RESEARCH

KEPCO Journal on Electric Power and Energy
p-ISSN 2465-8111, e-ISSN 2466-0124
Volume 6, Number 2, June 2020, pp. 129-135
DOI 10.18770/KEPCO.2020.06.02.129

Lightweight Energy IoT Standard Protocol and Test Certification Procedure

에너지 IoT 표준 프로토콜 경량화 및 시험인증절차에 관한 연구

Myunghye Park, Younghyun Kim, Nogil Myoung, Sukyung Kang, Changsoo Eun
박명혜, 김영현, 명노길, 강수경, 은창수

Abstract

The standardization of e-IoT (energy Internet of Things) communication and service, which is the energy field of energy, is to define the standard model and to demonstrate the practical model in order to take the lead and occupy the market where new market is created with the latest technology. In particular, detailed technical specifications are defined for developing a framework for IoT technology, the foundation technology of the 4th Industrial Revolution, securing interoperability through standardization, and operating a standard platform. In this paper, we propose a method for e-IoT standard protocol lightening and test certification procedure. The proposed method provides a product implementation method that can solve the problem of low power issue of e-IoT product in the future.

에너지분야 사물인터넷기술인 e-IoT 통신 및 서비스의 표준화 분야는 최신 기술로 새로운 시장이 창출되는 분야의 주도권을 확보하고 시장을 선점하기 위해 표준모델을 정의하고 실용모델을 실증하는 기술이다. 특히 4차 산업혁명의 기초 기술인 IoT 기술에 대한 프레임워크 개발, 표준화를 통한 상호연동성 확보, 표준 플랫폼의 운영 등을 위해 세부적인 기술규격들을 정의하고 있다. 본 논문에서는 e-IoT 표준 프로토콜 경량화 및 시험인증절차에 관한 방식을 제안한다. 제안된 방식은 향후 e-IoT 제품의 저전력 이슈에 대한 문제를 해결할 수 있는 제품 구현방안을 제공한다.

Keywords: *Energy IoT, LWM2M, CoAP, Interoperability*

I. Introduction

IoT (사물인터넷, Internet of Things)는 사물에 센서를 부착, 실시간으로 데이터를 주고받는 기술 또는 인프라를 일컬으며, 이를 통해 모든 사물에 새로운 가치를 부여함으로써 신성장 동력을 창출할 수 있는 중요한 기술로 언급되고 있다. IoT를 구성하는 기술은 크게 유무선 통신기술과 정보연계기술로 구분할 수 있으며, 특히 서로 다른 제조사가 만든 다양한 센서에서 얻어지는 데이터를 의미 있는 정보로 추출하기 위해서는 기기간 상호운용성을 보장하는 표준 및 가이드라인, 더 나아가 이를 손쉽게 활용, 제품 및 서비스를 개발할 수 있는 환경을 제공하는 것이 무엇보다 중요하다.

다양한 통신방식을 수용하고 제조사간 상호운용성 확보 및 개발편의를 제공하기 위해 IoT 공통기술인 디바이스 플랫폼(HDK, SDK)을 개발하였다. 통신방식으로는 LoRa, Wisun, Ethernet 인터페이스를 제공하고, IoT 산업계 표준으로 널리 활용되고 있는 LwM2M 국제표준 [6][7]을 디바이스와 게이트웨이에 탑재하였다. 특히 현장 요구사항인 저전력 운영을 위한 경량화, IoT 보안 취약성을 해결하기 위한 암호화·인증기술을 탑재, 최적화함으로써 다양한 사업에 손쉽게 활용될 수 있는 특징이 있다. 이처럼 개발된 기술은 2018년 4월 세계 최초로 LwM2M 인증을 획득하였으며, 전력 및 에너지 분야의 특화 기능에 대해 단체표준으로 제정함으로써 다양한 산업분야에 널리 활용될 수 있는 토대를 마련하였다.

디바이스 플랫폼은 IoT 산업의 확산을 위해 누구나 손쉽게 서비스를 창출할 수 있는 기반기술로서 활용될 수 있다. 일례로 고압아파트 수전설비 감시모니터링, 항공장애 등 원격감시 서비스 등 다양한 현장에서 사업화가 이루어지고 있으며, 이를 통해 IoT 서비스 확산을 위한 기반 인프라로 활용될 예정이다

본 논문의 구성은 다음과 같다. II장에서는 e-IoT 표준 프로토콜 기반 서비스 시스템을 소개하고, III장에서는 e-IoT의 경량화 방안으로 ID체계, 등록절차, 보안 프로파일, 현장단말 정보설정 등과 시험인증절차에 대해서 서술한다. 마지막으로 IV장에서는 결론을 맺는다.

Article Information

Manuscript Received October 18, 2019, Revised October 24, 2019, Accepted March 26, 2020, Published online June 30, 2020

M. Park, Y. Kim, N. Myoung, and S. Kang are with KEPCO Research Institute, Korea Electric Power Corporation, 105 Munji-ro Yuseong-gu, Daejeon 34056, Republic of Korea.
C. Eun is with Chungnam National University, 99 Daehak-ro, Youseong-gu, Daejeon 34134, Republic of Korea.

Correspondence Author: *Myunghye Park* (*myunghye.park@kepco.co.kr*)

This paper is an open access article licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International Public License.
To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0
This paper, color print of one or more figures in this paper, and/or supplementary information are available at http://journal.kepco.co.kr.

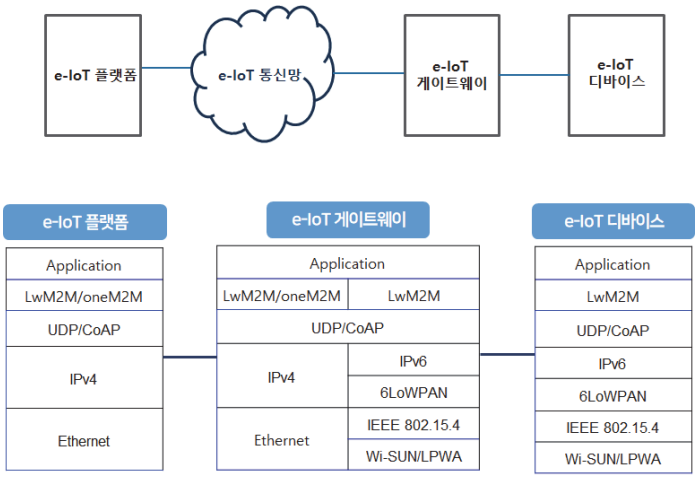

Fig. 1. e-IoT 서비스 시스템 구성도.

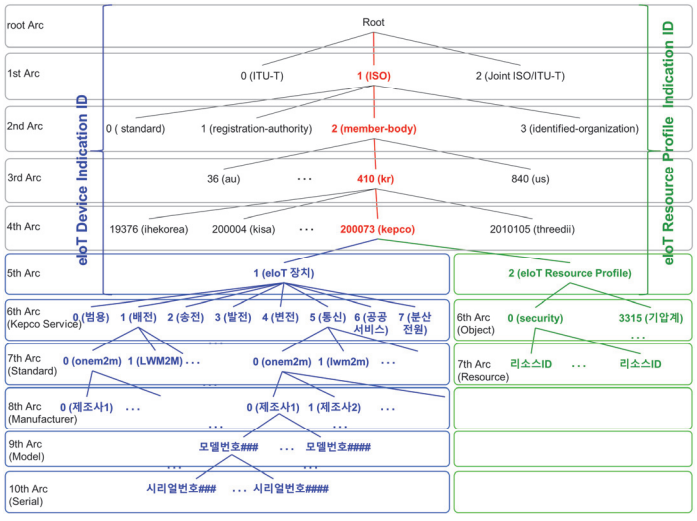

Fig. 2. OID 기반 한전 IoT 식별자 체계 개요.

II. e-IoT 표준 프로토콜 기반 서비스 시스템 개요

e-IoT 서비스 시스템은 종단의 전력에너지 시설에 부착되어 다양한 정보를 수집하는 e-IoT 디바이스, 디바이스들을 플랫폼에 연결해 주는 e-IoT 게이트웨이, 디바이스 관리 및 정보 수집을 통해 다양한 에너지 IoT 서비스를 가능하게 하는 e-IoT 플랫폼으로 구성된다 [1]-[5].

통신방식으로는 LPWA, Wi-SUN, Ethernet 인터페이스를 제공하고, IoT 산업계 표준으로 널리 활용되고 있는 LwM2M 국제표준을 디바이스와 게이트웨이에 탑재하였다. 특히 현장 요구사항인 저전력 운영을 위한 경량화, IoT 보안 취약성을 해결하기 위한 암호화·인증기술을 탑재, 최적화함으로써 다양한 사업에 손쉽게 활용될 수 있는 특징이 있다. 이처럼 개발된 기술은 2018년 4월 세계 최초로 LwM2M 인증을 획득하였으며, 전력 및 에너지 분야의 특화 기능에 대해서는 단체표준으로 제정함으로써 다양한 산업분야에 널리 활용될 수 있는 구조이다.

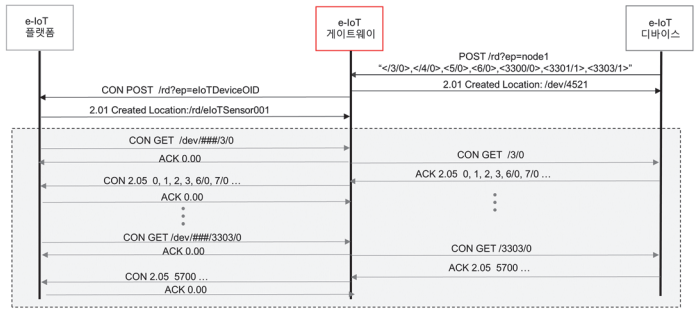

Fig. 3. LWM2M 전체 등록 절차(디바이스~게이트웨이~플랫폼).

III. 표준 프로토콜 경량화 방안

A. ID 경량관리 규격

한전 IoT 장치를 식별하는 목적으로 유일성을 보장할 수 있는 OID (Object IDentifier) 체계를 따른다 [1]. 한전 식별자, 한전 IoT 장치 식별자, 한전 IoT Resource 프로파일 식별자 체계를 하나의 트리로 표현하며 Fig. 2과 같다.

e-IoT 단말의 OID 체계를 따라 정의할 수 있다. 대역폭이 매우 낮은 무선 통신 구간 등을 고려할 때 OID를 경량화해서 사용할 수 있다. 한전에 사용되는 공통적인 부분을 제외하고 나머지 부분을 사용해서 정의한다. 예를 들어 아래와 같은 전체 Arc를 사용한 OID는 다음과 같다.

전체 OID: 1.2.410.200073.1.9.1.(제조사번호).(모델번호).(시리얼 번호)

이를 공통부분을 제외해서 다음과 같이 경량화 해서 사용할 수 있다.

실제 사용 OID: 1.9.1.(제조사번호).(모델번호).(시리얼 번호)

B. 등록절차 경량화

클라이언트 등록 인터페이스는 등록, 등록업데이트, 등록해제 동작으로 구성된다. 등록 동작은 서버에 클라이언트 및 Resource를 등록하는 것이며, 기본등록과 단순등록으로 나누어진다. 기본등록은 일반적인 경우에 사용되며, 단순등록은 데이터 통신 대역폭이 제한적인 경우에 사용된다. 등록 기능 인터페이스는 RFC 6690 CoRE 링크포맷(Link format) 기반의 Resource Directory를 이용한다. 클라이언트 Endpoint명 및 유효시간(Lifetime), 큐 모드(Queue mode)와 클라이언트가 지원하는 Object 및 Instance 정보 등을 서버에 등록한다. 일반적으로 UDP binding을 기본으로 하나, 슬립노드를 지원할 경우 'UDP with Queue Mode'로 설정한다. 등록기능(기본등록, 단순등록) LWM2M Client는 LWM2M Server에 시간 정보를 요청할 수 있다.

등록 요청 메시지를 받은 서버는 클라이언트의 IP 주소 및 포트를 저장한다. LWM2M은 복수개의 서버를 지원하므로, 클라이언트는 각 서버에 등록 기능을 수행할 수 있다. 클라이언트가 가지고 있는 기본 Object는 Security 및 Server, Access Control, Device, Connectivity Monitoring, Firmware Update, Connectivity Statistics 등이 정의되어 있다.

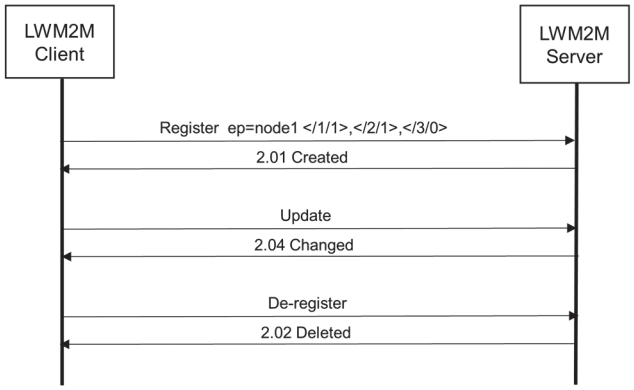

Fig. 4. LWM2M 기본 등록 동작.

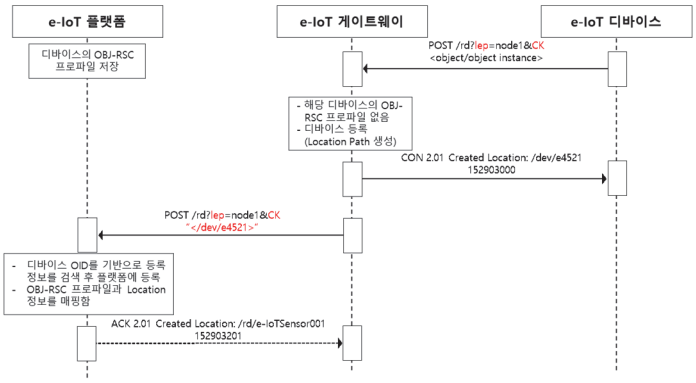

Fig. 5. LWM2M 단순등록 동작.

1) 기본등록 기능

등록 동작은 클라이언트의 전원이 켜지면 서버에게 'Register'를 전송하여 수행된다. 'Register' 메시지는 다음 파라미터를 포함한다.

① Endpoint Client Name (ep): 필수적으로 포함한다.
② Lifetime: 선택사항이 없을 경우 서버에서 86400을 기본값으로 설정한다.
③ LWM2M Version: 선택사항, 기본적으로 1.0 값을 넣는다.
④ Binding Mode: 선택사항, UDP binding은 U로 'UDP with Queue Mode'는 UQ로 표시한다.
⑤ Clock (CK): 선택사항, 시간동기 정보를 요청할 때 사용함. "GET" 옵션과 같이 사용할 수 없다.
⑥ Objects and Object Instances: 필수적으로 표시하는 항목으로 클라이언트가 갖고 있는 Object와 Object Instance 목록을 포함한다. RFC 6690에 정의된 Core Link Format (application/link-Format)형식으로 표현한다. 아래 예시는 LWM2M Server (1), Access Control (2), Device (3), Connectivity Monitoring (4), Firmware Update Object가 있는 경우이다.
예) </1/0>, </1/1>, </2/0>, <2/1>, <2/2>, </3/0>, </4/0>, </5>

Fig.4는 LWM2M 기본 등록 동작과정에서 시간동기 정보를 함께 요청한 과정을 설명한다. CK 옵션을 수신한 LWM2M 서버는 현재 시스템 시간 정보를 UNIX Time 형식으로 응답메시지 Payload에 포함하여 응답한다.

2) 단순등록 기능(Light-weight Registration)

단순등록 기능은 등록할 장치의 등록 정보, 즉 ObjectResource (OBJ-RSC) 프로파일 정보를 플랫폼에 미리 저장되어 있을 때 가능하다. OBJ-RSC프로파일은 LWM2M JSON형식으로 표현된다. 예를 들어 e-IoT 게이트웨이와 e-IoT 디바이스 제품을 설치하기 전에 제품 등록 과정을 통해서 OBJ-RSC 프로파일 정보를 오프라인 상에서 함께 등록한다. 오프라인으로 등록된 장치들의 정보는 실제 LWM2M 등록과정 이전에는 비활성화 되어 있다. 단순등록과정을 통해서 비로소 활성화될 수 있다.

단순등록은 플랫폼과 게이트웨이간 인터페이스 IFpg 구간과 게이트웨이와 디바이스간 인터페이스 IFgd 구간동작으로 구분된다. IFpg 구간 단순등록은 alternate path(예: /dev/e1234) 정보가 있을 경우, payload에 alternate path만 link-format으로 포함하고, alternate path가 없을 경우에는 payload에 아무 정보도 포함하지 않는다.

IFgd 구간 단순등록은 일반등록과 동일하게 payload에 Object와 Object Instance 목록을 link-format으로 포함한다.

단순등록 요청메시지 파라미터는 필수사항만 포함하고 필요에 따라서 선택사항도 넣을 수 있다. 단순등록 요청메시지를 처리하는 서버에서 해당 OBJ-RSC 프로파일 정보를 검색할 수 없을 경우는 "4.04 Not Found" 에러 메시지로 응답한다.

기본등록 과정과 달리 등록 메시지에 "ep={endpoint name}" 대신 "lep={endpoint name}" 옵션을 포함해서 등록한다. endpoint name으로 장치의 OID를 사용한다. 단순등록에는 OID 값에서 한전 공통 영역은 생략하고 사용하며, 5thArc부터 10thArc까지 값으로 OID를 구성한다. 여기서 lep는 light-weight endpoint client name의 약자이다. 단순등록뿐만 아니라, 단순등록업데이트에도 OID는 동일하게 공통 영역은 생략한다.

IFpg구간 단순등록 과정은 등록될 정보모델(Object)에 Prefix 정보(alternate path, 예: /dev/e1234)가 있는 경우에 payload에 link-format형식으로 포함해서 전달한다. 이 옵션을 확인한 서버는 lep 값을 기반으로 미리 저장되어 있는 OBJ-RSC 프로파일 정보를 검색하여 등록 과정을 마무리한다. 이때 등록 과정에서 생성되는 Location (Resource Path) 정보와 저장되어 있는 OBJ-RSC 프로파일을 매핑하여 Location 정보로 프로파일 정보를 검색할 수 있어야 한다.

TABLE 1
암호알고리즘 프로파일
(M: mandatory, O: Optional, N/A: Not Available)

암호	e-IoT 플랫폼	e-IoT 게이트웨이	e-IoT 디바이스
AES-128	M	M	M
SHA2	M	M	O
ECC	M	M	N/A
RSA	M	M	N/A

* AES: 대칭키 알고리즘(Advanced Encryption Standard)
SHA: 안전한 해시 함수(Secure Hash Algorithm)
ECC: 타원곡선암호(Ecliptic Curve Cryptograph)

3) e-IoT 보안 프로파일 경량화

e-IoT 규격 2.0 버전의 보안 프로파일은 TABLE 1과 같이 정

TABLE 2
보안 스펙 프로파일 (e-IoT 2.0)

Cipher Suite	e-IoT 플랫폼	e-IoT 게이트웨이	e-IoT 디바이스	참조
TLS_PSK_WITH_AES_128_CCM_8 {0xC0,0xA8}	N/A	M	M	RFC 6655
TLS_PSK_WITH_AES_128_ CBC_SHA256 {0x00,0xAE}	N/A	M	O	RFC 5487
TLS_ECDHE_RSA_WITH_AES_128_ CBC_SHA256 {0xC0,0x27}	M	M	N/A	RFC 5289

TABLE 3
보안 스펙 프로파일 (e-IoT 3.0)

Cipher Suite	e-IoT 플랫폼	e-IoT 게이트웨이	e-IoT 디바이스	참조
TLS_ECDHE_RSA_WITH_AES_128_ CBC_SHA256 {0xC0,0x27}	M	M	N/A	RFC 5289
TLS_PSK_WITH_AES_128_ CBC_SHA256{0x00,0xAE}	M	M	M	RFC 5487

* PSK: 사전 공유된 대칭키(Pre-Shared Key)
ECDHE: ECC 기반의 디피-헬만 키 교환 알고리즘
CBC: 블록 암호 운영 모드(Cipher-Block Chaining)

TABLE 4
Factory Mode Resource

ID	이름	동작	Instance	필수/선택	Type	설명
1036	Factory Mode	RW	Single	선택	Boolean	Factory Mode전환 관련 코드 0: Factory Mode 해제 1: Factory Mode 설정

의되어 있다.

TABLE 2에서 제시하는 보안 스펙 프로파일은 e-IoT의 개체별로 가용 암호알고리즘을 이용하여, 기밀성/무결성/인증의 주요 보안기능을 제공하기 위해 사용되는 스펙을 의미한다. 각 스펙의 자세한 동작방법은 참조규격을 따른다.

e-IoT를 현장에서 게이트웨이와 디바이스에 적용하고 또한 무선 환경을 고려해서 TABLE 3과 같이 보안 스펙 프로파일 2.0를 경량화 하였고 이를 규격 3.0에 반영하였다.

4) e-IoT 장치 진단 관리

e-IoT 장치진단관리는 e-IoT 서비스가 정상적으로 수행되지 않았을 경우 통신오류나 장치고장 등의 이상유무를 검출하고 그 원인을 파악하는 절차이다. 상세한 고장 원인은 LOG 파일을 통해서 진단된다.

a) e-IoT 장치 진단 절차

Fig. 6은 플랫폼에서 e-IoT 게이트웨이 및 디바이스의 이상을 진단하는 프로시저이다.

먼저 플랫폼은 이상이 있는 디바이스, 즉 주기적으로 보고가 올라오지 않는 디바이스에게 CoAP PING을 시도한다 [8].

CoAP PING이 성공했을 경우, 플랫폼은 해당 센서의 리소스를 조회한다 [8]. 리소스 조회가 실패했을 경우는 해당센서가 미연결된 것으로 판단한다. 리소스 조회가 성공했을 경우 센서의 Connectivity Monitoring 오브젝트의 Tx 성공/실패 리소스를 확인

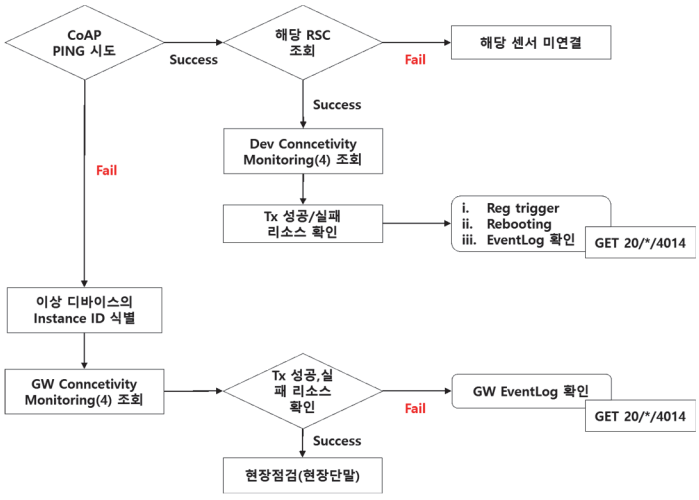

Fig. 6. 플랫폼에서 e-IoT 게이트웨이 및 디바이스 이상 진단 프로시저.

하고 재등록이나 Reboot 명령을 내리고 문제점 진단을 위해 디바이스의 LogData를 확인한다.

CoAP PING이 실패했을 경우, 플랫폼은 이상 디바이스의 Instance ID를 식별하고 해당 게이트웨이의 Connectivity Monitoring 오브젝트의 Tx 성공/실패 리소스를 확인한다 [8]. Tx 성공/실패 리소스 확인이 실패했을 경우는 게이트웨이의 이상으로 판단하고 GW의 LogData를 확인한다. Tx 성공/실패 리소스 확인이 성공했을 경우는 디바이스의 문제이므로 현장단말을 통하여 장치를 진단 관리한다.

여기서 LogData는 20번 EventLog 오브젝트의 4014 LogData 리소스(20/*/4014)를 의미한다.

LogData의 종류는 4010 Resource (LogClass)로 정의되어 있다. Generic, System, Security, Event, Trace, Panic, Charging 등 으로 분류된다. 일반적으로 Generic을 주로 사용한다.

LogData의 형식은 4015 Resource(LogDataFormat)으로 정의되어 있다. OMA-LwM2M TLV, OMA-LwM2M JSON, OMA-LwM2M CBOR, KEPCO data format이 있다. 일반적으로 KEPCO data format 사용하는 것을 권고한다.

b) KEPCO LogData Format

Log 관련된 정보모델은 20번 EventLog Object로 정의되어 있다. LogDataFormat 리소스(20/*/4015)의 100번 KEPCO data format은 다음과 같이 정의한다.

YYYY-MM-DD hour:min:sec.millisec |Log Level| Data

Log Level은 아래와 같이 6가지로 나누고, Log Level별로 확인이 가능해야 한다.

Level 1 = Critical(C),
Level 2 = Error(E),
Level 3 = Warning(W),
Level 4 = Information(I),
Level 5 = Debug(D),
Level 6 = Verbose(V)

LogData 형식은 제조사 자체 형식을 사용할 수 있다. 이때 LogDataFormat 리소스의 값을 101-255번 사이 값으로 한국전력

과 협의하여 할당해야 한다.

c) LogData 전송

장치진단관리 절차에서 로그데이터가 필요한 경우 e-IoT 플랫폼은 해당 장치의 로그 파일을 다음과 같은 절차를 통해서 획득할 수 있다.

e-IoT 플랫폼이 EventLog Object (20번)의 TxLogFile Resource (4019번)를 실행함으로써 LogData 파일 전송은 전송된다. LogData 파일은 CoAP Block-wise Transfer 기법을 이용해서 해당 장치가 전송한다 [8].

TxLogFile Resource를 LWM2M 제어를 할 경우 2개의 독립변수를 취할 수 있다. 첫번째 독립변수는 'From 시간' 의미하고 두번째 독립변수는 'To 시간' 의미를 갖는다. 시간의 형식은 "yyyymmdd-hhmmss'과 같이 표현한다. 만약 특정 날짜의 LogData 파일을 요청할 경우는 한 개의 독립변수만을 사용하면 된다. 한 개 독립변수를 사용하는 경우도 시간 형식은 동일하게 사용하며 그 중 'yyyymmdd' 값만 취한다.

Fig. 7은 e-IoT 플랫폼이 e-IoT 디바이스의 LogData 파일을 요청하고 LogData 파일을 전송하는 과정의 예시다. e-IoT 플랫폼은 2018년 5월 1일 15시 30분부터 2018년 5월 2일 9시 30분까지 LogData를 요청하는 제어 절차이다. TxLogFile 제어 요청 메시지를 수신한 e-IoT 디바이스는 해당 시간 조건에 맞는 LogData 파일을 생성하여 CoAP Block-wise Transfer 기법을 통해서 e-IoT 플랫폼에 전송한다 [8].

5) Factory Mode

Factory Mode는 현장에 위치한 e-IoT 게이트웨이와 e-IoT 디바이스의 저장되어 있는 정보를 수정하거나, 펌웨어 업데이트 등의 중요한 작업을 보안상으로 안전하게 수행하기 위해서 무선 통신 기술을 일시적으로 변경하는 것을 의미한다.

Factory 모드를 지원하기 위해서는 e-IoT 장치(게이트웨이와 디바이스)에 LPWA (LoRa PHY)와 Wi-SUN 를 동시에 지원하는 통신 모듈이 탑재되어 있어야 한다. 일반적인 서비스를 위한 동작은 LPWA (LoRa PHY) 무선 통신 기술을 이용하고, Factory Mode에서는 Wi-SUN 무선 통신 기술을 이용한다. Factory Mode를 제어하기 위한 정보 모델은 TABLE 4와 같이 Device (3번) Object에 Factory Mode Resource가 정의되어 있다.

Factory Mode 전환은 e-IoT 플랫폼과 e-IoT 현장단말을 이용해서 수행할 수 있다. Factory Mode 전환은 보안과 관련된 사항으로 현장단말로 수행되는 경우는 '단순 이벤트 보고' 를 통해서 플랫폼에 보고되어야 한다. 특히 Factory Mode 전환 요청 이벤트의 경우는 플랫폼의 통제 하에 수행되어야 하기 때문에 단순 보고 메시지에 대한 응답 메시지에 따라 게이트웨이에서 Factory Mode 진행 여부가 결정된다.

6) e-IoT 현장단말 - 정보 설정 기능

e-IoT 현장의 단말들의 네트워크 환경은 열악하기 때문에 e-IoT 플랫폼을 통해서 대용량 정보를 전달하는 데는 한계가 있다. 뿐만 아니라 e-IoT 플랫폼을 통해서 중요 정보를 전달해서 게이트웨이나 디바이스를 설정하는 것은 보완성이 취약성이 노출될 수 있다. 이런 이유로 e-IoT 현장단말을 이용해서 현장에서 직접 게이트웨이나 디바이스에 중요한 정보를 설정하는 할 수 있다. 이 기능을 현장단말 정보 설정 기능이라고 정의한다. 현장단말을 이용한 정보 설정 기능은 보안성을 높이기 위해서 Factory Mode를 정의하

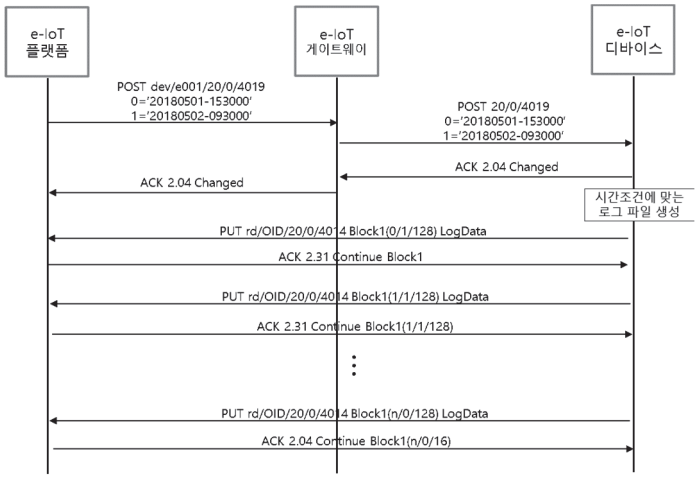

Fig. 7. 로그데이터 전송 절차.

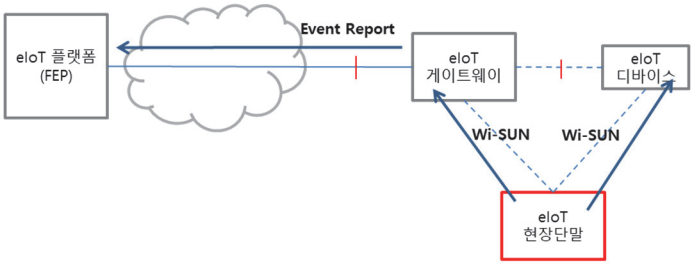

Fig. 8. e-IoT 현장단말 정보 설정 기능 개념도.

였다. 일반적인 서비스 동작에서 LPWA 통신 방식을 통해서 통신한다. 점검 기능과 현장 사진 업로드 기능은 이런 일반적인 상황에서 통신한다. 그런데 정보 설정 기능을 수행하기 위해서는 Wi-SUN 통신 방식, 즉 Factory Mode로 변환해야 한다. 이 모드에서는 Fig. 8과 같이 e-IoT 현장단말이 게이트웨이와 통신도 가능하고 디바이스와 직접 통신도 가능하다.

장치들의 정보를 수정하는 일은 보안적인 측면에서 매우 민감한 작업이다. 이를 위해서 Factory Mode를 통해서 1차적으로 안정성을 확보하였고, 2차적으로 정보 설정 이벤트를 정의하여 이를 플랫폼에 보고한다. 이를 통해 비정상적은 정보 설정 활동을 검출하여 대비할 수 있다. 이벤트 보고는 앞서 정의된 단순 이벤트 보고 기술을 적용한다.

정보 설정 기능은 현장에 위치한 게이트웨이와 디바이스를 대상으로 한다. 주로, 보안 비밀키 갱신을 위한 관련 정보를 변경할 때, 또는 펌웨어업데이트를 할 때 적용된다.

먼저 게이트웨이 정보 설정 과정에서는 현장단말이 게이트웨이와 직접 접속하여 정보설정기능을 수행한다. 대부분의 경우 e-IoT 게이트웨이는 LPWA 통신을 수행하기 때문에 현장단말은 LPWA 무선 통신상에서 KDF 기반 암호화를 통해서 안전하게 보안 채널을 형성한다. 안전한 형성된 보안 채널을 통해서 e-IoT 현장단말은 대상 e-IoT 게이트웨이의 "/.well-known/core" 라는 정보모델 접근 시작점을 요청하여 e-IoT게이트웨이에 관리되어 있는 정보 모델과 연결되어 있는 e-IoT 디바이스의 정보모델 리스트를 획득하여 온다. Device (3번) Object에 정의되어 있는 Factory Mode

Fig. 9. e-IoT 디바이스 시험구성도.

Fig. 10. e-IoT 게이트웨이 시험구성도.

(1036번) Resource를 대상으로 제어하여 게이트웨이를 Factory Mode로 변경한다. 제어 요청 메시지를 수신한 게이트웨이는 Factory Mode 전환에 대한 이벤트를 플랫폼에 보고하여야 한다. 이때 EventLog (20번) Object에 정의되어 있는 EventReport (4018번) Resource를 대상으로 단순 이벤트 보고 기능을 수행한다.

이벤트 보고를 수신한 플랫폼은 정상적인 상황의 이벤트 보고인지를 판단하여 정상일 경우는 “2.04 Changed” 응답 메시지를 전달한다. 만약 현장 단말이 파송되지 않은 지역에서 Factory Mode 전환 요청 이벤트가 발생하는 등의 비 정상적인 상황의 보고일 경우는 “4.06 Not Acceptable” 응답 메시지를 생성하여 전달한다. Factory Mode 전환 상황에서 게이트웨이는 플랫폼의 응답 메시지에 따라서 Factory Mode 전환을 판단한다. 수락한다는 의미의 “2.04 Changed” 응답 메시지를 수신 경우에만 Factory Mdoe로 전환하여 해당 통신모듈을 변경한다.

Factory Mode 변환의 성공을 의미하는 응답 메시지를 수신한 현장단말은 자신의 통신모듈도 또한 Factory Mode로 변환하여 게이트웨이와 통신연결을 수행한다. Factory Mode에서 무선 통신이 연결된 게이트웨이와 현장단말은 DTLS 핸드세이크 등의 절차를 수행하여 안전한 채널을 형성한다. 형성된 보안 채널을 통해서 설정 기능을 수행한다.

7) e-IoT 표준규격 검증을 위한 시험규격

e-IoT 표준규격과 본 논문을 통해 연구되었던 e-IoT 경량화 규격의 내용을 검증하기 위해서 시험대상이 e-IoT 디바이스인 경우와 시험대상이 e-IoT 게이트웨이인 경우에 대해 시험 규격서를 개발하였다.

a) IoT 디바이스 시험규격

시험대상이 e-IoT 디바이스인 경우 Fig. 9와 같이 기준장비 e-IoT 게이트웨이와 기준장비 e-IoT 플랫폼을 연동하여 상호운용성 시험을 수행한다.

e-IoT 디바이스의 시험규격은 디바이스의 자체기능 시험을 수행하며 시험 항목은 TABLE 5와 같이 크게 9가지 시험 집합으로 분류된다.

b) e-IoT 게이트웨이 시험규격

e-IoT 게이트웨이인 경우 Fig. 10과 같이 기준장비 e-IoT 디바이스와 기준장비 e-IoT 플랫폼을 연동하여 상호운용성 시험을 수행한다.

TABLE 5
e-IoT 디바이스 시험규격

구분	시험 집합	시험 목적
디바이스 자체 기능	단말 등록 (REG)	등록
		시간 동기화
		등록 업데이트
	등록 오브젝트 조회 (RRO)	LwM2M 서버 조회
		디바이스 조회
		Location 조회
		센서 조회
		이벤트 로그 조회
	데이터 수집 (DG)	센서 데이터 수집
		위치 데이터 수집
		복합 센서 데이터 수집
		히스토릭 데이터 수집(Time 변수)
		히스토릭 데이터 수집(리소스)
		단순 주기적 보고
	장치 관리 및 운영(DMO)	모니터링 데이터 관리
		NMS 데이터
		CoAP Ping
		디바이스 Sleep
		배터리 정보 조회
		Factory 모드(e-IoT 플랫폼 기반)
		Factory 모드(e-IoT 현장단말 기반)
		로그 데이터 전송
	단말 제어(DC)	설정 제어
		상태 제어
	단말 해지(DER)	등록 해지
	단순 단말 등록(SDR)	단순 등록
		단순 등록 업데이트
	디바이스 이동성 관리(DMC)	디바이스 이동성 관리
	보안(SEC)	KDF 기반 데이터 보안

e-IoT 게이트웨이 시험규격은 자체기능 시험이 8개 시험 집합, 중계기능 시험이 TABLE 6과 같이 9개의 시험 집합을 가진다.

IV. Conclusion

최근 전력시스템에서의 최대 화두는 디지털화이며, IoT 기술을 적용하기 위한 연구개발과 시범서비스가 진행 중에 있다. 한전의 IoT 기술규격인 e-IoT 표준기술은 디지털변환을 위한 초연결 지능형 전력망 구축사업의 기반기술로 활용되어 지능형 초연결 전력망 구축에 기여할 것으로 예상된다.

따라서 본 논문에서는 e-IoT 표준 프로토콜 경량화 방안을 제안하고 관련하여 e-IoT 기반 제품간 상호운용성 시험체계를 제안하였다. 사물인터넷 부문 3대 국제인증을 모두 보유하고 있는 한전의 e-IoT 표준 프로토콜 경량화 방안에 대해 ID체계, 등록절차, 보안 프로파일, 현장단말 정보설정 등에 대해서 서술하였으며, 프로토콜 경량화 방안으로 다음과 같이 제안하였다.

- ID 경량관리: 10단계 구조의 e-IoT 단말의 OID 체계를 한전에 사용되는 공통적인 5단계까지는 제외하고 나머지 부분만 사용.
- 등록절차 경량화: 디바이스-게이트웨이-플랫폼간 기본등록절

TABLE 6
e-IoT 게이트웨이 시험규격

구분	시험 집합	
e-IoT 게이트웨이 자체 기능	단말 등록(REG)	등록, 시간 동기화, 등록 업데이트
	등록 오브젝트 조회(RRO)	LwM2M 서버 조회, 게이트웨이 Connectivity 조회 등
	데이터 수집(DG)	센서, 위치, 복합 센서, 히스토릭 데이터 수집 등
	장치 관리 및 운영(DMO)	NMS 데이터, 배터리 정보 조회 등
	단말 제어(DC)	펌웨어 다운로드, 업데이트 등
	단말 해지(DER)	등록해지
	단순 단말 등록(SDR)	단순등록, 단순등록 업데이트 등
	보안(SEC)	인증서기반 DTLS보안세션
e-IoT 중계기능	단말 등록(REG)	등록, 시간동기화, 등록업데이트 등
	등록 오브젝트 조회(RRO)	LwM2M 서버 조회, Location 조회 등
	데이터 수집(DG)	센서, 위치, 복합 센서, 히스토릭 데이터 수집 등
	장치 관리 및 운영(DMO)	NMS 데이터, 배터리 정보 조회 등
	단말 제어(DC)	펌웨어 다운로드, 업데이트 등
	단말 해지(DER)	등록해지
	단순 단말 등록(SDR)	단순등록, 단순등록 업데이트 등
	디바이스 이동성 관리(DMC)	디바이스 이동성 관리
	보안(SEC)	KDF기반 데이터보안

차 대비 데이터 통신 대역폭이 제한적인 경우 기 저장된 장치정보를 일괄적으로 등록함으로써 절차를 단순화함.

- e-IoT 보안 프로파일 경량화: 무선 환경을 고려해서 게이트웨이와 디바이스에 적용되는 보안 스펙 프로파일을 최소화.
- e-IoT 장치 진단 관리: e-IoT 서비스가 정상적으로 수행되지 않았을 경우 통신오류나 장치고장 등의 이상유무를 검출하고 그 원인을 파악하는 위해 LOG 파일 진단.
- Factory Mode: 현장에 위치한 e-IoT 게이트웨이와 e-IoT 디바이스의 저장되어 있는 정보를 수정하거나, 펌웨어 업데이트 등의 중요한 작업을 보안상으로 안전하게 수행하기 위해서 무선 통신 기술을 일시적으로 LPWA에서 Wi-SUN으로 변경.
- e-IoT 현장단말 - 정보 설정 기능: 대용량 정보전달 및 보안 취약성을 고려하여 e-IoT 현장단말을 이용해서 현장에서 직접 게이트웨이나 디바이스에 중요한 정보를 설정하는 기능.

또한 e-IoT기술에 대한 시험규격 개발의 일환으로 디바이스, 게이트웨이 등의 제품에 대한 시험구성과 시험항목을 제시하였다. 향후 한전이 개발한 e-IoT 기술규격은 시험인증 공인기관인 한국정보통신기술협회(TTA)에서 'e-IoT 시험인증제도'를 시행함으로써 에너지분야 새로운 융합서비스 창출이 활발해질 전망이다.

References

[1] Internet of Things in Electricity and Energy Domain(e-IoT) – Part 1: System Specifications, TTAK.KO-10.1121-part1, 2018.

[2] Internet of Things in Electricity and Energy Domain(e-IoT) - Part 2: Simple Registration specification, TTAK.KO-10.1121-part2, 2018.

[3] Internet of Things in Electricity and Energy Domain(e-IoT) - Part 3: Data Report specification, TTAK.KO-10.1121-part3, 2018.

[4] Internet of Things in Electricity and Energy Domain(e-IoT) - Part 4: Field Terminal Service specification, TTAK.KO-10.1121-part4, 2018.

[5] Internet of Things in Electricity and Energy Domain(e-IoT) - Part 5: Physical Layer Specification in Narrowband Wireless Communication, TTAK.KO-10.1121-part5, 2018.

[6] OMA LwM2M Technical Specification, OMA-TS-LwM2M-V1_0_2-20180209-A, 2018. Available at: http://www.openmobilealliance.org/release/LightweightM2M/V1_0_2-20180209-A/OMA-TS-LightweightM2M-V1_0_2-20180209-A.pdf, Accessed on Jun. 2019.

[7] OMA LwM2M Technical Specification, OMA-TS-LwM2M-BinaryAppDataContainer-V1-20171205-C, 2017. Available at: http://www.openmobilealliance.org/release/LightweightM2M/V1_0_2-20180209-A/OMA-LwM2M-BinaryAppDataContainer-V1-20171205-C.pdf, Accessed on Jun. 2019.

[8] The Constrained Application Protocol (CoAP), RFC 7252, 2014.