# Security Issues of Power Line Multi-Home Networks for Seamless Data Transmission

Sunguk Lee

*Research Institute of Industrial Science and Technology*
*Pohang, Gyeongbuk, South Korea*
*Sunguk@rist.re.kr*

***Abstract***

*This paper provides discussion of security issues for power line networks (PLC). The home network based on power line communication has been used widely however security of PLC has not been discussed sufficiently. Though PLC uses power line as medium it has similar characterises with wireless communications in the view of security. The authentication and cryptographic scheme used in PLC standard are discussed. Also the usage of Intrusion Detection system (IDS) for PLC is discussed.*

***Keywords:*** *Security, Authentication, Intrusion Detection, Power line communication*

## 1. Introduction

Power line communication (PLC) uses existing power line as medium to transmit and receive data. Early PLC technology such as X-10 [1] was utilized for the sake of control and command of electric appliance in the industrial field with very low data rate. In recent years there has been great interest in PLC as one of candidate technologies for data communication and multimedia distribution in home or small office environment.

Several groups have released industrial standard for high speed power line commutation. Home Plug Powerline alliance [2] was established at 2000 and release Homeplug 1.0 standard whish provide 14Mbps raw data rate for data communication. HomePlug AV [3] standard which is most recent standard for supporting multimedia application provides 200Mbps raw data rate. The Universal Power Line Association (UPS) [4] released the Digital Home Specification (DHS) with chip-sets design by DS2. The High Definition power line communication (HD-PLC)[5] was proposed by Panasonic. The DHS and HD-PLC both support 200Mbps raw data rate.

The most interesting thing of power line communication is usage of existing power grid for communications. So user can communicate with just plugging in the PLC modem at numerous power outlets in house or office without any additional work for installation of cable. Though power line communication uses wire for communication it has similar characteristics with wireless communication such as wireless LAN and Bluetooth in the viewpoint of security.

The power line broadcasts the signal like as radio signal so this signal can reach other houses or offices unless power grid is isolated. This can cause significant security problems of power line communication. Therefore many apartments and buildings for offices share power line, security problem should be considered to use power line communication for home and office environment. Even though security is one of concerns of power line communications security issues are discussed at only few papers [6, 7, 8].

This paper is organized as follows: In Section 2 a brief description of security for home network is given. Section 3 describes the overview of power line communication. Section 4 describes security issues of power line communication. Conclusions are given in Section 5.

## 2. Security of Home Network

For safe communication several services for security such as authentication, confidentiality, integrity and access control should be provided. The authentication is service to identify the nodes which try to communicate with members of network. The confidentiality is to guarantee the privacy of data which is delivered. And integrity is to ensure the data is not modified by others.

Because Ethernet uses dedicated wire likes fiber optic cable an eavesdropper must be at the path between transmitter and receiver to eavesdrop data. However in wireless link and power line eavesdropper can try to get the data not only at the middle of path between sender and receiver but also at multiple points. Therefore wireless and power line communication is more vulnerable to eavesdropping. Furthermore security management should be performed as distributed manner in the case of ad hoc mode of wireless and power line communications because of lack of an underlying infrastructure.

Typically the security attack for network can be classified as passive and active attack. A passive attack means that malicious stations access the network and obtain the information transmitted in the network without disrupting the communications of stations in the network. Eavesdropping is an example of passive attack. The active attack is that an unauthorized node attempt to change, delete, inject the data in the network. Denial of service is one of active attack. The passive attack is more difficult to detect because passive attack does not affect operation of network. Encryption and authentication mechanisms are widely used against these attacks.

There are two protocols for authentication in IEEE 802.11 specification [9]. One is Open system authentication and the other is shared key authentication. The default authentication protocol of IEEE 802.11specification is Open system authentication. Using open system authentication everyone can get the authentication without verification process. Therefore this protocol is highly vulnerable to attack. Shared key authentication protocol uses a cryptographic mechanism for authentication. The supplicant uses cryptographic key which is shared with AP to encrypt message for request authentication. The WEP cryptographic technique is used for encryption however WEP is used rarely now because of its vulnerability. Wi-Fi Protected Access (WPA) is a security protocol developed by Wi-Fi alliance. WPA employs IEEE802.1x specification with an Extensible Authentication Protocol (EAP). Figure 1 shows an example of authentication process of IEEE 802.1x standard with EAP and RADIUS protocols.

The authenticator which is the access point in figure 1 communicates with authentication server with Remote Authentication Dial-In User Service (RADIUS) protocol. This is for supporting centralized authentication, authorization and Accounting (AAA) management.

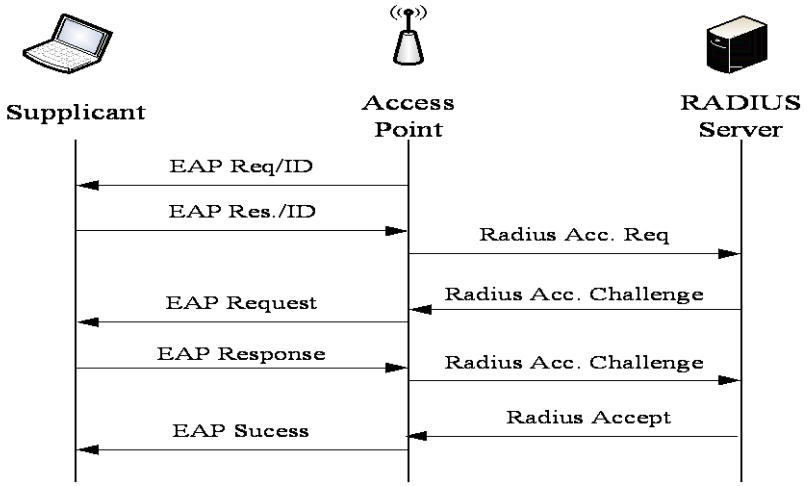


**Figure 1. Authentication Process of IEEE 802.1x Standard with EAP and RADIUS**

The Power line communication adopted almost similar security schemes with wireless LAN technology. PLC uses cryptographic mechanism like DES and AES. Table 1 shows the cryptographic protocol used at PLC standards. Simple connection mode and secure mode for authentication are supported at Homeplug AV. Also authentication standard such as 802.1x and EAP can be used in PLC with Homeplug AV specification. Because PLC does not have physical boundary like wireless communication PLC standard should provide management scheme of several virtual networks. The virtual network is based on relation of trust among members. The trustworthiness of members in the same virtual network make it possible to exchange keys securely, then authentication with shared key, confidentiality and integrity can be achieved by the networks. The virtual network can protect itself from eavesdropping by encryption.

**Table 1. Cryptographic Protocols of PLC Standards**

| Standard | Chipset Maker | Cryptographic protocol |
|---|---|---|
| Home Plug 1.0 | Intellon | DES |
| Home Plug AV | Intellon | 128 bits AES CBC |
| UPA-DHS | DS-2 | DES |
| HD-PLC | Panasonic | AES |

## 3. Overview of Power line Communication

The first PLC standard released by Homeplug Alliance is Homeplug 1.0 specification [10] which uses 4-28 MHz frequency band at the Physical layer. This specification provides 14Mbps raw data rate for data communication. The CSMA/CA scheme like IEEE802.11 was

adopted for medium access control (MAC). The Homeplug 1.0 specification supports just distributed scheme for access control like DCF in IEEE 802.11.

Homeplug AV specification has up to 200Mbps data rate for supporting audio and video signals. The Homeplug AV uses OFDM with 2-30 MHz of frequency band in physical layer. The MAC scheme of Homeplug AV speciation is a hybrid of TDMA and CSMA which is same MAC scheme of Homeplug1.0. The Homeplug AV supports several virtual networks which is called AV Logical Networks (AVLNs) and provides centralized scheme to manage the logical network. Each AVLN has a CCo (central coordinator) to manage the access control. The CCo broadcasts beacon signal which has the information for allocation period of TDMA and CSMA region. Figure 2 shows allocation of TDMA and CSMA at beacon period. The CSMA scheme is same with that of Home 1.0 specification.

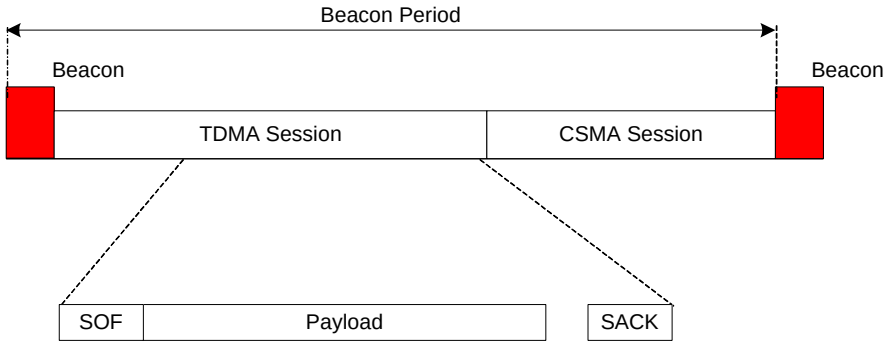


**Figure 2. Hybrid MAC Scheme of Homeplug AV**

The Digital Home Specification (DHS) [11] has been proposed by Universal Powerline Association (UPA). The UPA DHS operated in the frequency band of 2-30MHz and uses OFDM modulation in the physical layer. The MAC scheme of UPA specification [14] is a centralized MAC scheme based on TDMA which is called an Advanced Dynamic Time Division Multiplexing (ADTDM) Scheme.

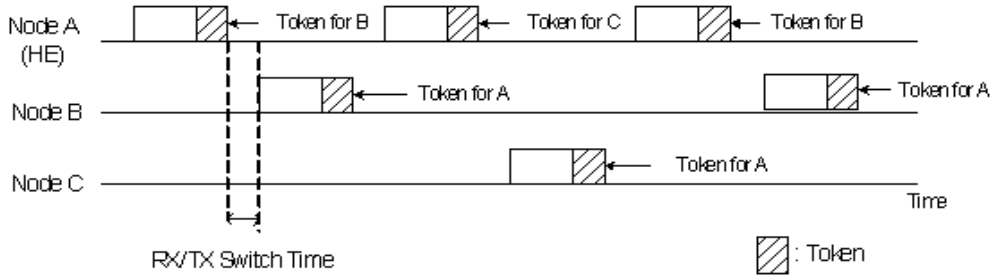


**Figure 3. Example of Transmission Procedure in UPA PLC Network**

The MAC scheme of UPA specification uses a master/slave system like the Bluetooth. The network is composed of a Head End (HE) and a Customer Premise Equipment (CPE). A repeater can be used if the signal from the HE does not reach all CPE in the network. Only one HE can be existed and control all channel access of all member in the same network. The information of channel access is distributed by token packet to

the all CPEs. Figure 3 shows an example of transmission sequence of network which has a HE and 2 CPEs. Node "A" which is the HE gives a right to access the channel to members in order by token.

The several specifications by different alliances such as Homeplug and UPA cannot support interoperability. Therefore international standard for PLC has been required. The IEEE1901 and ITU-T G specification provide MAC and physical layer specification. Both specifications utilize TDMA based contention free access and CSMA/CA based contention based access scheme in MAC layer.

## 4. Discussion of Security for PLC

Because power line communication has no physical boundary and power line can be shared by several users through power outlet PLC can be vulnerable to both internal and external attack. The most widely used schemes to prevent these attacks are based on cryptography and certification.

The admission access control of Homeplug specification uses a Network Membership Key (NMK) [7]. The admission access control is for allowing only permitted user to join the AVLN. In homeplug 1.0 specification all stations have the same default NMK and use it for providing plug and play service. Therefore it is very vulnerable to external attacks by malicious user.

The Homeplug AV [6,7] specification uses the NMK for admission access control of the AVLN. The several methods for distributing the NMK are proposed considering with convenience of usage and security. With successful authentication with correct NMK the station requests the Network Encryption Keys (NEKs) and receives it from the CCo. The NEK is used for cryptographic process for exchange the data securely with other stations in the same AVLN. The NEK is updated periodically and sent to all members in the AVLN by the CCo. The 128 bits AES CBC is used for encryption in Homeplug AV specification. The Device Access Keys (DAKs) which is unique for each PLC modem is also used for secure distribution of NMK.

The IEEE1901 standard [12] does not have any special admission access control scheme. The IEEE1901 adopts security scheme of the IEEE802.1x specification. The authentication process and CCMP (Cipher block chaining Message authentication code Protocol) mechanism are provided for security. The ITU-T G.hn [12] uses authentication scheme based on the Diffi-Hellman algorithm and CCM with 128 bits AES encryption standard. The pair-wise security is defined to protect from internal attack.

As mentioned above PLC specification uses authentication based on virtual network to prevent external attack such as eavesdropping and cryptography to keep confidential and privacy of the virtual network. However these security schemes can not eliminate vulnerability perfectly in the view of security. Authentication and cryptograph cannot protect vulnerability from malicious station which has already private keys. The virtual network is formed based on trust between stations but no one can confirm that every node is trustworthy.

Therefore, in my opinion, the intrusion detection [13] should be implemented to protect private information such as back account number, password in PLC based home network. The Intrusion Detection System (IDS) monitors network by collecting and analyzing of audit data to detect activities which is against the security. In the Ethernet, traffic monitoring function is implemented in switch, router and gateways normally. However power line communication does not have a fixed infrastructure like as wireless ad hoc network.

In PLC standards virtual network is managed by controller such as CCo in Homeplug AV and HE in UPA specification. The traffic in PLC does not go through the controller of virtual

network but the controller can listen these data. Therefore Network base IDS can be implemented at controller. But we have to keep in mind that every PLC station can be controller. So every station has to get IDS for supporting intrusion detection in the network. It means PLC network can have both network based and host based IDS. So we can design IDS for PLC flexibly. For example we can use a fixed controller of virtual network then this network has network based IDS which is just implemented at the controller with full visibility of network.

## 5. Conclusion

As the interest in power line communication becomes higher security scheme of PLC has been more important. This paper presents a brief overview of Power line communication standards and security issues of PLC. Similar with wireless network PLC supports authentication procedure and cryptograph for security of network. However these security schemes can not eliminate the vulnerability perfectly. Therefore usage of intrusion detection in PLC is discussed. More security standards for PLC should be researched in the future because the security scheme of PLC is not sufficient to protect critical private information.

## References

[1] http://www.x10.com/support/technology.
[2] Homeplug Alliance, http://www.homeplug.org.
[3] HomePlug AV White Paper, http://www.homeplug.org.
[4] Universal Power line Association, http://www.upaplc.org.
[5] HD-PLC whitepaper, http://www.hd-plc.org.
[6] R. Newman, S. Gavette, L. Yonge and R. Anderson, "Protecting Domestic Power –line Communication", ACM, Symposium on usable privacy and security, **(2006)** July, pp. 122-132.
[7] R. Newman, L. Yonge, S. Gavette and R. Anderson, "HomePlug AV Security Mechanisms", IEEE International Symposium on Powerline communications and its Applications, **(2007)** March, pp. 366-371.
[8] R. Nishi, H. Morioka and K. Sakurai, "Trends and Issues for Security of Home-Network Based on Power Line Communication", IEEE, International Conference on Advanced Information Networking and Applications, vol. 2, **(2005)** March, pp. 655-660.
[9] T. Karygiannis and L. Owens, "Wireless Network Security, 802.11 Bluetooth and Handheld Devices", National Institute of standards and technology, special publication 800-48.
[10] M. K. Lee, R. Newman, H. A. Latchman, S. Katar and L. Yonge, "HomePlug 1.0 Powerline Communication LANs –Protocol Description and Comparative Performance Results", International Journal on Communication Systems, vol. 6, Issue 5, **(2003)** April, pp. 447.
[11] "Digital Home specification white paper", Universal Power Line Association, **(2006)** May.
[12] Md. Mustafizur, C. S. Hong, S. Lee, J. Lee, Md. A. Razzaque and J. H. Kim, "Medium Access Control for Power Line Comunications:An Overview of the IEEE 1901 and ITU-T G.hn Standard", IEEE Communication Magazine, **(2011)** June, pp. 183-191.
[13] B. Mukherjee, L. T. Heberlein and N. N. Levitt, "Network Intrusion Detection", IEEE Network, **(1994)** May.
[14] Opera Specification Part *I*, http://www.upaplc.org.