Smart Media Journal / Vol.7, No.4 / ISSN:2287-1322
http://dx.doi.org/10.30693/SMJ.2018.7.4.52

마이크로그리드 환경에서 EMS와 원격 장치간 통신 보안

(Securing communication between EMS and remote devices in a Microgrid)

김미선*, 박경우**, 김종만***, 서재현**

(Mi-sun Kim*, Kyung-Woo Park**, Jong-Man Kim, Jae-Hyun Seo**)

요 약

마이크로그리드(MG:Microgrid)의 에너지 관리 시스템(EMS:Energy Management System)은 마이크로그리드 내 기기로부터 데이터를 수집, 분석하여 운영자를 비롯하여 사용자 및 타 시스템에 정보를 제공한다. 이 과정에서 유무선 통신망을 통하여 안전하게 정보를 제공하기 위한 방법이 필요하다. 본 논문에서는 마이크로그리드 내의 장치로부터 데이터를 수집하는 RTU(Remote Terminal Unit)와 EMS간의 데이터 전송 과정에서 발생 가능한 데이터의 노출 및 변조로부터 안전한 시스템을 개발하기 위하여 암/복호화, 키 관리 및 키 분배, 메시지 인증 기능을 제공하는 모듈을 설계, 구현하였다. RTU에 대해 하나의 VD(Virtual Device)를 연결하여 통신함으로써 RTU에 대한 연결 관리 및 키 관리의 효율성을 증대할 수 있다.

■ 중심어 : 마이크로그리드; 에너지 관리 시스템; 메시지인증; 키 관리; 기밀성

Abstract

Energy Management System(EMS) of Microgrid(MG) collects and analyzes data from devices in the microgrid to provide information to operators, users and other systems. In the middle of the process, it is required to securely provide information through both wired and wireless communication networks. In this paper, we design and implement a module that provides encryption and decryption, key management, key distribution, and message authentication functions, thus enabling the development of a system which is safe from the exposure and modulation of data potentially occurrable during data transmission between RTU(Remote Terminal Unit) and EMS. Our method can increase the efficiency of connection and key management for RTU by connecting a virtual device(VD) to RTU.

■ keywords : Microgrid; EMS; Message Authentication; Key Management; Confidentiality

Ⅰ. 서 론

최근 에너지 문제를 해결하기 위한 방안으로 기존의 전력망에 IT 기술을 융합한 스마트그리드(Smartgrid)가 제안되었으며, 이에 대한 실현방안으로 신재생에너지원을 기반으로 하는 소규모 전력망인 마이크로그리드 개념이 제안되어졌다[1]. 마이크로그리드의 복잡한 제어 구조와 에너지의 효율적 운용을 위하여 필요한 것이 에너지관리시스템(Energy Management System, EMS)이다[2].

스마트그리드 환경은 기존 SCADA(Supervisory Control And Data Acquisition)시스템의 통신 방식에 이더넷, TCP/IP 및 무선통신 기술을 접목하여 EMS 등 다양한 구성요소들과 유기적인 데이터 통신을 가능하게 하였다. 기존 SCADA 영역은 외부 통신망과의 독립된 폐쇄성을 유지하고 있었으나, 스마트그리드 시스템은 외부의 네트워크와 다양한 경로를 통해 상호 연결되는 형태를 취함으로써 보안 위협이 증가하였다[3].

따라서, 보안 요소를 고려하지 않았던 SCADA 제어 시스템의 프로토콜에도 보안적인 요소가 필요하였으며, 보안 인증과 키 교환 매커니즘을 권고하는 DNP3(Distributed Network Protocol 3)가 배포되었다. 그러나, 제어 시스템의 가용성이 우선시 되는 특성과 기존 디바이스들의 성능 문제로 실제로 DNP3가 권고하는 보안 표준이 적용된 사례는 드물다[4].

본 논문에서는 외부망으로 연결된 마이크로그리드내 EMS와 RTU간의 통신에서 데이터의 무결성과 기밀성을 제공하기 위한 원격 통신 보안 기술을 제안하였다. 이를 위해 본 논문에서

* 정회원, 목포대학교 정보보호학과
** 정회원, 목포대학교 융합소프트웨어학과
*** 전남도립대학교 신재생에너지전기과
본 논문은 한국전력공사지원 스마트 에너지 캠퍼스 사업으로 지원된 연구임.

접수일자 : 2018년 09월 12일
수정일자 : 1차 2018년 09월 27일, 2차 2018년 10월 22일
게재확정일 : 2018년 10월 30일
교신저자 : 박경우, 서재현 e-mail : kwpark@mokpo.ac.kr, jhseo@mokpo.ac.kr

는 EMS 내에 보안 관리자 모듈을 구성하여 RTU와 EMS간 전송되는 데이터에 대해 암/복호화, 키관리 및 키 분배, 무결성 검증 기능을 제공한다.

본 논문은 2장 1절에서는 스마트그리드의 구조 및 보안 표준, 키 관리 기술에 관한 관련연구를 기술하고, 2절에서는 본 논문에서 제시하는 마이크로그리드의 EMS 시스템 구성에 대해 설명한다. 3절은 EMS 시스템 내 보안관리자 모듈의 설계 및 구현에 대한 부분으로 본 논문에서 제안한 키 관리 및 분배과정, 암/복호화 과정, 메시지 인증을 이용한 무결성 인증 과정에 대해 기술하고 Casper/FDR[5] 툴을 사용한 시스템 검증 결과를 보인다.

Ⅱ. 본 론

1. 관련연구

가. 스마트그리드 구조

스마트그리드는 에너지 효율성을 극대화하기 위하여 발전, 송전, 배전, 분산전원, 가정, 공장, 빌딩 등의 기존 전력 인프라에 ICT를 융합한 복합 시스템으로 공급자로부터 소비자까지 전력을 공급하는 과정에서 신뢰성과 투명성을 제공하기 위하여 양방향 디지털 통신망을 사용한다.

스마트그리드를 구성하는 요소는 전력의 송배전 등을 관리하는 SCADA, 전력 정보의 전달을 위한 통신로, 고도화된 검침기반 시설(AMI:Advanced Metering Infrastucture), 사용자와 기기간 정보 전달을 위한 인터페이스 등이 있다[6].

전통적인 전력시스템은 폐쇄적인 SCADA 네트워크를 기반으로 운영되었기 때문에 최소한의 보안강도가 보장되었지만, 스마트그리드 하에서는 개방형 통신망과 연계되면서, 기존의 사이버 보안 위협들이 전력시스템으로 유입하게 된다[7].

스마트그리드는 그림 1과 같이 전력을 생산, 전송, 분배하는 물리적 전력시스템과 데이터의 교환, 통신, 처리를 수행하는 사이버 시스템의 결합으로 이루어져 에너지 효율성을 극대화할 수 있는 등 장점을 제공하고 있으나, 이로 인한 다양한 보안 취약점이 야기될 수 있다[8].

스마트그리드에 대한 보안 취약점은 물리적 전력시스템에 대한 공격뿐만 아니라 사이버 네트워크를 통한 공격이 포함된다.

본 논문에서는 스마트그리드의 보안 위협 중 데이터의 교환, 통신, 처리를 수행하는 사이버 시스템 영역에서 발생 가능한 보안 위협에 대한 보안 기술에 대한 연구를 수행하고자 한다.

스마트그리드의 사이버 시스템 영역에서의 주요 보안위협으로 비인가 접근에 따른 보안 위협, 통신 데이터 유출에 따른 보안 위협, 통신 데이터 위•변조에 따른 보안위협 등이 있다. 이를 위한 보안 요구로 기기인증, 데이터의 기밀성, 데이터의 무결성, 데이터의 부인방지, 네트워크 접근제어 등의 기술이 필요하다.

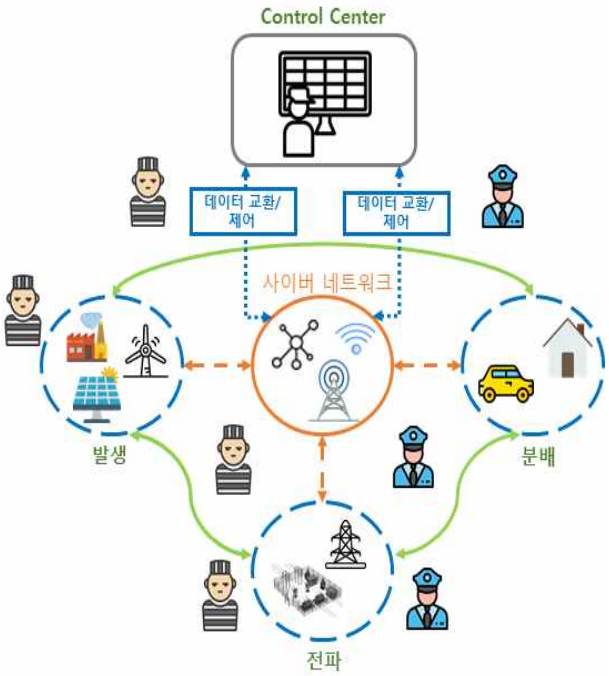

그림 1. 스마트그리드 구조와 보안 취약점

나. 스마트그리드의 보안 표준

SCADA 시스템의 보안성 향상을 목표로 ISO/IEC TC57 WG15에서 권고하고 있는 IEC 62351 표준[9]은 IEC 60870-5, IEC 61850, IEC 61970, IEC 61980을 기반으로 하는 전력자동화 프로토콜의 정보보안을 위한 표준으로 전자서명, 도청 예방, 침입탐지, 네트워크 및 시스템 관리, 역할기반 접근제어(RBAC, Role Based Access Control), 인증 및 보안 키 관리 등 스마트그리드 연계 정보의 보호방안을 제시하고 있다. IEC 62351 표준은 TCP/IP를 사용하는 전력 제어통신망에서 보안 강화를 위해 패킷 필터링을 구현하고 있으며, 기존 정보보안기술을 전력 제어시스템에 적용하여 전력통신 보안을 구현하였다. IEC 62351-4는 제어시스템의 무결성 유지를 위해 해시알고리즘과 디지털서명기술을 사용하고 접근통제와 도청방지를 위해 IETF RFC2246 TLS를 채택하였다. 중앙 제어장치(Master Station)와 현장 운영장치간 (Outstation)의 인증 암호화 메커니즘을 위해 2006년 발표된 IEC 62351-3과 IEC 62351-5에서의 권고사항인 TCP/IP에서 TLS 암호화 방식 및 메시지 인증 방식에 관련된 DNP3 profile을 수용하고 이를 실제적 구현할 수 있도록 구체화하여 2007년 3월에 DNP3 SA(Secure Authentication)을 발표하였다.

DNP3는 기존 전력 제어 시스템에 TCP/IP 네트워크를 지

원하는 통신 프로토콜로 SCADA 시스템의 표준인 IEC 60870-5를 기반으로 만들었으며, 원격지에 위치한 현장 운영장치로부터 정보수집, 제어명령 송신을 목적으로 하는 SCADA 시스템에 최적화되어 설계된 표준 통신 프로토콜이다. 2010년, DNP3는 IEEE Std 1815™-2010으로 배포되었고, 2012년 재개정을 통해 보안 인증과 키 교환 매커니즘을 제시하고 있다[3,10]. DNP3 프로토콜은 SA(Secure Authentication)을 포함하고, 트랜스포트 계층에서 기밀성 및 인증 기능을 제공하기 위하여 TLS(Transport Layer Security)를 사용하기를 권고한다. DNP3에서 키 교환은 1024비트의 RSA나 Diffie-Hellman 알고리즘을 사용한다. DNP3 SA는 버전5까지 보완되면서, 기존 버전이 갖고 있는 구조적 문제점을 해결하기 위해 취약한 사양들을 삭제하여 보안성을 높여 Smart Grid Interoperability Panel Cyber Security Working Group이 제안한 스마트 그리드를 위한 보안 표준 요구사항을 충족하였으나, 하위버전과는 호환이 되지 않는다. 또한, 폐쇄망 기반에 맞추어 개발되었기 때문에 인터넷과 같은 외부망과의 연결을 통한 공격 위협에 대한 보안성 향상이 필요하다.

제어 시스템의 가용성이 우선시 되는 특성과 기존 디바이스들의 성능 문제로 실제로 DNP3가 권고하는 보안 표준이 적용된 사례는 드물다. 인증과 암호화라는 보안 요소가 고려되지 않은 DNP3 프로토콜은 일반 네트워크의 스푸핑(spoofing), 변조(modification)등의 많은 공격 위험을 가지고 있다[4].

따라서, 본 논문에서는 외부망으로 연결된 마이크로그리드내 EMS와 RTU간의 통신에서 데이터의 무결성과 기밀성을 제공하기 위한 원격 통신 보안 기술을 제안하였다.

다. 스마트그리드의 키 관리 기술

스마트그리드에서 데이터의 무결성과 기밀성을 제공하기 위하여 키 관리 기술이 연구되고 있는 분야는 SCADA와 AMI 부분이며, SCADA에서 키 관리 기술에 대해 살펴본다.

SKE[11]에서는 SCADA 기반의 키 관리를 위하여 SUB-MTU(SUB-Master Terminal Unit) 와 RTU(Remote Terminal Unit) 또는 MTU와 RTU사이의 통신에서 사용되는 C-S(Controller to Subordinate) 통신을 기반으로 키 관리 방식을 구성하였다. 이 방식에서 SUB-MTU는 제어장치가 되고, RTU는 종속장치가 되며, KDC(Key Distribution Center)를 통해 각 장치의 키를 관리한다. 통신하는 두 장치간 GK(General Key)를 공유하며, 각 세션 통신에서는 GK를 통해 생성된 세션키 SK를 사용한다. 만일 GK가 공격자에 의해서 공격 받게 된다면 제어장치가 다시 GK를 생성하여 업데이트 한다.

SKMA[12]는 SCADA 시스템을 위한 키 관리 방식이다. SKMA에서 노드는 RTU, SUB_MTU, MTU가 될 수 있으며, KDC를 통한 3자간 키 확립 프로토콜을 사용한다. SKE가 공개키 암호 알고리즘을 사용하는 반면 SKMA는 대칭키 암호 알고리즘으로만 이루어져 있다는 장점이 있다[13].

본 논문에서는 SKE와 SKMA 키 관리 방식을 EMS와 RTU의 보안 통신을 위한 키 생성 및 분배 방식에 적용하도록 구현하였다. 제안하는 키 관리 방식은 마이크로그리드에 적용가능하도록 설계하여 RTU와 RTU간 직접 통신은 고려하지 않았다. 또한, 성능 제한을 가진 RTU가 보관해야할 키의 개수를 고려하였다.

표1은 기존의 관련 연구와 본 논문의 키 관리 방식을 비교한 것이다. 키 관리 기술의 기능적 요구사항으로 스마트그리드 내 RTU-RTU 간 직접 통신여부, 적용 알고리즘, RTU가 저장하는 키의 갯수 및 키 생성 주체로 분류하였다.

표 1. 키 관리 기술 비교 분석

기능적 요구	SKE	SKMA	제안방식
RTU-RTU통신	불가능	가능	불가능
적용알고리즘	공개키 알고리즘	대칭키 알고리즘	대칭키 알고리즘
RTU 저장 키 갯수	4	2	2
키 생성 주체	KDC	KDC	EMS내 보안 모듈

2. 제안된 마이크로그리드 EMS 시스템

가. 마이크로그리드 EMS 시스템 구성도

마이크로그리드는 마이크로그리드 내의 분산전원의 발전을 관리하며, 이에 맞게 부하를 조정하며 잉여전력은 에너지 저장장치에 저장을 하는 방식으로 독립적인 운전이 가능하다. 이를 위해 각 마이크로그리드에는 마이크로그리드 관리 시스템이 존재하며, 마이크로그리드의 필드 데이터 취득 및 관리 제어 기능과 분산전원의 발전 관리, 에너지 저장 장치의 관리, 전기 자동차의 활용, 이에 따른 전력 거래 등 여러 기능을 수행하게 된다[14].

본 연구에서 마이크로그리드 EMS 시스템은 그림2와 같이 구성하며, PV(Photovoltaic), PCS(Power Conditioning System), INV(Inverter), BMS(Battery Management System), ESS(Energy Storage System), 각종 센서 등 분산에너지 장치로부터 정보를 수집, 처리, 분석하여 사용자 및 운영자에게 서비스를 제공한다. 이를 위해 VD(Virtual Device), 분산운전 알고리즘, 자율운전 알고리즘, 최적화 알고리즘, 가상장치 관리자 및 보안관리자(Security Manager) 모듈로 구성한다. 구현 시스템에서 EMS는 물리적으로 안전한 곳에 설치된다고

가정하였으며, RTU와는 외부 통신망으로 연결된다.

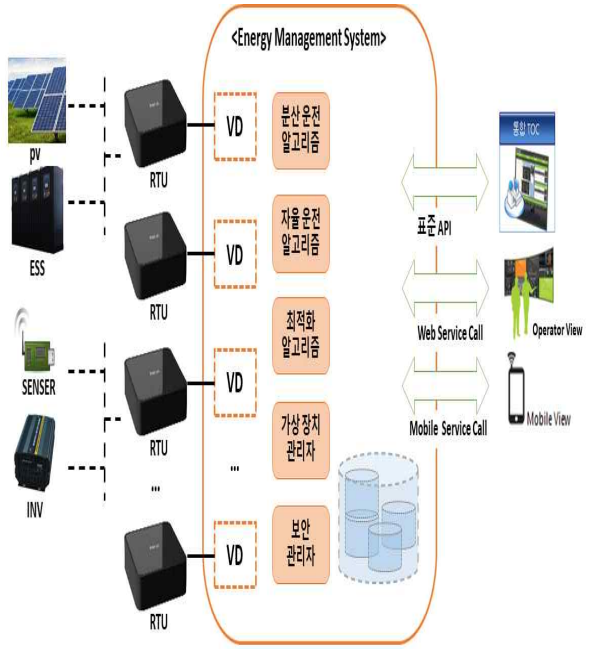

그림 2. 마이크로그리드 EMS 시스템

마이크로그리드 EMS시스템을 구성하는 RTU와 VD는 다음과 같이 정의한다.

·RTU

RTU는 원격지에 설치되어 분산 에너지 장치로부터 정보를 수집하고 이를 EMS에 전송하기 위한 게이트웨이로 동작한다. RTU는 EMS의 제어 명령에 따라 다른 장치들을 제어하는 역할을 수행하기도 한다.

·VD

VD는 각 RTU와 직접 통신하며 데이터를 수집, 제어하는 역할을 수행하며, RTU가 마이크로그리드 내에 추가될 때 가상 장치관리자를 통해 VD를 플러그인 방식으로 생성하고 RTU와 연결한다.

마이크로그리드내의 분산 에너지 장치와 RTU는 시리얼 통신으로 연결되며, RTU와 EMS 및 사용자 서비스는 TCP/IP 네트워크로 연결된다.

나. RTU와 VD간 설정

본 연구의 마이크로그리에서 RTU는 하나 이상의 분산 에너지 장치에 연결될 수 있으며, EMS에 연결되어 데이터 수집 및 제어메시지 전달의 역할을 수행한다. SCADA 구조에서 RTU는 SUB-MTU 또는 MTU와 통신하며 데이터 전달의 역할을 수행하는데 반해, 본 논문에서는 EMS와 직접 연결되어 RTU의 효율적인 관리를 위하여 RTU와 1:1로 연결될 수 있는 VD를 사용한다. 마이크로그리드 내에 새로운 RTU가 연결되면 EMS는 해당 RTU와 연결하기 위한 VD를 생성하고, VD는 RTU로 부터 데이터 수집, 제어 정보 전송 기능을 수행한다. 각 RTU에 대해 하나의 VD를 연결함으로써 RTU의 연결 및 해제 등의 관리를 효율적으로 수행할 수 있다.

RTU와 VD간 통신은 초기설정, 통상운영, RTU 제어의 세 가지 과정으로 나눌 수 있다.

첫 번째 초기설정은 RTU가 마이크로 그리드 내에 연결되어 EMS 에 등록하는 과정으로 RTU는 자신의 시리얼번호를 넘김으로써 VD와 연결될 수 있다.

두 번째 통상운영과정은 데이터 수집과정으로 RTU가 연결된 각 그리드내 장치로부터 데이터를 수집하여 VD에 전송하는 과정이다.

세 번째 RTU 제어 과정은 EMS가 장치에 대한 제어정보를 RTU에 전송하여 각 장치를 제어하는 과정이다.

본 연구에서 EMS는 RTU와 직접 통신하지 않으며, 각 RTU에 대한 모든 통신은 RTU와 연결된 VD를 거쳐 수행된다. 또한, 두 장치간 통신시에 데이터의 기밀성과 무결성을 보장하기 위한 암호화 및 메시지 인증을 위하여 두 장치간 공유키를 사용한다.

3. 보안관리자 모듈 설계 및 구현

가. 보안관리자 모듈

본 논문의 EMS 시스템은 마이크로그리드 내 RTU와 통신하며 RTU 등록 및 관리, 데이터 수집, 제어메시지 전송 등을 수행하기 위하여 VD를 사용한다. 각 장치와 RTU간에는 시리얼 통신으로, RTU와 VD는 TCP/IP를 통해 통신하게 되어, 통신상에 데이터는 개방된 공간에서 노출의 위협을 포함하고 있다.

보안 관리자 모듈은 RTU와 VD간의 통신과정에서 데이터의 변조 및 노출로부터 데이터를 보호하고, 전송 데이터에 대한 무결성을 검증하기 위하여 암/복호화, 키 관리 및 키 분배, 메시지 인증 기능을 제공하며, EMS의 하나의 모듈로서 구성된다.

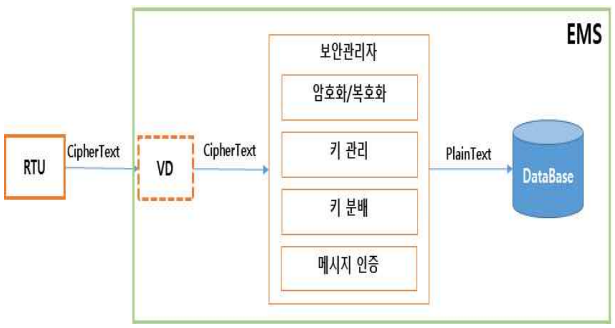

그림 3. 보안관리자 모듈과 데이터 기밀성 제공방식

그림 3은 EMS 내 보안관리자 모듈 구성과 데이터 기밀성 제공방식을 보이고 있으며, RTU가 각 장치로부터 수집한 데이터를 정규화 처리한 후 암호화하여 전송하면, EMS의 RTU와 연결된 VD가 이를 수신하고 보안 관리자 모듈을 통해 복호화 과정을 거친 후, 데이터베이스에 저장된다.

EMS에서 보안관리자 모듈은 키 분배 센터의 역할을 수행하며, 각 RTU와 VD를 위한 식별자 정의, 키 생성 및 키 분배를 수행한다. 보안 관리자 모듈은 각 VD와 RTU 간 공유되는 비밀키를 생성한다. 비밀키는 RTU와 VD간 실제 전송되는 데이터를 암호화하는데 사용되는 세션키를 생성하는데 사용된다. 또한 메시지 인증 과정에서 메시지 인증코드를 생성하는데도 사용된다.

나. 키 생성 및 분배

본 논문에서 키 생성 및 분배는 SKE[12]의 키 생성과정과 SKMA[13] 방식의 3자간 키 확립 프로토콜을 기반으로 하는 키 관리 방식을 제안하고자 한다.

통신과정에서 전송되는 데이터의 기밀성과 무결성을 보장하기 위하여 초기 설정단계에서 두 장치간 공유할 비밀키를 분배하는 과정이 필요하다.

이를 위해 VD는 그림 4와 같이 RTU의 초기 설정 과정에서 RTU의 시리얼 넘버를 받아 장치를 설정한 후, RTU의 식별번호와 VD 자신의 식별 번호를 전송하고, 키 공유를 위한 초기화를 요청한다.

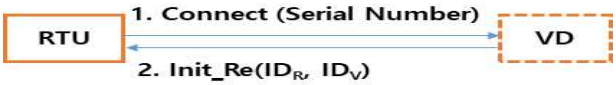

그림 4. 비밀키 설정을 위한 RTU와 VD 초기 설정 과정

VD와 RTU간 공유할 비밀키 생성은 SKE의 C-S(Controller to Subordinate) 통신을 사용하여 보안관리자가 제어장치, VD와 RTU는 종속장치가 된다. 제어장치인 보안관리자가 두 종속장치간 공유할 비밀키를 생성하여 분배하며, 분배된 키는 RTU와 VD간 데이터 전송시 암/복호화에 사용되는 세션키를 생성하는데 사용된다. 보안관리자가 두 노드간 공유할 비밀키를 생성하여 분배하는 과정은 SKMA 방식을 따른다.

표2는 Security Manager, VD, RTU간 비밀키를 분배하는 프로토콜에서 사용되는 프로토콜 파라미터와 그에 대한 설명을 보이고 있다.

표 2. 프로토콜 사용 파라미터

파라미터	의미
ID_V,ID_R	VD, RTU 식별자
N_V,N'_V,N_R	VD, RTU가 생성한 랜덤값
K_V	초기 배포된 SM-VD 공유키
K_R	초기 배포된 SM-RTU 공유키
K_{VR}	VD-RTU간 공유 비밀키
SK_{VR}	VD-RTU간 데이터암호화 세션키
TS	타임스탬프

그림 5는 Security Manager, VD, RTU간 비밀키를 분배하는 프로토콜 과정을 보이고 있다. 제안된 시스템에서 각 RTU는 EMS 내의 VD와 1:1로 연결되어 통신한다. RTU는 시스템에 연결되기 전에 EMS의 보안 관리자에게 초기 공유키를 배포받아 설치하게 된다.

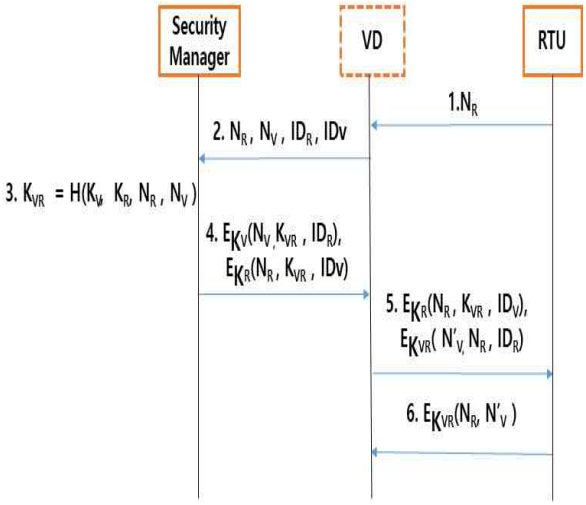

그림 5. 비밀키 생성 및 분배 프로토콜

VD로부터 공유키 설정을 위한 초기화 연결 요청을 받은 RTU는 초기 랜덤값 N_R을 VD에 전송하고, VD는 자신의 랜덤값 N_V와 식별자, RTU의 랜덤값, N_R과 식별자를 보안관리자에게 전송한다. 보안관리자는 N_V, N_R, K_V, K_R에 해쉬함수를 적용하여 VD와 RTU 간 공유 비밀키인 K_{VR}을 생성한 후, VD, RTU의 초기 배포 공유키로 암호화한 데이터를 VD로 전송한다. VD는 보안관리자로부터 받은 $EK_R(N_R , K_{VR} , IDv)$와 공유 비밀키로 VD의 랜덤값 N'_V를 암호화한 $EK_{VR}(N'_V, N_R , ID_R)$를 RTU로 전송하며, RTU는 복호화를 통해 N'_V를 찾아 이를 다시 암호화 한 $EK_{VR}(N_R, N'_V)$를 VD에 보냄으로써 공유 비밀키 분배 과정을 종료한다.

RTU와 VD에게 분배된 공유 비밀키 K_{VR} 은 이후 VD와

RTU간 수집 데이터의 통신과정에서 데이터 암호화를 위해 사용되는 세션키를 생성하는데 사용된다. 세션키 SK_{VR}은 RTU와 VD간 공유 비밀키 K_{VR}과 타임스탬프 값을 병합한 후, 해쉬하여 생성한다.

보안 관리자 모듈은 RTU와 VD에 설정된 초기 배포 공유키, RTU, VD 식별자, K_{VR} 등을 암호화하여 데이터베이스에 저장, 관리한다. 제안하는 키 관리 방식은 EMS와 RTU간 안전한 통신을 수행하고 제한된 성능을 가진 RTU가 보관하는 키의 개수를 최소화 할 수 있도록 RTU는 하나의 VD와의 연결만을 갖으며 이 연결에 필요한 키만을 공유하도록 한다. 이러한 키 관리 방식을 통해서 하나의 RTU는 최대 2개의 키만을 보유하게 되고, 키의 변조나 유출이 다른 RTU의 연결에는 영향을 미치지 않는다.

RTU와 VD간 공유키인 K_{VR} 이 공격자에 의해 노출, 변조되었다고 판단될 경우, 보안관리자 모듈은 RTU와 기존의 VD와의 연결을 끊고, 해당 VD와 연관된 정보만을 폐기한다. 그리고 RTU에 새로운 VD를 연결하여 키 공유를 위한 초기화를 요청하고 K_{VR}을 다시 생성하여 새로운 키를 사용하도록 통보한다. 기존의 키 분배 방식에서는 키 철회를 위해 KDC가 모든 노드에 키 철회 사실을 브로드캐스팅을 통해 알려야한다[6]. 그러나, 본 방식에서 RTU는 하나의 VD와의 통신만을 수행하기 때문에 두 장치간 키가 공격을 받았을 경우에도 다른 연결에는 영향을 미치지 않는다.

다. 데이터 기밀성 제공을 위한 암/복호화

EMS는 RTU로부터 마이크로그리드 내 스마트 기기 및 센서, 전력장치로부터 데이터를 수집, 저장, 관리하는 역할을 수행한다. RTU가 전송하는 데이터는 전력 운영관련 중요 정보 및 개인 프라이버시 침해가 우려되는 검침 정보등이 포함될 수 있어 데이터 기밀성 기능이 필요하다. 이를 위해 EMS 내에 RTU와 1:1로 통신하는 VD를 두어 RTU로부터 암호화된 데이터를 수집하여 기밀성을 제공하고자 한다. 데이터의 암호화를 위해 VD와 RTU는 초기 설정 단계에서 보안관리자가 생성한 비밀키를 공유하는 과정을 거치게 된다.

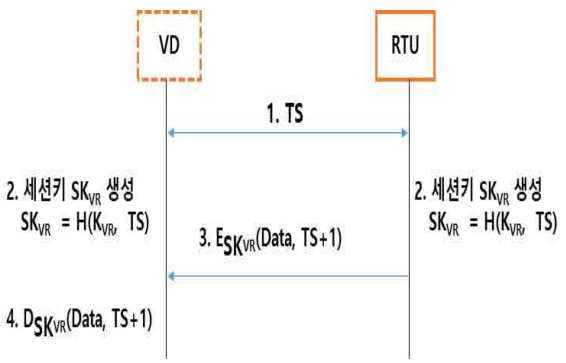

그림 6. 세션키 생성 및 데이터 암/복호화 과정

그림 6은 세션키의 생성 및 데이터 암/복호화 과정을 보이고 있으며, 공유된 비밀키 K_{VR}은 타임스탬프값(TS)과 함께 병합한 후 세션키를 생성하는데 사용된다.

RTU는 수집 데이터를 VD에게 전송하기 전에 각 장치로부터 수집된 데이터를 정규화 한 후, 세션키를 사용하여 암호화하여 VD에 전송한다. VD는 RTU로부터 수신한 데이터를 보안관리자 모듈에 전송하고, 보안관리자는 이를 복호화하여 데이터베이스에 저장한다.

라. 메시지인증 기법을 적용한 무결성 검증

해쉬함수를 사용하여 RTU에서 VD로 전송되는 데이터에 대한 메시지 인증과 VD에서 RTU로 전송되는 제어 메시지에 대한 인증을 통하여 데이터 무결성을 제공한다.

그림 7은 RTU가 수집된 데이터를 VD에 전송시 데이터의 무결성을 검증하기 위한 과정을 보이고 있다. RTU에서 전송되는 데이터는 세션키를 사용하여 암호화된 후 공유 비밀키(K_{VR})를 이용하여 MAC(Message Authentication Code)을 생성한 후, 암호화된 전송데이터와 함께 VD에 전송한다. VD는 전송된 데이터에 대해 해쉬값을 생성한 후 이를 비교하여 데이터의 무결성을 검증한다.

RTU가 VD에 전송하는 암호데이터(M)은 앞 절 세션키를 이용한 암/복호화 과정에서 생성된 $E_{SK_{VR}}$(Data, TS+1)을 의미한다.

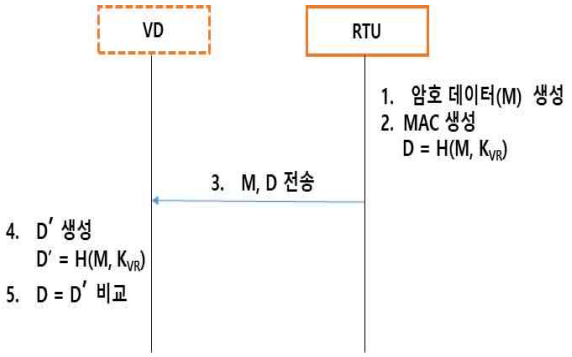

그림 7. 데이터 무결성 검증

그림 8은 EMS가 보내는 제어 메시지를 VD를 통해 전송하는 과정으로 제어메시지에 대해 공유 비밀키를 이용하여 해쉬한 후 RTU에 전송한다. RTU는 전송된 제어메시지에 대해 해쉬값을 생성한 후 이를 비교하여 제어 메시지의 무결성을 검증한 후, 이를 연결된 기기에 전송한다.

메시지인증 기법을 적용한 무결성 검증 과정에서 RTU의 프로세스를 최소화하기 위하여 제어메시지에 대해서는 암/복호화 기능을 사용하지 않고 해쉬만을 사용하여 제어 메시지의 무결성만을 체크하도록 하였다.

그림 8. 제어메시지 무결성 검증

마. 보안 관리자 모듈 구현 및 보안성 검증

(1) 시스템 구현

본 논문에서 제안한 스마트 그리드의 EMS 시스템의 데이터 기밀성 및 무결성을 제공하는 RTU, 보안관리자 모듈을 구현하기 위하여 다음과 같은 환경을 구축하여 테스트하였다.

표 2. 구현환경

	RTU	EMS
하드웨어	라즈베리 파이 3	Intel
OS	라즈비안	윈도우10
개발언어	C#	
해쉬함수	SHA-256	
암호화알고리즘	SEED	

RTU는 다양한 전력장치 및 스마트그리드 내 기기에 연결될 수 있으며, 수집 데이터의 형식이 다를 수 있다. RTU는 정규화 과정을 거쳐 통신 데이터를 정규화한 후 바이너리디지트로 변경한다. 정규화된 데이터의 형식은 그림 9와 같다.

```
[inv_cap] => 6531
[stat2] => RUN
[pow_dcv] => 9530216110
[pow_dcp] => 2533105443
[grid_rv] => 1356802465
[grid_sv] => 5320044687
[grid_tv] => 9610404030
[time] => 2018090717354827
```

그림 9. 정규화된 데이터 형식

(2) 보안성 검증

본 논문에서는 RTU와 VD간 데이터 통신의 기밀성을 제공하기 위한 암호기술을 구현하였으며, 이를 검증하기 위하여 Casper/FDR 툴을 사용하였다.

FDR(Failures-Divergences Refinement)은 알지브라 언어인 CSP코드로 명세된 통신 프로토콜에 대해 정형적 검증을 수행하여 안정성과 보안성을 검증하는 도구이다. Casper는 CSP 코드 문법의 어려움을 해결하기 위해 옥스퍼드 대학에서 개발된 컴파일러이며 간단한 문법으로 검증 하고자하는 프로토콜을 기술할 수 있으며, 기술한 코드를 토대로 CSP 코드를 생성할 수 있다[10].

앞서 제안한 암호화 프로토콜 절차들을 Casper 언어로 명세하고, FDR의 정형적 검증을 통해 안정성과 보안성을 검증하고자 한다.

그림 10은 본 논문에서 명세한 프로토콜의 절차를 Casper 언어로 명세한 Protocol Description이다.

```
#Protocol description
0.          ->  RTU    : VD
1.  RTU     ->  VD     : Nr
2.  VD      ->  SecuM  : VD,Nr,Nv,RTU
3.  SecuM   ->  VD     : {Nv,Kvr,RTU}{IK(VD)}, {Nr,Kvr,VD}{IK(RTU)}%enc
4.  VD      ->  RTU    : enc % {Nr,Kvr,VD}{IK(RTU)}
5.  VD      ->  RTU    : {Nv2,Nr,RTU}{Kvr}
6.  RTU     ->  VD     : {Nr,Nv2,TS1}{Kvr}
7.  VD      ->  RTU    : {DATA,TS1}{SK(VD)}
8.  RTU     ->  VD     : {DATA,TS1}{SK(RTU)}
```

그림 10. Protocol Description

그림 11은 Specification 부분으로 프로토콜의 요구사항을 표현하였다. RTU와 VD 간에는 전송 데이터를, 보안관리자(SecuM)과 RTU, VD간에는 K_{VR}값에 대한 기밀성을 유지해야함을 의미한다. VD는 K_{VR}, N_R, Nv2m 데이터 값을 통해 RTU에 대한 인증을 확인하고자 한다.

```
#Specification
Secret(VD,DATA,[RTU])
Secret(SecuM,Kvr,[RTU,VD])
Agreement(VD,RTU,[Kvr])
Agreement(VD,RTU,[Nr,Nv2])
Agreement(VD,RTU,[DATA])
```

그림 11. Specification

그림10, 11과 같이 Casper 언어로 명세하고, 컴파일을 수행한 후 FDR을 이용하여 검증한 결과는 그림 12와 같이 나타났다. 그림 12와 같이 Specification에서 기술한 각 부분에 대해 Finished:Passed 값을 출력함으로써 본 논문에서 구현한 데이

터 기밀성을 위한 프로토콜에 대해 안전성을 검증하였다,

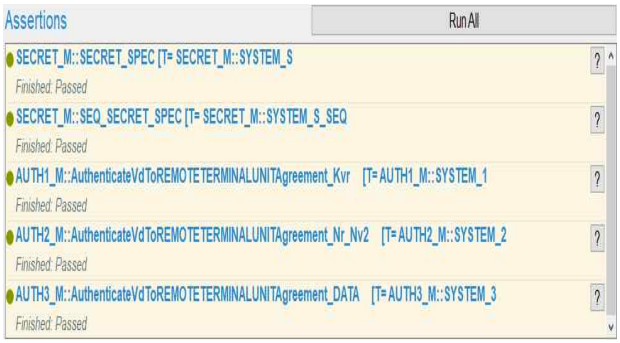

그림 12. Verification Results

III. 결 론

본 논문에서는 마이크로 그리드의 에너지 관리 시스템에서 수집, 운영, 관리하는 데이터의 기밀성 및 무결성을 제공하기 위하여 암/복호화, 키 관리 및 키 분배 기능을 제공하는 보안 관리 모듈을 설계하고 구현하였다. 본 논문에서 제안된 보안 관리자 모듈은 마이크로그리드 환경에 적합하게 구성하고자 하였다. 각 RTU로부터 데이터를 수집하기 위한 VD를 플러그인 방식으로 생성하고, 대칭키 암호방식을 적용하기 위하여 두 장치간 공유 비밀키를 생성하여 분배하였다. 이를 통해 RTU의 보관 키의 갯수를 최소화하고, 암/복호화 기능을 간소화할 수 있다. 또한, 정보 변조 및 유출이 발생하는 경우에는 다른 노드에는 영향을 주지 않고 RTU와 연결된 VD를 삭제한 후, 새로운 VD를 할당하여 새로운 키를 생성하여 관리함으로써 키의 안전성을 높일 수 있다.

EMS와 RTU간 통신 과정에 데이터의 무결성을 제공하기 위하여 해쉬함수를 사용하여 RTU에서 VD로 전송되는 데이터에 대한 메시지 인증과 VD에서 RTU로 전송되는 제어 메시지에 대한 인증을 수행하였다. RTU의 프로세스를 최소화하기 위하여 제어메시지에 대해서는 암/복호화 기능을 사용하지 않고 해쉬만을 사용하여 메시지 무결성만을 체크하도록 하였다.

본 연구는 마이크로그리드 환경에서 EMS 시스템과 원격장치간 통신 보안 연구로, 테스트베드 구축은 원격지 RTU와 EMS 시스템 간 통신상에서 키 분배 및 관리를 통한 데이터 암호화와 무결성 검증 여부를 테스트하기 위한 형태로 구현하였으며, 이후 지속적인 연구를 진행하기 위하여 스마트기기 및 센서들을 추가하여 확장구현하고 있다. 추후, 스마트그리드 시스템으로의 확장성을 위한 그룹 키 관리 방안 연구 및 마이크로그리드 EMS 시스템의 보안 위협 평가 방안에 대한 연구를 진행하고자 한다.

REFERENCES

[1] CERT, “Integration of Distributed Energy Resources: The CERTS MicroGrid Concept,” *LBNL-50829,* Oct. 2003.

[2] 조재훈, 박선홍, 이대홍, 조영임, 전명근, “마이크로그리드시스템의 분산 에너지관리시스템 설계를 위한 통합시뮬레이션 모델 개발,” *한국지능시스템학회 논문지*, 제21권, 제1호, 29-35쪽, 2011년 2월

[3] 박준용, 민남홍, 하기웅, 유기순, 송경영, “전력 제어시스템에서 안전한 보안 인증을 위한 메커니즘 소개,” *정보보호학회지*, 제24권, 제3호, 44-53쪽, 2014년 6월

[4] 권성문, 손태식, “제어시스템 DNP3 프로토콜 취약점과 보안현황,” *정보보호학회지*, 제24권, 제1호, 53-58쪽, 2014년 2월

[5] Casper : A Compiler for the Analysis of Security Protocols User Manual and Tutorial(2009), http://www.cs.ox.ac.uk/gavin.lowe/Security/Casper/manual.pdf(accessed Aug., 6, 2018).

[6] 최동현, 원동호, 김승주, “스마트그리드 환경에서의 키 관리 기술 동향 분석,” *정보보호학회지*, 제20권, 제5호, 2010년 10월

[7] 강동주, 김발호, 김휘강, “에너지 사용 맥락을 통한 AMI 네트워크에서의 데이터 이상 감지 방법론 제안,” *정보보호학회지*, 제24권, 제5호, 75-81쪽, 2014년 10월

[8] A. Sanjab, W.Saad, I.Guvenc, A.Sarwat and S.Biswas, "Smart Grid Security: Threats, Challenges, and Solutions," *arXiv:1606.06992v1 [cs.IT],* Jun. 2016.

[9] F. Cleveland, "IEC 62351 security standards for the power system information infrastructure," *IEC TC57 WG15 Security Standards ver 14*, Jun. 2012.

[10] IEEE, “IEEE Standard for Electric Power Systems Communications－Distributed Network Protocol (DNP3),” *7.Secure authentication*, pp.171-266, Oct. 2012.

[11] Cheryl Beaver, Donald Gallup, Willian Neumann, and Mark Torgerson, “Key Management for SCADA,”https://energy.sandia.gov/wp-content/gallery/uploads/013252.pdf, Mar. 2002.

[12] R.Dawson, C.Boyd, E.Dawson,and J.M.D.Nieto, “SKMA－A key management architecture for SCADA systems,” *in Proc. 4th Austral. Inf. Security Workshop*, vol. 54, pp. 183 - 192, Jan. 2006.

[13] D. Choi, H. Kim, D. Won, and S. Kim, “Advanced Key Management Architecture for

Secure SCADA Communications", *IEEE Transactions on Power Delivery*, Vol.24, No.3, pp.1154-1163, May. 2009.
[14] M. Zamani, T. Sidhu and A. Yazdani, "Investigations Into the Control and Protection of an Existing Distribution Network to Operate as a Microgrid: A Case Study", *IEEE Transactions on Industrial Electronics*, vol. 61, no. 4, pp. 1904-1915, Apr. 2014.
[15] 조재영, 나인호, "신재생에너지 연계형 에너지관리 장치의 운영 사례 연구," *스마트미디어저널*, 제7권, 제2호, 71-77쪽, 2018년 6월
[16] 차병래, 최명수, 박선, 김종원, "보안 강화를 위한 NFC 기반 전자결제 시스템의 2 팩터 인증 기술의 초안 설계," *스마트미디어저널*, 제5권, 제2호, 77-83쪽, 2016년 6월

저 자 소 개

김미선(정회원)
1996년 국립목포대학교 컴퓨터공학과 학사 졸업.
2000년 국립목포대학교 컴퓨터공학과 석사 졸업.
2007년 국립목포대학교 컴퓨터공학과 박사 졸업.
2012년 ~현재 국립목포대학교 정보보호학과 초빙교수
<주관심분야 : 정보보호, 프로그래밍 언어, 모바일 시스템 보안, 스마트그리드 보안, 사물인터넷 보안, 블록체인 기술>

박경우(정회원)
1986년 전남대학교 계산통계학과 학사 졸업.
1988년 전남대학교 전산통계학과 석사 졸업.
1994년 전남대학교 전산통계학과 박사 졸업.
1995년 3월~현재 국립목포대학교 융합소프트웨어학과 교수
<주관심분야: 컴퓨터공학, 분산 시스템, 시스템 소프트웨어, 정보보호 >

김종만(정회원)
1986년 전북대학교 전기공학과 학사 졸업.
1988년 전북대학교 전기공학과 석사 졸업.
1996년 전북대학교 전기공학과 박사 졸업.
2000년~현재 전남도립대학교 신재생에너지전기과 교수.
2010년~2015년 전남도립대학교 정보지원센터장, 취업지원센터장
1988년~1991년 현대중공업 산업전자개발부 연구원
1997년~1999년 (주)삼원그룹전기부 차장
2016년~현재 에너지밸리산학융합사업단장
1988년~현재 대한전기학회,한국전기전자재료학회,대한전자공학회,제어로봇시스템학회 정회원
<주관심분야 : 신경회로망,지능형센서응용,신재생에너지및 EMS시스템,제어계측 분야>

서재현(정회원)
1985년 전남대학교 계산통계학과 학사 졸업.
1988년 중앙대학교 전자계산학과 석사 졸업.
1996년 전남대학교 전산통계학과 박사 졸업.
1996년 9월~현재 국립목포대학교 정보보호학과 교수
2005년 1월~현재 한국정보보호학회 부회장
2015년 3월~현재 한국정보처리학회 부회장
<주관심분야: 정보보호, 시스템 및 네트워크보안, 스마트그리드 보안, 사물인터넷보안, 블록체인 기술 >