전력선 계측 시스템을 위한 보안 모듈의 설계

*허준°, *홍충선, *김태홍, **주성호, **임용훈, **이범석, **현덕화
*경희대학교 컴퓨터공학과
**한국전력공사 전력연구원

A Design of Security Module for Power-line Metering System

*Joon Heo°, *Choong Seon Hong, *Tae Hong Kim,
**Sung Ho Ju, **Yong Hun Lim, **Bum Suk Lee, **Duck Hwa Hyun
*Department of Computer Engineering, Kyung Hee University
**KEPRI KEPCO
{heojoon, cshong, ttahong}*@khu.ac.kr, {shju1052, adsac, leebs, hyundh}**@kepri.re.kr

요 약

전력선 통신 기술의 적용이 기존 전력 시스템 구성 장비들을 활용하며 적용될 경우 보안 기술의 부재는 심각한 문제를 야기할 수 있다. 대표적인 활용 분야가 될 전력선 계측 시스템의 경우 전송데이터는 공격자에 의해 쉽게 변조될 수 있다. 특히, 전송데이터가 과금이나 전력제어를 위한 데이터일 경우 변조된 데이터로 인해 심각한 피해를 초래할 수 있다. 본 논문에서는 전력선 계측 시스템에서 장비간 보안 키 생성, 전송데이터 암호화 및 데이터 인증을 위한 인증코드를 생성할 수 있는 보안 모듈을 정의하였다. 또한, 정의된 보안 모듈의 유효성을 검증하기 위해 계측 시스템을 구성하고 계측 데이터를 통한 검증을 수행하였다.

1. 서 론

전력 시스템의 광범위하고 계층적인 인프라가 통신 매체로 사용될 경우 그 활용 범위 및 비용의 절감은 매우 크다고 할 수 있을 것이다. 전력선 통신(Power Line Communication) 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.

UPLC(Ubiqutious Power Line Communication) 프로젝트는 기존에 존재하는 전력선 인프라를 활용해 전력 공급회사에서 소비 가정까지 이르는 계측 및 자동제어 통신 시스템을 설계하고 개발하는데 목적을 두고 있다. 이러한 시스템을 구축함으로써 전력 공급회사는 각 소비 가정의 계측 데이터(전기, 가스, 수도 등)를 원격에서 수집할 수 있으며, 나아가서는 전력을 포함하는 에너지 소비를 자동 제어할 수 있게 된다[7]. 현재까지 전력선 통신 기술은 전송 에러율 및 전송 속도 향상을 위한 다양한 노력이 시도되었다. 그러나, 전력선 통신을 위한 보안 기술의 경우 다른 유무선 통신 기술에 비해 그 정의와 적용이 매우 미흡한 실정이다[8][9][10][11]. 또한, 새로운 보안 기술이 적용되는 장비를 모든 기존 인프라에 재설치하는 것은 엄청난 비용 문제를 야기하게 됨으로, 기존 인프라에 적용할 수 있는 보안 기술의 개발 및 적용이 시급한 실정이다[1].

본 논문에서는 이러한 문제를 해결하기 위한 노력의 하나로 전력선 계측 시스템을 위한 보안 모듈의 기능을 정의하고 실제 계측 데이터를 활용한 검증을 수행하였다. 정의된 보안 모듈은 계측기(meter)와 수집 장치 중간에 위치하여 장비간 보안 키 생성, 전송데이터 암호화, 인증코드 생성의 기능을 수행하게 된다. 현재 전력인프라를 구성하고 있는 대부분의 계측장비가 보안 기술이 적용되지 않은 상태이므로 보안 모듈이 중간에 추가되는 방법을 사용하였으나, 추후에는 계측 시스템의 각 장비에 포함되는 형태를 가지게 될 것이다.

본 논문은 다음과 같이 구성되었다. 2장에서는 국내외 전력선 통신 관련 기술에서의 보안 기능 정의를 정리한다. 3장에서는 UPLC 프로젝트를 구성하고 있는 장비의 특징을 설명하고 현재 시스템에서의 공격 가능성에 대하여 기술한다. 4장에서는 보안 모듈을 구성하는 보안 키 생성, 전송 데이터 암호화, 인증코드 생성 기능을 각각 정의한다. 5장에서는 제안된 보안 모듈을 검증하기 위해 실험환경을 구성하고 계측 데이터를 통해 보안 모듈을 검증한다. 마지

막으로 결론과 향후과제에 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[9]) 및 국외(HomePlug[8], OPERA[10][11]) 전력선 통신 표준에서 정의하고 있는 보안 기능에 대해 정리한다.

■ KS X4600-1

고속 전력선 통신을 위한 국내 표준으로서 동일한 셀(Cell)내의 장비들은 같은 암호화 키를 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.

3. UPLC 프로젝트 구조 및 공격 가능성

UPLC 시스템[7]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.

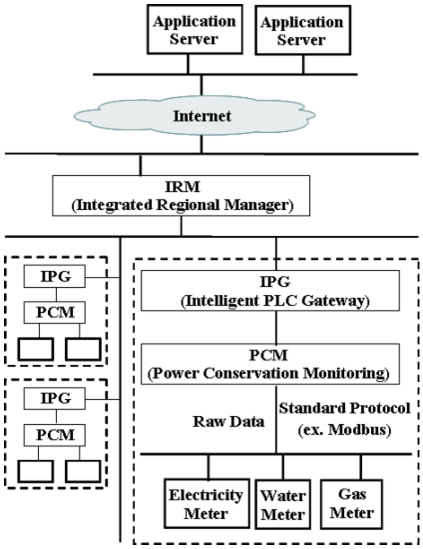

그림 1. UPLC 프로젝트 시스템 구조

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 하게된다. IRM은 다수의 IPG를 지역적으로 관리하고 계측데이터를 인터넷 망을 통해 응용서버에 전송하거나 지역내에 존재하는 장비들을 관리한다.

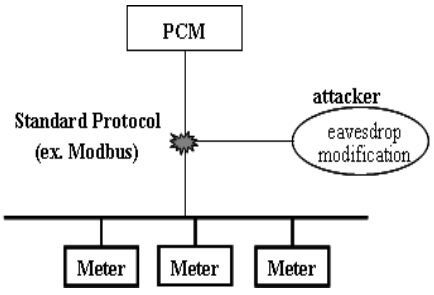

그림 2. 계측기와 PCM간 계측데이터의 취약성

이러한 시스템 구조에서 종단에 위치하는 계측기와 PCM 사이에는 Modbus[3]와 같이 기존 인프라에서 사용되던 데이터 전송 프로토콜이 사용될 것이다. PCM, IPG, IRM등의 장비는 전력선 통신의 활용범위에 따라 새롭게 정의되고 경우에 따라 보안기능이 적용되어 설치될 수 있으나 대부분의 기존 인프라를 사용하게 되는 계측기와 PCM간의 보안은 매우 취약하다고 할 수 있다. 그림 2는 이러한 취약

성의 예를 보여주고 있다. 공격자에 의해 쉽게 변조될 수 있는 데이터가 과금이나 시스템 제어와 같은 목적으로 사용되는 경우 이러한 보안의 취약성은 큰 문제를 야기시킬 수 있으며, 시스템 전체적으로도 신뢰성을 보장할 수 없게 된다.

4. 제안된 보안 모듈

앞서 설명한 전력선 통신과 관련된 국내외 표준에서 정의하는 보안 기능의 경우 단편적인 암호화 및 보안 키의 종류를 정의를 하고 있어, 기존 전력 인프라를 구성하는 장비에 적용하기에 어려움이 있다. 본 논문에서는 앞서 설명한 UPLC 계측 시스템의 계측기와 PCM 사이의 취약성을 개선할 수 있는 보안 모듈을 정의하고 있으나, 활용범위에 따라 IPG, IRM과 같은 관리 장비에도 적용될 수 있다. 그림 3은 제안된 보안 모듈을 구성하는 3가지 세부 모듈의 관계와 계측 시스템내에서의 위치를 나타내고 있다.

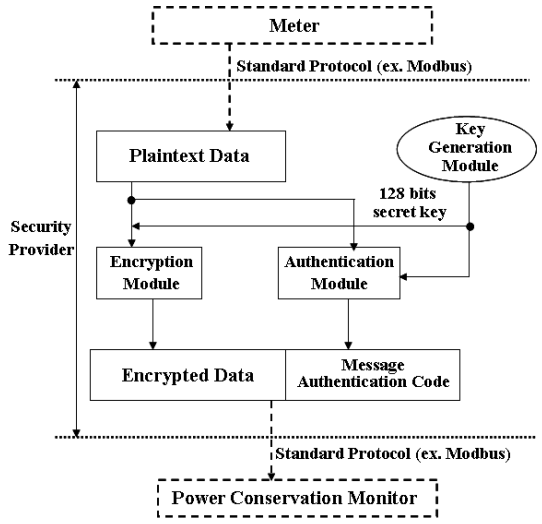

그림 3. 제안된 보안 모듈의 구조 및 기능

각 세부 모듈을 정의함에 있어 보안 관련 표준으로 정의된 키 생성, 암호화 및 인증코드 알고리즘을 적용하는 이유는 기술의 적용 및 확장성을 위해서이다. 전력선 통신이 IP네트워크, 센서네트워크 등과 연동되기 위해서는 규격화된 암호화 알고리즘을 사용해야 하며 실제 전력선 통신 프로토콜에 맞게 최적화되어 적용되어야 한다.

① 보안 키 생성 모듈(Key Generation Module)

전송데이터 암호화 및 인증코드 생성을 위해서는 가장 먼저 보안 키의 생성이 이루어져야 한다.
보안 키 생성 모듈은 계측기와 PCM 장비간에 Diffie-Hellman 알고리즘[4]을 기반으로 보안 키를 생성하는 역할을 수행한다.

② 암호화 모듈(Encryption Module)

데이터 에러율이 상대적으로 높은 전력선의 매체적 특성상 암호화 방식으로는 블록 기반의 암호화 알고리즘이 정의되어야 한다. 본 논문에서 제안하는 암호화 모듈은 128비트의 AES 알고리즘[2][4]을 사용한다. AES는 DES 알고리즘[6]에 비해 보안 강도 및 다른 통신기술과의 적용성도 높다고 판단된다. 암호화 모듈의 경우 통신 프레임의 구조 및 전송 방식에 따라 구현되어야 한다. 예를 들어 계측기와 PCM간의 통신 프로토콜로서 Modbus를 사용할 경우 암호화 모듈을 통해 암호화되는 프레임 형식은 그림 4와 같다.

Station ID	Function	Byte Count	Encrypted Data	Error Check	MAC
1 Byte	1 Byte	1 Byte	16 Byte	1 Byte	16 Byte

그림 4. 암호화된 전송 데이터

③ 인증코드 생성 모듈(Authentication Module)

데이터의 무결성을 검증하기 위한 인증코드의 생성은 HMAC-MD5 알고리즘[5]을 통해 수행된다. 이 알고리즘에서는 보안 키 생성 모듈에서 생성된 키를 사용하게 되며 생성된 인증코드는 암호화된 데이터 프레임 뒤에 추가된다. 그림 5는 이러한 관계를 전체적으로 표현하고 있다.

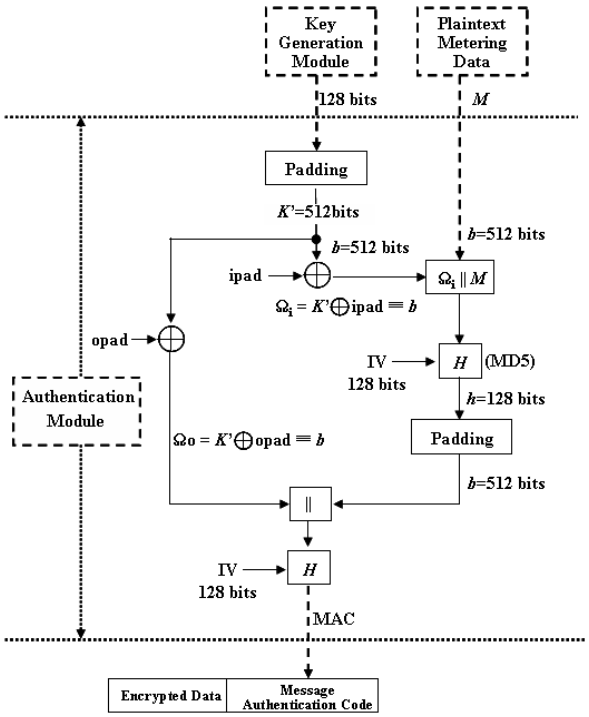

그림 5. 인증 코드 생성 모듈의 동작과정

5. 실험환경 및 구현

본 논문에서는 전력선 계측 시스템의 전송데이터 보호를 위해 장비간 보안 키 생성, 암호화 모듈, 인증코드 생성 모듈을 정의하였다. 이러한 모듈을 적용함에 있어 가장 중요한 부분은 Diffie-Hellman,

AES, HMAC-MD5등과 같은 보안 표준 알고리즘을 바탕으로 정의된 보안 기능을 계측 시스템 장비간 통신 특징에 맞추어 적용하는 것이다. 그림 6과 그림 7은 제안된 보안 모듈의 기능을 검증하기 위한 실험환경 및 구현 결과를 나타내고 있다. 실험을 위한 보안 모듈은 소프트웨어적으로 구현되었다. 그러나, 향후 계측기 및 PCM에 하드웨어적으로 구현된다면 연산을 위한 오버헤드 및 정확성이 향상될 수 있을 것이다.

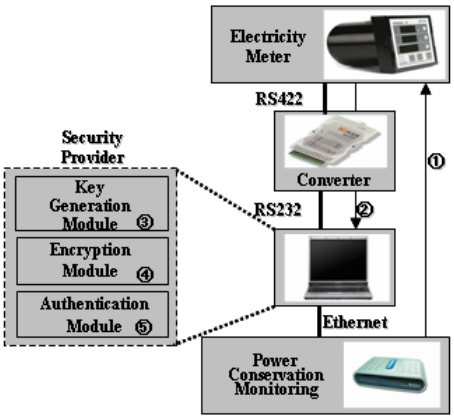

그림 6. 실험 환경

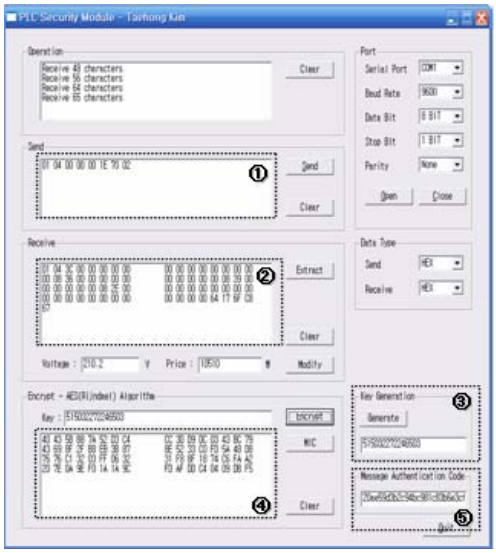

그림 7. 보안 모듈의 구현 결과 및 데이터

① PCM은 Modbus 프로토콜을 사용하여 전기 계측기에 현재 전압 값을 요청한다.
② 전기 계측기는 현재 전압을 측정하여 그 값을 보안 모듈에 전달한다.
③ 초기 설정과정에서 보안 모듈과 PCM 장비간에는 보안 키 생성 모듈에 의해 128비트의 키가 생성된다.
④ 암호화 모듈을 통해 전송데이터가 암호화되며 이때 ③단계에서 생성된 보안키가 사용된다.
⑤ 인증 모듈은 128비트의 인증 코드를 생성하여 전압 값의 무결성을 검증하는데 사용하도록 한다.

보안 모듈로부터 데이터를 전송 받은 PCM은 보안 키를 사용한 복호화 및 인증코드 확인을 통해 계측기에서 전송된 데이터가 안전하게 전송되었음을 확인한다.

6. 결론 및 향후과제

본 논문에서는 전력선 계측시스템을 위한 보안 모듈을 정의하고 실험환경을 통해 검증하였다. 보안 모듈을 정의하는데 있어 보안 관련 표준 기술들을 적용하여 다른 기술과의 확장성이 가능하도록 하였다. 전력선 통신을 다른 기술들과 함께 응용하기 위해서는 서로 다르게 정의되어 있는 보안 기능들을 통합할 수 있는 새로 기능이 요구되기도 하며, 향후 과제로는 이러한 요구사항을 도출하여 기존의 IP 네트워크 및 센서 네트워크와의 연동이 가능하도록 발전시켜야 할 것이다. 또한, 계측시스템 장비를 위한 인증 기술이 적용되어야 보다 신뢰성 있는 네트워크가 구축될 수 있을 것이다.

7. 참고 문헌

[1] Albert Treytl, Noel Roberts and Gerhard P. Hancke, "Security Architecture for Power-line Metering System," In proceedings of IEEE Factory Communication Systems 2004, pp. 393-396, September 2004.

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

[3] MODBUS Application Protocol Specification V1.1a, http://www.modbus.org

[4] FIPS Publication ZZZ, "Announcing the Advanced Encryption Standard (AES)," US DoC/NIST, 2001.

[5] Cheng, P., and R. Glenn, "Test Cases for HMAC-MD5 and HMAC-SHA-1," RFC2202, September 1997.

[6] FIPS Publication 46-3,"Data Encryption standard (DES)," US DoC/NIST, 1999.

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

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

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

[10] Opera Alliance, “OPERA Specification : Technology,” Jan. 2006.

[11] Opera Alliance, “OPERA Specification : System,” Jan. 2006.