http://dx.doi.org/10.14400/JDC.2016.14.5.333

개방형 자동 수요 반응 시스템 보안 취약성 분석에 관한 연구

채현호*, 이준경*, 이경학**
㈜나온웍스*, 남서울대학교**

A Study on The Security Vulnerability Analysis of Open an Automatic Demand Response System

Hyeon-Ho Chae*, June-Kyoung Lee*, Kyoung-Hak Lee**
NAONWORKS Co.,Ltd*
IACF, Namseoul University**

요 약 인터넷 기반 전력 수요 관리 망에서 소비자와 공급자간 전기에너지 공급과 사용을 최적화, 효율화하기 위한 기술은 스마트 그리드 망에서 핵심 요소 기술로 대두되고 있다. 현재 전력 수요 관리 망에서 수요 반응 신호를 전기에너지 공급자와 시스템 제공자 및 사용자까지 전달하는 개방형 자동수요반응 표준 프로토콜은 openADR 2.0b가 사용되고 있다. 본 논문은 가장 신뢰성 있고 전 세계적으로 확산되어 있는 EPRI 오픈 소스를 사용하여 개발한 VEN, VTN 시스템의 다양한 공격 취약성에 대한 분석을 목적으로 하고 있다. 공격용 시뮬레이터를 이용하여 EPRI 오픈 소스로 구현한 VEN, VTN 시스템을 다양한 방법으로 공격하여 분석을 수행하였고 분석 결과 VEN, VTN 시스템이 파라미터 변조 공격, 서비스 플로우 변조 공격에 대한 보안 취약성이 존재한다는 결과를 얻을 수 있었다. 개방형, 양방향 통신 환경의 스마트 그리드 망에서 openADR 2.0b 프로토콜을 구현할 때는 다양한 보안 취약성을 고려한 프로토콜에 특화된 보안 기술이 반드시 모색되어야 한다는 결론을 얻을 수 있었다.

주제어 : 스마트 그리드, 수요 반응, 스마트 그리드 보안, 개방형 자동 수요 반응, 가상 상위 노드, 가상 하위 노드

Abstract Technology to optimize and utilize the use and supply of the electric power between consumer and supplier has been on the rise among the smart grid power market network in electric power demand management based on the Internet. Open Automated Demand Response system protocol, which can deliver Demand Response needed in electric power demand management to electricity supplier, system supplier and even the user is openADR 2.0b. This paper used the most credible, cosmopolitanly proliferated EPRI open source and analysed the variety of security vulnerability that developed VEN and VTN system may have. Using the simulator for attacking openADR protocol, the VEN/VTN system that has been implemented as EPRI open source was conducted to attack in a variety of ways. As a result of the analysis, we were able to get the results that the VEN/VTN system has security vulnerabilities to the parameter tampering attacks and service flow falsification attack. In conclusion, if you want to implement the openADR2.0b protocol system in the open or two-way communication environment smart grid network, considering a variety of security vulnerability should be sure to seek security technology and services.

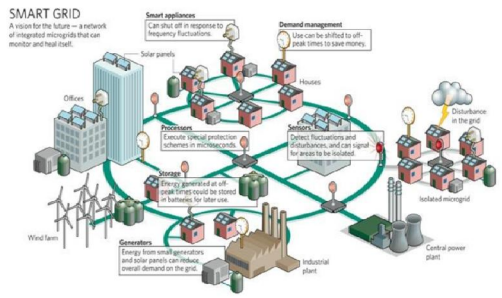
Key Words : Smart Grid, DR(Demand Response), Smart Grid Security, openADR(open Automated Demand Response), VTN(Virtual Top Node), VEN(Virtual End Node)

* 본 논문은 2015년 산업통상자원부의 재원으로 한국에너지기술평가원의 지원을 받았음.(No. 20151220100090).
Received 28 March 2016, Revised 29 April 2016
Accepted 20 May 2016, Published 28 May 2016
Corresponding Author: June-Kyoung Lee(naonworks Co.,Ltd)
Email: darkelan@naonworks.com

ISSN: 1738-1916

1. 서론

스마트 그리드(smart grid)란 [Fig. 1]에서 볼 수 있듯이 전기의 발전, 송전, 배전, 과정에 정보통신기술(ICT: Information & Communication Technology)을 접목하여 공급자와 소비자가 서로 상호 작용함으로써 전력망의 지능화 및 고도화를 추구하고 고품질의 전력 서비스를 제공하여 에너지 이용 효율을 극대화하는 전력망 시스템을 의미하는 것이다.



[Fig. 1] The Smart Grid Frontier[20]

이러한 스마트 그리드의 개념은 기존 공급 위주의 전력 정책이 환경 문제, 에너지 가격 급등 등으로 인해 한계에 봉착함에 따라 수요 관리 측면의 대안으로써 전 세계적으로 확산되고 있는 상황이다[1,2,3,4,5,6]. 현재 인터넷 기반 전력 수요 관리 망에서는 전기에너지 공급과 사용을 최적화 및 효율화하기 위해 필요한 수요 반응 신호를 공급자와 시스템 제공자 및 사용자까지 전달할 수 있도록 하는 개방형 자동수요반응 시스템 표준 프로토콜로써 openADR 2.0b 프로토콜이 핵심 기술로 성장하고 있다.

스마트 그리드에서는 전력 장비들에서부터 수용가의 가전 기기, 원격 검침 장치에 이르기까지 광범위하게 데이터의 전송이 이루어지는데, 이러한 데이터 전송들이 기존의 폐쇄된 전력망이 아닌 통합된 광대역 전력 통신망을 통해 이루어지게 된다. 따라서 스마트 그리드 상에서 전송되는 데이터들의 보안은 반드시 보장되어야 할 중요한 과제이다. 스마트 그리드 망에서 핵심 기술인 openADR 2.0b 프로토콜을 발표한 표준 단체에서 제시하는 보안 방법은 TLS를 이용한 전송계층 보안 프로토콜 사용 위주로 정의되어 있고 openADR 2.0b 프로토콜 및 서비스에 대한 취약성 분석 및 이에 대한 대응 보안기술 개발은 초기 단계이다. 또한 현재 국내 전력 수요 관리 보안 제품들은 웹 방화벽 외에 대안이 없으므로 openADR 2.0b 관련 취약성 보안 위협이 상존하고 있어 국내 수요관리 사업이 활성화 될 경우, 다양한 보안 취약점 이슈 및 사례 발생이 예견되고 있다. 이러한 상황은 국가 기간 자원인 전력 수요 관리 보안 이슈 발생 시 국민 불안감 조성 등의 심각한 사회적 문제로 발전될 수 있는 위험성을 내재하고 있다[7,8,9,10].

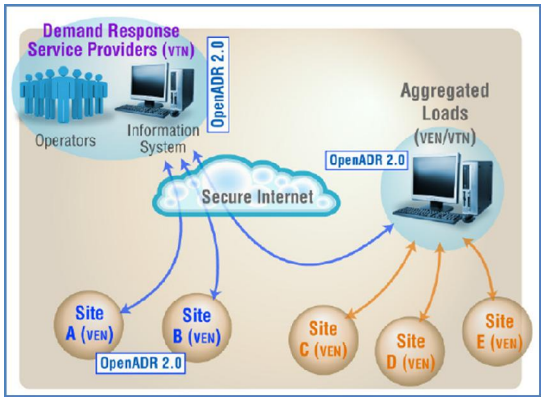
따라서 본 논문은 위와 같은 구조 및 특징을 갖는 스마트 그리드 망에서 가장 광범위하게 사용되고 있는 EPRI 오픈 소스를 이용하여 개방형 자동 수요 반응 시스템 구현 시 발생할 수 있는 openADR 프로토콜 특화적인 공격 취약성을 분석하였다. 본 논문의 구성은 다음과 같다, 2장에서 개방형 자동 수요 반응에 대하여 설명하였고 3장에서 오픈 소스를 이용한 개방형 자동 수요 반응 시스템을 구성하여 공격 취약성에 대하여 분석하였고 마지막 4장에서 오픈 소스를 이용한 개방형 자동 수요 반응 시스템의 취약성 대하여 고찰하고 정리하였다.

2. 개방형 자동 수용 반응 개요

수요 반응(Demand Response)이란 증가하는 전력 수요와 피크 부하에 대응하고 안정적인 전력망을 구축하기 위한 하나의 방법으로, 전력 소비자 측에서 전기 요금이나 공급자의 요청에 따라 전력 소비를 조절함으로써 전력 계통의 안정성과 신뢰성을 확보하는 기술이다. 이러한 수요 반응 서비스 활성화를 위해서는 표준화된 통신 방식과 데이터 형식이 필요하다[11,12,13].

openADR이란 개방형 자동 수요 반응(open Automated Demand Response)을 뜻하며 지능형 수요 반응에 적용되는 표준 통신 프로토콜을 말한다. 이 프로토콜은 상업용 openADR의 개발, 테스트 및 배포를 지원하기 위해 업계 관계자를 중심으로 2010년 설립 된 openADR Alliance[14]에서 개발한 지속성, 신뢰성 기반의 수요 반응 프로토콜 표준이며 국제 표준으로서 기존의 수동적인 수요 반응에서 벗어나 새로운 자동화된 수요 반응을 지원하고 있다. openADR은 openADR 1.0과 openADR 2.0a/b가 있으며, 현재 openADR 1.0은 부분적으로 사용

되고 있고, openADR 2.0이 주로 사용되고 있는 상황이다. openADR 2.0a는 자원이 제한되어 있고 간단한 DR 어플리케이션을 실행하기 위한 DR 시스템을 대상으로 하고 있어 Simple EiEvent 서비스만을 지원하고 있다. openADR 2.0b는 여러 가지 DR 어플리케이션을 실행하기 위한 DR 시스템을 대상으로 하고 있으며 EiEvent, EiReport, EiRegisterParty, EiOpt 서비스를 지원하고 있다. openADR 2.0 표준은 초기 2.0a 버전을 거쳐 정교한 장치들을 대상으로 한 2.0b 버전으로 발전하고 있다.



[Fig. 2] Possible relationships of VTN and VEN[17]

[Fig. 2]에서 볼 수 있는 것처럼 openADR 2.0b에서 제공하고 있는 주요 노드 및 장치는 크게 서버로 동작하여 정보를 제공하는 VTN(Virtual Top Node)과 정보에 응답하는 VEN(Virtual End node)으로 구분된다. 또한, VTN과 VEN간 상호 정보 교환을 위해 기존 개방 표준(HTTP, XMPP)을 사용하고 있다. 이러한 표준은 기본적으로 단순 VEN 제어를 위한 EiEvent 서비스, 전력 사용량 Report를 위한 EiReport, VEN 등록을 위한 EiRegisterParty, 스케줄링 서비스의 일종인 EiOpt 서비스를 제공한다. 또한, 2.0a 버전에서 사용되었던 HTTP PUSH와 더불어 PULL 방식의 데이터 전송을 지원하게 되어 VTN과 VEN간 상호 보완적인 DR 이벤트의 흐름을 제공한다[15,16,17].

openADR의 특징은 인터넷과 같은 기존의 모든 IP 기반 통신 네트워크를 통해 공통의 언어를 사용하여 DR 신호를 전달하는 에너지 공급자와 시스템 운영자를 위한 표준화된 방법을 제공하고 있는 것으로써 최종 사용자에 의하여 수요반응 이벤트가 외부 신호의 수신을 통해 자동적으로 개시되게 하는 자동화의 특징을 가지고 있다.

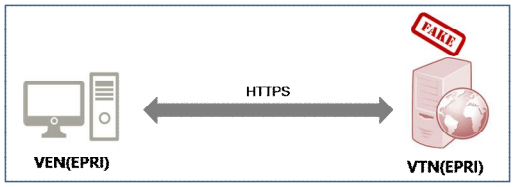
openADR의 효과는 전력 공급 업체에게 DR 프로그램 성능 증가, 소비자에 대한 신뢰성, 예측성, 일관성 증가, DR 프로그램 참여 증가, 소비자 서비스 증가와 같은 효과를 가지고 있을 수 있다. 소비자 입장에서는 DR 프로그램에 참여에 따른 에너지 비용 절감, 에너지의 효율 증가, 에너지관리장치 비용 절감 등의 효과를 가지고 올 수 있고 장치 제조업자에게는 복잡도 감소 및 신속하고 간편한 설치 및 운용의 효과를 가지고 올 수 있어 전력 수요 관리 서비스 망에서 핵심 기술로 성장하고 있다.

3. 개방형 자동 수요 반응 시스템 취약성 분석

본 논문은 개방형 자동 수요 반응 시스템 개발함에 있어 가장 신뢰성 있고 전 세계적으로 확산되어 있는 EPRI 오픈 소스를 사용한 VEN 및 VTN 시스템이 가질 수 있는 파라미터 변조 공격 및 서비스 플로우 변조 공격으로 나누어 개방형 자동 수요 반응 시스템 구현 시 오픈 소스를 이용할 경우의 공격 취약성에 대하여 분석을 수행하였다.

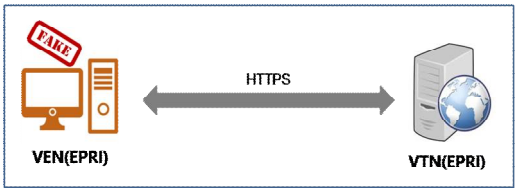
3.1 취약성 분석 시스템 구성

다양한 공격 취약성 분석을 위하여 EPRI 오픈 소스를 이용하여 openADR 2.0b 프로토콜을 구현한 VTN과 VEN 시스템을 연동하여 실제 전력 수요 관리 망과 같이 구성하여 두 가지 구성 망 타입 별로 공격 취약성을 분석하였다. 첫 번째 구성 망 타입은 [Fig. 3]과 같이 EPRI 오픈 소스를 이용한 실제 VEN 시스템에 EPRI 오픈 소스를 수정하여 공격자용 VTN 시스템을 만들어 연동시키면서 다양한 공격 취약성을 분석하였다.



[Fig. 3] Vulnerability analysis network using faked VTN

두 번째 구성 망 타입은 [Fig. 4]와 같이 EPRI 오픈 소스를 이용한 실제 VTN 시스템에 EPRI 오픈 소스를 수정하여 공격자용 VEN 시스템을 만들어 연동시키면서 다양한 공격 취약성을 분석하였다[18,19].



[Fig. 4] Vulnerability analysis network using faked VEN

3.2 openADR 파라미터 변조 취약성 분석

파라미터 변조 취약성 분석 방법은 파라미터 값 변조(case 1), 파라미터 타입 변조(case 2), 파라미터 버퍼 오버플로우 변조(case 3) 3가지 방법으로 공격을 수행하였다.

파라미터 값 변조 방법은 openADR 프로토콜 표준에 정의된 값의 범위를 벗어난 경우와 Request 값에 대한 변조된 값 또는 ID를 가진 Response로 응답하는 경우에 대하여 수행하였다. 파라미터 타입 변조 방법은 integer, float, double, string 등의 openADR 프로토콜 표준에 정의되어 있는 각 파라미터 타입을 변조하여 취약성 분석을 수행하였다. 파라미터 버퍼 오버플로우 변조 방법은 integer 최댓값, double 최댓값, string 최대길이 등의 파라미터 타입이 가질 수 있는 최댓값(버퍼)을 초과하도록 변조하여 수행하였다.

<Table 1>은 openADR 프로토콜에서 제공하는 EiRegisterParty, EiOpt, EiEvent, EiReport, OadrPoll Service로 분류하고 각 서비스 별로 가능한 Message의 페이로드 종류별로 구분하여 위에서 설명한 case1부터 case3의 공격을 수행하여 분석 결과를 정리하였다. 또한 추가로 <Table 2>에서는 EiEvent 서비스에서 oadrDistributeEvent 페이로드 부분의 다양한 파라미터들에 대하여 좀 더 세분화하여 공격 수행 분석 결과를 정리하였다.

분석 결과 오픈 소스를 사용하여 개방형 자동 수요 반응 시스템 구현 시 openADR 프로토콜 파라미터 변조 공격에 대한 취약성 분석 결과는 <Table 1> 및 <Table 2>와 같이 대부분의 파라미터들이 파라미터 값, 타입, 오버플로 변조 공격 유형에 취약한 결과를 나타내었다. <Table 1> 및 < Table 2>에서 “O”로 표시된 항목이 공격 가능 즉 취약성이 존재하는 것을 나타내며 공격 시 변조를 감지하지 못하고 오동작하거나 프로세스가 다운되는 상황이 발생하였다.

<Table 1> Security vulnerability analysis results of openADR protocol service parameter-tampering attack

Service	Message	case 1	case 2	case 3
EiRegisterParty	oadrQueryRegistration	O	O	O
	oadrCreatedPartyRegistration	O	O	O
	oadrCreatePartyRegistration	O	O	O
	oadrRequestReregistration	X	X	X
	oadrCancelPartyRegistration	O	O	O
	oadrCanceledPartyRegistration	O	O	O
EiOpt	oadrCreateOpt	O	O	O
	oadrCreatedOpt	O	O	O
	oadrCancelOpt	O	O	O
	oadrCanceledOpt	O	O	O
EiEvent	oadrDistributeEvent	O	O	O
	oadrCreatedEvent	O	O	O
	oadrRequestEvent	O	O	O
	oadrResponse	O	O	O
EiReport	oadrRegisterReport	O	O	O
	oadrRegisteredReport	O	O	O
	oadrCreateReport	O	O	O
	oadrCreatedReport	O	O	O
	oadrUpdateReport	O	O	O
	oadrUpdatedReport	O	O	O
	oadrCancelReport	O	O	O
	oadrCanceledReport	O	O	O
OadrPoll	oadrPoll	X	X	X

<Table 2> Security vulnerability analysis results of openADR protocol event parameter-tampering attack

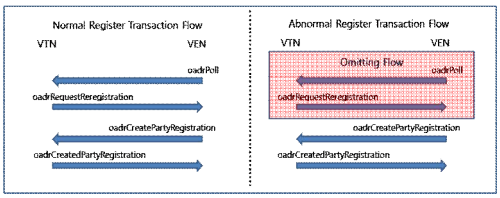
Service (Message)	Message	case 1	case 2	case 3
EiEvent (oadrDistributeEvent)	requestID	O	O	O
	vtnID	O	O	O
	eventID	O	O	O
	modificationNumber	O	X	O
	priority	O	X	O
	marketContext	O	O	O
	createdDateTime	O	X	X
	eventStatus	X	X	X
	testEvent	O	O	O
	vtnComment	O	O	O

	date-time	O	X	X
	duration	O	O	O
	startafter	O	O	O
	text	O	O	O
	value	O	X	X
	signalName	O	O	O
	signalType	X	X	X
	signalID	O	O	O
	oadrResponseRequired	X	X	X
	groupID	O	O	O
	resourceID	O	O	O
	venID	O	O	O
	partyID	O	O	O
	responseCode	O	X	O
	responseDescription	O	O	O

3.3 openADR 서비스 플로우 취약성

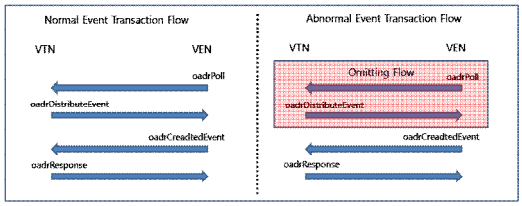
openADR 서비스 플로우 취약성 분석은 정상 동작중인 VEN과 VTN을 다른 단말 또는 해킹된 VEN 및 VTN에서 공격 하는 상황으로 Register, Event, Report 서비스에 대하여 서비스 별로 필요한 Transaction들 중 Transaction 생략하거나 서비스 별 필요한 Transaction들 중 Transaction 순서 변경하는 공격 방식으로 취약성을 분석하였다.

[Fig. 5]와 같이 openADR 프로토콜의 Register (EiRegisterParty) 서비스에서 VEN 단말과 VTN 서버 사이에 “oadrPoll” Request 메시지에 대한 “oadrRequestReregistration” 응답 메시지 Transaction 플로우가 생략된 환경에서도 VEN의 단말 접속 등록 XML 요청 메시지인 “oadrCreatePartyRegistration” 메시지를 정상적인 XML로 VTN 서버가 인식하여 정상 등록 확인 메시지인 “oadrCreatedPartyRegistration”로 응답하는 취약성을 확인할 수 있었다.



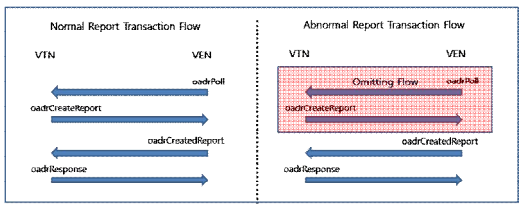
[Fig. 5] Security vulnerability analysis of Register service flow modification attack

[Fig. 6]와 같이 openADR 프로토콜의 Event(EiEvent) 서비스에서 VEN 단말과 VTN 서버 사이에 “oadrPoll” Request 메시지에 대한 “oadrDistributeEvent” 응답 메시지 Transaction 플로우가 생략된 환경에서도 VEN의 Event XML 요청 메시지를 조금 변경한 “oadrCreadtedEvent” 메시지를 정상적인 XML로 VTN 서버가 인식하여 정상 Event 확인 메시지인 “oadrResponse”로 응답하는 취약성을 확인할 수 있었다. Event 서비스에서 “oadrCreadtedEvent” 메시지에서 파라미터 값에 따라 Event 생성과 취소가 구분되는데 두 경우 모두 취약성을 확인할 수 있었다.



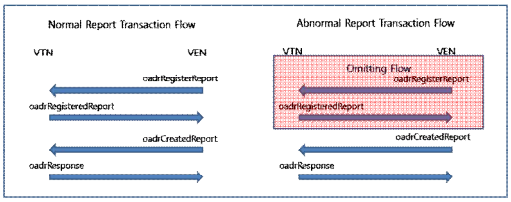
[Fig. 6] Security vulnerability analysis of Event flow modification attack

[Fig. 7]과 같이 openADR 프로토콜의 Report(EiReport) 서비스에서 VEN 단말과 VTN 서버 사이에 “oadrPoll” Request 메시지에 대한 “oadrCreateReport” 응답 메시지 Transaction 플로우가 생략된 환경에서도 VEN의 Report XML 요청 메시지인 “oadrCreadtedReport” 메시지를 정상적인 XML로 VTN 서버가 인식하여 정상 Report 확인 메시지인 “oadrResponse” 응답하는 취약성을 확인할 수 있었다.



[Fig. 7] Security vulnerability analysis of Report service flow modification attack(case 1)

[Fig. 8]과 같이 openADR 프로토콜의 Report(EiReport) 서비스에서 VEN 단말과 VTN 서버 사이에 “oadrRegisterReport” Request 메시지에 대한 “oadrRegisteredReport” 응답 메시지 Transaction 플로우가 생략된 환경에서도 VEN의 Report XML 요청 메시지인 “oadrCreadtedReport” 메시지를 정상적인 XML로 VTN 서버가 인식하여 정상 Report 확인 메시지인 “oadrResponse”로 응답하는 취약성을 확인할 수 있었다.



[Fig. 8] Security vulnerability analysis of Report service flow modification attack(case 2)

4. 결론

현재 전력망에서는 국가 차원의 스마트 그리드 환경을 구축하기 위해 인터넷 기반의 전력 수요 관리 시스템의 구축이 확산되고 있는 실정이다. 따라서 전력 수요 관리 사업자 및 스마트 그리드 시스템 제조사들은 전기에너지의 공급과 사용을 최적화 및 효율화하기 위하여 수요 반응 신호를 공급자와 시스템 제공자 및 사용자까지 전달하려는 시도를 하고 있으며 이를 위해 개방형 자동 수요반응 시스템의 표준 프로토콜인 openADR 2.0b 프로토콜의 신뢰성을 가지고 있는 EPRI 오픈 소스를 사용하여 시스템 개발 및 구축에 박차를 가하고 있는 상황이다.

본 논문은 가장 신뢰성 있고 전 세계적으로 확산되어 있는 EPRI 오픈 소스를 사용하여 개발한 VEN 및 VTN 시스템이 가질 수 있는 다양한 공격 취약성에 대하여 분석하였다. 공격 취약성 분석은 파라미터 변조 공격 및 서비스 플로우 변조 공격으로 나누어 수행하였다. openADR 파라미터 변조 취약성 분석에서는 파라미터 값, 타입, 버퍼 오버플로우 등의 변조 공격을 수행하였고 대부분의 파라미터들에 대한 변조 공격에 오픈 소스가 취약성을 가지고 있음을 확인하였다,

openADR 서비스 플로우 취약성 분석은 Register, Event, Report 서비스 플로우에 대하여 취약성 분석을 수행하였고 오픈 소스가 정상적인 서비스 수행을 위해 필요한 Transaction을 생략하거나 Transaction 순서 및 파라미터 값을 변경하는 변조 공격에 매우 취약성을 가지고 있음을 확인하였다. 스마트 그리드는 전력 인프라와 정보통신기술이 접목되어 전력 사용 및 관리를 최적화하는 기술로써 개방형 및 양방향 통신환경에 노출 되어 있어 다양한 보안 사고가 발생할 수 있다. 따라서 본 논문에서 분석한 결과를 바탕으로 openADR 프로토콜이 구현된 국내 개발 및 개발 예정인 전력 수요 관리 시스템에 대한 보안 취약성을 지속적으로 분석하여야 할 것이다. 또한 분석된 다양한 보안 취약성을 고려한 openADR 프로토콜 및 서비스에 특화된 보안 기술이 반드시 모색되어야 할 것이다.

ACKNOWLEDGMENTS

This work was supported by the Korea Institute of Energy Technology Evaluation and Planning(KETEP) and the Ministry of Trade, Industry & Energy(MOTIE) of the Republic of Korea (No. 20151220100090).

REFERENCES

[1] SmartGrid Website, http://www.smartgrid.org.

[2] Hyun-Jae Kim, Sung-Han Jo, “A Study on Consumer Protections for the Introduction of Smart Grid”, The Journal of Digital Policy & Management, 2011.

[3] Ji-Hyun Kim, Suk-Jun Lee, Ki-Yoon Kim, Suk-Jae Jeong, “Evaluation and Facilitation of the Korean Smart Grid Market”, The Journal of Digital Policy & Management, 2013.

[4] Hyun-Jae Kim, Chan-Kook Park, “A Study on the Evaluation Criteria for the Performance of Smart Grid Pilot Projects”, The Journal of Digital Policy & Management, 2012.

[5] Sung-Yong Lee, Snag-Soo Yeo, “Efficient Secret Sharing Data Management Scheme for Privacy Protection in Smart Grid Environment“, The Journal of Digital Policy & Management, 2013.

[6] Si-Jung Kim, Do-Eun Cho, “A Study on Secure Home Network in Envuronment Smart Grid”, The Journal of Digital Policy & Management, 2012.

[7] Bo-Seon Kang, Keun-Ho Lee, “A Scheme on Energy Efficiency Through the Convergence of Micro-grid and Small Hydro Energy”, Journal of the Korea Convergence Society, Vol. 6, No. 1, pp. 29-34, 2015.

[8] Keun-Ho Lee, “Analysis of Threats Factor in IT Convergence Security”, Journal of the Korea Convergence Society, Vol. 1, No. 1, pp. 49-55, 2010.
[9] NIST Cyber Security WG, “smart Grid Cyber Security Strategy and Requirements”, 2010
[10] Jae Jung Park, “DR(Demand Reponse) Technology for Smart Grid“, KERI, 2013.
[11] PIER, "Open Automated Demand Response Communications Specification(Ver. 1.0), 2009.
[12] W. M. Taqqali and N. Abdulaziz, “Smart Grid and demand response technology,” EnergyCon 2010 IEEE International, 2010.
[13] Jae Jung Park, DR(Demand Reponse) Technology for Smart Grid, KERI, 2013.
[14] openADR Alliance Website, http://www.openadr.org
[15] openADR 2.0 Profile Specification A Profile, openADR Alliance, 2011
[16] Jimyung Kang, Implementation of openADR 2.0a Profile for Demand Response in Smart Grid, KERI, 2013.
[17] openADR 2.0 Profile Specification B Profile, openADR Alliance, 2013.07
[18] Certified EPRI Open Source openADR 2.0b VEN & VTN Website, http://www.openadr.org
[19] openADR Open Source Toolkit: Developing Open Source Software for the Smart Grid, Charles McParland, IEEE Power and Energy Society General Meeting, 2011.
[20] David Heyerman “The smart Grid Frontier:Wide Open” http://tinycomb.com/2009/05/03 May 3, 2009

채 현 호(Chae, Hyun Ho)

・2002년 2월 : 동명정보대학교 정보통신과(공학사)
・2014년 8월 : ㈜엘림넷 책임 연구원
・2015년 7월 ~ 현재 : ㈜나온웍스 책임 연구원
・관심분야 : 네트워크, 정보 보안
・E-Mail : chhh@naonworks.com

이 준 경(Lee, June Kyoung)

・1995년 2월 : 인하대학교 전자계산학과(공학석사)
・2000년 8월 : ㈜LG정보통신 선임연구원
・2007년 7월 ~ 현재 : ㈜나온웍스 대표
・관심분야 : 네트워크, 정보 보안
・E-Mail : darkelan@naonworks.com

이 경 학(Lee, Kyoung Hak)

・1992년 2월 : 광운대학교 전자통신공학과(공학사)
・1994년 2월 : 광운대학교 전자통신공학과(공학석사)
・2007년 2월 : 광운대학교 전자통신공학과(공학박사)
・2012년 3월 ~ 현재 : 남서울대학교 조교수
・관심분야 : VR, S/W Platform
・E-Mail : khlee@nsu.ac.kr