PLC기반 원격검침인프라 보안시스템

주성호, 최문석, 백종목, 임용훈
한국전력공사 전력연구원

Security System for AMR Infrastructure based on PLC

Seong Ho Ju, Moon Seok Choi, Jong Mock Baek, Yong Hoon Lim
Korea Electric Power Research Institute

ABSTRACT

다양한 유무선 통신기술을 이용한 원격검침시스템 (AMR : Automatic Meter Reading)이 본격적인 사업단계에 들어섰으나, 인프라에 대한 기본적인 보안대책마저도 전무한 실정이다. 특히 외부 통신망을 이용할 경우 전력인프라의 보안취약성은 수많은 해커들의 표적이 되기에 충분하다. 이를 위해서는 각 기기들을 안전하게 인증, 관리하고 데이터를 보호해야 하지만 수많은 저사양 기기들을 원격으로 자동 인증, 관리하는 것은 쉽지 않다. 본 연구에서는 광범위 지역에 설치될 저사양 검침기기들을 자동으로 인증, 관리하며, 데이터보호 및 이를 위한 보안키 관리 메커니즘을 제시하고자 한다.

1. 서 론

최근 국내외 전력회사들은 경제성과 관리의 용이성, 다양한 부가가치 창출 등의 관점에서 원격검침의 타당성을 제기하고 구체적인 사업화를 계획, 진행 중에 있다. 15분 간격(해외의 경우 시간단위)로 검침데이터를 원격으로 수집하게 될 경우, TOU(Time of Usage), RTP(Real Time Pricing)과 같은 다양한 요금정책 적용이 가능해질 뿐만 아니라 DR(Demand Response)와 같은 수요관리 및 에너지소비 효율정책을 통해 부가가치를 창출할 수 있어 에너지검침의 자동화는 세계적인 추세라고 할 수 있다.[1] 하지만 원격검침시스템 구축에 따른 새로운 문제점들이 발생하게 되는데, 가장 심각한 것이 바로 보안문제이다.

계량기에서 중앙서버까지 자동화, 무인화된 원격검침시스템은 시스템, 네트워크, 데이터프로토콜 등 모든 측면에서 보안취약성을 내재하며, 특히 아래와 같은 검침환경으로 인해 사이버공격에 취약성을 가지게 된다.

- 검침단말의 저사양 H/W : 보안기능의 최소화
- 광범위 지역에 설치되는 수많은 단말 : 관리의 어려움
- 현장 단말에 대한 접근의 용이성 : 외부 공격의 용이성
- 검침프로토콜 및 운영절차의 공개성 : 외부 공격가능성

이러한 보안취약성을 극복하기 위한 노력없이 원격검침사업이 이루어질 경우 데이터 위·변조, 기밀 유출, 시스템/서비스 무력화 및 추가 사이버공격의 단초를 제공할 여지가 있으므로, 보안에 대한 충분한 연구와 대책이 수립되어야 한다.

본 논문에서는 원격검침시스템의 전반적인 보안현황에 대해 분석한 뒤, 가장 시급하다고 판단되는 검침기기 자동 인증 및 보안키 관리 기술에 대해 언급하고자 한다.

2. 원격검침인프라 보안성 분석

원격검침인프라는 검침의 신뢰성과 안전성을 보장하기 위해 PLC를 비롯한 다양한 유무선통신기술을 접목한 통합망을 기반으로 구축되고 있어, 기존 통신망의 보안취약성을 그대로 계승하고 있으며, 원격검침만의 특성에 따라 새로운 보안취약성도 내재하고 있다.[2] 본 연구에서는 기밀성, 무결성, 인증, 부인방지의 보안요소 측면과 보안키 전송기술 측면에서 원격검침시스템의 문제점을 제시하였으며, 이를 보안할 수 있는 방안을 표 1과 같이 제시하였다.

표 1 원격검침시스템 보안취약성 및 대응방안

안전성 기준	기존 AMR	본 연구결과	비고
기밀성	△	○	64비트 DES ⇒ 128비트 ARIA
무결성	×	○	메시지 인증 코드(MAC) 추가
기기 인증	×	○	공개키 기반 기기 인증서 제공
기기 폐기	×	○	기기 인증서 폐기목록 관리
메시지 부인방지	×	○	서명 추가
전방위 안전성	×	○	세션키 업데이트 기능 추가
보안키 분배 알고리즘	△	○	보안키 평문전송 ⇒ 공개키 기반 키 전송 프로토콜

표 1과 같이 데이터 기밀성과 무결성의 경우 보안키의 안전한 관리(생성, 분배, 갱신, 폐기)절차가 제시될 경우 보안 알고리즘의 업그레이드만으로 확보가 가능하며, 부인방지의 경우 검침값의 신뢰성 확보를 위해 공개키기반의 서명절차를 추가함으로써 지원이 가능함을 알 수 있다. 결국 기기의 인증/관리 기능과 보안키 분배/관리가 해결될 경우 현재의 원격검침시스템은 보안측면에서 훨씬 강화될 것으로 판단된다.[3]

3. 자동 인증 및 보안키 관리 메커니즘

원격검침시스템의 보안성 강화를 위해 설계한 원격검침 보

안 프로토콜(SSMP : Secure Smart Metering Protocol)은 크게 '사전 운용단계', '시스템 운용단계', '사후 운용단계'로 나뉘며, 각 절차에 대한 내용은 다음과 같다.

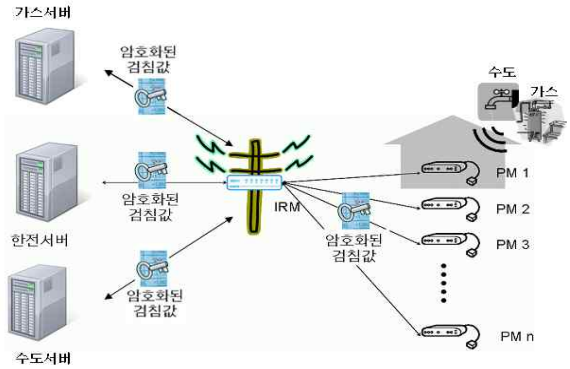

그림 1 원격(통합)검침시스템 구성도

3.1 사전 운용단계

SSMP를 운용하기 위한 모든 보안키 생성 정보를 준비하는 단계로서, 서버의 초기화, 제조사 보안키 및 인증서 생성, 기기의 초기화 및 등록 절차로 구성된다.

표 2 원격검침시스템 보안취약성 및 대응방안

```
struct SSMP_Certificate{
        unsigned char uid[6]; //Unique ID
        unsigned char order[24]; //base point order
        unsigned char a[24], b[24]; //타원곡선 방정식의 a,b
        unsigned char base_x[24], base_y[24]; //base point
        unsigned char enc_pub_x[24], sgn_pub_x[24];
                                //암호 및 서명 공개키 x좌표
        unsigned char enc_pub_comp_y, sgn_pub_comp_y;
                                //암호 및 서명 공개키 y좌표
        unsigned char role;     //0x01: 한전서버
                                //0x02: 가스서버
                                //0x03: 수도서버
                                //0x11: IRM
                                //0x12: PLC/전기검침기
                                //0x22: 가스검침기
                                //0x23: 수도검침기
        unsigned char r[21]; //서명값1
        unsigned char s[24]; //서명값2
        unsigned char validity[8]; //유효기간
        unsigned char reserved[24];}
```

3.1.1 서버 초기화

SSMP 서버는 인증서를 발급하는 CA(Certificate Authority) 서버, 기기의 ID, 공개키 및 인증서를 관리하는 RA (Registration Authority) 서버, 검침정보를 관리하는 MA(Metering Authority)서버로 구성된다.

CA서버는 인증서 발행, 관리, 폐기를 담당하며, 모든 기기의 인증서는 CA서버의 공개키로 서명되어 검증을 통과해야 인증이 완료된다. RA서버는 인증된 기기를 등록, 관리하며 모든 검침기기는 RA서버에 ID를 등록하고 짝을 이루는 공개키/개인키 쌍에 대응하는 인증서를 가지고 있어야 한다. MA서버는 검침기기와 직접 통신을 함으로써 필요한 검침정보를 송수신 한다.

3.1.2 제조사 인증 및 키 생성

모든 검침기기는 설치이전에 상위 서버의 인증, 등록절차를 거쳐야 하며, 이를 위해 검침기기 제조사는 사전에 상위 서버로부터 인증 및 등록절차에 의거 제조사 고유 ID 및 보안키를 부여받아야 한다. 이를 이용하여 향후 제조, 납품할 검침기기의 리스트 및 보안정보를 상위 서버와 안전하게 공유할 수 있게 된다.

3.1.3 검침기기 인증 및 키 생성

제조사에서 생산한 검침기기는 상위 서버에 ID 및 초기 보안키(검침기기가 자체적으로 생성, 저장한 공개키 및 비밀키)를 등록하고 인증받아야 한다. 기기의 인증 및 등록과정은 다음과 같다.

1) 각 기기는 자신의 공개키/개인키 및 고유키를 생성, 저장
2) 제조사는 생산한 모든 기기의 ID와 공개키 쌍에 서명하고 이를 상위 서버에 전송
3) 서버는 제조사의 서명을 검증하고 각 기기별 인증서를 생성하고 DB에 저장, 관리(인증서는 서버의 개인키로 서명된 값임)
4) 제조사는 서버로부터 인증서 리스트를 받아 각 기기에 해당하는 인증서를 저장

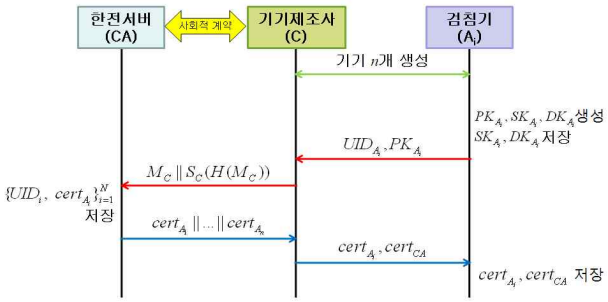

그림 2 기기 인증 및 등록 절차

3.2 시스템 운용단계

보안키 생성을 위한 모든 정보가 준비되어 암호학적 동작을 가능하게 하는 보안키가 활성화된 상태이다. 이 단계에서는 공유키를 전송하고 이를 기반으로 세션키를 생성하여 검침값을 암호화하여 송수신하게 된다.

3.2.1 공유키 및 세션키 설정

원격검침시스템에서는 토폴로지상 하위노드에서 공유키를 생성하여 상위노드로 전송하는 과정을 통해 각 기기간 고유의 공유키를 공유하게 된다.

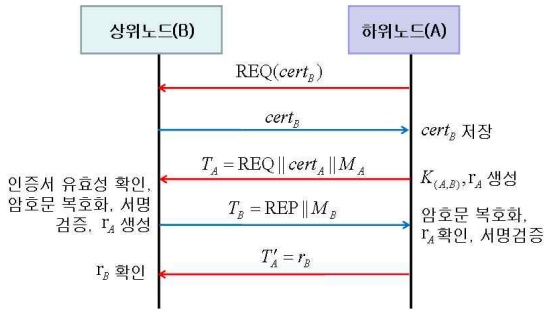

그림 3 공유키 전송 프로토콜

공유키 전송 프로토콜은 3.1절의 과정을 통해 배표된 인증서 및 공개키를 기반으로 이루어진다. 검침시스템의 토폴로지는 환경에 따라 변경될 수 있으며, 중간에 하나 이상의 리피터나

데이터 수집장치가 존재할 수 있으며, 이러한 경우에도 그림 3의 프로토콜에 준해서 공유키를 공유할 수 있다.

3.2.2 검침정보 전송

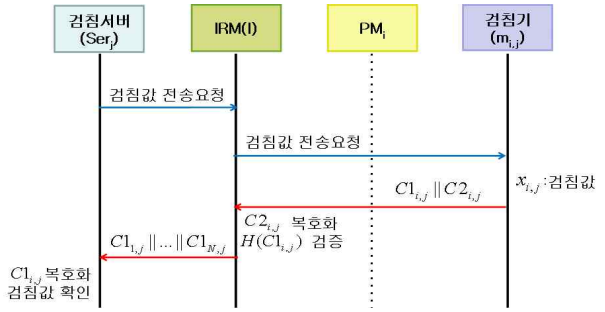

그림 4 검침정보 전송 프로토콜

실제 검침정보의 암복호화는 세션키로 이루어지며, 세션키는 공유키로부터 구할 수 있다. 세션키를 별도로 생성하는 이유는 보안키의 안전성을 확보하기 위함이며, 세션키는 필요에 따라 생성 및 갱신 주기를 변경할 수 있으마, 본 연구에서는 데이터 통신 주기, 데이터량, 신뢰도 수준을 고려하여 월 1회 갱신하는 것으로 하였다.

3.3 사후 운용단계

보안키 생성을 위한 정보가 무효할 경우로서 보안키가 훼손되거나 비활성화된 상태가 해당된다. 이때 키를 사요한 데이터의 처리, 즉 키의 유도 및 검침정보의 암복호화 동작이 불가능하며 인증서 갱신과정도 포함한다.

3.3.1 인증서 갱신

초기 인증서 발행시 유효기간을 설정함으로써 주기적으로 기기의 유효성 검증 및 보안상태 확인이 가능하도록 하였다. 따라서 인증서 기간이 만료되거나, 기기의 개인키 또는 고유키가 유출되었다고 판단될 경우 인증서를 갱신하거나 기기의 사용을 금지하여야 한다.

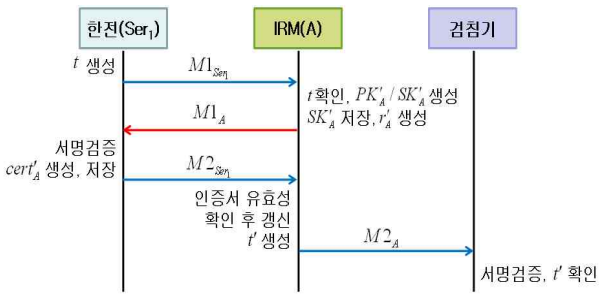

그림 5 데이터 전송장치의 인증서 갱신 절차

인증서 절차과정은 해당 기기에 따라 다르며, 서버와 직접 통신하는 데이터전송장치(IRM : Integrated Regional Manager)의 경우 그림 5와 같은 갱신절차를 거쳐야 한다. 주기적으로 갱신하는 경우와 유사시 임의로 갱신하는 경우도 절차상 차이가 약간 있을 수 있으나 큰 틀에서는 유사한 절차에 의거하여 동작하도록 설계하였다.

3.3.2 인증서 폐기

기기의 교체, 철거의 경우 해당 기기의 인증서를 폐기하고 폐기 목록을 관리함으로써 폐기된 인증서의 불법 유용 및 공격으로부터 보안성을 확보할 수 있다. 인증서버는 폐기된 기기의 목록을 주기적으로 확인하고 이를 데이터전송장치에 알려줄 의무를 가지게 된다.

4. 결 론

본 연구에서는 원격검침시스템의 보안성을 확보하기 위한 기본적인 보안프로토콜을 설계하고 각 기기별 기능과 보안상 절차를 제시하였다.

원격검침시스템은 단순 검침정보 수집에 한정되어 설계할 경우 수많은 보안상 문제점을 야기할 수 있어 구축이전에 다양한 시나리오에 따른 보안대책을 마련하지 않으면 안된다. 하지만, IT기술의 발전과 더불어 지능화, 고도화, 다양화되고 있는 사이버공격으로부터 완전히 보호받을 수 있는 시스템을 개발하는 것은 쉽지 않은 일이며, 이를 위해서는 기본적인 보안정책 수립과 시행이 우선적으로 이루어져야 한다.

본 연구를 통해 설계된 보안프로토콜은 자동화된 시스템이 해결해야 할 선행 문제인 기기의 자동 인증 및 보안키 관리의 문제점을 다루었으며, 후속조치로 데이터 및 기기의 실시간 모니터링, 자동화 프로토콜의 분석 및 보완, 임베디드시스템의 보안대책 등에 대해 연구를 진행하고 있다. 향후 스마트그리드가 활성화될 경우 본 연구결과는 보안정책의 기초자료로 활용가능할 것으로 예상된다.

참 고 문 헌

[1] K.Watanabe, M.Ise, T.Onoye, "Energy-efficient architecture of the wireless home network based on MAC broadcast and transmission power control", IEEE Trans. Consumer Electronics, vol. 53, no. 1, pp. 124-130, 2007, February.

[2] J.Heo, C.S.Hong, S.H.Ju, Y.H.Lim, B.S.Lee, D.H.Hyun, "A Security Mechanism for Automation Control in PLC-based Network", Proceedings of IEEE ISPLC2007, pp. 466-470, 2007, March.

[3] R.Newman, L.Yonge, S.Gavette, R.Anderson, "HomePlug AV Security Mechanisms", Proceedings of IEEE ISPLC 2007, pp. 366-371, 2007, March.