

Securing Powerline Communications

Vamsi Paruchuri

Department of Computer Science
University of Central Arkansas
Conway AR USA
vparuchuri@uca.edu

Ramesh Madakasira

Unified Gateways
Bangalore, India
ramesh.m@unifiedgateways.com

Arjan Durresi

Department of Computer Science
Indiana University-Purdue University Indianapolis
Indianapolis, IN 46202 USA
durresi@cs.iupui.edu

Uday Bhaskar Rao Abburi

Ordyn Technologies
Bangalore, India
uday.b@ordyn.com

Abstract— Powerline Communications represents an exceptionally promising alternative for high-speed Internet access and data networking. Its strength and popularity can be attributed to its ubiquitous nature and readily available infrastructure. Multiple applications are envisioned and powerlines have become increasing popular choice for creating residential networks. This communication medium has been well studied and standardization of the technologies are undergoing. However, the security aspects of PLC networks are not well studied and there is an urgent need for that. In this paper, we put forth several security requirements needed of PLC networks and justify them through multiple scenarios. We then propose a Security Architecture to realize these requirements.

Keywords—Security, Architecture, Powerline Communications

I. INTRODUCTION

Power line communications (PLC) have received tremendous attention in recent years as an alternative and cost-effective last-mile-access technology [1, 4]. Its strength and popularity can be attributed to its ubiquitous nature and readily available infrastructure. Power outlets are available very widely at every home can act as channels for broadband provisioning and thus increasing its popularity. Moreover, unlike other popular communication technologies, its bandwidth is fully symmetrical, in terms of up-link and down-link bandwidth.

New modulation techniques and technology have enabled this medium to become a realistic and practical means of communication. Several technologies have been developed that make use of power lines for broadband home networking applications. Recently, DS2, a company specializing in PLC devices, successfully developed PLC chips that can support a transmission speed of 400 Mb/s [2], which can be used to support a variety of multimedia applications. This continually growing bit rate that could be supported by PLC is further contributing to its popularity.

One of the biggest applications envisioned is PLC access network and PLC in home network: providing a local home network with the advantages of the power line, and combining access and in-home network capabilities for service and system integration. There are several applications for a PLC network in

the home: shared Internet, printers; files, home control, games, distributed video, remote monitoring security. The key asset is “no new wires.” Available products are in net-connected security, safety, and convenience service systems using narrowband communications.

The PLC networks must attach importance to guarantee several security requirements to realize the multiple envisioned scenarios. PLC networks are inherently broadcast in nature, making security aspects more critical. However, not enough attention has been given to this area.

In this paper, we first present some security requirements from various user scenarios. On major requirement from user perspective is minimal user intervention. We assume a network model constituting both PLC access network and PLC in-home network. We then present a layered security architecture, in which several different key layers are implemented. If the system is compromised or keys are outdated at one layer, for the update a key from a higher security layer is used to generate/transmit the new key.

The rest of the paper is organized as follows: Section II presents the PLC standardization efforts and related works. In Section III, we present the underlying network model and some use case scenarios using this model. Section IV details the security requirements that need to be guaranteed irrespective of the scenario. The multi-layered security architecture is introduced in Section V and we conclude in Section VI.

II. RELATED WORK

The usage of the power grid for control, maintenance, and charging purposes by the utility commodities has a long history [3]. The liberalization of telecommunications and the deregulation of electricity utilities have added new dimensions to the potential application of the electricity infrastructure for the most efficient use of the local loop.

Standardization efforts on PLC networks are in progress and have reached final stages. IEEE P1675 [6] deals with the standards for installing the BPL devices on underground (concealed) and overhead (open) power distribution lines. It

also deals with the required safety measures for these BPL devices so that the general public are not placed in danger. IEEE P1901 [7], “Standard for Broadband over Power Line Networks: Medium Access Control and Physical Layer Specifications”, will contain the specifications for sending high-speed (>100 Mbps at the physical layer) digital data between BPL devices. This standard uses transmission frequencies below 100MHz and is applicable for the BPL devices present in the first-mile and last-mile. IEEE1775 [8] standard is composed of the electromagnetic compatibility (EMC) criteria, and consensus test and measurements procedure for BPL devices.

Open PLC European Research Alliance (OPERA) [9] is a European, multi-organization R&D project which aims to standardize PLC systems and to develop business plans and procedures for network maintenance as well as service provisioning, along with market research to understand the requirements of end users. The Universal Powerline Association (UPA) [10] has attracted membership from PLC companies, utilities, electronic equipment manufacturers, and chipset providers to catalyze the growth of PLC technology by delivering UPA certified products that comply with agreed specifications.

HomePlug AV:

HomePlug Audio/Video (HPAV) specification [17] addresses high-speed powerline communication for multimedia traffics, which supports up to 200Mbps in order to transmit multiple HDTV streams. HomePlug AV uses cryptographic isolation to create virtual private LANs, called AV Logical Networks (AVLNs) [16]. When a logical network is formed, a Network Membership Key (NMK) is distributed to all its stations. Possession of the NMK defines the stations in the network, whose name is the security level and a hash of the NMK. The controller distributes a periodically changing Network Encryption Key (NEK) to each station, encrypted using the NMK. The NEK in turn encrypts data payloads. The encryption used is 128-bit AES CBC. Transmissions between networks are not encrypted with the NEK.

The NMK may be provided to a device in one of three ways: it may be provided by the host directly; it may be passed to a device using the Device Access Key (DAK); it may be passed using the less secure Unicast Key Exchange (UKE) protocol, in the clear.

While the first method is secure, it requires user intervention. For second method, the NMK providing device has to securely know the DAK of the new device. Finally, the third method relies on the assumption that it is hard to decode the message transmissions on the powerlines. However, this argument is very questionable and one might even argue that if the powerlines are secure enough to transmit cryptographic keys in the clear, they should be secure enough to transmit data without any encryption at all.

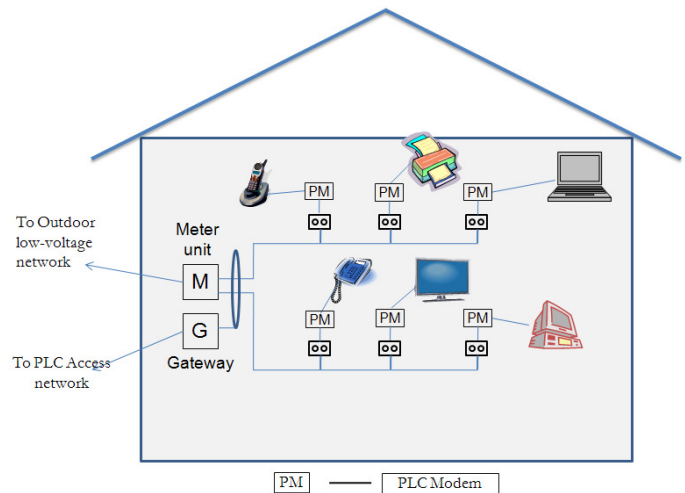


Figure 1. Structure of a PLC Indoor Network

Further, NMK is provided to all devices that connect to the network. Thus, emphasis has to be placed on not permitting *attack* nodes to connect to the network or connected nodes not to *leak* the NMK to *attack* nodes.

Other works:

Security issues related to PLC have been previously studied in [14, 15]. In particular, [14] studies a B2B scenario on information trading, and a process model supporting security. In the more recent work [15], the authors discuss the differences on the security between PLC and wired/wireless LANs. The authors state that it is possible that one can eavesdrop either using the inherent leaked signals or by simply peeling off the matting (wire tapping). The authors conclude that, specific measures are essential to secure PLC; however, they do not propose any specific solutions.

The security issues of a home automation system based on PLC are studied in [11]. Apart from analyzing the security threats, the authors also present some security protocols to address these threats. A security architecture, specific to REMPLI (Real-time Energy Management via Powerlines and Internet), is proposed in [13]. The problem of being sure if a device enrolling in the PLC network is the device the user thinks, is dealt in [5].

In this paper, unlike most of the previous works, which mostly address security issues for an in-home network, we consider both PLC Access Networks and In-home networks together.

III. BACKGROUND

A. Network Model

We assume a network model that consists of primarily two communication systems:

- In-home networks
- Access networks

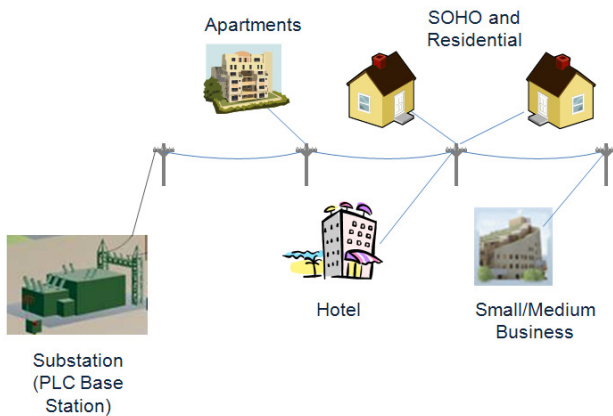


Figure 2. Structure of a PLC Access Network

In-home PLC Networks

An in-home network is a network owned and operated by the end user who uses internal house wiring to provide communication between outlets (Figure 1). The user can employ home networking devices, such as Ethernet-to-PLC or USB-to-PLC bridges, for connecting several computers, sharing printers, asynchronous digital subscriber line (ADSL), or cable modem connections. Feasible applications in the near future also include high-definition TV (HDTV) distribution systems, video surveillance systems, and hi-fi equipment.

The Gateway, which could be placed with the meter unit, connects the in-home PLC network to the PCL Access Network. All devices access the in-home PLC network through PLC Modems (PMs) which are directly plugged to the power outlets.

Access Networks

A PLC access network provides local loop access to homes and businesses using the electricity distribution grid. Access networks typically constitute of a PLC modem installed at the Transformers (substations) and provide connectivity to all premises in the neighborhood (Figure 2). From here forth we refer to these devices as Base Stations (BSes). PLC Access networks represent a low-cost highspeed alternative to traditional technologies employed for providing access, such as the public switched telephone network (PSTN), integrated services digital network (ISDN), ADSL, or hybrid fiber coax (HFC).

B. PLC Applications and Scenarios

PLC networks are targeted mostly at individual-home users. In an ideal scenario involving an isolated individual house, there might be a single user using the PLC network, with no interference with any neighbouring PLC networks. In such scenarios, eavesdropping could be very hard [1, 2]. In fact one can argue that no security measures are needed.

However, we envision several scenarios where a PLC network is not physically isolated. Several users might be using the network or worse, it is not hard to perform tapping/eavesdropping; hence, security aspects become critical. Some such scenarios are:

- An apartment complex, with residents of neighbouring apartments having their own PLC networks.
- A house shared by several residents, each desiring to have his own individual PLC (at least logical/virtual networks)
- A home office with frequent clients being to be able to have access to the Internet via the PLC at the home.
- A Small Business Office, with the Employer sharing the network with his employers.
- A Hotel providing Internet access to its guests using PLC network.

Each of the above scenarios demands several/varying security requirements.

IV. SECURITY GOALS

In PLC networks, eavesdropping cannot be prevented and further, the data transmissions are broadcast in nature. The goal is to make PLC networks as secure as wired LANs and can be summarized as follows:

- Confidentiality: The confidentiality of the data transmissions has to be assured. Even if an outsider is able to eavesdrop, the secrecy has to be preserved. Further, if it is similar to a hotel environment, where multiple users might be connected, each user has to be guaranteed privacy.
- Authentication: The identity of the access devices (like PLC modems) has to be verified and authenticated before they are added to the network.
- Integrity: The integrity of the messages has to be preserved. It has to be ensured that the messages are neither damaged nor deliberately changed, nor tampered with.
- User Intervention: All security processing defined within the specification must be handled without higher layer intervention. It would also be highly desired to keep the user intervention to the bare minimum.

V. PROPOSED SECURE ARCHITECTURE

In this section, we describe our proposed architecture to realize the security goals presented in the previous section. We refer to figure 3 for our description. We propose a multi-layer security architecture with three different key layers. A key from a higher layer is used to update/assign keys at a lower layer.

All the entities in each layer (i.e., PLC modems, Gateways and Base Stations) support both Asymmetric (e.g., RSA) and Symmetric key cryptography (e.g., 3DES). While most of the vendors currently ensure their products support some symmetric key encryption (e.g., 3DES, AES), we propose that the

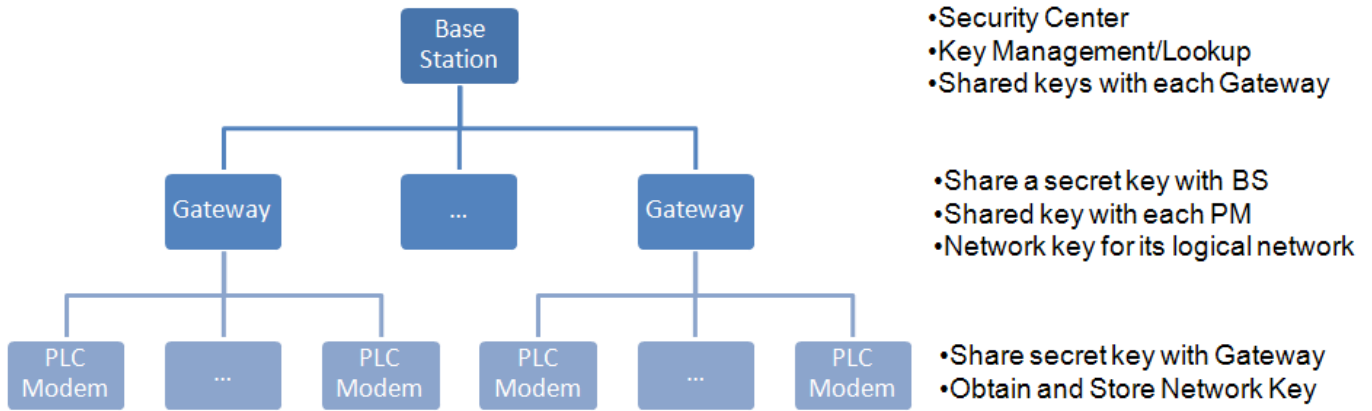


Figure 3. Proposed Layered Security Architecture

manufacturing vendors assign unique public/private key pair to each of these devices along with a certificate for validating these keys.

A. Hierarchy

Layer 1 includes the Base Stations (BSes). BSes authenticate the devices at lower layers and manage the keys. The responsibilities include the following:

- When a Gateway or a PLC Modem is added to the network, the certificate is passed on the corresponding BS of the network. The BS would verify the authenticity of the device and gives access to the device. The database at the BS is also updated. Thus, for verification the BS either needs to store the public keys of major vendors or might in turn have to request the Public Key Infrastructure (PKI) through the WAN it is connected to.
- BS would generate and securely communicate a shared key for each Gateway in its network. For secure communication, the BS uses the public key (GK^+) of the Gateway to encrypt the shared key (GK_s). The message format would be

$$E_{BK^-}(N, E_{GK^+}(GK_s, t))$$

where, N is a random nonce and t is the expiration time for the shared key. BK^- is the private key of the BS. The Gateway would then use the public key of the BS (BK^+) to verify the authenticity of the message and then its private key GK^- to retrieve the shared key.

- The shared key is periodically updated to limit the damage in case any device is compromised. However, considering that the Gateways might be hard to be compromised, the interval between two updates could be in weeks. Key updating is discussed later in this Section.
- In scenarios where an user wants to connect a *non-standard* PM to the PLC network or in scenarios where the public key of a PM are lost/expired/unverifiable but the user still trusts the PM and desires to connect the PM, the BS can generate a public/private key pair for the PM and send it to the PM/user.

Layer 2 consists of the Gateways of all the indoor networks. The functionality of these devices includes the following:

- Whenever a new PLC Modem is detected, the modem's credentials are obtained and passed on to the BS. Once BS responds positively, the PM is granted network access and added to the network. Since new PMs would be added infrequently, we consider that this would not impose any significant overhead on the BS.
- A Gateway stores the credentials of all PMs connected to its network. The Gateway also *remembers* the credentials of the PMs that were verified in the *recent past*. This *remembrance* is crucial to maintain the scalability. For instance, if the network is recovering from a power outage, without this remembrance, the BS would be overwhelmed by verification requests. Further, this would also permit mobility of the PMs – a user can plug in the same PM to power outlets in different rooms without having the Gateway requesting the BS to verify the same PM whenever it is reconnected.
- A Gateway generates and communicates a Network Key to all the PMs in its network. The PMs and the Gateway use

for broadcast communication. We note that this key is not used for any unicast communication; even for those between two local nodes.

- A Gateway also generates a unique shared key with each of its PMs and securely communicates them to each of the PMs using their public keys as discussed earlier in this section.

Finally, Layer 3 consists of the PLC Modems. The first time a PM is connected onto a PLC network, it broadcasts its credentials on the network in plaintext, without any encryption. Once the network Gateway listens to PM's beacon, it acknowledges the PM. The PM then waits for the Gateway to verify its credentials (with help of BS) and send a shared key using the PM's public key. The PM then uses the shared key for further communication.

B. Communication

All the communication is encrypted. We categorize communications as local and non-local.

For all non-local communication, a PM simply encrypts the messages with the shared key it shares with the Gateway. The Gateway would then decrypt the message and then again encrypt it with the secret key it shares with the BS and transmits on the PLC.

Local communication is between two nodes that are under the same Gateway, e.g., communication between a laptop and a printer. When node A, connected to the PLC network through PM_A , intends to communicate with a local node B (connected through PM_B), PM_A requests its Gateway for key establishment with PM corresponding to device B. The Gateway generates a shared key and securely communicates the same to both the PMs. The PMs would then start the communication process using the shared secret key.

Here, we would like to emphasize that it is critical that a PM does not use the network key for transmitting messages (unless they are intended to the entire network); but, instead a PM should use a secret key shared with the Gateway or the local device. In a house, where there is only one user using PLC to connect multiple devices to multiple services, this issue might not be significant. However, in a hotel/small office scenario, where there might be multiple users connected to the same PLC logical network, this is critical. If not, since every device has access to the Network Key of the logical LAN and because PLC is broadcast in nature, any device that can eavesdrop, can be able to decode all the messages being transmitted over the powerlines, thus violating the security objectives.

C. Updating Keys

We advocate periodically updating all shared keys for two reasons. First, it reduces the damage if any device has been compromised. Second and more important reason, is to ensure security even in networks where multiple users (possibly

strangers or worse, with conflicting interests) might be sharing the network. Further, in hotel like scenarios, the users might be connected only for short durations and might bring their own PLC Modems. If the keys are not updated periodically, and if a user can eavesdrop, then by connecting/registering once to a network, he obtains access virtually for unlimited duration.

However, since, all unicast messages are encrypted with shared secret keys, the damage that can be caused by such *illegitimate user* very limited. However, he might be able to use the network resources. For instance, he might access the printer and print whenever he needs to, though he is not authorized. Periodic updates would minimize such unauthorized access.

We note that the frequency of updates depends on the scenario – a single user at a home might not need to update the keys very often, while in hotel like environments, the updates have to be very frequent. However, we also note that since topology changes at layer 2 and layer 1 are very infrequent, so could be the key updates. Since, the network membership at layer 3 might be very dynamic, the updates needs to often. We believe that updating the keys at layer 3 and between PMs and Gateways every few hours provides reasonable security.

Two commonly used key update mechanisms are outlined in [18]. Let MK be a master key, H a derivation function (i.e. hash function), i an integer (initialization vector) and DK the derived key.

- Parallel: $DK_i = H(MK, i)$

- Serial: $DK = H(k-1, i)$ and $k_{n-1} = H(k_{n-1}, i+1)$ and $k_0 = MK$.

In general the serial method produces a key chain; for example the new key DK_5 is derived from DK_4 . Further, to directly derive DK_5 from MK, we need to apply the same hash function five times. However, in networks with high delays, serial method. Since, the delay in PLC networks is not considered to be significant, we propose to use the parallel method.

D. The end devices

Once a PM obtains access to the network and establishes shared key with the Gateway, the user can connect and securely communicate over the PLC network. The issue of verifying and trusting an end user device is not trivial and is out of scope for this paper.

Trusting and authenticating end devices has been addressed in literature [5]. However, here, we slightly deviate from the traditional approaches and propose that the network user needs to handle this, as in wired LANs. For instance, if one has an access to a Ethernet port, unless the network requires user authentication or a password, one can connect to the network. But, if the end device does not have appropriate interface (e.g., printer), the user has to manually set up the device to connect it.

VI. CONCLUSIONS

PLC is a promising candidate for the realization of cost effective solutions for “last mile” communications. After the deregulation of the telecommunications market, there is a strong interest in PLC from new Network Provider. However, the security aspects of PLC have not been well explored. In this paper, we outlined some security requirements based on several envisioned use-case scenarios. We also present multi-layered security architecture to meet the necessary security goals for PLC.

REFERENCES

- [1] International Symposium on Power Line Communications (ISPLC), <http://www.ieee-isplc.org/>
- [2] DS2 Press Releases: DS2 Introduces 400Mbps Powerline Communications Technology. www.ds2.es/press/record.aspx?id=95
- [3] Han Vinck and G. Lindell. "Summary of Contributions at the International Symposium on Power Line Communications and Its Applications." *ISPLC*, 2001.
- [4] Halid Hrasnica, Abdelfatteh Haidine, Ralf Lehnert, "Broadband Powerline Communications: Network Design", Wiley Publications, August 2004, ISBN: 978-0-470-85741-0.
- [5] Newman, R., Gavette, S., Yonge, L., and Anderson, R. "Protecting domestic power-line communications", in *Proceedings of the Second Symposium on Usable Privacy and Security (SOUPS)*, July, 2006).
- [6] IEEE. Standard for broadband over power line hardware. IEEE P1675. <http://grouper.ieee.org/groups/bop/>
- [7] IEEE. Draft standard for broadband over power line networks: medium access control and physical layer specifications. IEEE P1901. <http://grouper.ieee.org/groups/1901>.
- [8] IEEE. Standard for powerline communication equipment: electromagnetic compatibility (EMC) requirements: testing and measurement methods. IEEE P1775. <http://grouper.ieee.org/groups/bpl/> [3 October 2006].
- [9] OPERA (Open PLC European Research Alliance). <http://www.ist-opera.org/> [3 October 2006].
- [10] UPA (Universal Powerline Association). <http://www.upapl.org> [3 October 2006].
- [11] Zhong, Y. P. Huang, P. W. Wang, B. Liao, J R. Nicole, "An Efficient Security Scheme and Its Application in Intelligent Home System Based on Power-Line," in *IEEE International Symposium on Power Line Communications and Its Applications*, ISPLC , 2007.
- [12] S. Chenishkian, "Building Smart Services for Smart Home," in *Proceedings of the IEEE 4th International Workshop on Network Appliances*, pp. 215-224, 2002.
- [13] Albert Treytl and Thomas Novak, "Practical Issues on Key Distribution in Power Line Networks," in *Proceedings of IEEE Emerging Technologies and Factory Automation*, September 2005.
- [14] Gustavsson R, "Security Issues and Power Line Communication", in the *Proceedings of the 5th International Symposium on Power-Line Communications and its Application (ISPLC)*, 2001.
- [15] Ryuzou Nishi, Hitoshi Morioka, Kouichi Sakurai, "Trends and Issues for Security of Home-Network Based on Power Line Communication", *The First International Workshop on Ubiquitous Smart Worlds (USW'05)*, AINA, Mar. 2005.
- [16] Richard Newman, Larry Yonge, Sherman Gavette and Ross Anderson, "HomePlug AV Security Mechanisms", in *Proceedings of IEEE International Symposium on Power Line Communications and Its Applications (ISPLC)*, Pisa, Italy, 2007.
- [17] Afkhamie, K. H., S. Katar, L. Yonge, and R. Newman, "An Overview of the upcoming HomePlug AV Standard," proceedings of International Symposium on Powerline Communications (ISPLC 2005), Vancouver, BC, 2005.
- [18] M. Abdalla and M. Bellare, "Increasing the Lifetime of a Key: A Comparative Analysis of the Security of Re-Keying Techniques", *Lecture Notes in Computer Science*, Springer-Verlag, volume 1976, 2000.