# 전력선통신기반 원격검침시스템을 위한 효율적인 기기인증 및 관리체계

*주성호, 최문석, 임용훈, 최종협
한전전력연구원
e-mail : shju1052@kepco.co.kr

# Efficient Authentication and Management System for PLC-based AMR

*Seong-Ho Ju, Moon-Seok Choi, Yong-Hoon Lim, Jong-Hyup Choi
Korea Electric Power Research Institute

## Abstract

Security weakness in PLC network can be made up for by authentication and management scheme of PLC modules introduced in this paper. Each PLC module must pass the authentication procedure to work normally in PLC network as soon as being installed in the spot. Based on this scheme, all PLC devices are registered, certified, and managed automatically in central control center - AMR server, authentication server, NMS server, and DB server.

## I. 서론

현재 개발, 구축중인 PLC(전력선통신)기반 원격검침 시스템은 통신성능 및 검침가능여부 등 시스템의 기본적인 성능이나 신뢰성 측면에서만 중요성이 고려되어 왔으나, 대규모 사업계획이 수립됨에 따라 수많은 PLC 기기정보를 중앙에서 자동으로 등록, 관리하고 허가된 기기만 PLC 네트워크에 접속하여 동작할 수 있도록 하는 인증체계를 마련해야 한다. 하지만 현재까지 PLC 네트워크에서의 인증시스템은 단순히 데이터집중장치(IRM)에 직접 접속하여 PLC MAC 확인 후 수동으로 인증해주는 수준이므로 대규모 사업이 진행될 경우 수백만 개에 달하는 IRM에 개별적 접속을 통한 인증체계는 적합하지 않다. 또한 현재 PLC 정보관리체계는 전무한 실정이어서 수천만 개의 PLC 모듈(장비)에 대한 데이터베이스 구축, 관리를 위한 효율적인 방안이 절실한 실정이다.[1]

본 논문에서는 모든 PLC 장비(모듈)의 구매, 설치, 운용 등 제반 절차에 있어 자동적으로 인증, 관리할 수 있는 체계를 개발하고 실제 PLC 원격검침시스템에 적용할 수 있는 방안을 제안하였다.

## II. PLC 인증 및 정보관리 체계

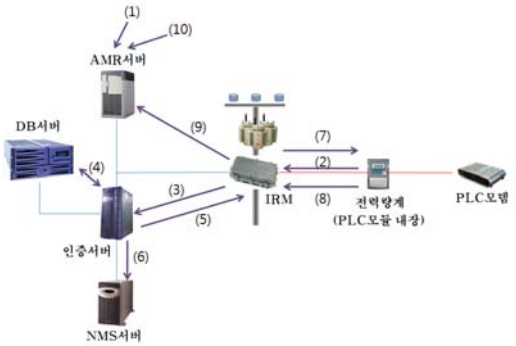


그림 1. PLC 기기인증 및 정보관리 구성도

그림 1은 PLC기반 원격검침시스템 구축 시작단계에서의 자동 인증 및 정보관리체계를 보여준다. 전력량계 자체 정보(계량기 ID, 종류 등)와 수용가 정보는 전력량계 설치시점에 AMR서버에 등록되며(1), 전력량계 내장형 PLC 모듈이 설치되면 자동 인증절차가 시작되어(2) 관리센터의 인증서버에서 인증이 되면((3)~(5))

정상적으로 동작할 수 있도록 등록이 완료된다. 이때 PLC 제조사로부터 미리 설치될 PLC 모듈의 MAC주소와 고유ID를 제공받아 DB서버에 등록, 관리해야 하며, 인증된 PLC 모듈은 NMS서버에 등록되어(6) 추후 자동 관리될 수 있도록 한다.

이러한 체계에서 또 하나의 특징은 PLC 모듈과 전력량계의 매칭오류를 줄여준다는 것이다. 그림 1의 (7) ~ (10) 절차는 현장에 설치된 PLC 모듈과 해당 전력량계의 ID 정보를 세트화하여 AMR서버에 전송함으로써 관리센터나 과금센터에서는 각 수용가에 실제 설치된 PLC 모듈과 전력량계의 정확한 정보를 확보할 수 있어, 지금까지 현장 설치과정에서 자주 발생하던 PLC 모듈과 전력량계간 매칭오류 문제점을 해결할 수 있어 설치 후 관리가 상당히 편리해진다.

## Ⅲ. 기기별 인증절차

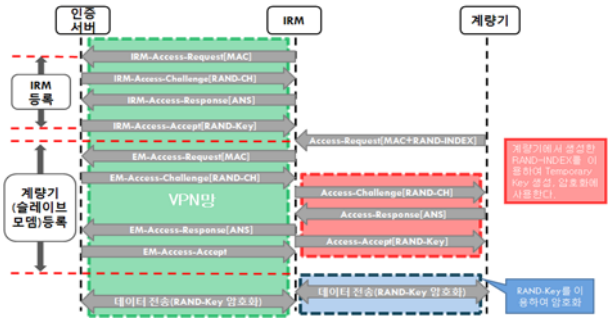


그림 2. IRM 및 PLC 모듈 인증절차

PLC기반 원격검침시스템에서는 현장에 설치되는 IRM과 단말장치인 계량기 내장형 PLC 모듈의 인증절차가 반드시 필요하며, 이는 그림 2에서 보여준다.

그림 2에서와 같이 IRM과 인증서버간 통신은 상용 인터넷망을 활용하므로 VPN을 통한 보안채널을 형성함으로써 상호 통신 보안성을 확보할 수 있다. 이를 기반으로 1차적으로는 IRM이 인증서버를 통해 인증을 받아야 하며, 2차로 계량기내 PLC 모듈이 IRM을 거쳐 인증서버에 인증을 요청하여 정상적으로 PLC 네트워크에 참여할 수 있는지 여부를 검증받게 된다.

여기서는 기존의 통신 보안키 평문 전송 문제[2]를 해결하기 위하여 기기 고유정보(MAC 주소 및 고유ID)를 활용한 임시키를 생성, 이를 초기단계에 적용하였다. 이를 통해 보안키의 외부 유출문제를 해결하였으며, 인증완료 시점에서는 실제 통신에 사용할 보안키를 새롭게 생성하도록 알고리즘을 설계하였다.

PLC 네트워크 토폴로지 특성상 IRM과 PLC 모듈사이에 리피터가 존재할 수 있으며, 리피터의 인증절차 및 리피터를 경유한 PLC 모듈의 인증절차는 그림 2와 유사하게 진행된다.

## Ⅳ. 보안키 갱신과정

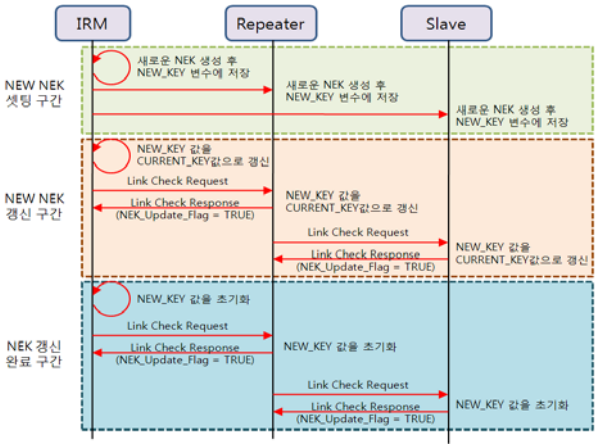


그림 3. PLC 보안키 갱신절차

국내 고속PLC 표준(KS X4600-1)[2]에 따라 구축되는 PLC 원격검침시스템은 기기간 통신에 사용될 보안키의 갱신절차가 없어 일정기간 패킷모니터링을 통해 보안키 유추가 가능하므로 그림 3과 같은 보안키 갱신절차를 활용함으로써 불법도청 및 패킷분석을 통한 보안키 도출이 불가능하도록 하였다.

## Ⅴ. 결론 및 향후 연구 방향

본 논문에서는 PLC기반 원격검침시스템의 기기 인증 및 관리체계를 새롭게 정의함으로써 대규모 상용화에 따른 보안적, 관리적 문제점을 해결할 수 있는 방안을 제시하였다. 설계된 인증 및 관리체계는 보안성 검토 및 실증시험을 통해 검증작업을 거친 후에 상용화 버전으로 보완될 필요가 있다.

## 참고문헌

[1] 기술표준원, “고속 전력선통신 국가표준 공청회”, 2006

[2] Standard, "High Speed Power Line Communication MAC and PHY", KS X4600-1, 2006