情 報 保 護 學 會 誌
第20卷 第5號, 2010. 10

스마트미터 보안 연구

남 궁 완*, 조 효 진*, 조 관 태*, 이 동 훈*

요 약

최근 기존의 전력시스템과 IT기술을 융합한 차세대 지능형 전력시스템인 스마트그리드 개발이 활발하게 이루어지고 있다. 스마트그리드의 핵심 구성요소인 스마트미터는 실시간으로 사용되는 에너지를 측정하여 사용자에게 제공되며 에너지를 효율적으로 사용하도록 도와준다. 또한 에너지공급업체는 스마트미터를 이용한 수요 반응 기술(Demand Response)을 통해 소비자의 능동적인 전력시장 참여를 유도하여 효율적인 에너지 사용이 가능하게 한다. 하지만 네트워크로 연결된 스마트미터는 기존의 네트워크시스템이 가지고 있는 보안 취약점을 가지고 있기 때문에 이에 강건한 보안메커니즘을 통해서 안전하게 보호되어야 한다. 본 논문에서는 세계 주요 국가에서의 스마트미터 보급 동향과 스마트미터가 가지고 있는 보안 위협들을 분석하고 대응책을 기술한다.

Ⅰ. 서 론

저탄소 녹색성장이 주목받으면서 산업시설의 효율적인 관리를 통해 탄소배출을 줄이고자 하는 움직임이 일고 있다. 효율적인 관리를 위해 IT기술 적용이 필수요소로 부각되면서, 기존 전력망에 IT기술을 적용한 스마트그리드가 주목받고 있다. 이에 따라 각 국가에서는 그린-IT를 추구하기 위하여 스마트그리드를 추진하고 있다. 지능형 전력망이라고 불리는 스마트그리드는 차세대 전력망으로 전력 시스템과 정보통신기술이 융합된 기술이다. 스마트그리드에서는 전기로 작동되는 모든 기기들이 유·무선 네트워크로 연결되며, 서로간의 정보교환을 통하여 유기적인 관계로 이루어진다. 현재 전력시스템은 에너지소요예측이 불가능하기 때문에 일반적으로 10%의 예비전력을 보유한다. 하지만 스마트그리드 환경에서는 스마트미터를 통해 실시간으로 사용되는 에너지를 분석함으로써 에너지를 효율적으로 분배할 수 있다.

스마트 그리드의 표준화는 현재 초기 단계로, 미국의 전력연구원(Electric Power Research Institute, EPRI)와 국립표준기술연구원(National Institute of Standard and Technology, NIST)을 중심으로 국제전자기술위원회(International Electrotechnical Commission, IEC)와 국제전기전자기술자협회(Institute of Electrical and Electronics Engineers, IEEE), 국제표준화기구(International Organization for Standardization, ISO), OpenAMI에서 전력관리 기술 및 전력망 보안기술에 대한 표준을 추진하고 있으며, 이에 더하여 전력연구원와 국립표준기술연구원은 스마트그리드 표준 프레임워크에 대한 상호운용성 표준을 진행하고 있다. 또한 국제표준화기구와 국제전기통신연합(International Telecommunication Union, ITU)을 중심으로 스마트그리드의 IT분야 국제 표준을 진행 중이다[2].

스마트미터는 스마트그리드에서 중요한 역할을 하는 필수구성요소로 자동으로 에너지를 계량 및 관리하는 기기를 말한다. 스마트미터는 사용되는 에너지를 실시간 체크하여 관련 데이터를 저장하며, 저장된 데이터는 사용자 또는 에너지공급업자에게 제공된다. 사용자는 현재까지 사용된 에너지 정보를 제공받음으로써 능동적인 전력소비에 참여할 수 있고, 에너지공급업자는 스마트미터에서 수집된 데이터를 통해 에너지수요현황을 파악함으로써 유동적인 전력 요금의 책정이 가능하다.

스마트미터의 표준은 스마트그리드의 일환으로 미국, EU 등의 주도하에 빠르게 진척되고 있다. 미국은 전력연구원(EPRI)와 국립표준기술연구원(NIST)을 중심으로 추진 중인 스마트그리드 내 AMI 관련사항을 언급하

* 고려대학교 정보경영공학전문대학원 ({ngw5608, mellmany, ckt27, donghlee}@korea.ac.kr)

고 있으며, 스마트미터는 미국표준협회(American National Standard Institute, ANSI)의 기술표준을 따른다. 또한 EU는 19개 전력회사를 중심으로 스마트미터 표준화 작업을 진행 중이며, OPEN(Open and Public Extend Network)Meter 협력조직에서 AMI(Advanced Metering Infrastructure) 스마트미터의 구성요소에 대한 기능, 통신, 네트워크관리, 보안적인 측면에 대한 표준을 추진 중 이다 [1][6][22].

최근 스마트그리드에 대한 사업이 확장됨에 따라 스마트미터 보안에 대한 관심 역시 높아지고 있다. 미국의 산업분석가인 Bob Lockhart는 "스마트미터는 스마트그리드시스템에서 높은 보안 문제점을 가지고 있다"고 언급했으며, 미국의 보안 컨설팅 업체인 IOActive는 "전기 및 소프트웨어에 대한 지식과 500달러짜리 장비를 이용하여 스마트미터를 조종할 수 있다"고 경고하였다[19][21]. 스마트미터는 현재 미터기가 위치한 댁외에 설치되기 때문에 물리적 공격에 취약하며, 거대한 네트워크로 구성된 스마트미터는 기존의 LAN공격에 취약하다. 뿐만 아니라 스마트미터를 통해 수집되는 데이터들은 사용자의 프라이버시를 침해할 수 있는 민감한 정보를 포함하고 있다. 따라서 정부를 비롯한 에너지관련 업자 및 네트워크관련업자들은 스마트미터의 보안이 필요하다고 여긴다. 미국의 Pike Research 연구조사에 따르면 세계적으로 2010년부터 2015년까지 스마트미터 보안을 위하여 총 575백만 달러(6,880억 원)가 투자될 것으로 예상된다고 밝혔다[21].

스마트미터 보안 관련 연구를 살펴보면, AMI에서 발생 가능한 사이버 보안 이슈[9][10]와 전력데이터와 관련 소비자 프라이버시 문제에 관한 연구[8]가 존재한다. 또한 미국 국립 SCADA(Supervisory Control And Data Acquisition) 테스트 베드(National SCADA Test Bed, NSTB)와 전력연구소(EPRI)에서 추진 중인 프로그램을 살펴보면, 잠재적인 위협 분석, 주요 보안 정보의 보급, IT기술과의 통합으로 인한 전력 시스템의 보안의 취약성 등이 언급되고 있다[3].

본 논문에서는 안전한 스마트미터 시스템을 위한 스마트미터보안에 초점을 둔다. 논문의 구성은 스마트미터에 대한 이해를 돕기 위해 국가별 스마트미터 구축 현황과 스마트미터의 특징 및 구성에 대해 살펴보고, 스마트미터보안의 요구사항과 위협 및 대응방안을 분석한다.

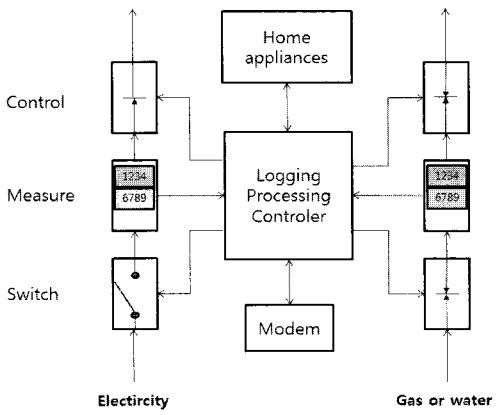
Ⅱ. 스마트미터의 특징 및 구성

2.1 스마트미터 정의

전통적인 미터시스템은 전자 방식으로 사용되는 에너지의 양을 측정하며, 한 달 또는 두 달에 한번 미터기에 기록된 전력량을 전기검침원에 의해서 직접 체크한다. 이에 반해 스마트미터는 실시간 에너지측정 및 양방향 통신이 가능하도록 설계된 미터기이다. 스마트미터는 에너지공급업자 및 시스템운영업자와 거대한 네트워크를 형성하며, 사용되는 에너지에 대하여 원격으로 요금이 청구된다. 또한 에너지공급업자는 유동적인 전력요금 책정을 위해 스마트미터를 이용하여 10분에서 최대 1시간 간격으로 데이터를 수집하여 기록한다. 스마트미터기는 시간대별로 측정되는 전력 요금과 현재까지 사용한 에너지사용료에 대한 정보를 사용자에게 제공한다. 또한 스마트미터는 플랫폼의 무결성을 위해 에너지공급업자에 의해 플랫폼 상태가 관리되어야한다. 따라서 에너지공급업자는 스마트미터 내부의 기능적 문제가 생겼을 경우 펌웨어를 업데이트하거나, 갑작스러운 에너지공급중단 현상이 발생할 경우 댁내에 저장되어있는 임시 배터리로 전환시킬 수 있다[1][16][20][23].

위에서 언급한 스마트미터의 특징을 다음과 같이 요약할 수 있다.

- 양방향 전력량 계량
- 메모리무단접근 감지 기능
- 유효전력량(kWh), 무효전력량(kVarh) 계측



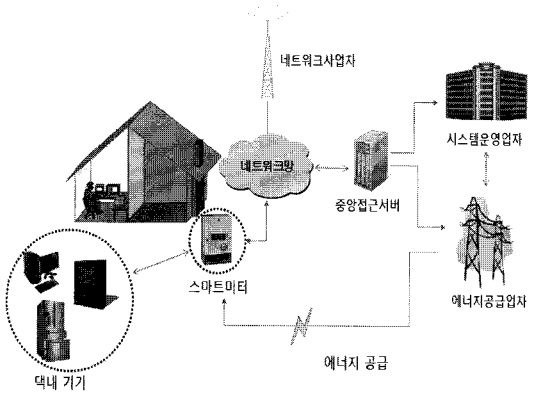
〔그림 1〕 스마트 미터 내부 구조

- 최대수요전력 제한기능
- 원격 관리 지원

2.2 스마트미터 시스템 구조

스마트미터를 통해 수집되는 데이터는 사용자뿐만 아니라 에너지공급업자에게도 유용한 정보를 제공한다. 에너지공급업자는 현재 계측을 하기 위해 사용되는 인력을 절감 할 수 있으며, 주기적으로 에너지소비현황을 분석함으로써 시간대별 에너지 수요를 보다 정확히 예측할 수 있다. 또한 요구되는 에너지양에 맞춰 에너지생산을 조정할 수 있기 때문에 에너지생산비용절감의 효과를 가진다.

스마트미터 시스템은 [그림 2]와 같은 구성요소로 이루어져 있다.[1] 우선 각 가정에서 에너지를 사용하는 사용자가 있으며, 스마트미터를 관리하고 에너지수요에 맞춰 공급해 주는 에너지공급업자가 존재한다, 또한 스마트미터는 네트워크를 통해 연결되기 때문에 스마트미터 시스템을 관리하는 시스템운영업자와 네트워크사업자가 존재한다. 스마트미터 시스템을 세부적으로 살펴보면, 마이크로컨트롤러를 통해서 사용되는 에너지를 계량하고 저장하는 스마트미터기가 있으며, 스마트미터를 통해 수집되는 데이터들을 효율적으로 저장, 관리하는 중앙접근서버[2]가 존재한다. 중앙접근서버를 통해서



〔그림 2〕 스마트미터 시스템 구조

1) 스마트미터 시스템의 국제표준이 아직 지정되지 않았기 때문에 네덜란드 스마트미터 시스템 구축사례를 통해서 구성요소를 소개한다[18].

2) 네덜란드 스마트미터 구축사례를 살펴보면 여러 개의 스마트미터로부터 데이터를 중앙접근서버(Central Access Server, CAS)통해 수집하여 저장한다[18].

에너지공급업자 및 시스템운영업자들은 데이터를 전송받는다. 또한 스마트미터는 여러 개의 포트를 통해서 댁내-스마트미터, 스마트미터-중앙접근서버, 스마트미터-기타외부장치 간의 통신을 지원한다[11][13][14][18].

Ⅲ. 국가별 스마트미터 보급 동향

3.1 국내

우리나라는 에너지 비용의 감소, 신재생에너지 발전, 국제경쟁력 확보의 목적으로 스마트그리드를 활발히 추진하고 있다. 2009년 6월 제주도 6000호를 대상으로 스마트그리드 시범단지를 추진하고 있다. 현재 전기연구원, 한전 등을 주축으로 2010년 12월까지 약 600억원을 투자할 계획이며, 2010년부터 기술 실증을 시작하여 2030년까지 스마트그리드시스템을 완료할 계획이다[6].

국내 스마트미터 보급 추진은 2020년까지 전체 가구에 보급할 계획이며, LS산전, 누리텔레콤 등을 통해 추진하고 있다. 지식경제부에서 발표한 보급 예정인 스마트미터는 [표 1]와 같이 두 가지 타입이 존재한다[5].

3.2 북미

미국은 에너지 효율과 절감을 위한 스마트그리드 사업을 통해 스마트미터 시스템 구축에 선두로 나서고 있다. 현재 캘리포니아 주를 중심으로 스마트미터 보급이 빠른 속도로 이루어지고 있으며, 전체에 보급된 스마트미터 1,000만대 중 600만대가 캘리포니아 주에 도입되었다. 시장조사기관인 Seed Planning의 스마트그리드 구축계획 자료에 따르면 스마트미터가 2025년까지 5,800만대가 보급될 것으로 예상된다.

〔표 1〕 보급 예정인 스마트미터 〈출처: 지식경제부〉

구분	활용대상	점유율	검침범위
		대수	주요기능
경제형	주택용(300kWh 미만), 2만원	56%	소비전력량
		1,000만대	원격검침, 시간별(1시간)·통신
일반형	300kWh이상 주택, 상가, 심야 용, 5만원 이상	44%	피크전력 계량
		800만대	원격검침, 시간별(15분)·통신

〔표 2〕 국가별 스마트미터 구축 계획 〈출처: Seed Planning 2009〉

(단위:1,000대)

국가	~2009	2010	2012	2014	2016	2018	2020	누계
미국	3800	7000	10000	22000	10000	3000	3000	58800
아일랜드	200	500	1100					1800
영국	50	50	100	1000	3000	6500	5000	16000
이탈리아	25000	3000						28000
오스트리아	20	100	200	400	800	900	800	3260
네덜란드	35	100	300	1600	2000	1000		5050
스웨덴	3800							3800
스페인	0	0	10	40	2400	2000	2000	6450
체코	5	10	40	100	400	800	1000	2500
덴마크	500	500	1000	200				2200
독일	10	10	10	300	600	1200	4000	10000
헝가리	1	25	60	80	150	300		620
핀란드	1000	800	200	150				2150
프랑스	50	50	3000	10000	10000			23100
벨기에	0	0	0	0	100	600	2000	4300
중국	0	0	0	100	400	800	1600	8000

캐나다는 온타리오 주의 전력회사인 Hydro One을 중심으로 스마트미터 보급을 추진하고 있다. 스마트미터는 2006년부터 보급하기 시작하였으며, 2009년 8월 기준으로 120만개가 보급되었다. Hydro One에서 발표한 내용에 따르면 2025년까지 자사의 전력시스템을 스마트그리드에 맞춰 업그레이드하며, 2010년까지 전역에 스마트미터를 보급할 계획이다[7].

3.3 유럽

EU는 2020년 이전에 가정의 80%이상 스마트미터를 보급하려는 계획을 가지고 있다. 이에 따라 이탈리아의 Enel사의 주도로 AMI프로젝트를 수행하고 있으며, 스웨덴, 덴마크, 핀란드를 비롯한 북유럽 국가들도 이에 맞춰 스마트미터 시스템 구축을 빠르게 추진하고 있다. 이탈리아는 1999년에 AMI프로젝트를 시작하여 2011년까지 전체 3600만 가구에 대해 스마트미터를 보급할 계획이다. 스웨덴은 2009년 모든 전력계량기의 자동검침을 의무화함으로써 스마트미터 시스템 구축의 발판을 마련하였고, 2009년까지 스마트미터 보급을 완료할 계획이다. 덴마크는 최적화된 스마트미터 시스템 구축을 위해 스마트미터 보급을 꾸준히 추진하고 있으며, Seed Planning이 발표한 자료에 의하면 2009년을 시점으로 매년 50만대씩 보급되어, 2014년까지 220만대가량 보급될 계획이다. 핀란드는 2014년까지 전 가구에 대해 스마트미터 설치를 의무화 하며, 2009년에 100만 가구에 대해 스마트미터 설치할 계획이다.

그 밖의 주요 선진국에서도 스마트미터 시스템을 구축하고 있다. 영국에서는 2009년을 시작으로 2020년까지 전체 2,600만 가구에 스마트미터를 보급할 계획이다. 프랑스에서는 배전회사인 eRDF(European Regional Development Fund)사를 통해서 2012년~2017까지 3,300만 가구에 스마트미터를 보급할 계획을 발표하였다[7].

3.4 아시아/오세아니아

중국은 2005년 '온라인 검침장치 혁명 프로젝트'를 통해 스마트그리드 시스템 구축의 발판을 마련하였다. 중국은 2010년까지 약 1억 개의 전자식미터를 보급할 계획이며, 2014년부터 본격적으로 스마트미터가 설치될 예정이다. 인도는 2008년 Saab Grintek에 의해 뉴델리 지역 스마트미터 보급 및 스마트미터 시스템 구축을 진행하고 있으며, 2012년까지 1,000억 달러를 스마트그리드 인프라 구축에 투자할 계획이다. 호주는 2009년 9월부터 빅토리아 주를 중심으로 스마트미터 보급 및

스마트미터 시스템 구축을 시작하였으며, 2013년까지 빅토리아 주 전체에 스마트미터를 보급할 계획이다. 일본은 태양열에너지를 사용하는 스마트그리드 개발을 추진하고 있으며, 2009년 하반기부터 스마트미터 시스템 구축 프로젝트를 시행 중이다. 그밖에 인도네시아, 싱가포르, 태국을 비롯한 많은 나라에서도 스마트그리드 사업이 추진되고 있으며, 지속적으로 확대되고 있다[7].

Ⅳ. 스마트미터 보안 위협

본 장에서는 스마트미터를 사용하는 스마트그리드 환경에서 발생 가능한 위협들을 서술한다. 위협은 [그림 3]과 같이 크게 2가지로 나뉘며, 사용자 또는 에너지공급업자의 사적인 이익을 위하여 스마트미터에 접근하는 내부위협과 제 3자의 악의적인 목적으로 에너지공급 시스템에 영향을 끼치는 외부위협이 있다.

4.1 내부위협

4.1.1 사용자 사기 유형

전통적인 에너지공급방식에서 에너지 사용료를 산출하는 주체는 에너지공급업자이다. 따라서 사용자는 에너지공급업자로부터 일방적으로 산출된 에너지사용료를 지불하기 때문에 사용자는 에너지사용량을 조작할 수 없다. 하지만 스마트그리드 환경에서 스마트미터는 사용되는 에너지에 대한 데이터가 저장되며, 네트워크를 통해 연결되어 사용자에게 정보를 제공한다. 만약 사용자가 자신이 사용한 에너지의 양보다 적은 비용을 지불하고 싶다면, 물리적 또는 네트워크 해킹기술을 이용하여 스마트미터에 저장된 데이터를 수정할 수 있다. 또한 스마트미터 내부에 작동되는 펌웨어를 수정하여 사용자에게 유리하게 작동되도록 변경할 수 있다. 이러한 공격은 사용자에게 스마트미터에 대한 모든 권한이 주어졌을 때 쉽게 가능하며, 물리적으로 스마트미터에 접근하여 역공학을 이용한 공격을 통하여 이루어 질 수 있다[15].

4.1.2 사업자 사기 유형

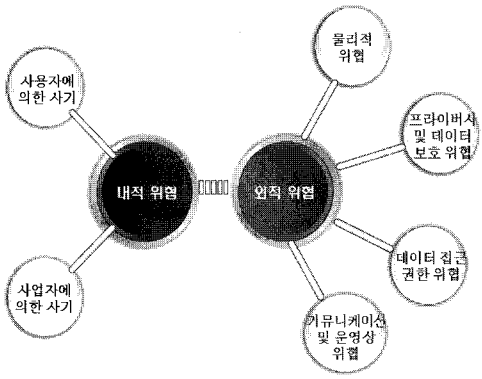
스마트미터를 통해 수집되는 데이터들은 사용자 이외에 에너지공급업자 및 에너지제공업자에게 제공되며, 이 데이터를 에너지 사용료를 산출하는데 이용한다. 하지만 데이터를 제공받는 에너지공급업자는 수익을 올리기 위하여 사용자에게 거짓된 정보를 제공하고, 잘못된 에너지사용료를 청구할 수 있다. 예를 들어 에너지공급업자가 요금이 가장 비싼 시간의 사용료를 변경하여 사용자에게 제공하거나, 요금이 가장 비싼 시간에 더 많은 에너지를 사용한 것처럼 속일 수 있다. 이러한 공격은 물리적인 공격으로 시스템에 접근하거나 관리자 권한을 가진 아이디를 통해서 이루어질 수 있다[15].

4.2 외부위협

4.2.1 물리적 위협

스마트미터는 댁외에 설치되기 때문에 권한을 가지지 않은 공격자에게 쉽게 노출된다. 스마트미터 내부에는 에너지 사용을 측정하기 위한 마이크로컨트롤러가 있으며, 올바르게 작동될 수 있도록 펌웨어가 실행된다. 따라서 공격자는 스마트미터를 악의적인 목적으로 사용하기 위하여 마이크로컨트롤러와 펌웨어에 접근해 조작하기를 원한다[12].

공격자는 여러 가지 방식을 이용하여 스마트미터를 공격할 수 있다. 가장 단순하지만 강력한 공격은 물리적 접근을 통하여 스마트미터에 저장된 데이터에 접근하는 것이다. 예를 들어 스마트미터에 물리적 보안장치가 존재하지 않는다면, 공격자는 스마트미터 내부에 위치한 램을 공격하여 스마트미터를 공격자가 조종 가능한 형태로 설정할 수 있다. 공격자는 바늘을 이용하여 메모리 칩의 전기신호를 감지하고, 분석하여 스마트미터를 조종할 수 있다. 또한 스마트미터 내부에 존재하는 에너지



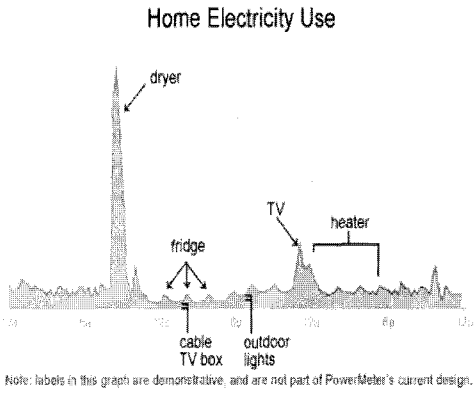
〔그림 3〕 스마트미터 시스템의 예상되는 위협

망과 스마트미터의 양방향 통신을 위한 칩에 대해 물리적인 해킹을 시도하여 보안코드를 얻어낼 수 있다. 얻어낸 보안코드는 에너지공급 네트워크에 접근하는데 사용되어 에너지공급 시스템 전체에 큰 영향을 미치게 된다. 또한 공격자가 스마트미터에 악성 코드를 감염시킬 수 있다. 감염된 악성코드는 다른 스마트미터 및 에너지공급 시스템 전체에 전파되어 시스템 전체의 모든 데이터가 노출되거나 광범위한 지역의 에너지공급중단 등의 치명적인 위험이 발생시킨다. 만약 공격자가 물리적으로 접근 가능할 경우, 공격자는 스마트미터에 악성코드를 감염시켜 스마트미터 내부에 저장된 데이터를 얻을 수 있을 뿐만 아니라 이후에 사용되는 에너지에 대한 데이터를 얻을 수 있다. 또한 악성코드는 다른 스마트미터에 전파되어 전체시스템네트워크에 영향을 주게 된다. 이러한 공격은 서비스 거부(Denial-of-Service, DoS)공격의 원인이 되어 대규모 에너지공급중단이 초래되기도 한다[4][12].

4.2.2 데이터 프라이버시 및 데이터 보호 위협

민감한 데이터가 수집되는 스마트미터의 최우선 과제는 데이터 프라이버시문제라고 할 수 있다. 특히 스마트미터에서 수집되는 데이터를 분석하면, 집안에서 생활하는 모든 생활 패턴을 알 수 있다. 현재 구글에서 테스트 중인 구글파워미터는 가정에서 사용되는 전기량을 실시간으로 보여준다. [그림 4]는 구글파워미터를 통해 댁내에서 하루 동안 사용되는 전기량을 나타낸 것이다. 그래프에 따르면 8시에서 9시경 가장 많은 전기를 소모한 것을 토대로 드라이기를 사용한 것으로 추측할 수 있다. 또한 10시부터 6시 사이에는 전기사용량이 최저이기 때문에 외출상태라는 것을 추측할 수 있다. 이밖에 기존에 알려진 가전기기의 전기소모량을 토대로 댁내에서 이루어지는 모든 생활 패턴을 유추해 낼 수 있다. 게다가 스마트미터에는 인적사항을 비롯하여 스마트미터ID, 연결되어 있는 댁내 기기 정보, 과금 정보, 등이 많은 정보가 저장된다. 만약 이러한 정보가 공격자에게 노출될 경우, 사용자의 프라이버시를 침해할 수 있으며, 다른 악의적인 목적으로 사용될 수 있다. [12][17][20].

스마트미터를 통해 수집되는 데이터는 시스템운영목적, 효율적인 에너지 분배와 같이 공익을 위해 사용되지만, 사용자의 개인정보를 비롯한 많은 정보들을 포함하고 있으므로 안전하게 다루어져야 한다. 하지만 데이터를 소유하는 주체가 자신에게 유리하도록 정보를 수정하여 악용할 가능성이 있다. 따라서 데이터 소유권 문제는 스마트그리드 시스템의 프라이버시 문제에서 가장 문제시 되는 부분이다[20].



〔그림 4〕 스마트미터를 통해 수집된 데이터
〈출처: 구글파워미터〉

4.2.3 데이터 접근통제 위협

전통적인 미터시스템에 비하여 스마트미터를 통해서 수집되는 데이터는 사용자의 개인정보를 비롯한 많은 정보를 포함하고 있다. 따라서 데이터를 필요로 하는 사용자, 에너지공급업자 또는 시스템운영업자는 정당한 방식으로 데이터를 사용해야 한다. 스마트미터 시스템은 여러 사업자들의 유기적인 관계로 이루어지기 때문에 각각의 사업자에 서로 다른 접근제어를 적용함으로써 데이터가 악용되어지는 것을 막아야 한다[14][15].

사용자는 사용되는 에너지의 양을 실시간으로 확인해야 되기 때문에 스마트미터를 통해 해당 정보를 제공받아야 한다. 하지만 사용자에게 데이터 변경 권한이 주어질 경우 사용되는 에너지의 양보다 적은 금액을 청구할 수 있다. 또한 에너지공급업자에게 데이터 변경 권한이 주어질 경우 실제로 사용된 에너지의 양보다 더 많이 사용자가 소비한 것처럼 속여 에너지사용료를 비싸게 청구할 수 있다.

4.2.4 커뮤니케이션 및 운영상 위협

스마트미터 시스템은 거대한 네트워크로 이루어져

있으며, 스마트미터를 통해 수집되는 데이터들은 에너지제공업자, 시스템 운영업자에게 전송된다. 또한 에너지제공업자는 신뢰성 있는 스마트미터 플랫폼을 제공하기 위하여 스마트미터의 상태를 원격으로 관리할 수 있어야 한다. 또한 스마트미터는 댁내의 여러 기기들과 유선 및 무선으로 연결되어 있기 때문에 공격자는 기존의 네트워크에서 사용되는 해킹기술을 이용하여 스마트미터 시스템을 공격할 수 있다. 예를 들어 공격자는 스마트미터와 댁내 기기의 통신을 도청함으로써 에너지사용에 관한 정보를 획득할 수 있다. 공격자는 획득한 정보를 바탕으로 전송되는 메시지를 위·변조하여 사용자에게 거짓된 정보를 주거나 재산상의 피해를 입힐 수 있다. 또한 특정 지역에 대해 에너지 소비율을 높여 광범위하게 에너지공급중단 현상을 일으킬 수 있다[12][14].

V. 스마트미터 보안 요구사항

5.1 기밀성

스마트미터를 통해 수집되는 데이터들은 매우 민감한 정보들을 포함하고 있다. 전기/물/가스의 실시간 사용량을 토대로 출·퇴근시간, TV시청, 식사, 샤워와 같은 사용자의 생활패턴을 분석할 수 있으며, 최소 에너지가 지속적으로 소모되는 시간을 바탕으로 외출 또는 휴가 여부도 알 수 있다. 이와 같이 스마트미터를 통해 수집되는 데이터들은 악의적인 목적으로 사용될 경우 사용자의 프라이버시를 침해할 수 있으며, 사용자의 재산에 피해를 입힐 수도 있다. 예를 들어 공격자가 특정 댁내의 스마트미터를 모니터링 함으로써 에너지 사용량에 대한 데이터를 얻는다면, 평소 댁내에 사람이 없을 때 소모되는 에너지의 양과 현재 소비되고 있는 에너지의 양을 비교하여 댁내에 사람이 있는지 여부를 알 수 있으며, 이러한 정보를 이용하여 공격자는 사용자의 재산을 침해할 수 있다. 따라서 스마트미터를 통해 수집되는 데이터들은 사용자의 정신적, 물리적 피해를 입힐 수 있기 때문에 반드시 기밀성이 유지되어야 한다[18][20].

스마트미터를 통해 수집되는 데이터는 스마트미터 내부 또는 신뢰되는 중앙접근서버에 저장된다. 만약 이러한 데이터들이 보안 메커니즘이 적용되지 않은 채 악의적인 공격자에 의해 외부로 유출된다면, 사용자의 개인 정보가 그대로 드러나게 된다. 따라서 스마트미터에 에너지공급업자로 전송되는 데이터는 안전한 통신기법에 의해 기밀성이 유지되어야 하며, 스마트미터 및 신뢰되는 중앙접근서버에 저장되는 데이터의 유출에 대비하기 위해 암호학적 메커니즘이 적용되어야 한다.

5.2 무결성

스마트미터를 통해 수집되는 데이터들은 에너지사용료 계산 및 전력 요금 책정에 이용된다. 따라서 수집되는 데이터들은 수정되거나 임의로 삭제되지 못하도록 보호되어야 한다. 예를 들어 사용자는 자신의 사용한 에너지보다 적은 에너지사용료를 지불하기 위하여 데이터를 수정 또는 삭제할 가능성이 있다. 또한 에너지공급업자에서는 수익을 위하여 사용자가 사용한 에너지의 양보다 더 많은 에너지사용료를 청구하기 위하여 데이터를 수정할 가능성이 존재한다. 따라서 위와 같은 불공정한 사건의 발생을 막기 위하여 메시지 위·변조가 이루어질 수 없도록 무결성이 보장되어야 한다[11][18].

사용자는 에너지공급업자가 제공하는 에너지사용료가 위·변조되지 않았음을 믿을 수 있어야 하며, 제공되는 정보들은 집 내부에 설치된 디스플레이기기를 통해서 사용자에게 쉽게 제공될 수 있어야 한다. 마찬가지로 에너지공급업자는 사용자가 보내는 에너지사용내역을 믿을 수 있어야 한다.

5.3 가용성

스마트그리드 환경에서 모든 에너지 공급 및 시스템 관리가 자동화로 이루어지며, 공급되는 에너지는 정상적으로 모든 가정 및 시설에게 공급되어야 한다. 또한 스마트그리드 시스템은 어느 한 지역에서 전력시설의 피해가 발생하더라도, 전체 전력망에 미치는 영향을 최소화 할 수 있어야 한다. 스마트그리드 환경은 거대한 네트워크로 이루어져 있기 때문에 일반적인 네트워크 환경에서의 해킹 위협을 동일하게 가진다. 그 중 가장 위협이 되는 공격 중 하나는 서비스 거부(DoS)공격이다. 예를 들어 공격자는 악성코드에 감염된 다수의 스마트미터를 조작하여 에너지공급업자의 서비스를 마비시킬 수 있다. 이때 에너지공급업자는 유동적인 전력 가격 책정 및 에너지 관리를 정상적으로 수행할 수 없게 된다. 또한 공격자는 여러 지역에 대해 동일한 방식으로 공격함으로써 전체 에너지공급시스템에 커다란 영향을 끼칠 수 있다. 따라서 이러한 공격을 막기 위하여 물리

적 보안대책 및 DOS탐지 기법이 이루어져야 한다[11][18].

에너지공급 뿐만 아니라 스마트미터를 통해 수집되는 데이터들은 사용자, 에너지공급업자와 같이 데이터에 접근할 수 있는 권한을 가진 대상에게 항상 제공되어야 한다. 사용되는 에너지 정보는 사용료를 산출하는 근거로 사용되기 때문에 사용자는 이 정보를 주기적으로 검사하면서 정상적으로 에너지 사용료가 청구되는지 알 권리가 있다. 또한 에너지공급업자는 정상적인 에너지 사용료 청구를 위하여 해당 데이터를 올바르게 전송받을 수 있어야 한다[11].

5.4 부인방지

사용자가 사용하는 에너지는 스마트미터를 통해서 측정되며 측정된 데이터는 스마트미터 내에 저장된다. 사용자는 실시간으로 현재까지 사용된 에너지의 양과 예상되는 한 달 에너지사용료에 대한 정보를 제공받는다. 사용자는 청구된 에너지사용료에 대해서 자신이 사용한 에너지양보다 더 많은 금액이 청구되었다고 부정할 수 있다. 따라서 사용자가 에너지사용기록에 대해 부인을 할 수 없도록, 저장되는 메시지는 부인방지가 제공되는 기법이 적용된 보안기법을 사용하여 안전한 곳에 저장·관리되어야 한다.

5.5 인증

스마트미터는 댁내의 모든 가전기기와 네트워크로 연결되어 있다. 따라서 정당한 사용자에 의하여 연결되는 기기인지 판별하기 위하여 기기인증기법이 필요하다. 만약 기기와 스마트미터 간 인증이 제대로 이루어지지 않은 채 통신이 실생활에 활용된다면, 악의적인 목적을 지닌 기기가 스마트미터에 접근하여 서비스를 가로채거나, 서비스를 받고서도 차후에 이를 부인하는 등 혼란을 더욱 가중시킬 것이다.

스마트미터와 댁내 기기의 인증 기술은 아직 구체화 또는 표준화 된 것이 없지만, 기존 홈 네트워크, 무선 단말 등에서 사용하는 인증 기술인 아이디/패스워드 인증 기술, MAC 주소 인증 기술, 암호프로토콜을 활용한 인증 기술, PKI 기반 기기 인증서 인증 기술이 그 대체 기술로 활용될 수 있다.

Ⅵ. 대 응 방 안

6.1 스마트미터의 플랫폼과 데이터 무결성 보호기술

사용자 또는 에너지공급업자에 의한 사기 행위를 막기 위하여 스마트미터를 통해 수집되는 데이터에는 적절한 접근 권한이 설정되어야 한다. 즉 스마트미터 내에 저장된 데이터는 임의로 삽입·변경·삭제하는 행위가 일어나지 않아야 하기 때문에 사용자와 에너지공급업자는 데이터를 읽을 수 있는 권한만을 부여받아야 한다. 또한 스마트미터 내에 기록된 데이터는 에너지사용료를 산출하는데 사용되므로 데이터의 무결성을 위해서 데이터에 대한 접근 권한 부여를 최소화하여야 한다[15].

또한 스마트미터의 가장 취약한 부분인 물리적 공격을 막기 위해서 스마트미터는 안전한 보안매체에 대해 보호되어야 한다. 물리적인 접근이 이루어질 경우 이를 감지하여 에너지공급업자 및 사용자에게 신속하게 보고되어 추가적인 피해가 발생되지 않도록 방지해야 한다. 또한 스마트미터 내부에서 작동되는 펌웨어를 임의로 삽입·변경·삭제가 이루어질 수 없도록 시스템을 설계해야 한다. 비록 스마트미터 하드웨어 가격이 높아지겠지만, 공격자에 의한 이러한 데이터 조작 행위를 방지하기 위하여 데이터 변조 방지 기능(Tamper-proof module, TPM)이 내장된 하드웨어를 스마트미터에 사용할 수 있다. 또한 데이터 변조 방지 기능(TPM)이 장착된 플랫폼에서는 스마트미터에 대한 불법적인 업데이트 및 악성코드 감염 여부를 확인할 수 있는 원격 검증 기술을 적용할 수 있다[4][12].

6.2 프라이버시 보호 기술

사용자의 프라이버시를 보호하기 위해서 스마트미터 내부에 저장되는 데이터는 효율적이고 안전한 암호화 기법이 적용되어야한다. 이에 대한 대안으로 높은 효율성을 지닌 대칭키 기반 암호화 기법인 AES (Advanced Cryptography Standard)를 들 수 있다. AES는 높은 효율성과 안전성을 지니고 있으며, 특히 암·복호화 계산 시간이 짧아 수많은 댁내 기기로부터 송·수신하는 데이터를 암·복호화해야 하는 스마트그리드 환경에 적합하다.

또한 스마트미터를 통해 수집되는 데이터에 대한 프

라이버시 보호를 보장하기 위하여 아래와 같은 사항이 만족되어야 한다[20].

- 데이터는 정당하게 생성되어야 한다.
- 데이터는 정당한 목적에 사용되어야 하며, 사적인 목적을 위하여 상업적으로 사용되지 않아야 한다.
- 데이터를 소유하는 대상은 안전한 메커니즘을 통해 데이터를 보존해야 하며, 필요 이상의 기간 동안 저장하지 않는다.
- 데이터의 접근은 권한을 가진 대상에게만 부여하며, 정당하지 못한 접근에 대한 보안대책이 강구되어야 한다.
- 데이터는 허가된 대상 이외의 제3자에게 전송되지 않아야 한다.

위와 같은 프라이버시 보호 요구사항들을 만족시키기 위해서는 기술적인 보안메커니즘 이외에 이를 사업자들에게 강제할 수 있는 프라이버시 보호 관련 법·제도 정책의 제도화가 필요하다. 현재 미국과 유럽 등 선진국가들의 경우 프라이버시 보호를 위하여 개인정보보호법이 이미 제정되었지만, 아직 국내에는 개인정보보호법이 제정되지 않았다. 따라서 프라이버시 보호관련 법·제도 및 스마트그리드 운영, 관리에 대한 법 제정 시급하다.

6.3 AMI 네트워크 보호 기술

거대한 네트워크로 연결된 스마트미터는 기존의 네트워크 해킹기법이 그대로 적용될 수 있기 때문에 안전한 데이터 전송을 위해서 보안메커니즘이 적용된 통신 프로토콜이 필요하다. TCP/IP, HTTP, FTP와 같이 현재 네트워크에서 널리 사용되는 프로토콜은 공격자들에 의하여 쉽게 도청당하는 단점을 가지고 있다. 따라서 안전한 통신을 지원하기 위하여 스마트미터 시스템은 IPSec(Internet Protocol Security), SSH(Secure Shell), TLS(Transport Layer Security), SSL(Secure Socket Layer)와 같은 검증된 보안 통신 프로토콜을 기본적으로 채택하여야 하며, 객체에 대한 정확한 인증을 통하여 IP/DNS 스푸핑과 같은 네트워크 공격을 막을 수 있어야 한다[14].

또한 공격자는 악성코드에 감염된 다수의 스마트미터를 조작하여 서비스 거부(DoS)공격을 시도할 수 있다. 이러한 공격은 에너지공급업자의 서비스를 마비시켜 사회적 혼란을 야기하므로 서비스 거부(DoS)공격을 사전에 방지하기 위하여 비정상적인 트래픽 탐지기술 및 변칙 탐지 기술이 필요하다. 만약 스마트미터가 공격에 악용될 경우, 공격에 대한 대응 및 분석을 위하여 스마트미터에 적합한 포렌식 기술이 필요하다.

Ⅶ. 결 론

스마트그리드는 기존 미터링 시스템과 같이 단순히 사용 전력 측정만을 위하여 사용되는 것이 아니라, 사용자의 직접적인 에너지 관리 및 판매와 에너지공급업자의 의한 원격 검침과 같은 다양한 서비스가 이루어지기 때문에, 이와 관련된 네트워크 산업뿐만 아니라 배터리 사업과 같은 타 산업과 연계되어 2030년경에는 스마트그리드 관련 산업이 세계적으로 약 1경원에 해당하는 시장으로 성장할 것으로 예측되고 있다. 특히 스마트그리드를 구축하기 위한 중요한 구성요소인 스마트미터는 사용자 또는 스마트그리드 시스템 전체에 영향을 줄 수 있는 민감한 데이터를 처리하기 때문에, 스마트미터에 대한 신중한 접근통제가 요구된다. 이에 본 논문에서는 차세대 전력망인 스마트그리드의 안전한 구축을 위하여 스마트미터의 예상되는 위협들을 살펴보고, 이러한 위협들을 제거하기 위한 보안 요구사항 및 대응 방안을 논의하였다.

스마트그리드 구축은 지구 온난화 대책 가운데 하나로, 에너지를 효율적으로 사용하기 위한 세계적으로 지지받고 있는 대안 중의 하나다. 스마트그리드 환경에서 보안 위협들은 개인의 재산상의 피해나 프라이버시문제를 야기하며, 교통 통제 불능, 금융시스템 마비와 같은 사회적 재난을 초래하거나, 병원 의료기기 작동불가로 인해 생명을 위협하는 심각한 문제를 발생시킬 수 있다. 이렇게 광범위한 피해를 초래할 수 있는 스마트그리드 내에서 보안 문제가 발생된다면, 2003년 발생한 1·25 인터넷 대란보다 그 피해 규모가 더욱 클 것이다. 당시 추정 피해액은 국내에서 1조 5,378억이었으며, 전 세계 피해액은 15조 4,830억 원이었다. 따라서 안전한 스마트그리드를 구축하기 위하여 예상 가능한 위협들을 막기 위한 보안기술을 개발하고 스마트그리드 관련 정보보호 법률을 제정하는데 적극적인 투자와 노력이 필요하다. 또한 예상하지 못한 보안 문제점에 대해서도 신속한 대처를 위한 시스템체계를 마련해야 한다.

참 고 문 헌

[1] 김석곤, "Global Smart Metering 산업수요 및 발전 전망,"

[2] 도윤미, 김선진, 허태욱, 박노성, 김현학, 홍승기, 서정해, 전종암, "스마트 그리드 기술 동향:전력망과 정보통신의 융합기술," 전자통신동향분석 제24권 제5호 , 2009. 10.

[3] 이경복, 박태형, 임종인, "정보보호정책 관점에서의 한국형 스마트 그리드 추진 방안에 관한 연구," 정보화정책 제16권 제4호, pp.73-96, 2009.

[4] 이상준, "차세대 전력 인프라를 위한 보안솔루션," 유넷시스템, 2009. 11.

[5] 장두석, "스마트그리드 산업의 동향 및 산업화 방안," 산은경제연구소, 2010. 1.

[6] 전황수, 하영욱, 조병선, "주요 국가의 스마트그리드 정책 동향," 전자통신동향분석 제25권 제3호 2010. 6.

[7] KOTRA "주요국 Smart Grid 정책/시장 조사," 자료10-021, 2010. 4.

[8] Elias L. Quinn, "Privacy and the New Energy Infrastructure," "http://ssrn.com/abstract=1370731," 2009.

[9] Frances M. Cleveland, "IEC TC57 Security Sarandards for the Power System's Information Infrastructure, Beyond Simple Encryption," IEEE PES Transmission and Distribution Conference and Exhibition, 2005/2006.

[10] Frances M. Cleveland, "Enhanceing the Reliability and Security of the Information Infrastructure Used to Manage the Power System," IEEE Power Engineering Society General Meeting. 2007.

[11] G. Lenzini, M. Oostdijk and W. Teeuw, "Trust, Security, and Privacy for the AMI," TAMI PEGASUS/Huisdraad, 2009. 7.

[12] Jeff McCullough, "AMI Security Consideration," Elster, ref WP42-1007B, 2010.

[13] Layla AlAbdulkarim and Xofia Lukszo, "Information Security Assurance in Critical Infrastructures: Smart Metering Case," INFRA International Conf. pp.1-6, 2008.

[14] Mohit Arora, "Advanced Metering: ecosystem, security threats and counter measures," in Industrial Control Designline, 2009. 2.

[15] Raymond C. Park, "Advanced Metering Infrastructure Security Considerations," Sandia report, ref. SAND2007-7327, 2007. 12.

[16] Rob van Gerwen, Saskia Jaarsma and Rob Wilhite, "Smart Metering," Hans De Keulenaer, 2006. 7.

[17] Ross Anderson and Shailendra Fuloria, "On the security economics of electricity metering," 9th Workshop on the Economics of Information Security, 2010.

[18] Sander Keemink, Bart Roos, "Security analysis of Dutch smart metering system," Universiteit Van Amsterdam, 2008. 7.

[19] Greentechgrid, "Smart Meter Security: A Work in Progress," 2009. 6.

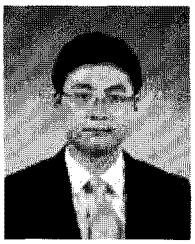
[20] Ofgem, "Smart Metering Implementation Programme: Data Privacy and Security," ref 94e/10, 2010, 7.

[21] PikeResearch "Smart Meter Security Investment to Total $575 Millions by 2015, but Meters Remain a Point of Vulnerability in the Smart Grid," Newsroom, 2010. 8.

[22] Openmeter, "http://www.openmeter.com"

[23] Oracle, "Smart Metering for Water Utilitys," 2009. 9.

〈著者紹介〉

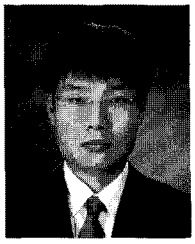


남 궁 완 (Wan Namgoong)
학생회원

2006년 2월 : 단국대학교 컴퓨터과학과 졸업(학사)
2009년 9월~현재 : 고려대학교 정보경영공학전문대학원 정보경영공학과 석사과정
관심분야 : USN 보안, 스마트그리드 보안

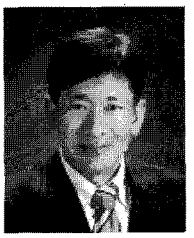
조 효 진 (Hyojin Jo)
학생회원

2009년 2월 : 고려대학교 산업정 보시스템정보공학과 졸업(학사)
2009년 3월~ 현재 : 고려대학교 정보경영공학전문대학원 정보경영공학과 석박사통합과정
관심분야 : 스마트그리드 보안, VANET 보안



조 관 태 (Kwantae Cho)
학생회원

2005년 2월 : 고려대학교 컴퓨터학과 졸업(학사)
2008년 2월 : 고려대학교 정보경영공학전문대학원 정보경영공학과 졸업(석사)
2008년 3월~현재 : 고려대학교 정보경영공학전문대학원 정보경영공학과 박사과정
관심분야 : USN 보안, 스마트그리드 보안



이 동 훈 (Dong Hoon Lee)
종신회원

1982년 8월 : 고려대학교 경제학과 졸업(학사)
1987년 12월 : Oklahoma University 전산학 공학석사
1992년 5월 : Oklahoma University 전산학 공학박사
1992년 8월 : 단국대학교 전자계산학과 전임강사
1993년 3월~1997년 2월 : 고려대학교 전산학과 조교수
1993년 3월~1997년 2월 : 고려대학교 전산학과 부교수
1993년 3월~1997년 2월 : 고려대학교 정보경영공학전문대학원 교수
관심분야 : 암호이론 및 프로토콜, 전산이론, USN 보안, 스마트그리드 보안