광대역 전력선통신 기반 보안기술 동향

백종목. 주성호. 김충효
한국전력공사

The study of BPLC security technology trend

Jongmock Baek. Seongho Ju. Chunghyo Kim
Korea Electric Power Coorporation

ABSTRACT

본 논문에서는 원격검침시스템의 기반기술이 되는 광대역 전력선 통신인프라에 필요한 보안요구사항을 도출하고 국내외 표준에 반영된 보안기술을 연구하였다. 전력선 통신망에서 자원의 가용성을 확보하기위해 사용자 및 기기의 인증기능과 접근제어기능을 검토하였으며 전력선통신 표준에 반영된 보안기술은 제각기 다른 방향으로 접근하는 것을 알수있었다. 특히 한국표준에 기술된 보안은 셀단위의 동일한 키를 사용하고 칩셀의 하위계층에서 58비트 DES알고리즘만으로 보안대책이 미흡하고 다른 보안솔루션이 적용이 필요한 것으로 사료 된다

서 론

전력선통신기술이 국내외적으로 24Mbps에서 200Mbps의 제품이 상용화 되어있으며 400Mbps의 기술을 개발하는 단계에 접어들었다. 전력IT분야의 정부지원으로 국산 전력선통신 핵심칩이 개발되었다. 또한 스마트그리드 환경에서 저탄소 녹색성장의 요소기술로서 인식되어 전력회사에서는 다양한 부가서비스 적용을 위한 시도가 진행되고 있다. 정부의 스마트그리드 2030비전에 따라 2020년까지 1790만가구에 스마트메타 보급시 전력선통신 기반의 원격검침기술은 중요한 역할을 할것으로 전망된다. 현재까지는 통신속도와 신뢰성확보를 통한 기술의 고도화가 화두였으나 본격적인 상용화 단계에서는 보안성 확보기술이 시급하게 대두되어 본 논문에서는 전력선 통신인프라에 요구되는 보안요구 사항과 동향을 연구하였다

본 론

1.1 안전한 BPL망을 위한 보안 요구사항

전력선 통신망은 사용자의 전원공급선로에 통신기능을 부가하여 전원공급과 통신매체로서의 역할을 할 수 있는 효율적인 기술이다. 이러한 장점을 활용하여 댁내 전력량계에서 인근 전주 집속장치강 별도의 통신선 없는 전력선통신 기술이 활용됨에 따라 안전한 BPL 망자원의 가용성 확보에 필요한 인증과 접근제어 보안기술에 대해 고찰한다

1.1.1 사용자 인증

BPL망에서 인터넷 뱅킹과 같은 서비스 사업자가 제공하는 서비스를 사용하기 위해서는 사용자인증이 필요하다. 이는 일반적인 인터넷 망에서 이루어지는 다양한 사용자 인증 기술을 수용할 수 있는 종합적인 사용자 인증 인프라 기술 개념으로 전력선 통신망에서도 적용되어야 하므로 고속 및 저속 BPL 융합 환경에 적합한 새로운 사용자 인증 기술도 필요하게 될 것이다. [그림1]에서 저속 및 고속 BPL 융합 환경에서 BPL 네트워크에 존재하는 사용자 인증에 관해 설명하고 있다. 본 논문에서는 현재 인터넷망에서 가장 널리 사용되고 있는 AAA 서버가 사용자 인증 기능을 제공한다고 가정하였다. 또한 이러한 환경에서 BPL망 안에 포함된 사용자를 인증하기 위한 Proxy 서버의 사용도 고려해 볼 수 있다.

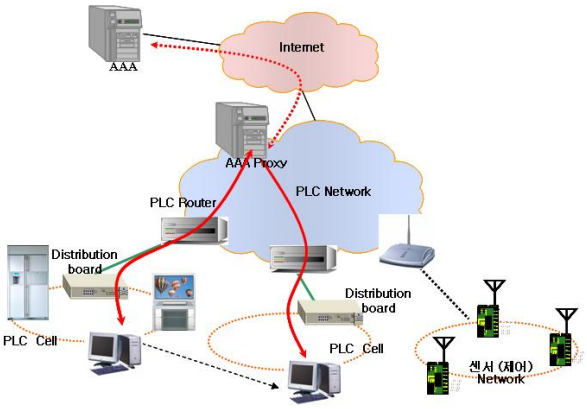

그림 1 BPL망에서의 사용자 인증
Fig. 1 User Authentication in BPLC network

1.1.2 기기 인증

BPL망 환경에서 허가되지 않은 기기의 접속방지를 위해 기기 자체에 대한 인증과정이 필요하다. 현재 통합 홈 네트워크 환경에서 기기인증은 미들웨어 레벨에서 제공되고 있다. UPnP의 경우 기기마다 부여된 Security ID로 기기의 홈 네트워크 등록과정에 인증이 이루어지고 있으며, HAVi의 경우에는 기기마다 고유한 인증서를 발행하여 인증시 사용하고 있다. 그러나, 현재의 BPL 기술이 이러한 방법에서 유용한지에 대한 검증 작업이 이루어져야 한다. 현재의 미들웨어 기술은 BPL기술을 널리 수용하고 있지 않은 상황이므로, BPL 디바이스 인증은 앞으로 많은 연구가 진행되어야 할 것으로 판단된다.

1.1.3 기기간 인증

BPL기반 인프라에서 서비스 제공을 위해서는 BPL 망 구성

요소간의 자원공유를 위한 신뢰가 전제되어야 하며 이를 위해서는 기기간 상호인증이 필요하다. 인증을 통해 기기간 안전한 채널이 형성되므로 이는 서비스를 위한 기본적인 보안기능이라고 할 수 있고 통합적 홈 네트워크 서비스 제공을 위해서는 다른 보안 기능과의 원활한 연동성이 확보되어야 한다. 즉, 사용자인증 기능, 접근제어 기능 등을 위해서는 기본적으로 기기간 인증 기능이 우선되어야 한다. 기기인증을 응용레벨에서 제공하는 경우도 검토할 수 있다. 전력 제어망 보안을 위해 Challenge & Responce 핸드쉐이크절차를 이용하여 적법한 기기를 인증하는 방법이 유럽표준에서 권고하고 있다.

1.1.4 접근제어

사용자마다 제공받을 수 있는 서비스의 종류가 다르고, BPL 망 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 주어져야 한다. 또한, 인증 정보 유출로 인한 불법적인 접근시도가 발생한 경우, 보안정책을 능동적으로 변경하여 공격에 대응하는 기능도 필요하다.

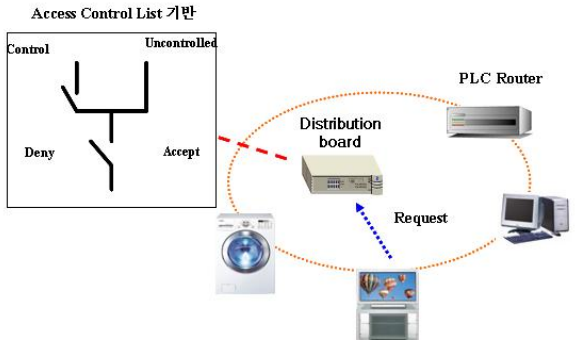

그림 2 BPL기기 접근제어 개념도
Fig. 2 The concept of access control

[그림2]에서 BPL망 환경에 적용할 수 있는 접근제어 개념을 설명하고 있다. 구성원 역할에 따라 권한을 정의하여 접근제어를 제공할 수 있으며 이는 보안정책에 따라 장비나 서비스의 관점에서 행해 질 수도 있다.

1.2 국내외 표준에서의 반영된 보안기술

1.2.1 KS X4600-1 (한국) [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 수행하며 최근 보안이 취약성을 고려 AES적용을 위한 활동이 있다. AV 네트워크를 위한 클래스 B의 경우 PHY레이어에서 3 DES 또는 AES 알고리즘을 사용해 암호화/복호화를 수행한다.

1.2.2 HomePlug (미국) [2]

대표적인 전력선 관련 국제 표준으로서 전력선 통신의 활용분야에 따라 5가지 보안 모드를 각각 정의하고 있으며, 각 모드는 서로 다른 보안 정책을 가진다. 암호화 키 및 패스워드를 사용하는데 있어 매우 다양한 종류의 보안 키생성 방식 및 절차를 정의하고 있다. 또한, 암호화 알고리즘으로는 AES CBC 또는 1024비트 RSA 방식을 사용하도록 정의하고 있다.

1.2.3 OPERA (유럽) [3]

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

1.3 국내표준 전력선 통신보안의 취약점

검침서비스는 댁내 수집장치와 계량기간에 유선 혹은 무선 통신으로 검침정보를 수집한다. BPL 통신을 위한 보안 기술은 동일한 셀(Cell)의 장비들이 동일한 보안키를 사용하는 단순한 개념의 보안 방법을 사용하고 있으며, 무선 전송 프로콜의 경우 아무런 보안 기술이 고려되지 못하고 있다. 현재 KS X 4600 1 규격에서 BPL 네트워크에서의 데이터 통신에는 보안을 위하여 56 비트 DES 방식의 암호화가 사용된다. 동일한 물리적 네트워크상에 공존하는 셀들을 구분해 주는 역할을 하는 것은 46 비트 길이의 GID로서 이는 동일한 물리적 네트워크 내에 무한개의 서로 다른 셀들이 공존할 수 있음을 의미한다. GID가 동일한 경우에만 스테이션들 간의 통신이 허용된다. 이와 같이 동일 셀에 속한 스테이션들은 암호화 키를 공유하며 56 비트 DES 방식의 암호화를 통해 데이터 통신에 대한 보안을 보장한다. 그러나, 이러한 방법만을 사용하게 되면 동일한 셀에 존재하는 모든 장비들이 동일한 보안키를 사용하게 되며, 보안키의 갱신 없이 계속 사용될 경우 외부로부터의 공격에 노출될 수 있다.

결 론

전력선통신기반 인프라구축이 확산되고 이를 이용한 원격검침 서비스가 시행되면서 전력설비의 가용성과 검침데이터의 신뢰성확보에 필요한 보안기술을 검토하였다. 보안요구사항에서 일반적인 망에서 사용되는 인증과 접근제어방법을 전력선통신 환경 적합하도록 관련분야의 연구가 필요함을 확인하였고 전력선 통신칩셀에서 제공하는 보안기술만으로는 한계가있으며 PLC이외의 구간에대한 보안대책도 필요할 것이다..

참 고 문 헌

[1] KS X4600 1. 고속전력선통신 MAC 및 PHY계층
[2] HomePlug Specification ver 1.0.
http:\\ www.homeplug.org
[3] Open PLC European Research Alliance. Spec. ver 1.0
http:\\ www.ist opera.org