신기술동향

스마트 그리드 보안 기술 동향

김미희 (한경대학교)

목 차 »

1. 서 론

기존 전력망의 비효율성 해소 및 저탄소 녹색성장의 일환으로 전력과 IT 융합을 통한 스마트 그리드 기술 개발에 대한 전세계적 관심이 집중되고 있다. 이러한 차세대 성장동력인 스마트 그리드 기술의 실현가능성을 높이기 위해서는 국가기간망이라는 특성상 무엇보다도 보안이 필수 요소이다. 전력망의 공격은 경제적 손실을 야기할 뿐 아니라 국가적 혼돈을 초래할 수 있다. 한 예로 미국 전력망이 사이버 스파이에 의해 공격당한 사건들이 보고되고 있어 스마트 그리드 보안의 중요성은 더욱 강조 되고 있다[1].

스마트 그리드를 위한 보안 연구를 위해 스마트 그리드를 위한 네트워크 구조의 특성 파악 및 요소 기술의 분석이 필요하다. 스마트 그리드 서비스를 제공하기 위한 네트워크 구조는 가정이나 사무실 등 작은 규모의 홈네트워크(HAN, Home Area Network)와 이러한 HAN들을 연결하는 지역네트워크(NAN, Neighborhood Area Network), 지역 네트워크 및 기존 전력망을 연결하는 광대역네트워크(WAN, Wide Area Network)가 계층적으로 구성되어 있다. 이러한 네트워크 구조에 맞는 보안 연구가 각 부분별로 제공되어야 함은 물론 그 보안 기법들은 유기적인 연동 및 협업이 필수적이다.

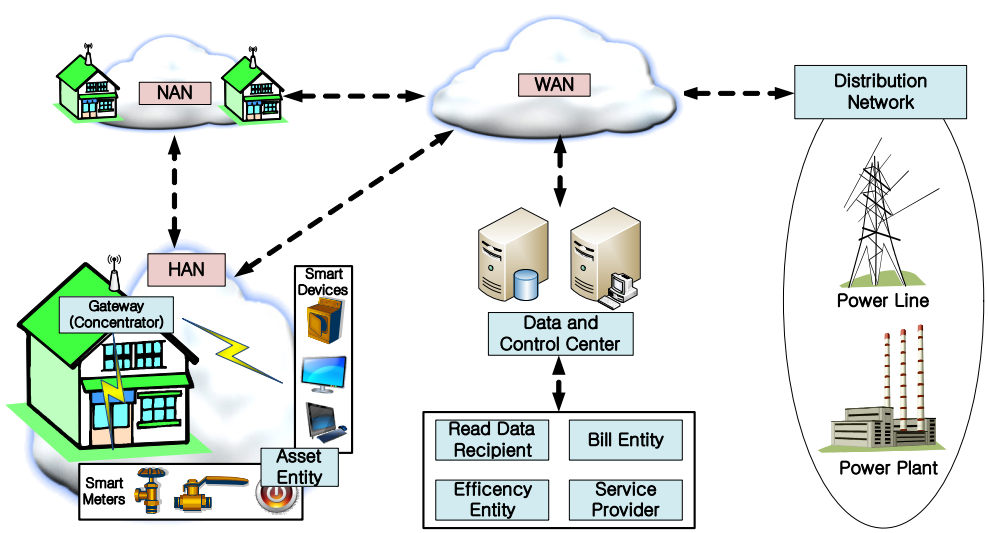
이러한 스마트 그리드 네트워크에 안전성을 제공하기 위한 보안 요소 중, 전력망의 특성상 가용성 및 지연민감 데이터 전송 보장, 프라이버시 보장 등이 가장 중요하다. 예를 들어, 전력망(electrical power grid)의 상태를 지속적으로 감시하는 스마트 그리드 내 실시간 전송 시스템에서는 최대 4 밀리초의 지연시간이 허용되며, 통신 장애는 바로 전력 손실과 직결되어 있어 지연민감 데이터의 전송 보장이 중요하다. 이러한 요소에 대한 최신 보안 연구를 공격대응, 통신의 가용성 보장, 실시간 전송시스템의 전송보장, 프라이버시 보장 연구로 나누어 살펴보자.

2. 스마트 그리드를 위한 네트워크 구조

기존 전력망에 IT 기술이 접목되어 효율적 전력 공급 및 유기적 제어 서비스를 제공하기 위해 스마트 그리드 네트워크는 그림 1과 같은 계층적 구조로 구성된다. HAN에서는 게이트웨이(스마트 미터기가 해당 기능 대체 가능)를 중심으로 스마트 미터기, 가전, 분산에너지자원(DER, 예, 태양열, 풍력발전용 터빈) 등으로 구성된 자산 개체(Asset Entity)들이 연결되어 있다. 스마트 미터기는 가정에서 사용한 전기 사용량, 수요, 퀄리티 등을 주기적으로 측정하고 게이트웨이를 통해 광역망에 연결된 데이터/제어센터(Data and Control Center)에 전송한다. 각 HAN의 게이트웨이들은 트리 또는 메쉬 구조로 연결되어 NAN을 구성하고 WAN을 통해 데이터/제어센터와 기존 전력망(Distribution Network)을 총체적으로 연결한다. 데이터/제어센터는 서비스 제공업체(Service Provider)와 데이터 수집(Read Data Recipient), 전기요금 계산(Bill Entity), 효율성 제공(Efficiency Entity)을 위해 상호 연결되어 있다.

3. 스마트 그리드의 국내외 추진 동향

국내에서는 세계 최대·최첨단 스마트 그리드 실증단지를 조기에 구축해 관련기술의 상용화·수출 산업화 촉진을 목적으로 제주도 구좌읍(제주 동북부 소재, 12개리)일대 약 6천호 가구 대상 실증단지를 구축해 스마트 그리드의 활성화를 위해 노력중이다(그림 2). 2008년 부지확정 및 개념정립의 기초단계를 시작으로 인프라 구축의 기본단계를 거쳐 2013년 통합운영의 확장단계를 진행해 왔다. 스마트 미터, 전기차 충전기, 전력저장장치, IT・에너지 등 170여개 민간기업의 참여를 바탕으로 2013년까지 2,395억원을 투입하여 진행해 왔으며, 보안 사고에 대해서는 '지능형전력망 구축 및 지원에 관한 특별법'에서 '정보보호 및 보안'에 대한 규정을 포함해 관련 법 내에 보안 규정을 강화하고 이를 대비하고 있다[3]. 이러한 노력과 함께 스마트미터 자체 취약성 보완을 위해 보안 칩이나 바이러스 연구, 통신구간에서 생성 및 전송 정보의 암호화, 상호 에지 네트워크 인증 및 로그 관리, 중앙 통합 보안



(그림 1) 스마트 그리드를 위한 네트워크 구조[2]

(그림 2) 제주도 스마트 그리드 실증단지 배치도[3]

관리 체계 구축, 생성 및 관리되는 대량의 데이터 관리 등의 연구가 진행되고 있으나, 아직까지는 실제적인 보안 메커니즘 설계 및 구축, 표준화 진행이 필요한 초기 단계라 볼 수 있다.

국외에서는 미국, EU 등을 중심으로 다양한 스마트 그리드 프로그램 및 법안을 마련하여 스마트 그리드 기술 개발에 박차를 가하고 있다. 그러나 아직까지 스마트 그리드 보안 분야의 연구 내용은 개념 정립의 기초단계라 볼 수 있다. 미국에서는 에너지 자립 및 노후 전력망의 현대화를 통한 경기부양 목적으로 Grid2030 국가 비전을 발표하고 진행하고 있으며, 스마트 그리드 보안 기술 부분에 대해 2009년 전력 인프라 보호법을 발의하여 전력기반 시설을 사이버공격으로부터 보호하기 위한 대책을 요구하였고 NIST 연구소에서 사이버 보안 워킹그룹을 운영하여 보안 연구를 진행하고 있다. EU에서는 신재생에너지 보급 확대 및 회원국 간 전력거래 활성화를 위해 스마트 그리드 사업을 진행하고 있고, 스마트 그리드 보안 기술 부분에 대해, 사생활 정보와 데이터 보호 조항을 포함하여 스마트 그리드 프레임워크 입법하였고(2011년), "스마트 그리드 비전 및 향후 연구개발 전략: 5개 연구부분, 19개 세부과제 선정"을 통해 "운영, 복구, 방어 계획을 위한 아키텍처와 도구 개발, 스마트 그리드 장애 및 외부 공격 대응 방안, 송, 배전 시스템의 사이버보안 및 복구 능력 향상 방법론"과 같은 보안 사항의 연구를 진행하고 있다.

스마트 그리드에 대한 관심이 높아지면서 2010년 IEEE International Conference on Smart Grid Communication 이라는 국제 학회가 개최되고, Cornell University, Carnegie Mellon University 등 전세계 유명 대학 및 연구소의 학자가 참석한 가운데 보안 내용을 포함하여 다양한 연구결과를 발표하였으며, 같은 해 IEEE Transactions on Smart Grid 라는 저널이 발간되기 시작하였다.

4. 스마트 그리드의 보안 위협 및 연구 동향

스마트 그리드의 보안 위협을 지적하고, 최근 연구가 진행되고 있는 스마트 그리드의 보안 연구 동향을 크게 공격대응, 통신 가용성 보장, 실시간 전송 시스템의 전송보장 연구, 프라이버시 보장 연구로 나누어 설명한다.

4.1 스마트 그리드의 보안 위협

스마트 그리드의 내부적 불안정한 시스템 운영으로 인한 가동 중지('08년 3월 미국 조지아주 해치 원자력 발전소)뿐 아니라, 웜바이러스에 의해 발전소 가동이 중지된 사고가 보고되고 있다. 또한 모의 해킹 실험에 의해 발전소의 제어 시스템도 침투 가능하다는 결과('08년 미국 TVA사)가 보고되었으며, 스마트미터를 통해 자가 전파되는 웜이 시연되기도 하였다('09년 블랙햇)[4]. 이러한 스마트 그리드의 보안 위협은 이에 대응하는 보연 연구의 필요성을 강조하고 있다.

4.2 공격대응

스마트 그리드 네트워크에서 가용성 측면의 보안 위협은 크게 공격 타겟 시스템에 따라 4가지 분

류로 나누어 볼 수 있다. 공급 시스템(Generation) 공격, 분산 제어 시스템(Distribution and Control) 공격, 스마트 미터기 공격, 스마트 마이크로 그리드 공격이 그것이다. 첫째, 공급 시스템을 타겟으로 하는 공격의 경우, 공격을 위해 공격자 입장에서는 상당한 양의 민감 정보가 요구되나, 여러 자산을 위협하며 공격의 범위가 확대할 수 있다. 분산 제어 시스템(Distribution and Control)을 타켓으로 하는 공격은 주로 거짓 데이터를 주입하여 전력 감시제어 시스템을 위협하는 공격으로, 거짓 데이터 주입 공격(false data injection attack), 은밀한 속임수 공격(stealthy deception attack), 로드정보 변경 공격(load altering attack) 등이 가능하다고 보고되고 있다. 셋째로 스마트 미터기에 대해서 호기심/의도적 도청, 비윤리적 고객들의 행위, 미터 데이터 관리 기관의 지나친 간섭, 가격 정보 변경 공격이 가능하다. 앞서 소개한 홈네트워크 구조에서 전력 생산이 이루어지는 분산에너지자원(DER)이 있는 경우를 스마트 마이크로 그리드라 하고, 여기에는 각 홈네트워크 간에 새로운 기능인 에너지 라우팅이 필요하다. 그러나 에너지 라우팅은 거짓 에너지 공유 정보를 삽입하는 공격에 취약하다. 각 시스템 구조 및 공격 특성에 맞춘 대응 메커니즘이 연구되어 왔고[5-8], 스마트 그리드 보안 연구의 주축을 이루고 있다.

4.3 통신의 가용성 보장

서로 상이한 데이터를 전달하는 멀티레이어 네트워크의 신뢰성 있는 전송 구조를 제공하기 위해서 인지라디오 기술이 주목 받고 있다. 인지라디오 기술은 무선 대역폭에 대한 요구 증가를 만족시키고 채널 효율을 높이기 위해 제안된 기술이다. 이는 채널 라이센스 유저(PU, Primary User)와 이차 유저(SU, Secondary User) 사이에 채널을 공유하도록 설계되었다. IEEE 802.22는 교외지역에서 TV 밴드의 화이트 스페이스를 공유하는 방식으로 표준화된 대표 인지라디오 기술의 표준이다. 관련 연구로서 IEEE 802.22 인지라디오 기술을 스마트 그리드 WAN에 적용하기 위한 구조가 제안되었다[9]. 자체 치유 및 공격에 대한 저항, 효율성 향상 등의 장점을 부각하고 있으나, 통신의 신뢰성을 높이기 위한 인지라디오 기술의 접목은 연구 초기 단계에 있고, 실질적인 적용에 대한 연구가 진행되어야 한다.

4.4 실시간 전송시스템의 전송보장

인터넷과 스마트 그리드 네트워크의 주된 차이는 데이터 처리량보다 메시지 지연이 더욱 중요하다는 사실이다. 특히 실시간 전송이 요구되는 감시 시스템의 프로토콜(예, GOOSE)이나 제어메시지(Control traffic)에서 그러하다. GOOSE 프로토콜은 전력 서브스테이션 네트워크에서 서브스테이션 이벤트, 명령어, 알람 등 지연민감한 메시지를 전달하기 위해 IEC61850에서 설계한 링크 계층 멀티캐스트 프로토콜로 2에서 10밀리초 내의 전송을 요구하고 있다. 이를 보장하기 위한 메커니즘 연구가 진행되고 있다[10].

4.5 프라이버시 보장

프라이버시 보장은 스마트 그리드 보안측면에서 또 하나의 중요 요소이다. 왜냐하면 스마트 미터기의 데이터는 단순히 전력 사용량이나 사용자의 계좌정보를 노출할 수 있을 뿐 아니라, 센싱 데이터를 통해 가정의 일상을 드러낼 수 있기 때문이다. 예로, 공격자는 샤워온수기 작동 주기를 통해 가족 구성원 수를 파악할 수 있고, TV가 on/off되는 사이클을 보고 현재 집 안에 사람이 있는지 등을 파악할 수 있다. 이러한 프라이버시 보장을 위해 서비스 제공자에게 필요한 정보도 제공하고 프라이버시도 보장하

는 방법이 연구되었다[11,12].

5. 결 론

앞에서 언급한바와 같이 스마트 그리드 네트워크의 각 요소별 안전성 대응을 위해 공격대응, 통신의 가용성 보장, 실시간 전송시스템의 전송보장, 프라이버시 보장 연구 등이 진행되고 있다. 이는 분명 스마트 그리드 기술의 실현가능성을 높이고, 새로운 산업 활성화, 그리고 나아가 국가경쟁력 강화를 가능하게 할 것이다. 그러나 각 보안 요소들이 유기적으로 융합하여 공격자들이 분산 공격하거나 공격자가 공격 타겟 시스템과 다른 네트워크에 존재하여도 그 대응력을 높이기 위한 연구는 활발히 이루어지지 못하고 있는 실정이다. 이러한 융합 보안 연구를 통한 실질적이고 총체적인 보안 프레임워크 조성이 앞으로 스마트 그리드 기술의 현실화를 앞당기고 스마트 그리드 서비스의 활성화를 촉진할 수 있으리라 기대한다.

감사의 말씀

본 연구는 2011년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No. 2011-0014020)

참 고 문 헌

[1] J. Meserve, “Sources: Staged cyber attack reveals vulnerability in power grid”, CNN, Sep. 2007.

[2] Y.M. Kwon, J.S. Kim, M.Y. Chung, H. Choo, T.-J. Lee, M. Kim, “State of the Art 3GPP M2M Communications toward Smart Grid”, KSII Transactions on Internet and Information Systems, Vol. 6, No. 2, pp.468-479, Feb. 2012.

[3] 제주 스마트 그리드 실증단지, http://smartgrid.jeju.go.kr/

[4] 스마트 그리드 보안 살펴보기, http://www.boannews.com/plan/plan_view.asp?idx=20523

[5] S. M. Amin, “Securing the electricity grid”, Bridge, Vol. 40, No. 1, pp.13-20, Mar. 2010.

[6] Y. Huang, H. Li, K.A. Campbell, and Z. Han, “Defending False Data Injection Attack On Smart Grid Network Using Adaptive CUSUM Test”, in Proc. CISS, 2011.

[7] S. Kim, E. Kwon, M. Kim, J. Cheon, S. Ju, Y. Lim, and M. Choi, “A Secure Smart-Metering Protocol Over Power-Line Communication”, IEEE Trans. on Power Delivery, Vol. 26, No. 4, Oct. 2011.

[8] Zhu, T., Xiao, S., Ping, Y., Towsley, D., Gong, W. “A secure energy routing mechanism for sharing renewable energy in smart microgrid”, in Proceedings of IEEE SmartGridComm, ,Oct. 2011.

[9] A. Ghassemi, S. Bavarian, and L. Lampe, “Cognitive Radio for Smart Grid Communications”, in Proc. SmartGridComm, 2010.

[10] Z. Zhang, and C.A. Gunter, “Application-Aware Secure Multicast for Power Grid Communications”, Int. J. Security and Networks, Vol. 6, No. 1, 2011.

[11] Lin, H.-Y., Tzeng, W.-G., Shen, S.-T., P. Lin., B.-S., “A Practical Smart Metering System Supporting Privacy Preserving Billing and Load Monitoring. In: Proceedings of International Conference Applied Cryptography and Network Security (ACNS), June 2012.

[12] 박남제, “지능형 전력망 구조의 개인정보 위협 및 보안관리 방안”, Internet & Information Security, 한국인터넷진흥원, 제3권 제2호, 3-17, 2012년.

저 자 약 력

김 미 희

이메일 : mhkim@hknu.ac.kr

- 1997년 이화여자대학교 전자계산학과(학사)
- 1999년 이화여자대학교 컴퓨터학과(석사)
- 1999년–2003년 한국전자통신연구원 연구원
- 2007년 이화여자대학교 컴퓨터공학과(박사)
- 2007년–2009년 이화여자대학교 컴퓨터공학과 전임강사
- 2009년–2010년 미국 North Carolina State University Postdoc Researcher
- 2011년–현재 국립한경대학교 컴퓨터웹정보공학과 조교수
- 관심분야 : 무선 네트워크 보안, 네트워크 프로토콜 설계