오를 범하고 있다. 즉, Edge Network로부터 생성된 전력정보를 중앙 집중 시스템으로 전송하고 이를 기준으로 전력사용량에 정보를 관리 및 운영하는데 사용된다. 그러나 난무하고 있는 다양한 기술의 가장 중요한 부문은 보안에 대한 기반을 확충하고 공격기법과 방어기법에 대한 누적된 정보를 생성함으로써 사이버 공격으로 인한 문제점을 사전에 인지하고 이를 기반으로 기술을 확보하고 개발되어져야 한다.

많은 전력망 기반의 기기들은 정보통신망과 융합되어지는 기술인 스마트그리드를 선호하고 앞 다투어 새로운 기술방법을 제시하고 있으나, 정보통신망에서의 침해와 침입에 대한 솔루션은 정확하게 제안되고 제시되어 지는 바가 없다. 따라서 표 7에서는 정보보

안을 위한 가장 기본적이면서도 스마트그리드를 구축함에 있어 잊기 쉬운 보안상의 문제점을 인식하고 전력망을 기준으로 하는 과도한 발전을 지양하고 정보통신망과의 융합으로 발생 가능한 보안상의 문제점을 제시 및 기술적인 방법을 우선시 하기위해 향후 정보보안의 과제를 짚어봤다.

표 7. 정보보안 과제
Table 7. Tasks for Information Security

| 구분 | 보안과제 | 특이사항 |
|---|---|---|
| 취약점 | - 이용자 인증 취약점 보안 및 개선 | 스마트그리드 구성망에서 3개의 네트워크 연결 고리간의 취약점 발생 가능 부분에 대한 보안 등, 필수 보안 요소인 물리적 제반사항의 보안 강화 |
| | - 전력 인증 취약점 보안 및 개선 | |
| | - 유무선 환경 보안 취약점 개선 및 보완 | |
| | - 주요 개인정보 취합을 위한 필터링 기술 개선 | |
| | - 무선랜 보안 기술 강화 | |
| | - 스마트그리드 구성 기기의 기기별 자체 보안 기술 개선 | |
| | - VPN 등의 암호화 통신 라인의 구축과 개선 | |
| 법제 | - 스마트그리드 관련 법 제정 및 시행 | |

#### 4.2.2. 보안 인력 확충

정보통신과 전력 부문의 전문 인력들이 각 분야별로 분리되어 있는 문제점을 해소함으로써 스마트그리드 통합전력통신망에 대한 보안을 위한 관리 및 운영의 타당성과 향후 보안과제를 해소할 수 있다.

물론 각 분야별로 흩어져 있는 전문 인력들을 타 분야에 대한 교육과 기술습득을 통해 보안과제에 대한 문제점 해소가 가능 하지만 정보통신과 전력망 인력구성 자체를 일원화함으로써 각기 전문 기술 분야에 대한 기술능력을 보장하는 형태인 그림 7과 같은 조직이 통합전력통신망 보안과제를 해소하는데 가장 효율적인 방안이다.

즉, 프로젝트를 관리하는 부문에서 인용되어진 조직관리 방법으로는 매트릭스와 프로젝트 방법을 유기적으로 운영함으로써 적절한 전문 인력 배치와 보안 단계별 프로세스를 프로젝트 단위로 분리 및 구성하고 각 단계마다 침해기법과 방어기법 등을 분리 구성과 학습을 통해 정확하고 빠른 침해 데이터베이스를 보유할 수 있다. 또한, 최종 단계별 조직구조에서 얻어낸 각 종 기법들을 융합보안 학습 정보를 구성함으로써 각 종 침해로부터 적절한 방어절차와 형태에 대한 정의를 할 수 있다.

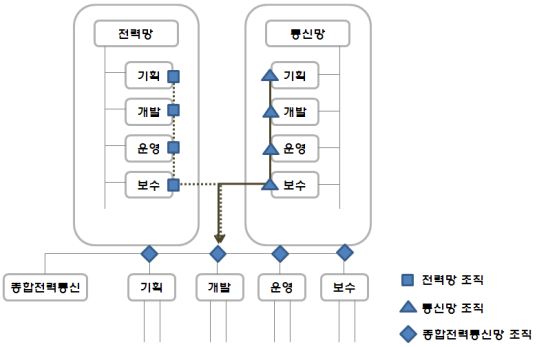


그림 7. 종합전력통신 조직형태
Fig. 7 Organization Type of Integrated Electric Communications

### 4.3. 스마트그리드 정보 보안 특성을 고려한 세분화된 정보 보안 모델 연구

스마트그리드 정보보안은 하나의 융합된 망에서 발생하는 사이버 공격에 대한 방어와 차단 기술의 습득과 구현은 아니다. 엄밀히 말하면, 정보통신 솔루션과 전력 관리 솔루션이라는 2개의 서로 다른 이질적인 기술의 융합으로 어느 하나만을 위한 보안 정책으로는 취약점과 공격에 따른 적절한 방어가 이루어지지 않는다. 따라서 정보통신 분야의 취약점과 공격기법, 방어기법 등을 기존에 학습되어진 데이터베이스를 기반으로 표 8과 같이 정보통신망에 대한 계층을 분리하고 계층별 공격과 방어를 위한 정보통신망의 단면적인 솔루션을 우선 확인해야 한다.

표 8. 정보통신망 특성 계층화 정보 보안
Table 8. Information Security of Characteristics of Information Communication Network by Levels

| 구분 | 정보보호 분야 | 공격과 방어 |
|---|---|---|
| Application | 네트워크, 시스템, 기타 공격 기반 대상 | TCP/IP Layer별 공격의 방법을 분석하고 사전에 공격의 유형과 목적 그리고 최종 결과를 유추할 수 있는 알고리즘을 구현 기존 방어방법으로 전력망과의 융합 이전에 솔루션을 제안 |
| Transport | | |
| Network | | |
| Physical, Datalink | | |

이후 스마트그리드의 성격과 목적에 준하는 전력부문의 기술을 정보통신과 융합하기 위해 2단계로 전력

기술에 대한 공격가능 취약점, 물리적 접근 가능경로, 공격에 따른 결과 등의 다양한 방법론과 솔루션을 표 9와 같이 제안하고 이 두 가지의 서로 다른 기술을 정보보호 기반의 융합으로 스마트그리드를 설계하고 구현되어야 한다.

표 9. 전력망 특성 계층화 정보 보안
Table 9. Information Security of Characteristics of Smart Grid by Levels

| 구분 | 정보보호 분야 | 공격과 방어 |
|---|---|---|
| Edge<br>Path<br>Center | 전력망의 경우는 특화된 사업으로 논리적인 접근을 통한 사이버 공격의 한계가 있어 물리적인 공격 대상 | 스마트그리드 구현을 위한 디바이스를 직접 물리적으로 접근 공격하는 기법이 가장 효과적으로 취약점을 침해하는 방법으로 Edge Network에 존재하고 최종 정보통신망과 연결되기 이전까지에 대한 하드웨어 사항과 제3의 불법 Chip변경등에 대한 솔루션 제안 |

또한, 정보의 형태를 일원화해서 정보통신망과 전력망을 이동하는 정보의 구성형태를 정보통신망의 패킷을 기준으로 전력망에서 통신망으로 전환 시 플래그를 패킷에 추가 구성하는 방법과 통합전력통신망으로 일원화된 정보망을 기준으로 기존의 사이버 공격으로부터 접근이 불가능한 새로운 형태를 구성하는 방법을 제안한다. 또한, 통합전력통신망의 보안모델로 제시되어진 클라우드 컴퓨팅(Cloud Computing)과 전력망 융합 보안, 인증을 통한 전력망 융합 보안의 3차원적인 방법론을 재 융합한 기술의 제시가 시급하다.

## V. 결 론

본 논문에서는 전력망과 정보통신망이 융합되어진 망 전체를 대상으로 기존의 정보통신망에서 발생하던 무수히 많은 사이버 공격이 스마트그리드 구현을 위한 망에서도 새로운 공격 패턴들이 지속적으로 연구되고 만들어지고 있으며, 실제 공격에 의해 피해를 보고 있다.

따라서 사이버 공격으로 발생 가능한 문제점을 사전에 파악함으로써 융합되어진 스마트그리드 전체 망을 3개의 망으로 구분하고 각 망별 공격기법과 방어기법을 확인하고 발생 가능한 경우 또한 확인했으며, 향후 발생 가능한 사이버 공격 패턴을 사전에 학습 가능한 공격으로 사전 분리하여, 미연에 새로운 전력통신망에 대한 보안과제를 해결하는 방향을 제시하였으며, 정보보안을 위한 기반과 인력확충도 과제를 해소하는 각 단계별 요구사항임을 확인했다. 이처럼 학술적인 차원과 향후 도래되어질 정보보안 문제에서 다양한 공격의 형태를 분석하고 보안정책을 적용함으로써 상호 이질적인 망의 연결에 따른 문제점을 해소함에 따라 적절한 보안정책을 적용시킬 수 있고 스마트그리드의 중앙 집중적인 관리를 통한 대응으로 발생가능한 문제점을 해소하는 관리 시스템 확장 연구와 대응모델에 대한 연구가 필요하다.

## 참고 문헌


[1] 이경민, 이정훈, 최형식, 추승우, 김철환, “차세대 친환경 전력시스템 스마트그리드(Smart Grid) -미국의 스마트그리드 프로젝트를 중심으로-,”2007 LG Global Challenger 탐방 결과보고서 요약본, 1-10쪽, 2007년.

[2] 박태진, “똑똑한 전기가 온다, 스마트그리드,”과학의 향기, 81-83쪽, 2009년 11월.

[3] 박찬국, “미국 스마트그리드 시장 현주소와 도전과제,”에너지경제연구원, 2009년 12월 30일.

[4] 홍일선, “미국이 스마트 그리드에 주목하는 이유,”LG Business Insight, 48-54쪽, 2009년 7월.

[5] 이일우, 박완기, 박광로, “스마트 그리드 기술 동향,”정보통신학회지, 제 26권, 제 9호, 24-33쪽, 2009년.

[6] 도윤미, 김선진, 허태욱, 박노성, 김현학, 홍승기, 서정애, 전종암,“스마트 그리드 기술 동향:전력망과 정보통신의 융합기술,”전자통신동향분석, 제 24권, 제 5호, 74-86쪽, 2009년 10월.

[7] 양일권, 정남준, 송재주, 이상호, “스마트 그리드 전개 방법론 연구,”대한전기학회 하계학술대회 논문집, 161-162쪽, 2009년 7월.

[8] 이경복, 독고지은, 유지연, 이숙연, 임종인, "스마트 그리드에서의 소비자 참여와 보안 이슈," 정보보호학회지, 제 19권, 제 4호, 21-35쪽, 2009년 8월.

[9] 김홍래, 문승일, "스마트 그리드(Smart Grid)의 이해," 전기의세계, 제 58권, 제 8호, 22-26쪽, 2009년.

[10] 전용희, "지능형 전력망(Smart Grid)과 정보보호," 정보보호학회지, 제 19권, 제 4호, 65-71쪽, 2009년 8월.

[11] 보안뉴스, http://www.boannews.com/, “스마트 그리드 보안 위협 이미 나타나”, 오병민 기자, 2009년 11월 13일.

[12] 박찬국, “전력인프라 사이버보안 이슈와 정책 대응,” 정보통신연구진흥원 주간기술동향, 통권 1398호, 1-10쪽, 2009년 5월.
[13] Patrlck McDaniel, Sean W.Smith,“Security and Privacy Challenges in the Smart Grid,”IEEE security & privacy , V. 7 No. 3, 75-77, 2009.
[14] 서정택, 이철원,“스마트그리드 사이버 보안 동향,”정보처리학회지, 제 17권, 제 2호, 37-45쪽, 2010년 3월.
[15] 김재철, 김철환, 원동준, "한국의 스마트 그리드 추진 현황," 전기의세계, 제 58권, 제 8호, 27-36쪽, 2009년.

## 저자 소개

**서우석(Woo-seok Seo)**

2006년 8월 숭실대학교 정보과학대학원 정보통신융합학과(공학석사)
2009년 9월~현재 숭실대학교 일반대학원 컴퓨터학과 (박사과정)
※ 주관심분야 : 정보보호, 네트워크 보안, 방화벽, Router & Network Design 등

**전문석(Moon-seog Jun)**

1981년 2월 숭실대학교 전자계산학과 졸업
1986년 2월 University of Maryland Computer Science 석사
1989년 2월 University of Maryland Computer Science 박사
1986년 9월~1989년 12월 University of Mary 강사
1989년 3월~7월 Morgan State University 조교수
1989년 9월~1991년 2월 New Mexico State University Physical Science Lab. 책임연구원
1991년 3월~현재 숭실대학교 정교수
※ 주관심분야 : 정보보호, 네트워크 보안, 전자여권, 암호학