PLC 홈네트워크의 보안 취약성 및 대응방안 분석

주성호, 임용훈, 박병석, 김태완, 김영현, 최문석, 이범석
한국전력공사 전력연구원

Analysis of Security Weakness and Countermeasure in PLC-based Homenetwork

Seong-ho Ju, Yong-hun Lim, Byung-seok Park, Tae-wan Kim, Young-hyun Kim, Moon-seok Choi, Beom-seok Lee
Korea Electric Power Research Institute

ABSTRACT

고속 PLC 기술의 실현으로 인한 외부 엑세스망과의 연동이 가능해지고, 댁내에서 저속/고속 PLC 기술의 활용으로 생활기기의 제어와 멀티미디어 서비스의 공급이 원활하게 이루어 질 경우 다양한 홈 네트워크 서비스를 제공할 수 있게 된다. 하지만 이러한 PLC 기술 기반의 다양한 서비스들이 PLC 엑세스망 및 홈네트워크를 통해 제공될 경우, 다양한 보안 취약성을 포함하게 된다. 따라서 현재 홈 네트워크에서 제기되고 있는 보안 취약성뿐만 아니라 PLC 기술을 적용할 경우 발생가능한 모든 보안적 문제점을 살펴볼 필요가 있으며, 이러한 문제를 해결하기 위해 제안되고 있는 보안 서비스 모델을 PLC 기반의 홈 네트워크 보안과 연관하여 최적의 보안시스템을 개발할 필요가 있다. 본 논문에서는 PLC망에서의 보안 취약성을 분석하고 이에 따른 대응방안을 분석하여 PLC기반의 홈네트워크 보급이 활성화될 수 있도록 한다.

1. PLC 적용 홈 네트워크에서의 보안

고속 PLC 기술의 실현으로 인한 외부 엑세스 망과의 연동이 가능해지고, 댁내에서 저속/고속 PLC 기술의 활용으로 생활기기의 제어와 멀티미디어 서비스의 공급이 원활하게 이루어 질 경우 다양한 홈 네트워크 서비스를 제공할 수 있게 된다. 이러한 서비스를 제공하는데 있어 게이트웨이를 통한 다른 유/무선 기술과의 연동도 함께 이루어 질 것으로 예상할 수 있다. PLC 기술을 적용한 홈 네트워크 서비스들은 크게 홈 엔터테인먼트 서비스, 홈 데이터 서비스, 홈 정보 서비스, 홈 오토메이션 서비스, 홈 시큐리티 서비스, 헬스케어 서비스 등으로 나눌 수 있다. 이러한 PLC 기술 기반의 다양한 서비스들은 다른 유/무선 기술들과의 연동 및 외부 엑세스 망을 통한 댁내 제어 등을 통해 제공될 수 있으며, 이에 따라 다양한 보안 취약성을 포함하게 된다. 따라서, 현재 홈 네트워크에서 제기되고 있는 보안 취약성을 살펴보고, 이러한 문제를 해결하기 위해 제안되고 있는 보안 서비스 모델을 PLC 기반의 홈 네트워크 보안과 연관하여 기술한다.

2. 안전한 PLC망을 위한 보안 요구사항

현재까지의 PLC 기술은 관련 장비를 생산하고 그 장비간 전력선을 통한 통신의 실현과 성능 향상에 초점을 두고 진행되어 왔다고 할 수 있다. 다른 유무선 프로토콜의 경우도 보안의 중요성은 침해나 사고 발생 후 논의되고 보완되는 경우가 많았다. 하지만 현재의 기술 개발 속도, 개인이나 가정 정보의 중요성을 생각해 보면, 현 시점에서 안전한 PLC망을 위한 보안 요구사항을 도출하고, 관련기술을 개발하여 적용하는 것이 매우 중요하다고 할 수 있다. 따라서, 안전한 PLC 망을 위해 필요한 요구사항들을 도출하고 현재까지의 개발 동향으로 볼 때 어떠한 보안 기술들이 적용되고 있는지에 대하여 기술하도록 한다.

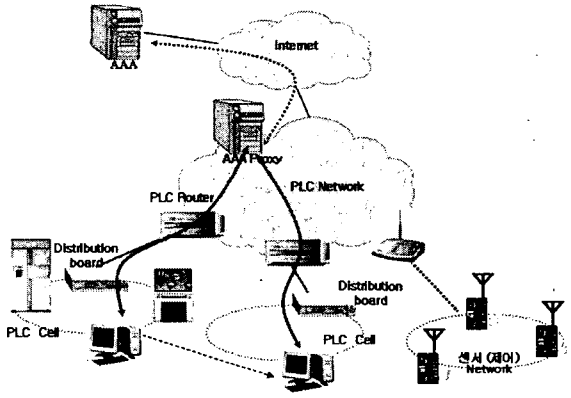

그림 1 PLC망에서의 사용자 인증

2.1 사용자 인증

PLC망에서 인증 기술은 댁내뿐 아니라 댁외에서도 PLC망 자원에 대한 원격 접근을 위해 필요하며, 댁내에서 인터넷 뱅킹과 같은 서비스 사업자가 제공하는 서비스를 사용하기 위해서도 필요하다. 따라서, 기존의 다양한 사용자 인증 기술을 수용할 수 있는 종합적인 사용자 인증 인프라 기술 개념으로 개발되어야 한다. PLC 망에서는 구성원의 의지에 따라 사용자 인증을 요청하는 경우도 있지만, 구성원 의지와 관계없이 구성원 상황에 따라 사용자가 인증이 되어 구성원에 적합한 서비스가 제공되는 경우도 예상할 수 있다. 그러므로, 기존의 사용자 인증 기술 외에 향후 고속 및 저속 PLC 융합 환경에 적합한 새로운 사용자 인증 기술도 필요하게 될 것이다.

또한, 인증 정보의 안전성 확보를 위해서 댁내외 인증정보가 분리되어 관리되어야 하므로 댁내에서 댁외의 인증 서비스를 받기 위해서는 댁내에서 사용되는 다양한 인증 기능이 댁외 사업자가 제공하는 인증 기능과 연동될 수 있도록 하는 정합 환

경의 개발이 필요하다. 그림 1은 저속 및 고속 PLC 융합 환경에서 PLC 네트워크에 존재하는 사용자 인증에 관해 설명하고 있다. 인증을 담당하는 서버의 역할을 여러 가지고 정의할 수 있겠으나, 이 그림에서는 현재 인터넷망에서 가장 널리 사용되고 있는 AAA 서버가 사용자 인증 기능을 제공한다고 가정하였다. 또한 이러한 환경에서 PLC망 안에 포함된 사용자를 인증하기 위한 Proxy 서버의 사용도 고려해 볼 수 있다.

2.2 디바이스 인증

불법 디바이스의 사용을 방지하지 위해서는 PLC망 구성요소인 디바이스 자체에 대한 인증 과정이 필요하다. 현재까지 디바이스 인증은 통합 홈 네트워크 환경에서의 미들웨어 레벨에서 제공되고 있다. 예를 들면, UPnP의 경우 디바이스마다 부여된 Security ID로 디바이스의 홈 네트워크 등록과정에서 디바이스 인증이 이루어지고 있으며, Havi의 경우에는 디바이스마다 고유한 인증서를 발행하여 디바이스 인증 수행 시 사용하고 있다. 그러나, 현재의 PLC 기술이 이러한 방법에서 유용한지에 대한 검증 작업이 이루어져야한다. 현재의 미들웨어 기술은 PLC 기술을 널리 수용하고 있지 않은 상황이므로, PLC 디바이스 인증은 앞으로 많은 연구가 진행되어야 할 것으로 판단된다. 또한, 현재 홈 네트워크 구성 디바이스 유효성 확인을 위한 시리얼 넘버나 인증서등은 개별 제조업체 등에서 자체적으로 발행하고 있다. 따라서, 향후 디바이스에 대한 다양한 사후 서비스 제공이나 유비쿼터스 컴퓨팅 환경에서 디바이스 및 사용자 인증 기능과 결합한 새로운 서비스의 제공을 위해서는 디바이스 인증정보에 대한 통일된 발급체계 및 관리체계에 대한 기술적, 정책적인 연구가 필요하다고 할 수 있다.

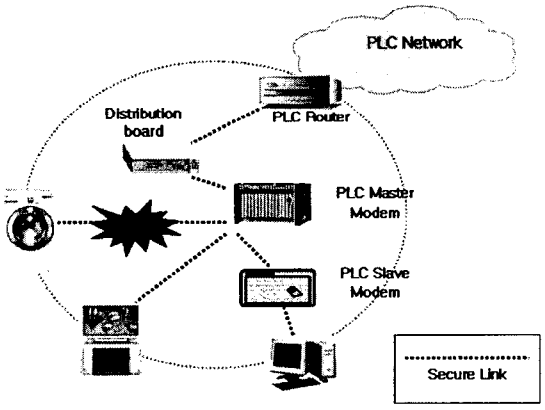

그림 2 PLC 기기간 인증 개념도

2.3 기기간 인증

원활한 PLC 기반 서비스 제공을 위해서는 기본적으로 PLC 망 구성요소간의 자원공유를 위한 신뢰가 확보되어야 한다. 이를 위해서는 구성요소간의 기기간 상호인증이 필요하다. 그림 2는 PLC 기기간 인증의 개념을 설명한 것이다. 인증을 통해 해당 기기간 안전한 채널이 형성되게 되며, 이러한 안전성을 기반으로 다양한 서비스들을 제공할 수 있게 된다. 기기간 인증 기능은 다양한 PLC 기반 서비스를 위한 기본적인 보안 기능이라고 할 수 있으므로 통합적 홈 네트워크 서비스 제공을 위해서는 다른 보안 기능과의 원활한 연동성이 확보되어야 한다. 즉, 사용자 인증 기능, 접근제어 기능 등을 위해서는 기본적으로 기기간 인증 기능이 우선되어야 하므로 다른 보안 기능과의 연동성이 고려되어야 한다.

2.4 접근제어

서비스에 따라 PLC망 자원에 대한 접근권한 제어 기능이 요구된다. 구성원별로 제공받을 수 있는 PLC 기반 서비스의 종류가 다르고, PLC망 구성요소에 대한 제어 범위도 다르므로 이에 대한 접근제어 기능이 필요하다. 유비쿼터스 컴퓨팅 환경을 고려할 때 접근제어를 위한 ACL(Access Control List)은 단말기기가 내장하고 있는 것이 효율적이라고 할 수 있지만 안전성 측면이나 사용자 편리성 측면에서 일관된 보안정책 따라 접근권한이 제어되어야 한다[1].

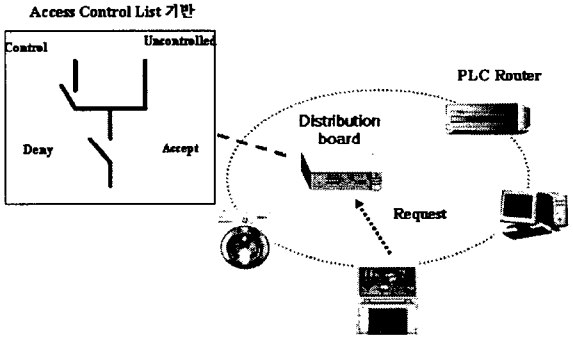

그림 3 PLC 기기간 인증 개념도

3. PLC망에서 보안 기술 적용

PLC 기술의 경우 다른 프로토콜들과는 상이하게 표준으로 정해지지 않아 보안 기술의 적용에 있어서도 특정 알고리즘을 규정하기는 쉽지 않다. 하지만, 현재까지의 기술 개발 동향이나 몇 가지 사례들을 조사해보면, 데이터 암호화/복호화를 위해 DES, Triple-DES가 널리 사용되는 것으로 판단할 수 있다. 또한, 앞으로의 기술 개발 동향과 다른 프로토콜들과의 연동을 고려해보면, AES 알고리즘이 사용될 가능성도 높다고 할 수 있다.

3.1 데이터 암호화/복호화

PLC 기술에서 데이터 암호화/복호화는 보안의 가장 기본적인 요소라고 할 수 있다. PLC 기술을 사용하여 데이터나 특정 제어프레임을 전송할 때 암호화/복호화를 통해 안정성을 확보하는 것은 가장 기본적이면서도 중요한 보안기능이라고 할 수 있다. <그림 7>은 다중반송파 송신기 블록도를 나타내고 있다. 그림에서 볼 수 있듯이 송신기의 가장 앞부분에 Encryption 모듈을 사용하여 데이터를 암호화한 수 전송하게 된다. 이때 사용되는 알고리즘은 여러 가지가 있을 수 있으나 현재까지의 개발 동향으로 볼 때 DES 알고리즘이 가장 보편적으로 사용되고 있다고 할 수 있다.

3.2 공유 Key 설정

PLC 네트워크에서의 데이터 통신에는 보안을 위하여 56-비트 DES 방식 및 다른 암호화 알고리즘이 사용될 수 있다. 동일한 물리적 네트워크상에 공존하는 셀들을 구분해 주는 역할을 하는 것은 46-비트 길이의 GID(Group ID)로서 이는 동일한 물리적 네트워크 내에 무한개의 서로 다른 셀들이 공존할 수 있음을 의미하게 된다. GID가 동일한 경우에만 스테이션 간의 통신이 허용된다. 이와 같이 동일 셀에 속한 스테이션들은 암호화키를 공유하는 방법이 정의되어야 한다. 하지만, 어떤 방법으로 암호화키를 공유하고 관리할 것인지에 관한 부분은 앞으로

많은 연구를 통해 개발되어야 한다. 공유키에 관한 부분은 PLC 기술 뿐 아니라 대부분의 프로토콜에서 핵심적인 부분으로 간주되고 있다[2].

4. PLC망 활용 시나리오에서의 보안이슈

본 장에서는 PLC 활용분야를 크게 3가지 시스템으로 구분하고, 그 활용 시나리오에서의 보안이슈에 관하여 설명한다.

4.1 정보기기 및 AV 시스템

PLC 기술은 정보기기간의 통신과 AV 전달을 목적으로 하는 많은 서비스 분야에 활용될 것이다. PLC처럼 유선의 형태로 존재하는 장비들은 상시(always-on) 접속 조건의 PC처럼 보안의 위험에 쉽게 노출 된다고 볼 수 있다. 특히, PLC를 사용할 때 현재까지 게이트웨이(Gateway)에 의한 종단 홈 네트워크는 보안에 안전하지 않기 때문에 보안의 위험은 일반적인 인터넷을 사용하는 통신보다 더 크다고 말할 수 있다. 만일 취약한 셀(cell)이 공격을 받게 되면 다른 네트워크에 있는 셀에 존재하는 많은 사용자와 장비도 위험을 받을 가능성이 있다. 악의적인 공격자가 취약한 셀 안에 존재하는 제어기기를 공격하고, 셀을 제어하여 기기들을 통제하면 심각한 결과를 초래하게 된다. 특히 현재까지 PLC의 특성상 이러한 공격을 받았을 때 기존의 유선 네트워크처럼 기타 장비를 통해 물리적으로 네트워크를 종료하기는 쉽지 않다. 이러한 문제를 해결하기 위해서는 앞서 언급한 사용자 인증 및 기기간 인증이 확실하게 보장되어야 할 것이다. 또한, 제어 메시지를 전송하고 이를 수행하는 과정에서의 메시지 암호화/복호화를 통한 보안 기능이 수행되어야 할 것이다.

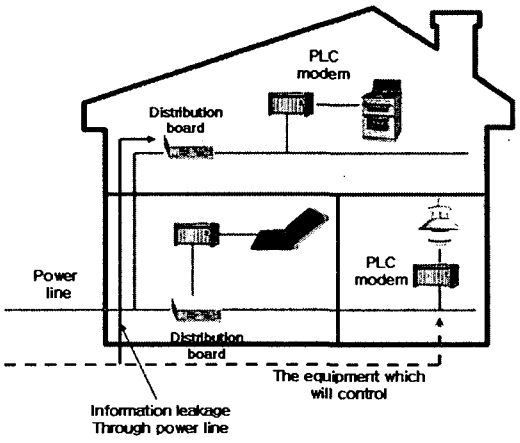

그림 4 제어시스템에서의 보안 이슈

4.2 제어시스템

일반적인 셀의 개념은 PLC 기술을 사용하는 많은 장비들이 전력이 연결된 상태로 특정 범위 안에 존재하는 것을 말할 수 있다. 이러한 환경에서 필요 상황에 따라 셀의 외부에서 접근하여 특정 장비를 제어할 수 있는 경우가 발생할 수 있으며, PLC망과 장비들은 이러한 기능을 제공할 수 있어야 한다. 항상 전력이 연결되어 있는 PLC 장비들이 인터넷에 연결 될 경우, PC기반의 네트워크 환경처럼 보안에 대한 위험성을 내포하게 된다. 예를 들어, 사용자가 외부로부터 TV를 제어하는 신호를 보냈지만 불법적인 공격자가 제어 시스템 및 메시지를 조작하여 전기나 가스를 제어할 경우 심각한 문제를 발생시키게 된다. 그림 4는 제어시스템에서 발생할 수 있는 보안의 문제점을 나타내고 있다.

4.3 공동시스템

각 가정에 존재하는 기기들은 GID를 통해 자신만의 논리적인 네트워크인 셀을 형성한다. 공동 시스템에서 특정 셀의 보안이 취약하게 되면, 전체 공동 네트워크는 취약한 셀을 통해 함께 위험에 노출될 수 있다. 공동 시스템에서 여러 개의 key를 사용하게 될 경우 key의 복잡성은 오히려 보안상의 취약성으로 발전할 수 있으므로 그림 5와 같은 중앙 관리형 보안 시스템의 구축이 더 좋은 방법으로 여겨지고 있다.

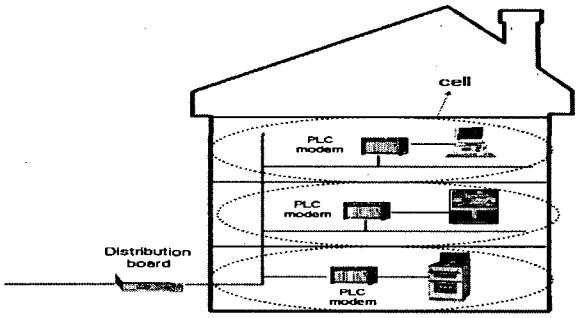

그림 5 중앙 관리형 보안시스템

5. 결 론

PLC 기술의 개발로 인한 다양한 서비스의 활용과 성능향상은 향후 경제적으로 큰 파급효과를 기대해도 좋을 만큼 발전하고 있다. 하지만, PLC 기술을 위한 보안 기술의 개발은 매우 미흡한 상황으로 판단할 수 있다. 보안 문제가 해결되지 않은 상태에서 PLC 기술의 보편화가 이루어지고 다른 기술들과 연동을 통한 서비스가 일반화된 후, 보안 문제의 심각성이 제기되면 그 상황에서의 보안문제는 더욱 어려운 문제로 남게 될 가능성을 배제할 수 없다. 따라서, 현재의 시점에서 PLC망의 보안상 취약성을 발견하고 그 해결책으로서 보안 요구사항을 도출하여, 앞으로의 기술개발에 포함시킬 수 있어야 한다. 본 문서에서는 PLC 망이 적용되는 홈 네트워크에서의 보안 취약성 및 서비스 모델에 관하여 기술하였고, PLC망 네트워크 보안 고려사항에 대해서 언급하였다. 또한 현재까지의 개발 동향을 토대로 활용할 수 있는 암호화 알고리즘과 PLC망 적용 시스템을 크게 3가지 시스템으로 구분하여 보안 이슈에 관하여 설명하였다. 현재의 상황에서 특정 알고리즘을 정의하거나 보안 시스템을 구성하기에 어려움이 있으나 본 문서에서 기술한 요구사항들과 활용 시나리오에서 발생할 수 있는 보안 취약성을 점차적으로 해결하고 관련 기술을 개발해 나가야 할 것이다. 또한, PLC 기술은 향후 다른 유무선 프로토콜과 연동되어 시너지 효과를 가져올 것으로 예상할 수 있으므로 통합 게이트웨이 및 미들웨어를 통한 보안에 관해서도 함께 연구와 개발이 진행되어야 할 것이다.

참 고 문 헌

[1] Y. Wu, X. C. Yun, "A High-Performance Network Monitoring Platform for Intrusion Detection", LNCS3391, Information Networking pp. 52-61, 2005.

[2] B. Schneier, Applied Cryptography, John wiley Sons, pp. 129-183, 1997.