# 전력선 통신 네트워크를 위한 혼합형 보안구조 설계

*윤영직°, *허준, *홍충선, **주성호, **임용훈
*경희대학교 컴퓨터공학과, **한국전력공사 전력연구원
{jigyoung, heojoon, cshong}*@khu.ac.kr, {shju1052, adsac}**@kepri.re.kr

# A Hybrid Security Architecture Design for Power Line Communication Network

*Young Jig Yoon° , *Joon Heo, *Choong Seon Hong, **Sung Ho Ju, **Yong Hun Lim
*Department of Computer Engineering, Kyung Hee University, **KEPRI KEPCO

**요 약**

전력선을 이용한 통신 기술(Power Line Communication, PLC)은 현재 국내외에서 큰 관심을 받는 연구 분야로 국내에서도 이에 대한 연구와 개발이 활발히 진행되고 있다. 이 기술은 전력선을 이용하여 음성·데이터·인터넷 등을 고속으로 이용할 수 있는 서비스를 제공하며 나아가 가정의 모든 가정기기들을 연결하는 홈네트워크를 구성할 수도 있다. 하지만 전력선 통신 기술에는 보안상 많은 문제가 존재한다. 그 이유는 전력선 통신 네트워크가 전력선과 IP망을 둘 다 사용하는 혼합형 네트워크로 구성되어 있기 때문이다. 이로 인해 기존 IP망에서 사용하던 보안 기술들을 그대로 전력선 통신 네트워크에 적용하기에는 많은 어려움이 따르며 새로운 기술을 개발하고 그것을 기존 인프라에 적용하는 것 또한 많은 어려움이 따른다.

이에 본 논문에서는 기존 IP망에서 사용하던 공개키와 대칭키 방식을 이용하여 서로 다른 네트워크로 구성되어 있는 전력선 통신 네트워크의 보안을 위한 혼합형 보안구조를 제안한다.

## 1. 서 론

전력선을 이용한 통신 기술은 현재 국내외에서 큰 관심을 받는 연구 분야로 국내에서도 이에 대한 연구와 개발이 활발히 진행되고 있다. 이 기술은 전력선을 이용하여 음성·데이터·인터넷 등을 고속으로 이용할 수 있는 서비스를 제공하며 나아가 가정의 모든 가정기기들을 연결하는 홈네트워크를 구성할 수도 있다. 또한 전력 시스템의 광범위하고 계층적인 인프라가 통신 매체로 사용될 경우 그 활용 범위 및 비용의 절감은 매우 크다고 할 수 있을 것이다. 비록 전력선 통신 기술은 매체 특성으로 인한 몇 가지 단점을 가지고 있지만, 계측 시스템 및 자동 제어 시스템을 위한 가장 유력한 기술로 여겨지고 있다. 유비쿼터스 시대를 위한 통신 기술의 융합 및 발전에 초점이 맞추어져 있는 최근의 개발 동향으로 볼 때 전력선 통신 기술은 매우 중요한 부분을 담당하게 될 것이다.

하지만 이런 전력선 통신 기술은 보안상에 많은 문제점이 존재한다. 그 이유는 전력선 통신망이 이름 그대로 전력선만으로 구성되어 있는 것이 아니라 전력선과 IP망으로 이루어진 혼합형 네트워크로 구성되어 있기 때문이다. 이로 인해 그 동안 IP망에서 사용해오던 보안 기술들을 전력선 통신 네트워크에 그대로 사용하기에는 많은 어려움이 있다. 그렇다고 새로운 보안 기술을 개발하는 것 또한 쉬운 일이 아니며 설사 개발되었다 하더라도 이를 적용한 장비들을 기존 인프라에 재설치 하는데 엄청난 비용이 필요할 것이다. 이와 같은 문제점으로 인해 전력선 통신을 위한 보안 기술의 경우 다른 유무선 통신 기술에 비해 그 정의와 적용이 매우 미흡한 실정이며 기존 인프라에 적용할 수 있는 보안 기술의 개발 및 적용이 시급한 실정이다[7].

이에 본 논문에서는 이러한 문제를 해결하기 위한 노력의 하나로 전력선 통신 네트워크를 위한 혼합형 보안 구조를 제안한다. 이는 새로운 보안 기술을 제시하는 것이 아니라 기존 IP망에서 사용해왔던 공개키와 대칭키 기술을 이용하여 전력선 통신 네트워크에 적합한 보안 구조를 제안하는 것이다.

본 논문은 다음과 같이 구성되었다. 2장에서는 국내외 전력선 통신 관련 기술에서의 보안 기능들에 관해 요약하고, UPLC(Ubiquitous PLC) 프로젝트를 구성하고 있는 장비의 특징과 공개키 기반 구조의 특징을 설명한다. 3장에서는 본 논문에서 제안하는 전력선 통신 네트워크를 위한 혼합형 보안구조에 대하여 설명한다. 마지막으로 결론과 향후 과제에 관하여 언급한다.

## 2. 관련연구

현재까지 전력선 통신을 위한 보안 기술은 단편적으로 정의되거나, 기존 IP망에서의 보안 기술들을 그대로 적용하기 위한 정의가 대부분을 이루고 있다. 본 장에서는 국내(KS X4600-1[1]) 및 국외(HomePlug[2],

OPERA[3][4]) 전력선 통신 표준에서 정의하고 있는 보안 기능에 대해 정리하고 공개키 기반 구조의 특징을 설명한다.

### 2.1 국내외 PLC 표준에서의 보안 정의

■KS X4600-1

고속 전력선 통신을 위한 국내 표준으로서 동일한 셀(Cell)내의 장비들은 같은 암호화키를 사용한다. 데이터 네트워크를 위한 클래스 A의 경우 PHY레이어와 MAC레이어에서 56비트 DES 알고리즘을 사용하여 암호화/복호화를 수행한다. AV 네트워크를 위한 클래스 B의 경우 PHY레이어에서 3-DES 또는 AES 알고리즘을 사용해 암호화/복호화를 수행한다.

■HomePlug

대표적인 전력선 관련 국제 표준으로서 전력선 통신의 활용 분야에 따라 5가지 보안 모드(Security Mode, Insecure, User-confirm, Secure, Lock-down)를 각각 정의하고 있으며, 각 모드는 서로 다른 보안 정책을 가진다. 암호화 키 및 패스워드를 사용하는데 있어 매우 다양한 종류의 보안 키 (DAK, DPW, PPK 등) 생성 방식 및 절차를 정의하고 있다. 또한, 암호화 알고리즘으로는 AES-CBC 또는 1024비트 RSA 방식을 사용하도록 정의하고 있다.

■OPERA

유럽의 전력선 통신 프로젝트 연합으로서 암호화 방식으로는 DES 알고리즘을 정의하고 있으며, 보안 키 설정 방식으로는 Diffie-Hellman 기반의 알고리즘을 사용하고 있다. 또한, 시스템을 구성하는 장비들의 인증을 위해서는 RADIUS 인증 서버 기반의 방식을 정의하고 있다.

위에 정리한 3가지 기술들은 전력선 관련 국내외 주요 표준임에도 불구하고 보안 기능에 관한 정의는 매우 단편적이거나 개념적으로만 정의되고 있다. 더욱이 이러한 방식들을 사용함에 있어서 모든 장비들이 보안 기능을 수행할 수 있다는 가정아래 정의되고 있어 적용을 위한 비용의 문제를 쉽게 해결하기 어려운 문제점을 가지고 있다.

### 2.2 UPLC 프로젝트

UPLC 시스템[5]은 전기, 수도, 가스 등의 종단 계측기(meter), PCM (Power Conservation Monitoring), IPG (Intelligent PLC Gateway), IRM (Integrated Regional Manager) 등의 장비로 구성되며 그 구조는 그림 1과 같이 계층적으로 구성된다.

그림 1과 같이 전력선 계측 시스템의 종단에는 전기, 수도, 가스와 같은 다양한 계측기들이 사용될 것이며, PCM은 이러한 계측 데이터를 일정한 간격으로 수집하거나 제어 메시지를 계측기에 전송하는 역할을 수행한다. IPG는 전력선 통신 기반의 게이트웨이의 역할을 수행하게 되며, 기존 IP망과의 연동 및 PCM 장비를 제어하고 관리하는 역할을 하게 된다. IRM은 다수의 IPG를 지역적으로 관리하고 계측데이터를 인터넷 망을 통해 응용서버에 전송하거나 지역 내에 존재하는 장비들을 관리한다.

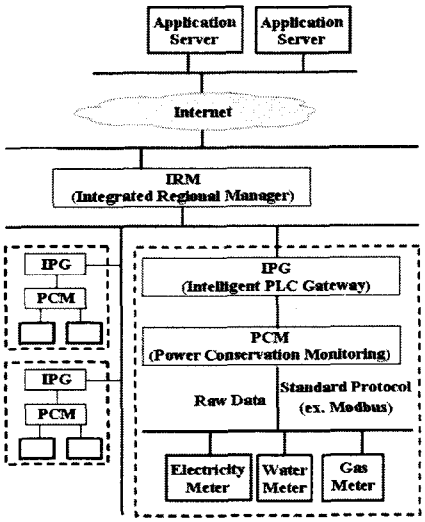


그림 1. UPLC 프로젝트 시스템 구조

### 2.3 공개키 기반 구조의 특징

공개키 기반 구조(PKI:Public Key Infrastructure)[6]는 기본적으로 인터넷과 같이 개방형 네트워크에서 안전하고 건전한 서비스가 이루어질 수 있도록 통신 정보의 기밀성, 인증성, 무결성, 부인방지 등 기본적인 보안 서비스를 가장 효과적으로 제공하는 기술이다. 이를 위해 신뢰할 수 있는 기관(인증기관: CA)에서 부여된 한 쌍의 {공개키, 개인키}와 인증서를 사용한다.

공개키와 개인키는 인증기관에 의해 동일한 알고리즘(예: RSA[6])을 사용하여 동시에 만들어진다. 생성된 개인키는 자신이 가지며 공개키는 인증기관에 등록되어 모든 사용자에게 공개된다. 공개키에 접근하기 위해서는 사용자 또한 인증기관에 등록이 되어야 한다.

공개키 기반구조에서 개인키와 쌍을 이루는 공개키는 인증기관(CA)에 등록되어 모든 이들에게 공개되어 있다. 이렇게 공개되어진 공개키는 송신측에서 메시지를 암호화하는데 사용되어지고 수신측에서는 자신의 개인키를 이용하여 암호화된 메시지를 복호화한다.

그림 2는 일반적으로 가장 많이 사용되고 있는 X.509 인증서[6] 기반의 공개키 암호화 전송과정을 나타낸다.

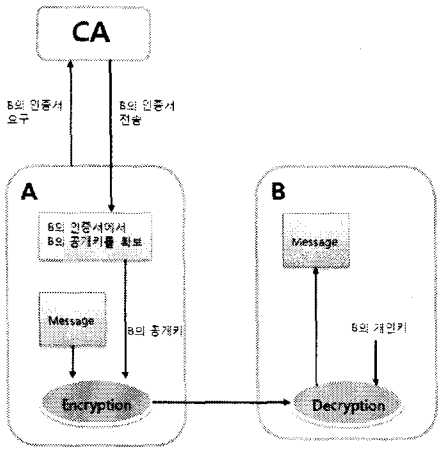


그림 2. 인증서 기반의 공개키 암호화 전송과정

그림 2에서 사용자 A는 사용자 B에게 메시지를 보내기 위해 메시지를 암호화하는 과정과 다시 이를 복호화 하는 과정을 나타내고 있다. 우선 A는 자신이 보낼 메시지를 암호화하기 위해서 수신측인 B의 공개키를 알아야 한다. 이미 A와 B는 자신의 공개키와 개인키를 생성하여 인증기관(CA)에 등록되어져 있기 때문에 A는 B의 공개키를 얻기 위해 CA에게 B의 인증서를 요구한다. CA로부터 B의 인증서를 받은 A는 인증서에서 B의 공개키를 확보하고 이 공개키로 자신의 메시지를 암호화하여 B에게 보낸다. B는 암호화된 메시지를 자신의 개인키를 이용하여 복호화한다.

### 3. 전력선통신망을 위한 혼합형 인증구조

그림 3은 공개키/대칭키 기반을 이용한 전력선 통신(PLC)망의 인증 구조의 개념을 설명하고 있다.

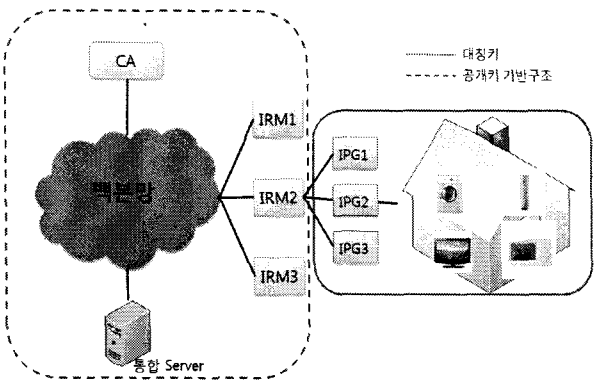


그림 3. 공개키/대칭키 기반 보안 구조

그림 3에서 PLC 기반 네트워크는 하나의 암호화 방식이 아닌 두 가지 암호화 방식(공개키를 사용하는 부분과 대칭키를 사용하는 부분)으로 혼합하여 사용하고 있는데 그 이유는 하나의 암호화 방식만으로 네트워크를 구성하기에는 많은 어려움이 따르기 때문이다.

위의 내용을 자세히 살펴보기 전에 우선 각 암호화 방식의 특징을 살펴보면

·대칭키의 경우 키의 길이가 짧고 동일한 키(암호화키=복호화키)를 서로 사용하기 때문에 공개키에 비해 연산속도가 빠르지만 키의 분배와 관리에 어려움이 많다.

·이에 비해 공개키는 키의 길이가 길고 암호화키(공개키)와 복호화키(개인키)가 서로 달라 대칭키에 비해 연산속도는 느리지만 키의 분배와 관리가 용이하다.

위와 같은 각 암호화 방식의 특징으로 인해 규모가 큰 PLC 네트워크에 하나의 방식만 사용하기에는 많은 어려움이 따른다.

만일 공개키 방식을 단말까지 적용할 경우 다음과 같은 어려움이 따른다.

첫 번째는 키 관리의 어려움이다. 공개키는 대칭키에 비해 키 관리 및 분배가 쉽다는 것은 단지 상대적으로 보안상 안전하다는 의미이지 보다 많은 키를 관리할 수 있다는 것은 아니다. 따라서 많은 단말들의 키를 몇 개의 CA에서 관리하기에는 많은 어려움이 따른다.

두 번째는 유동적인 단말의 수이다. 공개키 기반의 경우 인증을 위하여 새로운 단말이 생길 경우 이를 CA에 등록을 해야 하고 반대로 기존의 단말이 제거될 경우 탈퇴의 절차를 걸쳐 그 단말의 공개키를 CA에서 삭제를 한다. 하지만 한 가정에서 몇 개의 단말기만 고정적으로 사용하는 것이 아니라 필요에 의해 새롭게 사용하거나 사용하지 않을 수가 있다. 따라서 유동적인 단말로 인한 빈번한 등록과 탈퇴절차는 네트워크에 큰 부담을 줄 수 있다.

세 번째는 연산속도이다. 대칭키의 경우 키의 길이가 짧고 암호화키와 복호화키가 같기 때문에 빠른 연산이 가능하다. 이에 비해 공개키의 경우 지수승 연산을 하기 때문에 상대적으로 대칭키에 비해 많은 시간이 필요하다. 이에 따라 하단의 단말까지 공개키를 사용하면 너무 많은 연산시간이 필요하다.

이와 반대로 대칭키 방식만을 적용할 경우 앞서 설명했듯이 안전한 키의 분배와 관리가 어렵고 사용자는 통신하는 다른 많은 사용자의 키를 직접 관리해야 하므로 사용자의 부담이 커지며 공공기관이나 은행과 같이 보안에 많은 투자를 하는 곳과는 달리 사용자는 상대적으로 보안상 취약하므로 공격자에 의해 키가 유출될 위험이 크다.

이와 같이 하나의 암호화 방식으로 네트워크의 보안 구조를 형성할 경우 많은 어려움이 따르기 때문에 공개키 기반으로 하되 하단 부분은 대칭키를 사용함으로써 하나의 암호화 방식만을 사용하였을 때의

문제점을 보완하게 된다. 그리고 이미 업체에서 IRM과 IPG 장비간에 일정한 암호 방식을 사용하고 있기 때문에 결국 두 가지 방식을 이용할 수밖에 없다.

그림 4는 그림 3의 공개키/대칭키 기반 보안 구조를 바탕으로한 전체적인 키 생성 및 분배를 보여준다.

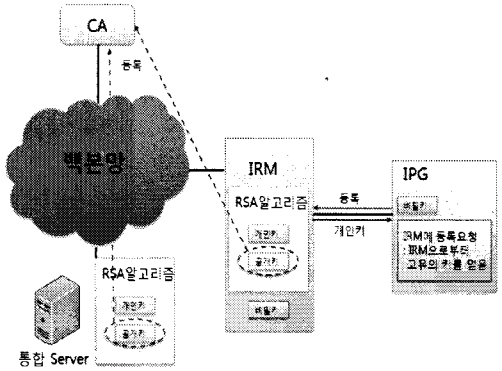


그림 4. 키 생성 및 분배

공개키를 사용하는 부분에서 통합 Server와 IRM은 RSA 알고리즘을 이용하여 한 쌍의 키(개인키, 공개키)를 생성하여 개인키는 자신이 보관하고 공개키는 CA에 등록을 한다. 반면 대칭키를 사용하는 부분에서 IPG는 IRM에 등록을 요청하면 IRM에서는 이 IPG를 등록하면서 이 IPG와 통신을 위하여 하나의 비밀키를 생성하여 IPG에 보내게 된다.

여기서 IRM은 공개키 사용 부분과 대칭키 사용 부분의 중첩된 부분이기 때문에 공개키 생성 알고리즘에 의한 개인키와 IPG와의 통신을 위한 비밀키를 둘 다 가지고 있다.

그림 5와 그림 6은 공개키 기반 구조를 사용하는 PLC기반 네트워크에서의 암호화 전송 방식의 개념을 설명하고 있다.

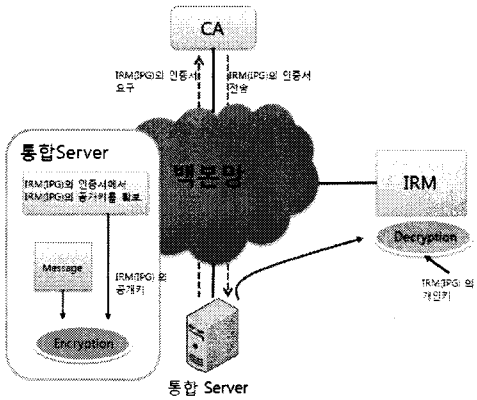


그림 5. 통합서버에서 IRM로의 암호화 전송

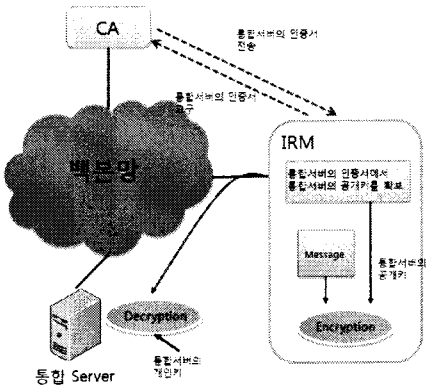


그림 6. IRM에서 통합서버로의 암호화 전송

그림 5에서 통합서버는 IRM에게 보낼 메시지를 암호화하기 위해 IRM의 공개키가 필요하다. 이미 통합서버와 모든 IRM의 공개키가 CA에 등록되어 있다고 했을 때 통합서버는 IPM의 공개키를 확보하기 위해 CA에 IRM의 인증서를 요구한다. 이렇게 CA로부터 IRM의 인증서를 받게 되면 거기서 IRM의 공개키를 알게 되고 이 공개키를 이용하여 보내고자 하는 메시지를 암호화하여 IRM로 보내게 된다. 그리고 IRM에서는 자신의 개인키를 이용하여 암호화된 메시지를 복호화하여 원래의 메시지를 받게 된다. 이와 같은 과정으로 그림 6에서는 IRM이 통합서버로 메시지를 보낸다. 먼저 IRM은 CA로부터 통합 Server의 인증서를 받아 통합 Server의 공개키를 확보한다. IRM은 인증서로부터 확보한 통합 Server의 공개키를 이용하여 보내고자 하는 메시지를 암호화한 후 통합 Server로 암호화된 메시지를 보내면 통합 Server에서는 보유하고 있던 자신의 개인키를 이용하여 IRM으로부터 받은 암호화된 메시지를 복호화한다.

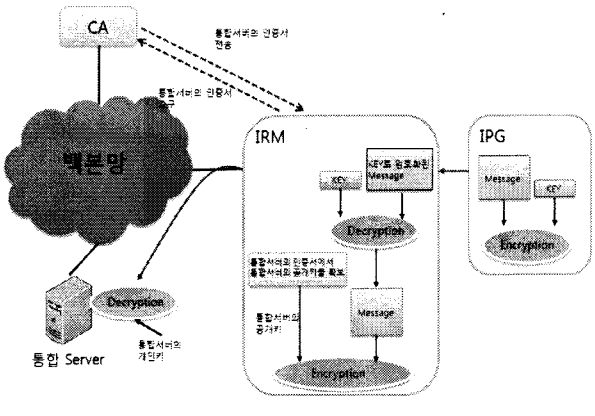


그림 7. IPG에서 통합서버로 메시지를 전송하는 과정

그림 7은 그림 5, 6의 내용을 바탕으로 한 IPG에서 통합서버로 메시지를 전송하는 과정을 보여주고 있다. 이 과정은 그림 5에서 보여준 과정과 비슷하지만 더 복잡한 과정을 수행하는데 그 이유는 IRM이 공개키 사용 부분과 대칭키 사용 부분의 중첩된 부분이기 때문이다.

우선 그림 7의 과정은 IPG에서 받은 메시지를 IRM에서 통합서버의 공개키로 메시지를 암호화하여 통합서버로 보내는 것까지는 그림 5와 같다. 하지만 이렇게 보내진 메시지는 통합서버에서는 아무 쓸모가 없다. 그 이유는 IPG가 IRM으로 메시지를 보낼 때 보안을 위하여 IPG와 IRM 사이의 비밀키로 암호화하여 보내기 때문이다.

그러므로 IRM에서는 IPG로부터 받은 메시지를 통합서버로 보내기 전에 IPG와 IRM 사이의 비밀키를 이용하여 복호화하는 과정을 먼저 수행한다. 이렇게 메시지를 복호화한 후에 그림 5의 과정을 거치게 되면 비로소 통합서버에서 IPG에서 보낸 메시지를 확인할 수 있게 된다.

## 4. 결 론

본 논문에서는 전력선 통신망의 보안을 위한 혼합형 인증구조를 제안하였다. IP망과 전력선과 같이 서로 다른 네트워크로 구성되어 있는 전력선 통신망은 기존의 IP망에서 사용하던 보안 기술들을 그대로 전력선 통신 네트워크에 사용하기에는 많은 어려움이 있다. 그러므로 기존의 보안 기술들을 응용하여 전력선 통신망에 적합하도록 보안 기술들을 사용하는 것이 가장 효율적인 방법이라 할 수 있다. 이를 위해 본 논문에서는 공개키와 대칭키라는 기존의 IP망에서 사용되었던 보안 기술들을 이용하여 전력선 통신망을 위한 혼합형 보안 구조를 제안하였다.

향후 과제로는 본 논문에서 제안된 인증 구조에 대한 보안성 및 성능 분석을 통하여 제안 사항을 검증하고 이를 통해 제안된 보안 구조를 개선하여 실제 전력선 통신망에서 안정적으로 사용이 가능하도록 해야 할 것이다.

## 참고문헌


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

[2] HomePlug Specification Version 1.0, http://www.homeplug.org

[3] UPLC(Ubiquitous Power Line Communication) project part of Korea Electric Power Corporation projects, http://www.kepri.re.kr/uplc

[4] Opera Alliance, "OPERA Specification : Technology," Jan. 2006.

[5] Opera Alliance, "OPERA Specification : System," Jan. 2006.

[6] Man Young LEE, "Internet Security Cryptographic principles, algorithms and protocols," WILEY, 2002.

[7] Joon Heo, Choong Seon Hong, Seong Ho Ju, Yong Hun Lim, Bum Suk Lee, Duck Hwa Hyun,"A Security Mechanism for Automation Control in PLC-based Networks",Proceedings of IEEE ISPLC2007, pp.466-470, Pisa, Italy, March 26-28 2007