情 報 保 護 學 會 誌
第20卷 第1號, 2010. 2

고속전력선통신이 적용된 홈네트워크의 보안취약점 분석

이 정 열*, 윤 진 희*, 전 해 성*, 김 학 범**

요 약

고속전력선통신(PLC : Power Line Communication)은 전력선을 통신회선으로 이용하여 종래의 방식보다 용이하게 LAN환경을 구축하는 기술이다. 예전부터 전력회사에서 검침 등에 이용되었던 기술이며, 근래에 들어 수십Mbps이상의 고속통신이 가능해지면서 다시금 주목을 받고 있다. 그러나 고속전력선통신은 기존의 네트워크 시스템과는 상이한 몇 가지 특성들을 가지고 있다. 따라서 기존의 보안적인 이슈뿐만 아니라 고속전력선통신 특유의 보안적인 고려도 필요로 하고 있다. 본고에서는 고속전력선통신에 대한 이해를 돕고자 그에 대한 대략적인 개요와 표준화 동향 그리고 고속전력선통신에서 고려해야 할 보안요구사항들에 대해 제시한다.

Ⅰ. 서 론

20세기말에서 21세기 초에 걸쳐서 네트워크기술은 비약적으로 성장하였다. 그리고 이런 네트워크기술의 발달은 인간생활에 근본적인 영향을 끼쳤다. 경제의 글로벌화, 인터넷, 글로벌커뮤니케이션, 디지털방송, 홈오토메이션 등은 이제 익숙한 개념들이다. 하지만 네트워크기술이 아무리 발달하더라도, 이런 기술을 받아들일 만한 강력한 인프라가 없다면 무용지물이다. 한때 인터넷의 보급에 크게 기여했던 ADSL은 이미 정보의 부하를 감당하지 못하여 뒤안길로 밀려났다. 그만큼 사람들이 고용량, 고품질의 데이터 사용이 크게 늘어났다. 이제 네트워크에도 양보다는 질의 시대가 온 것이다. 하지만 이런 흐름을 감당할 만한 기술이 있는가? 이런 의문에 대한 해결책으로 부상된 대안 중의 하나가 고속전력선통신이다.

고속전력선통신은 기존의 전력선이라는 인프라를 적극 활용할 수 있는 기술로 주목을 받고 있으며, 크게 성장할 만한 잠재성이 있는 분야이다. 그러나 고속전력선통신에는 선결되어야 할 많은 이슈들이 있는데 그 중 대표적인 것이 보안문제이다. 고속전력선통신은 데이터통신이 상정하지 않은 전력선을 통해 통신을 수행하며, 기존의 어떤 정보네트워크 케이블에도 적합하지 않은 50~60Hz의 주파수를 사용한다. 따라서 이를 이용한 공격기법들도 나올 것이며, 그에 대한 대비책도 마련되어야 할 것이다.

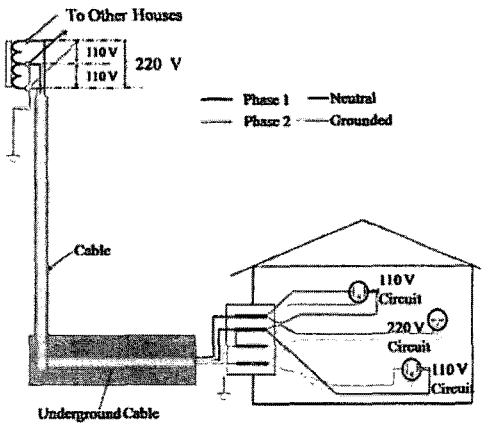
특히, 고속전력선통신이 유용하게 이용될 분야 중 하나가 홈네트워크 분야이다. 홈네트워크의 경우 기존의 디바이스에 LAN 포트를 추가할 필요가 없고, 댁내에서 추가적인 LAN배선을 하지 않아도 네트워크가 가능한 점 등 많은 이점이 존재한다. 그러나 홈네트워크의 특성상 개인의 프라이버시와 관련된 민감한 정보들이 저장되고 이동된다. 따라서 고속전력선통신이 적용될 경우의 민감한 보안취약성에 대해서도 고려해야 한다.

Ⅱ. 고속전력선통신의 개요

2.1 고속전력선통신 소개

고속전력선통신은 전력선을 통신회선으로 사용하는 기술로써 450kHz이하의 주파수를 사용하는 것을 저속전력선통신, 2~30MHz를 사용하는 것을 고속전력선통

* 동국대학교 국제정보대학원(02-2260-3733~5)
** 에스지어드밴텍(주)/동국대학교 국제정보대학원(khb0305@dongguk.edu)



〔그림 1〕 댁내 배선 Topology

신라고 부른다. 10~450kHz까지의 주파수를 사용하는 제품의 데이터 통신 속도는 9600bps정도이다.

원래 2001년부터 실용화가 논의되었던 기술이지만, 전력선은 근본적으로 높은 주파수의 전기신호가 흐르는 것을 상정하고 있기 때문에, 전력선통신에 의해 누설된 전파가 단파선을 이용하는 무선통신(아마추어 통신)이나 의료기기 등에 영향을 미칠 가능성도 지적되었다. 이에 따라, 추진파와 반대파와 사이의 긴 논의가 계속되었다.

현재는 고속전력선통신대응 어댑터가 차례로 발매되고 있으며, 이 어댑터를 인터넷모뎀 등의 기기와 콘센트에 접속해 놓으면, 어느 방에서든지 콘센트에서 전기를 통해 네트워크에 접속이 가능해진다. 집안 어디에서나 콘센트만 있으면 추가적인 배선은 불필요하다. 유선 LAN과는 달리 신규의 배선 또한 필요치 않다. 무선 LAN에서는 전파가 닿지 않으면 통신이 불가능 했지만 이러한 제약이 고속전력선통신에는 없다는 점 또한 장점이다.

고속전력선통신기술과 관련된 최초의 특허신청은 1920년대의 것으로, 발명자는 "장치의 시동과 정지를 위해 고안된 케이블을 통한 몇 가지 음성 주파수톤의 이용"이라는 특허를 발표하였다. 이 연구는 두 가지 방향으로 갈라져 연구가 진행되었다. 일부는 음성방송을 위한 기술을 목표로 하여 1940년대에 이미 이 장치가 양산되었다. 다른 하나는 노이즈가 방지된 제어시스템의 개발을 목표로 하여, 고속전력선통신을 사용하여 영상신호를 수Mhz의 주파수 범위로 전송하는 기술이 개발되었다.

1970년대에 들어서는 러시아에서 고속전력선통신의 프로토타입이라 부를 만한 기술이 연구되기 시작했다. 예를 들어, 전동차량에서 고압선전선을 통한 원격계측 데이터의 전송과 같은 기술들이 고안되었다. 1980년대에는 원격으로 정보를 수신 받아, 시내건축물의 전원 신호나 조명의 통신, 제어의 로컬네트워크를 형성하는 기술이 고안되었다.

이런 기술들은 고속의 정보전달이 필요하지 않아, 당시의 기술수준으로도 충분히 가능하였다. 그러나 준 디지털적 방법이나 아날로그적 방법으로는 고속통신을 현실화하는 것은 불가능하였다. 또한, 기술의 코스트와 성능수준에도 추가기능의 범위가 제한되고 있었다.

고속전력선통신기술에 대한 관심이 다시 등장한 것은 1990년대 중반 무렵부터로, 지멘스나 노르텔(Nortel) 등의 몇몇 대기업과 통신프로바이더 회사가, 케이블을 사용한 데이터, 회화전송의 시험적 프로젝트를 개시했다. 프로젝트는 몇 번의 실패를 하였으나, 세계적으로 고속전력선통신에 대한 관심을 환기시켰다. 또한 IEEE 등에 의한 고속전력선통신 표준안도 동시에 진행되었다.

이후, 고속전력선통신은 급격한 기술발전이 전 세계적으로 급격하게 진행되었다. 미국과 캐나다 등지에서는 HPA(Homeplug Powerline Alliance)를 결성하여, 2001년부터 고속전력선통신장치의 양산을 시작하였다. 유럽에서도 고속전력선통신관련 기술들과 제품들이 차례로 개발되고 있다. 독일 RWE는 2001년 여름 RWE Power Net을 통한 고속 인터넷 서비스를 시작하였으며, 스위스의 아스콤(Ascom) 역시 고속전력선통신모뎀의 양산을 시작하였다. 프랑스에서는 이후 5년 내에 누구나 고속전력선통신으로 인터넷을 이용할 수 있도록 하는 국가프로젝트를 발표하였다. 프랑스에서는 이 프로젝트를 위한 통신 인프라 구축을 위해 13억 달러의 투입을 상정하고 있다.

고속전력선통신 분야가 기술적으로나 경제적으로 많은 의미가 있다는 것은 확실하다. 새로운 구축이나 투자가 불필요한 기존의 전기배선을 사용하기 때문에 광대한 잠재적 이용자가 존재한다. 이를 통해 인터넷 및 관련통신의 이용자가 빠르게 늘어날 만한 기반기술 제공을 기대할 만한 기술이다.

2.2 고속전력선통신의 한계성

이런 기술적인 발전 성과에도 불구하고, 물리적인 한계와 결점을 가지고 있기 때문에 고속전력선통신이

Ethernet에 비해 이점만을 가지고 있다고 하기는 힘들다. 고속전력선통신은 기본적인 특징은 일반 전력선케이블을 쓴다는 점이다. 정보교환전용으로 만들어지지 않은 전기케이블을 쓴다는 점에서 고속전력선통신은 개념 그 자체에서 근본적인 결점을 가지고 있다.

고속전력선통신의 첫 번째 문제점은 50~60Hz의 주파수를 주로 사용한다는 것이다. 이 회선은 기존의 어떤 정보네트워크용 케이블에서도 사용되지 않던 주파수이다. 이로 인해 기존의 네트워크 인프라와의 호환성 문제가 발생한다. 또한 전기케이블에서 빈번한 신호반사문제를 어떻게 해결할 것이냐가 문제이다.

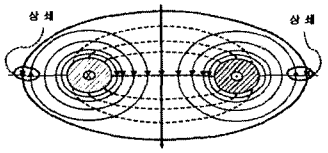
전송신호의 반사는 일반적으로 전송매체 구조의 비균질성에 의해 발생하기도 하나, 콘센트간의 간섭이나 멀티탭 등에 의해서도 빈번하게 발생한다. 이런 신호의 간섭은 주파수선의 변형을 불러온다. 이용자가 고속전력선통신에 접속하거나, 연결을 해제하는 것만으로도 신호의 변형이 발생한다.

또한 이런 효과는 방송전파나 광통신에서는 잘 알려져 있는 심볼간간섭(*ISI: InterSymbol Interface*)을 발생시킨다. ISI는 원래의 신호보다 늦거나 빠르게 신호들이 발생하는 현상을 말한다. ISI가 발생하는 원인에 관계없이, 결과적으로 신호스펙트럼이 크게 확장되거나 하나로 모아져서, 통신시간의 에러나 전송속도를 제한시키게 된다.

고속전력선통신 기술의 두 번째 문제점은 전기 노이즈이다. 일반적으로 전기케이블에는 별다른 노이즈 처리가 되어 있지 않다. 또한, 전기제품에는 다양한 잡음 노이즈가 발생하는데, 대부분은 우연히 발생하는 진폭 노이즈이지만 굉장히 빈번하게 발생된다. 결국 고속전력선통신은 그 구조상 다양하고 빈번한 전기노이즈에 노출되어 있는 것이다. "전기노이즈"라는 우연히 발생하는 노이즈는 고속전력선통신 전송속도 저하의 주요원인 중 하나이며, 노이즈레벨이 높을수록 통신효율은 떨어진다.

고속전력선통신기술의 세 번째 문제점은 전자기(電磁氣)와의 양립성이 요구된다는 점이다. 일반적인 전기신호와 고속의 데이터신호를 중첩하는 과정에서 신호의 변형이 발생하며, 동시에 전자파가 발생된다. 이러한 전자파는 다른 전파공간에 상호간섭 현상을 일으킨다. 이 문제에 대해 현시점에서는 뚜렷한 해결책은 없다.

고속전력선통신기술의 네 번째 문제점은 감쇄현상이다. 대용량의 추가정보를 필요로 하는 고속전송에서는 일반적으로 수십 MHz의 주파수영역이 사용된다는 점이다. 전송주파수영역이 커지면 커질수록 감쇄현상계수 또한 증폭된다.



<작표> Klaus Dostert, Propagation Channel Characterization and Modeling Outdoor Power Supply Grids as Communication Channels, ISPLC2005, April 2005.

〔그림 2〕 전력선에 의한 전계분포[11]

Ⅲ. 고속전력선통신의 표준화 동향

근래에는 고속전력선통신의 표준화가 국제적인 단위로 진행되고 있지만 그전에는 단체·지역별로 표준화가 진행되었다. 현재 고속 전력선 통신 표준은 HPA, UPA (Universal Powerline Association), CEPCA (Consumer Electronics Powerline Communication Alliance), OPERA(Open Plc European Research Alliance), ETSI (European Telecommunications Standards Institute), IEEE 등에서 개발되고 있다. 저속 전력선 통신의 경우 X10이 사실상 표준으로 산업체 등에서 오래 전부터 사용되어 왔고 최근에는 저속 전력선 통신 표준도 미국(LonWorks)과 유럽(KNX)를 중심으로 글로벌화 되고 있다.

3.1 해외 표준화 동향[1]~[7]

HPA는 2000년 4월에 미국에서 설립된 가장 오래된 고속전력선통신 표준화 단체이다. 미국을 중심으로 유럽, 아시아의 약 70개사가 가입하고 있으며, 임원사로는 인텔, 모토로라, 시스코, 텍사스인스트루먼트, LG, 샤프 등의 기업들이 있다. HPA의 기술 표준인 HomePlug는 Intellon사의 기술을 기본 기술로 사용하고 있고 고속전력선통신기기를 사용한 옥내 네트워크와 제품기술의 표준화 및 호환에 중점을 두고 있다. 저속에 해당되는 HomePlug 1.0은 4.3~20.9MHz의 주파수를 이용하여 14Mbps의 전송속도를 낼 수 있고 56bit DES 암호 알고리즘을 사용한다. 이후 *HomePlug 1.0*보다 더욱 빠른 85Mbps의 HomePlug 1.0 Turbo가 개발되었

다. HomePlug AV는 HDTV나 VoIP에 사용되는 기술로 2~28MHz의 주파수 대역을 이용한다. 이론상 200Mbps의 전송 속도를 가지고 있고 128bit의 AES 암호 알고리즘을 사용한다. 기존의 광대역 망과 고속전력선통신 네트워크 연결하는 것에 중점을 둔 HomePlug BPL은 현재 개발 중이고, HomePlug Command & Control(HPCC)은 저속의 저가기술로 가정 내의 조명, 환기, 그 외 각종기기의 제어를 담당하는 기술이다.

UPA는 고속전력선통신 기술과 관련한 다양한 분야의 기업이 모여 2004년 9월에 설립된 비영리조직으로 임원사로는 미국 Ambient, 캐나다 Corinex, 스페인 DS2, 프랑스 Schneider, 일본의 이토츄상사, 스미토모 전기공업, 도요네트워크가 참여하고 있다. UPA는 DS2 기술을 중심으로 하여 옥외와 옥내, 두 가지 이용형태의 공존을 위한 기술사양 및 변조방식 등의 표준화에 주력하고 있다. UPA 표준인 DHS(Digital Home Standard)의 변조 방식은 Windowed OFDM/QAM이며 전송속도는 200Mbps이고 2~32MHz의 주파수를 사용한다. 보안을 위해 3-DES 암호화를 이용하고 통신 최대거리는 150m이다.

유럽에서는 EU가 중심이 되어 국가 프로젝트로서 OPERA를 2004년에 설립했다. 유럽의 전력회사, 모뎀 제조업체, 칩 제조업체, 고속전력선통신 포럼, 대학 등이 참가하였는데 DS2 기술을 중심으로 현재의 시스템을 향상시키고 고속전력선통신 서비스를 개발하며 시스템 표준화를 목표로 하고 있다.

CEPCA는 고속전력선통신 유저인 가전·PC업계를 중심으로 2005년 6월에 발족한 비영리 조직이다. 소니, 미쓰비시, 파나소닉 등 일본 회사들로 주축이 된 CEPCA는 현재 가능한 다양한 전력선 기술들의 공존을 실현할 수 있는 표준을 개발 중에 있다. CEPCA에서 만든 표준 HD-PLC는 4~28MHz 대역을 이용하고 이론상 최대 전송 속도는 190Mbps이다. 보안을 위해 128bit AES를 이용하고 있다. 변조방식은 Wavelet OFDM 방식을 사용하고 통신 최대거리는 150m이다.

IEEE에서는 다양한 형태의 전력선 통신 시스템 표준을 만들고 있다. 이에는 결합장치와 안전성에 관한 검토, 특히 중압계 안전성 기준책정에 중점을 둔 IEEE P1675와 EMC의 시험과 BPL기기의 측정 순서·설치에 관한 표준을 개발하는 IEEE P1775가 있다. 또 IEEE P1901는 전력선 통신망에서 광대역을 위한 MAC 및 PHY의 표준을 개발하고 있으며 대표적으로 HPA, UPA, CEPCA, OPERA 등이 참여하고 있다.

X10은 전등을 켜거나 끄는 라이팅 애플리케이션 시장의 2/3 정도를 점유하고 있는 프로토콜로 역사가 오래된 기술이다. X10은 60bps 정도의 전송속도를 지녔기에 주로 단말 기기들을 제어하는 용도로 쓰인다.

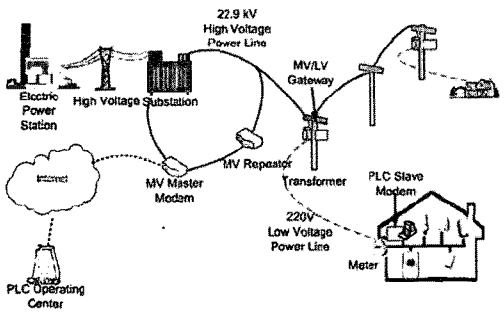
LonWorks는 빌딩 내의 시설 자동화를 위한 제어 표준으로 가정 자동화, 가로등 제어, 에너지 관리 및 시설 과금 등을 위해 사용되며 국제 표준화 기구 ISO/IEC 14908 표준에 근거한다.

3.2 국내 표준화 동향

국내의 경우는 지식경제부 기술표준원이 주관하고 한전 전력연구원, 전기연구원, 한국산업기술대학교 등이 참여하여 고속전력선통신 국가 표준 제정을 목표로 고속 전력선 통신 표준기술연구회를 발족하였다. 젤라인사의 기술을 기반으로 국가표준 KS X4600-1을 제정하였고 이 표준은 2009년에 ISO/IEC 12139-1로 채택되었다. KS X4600-1는 데이터 통신을 지원하는 24Mbps급 Class A와 초안상태인 Class B로 구성되는데 Class B는 멀티미디어 전송을 위한 200Mbps급 전송속도를 지원한다. ISO 표준의 주요 내용은 2~30MHz 주파수를 사용하여 변압기에 설치된 전력선통신 집중장치에서 수십에서 수백가정에 설치된 계량기의 검침데이터를 동시에 수집하고, 가구당 약 1Mbps 수준의 유효속도를 구현했다. 암호화에는 3-DES 또는 AES가 사용된다[9].

Ⅳ. 고속전력선통신적용 홈네트워크의 보안요구사항

지금까지의 고속전력통신기술은 하드웨어 및 네트워크 구성 중심의 속도향상에만 신경을 쓰고 개발되어 왔다고 말하여도 과언이 아니다. 그 예로 고속전력선통신 기술의 취약점 및 보안대책 마련에 관한 논문은 기술향상 논문에 비하면 모래사장에서 바늘 찾기와 마찬가지이다. 다른 통신기술의 경우는 보안의 중요성에 관한 예방, 적발, 교정에 관련한 많은 보안 기술들이 소개 되고 있는 반면, 전력선 통신은 거의 그러하지 못함이 사실이다. 개인의 사생활과 댁내 정보의 중요성을 생각해 보



〔그림 3〕 PLC Network Architecture

면, 고속전력선통신은 빠르고 신속한 통신 기술 발전 이전에 안전 통신 기술 발전에 힘써야 한다.

이러한 이유로 우리는 현재까지의 개발 동향으로 볼 때 어떠한 보안 기술들이 요구되고 있는지 살펴본다.

4.1 인증

고속전력통신 기반의 홈네트워크 인증은 기존 Ethernet 기술 기반의 인증방법과는 달리 인증 범위와 방식에서 다소의 차이를 가지고 있다. 홈네트워크의 특성상 프라이버시 정보에 대한 높은 보안수준이 요구되는 것은 물론, 높은 편리성이 동시에 요구된다. 또한, 기존에는 사용되지 않던 다양한 entry point가 사용됨으로써 그에 대한 보안요구사항 역시 다양화되는 경향이 존재한다. 모듈화된 기기간의 통합을 위한 기기간 인증 및 신뢰성에 대해서도 역시 고려가 필요하다. 따라서 기존의 인증방식을 그대로 적용하기에는 무리가 있으며, 홈네트워크의 특성을 고려한 인증방식을 필요로 한다

4.1.1. 사용자 인증

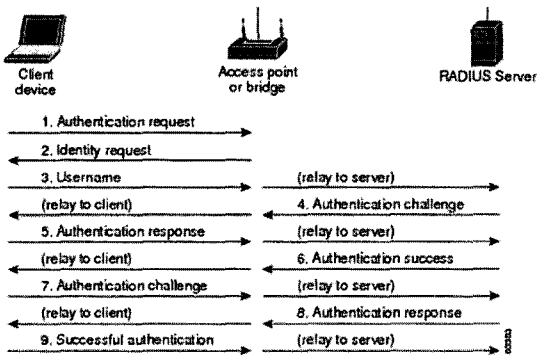
개인 사생활 보호에 대한 보안의식이 빠른 네트워크 구조와 기술의 발전으로 개인정보의 위협과 위험에 관한 사건 사고가 늘어남에 따라 더욱더 중요시 되고 있다. 자원 접근에 있어 우선적으로 식별되어야 할 사용자의 명확한 구분과 판단이 필요하며, 이 또한 앞으로 많은 기술적 보급과 발전이 예상되는 고속전력선통신 기술에 포함되고 짊어지고 가야 할 과제이다.

고속전력선통신에서 사용자 인증은 기존 인터넷 통신 네트워크 구조와 유사하게 이루어진다 사용자의 편리성에 맞게 인증절차를 간편화 할 것인지, 아니면 나날이 발전하는 고급 해킹기법에 대한 보안을 위해 편리성을 낮추고 사용자 인증 및 보안요구사항을 높일 것인지 고려해야 한다. 댁내에서의 접근과 댁외에서의 접근점 구분의 명확함이 필요하며 꼭 필요한 권한 부여방법과 절차 설계가 요구된다. AAA (Authentication, Authorization, Accounting) Server에 대한 인증, 혹은 특정 서비스 집단에 설치된 인증 서버를 통한 인증 등 여러 방법에 대해 인증 방법과 통합 절차를 연구 해 볼 필요성이 있다. 식별과 인증, 인가단계의 신뢰성의 손실은 이외의 모든 보안 요소의 견고함을 단 한 번에 무너트릴 수 있는 SPOF(Single Point of Failure)와 같은 지점이 될 것이다.

4.1.2 댁외에서의 디바이스 인증

전 세계적으로 불법 복제 소프트웨어로 골머리를 앓고 있는 지금, 모든 전자기기의 IP 주소 부여와 허용된 기기의 콘텐츠 접근 제한은 새로운 보안이슈이다. 불법 디바이스의 사용을 탐지해내지 못한다면 또 다른 많은 범죄와 사회적 손실을 만들어 낼 것이다. PLC 네트워크의 핵심적인 요소는 전력을 사용하는 기기 하나하나이다. 고속전력선 통신은 기존 인터넷 통신구조와 달리 전력을 이용한다는 면에서 더 많은 기기 접근 통제를 필요로 하며 더 많은 IP 주소를 필요로 한다. 통신 개체의 증가는 관리의 복잡함과 층화된 상세하고 명확한 구분을 필요로 하다. 현 디바이스 인증 기술은 홈 네트워크 환경 안에서 미들웨어 레벨에서 제공되고 있다. 예를 들면, UPnP(Universal Plug and Play)의 경우 디바이스마다 부여된 Security ID로 디바이스의 홈 네트워크 등록과정에서 디바이스 인증이 이루어지고 있으며, Havi(Home Audio Video Interoperability)의 경우에는 디바이스마다 고유한 인증서를 발행하여 디바이스 인증 수행 시 사용되고 있다.

하지만 이러한 절차는 미들웨어의 접근 가능함과 미들웨어 내의 데이터 등록 및 변경이 가능한 한 여러 보안 위협으로부터 안전하다고 말 할 수 없다. 이에 대한 미들웨어 보안 적합성 판단을 필요로 할 것이며, 한 단계 더 보안 된 디바이스 인증을 요구하게 된다. 결과적으로 사용자 인증에 사용되던 TTP(Trusted Third Party)에 대한 인증이나 PKI가 적용된 Device인증 방법 또한 디바이스 인증에 관련하여 고려해 보아야 한다.



〔그림 4〕 RADIUS를 이용한 디바이스 인증

4.1.3 댁내에서의 디바이스 인증

고속전력선통신기반의 홈 네트워크 구조는 사용자 및 디바이스 인증뿐만 아니라 장치 및 기기간의 상호의존성에 적합한 신뢰를 형성하고 보안이 유지 되어야 한다. 디바이스간 인증의 위협을 예로 들면, I/O 장치를 예로 들 수 있다. 키보드로 입력한 값은 특정 처리를 통해 모니터로 출력된다. 여기서 키보드의 입력 값을 공격자가 개입된 특정 하드웨어 모듈에 의해 일부 데이터를 전력선으로 형성된 은닉채널을 통해 지속적으로 유출시킨다고 가정한다면 이 또한 심각한 보안위협이 아닐 수 없다. 이에 대한 대책으로는 하드웨어 업체의 정기적인 감리 및 감사 절차를 예로들 수 있으며 이에 대한 대응방법 연구 또한 필수적인 요소라고 이야기 할 수 있다.

4.1.4 Access Control

사용자 인증, 디바이스 인증, 장치 간 인증에 관한 접근,통제에 대한 데이터가 실질적으로 생성되고 관리되어야 한다. 민감한 정보이기에 저장 위치 및 방법, 접근권한에 대한 통제가 명확해야 한다. 개인 사용자 및 기기 그룹별, 구성요소 등의 제어범위가 광범위하므로 여러 다른 각도에서 접근통제 기능이 필요하다. Access Control List 저장 위치와 효율, 그리고 안전성 측면 및 사용자 편리성 측면에서 일관된 보안정책 접근권한이 제어되어야 한다. 고속전력선통신의 ACL의 경우 다른 프로토콜들과는 달리 확정되어진 표준이 없어, 보안 기술의 적용에 있어서도 특정 알고리즘을 규정하기는 쉽지 않다.

4.2 플랫폼 대응

고속 전력선통신은 기존의 Ethernet이 주로 개인용 컴퓨터(PC)에만 적용되던 것과는 달리 다양한 플랫폼에 적용된다. 특히 홈네트워크에서 주로 사용되는 Embedded 기기들의 경우, 그 특성상 상용화 후에 기능을 수정하는 것은 매우 제한적이다. 예를 들어, 게이트웨이, 셋톱 등의 장비는 Embedded Linux 또는 Window CE 등을 주 OS로 사용하고 있으며, 방송 셋톱의 경우 ACAP(Advanced Common Application Platform)/OCAP(Open Cable Application Platform)이라는 브라우저에 대응되는 플랫폼을 사용한다. 따라서 고속전력선통신은 이런 다양한 플랫폼의 보안요구사항에 대해 초기부터 충분히 고려하여, 필요한 기능을 분석하고, 이를 구현할 필요가 있다.

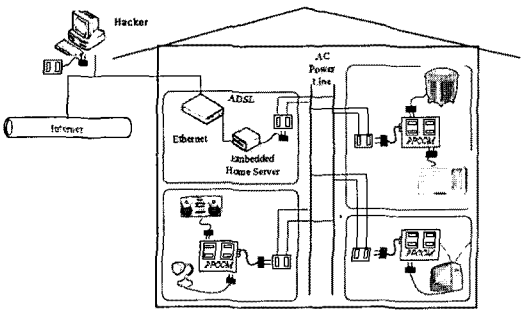
4.3 보안의 이원화

현재의 고속전력선 통신은 대부분 Ethernet 보안 프로토콜과 고속전력선 보안 프로토콜로 이원화 되는데, 이때 Ethernet과 고속전력선통신간을 연결해주는 역할을 하는 것이 PLC 어댑터이다. PLC 어댑터는 Ethernet의 암호화된 평문을 복호화 한 다음, 고속전력선 보안 프로토콜을 사용하여 다시 암호화 하여 메시지를 전송한다. 그런데 이런 이원화된 프로토콜은 무선 랜에서의 WAP-GAP과 같은 평문노출문제를 일으킬 공산이 크다. 이것은 현재 고속전력선통신이 댁내에서 주로 이용되고 댁외로는 확장되지 못해 발생된 한계이다. 결국 고속전력선통신이 댁외 단계까지 확장되는 아키텍처가 완성되어 네트워크가 일원화된다면 해결될 문제이지만 아직까지 실용화되기는 어려운 문제이다. 따라서 초기부터 이원화된 네트워크를 고려하여 이에 대한 대비책을 고려할 필요가 있다.

4.4 도청의 위협

기존의 Ethernet의 경우 도청의 문제를 광케이블이라는 매체를 사용함으로써 일정부분 해결하였다. 이에 반해 전력선 통신은 고속의 데이터전송을 상정하지 않은 일반 전력케이블을 매체로 사용함으로써, 발생되는 전자파가 그대로 노출되는 문제점이 있다. 이런 문제점은

그대로 도청으로 연결된다. 고속전력선통신은 네트워크에 대한 접근성을 높이지만, 동시에 도청의 위협 또한 다시 부각시킨 것이다.



〔그림 5〕 Hacker in PLC Based Home Network

앞으로 댁내의 가전기기는 고유한 IP를 가지며 이것을 이용한 접근이 가능해진다. 즉, 네트워크에 대한 entry point와 사용되는 정보의 양과 질이 급격히 늘어난다. 특히 홈네트워크의 경우 개인의 민감한 프라이버스 정보가 대량으로 이동된다. 이런 상황에서 매체적인 전자파차단이 전혀 없다는 것은 고속전력선통신의 크나큰 취약점이다.

데이터 암호화를 통한 전송 중의 취약점 보안도 필요로 하겠지만 동시에, 고속전력선통신 디바이스 개발사에 대한 독립적이고 투명한 감리 및 감사절차 또한 필수 요구사항으로 분석된다.

4.5 암호화

홈네트워크는 특성상 많은 가구가 하나의 네트워크에서 분기하여 서비스를 받는다. 또한 댁외 네트워크와 홈 네트워크가 물리적으로 보면 하나이며 구분되지 않기 때문에 댁외 네트워크와 홈 네트워크 간의 상호작용 속에서 데이터가 유출될 위험이 있다. 이 위험을 방지하는 방법으로 기본적이고 광범위하게 사용되는 것이 암호화이다. 사용자의 사생활 보호라는 측면에서 본다면 거의 모든 데이터는 암호화되어 처리되어야 한다. PLC에서 각 표준마다 암호화가 적용되었고 이는 아래의 표에서 일부분 확인할 수 있다.

〔표 1〕 표준별 암호화 프로토콜

표준	암호화
Homeplug	*DES or AES*
HD-PLC	AES
UPA	3-DES
KS X4600-1	3-DES or AES

V. 맺음말

본 논문에서는 고속전력선통신에 대한 대략적인 개요와 표준화 동향, 보안요구사항에 대해 살펴보았다. 고속전력선통신은 현재 홈네트워크 뿐만 아니라 방송, 자동차에 이르기까지 그 영역을 넓혀가고 있으며, 향후 우리 생활 곳곳에서 더욱 많이 사용될 것으로 예상된다.

고속전력선통신은 기존의 전력선이라는 인프라가 강력한 만큼 그 활용영역이 넓지만, 동시에 많은 문제점들이 존재한다. 특히 보안과 프라이버시 위협이 문제가 되고 있다.

그러나 아직까지 기술적, 제도적인 보안대책은 고속정보통신의 발전 속도에 비하면 미약한 수준이다. 따라서 향후에는 보다 현실적으로 고속전력통신의 취약점을 고려한 기술적인 대책과 이를 뒷받침할 만한 제도적인 보안대책들이 연구되고 논의될 필요가 있다.

참고문헌

[1] 이재조, "고속 전력선 통신 기술 및 산업동향", *HN FOCUS vol.15*, pp. 68-73, 2007.

[2] 장동원, 이영환, "전력선을 이용한 유비쿼터스 고속 데이터 통신 연구", 정보통신연구진흥원 주간기술동향 통권 1367호, Oct 2008.

[3] 도쿠다 마사미츠, "고속전력선 통신기술의 현황과 동향", *전기평론 2008*.

[4] http://www.homeplug.org.

[5] 임수빈, "고속 PLC 홈네트워크 솔루션", 한국통신학회지, 23(8), pp. 35~42, Aug 2006.

[6] *UPA DHS white paper v1.0, May 2006.*

[7] 박병석, 이영훈, 강철신, "NS-2를 이용한 전력선통신 KS-MAC 모델링 및 성능분석", 한국정보기술학회논문지, 6(5), pp. 81~87, Oct 2008.

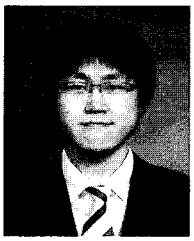
[8] *社団法人ロシア東歐貿易會, "新技術 PLCテクノロジー"*, ロシア技術ニュースレ, pp. 4~16, Jan 2006.

[9] 青山貞一, "ＰＬＣ受信障害フィールド實驗概要報告", pp. 1~6, Jul 2007.

[10] 홍기범, "국내 벤처기업 PLC 기술, 국제표준 채택", 전자신문, Oct 2009.

[11] Klaus Doster, "Propagation channel characterization and modeling outdoor power supply grids as communication channels", ISPLC2005, Apr 2005.

〈著者紹介〉

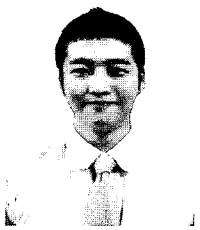


이 정 열 (Lee Jung Youl)
학생회원

2008년 2월: 동국대학교 정보통신공학과 졸업
2009년 3월~현재: 동국대학교 홈네트워크보안전공 석사과정
<관심분야> 정보통신공학, 홈네트워크보안

윤 진 희 (Yoon JIn Hee)
학생회원

2009년 2월: 동국대학교 컴퓨터공학과 졸업
2009년 3월~현재: 동국대학교 홈네트워크보안전공 석사과정
<관심분야> 통신공학, 정보보호



전 해 성 (Jeon Hae Sung)
학생회원

2009년 2월: 서울호서전문학교 사이버해킹보안과 졸업
2009년 3월~현재: 동국대학교 홈네트워크보안전공 석사과정
<관심분야> 포렌식, 정보보호

김 학 범 (Kim Hak Beom)
종신회원

1990년 8월: 중앙대학교 대학원 컴퓨터공학과 졸업(석사)
2001년 2월: 아주대학교 대학원 컴퓨터공학과 졸업(박사)
1991년 10월~1996년 6월: 한국전산원 주임연구원
1996년 7월~2001년 8월: 한국정보보호진흥원 기술표준팀장
2001년 9월~2003년 1월: (주)드림시큐리티 상무이사
2003년 2월~2005년 3월: (주)장미디어인터렉티브 상무이사
2005년 4월~2008년 3월: 정보보호연구소 부소장
2008년 4월~2009년 6월: SK인포섹(주) 수석컨설턴트
2009년 7월~현재: 에스지어드밴텍(주) 기술이사/본부장
2001년 3월~2009년 2월: 순천향대학교 공과대학 정보보호학과 겸임교수
2005년 9월~현재: 동국대학교 국제정보대학원 겸임교수
2007년 9월~현재: 아주대학교 정보통신대학원 겸임교수
2009년 8월~현재: CISSP 국제 공인 강사
<관심분야> CC 평가, 유비쿼터스 보안, 공개키기반구조(PKI)