Vulnerability Considerations for Power Line Communication's (PLC) Supervisory Control and Data Acquisition

Ali Hosseinpournajarkolaei[1], Hamid Jahankhani[2], Amin Hosseinian-Far[3]

[1]Najarkolaei@ieee.org , [2]Hamid@williamscollege.co.uk,
[3]Ahosseinianfar@glos.ac.uk

Abstract: Due to the increasing importance of communication networking, the Power Line (PL) channel has been considered as a good candidate for the communication medium. Power Line Communications (PLC) term stands for the technologies for the data communication over the electrical power supply network. The PL channels were not designed to transmit high speed data; therefore they exhibit hostile medium for communication signal transmission. There are many factors such as noises, attenuation, distance and etc. affecting the quality of the transmission over PL channels. This paper presents PL model in the first sections of the work. Then it covers the security assessment of the PL system in the Supervisory Control and Data Acquisition (SCADA) context.

I. Introduction

Recently there has been a big interest in utilizing the PL channel for communication due to its potential to telecommunication users [1]. PLC is using an existing power line system, i.e., this is great saving in cost and time. The general idea of PLC system is to modulate a radio signal with data and transmit it through PL channels in a different band of frequencies which are not used for supplying electricity. PLC technology can be divided into two categories; the narrowband and Broadband communication. The frequency range of up to 150 kHz is for narrowband with the theoretical bit rate of kilobits (up to 2 Mbit/s). The frequency range for Broadband technology is between 1.61-30 MHz with theoretical bit rate up to 200 Mbit/s [2]. The used frequencies and the modulation scheme are two main factors which have a significant influence on the efficiency of the system and also the speed of the PLC service. The best suitable modulation technique for PLC system is an Orthogonal Frequency Division Multiplexing (OFDM) [2]. OFDM is a Multi-Carrier modulation scheme in which a single high rate data-stream is divided into multiple low rate data-streams. It is also modulated by using sub-carriers which are orthogonal to each other. The main advantages of OFDM are its efficient spectral usage by allowing overlapping in the frequency domain (reducing the bandwidth by squeezing subcarriers until they overlap with each other) and multi-path delay spread tolerance [2].

In this paper, in section II, the Power Line channel will be briefly introduced. Moreover, simulations on the PLC model are represented. In section III, PLC noise is outlined. And section IV would present the security assessment of the PL system in the Supervisory Control and Data Acquisition (SCADA) context.

II. Power line Channels

The power line networks usually classified as high-voltage (100kV), medium-voltage (1-100kV) and low-voltage (110-380V). High Voltages are not suitable for data transmission, therefore conventional fibre optics or wireless radio-link is used for transmission of this data over the existing power lines with repeaters used in MV networks to mitigate the effects of noise interference. Couplers then can be used to by-pass transformers when the power is lowered from MV to LV [3]. Power grid consists of cascaded cables of diverse line lengths with a various number of branches of different line lengths and terminal loads. Switching on/off electrical equipment's change the terminal load, i.e. it results changing the frequency response of the network. The effect of changes in the power distribution system topologies over the PL channels are investigated in [4]. A simple topology for such a power distribution system was used to investigate the effect of variation in direct length, branch load, branch lengths and different number of paths.

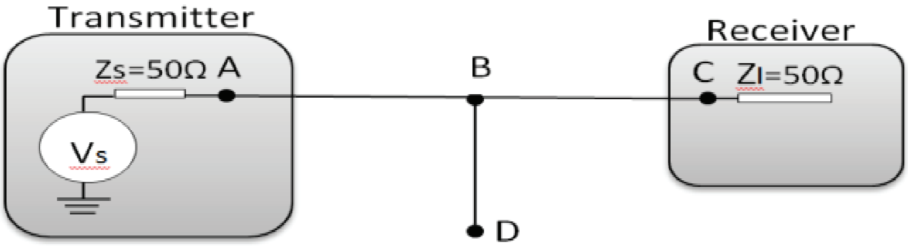

Figure 1: A Simple LV Power Line Network Configuration [5]

The multipath model is a widely used model for investigating the data transmission over power line networks and is given below:

$$H(f) = \sum_{i=1}^{N} g_{i\,.}\, e^{-(a0+a1f^{k})di} \;.\, e^{-j2\pi f d_{i/V_p}} \qquad (1)$$

where $H(f)$ is the frequency response of the channel, g_i the weighting factor, d_i the length of the data transmission path for various path numbers and N is the total number of paths.

As it can be observed from the results in [4] Variation in the direct line length from the transmitter results no multi-path fading as the channel response is a linear function of the frequency. The receiver can therefore recover the data transmitted using a single-carrier modulation transmission.

However the multi-path behaviour in [6] indicates that multi-carrier transmission would be suitable for data transmission over the power line channel in case of varying the length AC with one branch. The increase in the direct line length AC reduces the channel bandwidth and its effect on frequency response is similar to the no-branch case, the difference being that the frequency notches are superimposed on the frequency response.

From the simulation results in [6] it is observed that increasing the branch length BD increases the power line attenuation which is especially noticeable in higher frequencies.

In case of multipath with different numbers of paths, from the simulation results for number of path 4 and 10 shown in figures below, it can be observed that the position of notches do not change. But as the number of paths increases from 4 to 10 the attenuations of notched points and signal distortion tend to increase.

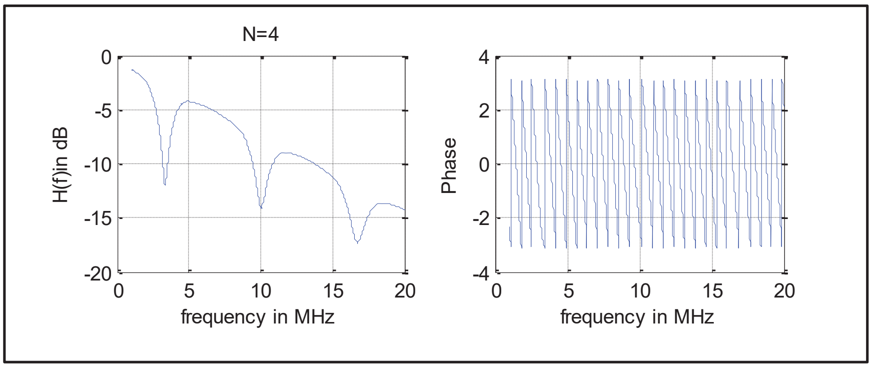

Figure 2: Multipath channel model with number of path=4.

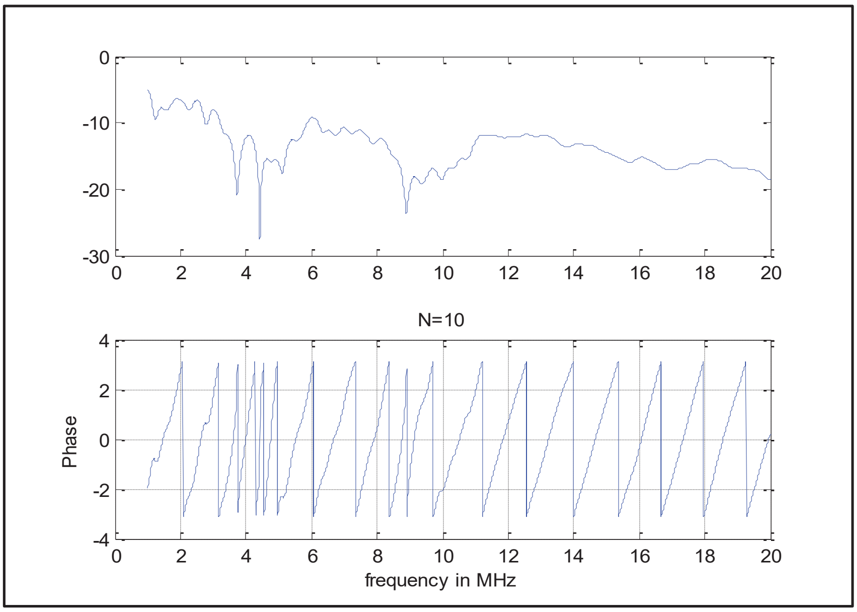

Figure 3: Multipath channel model with number of path=10

a. Narrowband Technology

The narrowband PLC are normally used in automation systems. The automation systems based on PLC technology are implemented with no any additional insulation of communication networks which results substantially reduction in costs for the installation and realisation of the new network within the existing buildings. The automation system in this system can be used in:

i) Central control of various home system such as controlling doors/windows
ii) Controlling connected devices to the internal wiring such as lighting, air conditions
iii) The Security function, sensor control [6]

Another application for narrowband technology is called smart metering. The smart meter system includes meters at the consumer site, communication medium between a service provider and consumer, such as a gas, an electric, or water, and data management systems in service provider site that make the information available. The smart meter transmits the collected data through PLC to a Meter Data Management System for data analysis and billing [7].

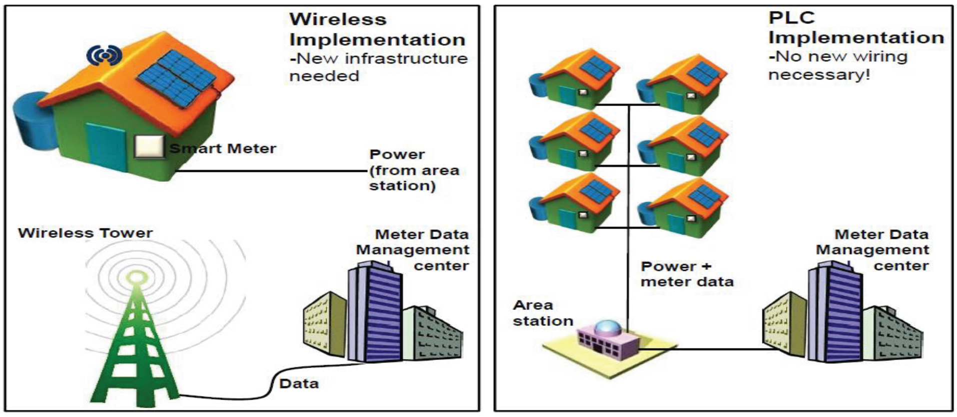
Wireless Implementation
-New infrastructure needed
Smart Meter
Power (from area station)
Wireless Tower
Meter Data Management center
Data
PLC Implementation
-No new wiring necessary!
Power + meter data
Area station
Meter Data Management center

Figure 4: The Basic Smart Metering System [8]

If you get a smart meter in your house/building you should get the following benefits:

Accurate bills; the smart meter sends information to your energy provider on how much energy you have exactly used, so no more estimated bills.

Could help to save money; by knowing what you're using, and having an idea of which appliances use the most energy, you may be able to reduce your energy usage and save money.

A standard in-home energy display; has a small screen which shows your energy usage at any one time with no any additional cost.

Reduced theft of energy; the energy theft detection is more easily therefore it can be easily prevented, meaning you won't have to pay for stolen energy [7].

b. Orthogonal Frequency Division Multiplexing (OFDM)

Nowadays in order to achieve higher data rates in communication system OFDM which is a multi-carrier modulation technique is being used. In OFDM scheme data will be transmitted by dividing a single wideband stream into several smaller/narrowband parallel bit streams. Each of these narrowband streams then modulated onto an individual carrier.

The narrowband channels are orthogonal vis-à-vis each other, and are transmitted simultaneously which results an increase in the symbol duration proportionately, and reduction on the effects of inter-symbol interference (ISI) which are induced by multipath Rayleigh-faded environments [2].

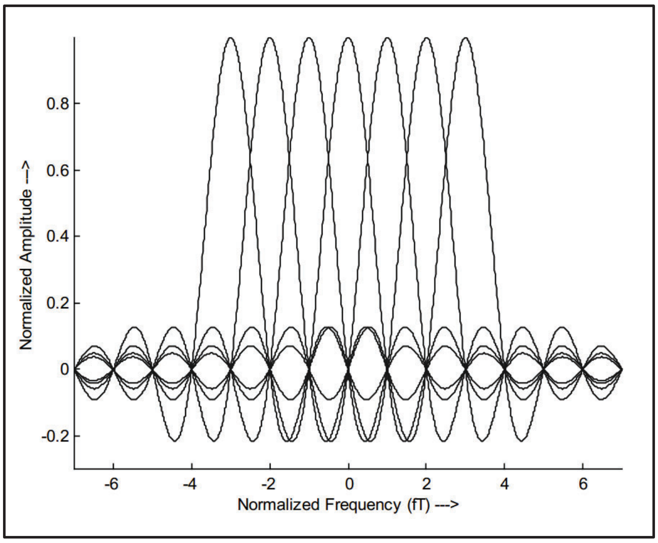

Figure 5: Basic OFDM System Architecture

The study on the effect of number of branches in power line networks indicated the possibility of degradation of the channel performance. Therefore in order to enhance the network stability and performance the multi-carrier modulation techniques such as OFDM can be considered [6].

III. Different Types of Noise on PLC

In order to design high speed data transmission over power line networks details knowledge of channel properties noise are required. Due to the signal distortion, cable losses and multipath propagation the noise is known as the most crucial factor effecting data communication over power line systems.

Normally in LV power line networks, the source of the noise can be internal (inside the network) or external (outside the network). Overall in BPL channels the additive noise normally classified into five different classes;

i) Coloured background noise: has very low Power Spectral Density (PSD) which also varies with the variation in frequency and resulted by summation of number of different noise sources with very low power.

ii) Narrow band noise: normally has sinusoidal signals with modulated amplitudes and caused by ingress of broadcast station in short wave broadcast bands and the medium.

iii) Periodic impulsive noise asynchronous to the mains frequency: have a repetition rate between 50 kHz to 200 KHz in most cases and normally resulted by switching power supplies.

iv) Periodic impulsive noise synchronous to the mains frequency: with the repetition rate of 50Hz or 100 Hz and are synchronous to the mains cycle and normally created by the power supplies operating synchronously with the mains cycle.

v) Asynchronous impulsive noise: which sometimes has a very high PSD value of more than 50 dB above the background noise and is normally caused by switching transients in the network [9].

a. MATLab Simulink model of different types of noise on PLC system

Asynchronous Impulsive Noise: to simulate the noise produced by turning on/off the electrical devices the scheme in Fig. 6 was used. The maximal delayed used at delay block is 100 the M-ary of Random Integer Generator was set to 100 with sample time 1/1000.

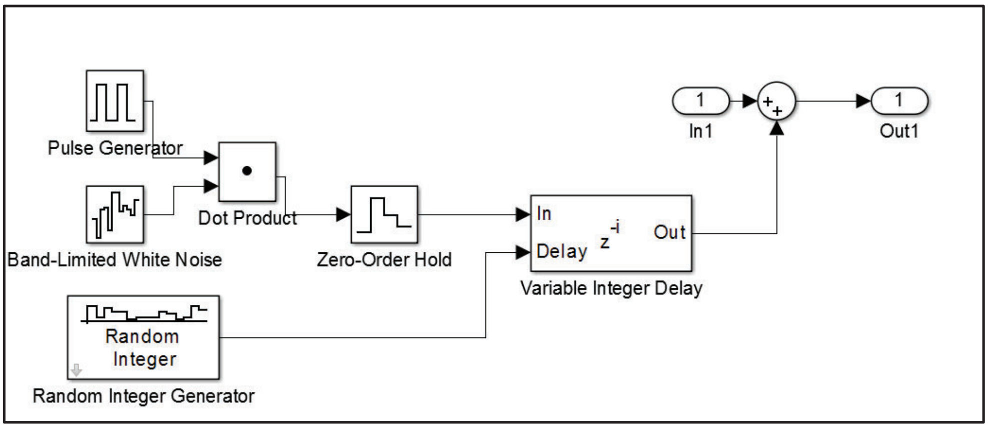

Figure 6: Asynchronous impulsive noise

Periodic Impulsive Noise: to simulate noise like that produced by switched power supplies, the scheme showed by Fig. 7 was used.

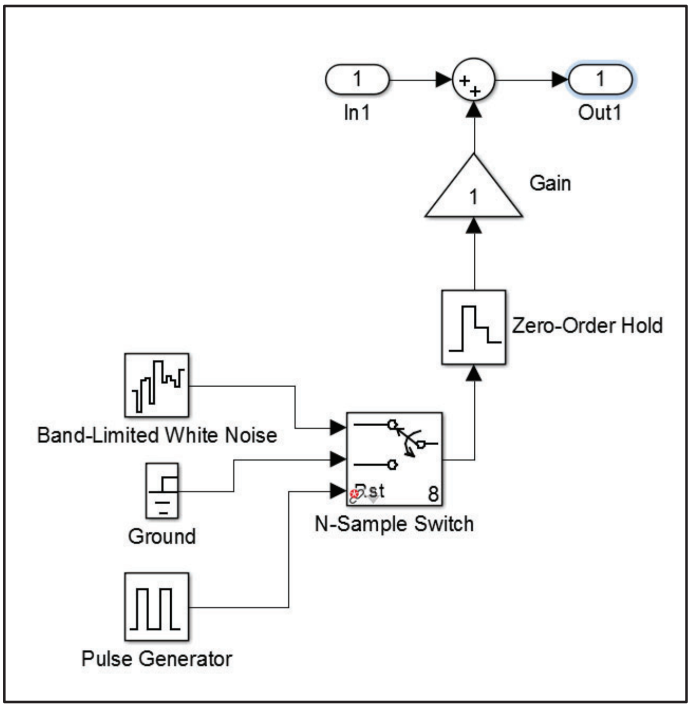

Figure 7: Periodic impulsive noise

Synchronous Impulsive Noise: as it can be seen in figure below, by adding a spectral colouring to the white noise together with a periodical rectangular signals synchronous impulsive noise can be modelled. This type of noise is caused by thermistors in light dimmers and copiers.

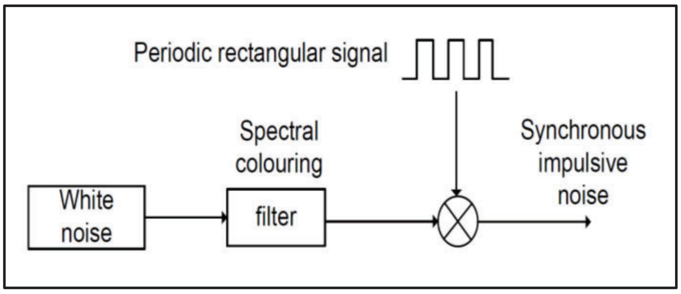

Figure 8: Periodic Rectangular Signal

The final model of applying different types of noises on PLC has been created with power line channel together with white Gaussian noise (Fig. 9).

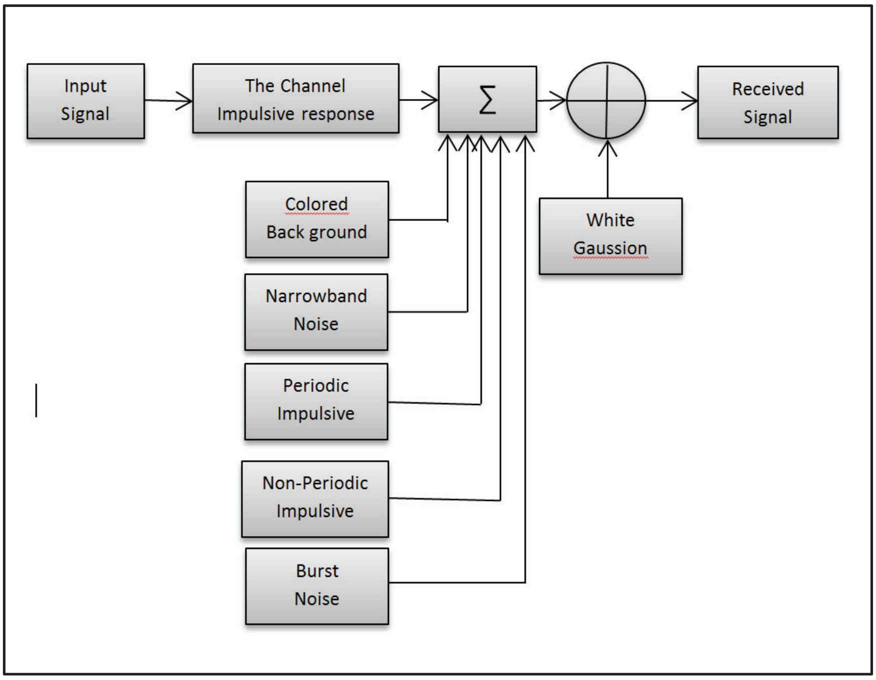

Figure 9: PLC Noise together with Gaussian Noise

The Power line channel model is modelled as a digital filter together with the source of interferences/noises. The PLC 16 QAM model with OFDM modulation which enables to simulate better data communication over power lines.

IV. Vulnerability Considerations for the PLC SCADA

SCADA is a combination of telemetry and data retrieval system and has existed long time before control engineering [10]. Smart Grids where the narrow band PLC is implemented are also vulnerable to threats associated with similar infrastructural systems. Ericsson (2010) points out that the threat SCADA arises in the access points (Fig. 10) available in them [11]. Moreover the complexity the SCADA make it difficult to consider the System of Systems' (SoS) frameworks for the security assessment. Knowing that the PLC model introduced above would be also exposed to security threats and vulnerabilities when it comes to application.

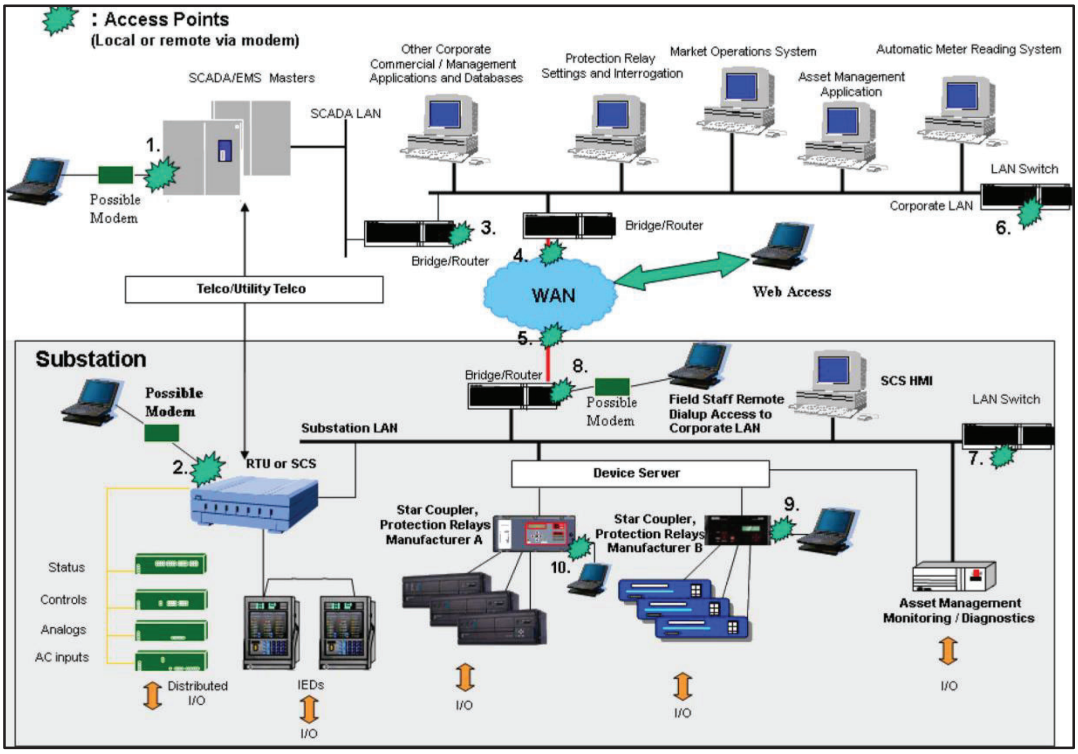
: Access Points
(Local or remote via modem)
SCADA/EMS Masters
SCADA LAN
Other Corporate Commercial / Management Applications and Databases
Protection Relay Settings and Interrogation
Market Operations System
Asset Management Application
Automatic Meter Reading System
LAN Switch
Corporate LAN
1.
Possible Modem
3.
Bridge/Router
4.
Bridge/Router
6.
Telco/Utility Telco
WAN
Web Access
5.
Substation
Possible Modem
Bridge/Router
8.
Possible Modem
Field Staff Remote Dialup Access to Corporate LAN
SCS HMI
LAN Switch
Substation LAN
2.
RTU or SCS
7.
Device Server
Star Coupler, Protection Relays Manufacturer A
Star Coupler, Protection Relays Manufacturer B
9.
10.
Status
Controls
Analogs
AC inputs
Distributed I/O
IEDs
I/O
I/O
I/O
I/O
Asset Management Monitoring / Diagnostics
I/O

Figure 10: Access Points to SCADA System [11]

Using Ericsson's domain categorisation of SCADA [11], the following domain's securities are considered for the above mentioned PLC model:

a. Public, Supplier, Maintainer Domain

One of the main security considerations in this domain would be provision of appropriate encryption/decryption technique in order to avoid public access to the data transferred via PLC. Furthermore, the maintainer domain should be contracted in a way which avoids future potential eavesdropping scenarios by third parties.

b. Power Plant Domain

Injection from the power plant can be performed in various ways and the vulnerabilities and risks would depend on the system involved as the medium. Therefore security consideration should be presented for each individual SCADA.

c. Substation Domain

Distance between branches and securities involved in losing data due to lack of repeater on the way should be considered in domain. A longitudinal analysis of potential extensions to the PLC, to the distance between branches and any probable amendments should be considered before implementation of the Smart Grid.

d. Telecommunication Domain

Securing gateways in the Smart Grid is an area to be considered for implementation. Use of repeaters, electrical physical structures and the bridges used may also lead to physical security threat. Data does not pass into transformer and therefore the bridges are used. The physical bridge outside the transformed is subject to the main access point for eavesdropping.

e. Real-Time Operation Domain

Noise as a result of increased attenuation which then leads to poor data is a major threat in the real-time operation domain. However the physical unintentional threats such as systems' failure should also be considered.

f. Corporate IT Domain

Failure in the software used for the control system of the Smart Grid is susceptible to damage. Similar to any other information system, software is likely to be influenced by poor algorithm or external viruses.

V. Conclusions

To conclude, this major project gives the detail knowledge of a current key issue in the field of power line communications. Various effects on PLC (such a different number of paths) have been investigated. Different types of noise on PLC were modelled and simulated theoretically; and the threats and risks associated with the practical implementation of Smart Grid using the PLC is analysed. Domain classification is used for breaking down different facets for consideration. This would simplify the complexities and integrations involved in Smart Grid.

References

[1] J. Anatory, N. Theethayi, M. M. Kissaka and N. .. Mvungi, "Broadband PowerLine Communications: Performance Analysis," World Academy of Science, Engineering and Technology, 2008.

[2] D. G. Agrawal, R. K. Paliwal and P. Subramanium, "Effect of Turbo Coding on OFDM Transmission to Improve BER," *International Journal of Computer Technology and Electronics Engineering (IJCTEE),* vol. 2, no. 1, pp. 94-102, 2011.

[3] Industry of Canada, "Broadband over Power Line (BPL) Communication Systems," Industry of Canada, 2012.

[4] A. Hosseinpournajarkolaei and A. Hosseinian-Far, "Channel Characterization for Broadband Power Line Communication System," in *6th Sastech Intl Conference*, KL Malaysia, 2012.

[5] A. Hosseinpournajarkolaei, J. Lota and W. Hosney, "Challenges Facing The Design of Broadband Power Line Communication (BPLC) Systems," in *UPEC-Brunel University of London*, London, 2012.

[6] A. Hosseinpournajarkolae, J. Lota and W. Hosney, "Design of Broadband Power Line Communication system for UK Power line system," in *University of East London*, London, 2012.

[7] Consumer Focus UK GOV, "Smart meters – what are they and how can I find out more?," Consumer Focus, 2013. [Online]. Available: http://www.consumerfocus.org.uk/get-advice/energy/smart-meters-what-are-they-and-how-can-i-find-out-more/benefits-and-

disadvantages-of-smart-meters. [Accessed 29 Aug 2013].

[8] A. D. L. Fernandes and P. Dave, “Power Line Communication in Energy Markets,” CYPRESS, San Jose US, 2011.

[9] D. Chariag, Y. Guezgouz, J. Raingeaud and C. Lebunetel, “Channel Modeling and Periodic Impulsive Noise Analysis in Indoor Power Line,” in *IEEE International Symposium on Power Line Communications and its Applications*, 2011.

[10] R. J. Robles, M.-K. Choi, E.-S. Cho, S.-S. Kim, G.-C. Park and S.-S. Yeo, “Vulnerabilities in SCADA and Critical Infrastructure Systems,” *International Journal of Future Generation Communication and Networking ,* vol. 1, no. 1, pp. 99-105, 2008.

[11] G. N. Ericsson, “Cyber Security and Power System Communication—Essential Parts of a Smart Grid Infrastructure,” *IEEE Transactions on Power delivery,* vol. 25, no. 3, pp. 1501-1507, 2010.