IOSR Journal of Engineering (IOSRJEN)
e-ISSN: 2250-3021, **p**-ISSN: 2278-8719
Vol. 3, Issue 12 (December. 2013), ||V3|| PP 01-06

Security issues of Power line Communications

Abdelraheem Mohamed Elkhalifa, Dr. abdelrasoul jabar alzubaidi
1 Sudan Academy of Sciences (SAS); Council of Engineering Researches & Industrial Technologies,
[2] Electronic Dept- Engineering College –Sudan University for science and Technology

Abstract: - This paper provides discussion of security issues for power line communications (PLC) networks and we put forth several security requirements needed for that network. Security is a major issue for the deployment of local area networks in companies, where the development of IP telephony applications is sustained. In such a background, it is essential to have reliable security mechanisms to avoid unauthorized listening to communications.

This power line communications represents an exceptionally promising alternative for high-speed Internet access and data networking. The communications medium has been well studies and standardization of the technologies are undergoing. The home network based on power line communication has been used widely however security of PLC has not been discussed sufficiently and not well studies and there is an urgent need for that. Though PLC uses power line as medium it has similar characterizes 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, authorizations, server, Intrusion Detection, modem, Power line communi cation.*

I. 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. 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. Power line communications (PLC) have received great attention in recent years as an alternative and cost –effective last –male –access technology. Its strength and popularity can be referring to its omnipresence nature and easily available infrastructure. Power outlets are available very widely at every home can act as channels for broadband supplying 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. The 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 power line, 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 system using narrowband communications.

II. OVERVIEW OF NETWORK SECURITY ISSUES

As with any other network, PLC can be subjected to various types of attacks either to interfere with PLC operation or to intercept the transmitted information. However, the advantage of PLC networks comes from the medium them use- the electrical wiring, which makes them particularly resistant to attacks since they are not easily accessible. To avoid any information disclosure, the network traffic must be encrypted in such a way that anyone not belonging to a PLC logical network cannot recover and decipher (decode) it.

In addition to eavesdropping, the main attacks to which a network can be subjected are those that aim at preventing its operation until it collapse or at having access to it and reconfiguring it as wished.

The only counterattacks in response to these types of attacks are cryptography, which prevents intruders (strangers) from having access to data exchanged over the network; authentication which allows the identification and authorization of anybody wishing to send data; and integrity control, which is used to know whether the data sent, was not modified during the transmission.

2.1 Cryptography

Making a text or message incomprehensible (unclear) through the use of an algorithm is not new. The Egyptians, like the Romans, employed methods used to encode a message. These techniques, which were relatively simple originally, have changed, and cryptography has been recognized as a science since World War II. The basic principle of cryptography is illustrated in **figure 1** an encryption key is used to encode a plain text. At any time during the transmission, somebody can recover the encrypted text, called a cryptogram, and try to decipher it using various methods.

2.2 Cryptology

Cryptography only involves encryption design and methods. Trying to decipher encrypted text is called cryptanalysis. Cryptology designates the study of cryptography and cryptanalysis.
In France, for example, there are strict (tough) regulations concerning the length of the keys used for encryption purposes. A key with a maximum length of 40 bits can be used for any public or private use. For private use, the length of the key may not exceed 128 bits; the key must be transmitted to the local cyber security authorities. In the USA or in Japan, the regulations are different and one should take care to know the restrictions on the length of keys to be used.

There are two cryptography techniques: symmetric-key cryptography and Asymmetric-key cryptography, better known as public-key cryptography Symmetric-key cryptography is based on the use of a single key used to encrypt and unscramble data. All persons wishing to transmit data securely must therefore share the same secret: the key. This process is illustrated in **Figure2**. The clear fault in this system resides in how this secret key is shared and transmitted between the sender and receiver.

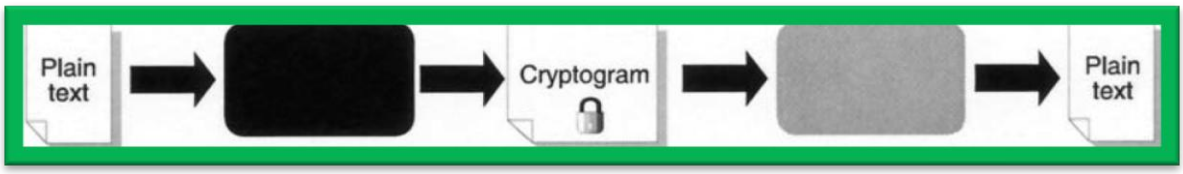


Figure1 Data encryption

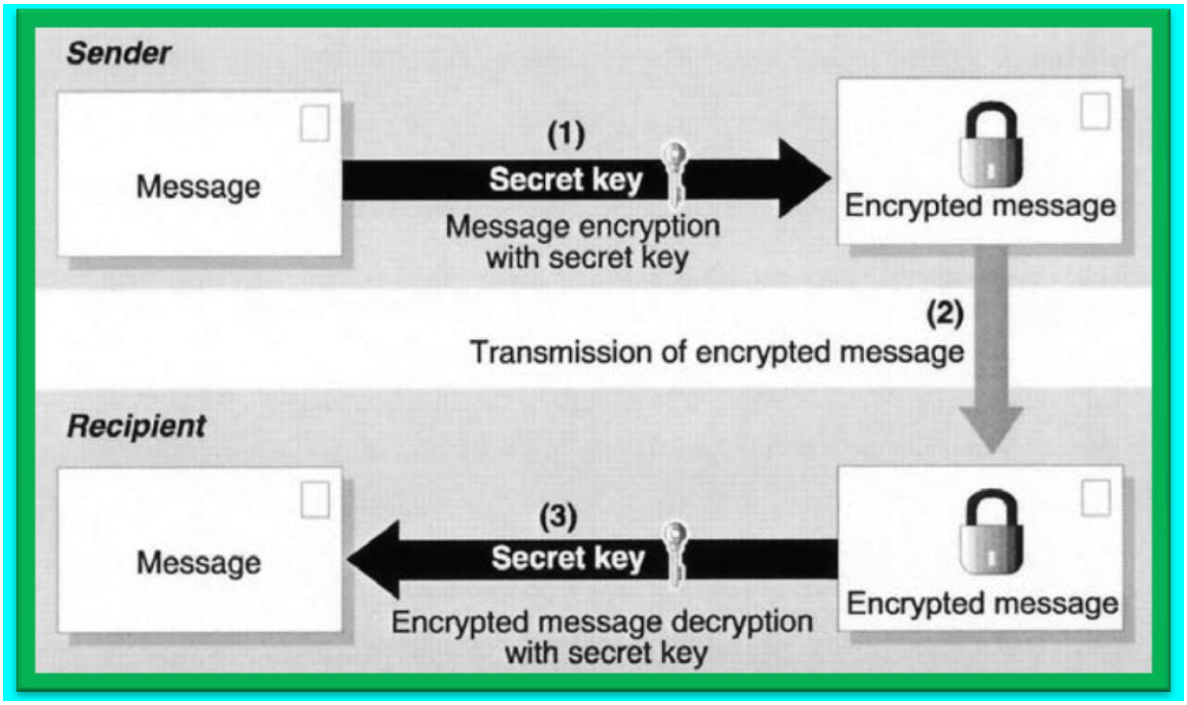


Figure2 Symmetric-key cryptography

Various symmetric-key cryptography algorithms have been developed, in particular DES (Data Encryption Standard), IDEA (International Data Encryption Algorithm), series RC2to RC6, and AES (Advanced Encryption Standard).

DES (Data Encryption Standard) algorithm was jointly developed in the seventies (1970) by IBM and the NSA (National Security Agency).

The DES is an encryption algorithm known as "by blocks" .The length of the key used is fixed (40 or 56 bits). The purpose of the DES is to carry out a set of permutations and substitutions between the key and text to be encrypted so as to encode the information.

IDEA (International Data Encryption Algorithm) is an algorithm with 128-bit key length. The text to be encrypted is divided into four sub-blocks.

Each round is a combination of exclusive "or," addition modulo2^{16} and multiplication modulo2^{16}. On each round, the data and the key are combined. This technique makes the IDEA particularly secure.

The IDEA is implemented in PGP (Pretty Good Privacy), which is the world's most widely used software.

III. SECURITY FOR PLC NETWORKS

HomePlug implements a PLC private network system based on encryption keys known by authorized PLC devices in this network for increased PLC network security.

This mechanism is based on the secure, reliable, and simple registration for the network manager or user of the various PLC devices of the same logical network. These functionalities make the deployment of PLC networks easier.

The main characteristics of the registration of a PLC device in a PLC network are the following:-

• ***Security***. A device can be registered in a PLC network only if it has the suitable encryption keys and only if it is authorized and registered by the network managing devices. It must be possible to easily attach new devices and also to quickly remove devices from a PLC network.

• ***Reliability.*** The same PLC network must provide stability in the configuration of encryption keys and support the electrical connections/disconnections of the network PLC devices in a stable manner. It must also be possible to recover an original configuration if the keys are lost or if a device is reconfigured.

• ***Simplicity***. Managing the configuration of the encryption keys of the various PLC logical networks must be simple for a network manager.

For this purpose, a single key used for data exchange encryption over the electrical network is defined by Homeplug1.0 and Turbo. Homeplug AV, which is more sophisticated, defines several network keys that are managed by the network coordinating device that centralizes the keys.

Therefore, a PLC logical network is based on an encryption key called a NEK (Network Encryption Key) in the Homeplug specification that encrypts the data exchanged between the various PLC devices (See figure 3) bellow.

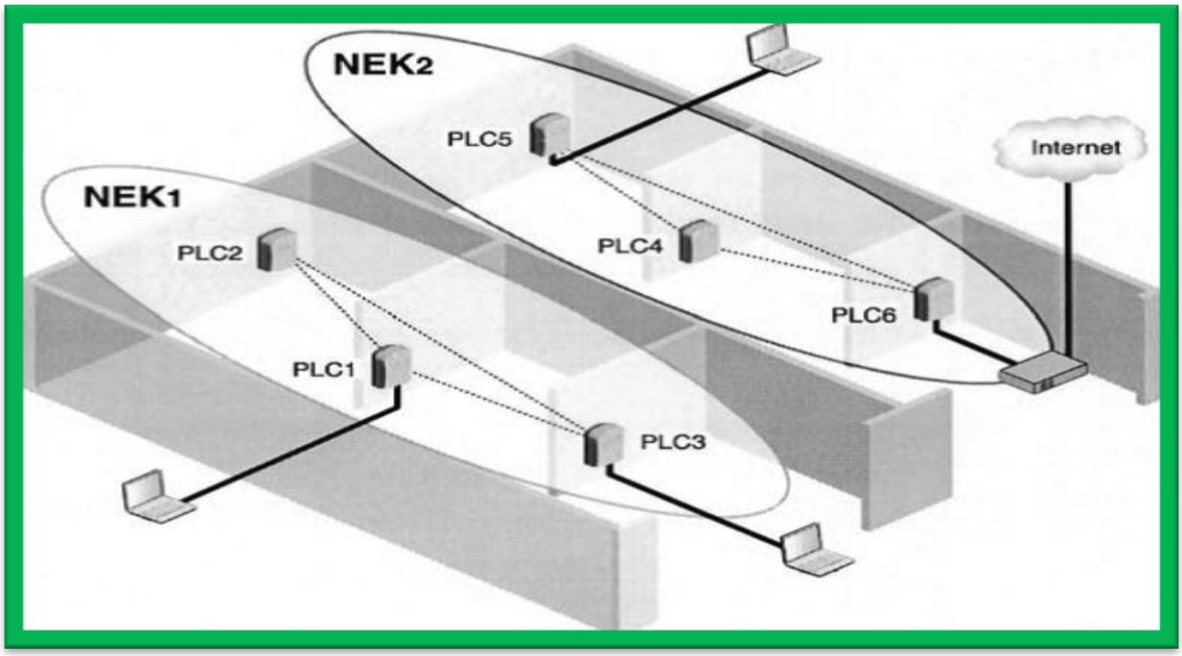


Figure 3. PLC logical networks with various NEK

A PLC network can be configured with a NEK in several ways:-

- ***Via the Ethernet interface.*** A configuration frame of the NEK is sent in broadcast mode to the PLC devices of the same network using a configuration tool.

All the PLC devices connected by means of their Ethernet interface recover this configuration.

- ***Via the electrical interface.*** A configuration frame of the NEK is sent by means of the electrical network to the connected PLC devices. This is only possible if a second key, called DEK (Default Encryption Key) is known. This key, which is specific to each PLC devices, is recorded in the device memory by the manufacturer by following Homepluge specifications.

The DEK is used by two PLC devices –the configuring station device and the device which must receive the new NEK- for the encrypted NEK exchange over the electrical network.

- ***Via a Web interface***. If the PLC devices are advanced, like those of the Asoka USA brand, the key configurations can be managed by a single web interface.

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 transmission has to be preserved. Even is 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. SECURITY OF HOME NETWORK

For safe communication several services for security such as authentication, confidentiality, and 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 (sly) 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 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 4** 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 4** communicates with authentication server with Remote Authentication Dial-In User Service (RADIUS) protocol. This is for supporting centralized authentication, authorization and Accounting (AAA) management

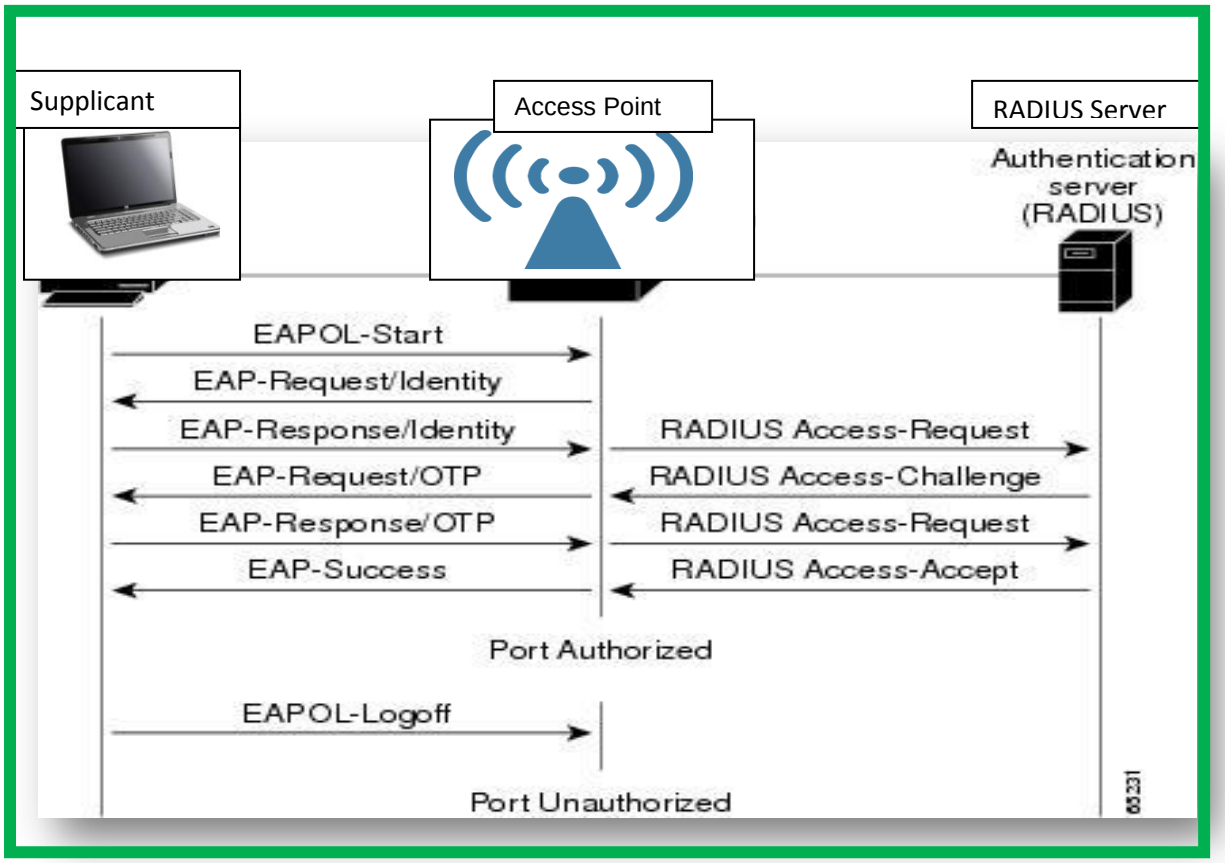


Figure 4. Authentication Process of IEEE 802.1x Standard with EAP and RADIUS

Remote Access Dial-In User Service (RADIUS): Network authentication protocol and service originally used in wired networks for remote host access to networks. It is an Authentication, Authorization and Accounting (AAA) client-server protocol. RADIUS is now used often in large-scale wireless networks for authenticating users and creating dynamic encryption keys. Some commercial products are Cisco ACS*, Microsoft IAS* and Funk Steel-Belted RADIUS*

3.1 AAA Phases

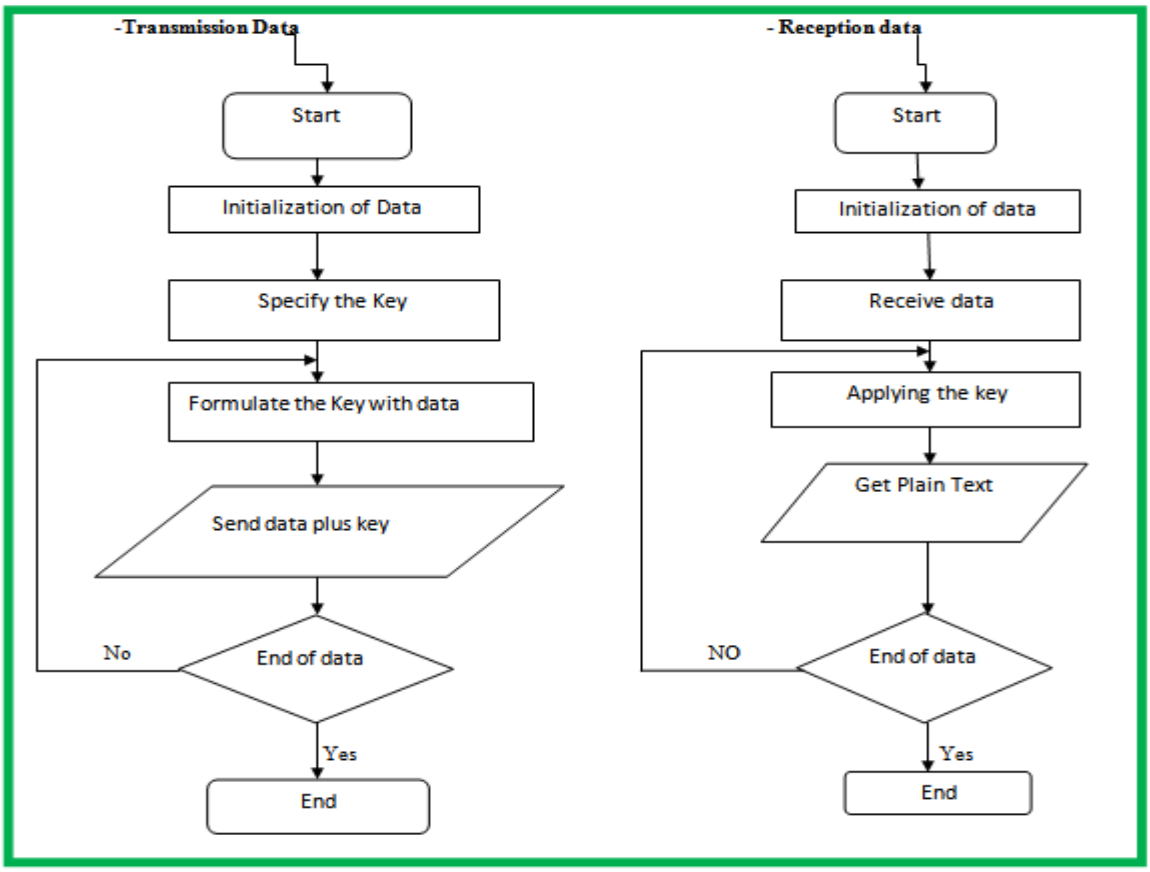
- **Authentication phase:** Verifies a user name and password against a local database. After credentials are verified, the authorization process begins.
- **Authorization phase**: Determines whether a request is allowed access to a resource. An IP address is assigned for the dial-up client.
- **Accounting phase**: Collects information on resource usage for the purpose of trend analysis, auditing, session time billing, or cost allocation. The Power line communication adopted almost similar security schemes with wireless LAN technology. PLC uses cryptographic mechanism like DES and AES. Table 1 show 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

VI. Security Algorithm

The flowchart for the security algorithm is:-



- Start
- Initialize the data
- Inter the specify key
- Inject key with data
- Send data with key
- Check if end of data given from modem, if yes then send the message to the receiver else go to formulate the key with data.

VII. CONCLUSION

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. 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 cannot eliminate the vulnerability perfectly. Therefore usage of intrusion detection in PLC is discussed. And we also must present multi- layered security architecture to meet the necessary security goals for PLC. 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] Homeplug Alliance, Http://.homeplug.org.
[2] HD-PLC whitepaper, http://www.hd-plc.org
[3] Xavier Carcelle, Power Line Communications in Practice
[3] **J. Anatory** *University of Dodoma, Tanzania&* **N. Theethayi** *Bombardier Transportation, Sweden*
[4] Broadband Power-line Communication Systems THEORY & APPLICATIONS