情 報 保 護 學 會 誌
第19卷 第4號, 2009. 8

지능형 전력망(Smart Grid)과 정보보호

전 용 희*

요 약

기존의 전력망에 정보기술을 융합하여 전력 공급자와 소비자가 양방향 통신을 통하여 에너지 생산과 소비 효율을 최적화 할 수 있는 지능형 전력망이 개발되고 있다. 특히 우리나라는 이 기술의 세계 선도국가로 지정되어 스마트 그리드 구축을 위한 로드맵을 수립할 예정으로 있다. 그러나 전력망이 통신망에 융합되면서 정보통신 인프라에서 발생하고 있는 보안 문제가 전력망에서도 그대로 재현되고 있다. 따라서 전력 인프라에 대한 사이버 공격을 방지하고 대응하기 위하여 정보보호 기술이 개발단계 초기부터 고려될 필요가 있다. 본 논문에서는 스마트 그리드와 같은 국가적인 주요 인프라를 보호하기 위한 정보보호 기술의 필요성과 요구사항 등에 대하여 살펴보고자 한다.

Ⅰ. 서 론

전력망에 통신망을 접목시켜 전력계통시스템의 제어를 통하여 발전·송전·배전의 전 과정에 대한 통제가 가능하여 지고, 결과적으로 에너지 사용의 효율성을 높이고자 하는 것이 에너지 인터넷이라고 불리는 지능형 전력망(Smart Grid)의 목표이다. 즉 기존 전력망에 정보기술(IT)을 융합하여 전력 공급자와 소비자가 양방향으로 실시간으로 정보를 교환함으로써 에너지 효율을 최적화하는 차세대 전력망이라고 할 수 있다.

지능형 전력망의 핵심기술로는 첨단 검침 인프라(AMI: Advanced Meter Infrastructure), 첨단 송배전 자동화, 분산 발전, 전기자동차 충전 하부구조 및 재생에너지 발전 등이 있다. AMI는 지능형 전력망, 통신 하부구조 및 지원 정보 하부구조의 융합으로 이루어진다.

스마트 그리드가 구축되면 소비자는 '똑똑한 전기'를 사용하게 됨에 따라, 전기 사용 요금과 사용량 정보를 실시간으로 알 수 있게 되고 가장 경제적인 시간대를 선택하여 전기를 사용하게 된다는 개념이다. 이렇게 되면 소비자는 그 동안의 수동적인 전력 소비 패턴에서 벗어나 전력 사용 시간대를 요금에 따라 선택 조정하는 등의 능동적인 전력 소비 패턴으로 전환하게 된다.

모든 IT 융합에서와 마찬가지로, 스마트그리드 역시 사이버 보안문제가 해결되어야 한다. 우리나라가 스마트 그리드 선도국가로 지정된 만큼, 스마트 그리드의 안전한 구현을 위한 보안 기술의 개발에 대하여도 구체적인 계획을 수립하여야 할 것이다.

따라서 본 논문에서는 스마트 그리드와 같은 국가적인 주요 인프라를 보호하기 위한 정보보호 기술에 대하여 알아보고자 한다.

Ⅱ. 지능형 전력망

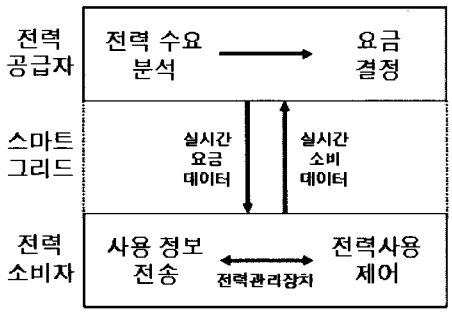
2.1 개요

지능형 전력망은 에너지를 절약하고, 비용을 줄이고 또한 신뢰성을 증가시키기 위하여 디지털 기술을 사용하여 공급자로부터 소비자까지 전력을 전달하게 된다. 정부의 녹색 성장 핵심과제 중에 지능형 전력망이 포함되어 있으며, 개발 과제 속에는 첨단 검침 인프라와 초고속 인터넷, 홈 네트워크 연동 기술 개발 및 표준화, IPTV, 홈서버, 휴대단말 기반의 사용자 전력 제어 서비스 개발 등이 세부적으로 포함되어 있다.

기존의 배전망은 대부분 화력이나 원자력 발전소 등에서 생산된 전력을 여러 단계의 변전 과정을 통하여 일반 소비자에게 단 방향으로 전달한다. 그러나 앞으로는 개인이나 기업에서 풍력, 태양광, 재생 에너지 발전 등을 통하여 생산된 잉여 전기가 전력망으로 공급될 수

* 대구가톨릭대학교 컴퓨터정보통신공학부(yhjeon@cu.ac.kr)

있는 양방향 전력 전달 방식으로 변하게 된다. 이런 변화로 에너지 소비에 대한 효율성, 전력 흐름의 실시간 관리 및 양방향 계량이 필요하게 된다. [그림 1]은 지능형 전력망의 기본적인 개념을 보여준다.



〔그림 1〕 지능형 전력망 개념도

지능형 전력망의 특징 중에서 소비자들에게 가장 분명하게 나타나는 것은 에너지 소비 효율성을 위한 지능형 계량기(smart meter)일 것이다. 이 계량기를 통하여 첨두(peak) 혹은 비첨두(offpeak) 부하 기간동안의 전력 생산 비용 차이를 반영하는 과금 체계가 가능하여 진다. 예를 들어, 일반 가정에서 전력을 많이 소비하는 온수 히터라든지 혹은 세탁기 등이 전력 요금이 싼 시간대를 선택하여 동작되도록 하는 부하 제어 스위치 등이 등장할 것이다. 이를 위하여 통신과 계량기 기술이 지능형 장치에게 각 가정에서의 에너지 수요, 에너지 사용량, 에너지 사용 시간에 대한 정보를 공급하게 된다. 또한 재생 에너지 생산을 통한 전력 소비로 첨두부하에 대비하기 위하여 생산하는 발전량을 줄일 수 있고, 결과적으로 탄소 가스의 배출 감소에도 큰 효과가 있을 것으로 기대된다.

2.2 기능

지능형 전력망은 정보기술을 이용하여 전력망의 효율성, 연결성 및 비용 이득을 위하여 전력망 인프라와 정보 인프라를 통합하는 것이라 할 수 있다. 지능형 전력망에서의 정보의 근원지는 다음과 같은 것이 있다[1]:

먼저 발전 부분의 정보 소스이다.

- 장비-상태 정보
- 전송망 상호연결 감시 센서 정보
- 발전 장비의 전반적 부하 상태

전송 부분의 정보 소스는 다음과 같다.

- 고압 전력선 상태 감시 센서 정보
- 전송 변전소 장비 상태 감시 센서 정보
- 전송망 상태 감시 PMU(Phasor Measurement Units) 정보
- 전송망 주변 환경 센서 정보
- 전력선 상태 감시 센서 정보
- 배전 변전소 장비 상태 감시 센서 정보
- 피더(feeder) 상태 감시 센서 정보
- 배전망 전력 상태 및 품질 측정 센서 정보

소비자로부터의 정보 소스는 다음과 같은 것이 있다.

- 전반적인 전력-사용 정보(계량기 정보)
- 전력-사용 패턴 정보
- 가정 내 장치에 의한 전력 사용에 대한 입상적 정보
- 전력망에 대한 가정 내 분산-발전 소스 정보
- 소비자 전력-사용 선호 정보(예: 부하 감소 프로그램 참여 의지)

미국 에너지 성(DOE: Department of Energy) Modern Grid Initiative 보고서에 의하면, 현대적인 지능형 전력망은 다음과 같은 기능을 가져야 한다[2]:

- 자기-복구(self-healing): 시스템 문제 탐지 및 대응을 위하여 임베디드 센서 및 자동제어 장치로부터의 실시간 정보를 이용하여 정전, 전력 품질 문제 및 서비스 손상을 자동으로 방지 및 완화시킬 수 있어야 한다.
- 그리드 운영에 소비자의 참여: 실시간 양방향 통신을 통하여 소비자가 에너지 절약에 참여할 수 있고, 태양광 발전, 풍력 및 재생 에너지를 그리드에 되 팔수도 있게 된다. 이를 위하여 그리드 설계, 운영 및 통신에 소비자의 장비 및 행위를 반영해야 한다. 이렇게 함으로써 가정 및 비즈니스에 위치하는 지능형 장치 및 지능형 빌딩과 같은 에너지 관리 시스템 통제가 가능하여 진다.
- 공격에 대한 저항성: 인간이 만들거나 자연적인 붕괴를 식별하고 대응하는 기술을 채택해야 한다. 실시간 통신으로 특정 영역을 고립시키거나 손상된 설비를 우회하여 전력 흐름을 변경 할 수 있어야 한다.
- 고품질의 전력 공급: 안정적인 전력 공급으로 정전 시간을 감소시켜야 한다.
- 발전 선택권의 수용: 지역 수준에서의 연료 전지,

재생 에너지, 소형 터빈과 같은 분산 발전 시스템을 수용해야 한다.

- 개방 전력 시장의 활성화: 분산 발전 시스템을 통하여 태양광 발전, 소규모 풍력 터빈과 같은 대체 에너지 소스에서 생산된 전기를 판매 할 수 있어야 한다.
- 스마트 그리드의 효율적인 운영

2.3 특징 및 기술[3]

2.3.1 특징

스마트 그리드는 요구 기능을 수행하기 위하여 광범위한 특징을 제공한다.

- 부하 조정: 전력망의 부하는 시간에 따라서 상당히 변할 수 있다. 지능형 전력망에서는 부하 조정 알고리즘을 통하여 전력망의 실패율을 감소시켜야 한다.
- 수요 대응 지원: 소비자 댁내에 설치된 지능형 장치와의 양방향 통신을 통하여 피크 부하 동안의 전력 수요를 감소시킴으로써, 추가 발전에 따른 비용을 절감할 수 있다.
- 부하에 대한 탄력성: 네트워크 구조로 된 복수의 경로를 통하여 부하에 탄력성을 제공한다.
- 전력 생산의 분산화: 풍력발전이나 태양광 발전과 같은 개별 소비자의 발전 시설을 허용하고, 잉여 전력을 되 팔수 있게 된다.
- 소비자에 대한 가격 신호: 지능형 계량기를 통하여 시간대별 전력 가격 정보를 교환함으로써 맞춤식 전력 사용이 가능하여 진다.

2.3.2 기술

일반적으로 지능형 전력망 핵심 기술은 아래와 같이 5개로 그룹화 될 수 있다[2]:

- 통합된 통신: 지능형 전력망을 위한 통신 방식은 BPL(Broadband over Power Line), WiFi, WiMax, 3G 셀룰라, TDMA/CDMA, VSAT(Very Small Aperture Terminal) 위성과 같은 여러 형태의 무선망 및 고속 인터넷 백본망, 전력선(PLC: Power Line Carrier) 통신, RFID(Radio Frequency IDentification) 통신 같은 통합된 통신 형태가 될 것이다[4].
- 센싱 및 측정: 전력망의 안정성, 장비 상태 감시, 에너지 관리 정책 지원 등을 위한 센싱 및 측정 기술이 필요하다.
- 지능형 계량기: 지능형 계량기를 통하여 효율적인 전기 사용이 가능해진다.
- PMU(Phasor Measurement Unit): 전력 품질을 감시하고 자동 대응하는 고속 센서 기술이 필요하다.
- 장거리 측정 시스템: 지역적이고 전국적인 규모에서 실시간 감시 체계를 제공하는 PMU의 네트워크이다.

기타 아래와 같은 기술이 필요하다.

- 첨단 부품: 초전도, 결함 감내, 에너지 저장, 전력 전자 및 진단 부품 기술 등에서 혁신이 필요하다.
- 첨단 제어: 특정 전력망의 붕괴와 정전에 대한 신속한 진단과 정확한 해결책을 위한 전력 시스템 자동화 기술이 필요하다.
- 개선된 인터페이스 및 결정 지원: 전력망의 효율적인 운영 및 관리를 위한 시각화 기술, 소프트웨어 시스템, 훈련용 시뮬레이터 등의 정보 시스템 기술이 필요하다.

2.4 개발 전략

전력망에 IT 기술이 접목되면서 융합에 따른 보안 문제가 제기되고 있다[5]. [6]에서는 인터넷의 역사로부터 배울 수 있는 스마트 그리드 구축을 위하여 지켜야 할 12가지를 다음과 같이 제시하고 있다:

① 확장성 있는 서비스-지향 스마트 그리드 구조
② 통신 프로토콜의 정의 및 표준화
③ 보안 및 암호화
④ 에너지 관리 및 통신 도구
⑤ 개방 API(Application Programming Interface)
⑥ 킬러(killer) 애플리케이션의 발견
⑦ 소비자에 대한 다양한 인터페이스 제공
⑧ 인터넷에서의 IETF(Internet Engineering Task Force)와 같은 소위 "SGTF(Smart Grid Task Force)"의 결성
⑨ 명령 및 제어(C&C: Command and Control) 통신과 같은 특정 접근만을 허용하는 시큐어 그리드

계층(secure grid layer) 구축
⑩ 자동화된 자기-복구 능력
⑪ 국가 단위의 기술 시험 환경 구축
⑫ 스마트 그리드에 대한 경제성, 라이프 스타일 증진, 에너지 보존 및 재생 에너지 통합 효과 측정 및 평가

지능형 전력망의 성공적인 구축을 위하여 인터넷으로부터 구축된 그 동안의 지식을 잘 사용해야 한다는 것이다. 국가적인 지능망 구축 로드맵을 작성할 때도 이러한 점이 잘 반영되어야 할 것으로 생각된다.

Ⅲ. 정보보호의 필요성

3.1 필요성

지능형 전력망의 효과적인 운용을 보장하는 사이버 보안의 역할에 대하여 미국의 에너지 성(DOE) 에너지 부문 계획에 문서화되어 있다. 미국의 국가 하부구조 보호 계획(NIPP: National Infrastructure Protection Plan)에 의하면 사이버 보안은 다음과 같이 정의된다[2]:

"기밀성, 무결성 및 가용성을 보증하기 위하여 전자정보 및 통신 시스템과 서비스(그리고 그 속에 포함된 정보)에 대한 손상, 권한이 없는 사용 및 남용을 방지하고, 필요한 경우, 복구까지를 포함 한다".

그리드에 대한 위험 요소는 다음과 같다:

- 그리드의 복잡성이 취약성을 도입할 수 있고, 잠재적인 공격 노출 및 비고의적 에러를 증가시킬 수 있다.
- 상호 연결된 네트워크가 통상적인 취약성을 도입할 수 있다.
- 통신 붕괴에 대한 취약성 및 서비스 거부(DoS: Denial of Service) 공격이나 소프트웨어 및 시스템 무결성을 침해할 수 있는 악성 소프트웨어 유입의 가능성을 증대시킨다.
- 잠재적인 공격을 위한 진입점과 경로의 수가 증가한다.
- 고객의 비밀성을 포함하여 데이터 기밀성의 침해가 가능하다.

시스코사에서 보는 지능형 전력망에 대한 정보보호 필요성은 다음과 같은 요인에서 지적하고 있다[7].

- 그리드 하부구조와 IP-기반 유선 및 무선망과의 혼합
- 지능형 계량기, 센서, 원격 검침 및 제어 시스템 같은 새로운 네트워크 종단점의 유입
- 입상적(granular) 접근 정책 및 고용원, 계약자 및 소비자와 같은 원격 사용자 그룹을 위한 제어에 대한 요구 증가
- 사이버 위협을 은폐하기 위한 위협 기술의 진화
- 규제적 컴플라이언스 요구사항

미국 DOE에서도 현대적인 그리드를 도입하는데 해결해야 할 기술적인 장벽 중에 보안 기술을 명시하고 있다[8]. 특히 분산 에너지 자원 소유주, 독립 전력 생산자, 소비자의 수요 대응 및 자동화 검침 프로그램 등에 반드시 보안 기능이 구축되어야 하며, SCADA (Supervisory Control And Data Acquisition) 및 보호 계전기 시스템의 보안이 보장되어야 함을 명시하고 있다.

3.2 지능형 전력망의 취약성

지능형 전력망의 핵심 기술인 첨단 검침 인프라 즉, 지능형 계량기(스마트 미터)의 취약성을 이용하면 금전적 이득을 취할 수 있기 때문에, 악성 해커의 타깃이 될 것으로 예상된다[9]. 만약 해커가 계량기를 침해하게 된다면, 에너지 비용을 즉각 조작할 수 있고 발전 에너지 계량기 수치를 조작할 수 있다. 이미 미국 내의 전력망에 대한 소비자 사기 행위가 발생하고 있으며, 그 액수는 60억불에 달하는 것으로 평가하고 있다.

기계적인 계량기에서 디지털 계량기로 전환됨에 따라, 공격 행위가 조잡하고 위험한 물리적 시스템 조작에서 원격 침투와 복잡하고 여러 가지 상태 정보를 보유한 컴퓨터의 조작으로 이동하게 될 것이다. 이것으로 더욱 정교한 공격이 가능하여 지고, 개인 전력 사용량에 대한 변경과 같은 소규모 공격이나, 전력망에 대한 대규모 공격 개시 형태로 전개될 수 있다. 예를 들어, 지능형 계량기 사이에서 확산되는 웜이 최근에 실제로 제작되었다[9]. 계량기 봇(meter bots), 분산 서비스 거부(DDoS: Distributed Denial of Service) 공격, 사용 기록기(usage logger), 지능형 계량기 루트킷, 계량기-기반 바이러스 및 다른 악성 소프트웨어가 출현할 것이 거의 확실하다.

또한 지능형 전력망에 저장된 에너지 사용 정보를 통하여 고객의 비밀성이 침해될 수 있다. 전력 소비 습관

과 행위 등이 노출된다. 예를 들어, TV 시청과 같은 특정 활동이 탐지될 수 있는 전력 소비 징후를 가지게 된다.

따라서 지능형 전력망의 도입과 함께 필요한 정보보호 관련 기술에 대하여도 조사될 필요성이 존재한다.

Ⅳ. 정보보호 기술

4.1 요구사항 문서

지능형 전력망에 적용될 수 있는 많은 요구사항 문서들이 존재한다. 현재로는 NERC Critical Infrastructure Protection(CIPs) 만이 지능형 전력망의 특정 도메인에 대하여 의무적이다. 다음의 문서들이 지능형 전력망 CSCTG(Cyber Security Coordination Task Group)의 구성원들에 의하여 보안 요구사항으로 식별되었다[2].

다음의 표준들은 지능형 전력망과 직접 연관이 있다.

- NERC CIP 002, 003-009
- IEEE 1686-2007, IEEE Standard for Substation Intelligent Electronic Devices Cyber Security Capabilities
- AMI System Security Requirements, 2008
- UtilityAMI Home Area Network System Requirements Specification, 2008
- IEC 62351 1-8, Power System Control and Associated Communications-Data and Communication Security

그 외에 제어 시스템에 적용할 수 있는 문서로는 다음과 같은 것이 있다:

- NIST SP 800-82, DRAFT Guide to Industrial Control Systems(ICS) Security, Sept. 2008.
- NIST SP 800-53, Recommended Security Controls for Federal Information Systems, Dec. 2007.
- ANSI/ISA-99, Manufacturing and Control Systems Security, Part 1: Concepts, Models and Terminology and Part 2: Establishing a manufacturing and Control Systems Security Program
- 기타

4.2 개발 전략

지능형 전력망의 개발과 함께 지능형 전력망 정보보호 기술이 개발되어야 할 것으로 보이며, 아래와 같은 여러 가지 목표를 가지고 추진되어야 할 것이다[9].

- 소비자 보호를 위한 법적 제도가 확립되어야 한다. 의료정보보호를 위하여 미국에서 도입된 HIPAA (Health Insurance Portability and Accountability Act)와 마찬가지로 지능형 전력망을 위한 법제화가 이루어져야 한다. 이 법에서는 소비자 데이터 수집 방법, 데이터의 사용 권한, 정보 오남용에 대한 벌칙 등에 대하여 규정하여야 할 것으로 보인다.
- 정부, 학계 및 산업계가 지능형 전력망에 대한 보안 기술을 광범위하게 평가하고 시험해야 할 것이다. 특히 지능형 계량기에 대한 설계 단계에서 보안 기술이 포함되도록 하여야 할 것이다. 지능형 전력망 시스템에 대한 평가 기준도 확립되어야 할 것이다. 관련 기술 개발의 경쟁 체제 도입, 표준 제정 및 보안 전문가에 의한 독립적인 소스 코드 검토, 공공 시험 기관의 설립 등을 통하여 시스템의 품질을 개선할 수 있도록 유도하여야 한다.
- 지능형 전력망 실패에 대한 복구 전략이 확립되어야 한다. 복잡한 소프트웨어 시스템으로 하여금 자연스럽게 이용될 수 있는 버그를 가질 수 있으며, 이에 대한 소프트웨어 패치 관리 대책을 수립하고, 침해 시스템의 신속한 식별과 고립이 가능하도록 해야 할 것이다.

4.3 기능적 보안 요구사항

지능형 전력망 보안 기술이 효과적이기 위하여 종단간에 걸친 보안 능력이 필요하며, 이렇게 하기 위하여 위협을 탐지하고 완화할 수 있도록 여러 지점에 방어 메커니즘을 보유하는 계층화 구조가 필요하다. 기능적인 보안 요구사항은 다음과 같다[7]:

- 통합 물리 보안: 지능형 전력망에서 고려해야 할 첫 번째 사항으로 침입자로부터 그리드를 보호하는 물리적 보안을 지적하고 있다. 이를 위하여 IP 백본에 통합될 수 있는 비디오 감시, 카메라, 전자 접근 통제 및 긴급 대응 능력을 포함하여야 한다. IP 망과의 통합을 통하여 중앙 관리 및 통제, 모니터링 및 기록 능력, 정보에 대한 신속한 접근 등이 가능하여 진다.
- 신분 및 접근 통제 정책: 고용자, 계약자, 고객을

포함하여 지능형 전력망에 접근을 할 수 있는 여러 사용자 그룹이 존재한다. 이러 사용자 그룹에 대한 접근은 입상적(granular)으로 이루어져야하며, 권한부여는 "알 필요가 있는(need to know)" 자산에만 허용되어야 한다. 예를 들어, 종업원은 특정 지능형 제어 시스템에 접근할 수 있고, 계약자는 타임카드 응용에만 접근하고, 그리고 고객은 온라인으로 에너지 소비와 계산서(bill)를 볼 수 있도록 하는 인터넷 가능 접근을 할 수 있다.

강한 인증 메커니즘을 통하여 신분이 검증되어야 한다. 강한 패스워드를 사용해야 하고, 모든 시도는 기록되어야 한다. 지능망에 대한 접근은 명시적인 접근 허용을 통해서만 부여되는 "디폴트 거부" 정책을 구현해야 한다. 게다가, 허용되지 않는 접근을 방지하기 위하여 모든 접근점은 강화되어야 하며, 정상 운용을 위하여 필요한 포트와 서비스만이 실행되어야 한다.

- 강화된 네트워크 장치 및 시스템: 효과적인 보안 구조의 기반은 인프라 자체를 보호하는 것이다. 라우터와 교환기 같은 핵심 요소가 취약성이나 접근을 위한 방법을 제공하지 않도록 적절히 보호되어야 한다. 만약 이런 장치들이 침해된다면, DoS 공격을 통하여 전력망 운용을 방해하기 위하여 혹은 더욱 중요한 제어 시스템에 접근 하기 위하여 사용될 수 있다.
- 위협 방어: 효과적이고 계층적인 방어를 구축하기 위하여 전체 인프라에 걸친 광범위한 보안 원칙을 주의 깊게 적용해야 한다.
  - DoS 공격이 전력망의 기능을 약화시킬 수 있다. 네트워크 분할 및 접근 제어로 인하여 인터넷에서 기원하는 DoS 공격이 제어 시스템에 어떠한 영향을 미치지 않도록 해야 한다.
  - 중요 클라이언트 시스템, 서버 및 종단 기기를 보호하기 위하여 호스트-기반 침입방지시스템(IPS)과 앤티 바이러스 능력을 갖추어야 한다.
  - 인프라에 진입을 시도하는 외부 위협을 식별하기 위하여 네트워크-기반 IPS도 설치되어야 한다.
  - 페리미터(perimeter)와 인터페이스를 가지는 요소가 안전함을 보장하도록 취약성 평가가 주기적으로 수행되어야 한다.
- 전송 및 저장 데이터 보호: 다른 네트워크 세그먼트 사이의 접근 정책을 시행하기 위하여 방화벽 기능을 구현해야 한다. 안전하고 기밀성 데이터 전송을 위하여 암호 알고리즘을 적용한 가상사설망(VPN) 구조를 지원해야 한다. 서버와 종단 장치상의 중요 자산을 보호하기 위하여 호스트 암호화 및 데이터 저장 보안 능력을 허용하여야 하며, 유무선 연결 상에 유비쿼터스 보안을 제공해야 한다.
- 실시간-감시, 관리 및 상호협동: 보안 사고의 타깃이 되거나 취약성 있는 네트워크 요소를 알기 위하여 실시간 감시체계가 수립되고, 관리 및 상호협동하여야 한다.

V. 맺음말

2009년 7월 9일 이탈리아에서 개최된 G8 확대정상회의 기후변화 세션에서 '세계를 바꾸는 기술(전환적 기술)' 7개를 선정했는데, 이 중 지능형 전력망 기술 개발을 선도할 국가로 우리나라가 지정된바 있다. 우리나라는 이미 지난 3월 세계 최초로 스마트 그리드 기술의 국가 단위 발전 로드맵을 작성한 바 있으며, 스마트 그리드 구축을 위한 로드맵을 오는 11월 수립할 계획으로 있다.

2009년 7월 초에 발생한 7.7 DDoS 공격처럼, 만약 전력 인프라에 사이버 공격이 발생하면 국가적인 정전 사태와 같은 초유의 비상사태가 생길 지도 모른다. 따라서 국내에서도 정부와 산업체, 학계 및 연구소 등이 컨소시엄을 형성하여 점차 지능화·다양화되고 있는 사이버 공격에 대응할 수 있는 개발 전략을 수립하여야 할 것이다. 따라서 본 논문에서는 지능형 전력망의 도입에 따른 정보보호 기술의 필요성에 대하여 강조하고자 하였다.

지능형 전력망을 위한 정보보호 기술을 구현하기 위해서는 전체적인 보안 위험 관리 프레임워크가 개발되어야 한다. 이 프레임워크는 민간 및 공공부분에서 개발된 기존의 위험 관리 방식을 기초로 하여야 할 것이다. 이 프레임워크에서 지능형 전력망의 위험을 평가하기 위하여 전체 시스템에 대한 영향, 취약성 및 위협 정보를 결합하기 위한 프로세스를 확립해야 할 것으로 생각된다.

참고문헌

[1] Venkat Pothamsetty and Saadat Malik, Smart

Grid: Leveraging Intelligent Communications to Transform the Power Infrastructure, Cisco White Paper, Feb. 2009.

[2] U.S. Department of Energy, National Energy Technology Lab., Modern Grid Initiative, http 자료.

[3] Wikipedia encyclopedia, Smart Gird. May, 2009.

[4] DOE Office of Electricity Delivery and Energy Reliability, Integrated Communications, July 2007.

[5] 정수환, "융합보안 R&D 이슈 및 방향", 정보보호학회지 제 19권 제 3호, 한국정보보호학회, pp. 11-13, 2009년 6월.

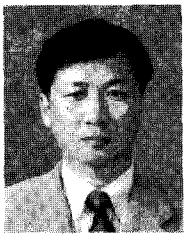
[6] Balaji Natarajan, A dozen things the Smart Grid can learn from the Internet, earth2tech. 2009. 4.30.

[7] Cisco White Paper, Security for the Smart Grid, 2009.

[8] DOE Office of Electricity Delivery and Energy Reliability, Barriers to achieving the modern grid, July 2007.

[9] Patrick McDaniel and Stephen McLaughlin, "Security and Privacy Challenges in the Smart Gird", Secure Systems, May/June, pp. 72-74, IEEE, 2009.

〈著者紹介〉



전 용 희 (Yong-Hee Jeon)

종신회원

1971년 3월~1978년 2월: 고려대학교 전기전자전파공학부, 학사

1985년 8월~1987년 8월: 미국 플로리다 공대 대학원 컴퓨터공학과

1987년 8월~1992년 12월: 미국 노스캐롤라이나주립 대학원 Elec. and Comp. Eng. 석사, 박사

1978년 1월~1978년 11월: 삼성중공업(주)

1978년 11월~1985년 7월: 한국전력기술(주)

1979년 6월~1980년 6월: 벨기에 벨가톰사 연수

1989년 1월~1989년 6월: 미국 노스캐롤라이나주립대 Dept of Elec. and Comp. Eng. TA

1989년 7월~1992년 9월: 미국 노스캐롤라이나주립대 부설 CCSP (Center For Comm. & Signal Processing) RA

1992년 10월~1994년 2월: 한국전자통신연구원 광대역통신망연구부 선임연구원

1994년 3월~현재: 대구가톨릭대학교 컴퓨터 · 정보통신공학부 교수

2001년 3월~2003년 2월: 대구가톨릭대학교 공과대학장

2004년 2월~2005년 2월: 한국전자통신연구원 정보보호연구단 초빙연구원

2007년 1월~2007년 12월: 한국정보보호학회 학회지 편집위원장

2008년 1월~현재: 한국정보보호학회 부회장

2009년 1월~현재: 한국정보과학회 정보보호연구회 위원장

<관심분야> 네트워크 보안, DDoS 탐지 및 대응 기술, 산업제어 시스템보안, 통신망 성능분석