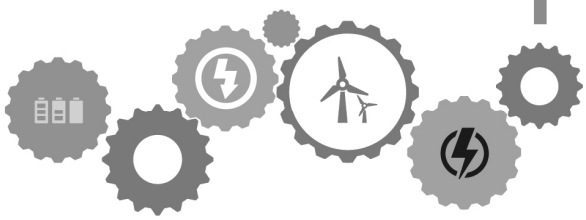
DOI http://dx.doi.org/10.18770/KEPCO.2017.03.02.073

AMI의 보안 취약성 및 기술 현황

Security Vulnerability and Technology Status of AMI

광주과학기술원 Commuications and Computing Lab. (CCL)
조한성, 이용구, 정상인, 최진호



Abstract

Recently, a number of foreign electric power companies including domestic Korea Electric Power Corporation (KEPCO) have actively engaged in the construction of a power grid with the concept of a smart grid. The Smart grid is a technology that increases the efficiency of the power by converging the information network with the power grid. It can maximize the energy efficiency through the two-way communication between the utility and the consumer. However, as the power grid converges with the information and communication network, security threats are increasing more than existing power grids. Due to the nature of the power grid, the damage caused by security threats is not only personal privacy but also economic loss of society. So smart grid becomes the target of hackers. In this paper, we discuss security vulnerabilities of Advanced Metering Infrastructure (AMI), which is a core technology of smart grid construction, and the corresponding security technologies to prevent security damage of smart grid.

최근 국내의 한전을 비롯한 해외 여러 전력회사에서 스마트 그리드라는 개념의 전력망 구축을 위한 활동이 활발하게 이루어지고 있다. 스마트 그리드는 전력망에 정보통신망을 융합하여 전력의 효율성을 증대시키는 기술로, 전력 사업자와 소비자가 양방향 통신을 통해 에너지 효율을 극대화 시킬 수 있다. 그러나 전력망이 정보통신망과 융합되면서 기존 전력망보다 보안의 위협이 증대되고 있다. 전력망 특성상 보안의 위협으로 인한 피해는 개인의 사생활뿐만 아니라 사회의 경제적 손실까지 이어져 그 피해규모가 크므로, 스마트 그리드는 여러 해커 집단의 공격 대상이 되고 있다. 본 논문에서는 스마트 그리드의 보안 피해를 예방하기 위해, 스마트 그리드 구축의 핵심 기술이라 할 수 있는 Advanced Metering Infrastructure (AMI)의 보안 취약점과 그에 대응하는 보안 기술 현황을 살펴보도록 한다.

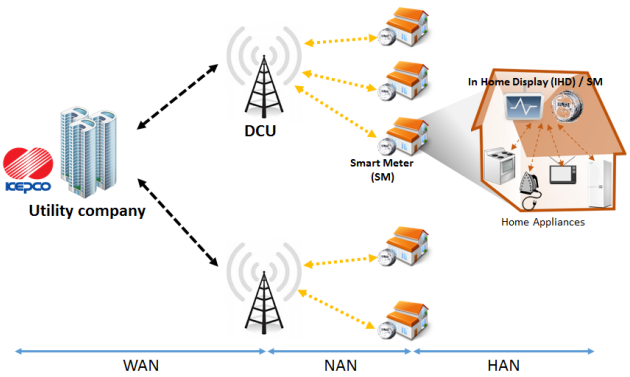
Keywords *: Smart Grid, Advanced Metering Infrastructure, AMI, Security*

I. INTRODUCTION

전 세계적으로 에너지 자원의 고갈에 따라 전력 사용을 효율적으로 관리하는 문제가 주목 받고 있다 [1]. 이에 따라 스마트 그리드라는 차세대 지능형 전력망의 구축 및 관련 기술 개발이 국내외에서 활발하게 이루어지고 있다. 스마트 그리드는 기존의 전력망에 ICT 기술을 접목하여 전력 공급자와 소비자가 양방향으로 실시간 정보를 교환하게 함으로써 에너지 효율을 최대화하는 기술이다.

전력망과 ICT 기술과의 융합은 에너지 측면에서는 효과적일 수 있으나, 보안 측면에서는 여러 위협 요인들을 증가시킨다. 스마트 그리드는 전력 공급 및 수요 상황 예측뿐만 아니라 원격 관제가 가능하기 때문에 네트워크를 통한 사이버 해킹에 의해 정전이 발생할 수 있다. 특히 가정 AMI의 경우 전력 사용량을 조작하여 금전적인 이득을 취할 수 있으며 이는 사회적 경제 손실로 이어질 수 있다. 또한 전력 소비 패턴 유출을 통한 개인의 사생활 침해가 우려된다 [2]-[4]. 따라서 스마트 그리드 구축에 앞서 보안 대책이 뒷받침되어야 한다.

이에 따라 본 논문에서는 스마트 그리드의 핵심 역할을 하는 AMI의 보안에 대하여 살펴보고자 한다. 논문의 내용은 다음과 같이 구성



| Fig. 1 | AMI 구조

하였다. II 장에서는 AMI의 간단한 설명과 함께 보안 취약점 및 보안 공격 종류에 대해 알아본다. 또한 이에 따른 실제 피해 사례에 대해 살펴볼 것이다. III 장에서는 앞서 정리한 보안 위협에 대처하기 위한 AMI의 보안 표준 기술을 국내와 국외로 나누어 살펴볼 것이다. 마지막으로 IV 장에서 결론을 맺는다.

II. AMI 보안

A. AMI 개요

AMI는 자동검침 (AMR)에서 발전된 양방향 원격검침시스템으로서 유무선 통신을 이용해 전력 소비자와 전력회사 사이를 연결해주는 서비스 기반을 일컫는다 [5]. 이는 스마트 그리드 실현에 있어서 핵심 역할을 하며, 미래 지능형 전력망 운용을 위해 최우선적으로 구축되어야 한다. AMI의 주요 구성요소로는 스마트 미터, 가정 내 디스플레이 (IHD), 데이터 집중 장치 (DCU) 등이 있다. 스마트 미터란 사용가의 에너지 사용량을 실시간으로 측정하고 계량 정보를 공급자 및 사용자에게 제공하여, 가격 정보에 대응해 에너지 효율 향상 및 수용가의 에너지 사용을 적정하게 제어할 수 있는 기능을 갖춘 디지털 전자식 계량기이다 [6]. IHD란 전력 회사의 고객들이 차트 또는 그래프의 형태로 시간당 사용한 전력량 등을 확인할 수 있도록 해주는 장치이다. IHD는 고객이 원하는 다양한 에너지 관련 정보를 소비자에게 제공하고, 전력회사로부터 과금 정보 및 에너지 가격 정보 등을 받아 소비자로 하여금 에너지 소비패턴을 관리할 수 있도록 한다 [7]. DCU는 AMI 네트워크 구축을 위해 다기종의 스마트미터와 IHD 등을 다양한 유무선 통신으로 네트워킹 할 수 있는 장치이다. 이 장치는 측정된 에너지 사용 데이터를 모으고, 이 데이터를 분석 및 전력회사에게 전달해 가격을 책정할 수 있도록 한다 [8]. DCU의 양방향 통신 기능 덕분에 사용자는 실시간으로 에너지 사용에 대한 분석 및 가격 정보를 제공 받을 수 있으며 각종 전력 관련 서비스를 제공 받을 수 있다. Fig. 1은 AMI의 구조이다.

AMI는 전력회사와 DCU 사이의 데이터 통신을 위한 Wide Area Network (WAN), DCU와 스마트미터를 연결하기 위한 Neighborhood Area Network (NAN), 그리고 스마트미터와 가전기기 사이를 연결하기 위한 Home Area Network (HAN)로 이루어져 있다. WAN은

| Table 1 | AMI 보안 취약요소

취약요소	설명
Plaintext NAN Traffic	• NAN에서 암호화되지 않은 평문 전송
Bus Snooping	• 하드웨어에 접근하여 직접 정보 획득 • 직렬 버스로부터 통신 정보 획득
Improper Cryptography	• 키 생성 알고리즘 및 암호화 취약 • 키수열 재사용 및 짧은 키 사용, 부적절한 initial vector (IV) 사용
Direct Tampering	• 직접적인 하드웨어 접근을 차단하기 위한 Tamper-Protection 기능의 취약점
Stored Keys and Passwords	• 인증, 암호화 등을 위해 미터기에 저장된 패스워드와 키의 노출 가능성
Cryptographic Key Distribution	• 훔친 키나 검증되지 않은 인증서로 통신 내용 복호화 가능
Insecure Primary Interfaces	• 적외선 통신의 보안 취약점
Meter Authentication Weaknesses	• 미터기가 NAN 장치의 인증을 받는 절차에서 비롯되는 취약점
NAN Authentication Weaknesses	• NAN 장치가 미터기의 인증을 받는 절차에서 비롯되는 취약점
Firmware Implementation Flaws	• 펌웨어 구현상의 오류는 서비스 거부, 기기의 비정상적인 작동 등으로 연결
Name Resolution Deficiencies	• DNS와 같은 프로토콜이 정교한 수준의 보안까지 설계되지 않는 것에서 비롯되는 취약점
Weak Default Configuration Properties	• 보안 설정을 사용자에게 위임하는 기기들의 경우, 부적절한 환경 설정에서 비롯되는 취약점
Traffic Routing Deficiencies	• 통신 경로를 정할 때, 해커가 중간에 자신을 거치도록 하는데서 비롯되는 취약점
Denial of Service Threats	• 서비스 거부 공격을 통해 리소스를 독점하거나 다른 사용자의 이용을 방해
Information Disclosure Threats	• 일부 통신에서 헤더, 트레일러, 인증 값 등이 평문으로 전송되는 것에서 비롯되는 취약점
Static Authentication Credentials	• 변경되지 않는 고정된 인증서 및 암호키를 사용하는 경우에서 비롯되는 취약점
Deficient Random Number Generators	• 현실적으로 난수 구현의 어려움에서 비롯되는 취약점
Network Time Services	• 시스템간 동기화를 위해 쓰이는 network time protocol (NTP)와 global positioning system (GPS)에서 비롯되는 취약점

NAN에서부터 전력회사에 이르기까지 장거리 영역의 통신을 담당하며, 실시간 모니터링, 전력 시스템의 상태 정보를 이용한 실시간 제어 및 보호 어플리케이션 등을 지원한다 [9]. NAN은 배전망과 변전소에서부터 최종 소비자 사이의 데이터 전송을 담당하는 통신 네트워크이다. 즉, NAN은 WAN과 HAN을 연결해주는 중간 역할을 하며, 스마트 미터와 DCU간의 통신 네트워크로 이루어진다. 다수의 HAN과 연결되어 스마트미터로부터 다양한 정보들을 DCU가 저장하고 처리할 수 있도록 하고, 이 정보들을 WAN을 통해 전력회사로 전달해주며, 그 반대의 정보 전송 또한 가능하게 한다 [10][11]. HAN은 스마트미터와 각종 가전기기 간 통신을 위한 네트워크이며, AMI를 구성하는 네트워크의 최하위단으로 WAN과 NAN을 통해 전력회사로부터 효율적인 에너지 분배를 위해 모니터링 되고 제어될 뿐만 아니라 사용자에게 스스로 스마트한 에너지 관리를 할 수 있는 기회를 제공한다 [12][13].

B. AMI 보안 취약요소

본 절에서는 스마트 그리드 중 핵심이라고 할 수 있는 AMI의 보안 취약점에 대해 알아보기로 한다. 2011년 InGuardians사에서 AMI attack methodology라는 문서를 발표하였다 [14]. 이 문서에서는 주로 NAN 영역에서의 AMI 보안 취약점을 18가지로 분류하여 기술하고 설명하고 있다. 각각의 대한 내용을 Table 1에 정리하였다.

C. AMI 보안 공격

앞서 살펴본 보안 취약성으로 인해 해커는 다양한 종류의 AMI 보안 공격이 가능하다. 본 절에서는 AMI에 대한 공격을 3가지로 나누어 살펴보도록 한다.

1) 스마트미터 공격

물리적으로 스마트미터에 접근하여 적절하지 못한 템퍼링 보호 기술을 악용하여 환경설정 정보, 암호화 키, 펌웨어 등 중요한 정보를 추출하는 공격이 있다. 또한 악성코드를 이용하여 주변 스마트미터를 감염시켜 미터의 서비스 거부 공격, 미터의 인가되지 않은 동작 등의 공격이 가능하다. 스마트미터의 ZigBee 통신에서 키 교환시 정보 탈취, 통신 방해를 위한 재밍 공격도 가능하다 [15].

2) DCU 공격

DCU도 스마트미터와 마찬가지로 물리적으로 접근하여 DCU에 저장된 사용자 아이디, 비밀번호, 암호 키 등을 추출할 수 있다. 또한 DCU에 통신망으로 통해 접근한다면 무차별 대입 공격 (Brute Force Attack)으로 아이디, 패스워드 및 디폴트 패스워드 설정과 같은 적절하지 못한 계정 관리 취약점 등을 이용하여 DCU의 관리자 권한 획득이 가능하다. 이렇게 DCU의 관리자 권한을 획득하게 되면, 광범위한 규모의 연결 종료 신호 등 악의적인 스마트미터 제어가 가능하게 되고, 상위 시스템인 Meter Data Management System (MDMS)에 접근할 수 있는 공격 경로로 악용이 가능하다 [16].

3) 유무선 통신 프로토콜 공격

AMI 시스템은 ZigBee, Power Line Communication (PLC) 등 다양한 유무선 통신 기술이 사용되며, 통신 프로토콜을 분석하여 여러 가지의 공격이 가능하다. 패킷 도청을 통해 아이디, 패스워드 정보 및 계량 정보 등을 추출할 수 있으며 패킷 변조를 통해 정보 조작도 가능하다. 또한 채널 소모, 한 개의 노드가 다양한 노드의 역할을 흉내 내는 Sybil 공격, 많은 양의 트래픽을 이용한 서비스 거부 등의 공격도 가능하다. 유무선 통신은 스마트미터, DCU, MDMS 시스템을 연계하기 때문에 보안 중요성이 매우 크다 [16].

D. 스마트그리드 보안 관련 피해 사례

앞서 AMI의 보안 취약점과 그에 따른 해커들의 다양한 방법을 통한 공격에 대하여 살펴보았다. 본 절에서는 스마트그리드의 보안 취약으로 인해 일어난 실제 피해 사례에 대해 살펴보도록 한다.

대표적인 사례로 2010년 스턱스넷을 이용해 이란의 우라늄 농축 시설을 공격하여 원심분리기를 감염시킨 사건과 중국의 1000개의 주요산업 시설에 스턱스넷을 감염시킨 사건이 있다 [17][18]. 스턱스넷이란 전력 제어시스템을 공격하는 악성코드 프로그램으로서 국가의 주요 기반 시설에 혼란을 주는 목적으로 개발되었다. 또한 최근 2015년에 우크라이나에서 사이버 공격으로 인하여 정전 사태가 발생하였다 [19]. 이는 해커들에 의해 대정전이 발생한 사례로서, 3개의 변전소에 대한 일시적인 기능정지를 발생시켜 수십만 가정의 정전을 초래하였다. 이때 해커들은 BlackEnergy로 알려진 트로이 목마 바이러스 malware를 사용한 것으로 추정된다. BlackEnergy는 KillDisk라는 악성코드를 컴퓨터에 심어서 컴퓨터가 부팅을 할 수 없는 상태로 만들어 정전을 유도한다. 주로 메일에 첨부된 Microsoft Office 파일을 통하여 감염된다.

우크라이나 정전 사태와 같은 대규모 테러 사건뿐만 아니라 스마트미터 해킹으로 인한 심각한 경제적인 손실을 초래한 사례도 있다. 2009년 푸에르토리코에서는 전력 계량 미터 제조업체 직원이 미터에 자석으로 바늘이 움직이지 않도록 하여 적외선 통신 포트를 사용해서 스마트미터의 소프트웨어를 바꾸어, 전기 요금이 통상의 50~75%가 되도록 설정을 변경하는 수법으로 전기의 도난이 일어났다. 이로 인해 미터기 한 대당 전기 요금 피해는 약 300~1000 달러에 이른다. FBI에 의하면, 전체 피해가 약 4억 달러에 달할 것으로 추정된다 [20].

푸에르토리코 사례의 가장 근본적인 문제는 사용자 인증 단계에서의 허술함이다. 보다 체계적이고 강력한 인증 프로토콜이 필요하며, 더불어 이를 위한 보안키 전송이 매우 중요하다. 이외에 전력망의 사이버 침해 사건 및 모의 해킹 사례를 Table 2에 정리하였다.

| Table 2 | 전력망 보안 관련 피해 및 모의 해킹 사례 [21]-[26]

시기	사례
2007년	• 전력망 해킹으로 브라질에서 대규모 정전 사태 발생
2009년 3월	• 미국에서 스마트 미터 해킹을 통한 운영센터 침입 사건 발생
2009년 4월	• 미국 전력망 내에 중국, 러시아 사이버 스파이가 설치한 것으로 추정되는 악성 프로그램 발견
2009년 10월	• 미국 제어시스템 보안 학회에서 ZigBee 통신 기반 스마트미터의 데이터 및 암호키를 알아내는 해킹 기술 발표
2010년	• Black Hat에서 무선 통신 감청을 통해 수집한 통신을 재송신(replay) 하는 공격이 가능함을 확인
2016년	• 사이버 공격에 의해 우크라이나 피브니치나 변전소의 전력망 마비되어 수도 키예프에서 대규모 정전 발생

| Table 3 | 국내 AMI 보안 표준 [27]-[32]

표준	내용
KS C IEC 60870-5-104	• ISO/IEC 60870-5-104에 대한 국내 표준 • 표준 전송을 위한 네트워크 접근 규약
KS X ISO/IEC 27001	• ISO/IEC 27001에 대한 국내 표준 • 정보보안 관리시스템에 대한 요구사항
KS C 1231-1	• AMI 환경에서 설치 및 운영되는 전력량계에 대한 표준 • HAN, NAN, WAN에 연결될 수 있는 양방향 통신에 대한 보안
TTAK.KO-12.0182	• 스마트 그리드 모델 정의 및 기술적 측면의 보안 요구사항 도출
TTAK.KO-12.0258	• 스마트 그리드 적용을 위한 HAN 기기 보안 메커니즘
TTAE.IT-X.1111sup26	• 원격검침 기반시설을 중심으로 하는 서비스 구간에서의 보안 기능 구조 정의

III. AMI 보안 기술 현황

A. 국내

국내 여러 기관이 AMI 보안과 관련하여 표준을 제시하고 있다. 국내에서는 스마트그리드협회, KS 스마트그리드 표준화, 한국정보통신기술협회 (TTA) 등에서 표준들을 제시하고 있다. 이는 자체적인 표준과 더불어 해외의 표준들을 국내에 적합하게 적용시키는 것 또한 포함하고 있다. 관련된 국내 표준은 Table 3과 같다.

표준과 더불어 보안 관련 기술 개발도 한창이다. 한전 KDN에서는 국내 최초로 스마트 그리드 분야에 특화된 기기 보안인증 시스템 개발에 완료했다 [33]. 이 기술은 현재 제주도 스마트 그리드 실증단지 및 한전KDN 대전 충남지사 사옥에 실증 테스트베드를 구축 중에 있다. 또한 올해에는 한국전자통신연구원 (ETRI)에서 AMI에서 스마트미터 기기의 인증을 위해 스마트미터 기기와 DCU 사이에 적용되는 네트워크 접속제어 프로토콜 기술을 개발했다 [34]. 이 기술은 기기 간 상호인증 및 키 분배를 제공하는 프로토콜로 국제표준 규격을 준수해 IoT와 같은 경량 기기에서도 동작 가능한 보안 기술이며, 누리텔레콤이 노르웨이에서 수주한 800억원 규모의 해외 AMI 시스템 구축 프로젝트에 적용되었다.

B. 국외

국외에서는 국제 전기 기술위원회 (IEC), 국제 전기전자 기술자협회 (IEEE), UCAIug 등에서 적극적으로 스마트 그리드 보안 관련 표준을 수립하고 있다. IEC는 전력 시스템에 대한 보안 표준 IEC62351 시리즈를 제정했고, IEEE는 스마트 그리드 기기 및 시스템에 관한 보안 표준을 제정하였다. UCAIug는 AMI-SEC라는 팀을 신설하여 AMI에 보안 위협 모델을 연구하고 AMI 보안 요구사항을 작성하여 배포하였다. 또한 AMI-SEC는 여러 전력회사, HomePlug, ZigBee Alliance, IEEE, NIST, EPRI 등의 단체와 연구결과를 공유하고 있다. 미국의 경우 표준기술연구소 (NIST)에서 2007년부터 스마트 그리드 보안 표준 개발을 주도하고 있다. NIST는 AMI를 스마트 그리드 실현을 위한 표준화 선결 추진 대상의 일부로 지정하여 관련 주요 표준 및 가이드라인을 권고하였고, IPv6에 기반한 AMI의 종단 간 통신을 위한 관련 표준의 개정 작업을 Priority Action Plan (PAP)의 하나로 진행 중이다. 유럽의 경우 유럽정보보호원 (ENISA)에서 AMI를 포함한 스마트 그리드 보호를 위한 10가지 보안 권고사항을 발표했다. 또한 EU의 19개 전력회사가 모여 진행 중인 OPEN meter 프로젝트에서는 AMI 구성요소 각각에 대한 보안 요구사항을 포함하는 문서를 발표했다. 이는 스마트미터, 데이터 집중 장치, 미터 관리 시스템 간 통신 시 보안 요구사항으로서 안전한 broadcasting, relay attack 탐지, 보안 관제, 이상 징후 탐지를 제시하였다. 독일 연방정보보안청 (BSI)에서는 스마트미터 게이트웨이 보호 프로파일을 개발하고 이를 EU 표준으로 적용하고 있다. Table 4는 각 기관에서 제시한 표준의 일부를 정리하였다.

IV. 결론

한전은 2020년까지 국내 전기사용고객 2,000만호 전체에 AMI를 구축할 예정이다. AMI는 기존에 비해 효율성이 증가하는 반면 양방향 통신으로 인하여 주변의 기기들과 상호 연결성이 증대되어 분산된 사용자 단에서 전력망 시스템으로 접근할 수 있는 경로가 많아져 보안관리가 쉽지 않다. 특히 무선 통신 기반의 AMI의 경우, 기존 무선 통신의 보안 취약성을 포함하므로 보안 강화가 필수적이다. 따라서

| Table 4 | 국외 AMI 보안 표준 [35]-[40]

표준	내용
IEC 62351 (Part 0 ~ 11)	• 전력시스템 전반에 걸친 종단 간 보안에 대한 구체적인 요구사항 및 아키텍처를 제시 • 정보보안, 통신 프로토콜의 보안위협을 제거하기 위한 보안 대책 표준 등 전반적인 스마트 그리드 보안 표준 제시
IEEE 1686-2013	• 접근, 운영, 구성, 데이터 검색에 대한 보안 등을 다룸 • 필요한 보안 표준을 불만족시 사용자에게 경고
NIST SP 800-53	• 보안제어, 사용되는 기술 등에 대한 세부적인 보안 지침 제공 • 의도한 보안 요구사항에 부합 여부 진단 지침 제공
NIST SP 800-82	• 산업제어시스템 보안을 위한 가이드 정의 • 네트워크 구조, 관리, 운영에 대한 보안통제 등을 포함
NISTIR 7628	• 새로운 상호 의존성과 취약성 공개 • 위험 평가 및 적절한 보안 요구사항을 적용하고 파악하기 위한 지침 제시
BSI-CC-PP-0077	• 스마트미터 게이트웨이의 보안 모듈을 위한 표준

스마트 그리드 구축에 앞서 스마트 그리드의 핵심 역할을 하는 AMI의 보안 취약점을 점검하고 관련 규정 제정 및 기술개발이 필요하다.

본 논문에서는 AMI의 보안 취약점과 여러 유형의 공격 및 실제 피해 사례에 대해 먼저 살펴보았으며, 이에 대한 국내외 보안 관련 표준 및 기술들에 대해 알아보았다. 본 논문에서 정리한 내용을 통해, 다가올 AMI는 기존의 보안을 보강하는 강력하고 원천적인 보안이 필요할 것으로 예상된다.

ACKNOWLEDGEMENT

This research was supported by Korea Electric Power Corporation(Grant number : R15XA03-60)

본 연구는 한국전력공사의 2016년 선정 기초연구개발과제 연구비에 의해 지원되었음(과제번호: R15XA03-60)

REFERENCES

[1] Farhangi, Hassan. “The path of the smart grid.” IEEE power and energy magazine 8.1 (2010).

[2] McDaniel, Patrick, and Stephen McLaughlin. "Security and privacy challenges in the smart grid." IEEE Security & Privacy 7.3 (2009).

[3] Khurana, Himanshu, et al. “Smart-grid security issues.” IEEE Security & Privacy 8.1 (2010).

[4] Anderson, Ross, and Shailendra Fuloria. “Smart meter security: a survey.” University of Cambridge Computer Laboratory, United Kingdom (2011).

[5] Available: http://www.najunews.kr/news/articleView.html?idxno=213258. Accessed on June. 2017.

[6] 이재환, and 조성선. “스마트그리드의 기반 스마트미터 추진 동향 및 시사점, 정보통신산업진흥원.” (2011).

[7] Choi, Tae-Seop, et al. “Analysis of energy savings using smart metering system and IHD (in-home display).” Transmission & Distribution Conference & Exposition: Asia and Pacific, 2009. IEEE, 2009.

[8] Prakash, Punya. “Data concentrators: The core of energy and data management.” White paper, Texas Instruments (2013).

[9] 윤성국, “스마트그리드 통신 네트워크 구성과 전력선 통신의 역할.” 한국통신학회지 (정보와통신) 31.11 (2014): 95-101.

[10] Hossain, Ekram, Zhu Han, and H. Vincent Poor. Smart grid communications and networking. Cambridge University Press, 2012.

[11] Yu, Rong, et al. “Cognitive radio based hierarchical communications infrastructure for smart grid.” IEEE network 25.5 (2011).

[12] Available: http://blogs.gartner.com/it-glossary/home-area-network-han/. Accesed on June. 2017.

[13] Balakrishnan, Meera. “Smart Energy Solutions for Home Area Networks and Grid-End Applications.” Proc. Smart Energy (2012): 67-73.

[14] Carpenter, M., et al. “Advanced metering infrastructure attack methodology.” InGuardians white paper (2009).

[15] 남궁완, et al. “스마트미터 보안 연구.” 정보보호학회지 20.5 (2010): 20-30.

[16] 김신규, 전유석, and 서정택. “AMI 보안 취약점 점검 항목에 관한 연구.” 정보보호학회지 22.5 (2012): 73-78.

[17] Available: http://news.chosun.com/site/data/html_dir/2011/01/17/2011011700132.html. Accessed on June. 2017.

[18] Available: http://www.boannews.com/media/view.asp?idx=23041. Accessed on June. 2017.

[19] Available: http://thehackernews.com/2016/01/Ukraine-power-system-hacked.html. Accessed on June. 2017.

[20] Available: https://krebsonsecurity.com/2012/04/fbi-smart-meter-hacks-likely-to-spread/.Accessed on June. 2017.

[21] Available: https://phys.org/news/2009-11-brazil-blackouts-

result-cyber-hacking.html. Accessed on June. 2017.
[22] Available: http://www.boannews.com/plan/plan_view.asp?idx=20523. Accessed on June. 2017.
[23] Available: http://www.koreatimes.com/article/20090409/515926. Accessed on June. 2017.
[24] Travis Goodspeed, "AMI Hacking Demonstration", Control System Cyber Security Conference 2009, Oct. 2009.
[25] Available: http://www.blackhat.com/html/bh-us-10/bh-us-10-home.html. Accessed on June. 2017
[26] Available: https://www.cyberscoop.com/blackout-ukraine-probably-bigger-deal-think/. Accessed on June. 2017.
[27] Telecontrol equipment and systems - Part 5 - 104 : Transmission protocols - Network access for KS C IEC 60870 - 5 - 101 using standard transport profiles. KS C IEC 60870-5-104. 2012.
[28] Information technology — Security techniques — Information security management systems — Requirements. KS X ISO/IEC 27001. 2014.
[29] The Smart Meter - Part 1 : Function requirements. KS C 1231-1. 2016
[30] Security Requirements for Smart Grid. TTAK.KO-12.0182. 2011.
[31] Security Mechanism of HAN Devices for Smart Grid. TTAK. KO-12.0258. 2014.
[32] Security functional architecture for smart grid services using telecommunication networks. TTAE.IT-X.1111sup26. 2016.
[33] Available: http://www.koit.co.kr/news/articleView.html?idxno=60595. Accessed on June. 2017.
[34] Available: http://www.etnews.com/20170328000244. Accessed on June. 2017.
[35] Security Standards for the Power System Information Infrastructure. IEC 62351. 2012.
[36] IEEE Standards for Intelligent Electronic Devices Cyber Security Capabilities. IEEE Std 1686-2013. 2014.
[37] Security and Privacy Controls for Federal Information Systems and Organizations. NIST SP 800-53. 2013.
[38] Guide to Industrial Control Systems (ICS) Security. NIST SP 800-82. 2011.
[39] Guidelines for Smart Grid Cybersecurity. NISTIR 7628. 2014.
[40] Protection Profile for the Security Module of a Smart Metering System. BSI-CC-PP-0077-2013. 2013.