검침데이터 기밀성확보를 위한 구조분석 및 설계

백종목°, 최문석*, 임용훈*
°*한국전력공사 전력연구원
e-mail: {baekjmo, cms96, adsac}@kepco.co.kr

Analysis and design of Meter data structure to secure confidentiality

*Jong-Mock Baek, *Moonsuk Choi, *Yong-hun Lim.
*KEPCO Research Institute

● 요 약 ●

유틸리티에서 검침은 고객에게 제공한 에너지의 사용량을 계량하고 요금을 부과하기위한 중요한 정보이며 검침방법이 종래의 인력검침에서 자동원격검침으로 발전함에 따라 계량기에서 검침서버로 전송되는 통신망에서 보안관리가 중요시 되고 있다. 보안의 방법은 중간의 통신망 형태, 통신 매체, 전송되는 데이터의 구조등을 반영하여 적정한 보안방법이 적용되어야 하겠지만 본 논문에서는 현재 전기검침에 적용되는 국제규격DLMS/COSEM데이터의 구조를 분석하고 기밀성을 보장하기위한 방안을 제시하였다.

키워드: 검침데이터(meter data), 데이터 기밀성(Data Confiedntiality)

I. 서론

유틸리티 사용량이면서 전기요금을 산정하는 과금자료인 검침데이터에 대해 기밀성이 보장하는 방안을 제시하기 위해 암호화하는 구조적인 방법을 연구하였다. 전력회사는 원격검침의 주요방식으로 전력선을 이용한 검침인프라를 구축하여 원격검침망을 확대 구축하는 관계로 기존에 구축된 전력선 통신시스템의 자원과 통신방식의 특성에 대해 충분히 고려했다. 전기검침을 위해 계량기의 데이터를 교환하는 통신규약인 IEC62056을 분석하여 암호화에 필요한 대상을 선정하였으며 사례로 정기검침 데이터에 대해 암호화 대상 부분을 분석하였다.

II. 검침데이터 기밀성 확보

1. 보안 검침시스템 개요

전력선 통신망기반의 저압원격검침 시스템의 보안기능이 적용된 기본적인 구성도는 [그림 1]과 같다. 인증서버는 기기의 ID 및 인증서 정보를 바탕으로 현장기기의 인증여부를 결정한후 인증대상으로 확인되면 인증처리하고 NMS서버에게 기기등록 요청을 하게 된다.

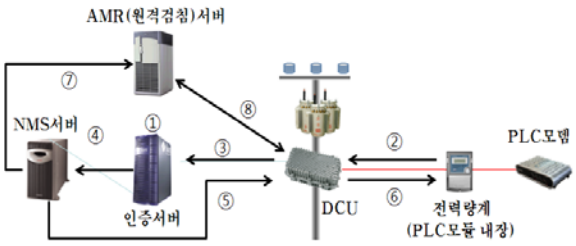

그림 1. 보안 원격검침시스템 네트워크 구성도
Fig. 1. The Network Structure of secure AMR

NMS서버는 DCU를 통해 현장기기를 등록하고 AMR서버에게 기기등록 완료 통보 및 검침개시 요청을 하면 검침 스케쥴러에 의해 원격검침이 진행된다.

2. 검침데이터 수집 통신규격

전력사에서는 원격 전기검침을 위한 저압전자식 전기계량기의 통신 프로토콜 규격으로 IEC62056의 DLMS(Device Language Message Spec.)[1]을 채택하여 등록규격 RS - 6625 - 0037로 지정 운영하고 있으며 G-Type 전자식 전력량계의 통신규격은 주요 표준은 [표 1]과 같다. 보안을 고려한 부분으로 IEC 52056-53과 62에 Authentication 절차로 LLS(Low Level Security)와 HLS(High Level Security)를 정의하고 있으며 본 논문에서는 Meter에서 보안 H/W플랫폼으로 전송된 HDLC/DLMS packet을 해석하여 필요한 부분을 암호화하여 기밀성을 보장하는 방안을 제시 하였다.

표 1. G-Type 저압전자식 전력량계 통신규격
Table 1. The communication spec. of G-Type meter

IEC NO.	제 목
62056	Electricity metering data exchange for meter reading, tariff and load control
62056-42	Physical layer services and procedures for connection (2002)
62056-46	Data Link Layer using HDLC-Protocol
62056-53	COSEM Application layer (2006)
62056-61	OBIS Object Identification System (2006)
62056-62	Interface Objects (2006)

3. 검침데이터 구조분석

계량기내 보안H/W플랫폼 모듈에서 DLMS/COSEM규격의 검침데이터를 암호화 하여 전송하면 중앙의 서버에서 데이터를 복호화함으로서 검침데이터의 기밀성을 보장하며 통신망 구간의 검침데이터는 별도의 보안통신프레임 프로토콜규격(SSMP)을 정의 하였다. 기기인증을 위한 헤더정보 참조기능이외에는 DCU에서 열어보지 않으므로 End-to-End간의 기밀성을 보장할수 있다.

3.1 IRM-보안H/W플랫폼-MPLC구간 보안통신

IRM - 보안H/W플랫폼 - MPLC간 통신은 Serial Control Frame을 통해 이루어진다.

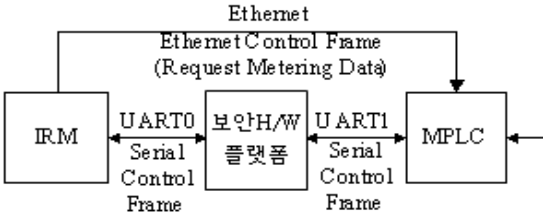

그림 2. DCU 내부 기능모듈간 신호연결도
Fig. 2. The Signal Flow Diagram of DCU

보안H/W플랫폼은 M-PLC로부터 Serial Control Frame을 수신하면 Device MSG를 이루고 있는 보안통신 frame을 해석한다. 그리고 적절한 프로세스를 거쳐 그 결과를 IRM이나 MPLC에 Serial Control Frame의 형태로 전달한다.

3.2 SPLC-보안H/W플랫폼-Meter구간 보안통신

SPLC와 보안H/W플랫폼간은 SSMP규격으로 통신하며 보안H/W플랫폼과 Meter간 통신은 DLMS/ COSEM규격을 적용한다. 보안H/W플랫폼에서는 보안통신 프로토콜 프레임내 MSG의 Value에 포함된 검침패킷을 Meter로 전송하고 Meter로부터 전송된 검침 프로토콜패킷은 처리후 보안통신프로토콜 SSMP 프레임을 생성하여 SPLC에 전송한다.

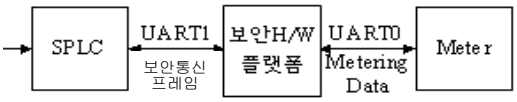

그림 3. 계량기 내부 통신모듈간 신호연결도
Fig. 3. The Signal Flow Diagram in Meter

3.3 DLMS Packet Encryption 대상 선정

보안H/W플랫폼에서 암호화 작업을 해야 할 검침 패킷으로 IEC62056-46 및 53에서 정의된 대상 패킷은 [표 2]에 나타내었다.

표 2. 암호화 대상 패킷 항목
Table 1. The Encription Target in HDLC/DLMS Packet

NO	항목	OBIS Code (hex)
		A B C D E F
102	계기종류 및 기타정보	01 80 80 80 81 FF
26	전력량(월별)	00 00 62 01 01 FF
26	전력량(정기검침)	00 00 62 01 01 VZ
27	최대 수요전력(월별)	00 00 62 01 02 FF
27	최대 수요전력(정기검침)	00 00 62 01 02 VZ
43	Load Profile	01 00 63 01 00 FF

전력량 정기검침패킷을 캡처하여 암호화 대상을 표시하면 아래의 회색음영부분이 된다.

7E A0 55 23 02 03 1E CA E8 E6 E7 00 C4 01 81 00 01 01 02 0C 06 00 00 00 00 06 00 00 00 05 09 04 ..... 00 06 00 00 00 00 06 00 00 00 00 09 04 00 00 00 00 80 86 7E

III. 결론

원격검침망에서 보안H/W플랫폼이 개입된 보안통신기능과 절차를 정의하였으며 전력선 통신망 기반의 원격검침망에서 전송되는 검침데이터의 기밀성 확보대상선정과 예시를 제시하였다. 검침데이터의 보안수준향상을 위해 지속적인 연구가 필요하다.

참고문헌

[1] DLMS: Device Language Message Specification. http://www.dlms.com