Secured Power Line Communication Based Network for Advanced Metering In Smart Grids.

Zephania Philani Khumalo

2017

Secured Power Line Communication Based Network for Advanced Metering In Smart Grids

by

Khumalo Zephania Philani

(Student Number: 20250262)

Thesis submitted to the Faculty of Engineering and the Built Environment in fulfilment of the requirements for the degree of

Master of Engineering in Electronic Engineering

at the

Durban University of Technology

July 2017

Approved for Final Submission

Supervisor: Professor B Nleya	Student: Zephaniah Philani Khumalo
_____	_____
Date	Date 14/08/2017

Plagiarism Declaration

I declare that the content of this thesis is my own work. Where collaboration with other people has taken place, or material from other parties is used, it is indicated in the acknowledgement or referenced.

I authorise the University to lend this thesis to other institutions or individuals for the purpose of scholarly research.

This work is submitted for the degree of Master of Engineering in Electronic Engineering and it has not been submitted to any other University or Institution for any other degree or examination

Signature_____ Date 14/08/2017

Name: Student number:

ZP Khumalo 20250262

Acknowledgements

I would like to express my gratitude to my supervisor and Andrew for their dedication in assisting with my research. Their guidance, knowledge and encouragement have helped me accomplish my dreams.

Furthermore, I would like to thank DUT financial aid scheme in funding my research. Through this research I have learned a lot. I am also eternally grateful to my family's unending support.

Finally, in all of this work I thank God for good health, strength, knowledge and endurance.

Zephania Phitlani Khumalo

Abstract

A Smart Grid (SG) generally refers to a modernized power grid system that incorporates Information and Communications Technologies (ICT) so that a two way communication between the grid system (utility) and power users ensures power supply efficiency and optimization to the users. In a way, an SG is an evolved version of legacy power grid systems that manages electricity demand in a sustainable, reliable and economic manner, built on advanced infrastructure and tuned to facilitate the integration of all involved. The provisioning of duplex communication between the utility and its users (customers) allows key devices such as SMs to interact directly with the utility's control center (CC). SGs are destined for provisioning a cleaner environmental sustainable and renewable energy for the future. Its successes mostly rely on advanced ICT design and architecture. It is imperative that it meets the future data transmission and design performance requirements in terms of robustness, reliability, and at the same time ensuring end-to-end data exchanges with minimal latencies and losses.

The incorporation of ICT, however, results in security and access control challenges, as a result complex network arrangement may be exploited by hackers among other things, access private information and sensitive data, hence the necessity to address vulnerabilities of such systems. Typical consequences or repercussions of security and access control threats include energy theft by way of altering of SM data. At present, it is cost effective to implement the ICT related infrastructure on the currently unused power line spectrum (i.e. above 50Hz) hence in this work, Power Line Communication (PLC) is elected for provisioning this platform.

As such, PLC implementation shall imply the digital communication in power lines concurrently with electrical power transmission and ensuring uninterruption of either of the services, as well as guaranteed efficiency. We address approaches to increasing the data rate of transmission and reduction of bit error rates. That will enhance the performance of PLC and redevelopment of reliable ICT without additional cost to the existing infrastructure of electrical grids. We also address security and access control by implementing Advanced Encryption Standard (AES) protocol to secure SG related data in our proposed security and access control framework. Results show that the system has low computational requirements, minimal latency and as well ensures confidentiality and integrity. The simulation is run on a combined MATLAB/ OPNET platform.

List of Acronyms

AMI	Advanced Metering Infrastructure
AC	Alternating Current
AMR	Automatic Meter Reading
AMS	Advanced Metering System
AES	Advanced Encryption Standard
ARR	Automatic Repeat Request
APDU	Application Protocol Data Unit
AWGN	Additive White Gaussian Noise
ASK	Amplitude Shift Keying
BPL	Broadband Power Line
BER	Bit Error Rate
BPSK	Binary Phase Shift Keying
CAL	Common Application Language
CSMA	Carrier Sense Multiple Access
CDMA	Code Division Multiple Access
CCM	Cipherblock Chaining Message
CU	Coupling Unit
CEBus	Consumer Electronic Bus
CDCR	Collision Detection and Collision Reduction
DNP3	Distributed Network Protocol Version 3
DC	Data Concentrator
DLL	Data Link Layer
DQPSK	Differential Quadrature Pulse Shift Keying
DTT	Digital Terrestrial Television
DSM	Demand Side Management
DAB	Digital Audio Broadcasting
DVB	Digital Video Broadcasting
EIA	Electronic Industries Associations

EEPROM	Electrically Erasable Programmable Read-Only Memory.
FCS	Frame Check Sequence
FFT	Fast Fourier Transform
FDM	Frequency Division Multiplexing
FEC	Forward Error Correction
FSK	Frequency Shift Keying
GPRS	General Packet Radio Service
GSM	Global System for Mobile communications
HPA	HomePlug Powerline Alliance
HDTV	High Definition Television
ITU	International Telecommunications Union
IEC	International Electrotechnical Commission
IP	Internet Protocol
ISO	International Standards Organization
IEEE	Institute of Electrical and Electronics Engineers
IDFT	Inverse Discrete Fourier Transform
IDS	Intrusion Detection System
LON	Local Operating Network
LM	Load Management
LCD	Liquid Crystal Display
LV	Low Voltage
MAC	Media Access Control
MDMC	Metering Data Management Centre
MCU	Micro Controller Unit
MV	Medium Voltage
NPDU	Network Data Protocol Unit
OPNET	Optimization Network Tool
OFDM	Orthogonal Frequency Division Multiplexing
OSI	Open System Interconnect

PLC	Power Line Communications
PKI	Public Key Infrastructure
QoS	Quality of Service
QAM	Quadrature Amplitude Modulation
QPSK	Quadrature Phase Shift Keying
RF	Radio Frequency
RSA	Rivest, Shamir, and Adelman
SSM	Supply Side Management
SM	Smart Meter
SNR	Signal to Noise Ratio
SG	Smart Grid
TDMA	Time Division Multiple Access
UART	Universal Asynchronous Receiver/ Transmitter
VPN	Virtual Private Network
WIMAX	Worldwide Interoperability for Microwave Access

Table of Contents

List of Figures

List of Tables

1 Introduction

1.1 Background

Current electricity power supply and generation systems have been in existence for quite some time. There are no indications that these current systems will be decommissioned in the near future. Their heavy reliance on fossil energy such as oil and coal are not sustainable as these fossils are fast depleting [1]. These fossils are non-renewable and thus the reserves on earth are fast depleting [1]. This inevitably has led to a gradual energy crisis that has prompted global strides to identify alternate energy resources that could sustain long-term power requirements as well as industry development. Prospective renewable energy resources include but are not limited to wind, hydro plants, solar, tidal and geothermal installations [2], all of which collectively are referred to as "green energy" solely because they do not release carbon dioxide (CO_2) into the air in the process of electricity power generation [2].

It is important to replace the current fossil fuels because they are environmentally unfriendly [2]. The key to the energy power systems crisis is to integrate different renewable energy resources that are automated and intelligently managed. These would ensure their effectiveness and efficiency. The automation management and intelligence are envisioned to offer a diversity of advantages in terms of digitalization, flexibility, intelligence and resilience [3], thus the name Smart Grid (SG) [2] [3].

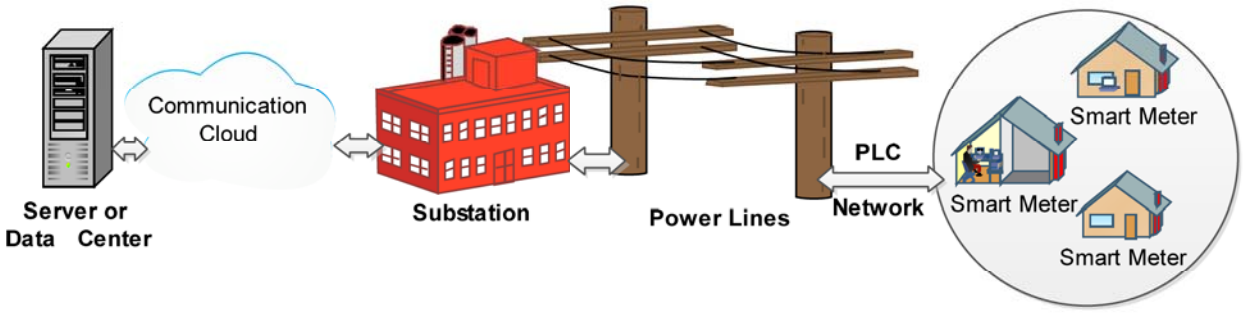


Figure 1-1 Generic Diagram of Smart Grid Two Way Communications [2]

The SG is a promising solution towards integrating and availing renewable resources to the current energy grid. Such a grid is an ideal platform for energy consumers to contribute to the electricity enterprise. A typical SG has distinct mechanisms and functions in comparison to the traditional energy grid in that it facilitates two-way communication between users (meters) and the central

controls. Figure 1.1 shows the generic diagram of SG two-way communications. Facilitating the two-way data transmission is possible through the deployment of an enabling AMI that holds a key element in the SG system named SM. A SM typically has a processing chip and a non-volatile storage that performs smart tasks such as being able to report intervallic usage to consumers as well as facilitating interaction at the power supply utility directly with SM appliances at home to control them [3].

The two-way communication helps in matching demand versus supply. The main SG services include [2], [3]:

- Automatic meter reading.
- Power grid monitoring: peak voltage, peak factor, and a degree of synchronisation as well as current levels in the power grid structure supervised in real time.
- Demand Side Management consists of two parts:
    - Load shifting.
    - Power conservation.
- Home networking amongst electrical appliances for power management.
- Vehicles power technology: The power stored in charged cars can be put back to the power grid.
- Self-healing system: the SG system should be able to heal automatically.
- Flexibility counter to attacks: increasing power grid robustness, protecting key assets from physical attacks and improving flexibility.
- Equipment management and performance efficiency: the state of all equipment and operational efficiency can be monitored.
- New markets operations: SG will join in and open new trades to the power grid.

From an operation perspective, the smart control centres monitor key electric components remotely almost in real time, this results in smart transmission infrastructures using new technology paradigms to enhance the energy excellence; and the smart substations coordinate their devices [4]. A smart substation manages power quality and reliability. Enhanced substantial progresses in system automation as earlier cited, improves the future power usage paradigm in all the power generation, storage, transmission and distribution phases. A quick, reliable and secure communication network

infrastructure and platform is critical to efficient energy system management. The network is required to link the magnitude of electric equipment in scattered locations and interchange their status data and control commands periodically and in some instances in real time [4].

The SG intelligence is practically viable if the associated data exchange amongst numerous key functional units is advantageous and reliable. The existing communication capabilities of the present energy systems are restricted to local areas that apply basic functionalities for system observation and control, such as energy line communications [4], [5] and the supervisory control, none of which meet the demanding communication desires for the automated and intelligent management in SG. Future power generation and distribution systems comprise both power generators and associated consumers that are scattered over vast areas and connected all together to form a single management network. Real-time duplex data exchanges are thus imperative to support the power system management tasks, which intermittently, need time-sensitive and data-intensive data interchange [5].

The emergence as well as gradual development of the internet, GSM based networks, satellite networks, wired and wireless local area and personal networks, coupled with the introduction of innovative networking services, and has tremendously enhanced capabilities for data and information exchanges. Nevertheless, the current networking technologies have not been leveraged or exploited enough in power systems for optimised management [5].

Although the presently obtainable networking platforms and expertise have significantly assisted in communication requirements, rolling them out to energy systems to address their specifics is a challenge. It is imperative to first identify the communication scenarios and characteristics in power systems to develop, identify and design practical usable network solutions [6]. In particular, issues relating to promptness, reliability and security are paramount. At this transitional phase of emigrating to the next electric energy generation systems, the study on the communication structural design for automatic and smart system management is still at a nursery stage. Various design and implementations such as PLC challenges are awaiting solutions [7].

The current PLC challenges in SG are harsh medium environment for data transmission and unpredictable and varying characteristics such as time, frequency and location [6]. Limited and inaccurate theoretical models of power line environment are the main technical challenges such as

- Signal attenuation
- Signal distortion
- Noise

Digital Signal Processing (DSP) is the promising key to overcoming such harsh conditions of the power line environment. Furthermore, spread spectrum technology has been identified as a detriment rather than a benefit in overcoming these challenges. Another possible solution can be the use of OFDM [7].

Various standards were developed in order to ensure reliable communications and inter-operability of PLC, especially for the SG and home networking. Examples of such standards are: CENELEC, FCC, ARIB, Homeplug etc. Power Alliance specify the ranges for operation of PLC. If a worldwide standard for PLC were to be established, this would have a positive impact on adoption of PLC. So far, the G3-PLC standard is the most robust scheme available, and the IEEE 1901.2. The working group is dedicated to developing a universally acceptable standard worldwide [8].

1.2 SG Services [8]

The main SG services include:

- Automated smart metering and reading
- Vehicle to power grid technology
- Power grid monitoring
- Demand Side Management (DSM) e.g. load shifting or demand response and energy conservation
- Networking houses between electrical devices for power administration
- Automatic meter reading.

1.3 SG Characteristics [8]

The SG is generally characterized by the following goals:

User's participation: all users will receive price signals and adjust their consumption accordingly. On demand, response program customers give authority to the utility to control their smart electrical devices in their homes. This allows the utilities to turn their devices off in case of emergency or during peak periods.

Power factor correction: if the system monitors the power factor such as current and voltage, the utility is able to identify the power grid glitches.

Incorporating all generation plants and power storage: SG objective is to incorporate distributed electrical generation plants, e.g., micro grids and renewable energies with the power grid. Thus, handling the energy produced would be easier.

Self-healing smart system: the energy grid must be able to self-heal in an automatic manner. The system will react accordingly based on the collected information. Resilience against malicious attacks: this characteristic can be given by enhancing energy grid robustness, guarding key possessions from physical attacks and in providing redundancy in the energy grid [8].

Asset managing and operation efficiency: assets quality and efficiency that are employed in the power grid will be supervised. The example of this operation is cable temperature measurements.

New market place and operations: SG will incorporate and open new trades to the power grid. For instance, it integrates IT infrastructure to the power grid.

1.4 Security Issues

A SG is generally a widely distributed system encompassing various power generation facilities to every energy utilizing equipment such as home appliances and other systems. The large-scale nature has improved the potential of distant operation of power management and distribution system and thus interceding security threats in the process [9] and ensuring security against theft and abuse of energy as well as malicious activities in SG.

Ensuring cyber security in a SG is quite a complex task mainly due to the diversity of the systems involved. Ensuring security in a SG needs uninterrupted observation to ensure that any potential attack is detected timeously and appropriate remedial action can be taken. In addition, monitoring various SG parameters can assist in identifying any suspicious, abnormal

as well as malicious activities [9]. Furthermore, having a rapid restoration plan is also important. As a recommendation, SG security mechanisms should be enforced at both the physical and logical layers. At physical layer level, SG systems and components must be secured from harm, tampering, theft, vandalism and sabotage. Examples of physical layer security include installation of fence, video surveillance, and alert system. In contrast, the logical layer in the digital data must be protected. Logical layer security mechanisms have been proposed in the literature and these include [9]:

- *Encryption*: the need to cipher the data in the SG from meter to utility centre is critical towards the prevention of snooping, hence preserving the confidentiality of data. Strong but efficient algorithms can be used; however, all SG devices, for example, meters, collectors, processors, and routers, must be enabled with encryption processing capabilities.

- *Authentication*: It is the method of determining that a user or individual is, really, the same individual as claimed. SG applications should have strong authentication capabilities, to detect and reject unauthorized connections between its components, for example, meter and the utility interfaces.

- *Applications Security Controls:* SM applications should be coded properly so that cyber criminals cannot access a meter to mount buffer overflow attacks or to embed a malware. Data validation is an example of one of the techniques that could be used.

- *Security Patches:* Security patches protect an application from known malicious attacks; consequently, codes should be kept up to date with latest patches.

- *Malware Removal:* The use of antivirus and antispyware software through the SG applications will identify and eliminate malwares from the system.

Overall security objectives include:

- *Integrity*: protecting against illegal modification or discarding of information.
- *Confidentiality*: keeping data confidential to protect privacy and misappropriation of information by an unauthorized entity. This also limits data access and disclosure.

- *Availability*: ensuring reliable access to information and services whenever such a need arises.

Availability and integrity ensure overall system reliability. However, due to the unavoidable systems communications with users, privacy is also being developed in this two-way data communication system that connects the whole system comprising SMs, data collectors, communications network, and utility data centres [10]. Overall, to ensure cyber security in SG, we need uninterrupted observation so that any possible attack can be spotted on time and action can be executed rapidly. The examples of methods planned so far to handle security concerns include a public key infrastructure, which is a mechanism that binds public keys with sole user identities by a Certificate Authority (CA). Briefly, we note that within the framework of SG, several operational as well as management goals, which have always been difficult as well as infeasible to practically resolve in conventional energy system grids, become easy and possible to solve [9] [10].

So far in this preliminary review, it was discovered that most of the research in the SG operation management objective is driven to improve power efficiency in terms of demand and supply though sophisticated automation. In the process, this leads to a secured advanced enabling management infrastructure. Such a process leads to a proliferation of extra functionalities hence more new management services and applications will emerge to enhance grid efficiency. In this research, we focus on a secured AMI in an SG environment [11].

1.5 Research Focus

Smart metering enables semi-duplex data exchange between the meters and control centers. This enables more efficient remote monitoring, as well as remote controlling of home power consuming appliances such as lights, geysers etc. It has also been established that smart metering will improve the reallocation of energy consumption, leverage the awareness of energy consumed, facilitate in energy saving and consequently lead to emission reduction. A typical AMI is gradually evolving into a conglomeration of diverse legacy systems blended with next generation expertise and associated architectural approaches, based on different standards and regulations that all need to be combined into a seamless communication network to support the challenges of the future power network. The communication between the SMs and the control centers is made through channels which are prone to security breaches. To support this objective, a wide range of security issues have to be addressed. These include [12]:

- An enabling communication infrastructure, that guarantees full connectivity to all SG elements.
- Device physical security: The individual SMs have to be secured from malicious tempering.
- Network physical security: This is to ensure robust connectivity between SMs and control centers at all times.
- Software security: This is to ensure every SM runs all its functions based on the firmware installed on the hardware and that it is remotely upgradeable without any vulnerabilities.
- Communications security: This is to ensure compatibilities with respect to the various communication environments (from physical to application layers) within the SG.
- Logical security (semantic security) to ensure reliable and secure data exchanges within the SG network.

Based on the above, the primary objectives of this research project are to:

- Survey security threats in PLC (SG) and possible solutions.
- Identify an effective security framework for an SG network.
- Explore a candidate encryption or decryption algorithm that ensures security as well as minimal latency when implemented.
- Ensure smooth data aggregation as well as its safeguarding in a SG network.

1.6 Overview of the Thesis

The focus of this thesis is on a secured PLC based energy management system in SG environment namely the AMI services critical in any SG network. Therefore, a study on the general SG infrastructure, services and their requirements is presented. The protocols used in SG network is also crucial therefore, protocols and standards are evaluated. The PLC architecture is discussed in depth and the noise characteristics of the PLC channel are simulated using MATLAB in Chapter 2. Integration of renewable sources and physical security in general, as well as theft detection and avoidances of energy in a SG are discussed in Chapter 3. Chapter 3 also introduces theft detection and monitoring systems. Monitoring requirements with regards revenue were introduced and proposed as the best theft detection and monitoring system that can be implemented. Chapter 4 was devoted

to data aggregation and logical (semantic) security. The framework to enhance SG semantic security is explained. Potential attacks, DNP security, cryptology, channel security issues are discussed. The comparison of different encryption schemes are discussed in Chapter 4 and the best encryption scheme is selected with in-depth explanation that includes the modification to suit PLC network design on the SG. In Chapter 5, the resilience of PLC is introduced where physical security, cartographic techniques, IP addressing, addressing requirements, robustness and network flexibility are discussed. The firmware diversity is also discussed together with IP address encryption. Modelling and simulation of a proposed security model are discussed in chapter 6. The simulation model to analyse security of data is executed in Chapter 6. The PLC system is modelled using Java NetBeans 8.5 compiler and OPNET to prove that it is secure and has a robust architecture. Modelling and analysis help to prove some anticipated results, objectives and outcomes of the project. If the anticipated results do not meet the design's needs, it has to be adjusted and some parameters remodelled and re-simulated.

The conclusion of this thesis is in chapter 7 where the discussion and future research are suggested.

1.7 Research Problem

The introduction of SGs technology is an excellent option but it has inherited a growing number of serious problems calling for immediate action. The increasing public health emergency and the potential for a national cyber security and hacking crisis on utility SGs are issues that demonstrate the insecure SG. The costly impact on the public will continue to grow until this problem is stopped by implementation of secure SG.

The major problem identified on the SG is the security of data transmitted on the network. If the network is insecure it becomes vulnerable to a vast number of cyber-attacks. The attacker aims to destroy the load management services by stealing and modifying private and sensitive data that is used by an electricity utility for billing purposes. SG presented gaps on the network such as data security vulnerabilities. Although it is good practice to introduce SG technology to improve power quality of supply, the use of digital technology also exposes security threats on SG system. SGs mostly have a complex network arrangement and private sensitive information which requires protection technology to secure it. Energy stealing is one of the biggest problems related to the SGs application. This research discusses SG security technologies problems that are identified, and offers possible effective solutions. There is need for a robust communications protocol to implement

security functionalities that overcome SG security challenges. The solution is encryption of messages and minimizing delays caused by cryptographic processes, and guaranteeing integrity of these messages with negligible latency. The summary of problems identified are listed below [13]:

- Overcharging customers due to data inaccuracy.
- Denial of quality of service (QoS).
- Reliability SG network problem caused by insecure system.
- Privacy invasion crisis on AMI.
- Interference with electronics (eavesdropping).
- Intruders hacking the system (cyber-security problem).
- Remote disconnection of power causing major disruptions.
- Environmental costs.
- Problem of control of household electrical use.
- Burdensome and excessive costs.
- Costs exceeding benefits.
- Fraudulent claims and unavailable information.

1.8 Approach to Solving Problem and Methods

Secure information storage and transportation are extremely vital for power utilities, especially for billing purposes and grid control. To avoid cyber-attacks, efficient security mechanisms should be developed and standardization efforts regarding the security of the power grid should be made [14]

IEC 62351 defines cyber security for the communication protocols defined by the previous four sets. Security is a major concern with SGs, which are especially vulnerable to attack because of the two-way communication between devices and the utility grid [15].

1.8.1 Survey on Advanced Metering Infrastructure AMI

A comparative study and investigation is conducted on the current AMI security schemes. This survey looks at performance of the current security schemes that are utilised by the electricity utilities to conduct load management activities for efficiently running the power grid. Power Line Communication is intensively investigated on how it transmits data and its security protocols. The survey is conducted on Advanced Metering Infrastructure system including PLCs, SG protocols

used etc. The PLC infrastructure is also investigated on the security feasibility due to the load management aspect. The theft detection avoidances approach is also investigated [16].

1.8.2 Investigating and Enhancing Semantic and Physical Security for SGs

Sematic security framework conceptual design cryptology model was implemented. The SMs attack detection scheme was introduced to improve security by preventing the attacker from compromising the SM. The current sematic security is intensively investigated in order to identify any existing security gaps. Using these gaps the new security framework and security rules is created. A framework on how to enhance physical and sematic security is crucial in order to have a stable load management system.

1.8.3 Testing Current Available Security Schemes and Encryptions

The data transmitted from the SM was simulated to test the protocols. The test was for protocols data security, robustness and integrity. The security schemes such as authentication, encryption, data speed and bandwidth required are tested. The simulation tool such as OPNET JAVA and MATLAB were used to test the integrity of the encryption of the data on AMI system. After the test has been conducted on few selected security schemes and encryption protocols the best encryption scheme will be selected based on the encryption speed, resilience and robustness of the protocol. The encryption allowable key must not be less than 128 bits.

1.8.4 Resilience and Robustness in PLC Systems Study

PLC is a part of Advanced Metering Infrastructure and SG. Since PLC is a network that is already available, it can be integrated easily onto the AMI. This is thoroughly investigated. Channel noise, modulation scheme i.e. OFDM, data speed as well as the bandwidth are investigated

1.8.5 Modelling and Simulation

This section models and analyses the security scheme used to prove data integrity. Modelling and analysis of a proposed scheme ensures resilience and robustness. Simulation is performed to prove the concept claimed.

1.8.6 Summary Conclusions

To conclude the chapter, it is noted that a SG is a modernized grid system that manages power demand in a sustainable, reliable and economic manner, built on advanced infrastructure and tuned to facilitate the integration of all involved. The SG provides more power to meet rising demand,

increase reliability and efficiency of power supplies and at the same time will be able to integrate low carbon energy sources into power networks. SGs possess demand response capacity to help balance electrical consumption with supply, as well as the potential to integrate new technologies to enable energy storage devices and the large-scale use of electric vehicles.

The duplex communication helps in matching demand versus supply. Key SG services include:

- Automatic meter reading.
- Power grid monitoring: peak voltage, peak factor, and a degree of synchronisation as well as current levels in the power grid structure supervised in real time.
- Demand Side Management consists of two parts:
    - Load shifting.
    - Power conservation.
- Home networking amongst electrical appliances for power management.
- Vehicles power technology: The power stored in charged cars can be put back to the power grid.
- Self-healing system: the SG system should be able to heal automatically.
- Flexibility to counter attacks: increasing power grid robustness, protecting key assets from physical attacks and improving flexibility.
- Equipment management and performance efficiency: the state of all equipment and operational efficiency can be monitored.

Security and access control is also a threat in such systems. Key related problems include:

- Overcharging customers due to data inaccuracies.
- Denial of quality of service (QoS).
- Intruders hacking the system (cyber-security problem).

2 Smart Grid Architecture and Communications Infrastructure

2.1 Background

As emphasized in chapter one, the SG generally enables utilities to efficiently and economically balance out power consumption by re-distributing loads around to where there is relatively more demand. In that way, the utility can also maximise power feed as well as reduce consumption [17]. Electronic billing for customers is made possible through the AMI system. In this chapter, we review the protocols, SMs architecture and security issues that could adversely affect the AMI system implementation. Firstly, we look at the general SM architecture, followed by a discussion and review on the state of the art of AMI systems and related security aspects. Transmitting of data via PLC has long been practised, but it was never done on a large scale for both commercial and non-commercial purposes. The energy sector for long has used this facility in isolation [18]. A typical PLC system is illustratedin Figure 2.1.

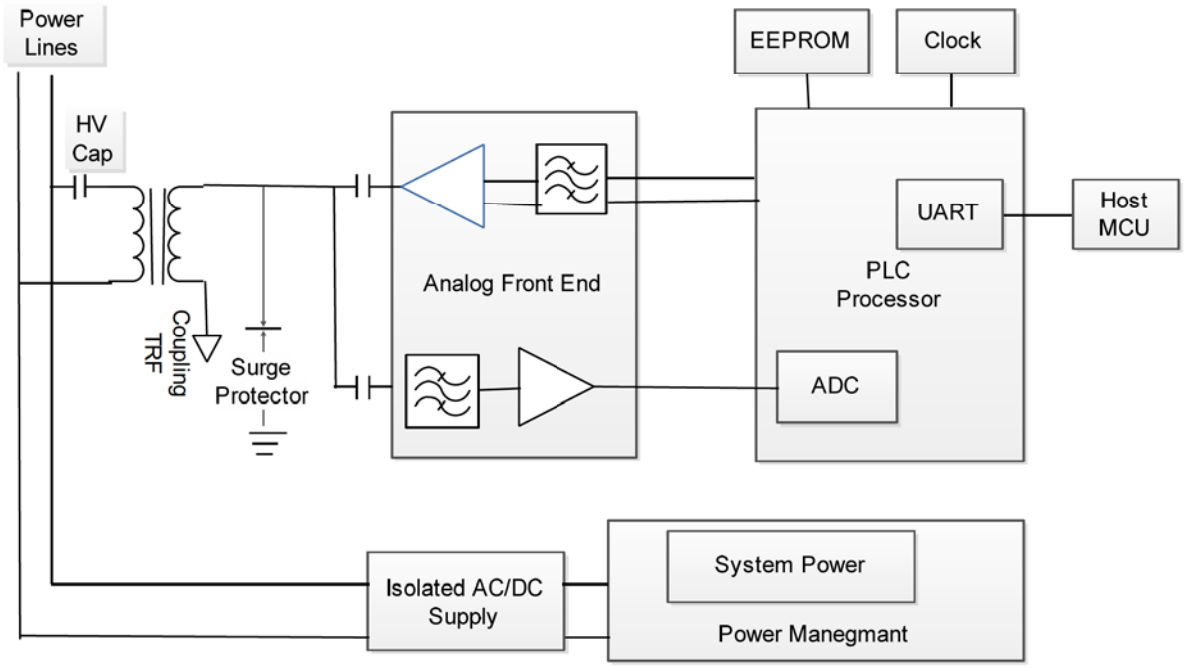


Figure 2-1 PLC System Block Diagram [19]

It comprises a coupling transformer (TRF), surge protector, analogue front end, PLC processor, power management circuit, as well as AC/DC supply. The Electrically Erasable Programmable

Read-Only Memory (EEPROM) and Clock are incorporated in the processor. A Universal Asynchronous Receiver/Transmitter (UART) capability makes it possible for the system to communicate with the host MCU via RS 232 C [19].

There are numerous reasons that hamper PLCs from being a common choice as SG communication platform. These include [20]:

- The fact that power is sent to the consumer from the generation station via three stages.
- Transmission of data through three different voltage levels e.g. high voltage (HV), medium voltage (MV), as well as low voltage (LV) intricate the use of PLC as a data transmitting platform.
- Unipolar coded data signals introduced to a power line cannot traverse a transformer since this is AC coupling and thus the DC components of the data signals will discard.
- Introduce bypass equipment across transformers to facilitate DC coupling will escalate costs as well as increase overall design and structural complexity.
- The transmission and distribution losses of energy lines secludes PLC network.
- The impulsive noise reduces the data signal quality by introducing additive noise into the system.
- Since power lines at high frequencies are not insulated, they exhibit themselves and act like antennae and for that reason they ultimately interfere with generated signals from high tension wires nearby.

Current power grids are almost becoming obsolete and require upgrading. Because the multiple and frequent failures associated with them pose a national security threats as well as economic instabilities [21]. Modernising them by introducing SG architectures will provide effective solutions to the problems currently posed. A resilient communication network implementation on the power grid will ensure a robust power management system. If the distributive generation is included on the system, it will reduce the peak load demands on the central energy generation side. In doing so, the grid separates itself from the affected segment [22]. The different modes of communication within the SG are shown in Figure 2.2. Note that it the communication medium is in a way interface between the generator and the power consumer (user).

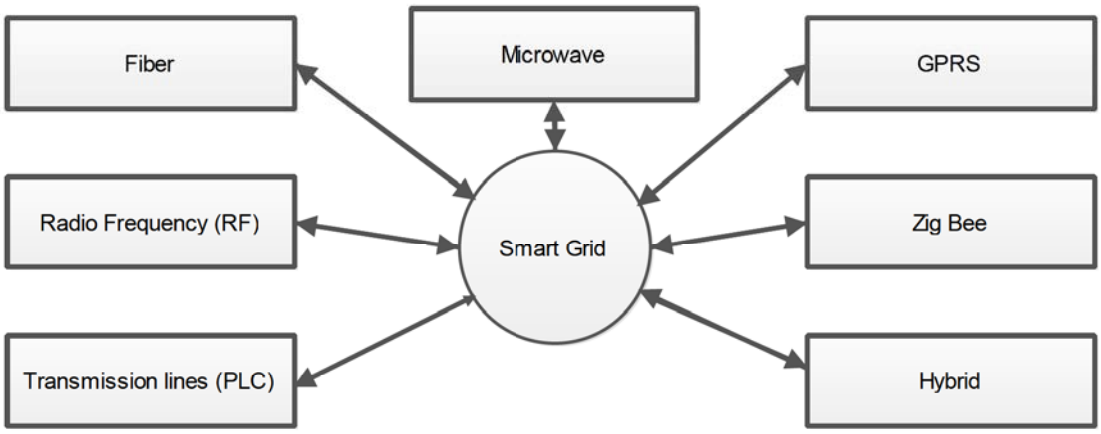


Figure 2-2 Alternate Communication Medium for SG [23]

The power and data flow in the current power grid emanate or originate from generating sites and terminate at the consumer end. As such the use of SMs has numerous advantages over conventional meters as there exists a defined communication interface between the power grid and consumer. Summarily these advantages include [24]:

- Remote or distant meter reading.
- Control over the appliances through remote site.
- Live tracking of electricity changes and current load.
- Programmable duration and timing of device operability.

SG technology has a choice to join all transmission interfaces directly to the sources or can be controlled via the central grid. In that way all communication between transmission interfaces and that of the consumers are bi-directional [25]. Selection of the best suitable data transmission medium to support SG, can be made from the various available transmission technologies depending on the utility's design and requirements [Figure 2.2]. In this work, PLC is selected and ultimately we will incorporate security enhancements so that it reliably delivers power loads through a secured load data management system. It is a candidate for the solution of this power deployment constraint [25]. As such PLC related applications make use of varying frequency spectra as well as data rates depending on the technology choices and requirements. Its introduction undoubtedly brings about excellent technology improvements, but there are a number of complications that also emerge as result of its implementation, i.e. data security [26]. An analog SM system architecture is shown in Figure 2.3.

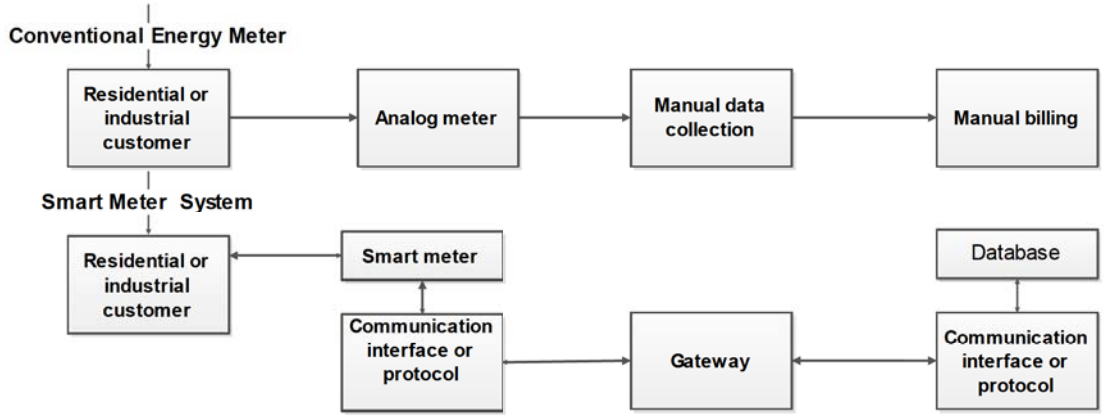


Figure 2-3 Analog and SM Block Diagram [27]

As cited before, we will investigate PLC related challenges together with various security protocols at various levels in order to derive a solution for them. The associated data shall be safeguarded by encryption and authentication. By way of simulation, it will be demonstrated, that such networks can be securely utilized in load management. We will consider utilizing Advanced Encryption Standard (AES) based encryption techniques to secure data efficiently [27].

2.2 PLC Cable Transfer Function

Power line cables mostly comprise of three conductors namely, live, neutral, and earth. Any two of the three conductors can be used for data communication. In most cases, since live and neutral have equal wire gauging; they are therefore used for power line data communications, but is also possible to use other combinations as well. Overall the two conductor PLC system can be modeled as a two port network. Whose transfer function is modeled using chain matrix ABCD theory [28]. As such the ABCD matrix can be used to calculate the transfer function of the system and consequently compare it with existing theoretical results [29]. An illustration of a two port network connected to a voltage source and load is shown in Figure 2-4

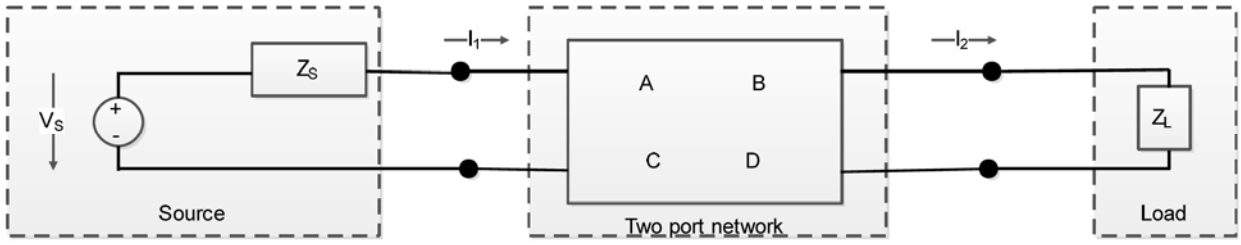


Figure 2-4 Two port Network Connected to a Voltage Source and Load [30]

2.2.1 Modelling

To carry out the calculation of ABCD representation of two-port circuit we follow the approach in [31]. The output voltage and the current of a two port circuit can be expressed as;

$$\begin{bmatrix} V_1 \\ I_1 \end{bmatrix} = \begin{bmatrix} A & B \\ C & D \end{bmatrix} \begin{bmatrix} V_2 \\ I_2 \end{bmatrix} \tag{1}$$

Where;

A, B, C and D are the constants chosen. It becomes simple to show that if for a given a set of cascaded two-port circuits, the resulting ABCD constants are simply derived from the product of the individual sets of ABCD matrices. Looking at figure 2-4 and using the ABCD model for the two-port circuit, it is easy to calculate the transfer function of the circuit as well as input impedance Z_1 [31] as follows;

$$H = \frac{V_L}{V_S} = \frac{Z_L}{AZ_L + B + CZ_LZ_S + DZ_S} \tag{2}$$

The input impedance of two port circuit Z_1 can be calculated using equation 3 as follows;

$$Z_1 = \frac{V_1}{I_1} = \frac{AZ_L + B}{CZ_L + D} \tag{3}$$

Its known from basic circuit theory that, two parallel cables can be modelled as a transmission line and as such the resulting system can be can be characterized by a characteristic impedance Z_C.and propagation constant is γ.The characteristics impedance Z_C and the propagation constant γ are respectively calculated from 4 and 5 as follows;.

$$Z_C = \sqrt{\frac{R + j\omega L}{G + j\omega C}} \tag{4}$$

$$\gamma = \sqrt{(R + j\omega L)(G + j\omega C)} \tag{5}$$

Where;

R, L, G and *C* are, per-unit-length resistance (Ω/m); inductance (*H/m*), conductance (*S/m*) and capacitance *(F/m),* respectively, and ω is angular frequency (*rad/s*).

$$\begin{bmatrix} A & B \\ C & D \end{bmatrix} = \begin{bmatrix} \cosh(\gamma l) & Z_C sinh(\gamma l) \\ \frac{1}{Z_c} sinh(\gamma l) & \cosh(\gamma l) \end{bmatrix} \tag{6}$$

If we replace the bridge tap with the equivalent impedance Z_{eq}; which can be seen from terminals A and B; then the circuit can be simplified and Z_{eq} can be calculated as depicted in equation 7

$$Z_{eq} = Z_C \frac{Z_{br} + Z_C \tanh(\gamma_{br} d_r)}{Z_C + Z_{br} \tanh(\gamma_{br} d_r)} \tag{7}$$

where,

Z_C and γ_{br} are characteristic impedance and propagation constant of the branch circuit. For each sub-circuit, it is possible to calculate an ABCD matrix (Φ_i $i = 0, 1, 2, 3$) and the ABCD matrix for the total circuit Φ [32]; is shown is equation 8.

$$\Phi = \prod_{i=0}^{3} \Phi \tag{8}$$

where,

$$\Phi_0 = \begin{bmatrix} 1 & Z_S \\ 0 & 1 \end{bmatrix}, \Phi_1 = \begin{bmatrix} \cosh(\gamma_1 d_1) & Z_1 sinh(\gamma_1 d_1) \\ \frac{1}{Z_1} sinh(\gamma_1 d_1) & \cosh(\gamma_1 d_1) \end{bmatrix}, \Phi_2 = \begin{bmatrix} 1 & 0 \\ \frac{1}{Z_{eq}} & 1 \end{bmatrix}$$

$$\Phi_3 = \begin{bmatrix} \cosh(\gamma_1 d_1) & Z_2 \sinh(\gamma_2 d_2) \\ \frac{1}{Z_2} \sinh(\gamma_2 d_2) & \cosh(\gamma_2 d_2) \end{bmatrix}$$

Z_1, γ_1, Z_2 and γ_2 are the characteristic impedances and propagation constants [32]. The equations for the ABCD matrix elements for the circuit of Figure 5 are given by

$$A = \cosh(\gamma_2 d_2)\alpha + \frac{\sinh(\gamma_2 d_2)}{Z_2}\beta \tag{9}$$

$$B = Z_2 \cosh(\gamma_2 d_2)\alpha + \cosh(\gamma_1 d_1)\beta \tag{10}$$

$$C = \cosh(\gamma_2 d_2)\xi + \frac{\sinh(\gamma_2 d_2)}{Z_2}\vartheta \tag{11}$$

$$D = Z_1 \cosh(\gamma_1 d_1)\xi + \cosh(\gamma_2 d_2)\vartheta \tag{12}$$

where,

$$\alpha = \cosh(\gamma_1 d_1) + \frac{Z_s}{Z_2} \sinh(\gamma_1 d_1)$$

$$\beta = Z_1 \sinh(\gamma_1 d_1) + Z_s \cosh(\gamma_1 d_1)$$

$$\xi = [Z_1 \cosh(\gamma_1 d_1) + Z_S \sinh(\gamma_1 d_1) + Z_S \sinh(\gamma_1 d_1)]/(Z_1 Z_{eq})$$

$$\vartheta = [Z_1 \sinh(\gamma_1 d_1) + Z_S \cosh(\gamma_1 d_1)] \; / Z_{eq} + \; \cosh(\gamma_1 d_1)$$

Then, by using equation 2, the circuit transfer function can be calculated. For channels with more bridge taps, the calculation of the resultant channel transfer function is done using a similar approach.

2.3 PLC Channel

A PLC channel consists of two different bands, namely narrowband and broadband. The narrowband PLC network channel currently under scrutiny in terms of its candidacy for data transmission. Generally, it provisions a reserved low data speed in the order of kilobits per second just for data management and control and that sufficing for smart metering. This implies that it has less bandwidth while the broadband band as expected has a much wider bandwidth [33]. The electrical cables between the substation and the customer are used as an access channel for data services. PLC have substantial signal quality problems as well as a huge interference on the transmission line itself. The effect of signal attenuation and signal cross coupling are investigated [34]. A typical PLC AMI is shown in Figure 2.5.

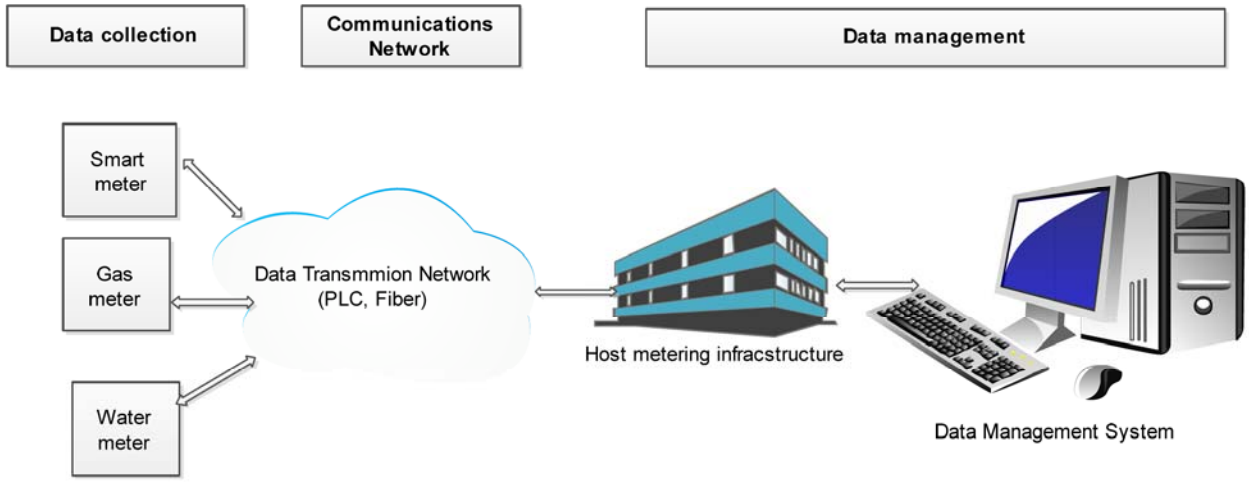


Figure 2-5 AMI [35]

The SMs are all connected to a data concentrator; whilst the data concentrator Coupling Unit (CU) is connected to a Data Management Centre (DMC) using a backbone network. A star topology configuration is often advocated. We recall that a SM's primary function is to bring data to utility

enters using a duplex communication network as well as provide load management e.g. remote controlling of user appliances such as geysers, air conditioners and lights[36].

It however suffers from signal interference as indicated before. This interference leads to signal frequency fading or attenuation. The distance between the SMs and the concentrator needs to be regulated or chosen appropriately commensurate with desired performance e.g. speed and low loss probabilities of the data. Notably power line links characteristics resemble those of a low pass channel up to ranges of about 300 meters and the characteristic resemblance diminish once this length is exceeded. The length limit can be different on various network types depending on the network topology. The extended network branches are liable for aggregating attenuation on the PLC network [36], [37].

As the nature and type of communication medium is a key component of the SG or for any data transmission network, there exist numerous communications platforms and technology standards that the load management utilities can utilise. Typically we have: Wireless - ZigBee, GSM, GPRS, 3G, WiMAX, RF and wireless mesh, wired - ADSL, fibre, copper and PLC [38]. These are further tabulated next.

Table 2-1 Smart Grid Communications Technologies [39]

Technology	Spectrum	Data rate	Coverage range	Application	Limitations
GSM	900-1800MHz	Up to 14.4 kbps	1-10 Km	AMI, Demand Response, HAN	Low data rate
GPRS	900-1800MHZ	Up to 170 kbps	1-10 Km	AMI, Demand Response, HAN	Low data rate
3G	1.92-1.98 GHz 2.11-2.17 GHz	384 kbps-2Mbps	1-10 Km	AMI, Demand Response, HAN	Costly spectrum fees
WiMAX	2.5-Ghz, 3.5GHz, 5.8 GHz	Up to 175 Mbps	1-50 Km	AMI, Fraud Detection	Not wide spread
PLC	1-30Mhz	2-3 Mbps	1-3 Km	AMI, Fraud Detection	Harsh noise channel environment
ZigBee	2.4GHz and 868-915 MHz	250 kbps	30-50 m	AMI,HAN	Low data rate, short range

Conclusively we note that out of the tabulated technology platforms, PLC is chosen as the better candidate because as it has a direct connection to the meters. It is also cost effective and the infra-

structure is readily in existence and widely available. Moreover it is a technique that utilises existing power lines to transfer data at relatively modest speeds [39]. The choice was based on the following [40]:

- Protocol suitability- How suitable is the protocol to be used in PLC network.
- Smart metering support - How PLC supports smart metering?
- Bandwidth- How big the band is and how it is suitable for PLC data transmission.
- Security implementations- Is it feasible to implement security rules on the PLC network.
- Integrity- Consistency, accuracy, and trustworthiness of data. The data must not be changed while in transit.

To wind up this section, we note that energy flows over power lines at 50 Hz. Data signals can be injected in the spectrum above the 50Hz. The injection of high frequencies on the power lines will lessen interference from them as is the case currently. The usable spectrum can also be used for voice alongside data. PLC systems can be designed for narrowband or broadband and its spectrum generally flexes from 1–30MHz [41], [42]. Shannon's Theorem states that the bandwidth can be megabits per second (Mbps) of throughput, which is dependent on the Signal-to-Noise Ratio (SNR) [43] as well as the type coding. Specifically certain coding techniques have much higher spectral efficiencies (bits/Hz). Sharing the network equipment and infrastructure leads to congestion, interference and data security problems. To overcome these problems, solutions rely on sophisticated signal processing and encoding. Orthogonal Frequency Division Multiplexing (OFDM) can be used to overcome PLC network signal problems. It enhances spectral efficiency and robustness against signal interference. Noisy electrical networks are a major concern [44]. It also uses adaptive encoding techniques to balance signals across diverse frequencies channels to overcome variances in the infrastructure and random sources of noise. Medium Access Control (MAC) protocols like Carrier Sense Multiple Access and Collision Avoidance (CSMA/CA) as well as other methods such as Time or Frequency Division Multiplexing (TFDM) [45] can be used.

Narrow Band Power Line Communication (NB-PLC) technologies are used widely in smart metering all worldwide [45]. Frequencies that are below 500 kHz are characterized as low signal weakening and attenuating, whereas those that are more than 1 MHz are highly attenuated due to

the capacitive coupling to earth [46]. NB-PLC signal travel long distances underground, compared to the Broad Band Power Line Communication (BB-PLC). In Europe, frequencies between 9-95 kHz (CENELEC A) are restricted for use in applications that monitor and control the low-voltage distribution network. The most used PLC technologies for smart metering use frequency shift keying (FSK) or Spread- FSK as specified in the IEC 61334 standard [46].

2.4 PLC Standards

Standardisation is key to PLC implementation and as such they are being they are utilised to calibrate parameters such as usable frequencies, signal, security of the network and other parameters. Standards organisations such as ITU, IEC, ISO, IEEE, e.tc. They regulate on how the technologies are deployed on PLC networks. e.g., standards such as G3 and IEEE P1901 focus on robustness of such networks [47].

The environment where PLC operates is prone to various kinds of interferences. The robustness of G3 to withstand noise makes PLC the choice for worldwide deployments. G3 standard is managed by the G3 Alliance. It operates on the of 3-95 kHz band. It is bi-directional and its data rate ranges from 20–40 kbps in the A-band. G3 uses OFDM modulation scheme to offer high protection against interferences and signal attenuations [50]. PLC technologies support DLMS/COSEM and offer 128-bits AES for Cypher block Chaining Message (CCM) for extra data transmission security.

Higher data rates requirements have prompted further research such as re-visiting existing NB-PLC solutions. The Power line Related Intelligent Metering Evolution (PRIME) Alliance was introduced in 2007 and it has so far detailed an NB-PLC resolution based on the OFDM, working in the CENELEC A band. It is capable of attaining up to 128 kbps with no FEC and 61.4 kbps with FEC.

The design objectives of G3-PLC designers focused on developing a robust Physical Layer (PHY). Furthermore, the G3-PLC specification re-uses the existing standards with the MAC layer based on IEEE 802.15.4. The first international standards on the next-generation of OFDM-based NB-PLC to be approved were ITU-T recommendations G.9955 (2011) and G.9956 (2011). These two recommendations contains the PHY and Data Link Layer (DLL) specifications respectively for the three NB-PLC technologies. Also the IEEE pursued the standardization of OFDM-based NB-PLC and this project started in 2010 with the launch of the IEEE P1901.2 projects, which were sponsored by the IEEE communications society [51]. The IEEE 1901.2 standard is based on G3-PLC, and

specifies only the PHY and MAC layers. Thus, bootstrapping, authentication and routing are not defined. IEEE 1901.2 also includes a standalone mandatory clause and NB-PLC coexistence mechanism that allows non-interoperable NB-PLC technologies to share the same frequency band [51]. The NB-PLC specified technology in ITU-T G.9903, ITU-T G.9904 and IEEE 1901.2 shows resemblances. Despite the resemblances between ITU-T G.9903 and IEEE 1901.2, there are differences that make the two NB-PLC technologies non-interoperable. The core differences are: MAC support 1280-Byte MTU in 1901.2 instead of 511-Byte MTU for G3-PLC. An additional super ROBO mode in IEEE 1901.2 repeats six times the data, while G3-PLC uses it only for the Frame Control Header (FCH). G3 uses information elements frames whereas IEEE P1901.2 is limited to PHY and MAC layers [52].

2.4.1 X-10 Technology

The X-10 is an old technology approach that has been used extensively on the PLC network. It uses Amplitude Shift Key (ASK) modulation. X-10 uses power line carrier technology to allow the devices to communicate with each other using the existing wiring in the house. It uses 120 kHz carrier timed with 240 VAC power line and zero crossing to represent digital data [52]. This technology is quite universal and has always been popular for lone homes. This protocol was initially unidirectional and eventually its latest version was improved to be bidirectional. The main reason why this technology has limitations is due to the poor bandwidth handling. Its transmission rate is 60 bps but reduces to an effective20 bps due to retransmissions and line control. The low data rate limits this protocol's ability to perform more sophisticated functions. Its main advantage is that of easy installation as well as relatively low implementation costs [53].

2.4.2 Home Plug

Home Plug Alliance was founded by a group of industry companies. In March 2000 Home Plug specification was developed. The baseline technology selected in June 2001 was Home Plug 1.0 followed by Home Plug AV in February 2003. In January 2004, Home Plug BPL was developed [54]. There are four main Home Plug specifications listed as follows [55]:

- Home Plug Command & Control is a low speed and low cost technology.
- Home Plug 1.0 is a specification for data transmission for home appliances through power lines at a data rate of up to 14 Mbps.

- Home Plug AV is a home plug technology that is designed to handle multimedia data.
- Home Plug BPL is a home plug technology designed to handle high-speed data and it can be used for internet access.

2.4.3 Home Plug 1.0

Power lines are originally meant to distribute power at 50-60Hz. Due to advances in technology, the power lines were also used to carry data. The utilization of this medium for data communications at higher frequencies that are more than 50Hz poses new challenges [56]. They are mostly made up of different types of conductors and terminated at the load side with varying magnitudes of impedances. For this reason, frequencies and the signal can reach the receiver with very little signal, but other frequencies can be pushed to reach the noise amplitude. The PLC networks are also sensitive to external noise and interferences [57]. There are a few types of appliances that introduce noise on PLC such as transformers, switching power supplies and halogen lamps. This noise reduces the integrity of the signals transmitted on the network. Home Plug 1.0 equipment overcomes these problems by utilising an adaptive method. Robust transmission method, combined with FEC and Automatic Repeat Request (ARR), are employed. OFDM (which we discussed earlier) is also used as a modulation technique in the Home Plug 1.0 [57].

2.4.4 Home Plug AV

Home Plug AV (HPAV) is a recent specification standard by the Home Plug Power Line Alliance. Its main drive is to offer high quality multimedia data communication and networking over existing power line inside homes. HPAV uses advanced PHY and Me MAC technologies that run at 200 Mbps for video, audio and data streaming [58]. The Physical Layer uses 200 Mbps to deliver a 150 Mbps data rate with strong communications capability over noisy power line. The MAC layer is intended to support both Time Division Multiple Access (TDMA) and Carrier Sense Multiple Access (CSMA) on AC line cycle synchronization. The TDMA offers a very good Quality of Service (QoS). HPAV uses 128-bits AES to offer high data security [59]. HPAV is reverse compatible with Home Plug 1.0 and gives numerous modes that enable multi-network process and BPL. HPAV is an excellent network for the transmission of High Definition (HD) data and entertainment that includes HDTV, SDTV and audio at home [59].

2.4.5 Home Plug Physical Layer

We mentioned in the previous sub-section that OFDM is used in Home Plug technology specifications and its primary function is to divide the available spectrum into a number of narrowband and low data speed usage sub carriers. Consequently each narrow band sub carrier can now be modulated using various modulation formats. If the sub carrier selects the arrangement spacing as small, by doing so, the channel transfer function decreases to a constant within a sub carrier bandwidth. In this manner, frequency channels are divided into various sub-channels, which eliminate the need of equalizers. OFDM uses 84 equally spread-out small carrier bands between 4.5 MHz and 21 MHz The cyclic prefix and various modulation methods such as Binary Differential Phase Shift Keying (BDPSK) and Differential Quadrature Phase Shift Keying (DQPSK) are used to eliminate the necessity for any equalization. The channel noise is removed by FEC and data interleaving [60].

2.4.6 Home Plug MAC Protocol

The associated MAC protocol has a wide range of implementing challenges. Home networks must be able to support various applications starting from a small file transfer to very high QoS demanding applications. The Home Plug MAC is designed to combine with the already existing physical layer MAC protocols and together address QoS requirements. It has been successfully tested for compatibility with the IEEE 802.3 frame structure. Generally it encrypts the Ethernet frames prior to tunnelling them over the power line. A de-assembly and reassembly approach is utilised if the whole packet cannot be fitted into a single frame [61], [62].

2.4.7 CEBus

The Consumer Electronics Bus (CEBus) standard was developed by Electronics Industry Association EIA for home automation networks. The EIA 600 defining a CEBus is an open standard. Since CEBus is an open standard, anyone can develop equipment and use this protocol. Generally the standard uses 230V AC power line, Twisted Pair (TP) cable, coaxial cable, Radio Frequency (RF) and Infrared (IR) [63]. It uses spread spectrum techniques to overcome data transmission barriers that are almost found at home electrical power line. The spread spectrum signal function is to spread transferred signal over different frequencies, instead of only one frequency. The CEBus power line carrier sends data signal in a series of frequencies between 100Hz to 400Hz and uses a language called Common Application Language (CAL) as defined by EIA-600 standard. The 10 kbs data communication provides serial communication and control of devices. The CEBus uses

packets on peer to peer home automation using CSMA/CDCR protocol. The CEBus commands are based on CAL. The CAL is an application to application programming language. The commands are specific e.g. volume up, volume down, play pause and some other command for energy management. There are two CEBus channels namely: data and control channel. The control channel is used to execute controls such as trip the geyser breaker. The data channel is used for data transmission like collecting the consumer daily consumption. To prevent tampering with the communication link, the CEBus uses authentication service and ensures privacy through data encryption [64]. The CEBus implementation of ISO/OSI communication protocol and its layers is depicted in Table 2.2.

Table 2-2 CEBus OSI Protocol Layers [65]

Layer	OSI
7	Application
3	Network
2	Data Link
1	Physical

The CAL operates on the application layer that includes the data interpretation and the data content architecture. The application layer contains data transport and its purpose is to form the Application Protocol Data Unit (APDU), data encryption, authentication and an end to end acknowledgment facility. The network layer's function is to make and parse Network Data Protocol Unit (NPDU), media data channelling and segmentation services. Data link layer also uses the NPDU and it deals with CSMA protocol for error detection and data transportation. Data link accepts the data packets and projects the duplicates of these packets. Data link also maintains the node and system address. The Physical Layer handles the medium interface, symbol encoding and decoding [66].

The CEBus packet frame format for power line is shown in Figure 2.5.The preamble eight bits are sent at the start of the frame and comprise a random number utilised for collision detection. The Data Link Protocol Data Unit (DLPDU) is used to determine the packet type, the priority of the packets and Data Link Layer (DLL) class. The DLPDU also encompasses sender and the receiver addresses [66]. The NPDU is made of APDU, data routing and the data segmentation information header. The APDU is created by data transport sub-layer.

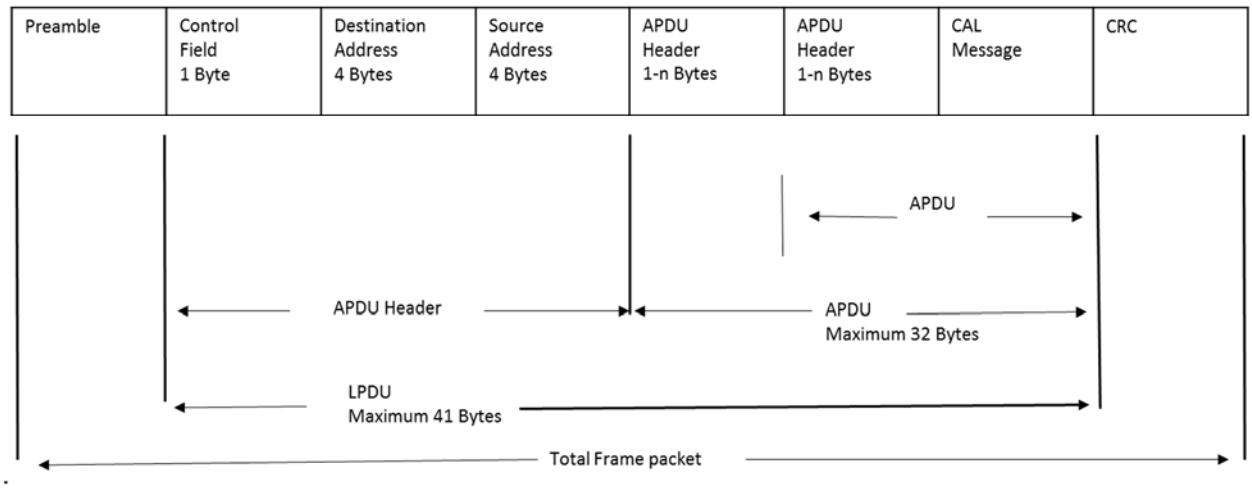


Figure 2-6 CEBus Frame Structure [67]

The field at the end of the frame of CEBus is called Frame Check Sequence (FCS) and is appended by DLL and it provides packet error detection [67]. The CEBus protocol stack is depicted in Table 2.3.

Table 2-3 CEBus Protocol Stack [68]

OSI Layer	Function
Application	CAL interpreter Context Data Structure
Network	Build/Parse APDU, End to End ACK service, Message Authentication and encryption
Data link	Build/Parse APDU, CSMA Product, Error detection and retransmission
Physical layer	Medium Interface, Symbol timing and encoding

2.4.8 The Local Operating Net (LON)

LON technology was developed around 1990 by Echelon Corporation [69]. This technology provides a peer to peer communications protocol. LonWorks is used for industrial and smart technology supervision. It also supports a big range of communication mediums, and the PLC is one of them. This protocol is CSMA based on Ethernet Local Area Network (LAN) using CSMA which are interconnected by a broadcasting transmission channel, so that if an adapter sends a frame, all adapters that are on the LAN can acquire the same frame. Summarily a CSMA/CD mechanism's features are as follows; [70]:

- A node may transmit data any time.

- A node not transmit data if the carrier senses data is being transmitted by another adapter (carrier detect).
- A node terminates its communication if it detects another adapter transmission (collision detection.)
- Before trying to re-transmit, the node will wait for a random time that is less compared to the time taken to transmit a frame.

LonWorks uses narrow band spectrum modulation scheme using the frequency band from 120 to 140 kHz. The present noise on the channel is prevented by the use of multi bit correlation and panted noise cancelation. LonWorks uses MAC protocol and Lon Talk. OSI protocol comprises all seven layers. The seven layers are: Application layer, Network layer, Transport layer, Session layer, Presentation layer, Data link layer and Physical layer [71]. The OSI model layers are listed is Table 2.4.

Table 2-4 OSI/ISO Reference Model [72]

OSI	OSI Layer	Purpose
7	Application	Network Process Application
6	Presentation	Data presentation and encryption
5	Session	Session control (Control and Disconnect)
4	Transport	Delivery and sequencing
3	Network	Routing data to destination
2	Data Link	Media Access Control (Physical Addressing)
1	Physical Layer	Hardware

Lon Talk protocol uses all the seven layers and it is thus a robust as well as versatile protocol.

2.4.9 PLC Technologies Comparison Analysis [73]

A summary legacy PLC technologies and their comparisons is provided in Table 2.5.

Table 2-5 PLC Technologies Comparisons [19]

Technology	Frequency	MAC	OSI Layer	Data rate	Communication	STD	Cost
X-10	50Hz	-	-	20-60 bps	Duplex	Open	Low
CEBUS	Spread spectrum	CSMA/CDCR	Four layers	10 kbps	Duplex(Peer to Peer)	Propriety	High
Lon Works	Carrier frequency dependent	Predictive CSMA	All seven layers	3-5.5 kbps	Duplex	Open	High
HomePlug	DCSK spread spectrum	Adaptive back off Algorithm	MAC Net3work layer	1.2-7.5 kbps	Duplex	Open	Low

This table mainly highlights on technological limitations. Performance parameters of interest used in the comparisons are communication data rate or bandwidth, cost and standards. Lately the attention of PLC has moved to low-frequency narrow band PLC which operates below 500 kHz and a sustainable data speed of about 500 kbps. This band is mostly utilised for control and automation. As such the PLC network is a potential competitor of wireless communication. However comparatively the evolving of PLC related technologies is sluggish in comparison to that of wireless technologies mostly this being attributed to problems of channel modelling [75].

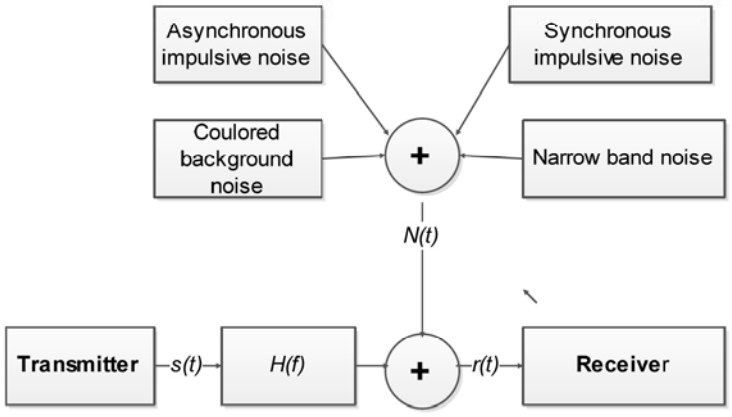


Figure 2-7 Noise Introduced on the Channel [76]

Background noise is always present in any data transmission network and it originates from various electronic components used to build the communications hardware [77]. It is quantified by the notion of power spectral density (psd) and can generally be expressed as:

$$A(f) = A_{\infty} + A_0 e^{\frac{-f}{f_0}} \tag{13}$$

where

A_∞ is the power spectral density for frequency, f $\rightarrow\infty$.

A_0 is the power spectral density at 0-50Hz.

As such, this equation enables us to model background noise as a white noise process. In addition, we can also take into consideration, short wave range narrow-band noise which mainly originates from nearby and interfering broadcasting stations [77]. The latter (narrow-band noise) can be modelled as a sum of multiple sine wave noise with different amplitudes as shown in equation 14:

$$n(t) = \sum_{i-1}^{N} A_i(t)\sin(2\pi f_i + \varphi_i) \tag{14}$$

where

N is the number of waves each with a distinct f_i amplitude $A_i(t)$ as well as phase φ_i. The amplitude $A_i(t)$ is a constant. The phase φ_i takes arbitrary values within intervals [0; 2π]. Asynchronous impulsive noise is characterized by both high and short spikes of voltages with durations up to 100 micrometres. These can reach 2 kV levels. It originates from switching equipment in the network. In addition we also have synchronous impulsive noise which derives from thyristors in light dimmers [77].

Generally, the noise interference problem is quite an intricate one as it encompasses contributions from a range of source types such as broadband and narrowband interference as well as other diverse forms of impulsive disorders that occur as shown in Figure 2.6. The harshness of the networks makes PLC network modelling a challenge, e.g. due to frequency mismatches caused by reflections and in addition, the presence of high signal attenuation and huge low pass characteristics that limit bandwidth. Besides these problems they are more weakened by background noise and consequently an extensive study on channel noise characterisations quite crucial in order to ensure more accurate channel modelling results [77], [78]. As it is exposed and prone to high levels of noise interference. Such communication channels do not represent Additive White Gaussian Noise (AWGN) channel.

2.5 PLC Channel Attenuation

Once again it is reiterated that a PLC based network is a cost effective solution since it uses available infrastructure. Numerous aspects such as topology of the network, multipath signal transmission and cable losses affect the PLC channel's ability to transmit the data effectively. The param-

eters such as frequency medium used and data transmission distance have major effects on attenuation in signal. The noise introduced by the channel like impulsive noise, narrow band noise and coloured noise has a major effect on PLC channel attenuation [79]. The channel is shown next in Figure 2.8.

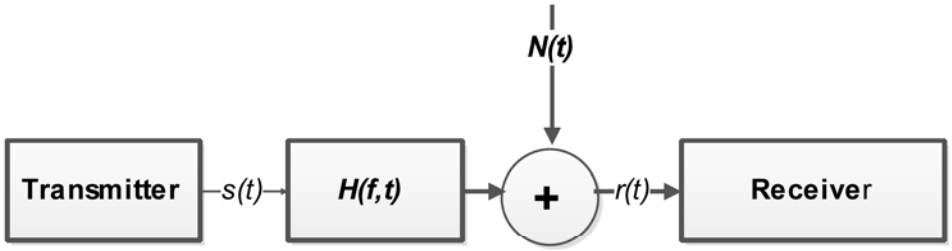


Figure 2-8 Power Line Communication Channel [80]

The LV energy lines is the energy of a communications cable that connects substations to domestic houses. The causes of noise at LV can be internal or external. A list of power line noise types is listed as follows [80]:

- Coloured Background Noise.
- Narrow band noise.
- Periodic impulsive noise.
- Asynchronous impulsive noise.

All these noise types are collectively referred to as noise. Coloured, background and narrow band noise are known as background noise, which mostly spread all over the spectrum, as their rate of change of magnitude is very slow. On the other hand, the last three are called impulsive noise since their amplitude changes rapidly. Background noise is known to be Additive White Gaussian Noise (AWGN) W_k for PLC analysis [81]. The impulsive noise is;

$$i_k = b_k * g_k \tag{15}$$

where,

i_k is the impulsive noise

b_k is Poisson noise and

g_k is White Gaussian Noise and the Gaussian variance is given by $2\sigma^2$

The total noise n_k is;

$$n_k = W_k + i_k \tag{16}$$

$$n_k = W_k + i_k \tag{17}$$

$$n_k = W_k + b_k * g_k \tag{18}$$

The probability of noise distribution is given by:

$$p_k(t) = e^{-\lambda t}(\lambda t)^k / k \tag{19}$$

The transmitted signal is

$$r_k = a_k + n_k \tag{20}$$

If the modulation technique used is OFDM with BPSK as a bit modulation, then the signal can be expressed as:

$$r_k = \frac{1}{\sqrt{M}} + \sum_{m=1}^{M-1} a_m \, e \frac{j2\pi mk}{M} + W_k + i_k \qquad k = 0,1,2,3 \ldots \ldots \ldots, M-1 \tag{21}$$

where,

M is number of sub channels.

a_m is (+1, -1) BPSK symbols.

2.6 A Multipath Channel

2.6.1 Modelling

When a PLC data signal propagates, it follows arbitrary paths as illustrated in the next figure. The transmission pattern is more or less similar to wireless transmission. An example multipath signal propagation diagram is sketched as in Figure 2.9.

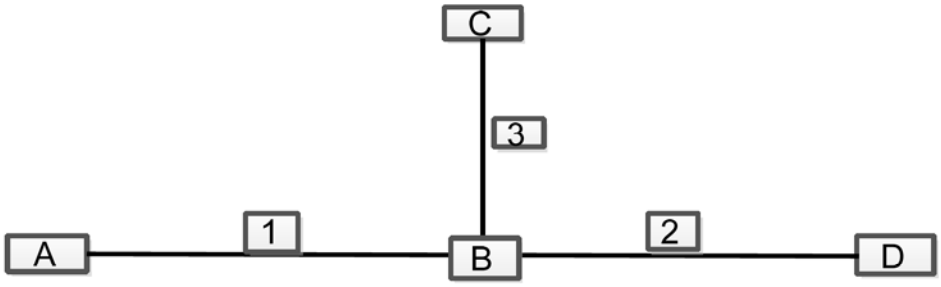


Figure 2-9 Multipath Signal Propagation

If C is the point of transmission and D is the point of receiving, then the signal transmitted at point C can take the following possible routes:

1. D – 3 – 2 – C
2. D – 3 – 3 – D
3. D – 3 – 1 – 3 – D
4. D – 3 – 1 – 1 – 2 – C

As illustrated in Figure 2.9 four different routes are followed. The signal power as well as Bit Error Rate (BER) will depend on the route traversed as well as its span. Multipath data signal propagation is also liable for signal delay τ_1 in PLC network and is expressed as

$$\tau_i = \frac{d_i \sqrt{\varepsilon_r}}{c_o} = \frac{d_i}{v_p} \tag{22}$$

where,

d_i = Length of the path,

c_o = Speed of light and

$\sqrt{\varepsilon_r}$ = Insulation dielectric constant

$$H(f) = \sum_{i=1}^{N} g_i A(f, d_i).e^{-j2\pi f \tau_i} \tag{23}$$

The *H(f)* is the channel frequency response of two points in a communication system and the A(*f,di*) represents cable losses, *f* is the frequency of operation and *gi* is the weight factor $|g_i| \leq 1$

The attenuation factor is:

$$\propto (f) = a_0 + a_1 f^k \tag{24}$$

a_0 and a_1 are the attenuation parameters and this equation leads to:

$$A(f, di) = e^{-\propto(f).d} = e^{-(a_0 + a_1 f^k).d} \tag{25}$$

Using $A(f, di)$ in $H(f)$ finally the PLC transmission line's transfer function is;

$$H(f) = \sum_{i=1}^{N} g_i . e^{-(a_0 + a_1 f^k).d} . e^{-j2\pi f d_i / v_p} \tag{26}$$

where;

g_i =weighing factor.

$e^{-(a_0+a_1 f^k).d}$ = attenuation factor.

$e^{-j2\pi f\, d_i/v_p}$ = delay factor.

The IEEE P1901 standard gives the operations of PLC, with two modulation techniques implemented by physical layer as follows:

- Fast Fourier Transform OFDM: It uses FEC scheme with Convolutional Turbo Code (CTC) as underlying coding technique.

- Wavelet OFDM: It involves FEC, using Concatenated Reed-Solomon (CRS) and Convolutional Code, and it provides an option to add Low Density Parity Check (LDPC) to reduce errors.

2.6.2 Simulation

MATLAB was used to simulate the model for PLC channel for N=14, where N is the number of point in a channel. MATAB is used for the simulation. Modelling is a way to create a virtual representation of a real situation of a system that includes software and hardware. Since the software components of this model are driven by mathematical relationships, it is possible to simulate this virtual representation under a wide range of conditions to map up similar practical PLC equivalentcharacteristics.

The MATLAB code used is as follows:

```
clear all; clc;
N1= 14; k=1; a0=0; a1=7.8e-10;vp=1.5e8
g2(1:N1)=[0.030,0.044,0.106,-0.059,-0.044,-0.041,0.039,-0.038,0.072,-
0.034,0.065,-0.056,0.042,-0.060];
d2(1:N1)=[91,105.4,114,143,149,202,260,321,412,491,568,742,960,112];
ff=1:0.01:20;
f=100:2000;
for m=1:N1
H2(f,m)=g2(m).*exp(-(a0+a1.*((ff.*1e6).^k)).*d2(m)).*exp(-
2i.*pi.*(ff.*1e6).*(d2(m)./vp));
end
H02(f) = sum((H2(f,1:14))');
magH2(f)=10*log10(abs(H02(f)));
angH(f) = angle(H02(f));
```

```
subplot (2,1,1),plot (ff,magH2(f))
title('N=14');
xlabel('frequency in MHz');ylabel('H(f)in dB')
subplot(2,1,2),plot(ff,angH(f))
xlabel('frequency in MHz');
ylabel('Phase')
grid on
```

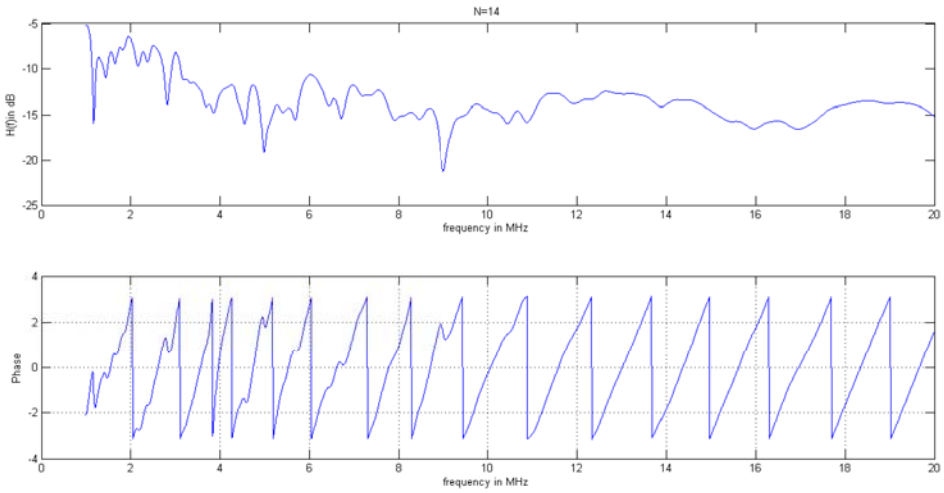


Figure 2-10 PLC Gain and Phase Plot for N=14

The PLC Channel Model Attenuation and Path Parameter for N=14 is shown in tabulated form in Table 2.6.

Table 2-6 PLC Channel Model Attenuation and Path Parameter for N=14

Attenuation Parameter					
K=1	$a_0 = 0$	$a_1 = 7.8 * 10^{-10}$ s/m			
Path Parameters					
i	g_i	d_i/m	i	g_i	d_i/m
1	0.029	90	9	-0.071	411
2	0.0430	102	10	-0.035	490
3	0.0103	113	11	0.065	576
4	-0.058	143	12	-0.055	740
5	-0.045	148	13	0.042	960
6	-0.040	200	14	-0.059	1130
7	0.038	260			
8	-038	322			

2.6.3 Binary Phase Shift Keying

BPSK is also considered as a candidate modulation scheme for PLC data. Basically it is a digital modulation technique which uses signal phase shift to represent digital numbers of zero and one by accordingly shifting a single carrier's phase. The carrier of amplitude A is mathematically expressed as:

$$s(t) = A.\cos 2\pi f_c t \tag{27}$$

The power dissipated across a 1-Ohm resistor is:

$$\int_{-T/2}^{T/2} s(t^2).dt \tag{28}$$

$$P = A^2/2 \tag{29}$$

$$A = \sqrt{2P} \tag{30}$$

For when symbol is changed the phase changes by 180 degrees.

For symbol "1" is given by

$$S_1(t) = \sqrt{2P}\cos 2\pi f_c t \tag{31}$$

For and symbol for "0" is given by

$$S_2(t) = \sqrt{2P}\cos 2\pi f_c t + \pi \tag{32}$$

$$S_2(t) = -\sqrt{2P}\cos 2\pi f_c t \tag{33}$$

Based on equations 31 and 33 BPSK signal can be calculated and answer is given in equation 35

$$S_2(t) = \sqrt{2P}\cos 2\pi f_c t + \pi = -\sqrt{2P}\cos 2\pi f_c t \ \ for\ binary\ 0 \tag{34}$$

$S_2(t) = b(t)\cos 2\pi f_c t$ for binary 1 where f_c is frequency base bond. Therefore the signal space can be represented by a single base frame.

$$s(t) = b(t)\cos 2\pi f_c t \tag{35}$$

where for binary 1 and -1 for binary 0.

Using this formula, a constellation for BPSK can be plotted.

2.6.4 BPSK Signal Generation

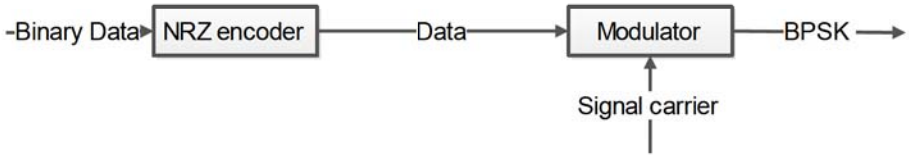


Figure 2-11 BPSK Signal Generation Block Diagram

The block diagram in Figure 2.11 shows how BPSK l is generated. As shown the data stream is first encoded using Non-Return to Zero Encoder (NRZ) and further carrier modulated in a balanced modulator.

The BPSK signal fed in a PLC channel is shown in Figure 2.12.

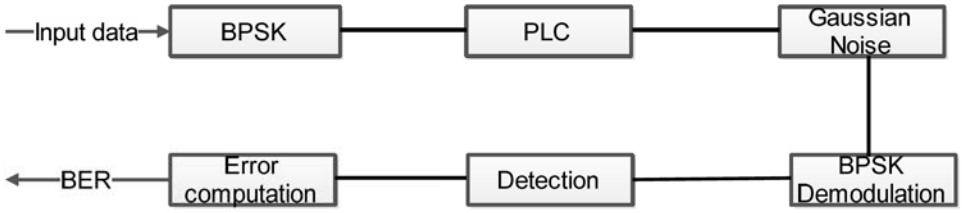


Figure 2-12 BPSK Signal Throughput PLC Channel

This process is used to evaluate its performance (BPSK). As can be seen in this block diagram additive white Gaussian noise (AWGN) is introduced. Ultimately the noise corrupted signal is demodulated at the receiver. As seen inform the graph, the error probability improves with increase in the S.N R.

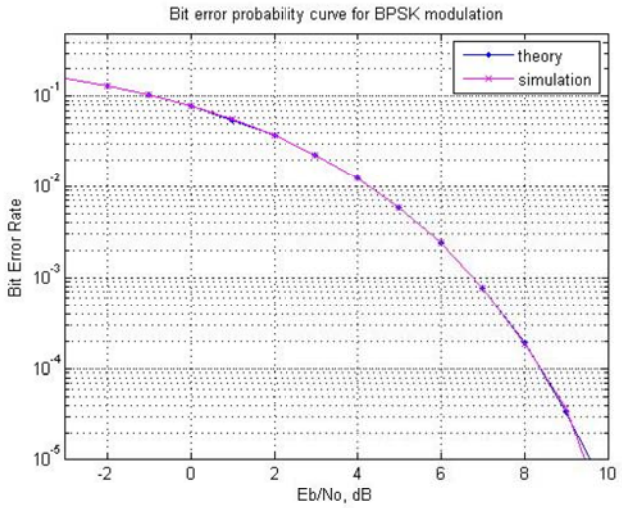


Figure 2-13 Bit Error Rate [82]

The graph in Figure 2-13 shows us the error probability curve for BPSK modulation theory calculated vs the simulation. Bit error rate BER is a parameter which gives an excellent indication of the performance of a channel such as PLC or fibre optic system. As one of the main parameters of interest in any data channel is the number of errors that occur, the bit error rate is a key parameter. The curve of two results shows that the theory and simulation gives us quite similar results. A knowledge of the BER also enables other features of the channel such as the power and bandwidth, etc to be tailored to enable the required performance to be obtained.

2.6.5 Signal to Noise Ratio

When evaluating communication systems, a key performance measure is the Signal to Noise Ratio (SNR).

$$SNR = \frac{P.Signal}{P.Noise} \tag{36}$$

$$ratio\ in\ [dB] = 20\log_{10}(ratio\frac{V_{signal}}{V_{noise}}) \tag{37}$$

The lower (< 20dB) the SNR the poor is the performance of the communication system. The recommended SNR for data is typically 30 to 40 dB. As mentioned before, there are several contributory noise forms. These range from TV to computers plugged onto the power grid thus inserting noise onto the power line. Noise levels increase as the signal transmitted traverses the PLC line. At the same time the data signal gradually suffers degradation. The higher the attenuation level, the lower is the power at the received end, and this can cause the signal to be undetected. The attenuation levels in a power line network as shown previously is typically high, approximated at 100 dB and this places a restriction on the transmitter to the receiver distance. A repeater can be used to overcome the signal degradation. The use of filters can decrease the Signal-to-Noise Ratio as the noise levels are contained to a certain degree. If all household was blocked then a significant amount of noise levels will be prevented from entering the grid. PLCs are considered as a harsh atmosphere when it comes to attenuation but these constraints nevertheless exist in most communication systems [83].

2.7 Introduction to OFDM

OFDM is another candidate modulation scheme. It converts any bit-rate data signal into numerous parallel bit-rate signal and modulates each signal on distinct subcarriers. The total bandwidth (BW) is divided into (n=5) channels. The FDM division function is depicted in Figure 2.14.

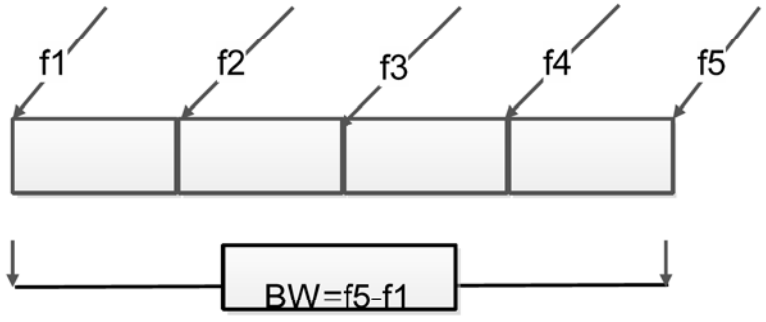


Figure 2-14 FDM Division [84]

$$f1 - f2 = BW/n$$

Due to interference, closer channel FDM divisions require guard bands to isolate them to mitigate for the interference. The Cyclic Prefix (CP) can be used for the same purpose of interference reduction. An FDM block diagram incorporating guards is shown in Figure 2.15.

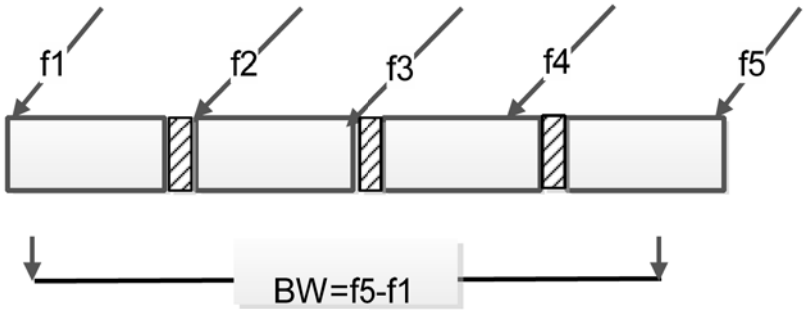


Figure 2-15 FDM with Guards [84]

The bandwidth of n-th channel = $f2-f1$. The guard's bandwidth introduces e orthogonality to sub-carriers. Orthogonal sub-carriers remove the inter channel interference. In orthogonal concept, two signals should be uncorrelated over the duration of time of a symbol. Thus,

$$\int_0^T S1(t).S2(t).dt = 0 \tag{38}$$

Figure 2.16 shows an OFDM Transmitter.

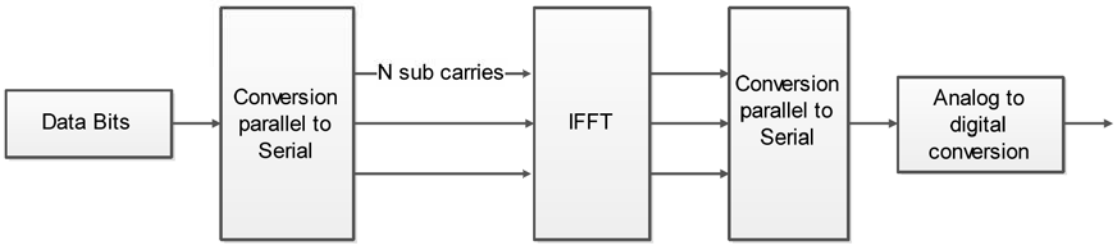


Figure 2-16 OFDM Transmitter Block Diagram

Referring to the block diagram, a serial bit data stream is equally distributed among parallel sub-carriers to decrease bit rate per channel. This process allows the increasing of symbol duration for multicarrier modulation schemes to remove Inter Symbol Interference (ISI). Splitting the data stream into many parallel streams as shown in the block diagram 2.14 increases the symbol duration in each stream. This delay spreads only as a small fraction of the symbol duration. The modu-

lation followed by serial to parallel conversion generates frequency components, which are converted to time samples using Inverse Fast Fourier Transform (IFFT). The OFDM symbol is generated after IFFT, which is:

$$x[n] = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} X[i] e^{2\pi ni/N} \quad , \quad 0 \leq n \leq N-1 \tag{39}$$

Each $x[n]$ represents a sum of modulated symbols with frequency modulated by $e^{2\pi ni/N}$ factor. After the addition of CP to the symbols, they are passed through the parallel to serial (p/s) converter. A symbol preceding CP makes convolution between channels and OFDM symbols circular in nature.

$$H(f) = \sum_{i=1}^{N} g_i . e^{-(a_0 + a_1 f^k).d} . e^{-j2\pi f d_i / v_p} \tag{40}$$

IFFT is executed to create OFDM signal, and CP is added to reduce ISI. The analytic work is performance calculation of blend of different modulation methods like BPSK, QAM, and FFT, cosine, OFDM, Error detection code parity check and different receiver structures. MATLAB simulations can be executed and different results can be compared.

2.7.1 OFDM Model for PLC

For simulation purposes, our PLC is created incorporating a transmitter, receiver and channel blocks. The system was designed and comprises the following: a Coding block, interleaving, mapping, pilot insertion S/P concert we IFFT and PS converter with cyclic prefix to the channel the same sequence is executed in reverse order on all blocks to output the data. Data is transferred in parallel stream by passing it via an S/P converter. A protect interval is used to prevent ISI (inter symbol interference). A cyclic prefix (CP) is created by a few of last samples of the OFDM symbols. CP also creates provisions to further protect the interval between adjacent transferred OFDM symbols in time area. IFFT block transfers data from frequency to time area. The basic PLC model with OFDM system is shown in the Fig. 2-17.

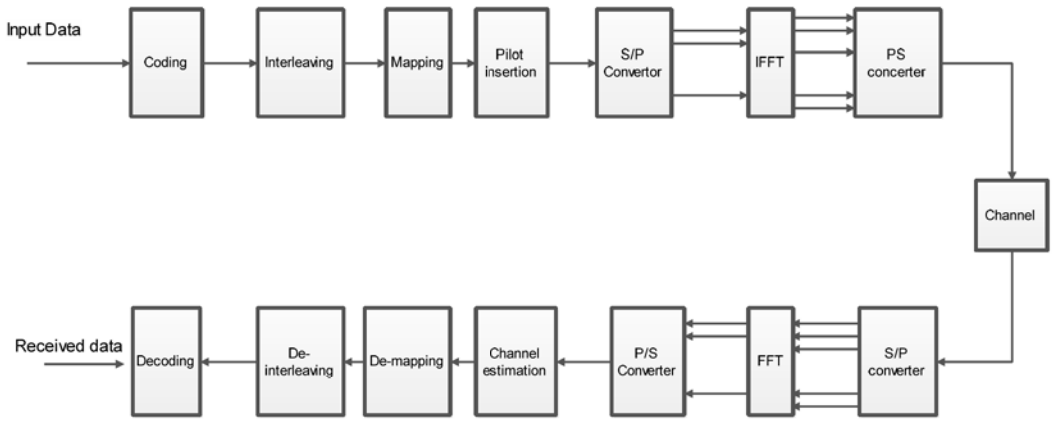


Figure 2-17 Model of PLC with OFDM System [86]

The IEEE P1901 standard for PLC systems proposes two filter bank multicarrier (FBMC) techniques, namely F-OFDM and W-OFDM. These two modulation schemes are studied for NB-PLC transmission in MV power lines to determine the maximum achievable data rates in NB-PLC signal transmission. As in conventional OFDM, inputs to an F-OFDM system are signals of the form:

$$S_k(t) = \sum_n S_k[n]\delta(t - nT) \tag{41}$$

where

$S_k[n]$ is data symbols.

k is the subcarrier index.

T is the symbol rate.

The difference between OFDM and FBMC is in the choice of the impulse responses of the shaping filters $p_T(t)$ and $p_R(t)$ used at the transmitter and the receiver. In OFDM, $p_T(t)$ is a rectangular pulse of duration equal to T, whereas $p_R(t)$ is also a rectangular pulse but of smaller duration T_{FTT} $< T$, where $T_{FTT} = 1/B$ and B is the subcarrier frequency spacing. In FBMC systems designed for maximum spectral efficiency, the duration of both shaping pulses is chosen equal to T_{FTT}. Moreover, the durations of $p_T(t)$ and $p_R(t)$ are longer than the symbol duration T (usually an integer multiple of T), causing the overlapping of successive data symbols [87].

To reduce the transient phenomenon, the time taken of $p_T(t)$ is prolonged by a time period greater than the duration of the channel impulse response. This is done by adding a Cyclic Prefix (CP) to all OFDM symbol. At the receiver, $p_R(t)$ is aligned in time with the transmitted symbol after the latter has reached its steady state. In F-OFDM, the rectangular shaping pulse is replaced by a pulse

to smooth transition of data at the edges. A $p_T(t)$ option often used in practical F-OFDM transmission is the raised cosine pulse:

$$p_T(t) = \prod\left(\frac{t - T/2}{T}\right) \otimes h(t) \tag{42}$$

where $\otimes$ denotes convolution and;

$$\prod\frac{t}{T}\begin{cases} 1, & |t| \le T/2 \\ 0, & otherwise \end{cases} \tag{43}$$

$$h(t) = \frac{\pi}{2T_0}\sin\left(\frac{\pi t}{2T_0}\right)\prod\left(\frac{t - T/2}{T_0}\right) \tag{44}$$

T_0 is the adjacent F-OFDM symbols caused by overlapping period and is referred to as the roll-off period.

2.7.2 Modulation Techniques for Power Line Communication Channel

A candidate modulation scheme for PLC must be carefully selected since the properties of the network are different from other communication channels due to noise and interference. The scheme should exhibit excellent spectral efficiencies and at the same offer excellent noise cancellation if possible.

Single-carrier modulation and spread spectrum modulation schemes seem to be excellent choices since they have better immunity. Media Access can be attained by employing CDMA, which offers multiple access without coordination or synchronisation. Such an example OFDM diagram is shown in Figure 2.18.

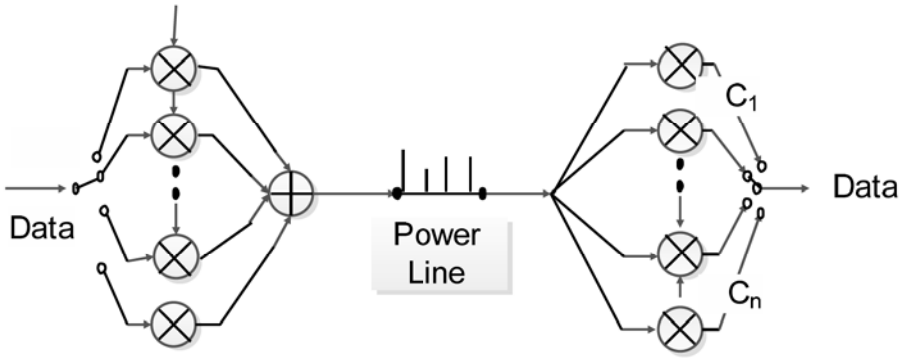


Figure 2-18 OFDM [88]

This approach can offer an excellent signal to noise separation and masking which results in PLC network robustness against various kinds of interference.

Summarily OFDM system features are listed as follows;

- The error correcting and coding as well as mapping of bits onto symbols using QAM.
- OFDM uses IFFT to modulate orthogonal sub-carriers.
- OFDM Synchronization: The data prefix is used to detect the start of each frame.
- OFDM executes the demodulation of the received data by using FFT.
- The channel can be predicted by using a training sequence.

2.8 PLC Network Data Concentrators

Data concentrators are devices that manage SMs and other SG devices. Data concentrator offers the connectivity between devices and utility. Figure 2.19 illustrates message exchange between server and data concentrators.

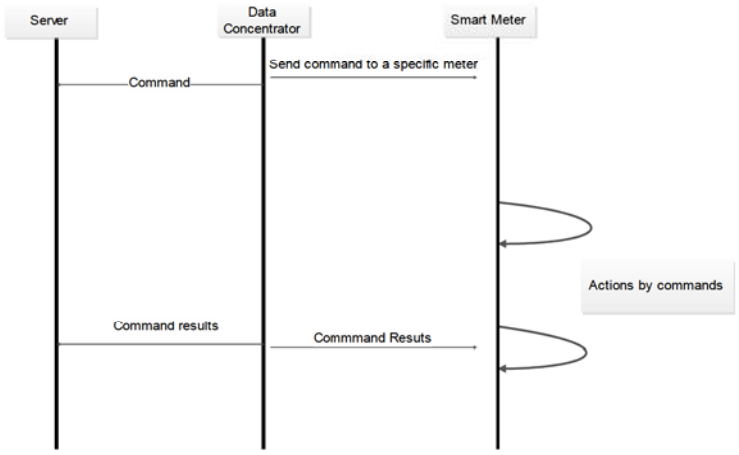


Figure 2-19 Message Exchange between Server and Data Concentrators [92]

The following are its primary functions:

- Discovery of SG devices.
- Safeguarding s reliable channel communications.
- Securing devices to communicate on the encrypted Channel or medium.

- Coordination of the communication of devices bidirectional.
- Monitoring the conditions and the operations of the devices (maintenance and operation functionality).
- Timeous readings, profile loading, billing information and remote management.
- Real-time topology displaying as well as performance management and benchmarking.

A data concentrator is thus a key device in the AMI data management. The concentrator communicates the information to the utility's servers. The data obtained can be used by the utility to provide information for billing services and improve customer services such as real-time energy analysis and usage information. The other benefits of data concentrator are fault detection, initial diagnosis and further improving the operational cost [93]. As such two types of networks connect data concentrators:

- Neighbourhood Area Network.
- Wide Area Network.

Typical message exchanges between data concentrator and SMs is shown in Figure 2.20

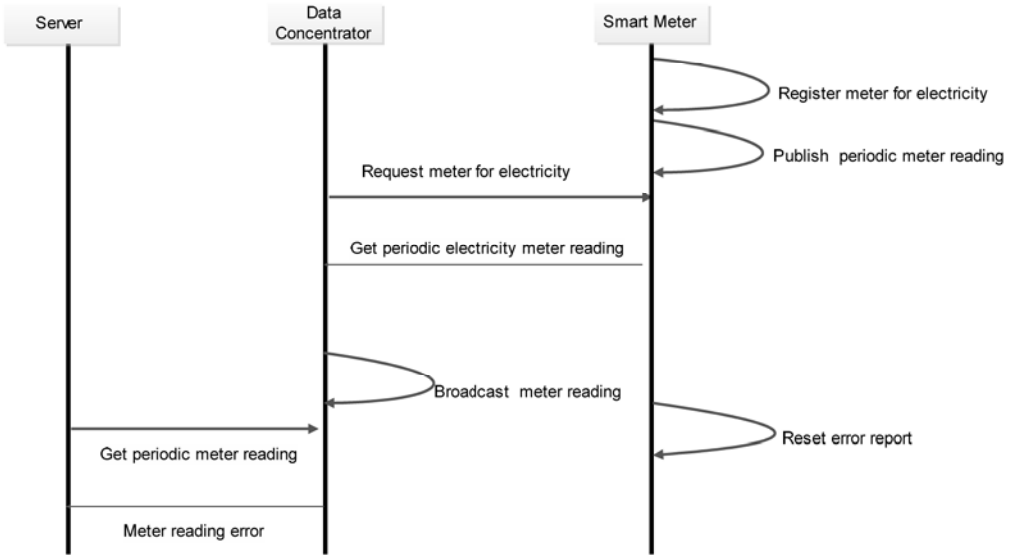


Figure 2-20 Message Exchange between Data Concentrator and Smart Meters [94]

Note that data concentrators are commonly located in transformer centers, and collect this data from several different homes in order to transfer this data to the utility.

2.9 Summary Conclusions

In this chapter, SG architecture and general communications infrastructure were introduced. We also discussed the PLC communications platform. The PLC was modelled as a 2 port network and transfer function evaluated using MATLAB. PLC associated standards were also explored and a comparison carried out Key findings of this chapter are as follows:

- A typical SG incorporates several layers that include; a power system layer that encompasses distributed power generation, transmission, distribution as well as consumer systems;
- It has a power control layer, that monitors and controls the entire SG; a communication layer, which facilitates semi duplex data exchange within the SG environment;
- A security layer is provisioned so as to ensure data integrity, confidentiality, authentication as well as availability;
- An application layer, facilitates various innovative SG applications to power users and utilities, a key example being advanced metering infrastructure (AMI) which is a key application in the realizing of a SG.
- The communication layer is one of the most critical elements that enables SG applications.
- AMI associated data can be transmitted on the PLC platform.
- A simulation of this channel show that performance is related to SNR.
- In order to achieve improved performance, a combination of spectral efficient coding techniques as well as modulation schemes can be carefully chosen for the goal.

3 Theft Detection and Avoidances

3.1 Background

Many SM theft detection approaches such as abnormalities behaviour, consumption pattern etc. have been provided and implemented to protect privacy of both the utility collector and the power consumer [95]. These techniques can be applied to different schemes to improve the data's privacy. In doing so, sensitive data can be compromised. This section reviews theft detection techniques to improve physical security on the SMs. The proposed solution is to protect sensor nodes from being compromised, thus enabling them to detect and report any suspicious activities [95].

Sensor node protection should be implemented as early as possible. An example would be to implement a couple-based scheme. In this case each sensor node builds couples with a neighbourhood sensor, and then the two mutually monitor each other. As a result, any attempt to compromise the node can be detected. The approach can be extended to the SM network in order to improve and enhance security at that level [96].

SGs can update customers about their consumption behaviour as well as monitor the electrical grid remotely. However, SGs are exposed to a vast number of security threats and challenges partly this attributed to inter-operability issues. We reiterate that securing AMI at all times is important due to the data it carries. In this regard, secure protocols are used to enhance security [95] [96]. In the next section we describe as well as explore physical attacks.

3.2 Physical Attack

This attack aims at compromising the SM by using a programming board and a serial cable. However, the proposed detection scheme resists this attack by building a couple that are monitoring each other. The attack is easy to launch since the SM is located outside the consumer premises. Physical attack can also be enhanced at the physical layer by locking up the communication equipment.

3.3 System Attack Objectives

Attackers always aim to disrupt the smooth operation of a SG network. They often succeed in doing so by first monitoring a consumer's activities and then ultimately, steal information or even intentionally disrupt services. A challenger or attacker can capture data via an IP address or by directly

tapping from the line. Often when SM is attacked or its data is compromised, the customer's actions and behaviour are distorted. While the attacker is monitoring the customer's behaviour in the process the data is compromised [98]. A typical attacker's tree is illustrated in Figure 3.1in which all motives are also summarised.

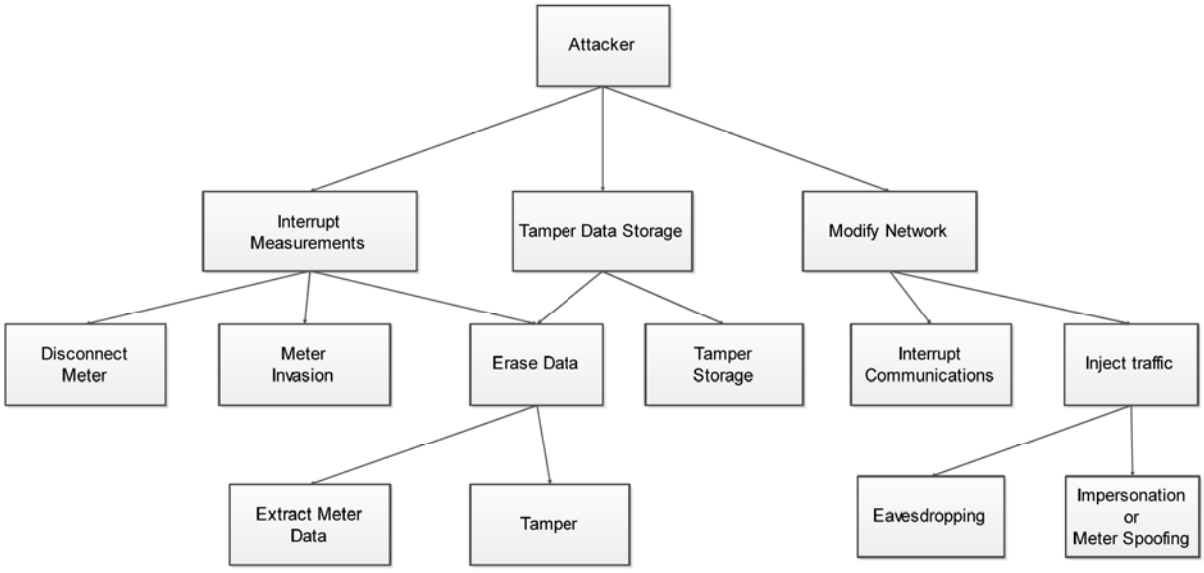


Figure 3.1 Attackers' Tree [99]

The designers of SM did not dwell much on resolving the SM security implementations as SM major function is to read the usage, save the data, and then transfer it via two-way transmission network to the utility collector. The SM manufacturers assumed that the encryption and decryption of data will be resolved by the protocol designers. SMs are typically a low-end devices and they have less computing power build in their microprocessor [100]. In order to implement encryption hardware upgrade is required and that may have costly implications and costly results. If encryption such as Secret Key or Public Key Infrastructure (PKI) is installed, in SMs it will enhance confidentiality of the data. Physical security on the meter is also significant since it makes it challenging for the enemy to physically tamper and gain access to the meter. The cost to implement security on SMs create a big challenge in securing them [101]. AMI challenges are summarised by Figure 3.2.

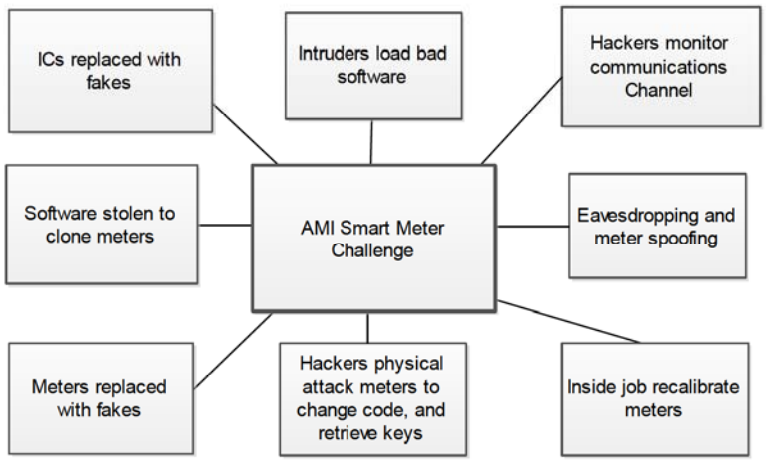


Figure 3.2 AMI Challenges [102]

Intrusion Detection System (IDS) will prevent the challenges and weaknesses of the protocol from being compromised and resulting in costly consequences. Whenever security is put in place prevention measures must also be developed to enable a complete monitoring of the system as one of the security solutions. If security measures are not implemented, there can be an enormous disastrous impact on the overall AMI system [102].

AMI comprises of bidirectional transmission of data and power measurement facilities that assist in power pricing and Demand Side Management (DSM). The system self-healing functionality can be performed using AMI. To prevent intrusion on the AMI system, IDS is employed to monitor and to detect any undesirable entity trying to gain access into the system illegally. We regard IDS as a second line of security solution since the primary solution is AES algorithm, which performs cryptography [102].

SMs can be stolen on the network or can be tampered with and spoofed in order to steal data. To overcome this security threat it is required to come up with a solution to avoid or minimize this SM data stealing by implementing a SM theft detection mechanism. Protecting AMI network is vital. It is proposed that AMI monitoring architecture shall use a distributed scheme, where sensors are located on the meter network and where most of the data is processed [103]. A centralized component will coordinate the sensors' tasks and collect upper level alerts. The IDS block diagram in shown in Figure 3.3.

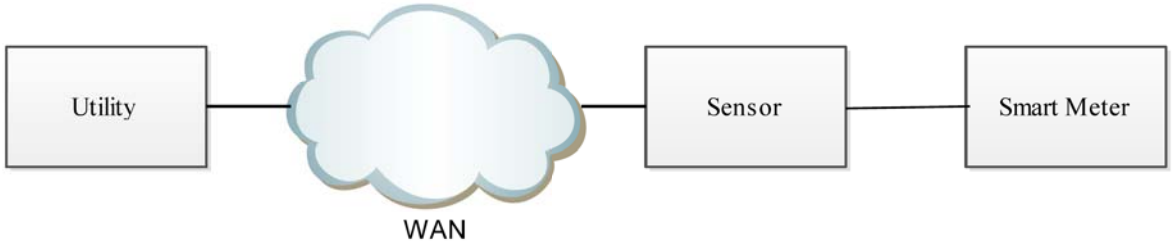


Figure 3.3 Intrusion Detection Systems [103]

The detecting processes of intruder's activities are based on the following [103]:

- **Signature Detection**

  Signature detection scheme looks for patterns of intruder's behaviour by making use of a database of predefined attack signatures.

- **Anomaly Detection**

  Anomaly detection is based on identifying deviations behaviour profile using statistical measures.

- **Specification Detection**

  Specification detection is used to identify deviations of correct behaviour from using logical specifications.

The block diagram of Wide Area Network (WAN) Intrusion Detection System (IDS) is shown in Figure 3.4.

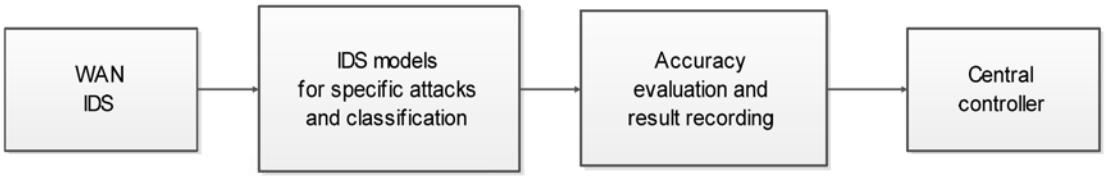


Figure 3.4 WAN Intrusion Detection System [104]

The intrusion detection methods are different for few vital reasons. The first reason is that, signature based IDS are using the blacklist method. The second being that anomaly and specification-based IDS uses a whitelist method. The blacklist method involves the knowledge base of malicious activity. The whitelist method involves training of the system, and identification of the system's

normal behaviour. The two methods have complementary restrictions and advantages. The black-list based IDS cannot identify unknown attacks and will need daily updates. The limitation of whitelist methods is that it provides no information about the causes of attacks. The signature and anomaly based IDS schemes belongs to the family that monitors activity at low level. Specification-based IDS scheme involves a high-level and understanding of the intruder's activity that are monitored [105] [106].

When SMs were introduced intruders had attempted to spoof or alter SMs in order to steal the utility data. Some methods used to steal data are unsophisticated; and others are sophisticated. Remote reading of SMs has abolished the monthly bodily visit by utility operators to read the meter and inspect them. The use of SMs introduces the threat of cyber-attacks. Energy hackers are creative and tireless as long as there is something that is worth stealing. Utilities and electricity sellers must continue to provide robust defensive and detective methods to discourage these attempts or to recognize and deny access into the system [107].

3.4 Monitoring Requirements and Current Approaches

The application of an AMI introduces significant increase to cyber security attacks. The complex AMI devices connected on the network as well as access points enable ways to enter to the system and it can be destructive to the system at some point. The motive of attackers may be any of the following [108]:

- Energy fraud.
- Service disruption.
- Stealing of sensitive information.
- Abuse of communication infrastructure.

Malicious attacks activities that could be achieved can result in a substantial monetary impact on the utilities. Due to this reason, it is important that the utilities utilise detection scheme in identifying malicious actions to mitigate security threat before their execution. Implementing of IDS system has challenges, which include [108]:

- the manner in which the information should be collected

- Installation of the sensors.
- the choice of IDS technologies best suited for triggering alarms
- Mechanisms of notifying relevant operators.
- Relaying and exchange of intrusion detection related data.
- Data aggregation and correlation method to be used in order to precisely distinguish malicious events versus legitimate ones

As a precaution, it would be necessary to safeguard against false alarms. Intermittent or accidental malfunctioning of intrusion detection systems can trigger such alarms. Human and operational errors can also trigger the same. Theft Detection and Revenue Protection

Without any theft detection mechanisms in place the utility personnel rely on tips from fellow employees and the community members to inform them about any power theft It is necessary to note that SM inbuilt theft detection methods have limitations with regards to energy theft. Detection of energy theft remotely, as well as by other measurement techniques are not easy to implement. Generally robust detection mechanisms are desirable as they offer more assured protection. There are several ways of implanting such mechanisms. A few of these methods are outlined in [109] as follows:

- Designing a centralised Meter Data Management (MDM) that executes and analyses time sequence data received and comparing them to historic trends and associate with other similar dwellings or businesses.
- Redundant deployment of SMs i.e. adding redundant meters at different parts of their infrastructure.
- Designing enhanced tamper-resistant resolutions and embedded sensors in the meter that report reprogramming or tampering attempts.

However, more emphasis has been focused on the centralized MDM approach, for the following reasons [110]:

- Its popularity as most AMI deployments have followed this approach.

- No additional support technologies required for its deployment.
- In a way, it does not involve or trigger an overhaul of existing equipment.

3.5 Summary Conclusions

In chapter 3, our focus was on identifying a set of characteristics of a scalable and monitoring architecture for AMI IDS technologies. They were chosen as they have promising functionalities as well as advantages.

Energy theft detection is difficult to eradicate in SGs. The introduction of AMI has further brought about an increase in energy theft. New technologies are being tested to try and alleviate this problem.

4 A Framework for Enhancing PLC Semantic Security

4.1 Semantic Security Overview

In this chapter, we discuss semantic security with regards to PLC platforms in an SG environment. We also investigate security enhancements in order to improve security design objectives. By nature, power line infrastructures are prone to security threats. PLC was never provided with any inbuilt security features, upon which SMs can rely for a secured AMI service. Thus the need to secure and enhance the load management system over such a network. In such designs, authentication must be taken as a primitive, and at the same time prerogative consideration. As such all data transmitted on the network has to be encrypted so as to protect it from any malicious intents.

We hereby advocate for AES as the ultimate solution towards AMI that PLC as the communications platform, and associated accessories such as SMs and data. An associate algorithm will then be customised accordingly to suit our design objectives as set out in the introductory chapters. In that way the response processing time will improve, thus assuming on 128 bits key length [111]. As noted before disruptive activities can easily affect the whole SG system. In any case associated communications threats can be broadly categorized as follows:

- **Denial of Service (**DoS) - The network is blocked; data transmission is slowed significantly to the extent of halting
- **Integrity Threat-** Data can be modified as it traverses the system, due to lack of encryption and authentication.
- **Disclosure Threats-** Protection of PLC system against disclosure of customer data can easily be violated or compromised.

4.2 Potential Attacks

It may be necessary to consider a few intruder scenarios to determine vulnerability of any system and ultimately as a consequence try to work out counter measures [112].

- An attacker can block the data's transmission line by continuously sending unwanted data. This puts the system under severe strain and may result in it halting.

- An intruder can alter synchronisation time thus causing the SMs on the network to be out of synchrony with control centre servers. This results in wrong time stamping of the gathered data and its rejection as a result.
- An intruder can switch off the appliances.
- An attacker can send ping messages on the network and by so doing slowing down network response (DoS).

The diagram below summarizes an attack scenario

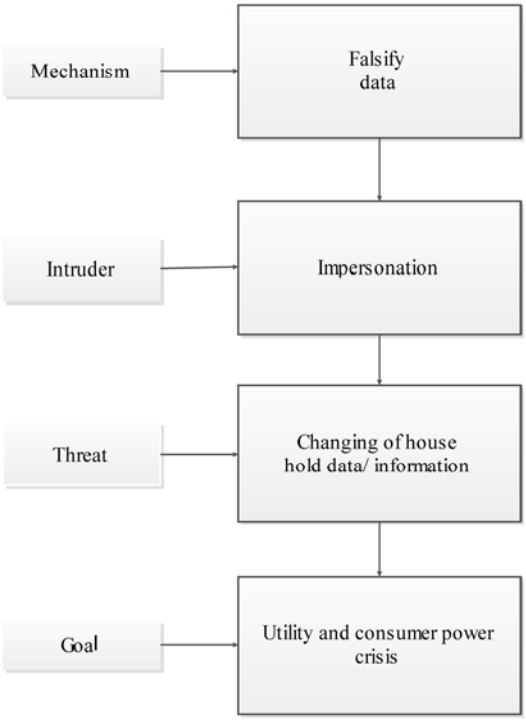


Figure 4-1 Attack Scenario [113]

4.2.1 Dictionary Attack

In cryptanalysis, dictionary attack is a method of crushing a cipher or authentication mechanism by attempting to determine its decryption key. Such techniques are employed by trial and error of multiples of key possibilities, typically words in a dictionary in the hope of matching it with the decryption key. In that way an adversary may eventually successfully decrypt the data. Once the combination matches, this implies that the attacker has succeeded. Such attempts are known to succeed quite often [114].

Once the SM encrypts the usage data it then sends it to the utility collector. However, the proposed secure usage reporting protocol resists the attack by adding a random number. In reality, it may happen that an adversary knows the possible range of data which is reporting every time, since the SM reports to the utility collector in a very short period of time, and typical consumers in residences use small amount of energy in a very short period, which is usually a few kilowatts. Dictionary attack is possible, if we do not add a random number in the encryption data. If we create the attack without considering a random number, an adversary can compare the pattern of encrypted data with a known array of usage consumption and in that way the information can be compromised [115].

4.2.2 Message Replay Attack

A replay attack is another attack method whereby a valid data is maliciously transmitted or fraudulently repeated or delayed. This technique is carried out either by the sender or by adversaries who intercept data and retransmit it, possibly as part of masquerade attack by making use of IP packets substitution. This attack attempts to bypass the authentication method by resending the authenticated messages. An adversary, who eavesdrops on the network, captures the authenticated messages, e.g. a challenge and response between two parties [116]. Then the message of an authorized party is resent to the other end, e.g. the response of the authorized party that will pass the challenge. In fact, an adversary does not need to know the encryption key or the content of the message but needs only to resend the message for authentication.

4.2.3 Traffic Analysis

Traffic analysis is a method of intercepting and examining messages in order to determine the information patterns in a communications channel. It can be executed even if the messages are encrypted and cannot be decrypted. This type of attack aims to assemble all communication activities of a specific node in order to produce the patterns of activities. An attacker is incapable of knowing the message contents by decrypting it instead, the attacker will observe the time that the SM sends data to the utility. The proposed encryption scheme can resist this attack; in fact all SMs must report to the encrypted token, even if there is no energy consumption. Without reporting to the utility each time, the traffic analysis attacks can violate the consumer's privacy by using data patterns in the communications channel [116].

The attacker can recognize what time the householders are at home or out of home by observing the messages which are sent from the SM even if the data is encrypted. However, the proposed scheme can resist this attack by securing usage reporting protocol. Every single SM will report to the encrypted token even if there is no energy consumption at that particular moment, once the token is received [117]. For instance, the token will be sent from the utility collector to every SM, and they will in turn report the usage consumption e.g. 100 kWh or the value of 0. As a result, an attacker is not able to distinguish the pattern activities of a specific SM [117].

4.2.4 Impersonation Attack

Impersonation attack aims to impersonate the authorized party in the network in order to deceive the victim. An adversary places a fake SM on the network, which will then communicate with the victim's SM to potentially affect privacy by analysing the packets. However, this scheme can be directed either to the building couple or to the reporting protocol [118]. Firstly, an adversary cannot build a couple in the network even if he or she has inserted a fake SM. However, without the scheme considerations an adversary can impersonate the SM with a fake one together with another couple will be unaware about the attack. Secondly, the proposal for secure usage reporting protocol prevents an impersonation of the utility collector. It may occur that an adversary inserts a fake utility collector into the network, however, the SMs report only to the approved token that are encrypted by the utility collector's private key [119]. Even if the adversary sends a fake token to collect the usage from SMs still cannot forge a utility collector's private key. In order for an attack to occur, the adversary needs to compute the private key of the utility collector that will then encrypt the token.

4.2.5 Eavesdropping Attack

Eavesdropping attack is known as a passive attack where by an adversary can simply capture the communication packages on the network between the SMs and utility collectors. Subsequently, an adversary attempts to analyse the packages in order to obtain the data content of the packets. This attack is highly possible to occur since all SMs in the network communicate using PLC network [120].

Any adversary who can tap on the PLC network can capture the packets quite simple. Therefore once the content of packages is contained, then the consumer's privacy is violated. In fact the proposed scheme can resist this violation by encrypting all PLC network data with a strong encryption

scheme. The communication between the SMs and the utility collectors are encrypted by the utility collector key such that an adversary cannot know the content without the knowledge of the utility collector's private key [120]. An adversary can capture communication packets between the utility collector and a SM, but he or she cannot decrypt them. In fact, computing the private key relies on the complexity of the encryption algorithm in this case AES is used, which is considered to be difficult to decrypt. As a result, the adversary needs to have knowledge or be able to compute the private key of the utility collector with the purpose of analysing the packets [120].

4.3 DNP Secure Authentication and X509

The Distributed Network Protocol (DNP) is widely used to provide security to load management services through TCP/IP. It can be used to secure data on the Intelligent Electronic Devices (IEDs) as well as on Supervisory Control and Data Acquisition (SCADA) system [121].

It is also widely used globally for electricity data management associated communications. DNP authentication makes use of challenge response and Hashed Message Authentication Code (HMAC). The HMAC is an authentication scheme whereby the sender performs the hash calculation, then send the message [122]. Figure 4.2 illustrated DNP protocol functions.

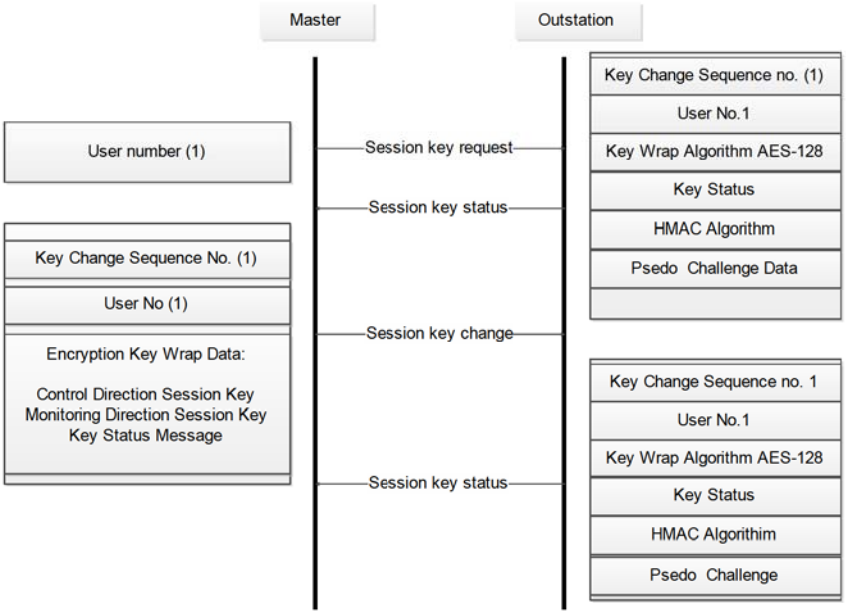


Figure 4-2 DNP Authentications [123]

4.3.1 DNP Cryptography

DNP authentication makes use of two secured techniques, namely symmetric cryptography and hashed data authentication. The use of DNP assumes that the utility and the SM will share one secret key. The secret key is utilised to create a session key. Because the secret key or the update key is only utilised to create session keys, this update key could be used for the lifetime of the device if the security policy of the company allows it [123]. Figure 4.3 illustrates the handshake process.

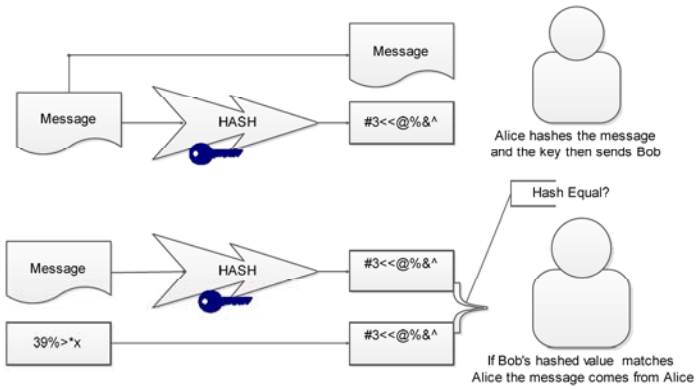


Figure 4-3 Secure Authentication Handshakes [124]

Prior to challenge response schemes, execution of a handshake process between both parties communicating is employed to set up the encryption keys that will be utilised when performing the hashing function. The following are secure authentication handshake sequential procedures [125]:

- The master sends the session key status and the request is sent to the outstation.
- The session key status message is received and the reply is sent back with a specific encryption HMAC, and it sends a random figure as a challenge data.
- The master station generates two keys.
- The decryption of the message is performed by the outstation and retrieves the session keys.

To safeguard and conform to robust security, the master updates the session keys every time depending on the system settings. The execution of secure authentication challenge response is depicted in Figure 4.4.

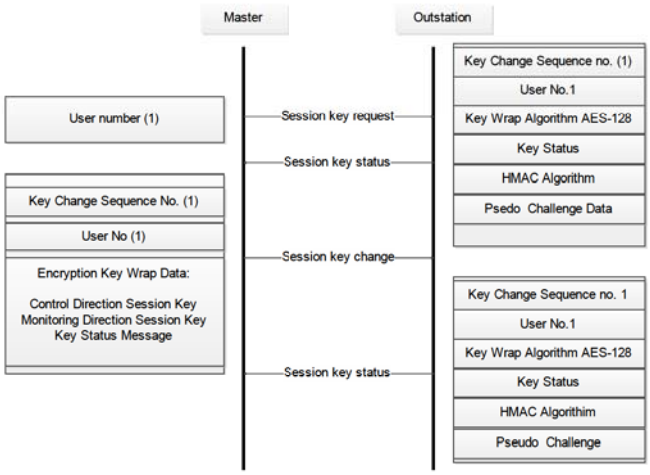


Figure 4-4 Secure Authentication Challenge Responses [125].

The challenge response security mechanism scheme is a two-way communications. The SM can challenge a control operation from the utility centre, or the utility can challenge the data sent from the meter [125].

- To start the challenge, authentication challenge the message is sent.
- To reply the challenger calculates the HMAC and sends the value to the challenger.
- The challenger then authenticates that the received HMAC obtained value matches to its calculation.
- If the calculation matches the data and the data source are authentic.

DNP secure authentication makes use of cryptography to enhance security on its protocol. Management of update keys is a challenge in symmetric cryptography. If one key is utilised in all SMs, there is a possibility of an attacker gaining access to all SMs. For that reason, each should have its own key. To overcome the problem of using a single key, the automated key distribution mechanism is opted for.

4.3.2 X.509

Using public key cryptography is a feasible option for PLC based AMI for the purpose of securing load management. Public key solves the problem of key distribution. We hereby explore this protocol as a possible option for securing PLC SG. The protocol performs well, it provides Certificate Authority (CA) by issuing digital certificates and certifies public keys of users by validating applicant's identity prior to digital certificate issue. The certificates can be distributed on an unsecure

channel since they are not confidential and they also expire. Some certificates get revoked and cannot be used and are placed on Certificate Revocation List (CRL). There are two Public Key Infrastructure (PKI) schemes X.509 and Pretty Good Privacy (PGP) but we will focus on X.509 because it is widely used [126]. The key X.509 issue certificate is shown in Figure 4.5.

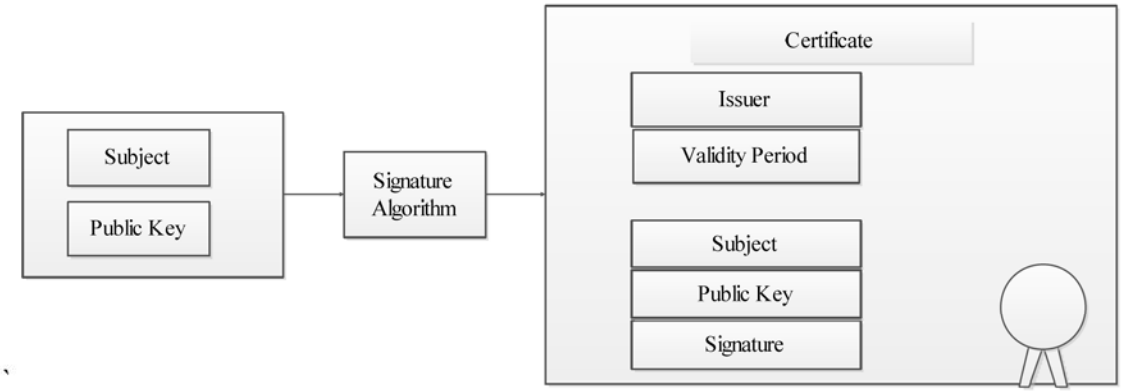


Figure 4-5 Key Certificates [127]

Digital signing of each packet of data that ensures good authentication but on the other hand, this process creates high data overhead, which is a short coming of the X.509 protocol. The time required to verify and sign the CA will increase the bandwidth requirements. The verification of data by signature is very costly due to computational process. The AMI network using this protocol will try to verify the fake packet signatures that are sent by the intruder and this slows down the network. For this reason, the X protocol is not ideal for adoption. The security that is provided by X.509 is also not robust since several cryptanalysis researchers have successfully hacked it and demonstrated that two certificates that contain same signatures can be reconstructed using collision attack on MD5 hash function [127].

4.4 Semantic Security

There are two types of security on any electronic device or communication channels namely: physical and semantic security. This section will discuss semantic. Physical security is discussed in details in chapter 3.

In cryptography, a cryptosystem is semantically secure if the cipher test of a message or data cannot be decrypted to determine the content of the message. The SM functions and the security depends on the firmware that is installed and running on its hardware. At this stage there is no firmware that is deemed to be stable and vulnerability free thus there is a reason for a periodical firmware updates.

There are several ways of updating the firmware patch of the SMs whenever weakness is discovered [128].

One of the techniques can be to dispense the patches update from the control centre to all SMs. Another technique can be by means of peer SM communication to perform firmware patch updates. The trick of this technique is testing that all SMs have been updated correctly and without errors [128]. This method is problematic subsequently because a device that has been interfered with can be utilised to spread erroneous version of the firmware patch update. It is proposed that each SM shall have proper CPU power and memory to allow firmware diversity. SM device shall have two firmware versions on it; one version should be the updated version. Prior to the new firmware update is applied to the SM; the firmware update is then tested for its consistency with the firmware that was loaded previously for conformance [129]. This technique is the solution to the spreading of malicious patch and undesired updates.

4.4.1 Cryptology, Cryptography and Cryptanalysis

Cryptology is a study of cryptosystems, and it is subdivided into two disciplines. Cryptography is the design of cryptosystems. Cryptanalysis is the study of breaking of cryptosystems with an aim to find the vulnerability or weakness in them that will permit the retrieval of plain text without knowing the key or algorithm.These two aspects are closely related; when setting up a cryptosystem [130].

Cryptography is a technique of keeping and transferring data in a form that only those who have the key or for whom are intended to can decrypt and read the message. The encryption process and the possible eavesdropping of asymmetric algorithm are illustrated the Figure 4.6. This type of algorithm is considered slower than a symmetric key algorithm.

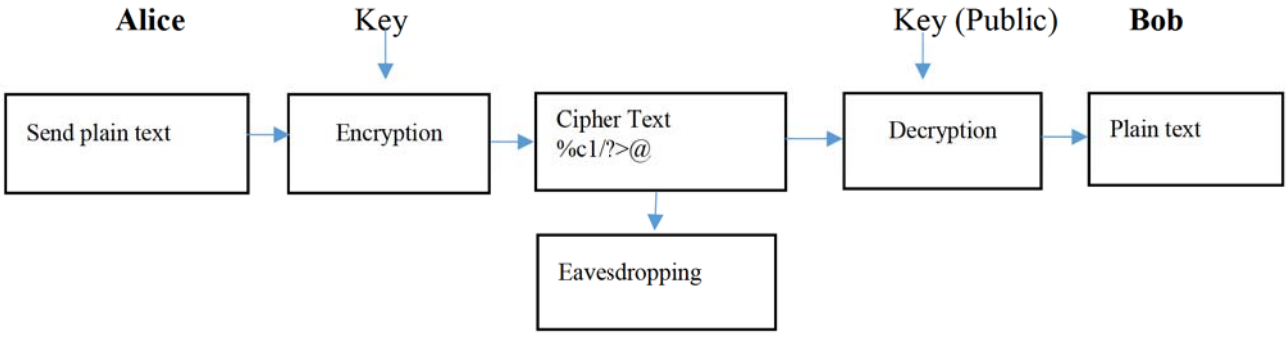


Figure 4-6 Public Key (Asymmetric) Cryptosystem Diagram [131]

Alice sends an encrypted message to Bob, Alice and Bob will follow the steps listed below:

1- Key generations: Bob generates two keys one to encrypt (public) and the other to decrypt (private).

a. Generate two random prime numbers p and q that are the matching size.

b. Compute $n = q \times p$.

c. The public key is n and the private key is (p, q).

2- Encryption: Alice receives the public key from Bob that is, n and then encrypts the message M for Bob.

a. Express the message plaintext as a number.

b. Compute the cipher-text.

c. Send Cipher-text C to Bob.

3- Decryption: Bob receives the C from Alice.

a. Recover the four message plaintexts.

b. Distinguish the plain text from four messages.

c. Recover the original messages.

The symmetric encryption block diagram where only one key is used for encryption and decryption ID shown in Figure 4.7.

This type of algorithm is considered to be relatively fast and efficient in comparison with a newly developed version algorithm that makes use of asymmetric algorithm.

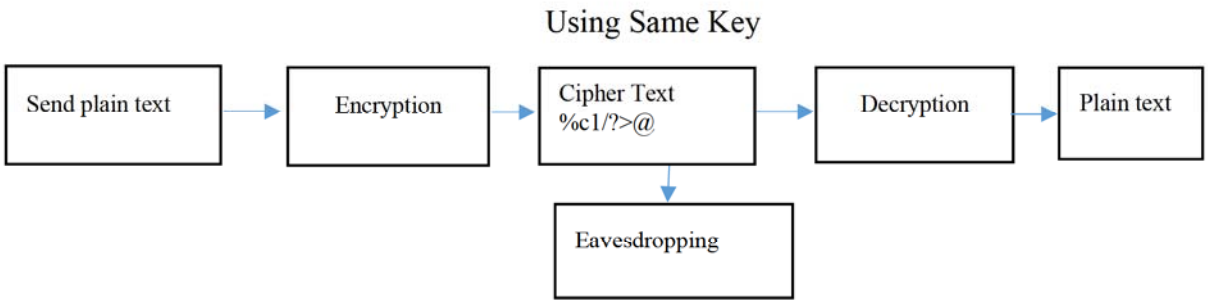


Figure 4-7 Symmetric Encryptions [131].

The attack motives summary is shown in Table 4.1

Table 4-1 Attack Motive Summary [132]

Treats	Vulnerability	Impact
1. Tamper	Management application	Disruption service
2. Masquerade	Lack of Authentication	Impersonation
3. Authentication bypass	Poor proper metering protocol	Manipulation of parameters
4. Meter storage tampering	Non-firmware integrity protection	Attacker can shut down the meter

4.5 Comparison of Encryption Algorithms for Data Communications

The National Institute of Standards and Technology (NIST) was looking for a best encryption standard to be used worldwide and evaluated few candidates for new Advanced Encryption Standard (AES). The evaluations were done based on security, hardware efficiency, software, and flexibility. The hardware efficiency is particularly a significant aspect used to distinguish among competing algorithms. Other evaluated candidates did not fulfil the conditions indicated above to the same degree. Few algorithms were compared and analysed for security [133]. The algorithms are as follows: DES, AES, MARS, R6C, Tow fish Serpent and RSA. The evaluation will carried out considering performance measures such as computational time, memory utilization and size of data. The encryption plays a major role in enhancing data security against eavesdropping attacks. The encryption and decryption algorithm can be characterised into two types, which are symmetric key and asymmetric key algorithms [134]. We will compare both the symmetric and asymmetric algorithms for usage in an AMI system.

4.5.1 Data Encryption Standard (DES)

The DES falls on the block cipher group and it has a size of 64-bits block and 56-bits key. It uses 16-rounds of substitution and permutation. In one of the rounds the data and key bits are shifted, permutated, XORed, and sent to eight boxes [134]. Eventually the lookup tables are called the DES algorithm. The decryption uses the same process that is executed on encryption but it is executed in reverse. The DES makes use of 56-bits key for encryption. This key size is small and it can be broken using brute-force approaches. The DES key is quite small and it has been deliberated that the algorithm is outdated. In 1998, the Electronic Frontier Foundation (EFF) built a DES computer that can decode DES data for time duration of less than one week [135]. This type of encryption cannot be used due to the reason given above.

4.5.2 Triple DES (3DES)

Triple DES was created to address the DES security problems instead of designing the entire cryptosystem. It was designed to purely extend the DES key size by executing the algorithm three times in series with three different keys. The key size in that way was expanded to 168 bits. This key size is beyond the scope of brute-force techniques. It is not fully trusted since the original algorithm was not intended to be utilised in this manner. The 3DES is still used by some of the internet protocols. We will not consider using the modified version of DES due to encryption slow speed. It is derived from DES that causes many problems in encryption process [136].

4.5.3 Advanced Encryption Standard (AES) or Rijndael

AES is a type of encryption algorithm that uses 10, 12, or 14 rounds on encryption and decryption process. The key size is flexible it can be 128,192 or 256 bits. To give better security AES make use of some types of alteration. The substitution, the mixing and adding of a key in each round of AES expect the last transformations. NIST has led competitors to come with a new replacement for DES. The victor was pronounced in 2001 and it was named the Rijndael [136]. Eventually Rijndael was named Advanced Encryption Standard.

The military says it can be difficult technically and economically to attack keys of the size that is approximately about 90 bits. The only known attacker can attack keys up to 70 bits. The AES 128-bits would be very difficult to break. This means you need at least 1000 times faster system that is the fastest more than a personal computer. At this stage, there is no confirmation that AES has any vulnerability. Some cryptanalysis have tried AES and making attacks other than exhaustive search,

such as brute force AES-128 offers an adequately huge amount of possible keys; in so doing exhaustive search is not practical. There has been technological breakthrough that tried to hack AES but there were no success rather than exhaustive search [136].

Rijndael is identified by block size and key sizes that consist of at least 128 bits and a highest number of up to 256 bits. If one byte equals eight bits, with the block size of 128 bits, therefore 128 divided by 8 will be equal to16 bytes. It functions on a 4×4 matrix of bytes. Most of its algorithms are executed in a finite field. Its cipher data is defined as a number of replications of alterations of rounds that transform the input plain text into the final output of cipher text [137].

4.5.4 Goals of AES

An AES represents a strong and robust symmetric block cipher for commercial use in the next century. The following are reasons why it is considered a contender [138].

- It is very efficient more than the Triple DES.
- It is more secured than Triple DES.
- Its key sizes are: 128, 192, and 256 bits and it is difficult to break it.
- It is publicly defined and evaluated.

NIST developed the algorithm's specifications and assessment criteria that would be utilised to compare the applicant's algorithms. The assessment criteria were divided into three categories as follows [139]:

Security: The security is the most significant feature in the assessment and includes features such as robustness of the algorithm to cryptanalysis, accuracy of its maths, randomness of the algorithm output, security if equated to other contenders and the costs.

Costs: The costs includes licensing necessities, time, speed efficiency overboard, and memory necessities. The speed of the algorithm on a variety of platforms that need to be considered are as follows 128, 192 and 256 bits data.

Algorithm Implementation: The algorithm must be flexible, secure and efficient. Rijndael's key span is well-defined to be either 128, 192, or 256 bits. A data block to be administered using Rijndael is separated into an arrays of bytes, and each of the cipher processes is byte-oriented.

Rijndael's rounds consists of four layers. In the first layer, an 8 x 8 S-box is executed in each byte. The second and third layers are utilized for linear layer mix, where by the rows of the array are moved, and the columns are mixed. In the fourth layer, subkey bytes are XORed into each byte of the array. Eventually in the last round, the mixing column is omitted [140].

4.5.5 Attribute Based Encryption (ABE)

ABE is a recent public key cryptography where by the cipher text depends on a user attribute. Two scientist named Sahai and Waters introduced ABE in 2005. The user can decrypt the cipher text, if he or she is in possession of secret keys that are related to a set of attributes that fulfills the associated policy. The algorithm offers a numerous advantages by reducing organizational boundaries and increasing functioning flexibility. It is mostly used to encrypt logs, there two types of ABE encryption such as key police based ABE (KP-ABE) and ciphertext - police ABE (CP-ABE). The protocol consist of three algorithm, key generation, encryption and decryption [141].

Key generation generates keys to public and global parameters when given the security rules or parameters. If the receiver to whom a message is intended is *i*. The protocol consists of three algorithms:

Let $N = q_1 q_2$ where q_1 and $q_2$are primes. When $g \in \mathbb{Z}_{N^2}$ such as g has order of multiple of *N*. if $\lambda(N) = lcm(q_1 - 1, q_2 - 1)$ where *lcm* is a common multiple. The public key is $i\ PK[i] = (N, g)$ and the secret key is $SK[i] = \lambda(N)$

In Encryption if $M \in \mathbb{Z}_N$ is the message and a random number is selected $r \in \mathbb{Z}_N$ the cipher can be represented by:

$$c = E(M) = g^M r^N mod\ N \tag{45}$$

The decryption of *M* can be calculated from:

$$M = D(c) = \frac{L(c^{\lambda(N)} mod\ N^2}{L(c^{\lambda(N)} mod\ N^2} mod\ N \tag{46}$$

Where –*L* takes a set of input from $\{u < N^2 | u = 1 mod\ N\}$ and computes $L(u = (u-1)/N$ .The homomorphism is shown in this way. If $c_1 = EM_1$ and $c_2 = EM_2$ are two ciphertexts, for $M_1, M_2 \in \mathbb{Z}_N$ Then, $D(c_1.c_1 mod\ N^2 = M_1 M_2\ mod\ N$ it is seen that r^N is used to make the homomorphic

computation in deterministic; the same message can be encrypted into different ciphertexts to prevent dictionary attacks.

Its shortcomings are as follows:

- Key generation.
- Key-revocation.
- All ABE schemes depends on central key distribution and thus if the centralised key distribution fails, then the entire systems also fails.
- The access structure is specific and requires user to have at least a single attribute.

Unlike in outdated circumstances where one party encrypts a message for another targeted party, distributed systems require more flexibility. It is a general expressive way of defining asymmetric-key encryption technology for policy implementation based on attributes. Its algorithms are usually computationally intensive and involves pairing operations and exponential equations computation is complex and increases linearly with the size of attributes [142]. Using its implementation in mobile devices can be very challenging because mobile applications schemes have limited computation power. Mobile devices will need a semi-trusted server to reduce the computational load required for cipher text decryption [143]. Using this technology in PLC SG will not be feasible due to a number of SMs that contain data with variety of customers attribute. The bulk customers will have huge attributes and additional equipment for computation and decryption will be required.

It was decided that ABE cannot be used for PLC data encryption because of the following reasons:

- ABE is more expensive due to added functionality to the standard public key cryptography.
- The encryption time will only depend on the size of attributes.
- The key generation time will depend on the size of Boolean formulae.
- Servers that generate user private keys may become a bottle neck.
- ABE is a public key cryptography and public key cryptography cryptology are relatively slow to encrypt or decrypt.
- ABE security is only achieved at 4096 bits while AES is achieved at 128 bits.

4.5.6 RSA

RSA uses a public key cryptography algorithm. It is regularly used on asymmetric algorithm that was termed after three mathematicians who originated it. It was created by Rivest, Shamir, and Adleman. It is currently is used by many software products that are out in the market [144]. It can

be used for key exchange, digital signatures, and encryption. The algorithm utilises an adjustable size encryption block and key size. The keys are derived from a huge number, which is the product of two prime numbers selected according to distinct guidelines. It is mostly used in securing the communication channels and to verify the identity of users over the communication network. The authentication server executes public key authentication with the customer by signing a unique note from the customer with the private key, we call this digital signature. Encryption and decryption algorithms of consume a substantial quantity of computing time, memory, and battery. It is generally slow due to this computing time algorithm. This algorithm cannot be employed to encrypt PLC SG [145].

4.5.7 MARS

MARS uses complex structure like eight forward mixing rounds without the key, eight forward round transformation with the key, eight backward transformation rounds with the key, and eight backward rounds mixing without the key. In each of the eight rounds of MARS algorithm there is what is called type-3 Feistel network. It has a block length of 128 bits and one word has 32 bits length. We have few disadvantages on MARS when it is implemented. The few disadvantages are listed below as follows [145]:

- It requires 2KB table for S-boxes.
- It is deemed weak when checking the extended key on the key schedule.
- Its rotations with variable shift amount is not good.

4.5.8 RC6

The RC6 has numerous parameters and is written as RC6-w/r/b. The w stand for word length, r represent the number of rounds, and b stands for length of key with bytes. We write the code with the recommended parameters for AES such as RC6-32/20/32 [145].

4.5.9 Serpent

The serpent algorithm was originated by Ross Anderson, Eli Biham and Lars Knudsen to be entered on the applicant for the Advanced Encryption Standard. The serpent seems faster than DES and it is more secure as compared to the Triple DES. The serpent algorithm uses twice as many rounds as are required to block all presently identified shortcut attacks. That means that Serpent is secured

against unidentified attacks that may be capable of defeating the regular 16 rounds used in other types of encryption algorithms [145]. The round function comprises of three layers: the key XOR operation, 32 parallel applications of one of the eight specified 4x4 S-boxes, and a linear alteration. In the last round, a second layer of key XOR replaces the linear alteration [146].

4.5.10 Twofish

Twofish consist of two models such as Feistel model and non Feistel. Its block cipher is intended to be extremely safe and extremely flexible. It is well suited for huge microprocessors. The eight-bit smart card microprocessors, and devoted hardware are good example [146]. No attacks can break the full sixteen round version of the algorithm. An Attack have been identified to have attacked a weaker five round Twofish, but the algorithm is very secure when the full sixteen rounds are executed. Twofish is a 128-bits block cipher, meaning that data is encrypted and decrypted in 128-bits chunks. Its key length or size can differ, but the AES is defined to be either 128, 192, or 256 bits. The round function acts on 32-bits words with four key dependent 8x8 S-boxes [147].

4.6 AES Encryption Selected for PLC Security

4.6.1 AES Back Ground

In 1997 NIST called a meeting to select new encryption standard [148]. The old DES was no longer deemed adequate for current and future data protection and security. The DES standard has been in operation since 1976. Due to the technology advance, DES was attacked in 1998 therefore, the DES algorithm was considered unsafe. The Electronic Frontier Foundation (EFF) designed the DES cracker and they obtained the RSA and DES challenge. Triple DES was created but it was too slow to process the encryption algorithm. NIST was opting for an easy to implement security algorithm that will provide robust security, efficient and flexible. Eventually NIST called competition for the best algorithm that took three years and five finalist were selected. NIST selected an algorithm that was originated by two Belgian computer scientists, Vincent Rijmen and Joan Daemen [149].

In 2001, the Federal Information Processing Standards Publication (FIPSP) publicised a standard algorithm of the Rijndael as a new innovative standard for encryption. The standard was named Advanced Encryption Standard (AES). AES is currently the best algorithm and we selected it for PLC data security due to its encryption latency, hardware, software, and history that it has not been cracked before rather than exhaustive search [150].

4.6.2 AES for PLC

The data security can be implemented using AES to encrypt and decrypt data. The data has to be authenticated. Lost packets of data that are retransmitted and repeated data should be authenticated [150]. The SMs are authenticated before they are requested for data in order to prevent the meter spoofing and masquerade. Due to less security on the SM build in software there is a need to secure data on the transmission network.

The study has been conducted on few encryption protocols like RSA Twofish, R6C, Serpant, MARS, DES, 3DES and AES. AES has proven to be the best with respect to data block size against data execution time and AES has proven to be the fastest and efficient encryption method for PLC.

AES provides low cost and low frequency encryption, essential and appropriate for security and low resource applications. The AES algorithm utilises 128 bits block and other three diverse sizes of keys which are 128, 192 and 256 bits. Rijndael permits numerous block sizes of 128, 192, and 256 bits. AES uses symmetric key algorithm that utilises the same key for both encryption and decryption of data. The cipher text created by the AES encryption is of the equal size as the plain text [151].

A GF (Galois field) is a field with a finite number of elements. The GF is always a field that is a power of a prime. The notation to represent a GF (p), where p is the prime number. For the S-box, the field GF (2^8) was chosen. There are several reasons to why this field was chosen. One obvious reason is that the power of 8 was chosen because there are 8 bits in a byte. The prime 2 was chosen because binary is represented as two possible digits a 1 or a 0. In addition arithmetic is simple to do in this field because addition and subtraction are redefined as the exclusion or (XOR) operation. Invertability and resistance to algebraic attacks were also considered when forming the S-box. [151]

The MixColumns transformation operates on the State column by column, treating each column as a four-term polynomial. The columns are considered as polynomials over GF (2^8) and multi plied by a fixed polynomial a(x) modulo x^4 +1given by equation 47.This can be written as a matrix multiplication as follows: AES also makes use of multiplication state matrix called GF (2^8)

$$m(x) = x^8 + x^4 + x^3 + x + 1 \tag{47}$$

and its matrix is;

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} s_{0,0} & s_{0,1} & s_{0,2} & s_{0,3} \\ s_{1,0} & s_{1,1} & s_{1,2} & s_{1,3} \\ s_{2,0} & s_{2,2} & s_{2,3} & s_{2,3} \\ s_{3,0} & s_{3,2} & s_{3,3} & s_{3,3} \end{bmatrix} = \begin{bmatrix} s'_{0,0} & s'_{0,1} & s'_{0,2} & s'_{0,3} \\ s'_{1,0} & s'_{1,1} & s'_{1,2} & s'_{1,3} \\ s'_{2,0} & s'_{2,2} & s'_{2,3} & s'_{2,3} \\ s'_{3,0} & s'_{3,2} & s'_{3,3} & s'_{3,3} \end{bmatrix} \quad (48)$$

The key and the input information are denoted as state and are organised in a 4x4 matrix each of bytes. The 128-bits key is distributed into 4x4 byte matrix. This is Figure 4.8.

State

A_0	A_4	A_8	A_{12}
A_1	A_5	A_9	A_{13}
A_2	A_6	A_{10}	A_{14}
A_3	A_7	A_{11}	A_{15}

Key

K_0	K_4	K_8	K_{12}
K_1	K_5	K_9	K_{13}
K_2	K_6	K_{10}	K_{14}
K_3	K_7	K_{11}	K_{15}

Figure 4-8 Structure of the Key and the State [152]

AES is presented on its original form first. It was then modified from its original encryption code to enhance security without compromising the speed performance to suit the PLC load management system. The modification will make use of synchronisation to cater for DoS, and quick authentication to prevent and minimise delays due to encryption processes [153]. The selected AES for securing PLC load management is based on the following properties.

It is a secure and less vulnerable to cryptanalysis than DES and any other latest asymmetric algorithms.

- It can handle bigger key sizes than DES.
- Its encryption process is quicker in both hardware and software.
- It has 128-bits block size that ensures that it is less exposed to attacks.
- It is a prerequisite to the latest U.S. and international standards.
- It will be the best to protect the PLC data.

4.6.3 AES Mathematics and Background

The structure of the AES used to perform encryption is illustrated in Algorithm 1. We consider AES-128 only. To convert the plaintext $P = (p_1, p_2, \ldots, p_{16})$ (128) and key $K = (k_1, k_2, \ldots, k_{16})$ (128) into a 4×4 array the algorithm 1 is executed shown in Table 4-2.

Table 4-2 AES -128 Encryption Algorithm

Algorithm 1: The AES-128 encryption function.

```
Input: The 128-bit plaintext block P and key K.
Output: The 128-bit ciphertext block C.
X ← AddRoundKey (P,K)
for i ← 1 to 10 do
X ← SubBytes (X)
X ← ShiftRows (X)
if i 6= 10 then
X ← Permutation (X)
end
K ← KeySchedule (K)
X ← AddRoundKey (X,K)
end
C ← X
return C
```

The state matrix of 128-bit plaintext input block to AES is arranged in the following fashion depicted in equation 49.

$$\begin{bmatrix} p1 & p5 & p9 & p13 \\ p2 & p6 & p10 & p14 \\ p3 & p7 & p11 & p15 \\ p4 & p8 & p12 & p16 \end{bmatrix} \tag{49}$$

The corresponding *(CT)* and ciphertexts *(CT)* are respectively depicted in equation 50.

$$\mathrm{CT} = \begin{bmatrix} x_{0,0} & x_{0,1} & x_{0,2} & x_{0,3} \\ x_{1,0} & x_{1,1} & x_{1,2} & x_{1,3} \\ x_{2,0} & x_{2,2} & x_{2,3} & x_{2,3} \\ x_{3,0} & x_{3,2} & x_{3,3} & x_{3,3} \end{bmatrix} \quad \mathrm{CT}' = \begin{bmatrix} s_{0,0} & s_{0,1} & s_{0,2} & s_{0,3} \\ s_{1,0} & s_{1,1} & s_{1,2} & s_{1,3} \\ s_{2,0} & s_{2,2} & s_{2,3} & s_{2,3} \\ s_{3,0} & s_{3,2} & s_{3,3} & s_{3,3} \end{bmatrix} \tag{50}$$

where $x_i \in \{0, \ldots, 255\}$ $\forall i \in \{1, \ldots, 16\}$.

We also define the key matrix for the subkeys used in the ninth and tenth round as shown in equation 51:

$$\mathrm{K}_{10} = \begin{bmatrix} k_{0,0} & k_{0,1} & k_{0,2} & k_{0,3} \\ k_{1,0} & k_{1,1} & k_{1,2} & k_{1,3} \\ k_{2,0} & k_{2,2} & k_{2,3} & k_{2,3} \\ k_{3,0} & k_{3,2} & k_{3,3} & k_{3,3} \end{bmatrix} \quad \mathrm{K}_{9} = \begin{bmatrix} k_{0,0} & k_{0,1} & k_{0,2} & k_{0,3} \\ k_{1,0} & k_{1,1} & k_{1,2} & k_{1,3} \\ k_{2,0} & k_{2,2} & k_{2,3} & k_{2,3} \\ k_{3,0} & k_{3,2} & k_{3,3} & k_{3,3} \end{bmatrix} \tag{51}$$

The encryption repeatedly makes use of a number of round functions. The SubBytes step is the only non-linear in AES the block cipher. The permutation consist of an S-box applied to the bytes of the state. The input byte x is related to the output y of the S-Box by the relation. $= A - 1 + B$, where A and B are constant matrices. The function S is referred as the SubBytes function and $S-1$ as the inverse of the SubBytes function [153]. The ShiftRows function is a byte-wise permutation of the state. The KeyScheduler generates the next round key from the key sequence. The first round key is the input key with no changes. The keys are generated using the SubBytes function and XOR operations. Each column of the state matrix is considered as a four-dimensional vector where each element belongs to F (28). A 4×4 matrix M whose elements are also in Γ (28) is used to map this column into a new vector. This operation is applied on all the four columns of the state matrix [154]. Here M and its inverse $M-1$ are defined:

$$\mathrm{M} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \qquad \mathrm{M}^{-1} = \begin{bmatrix} 14 & 11 & 13 & 9 \\ 9 & 14 & 11 & 13 \\ 13 & 9 & 14 & 11 \\ 11 & 11 & 9 & 14 \end{bmatrix} \tag{52}$$

All the elements in M and $M-1$ are elements of F (28) expressed as a decimal digit. AddRoundKey: Each byte of the array is XORed with a byte from a corresponding array of round subkeys. The AES key scheduling is shown in table 4-3

Table 4-3 AES Key Schedule Algorithm

Algorithm 2: The AES-128 KeySchedule function.

```
Input: (r - 1)th round key (X = xi for i ∈ {1, . . . , 16}).
Output: rth round key X.
for i ← 0 to 3 do
x(i<<2)+1 ← x(i<<2)+1 ⊕ S(x(((i+1)∧3)<<2)+4)
end
x1 ← x1 ⊕ hr
for i ← 1 to 16 do
  if (i - 1) mod 4 6= 0 then
  xi ← xi ⊕ xi-1
  end
end
return X
```

4.6.4 AES Encryption and Decryption

AES algorithm works in a variety combination of data such as 128 bits. The key length of 128, 192, and 256 bits is employed by AES making this encryption the best. The encryption depends on

the algorithm key length for its name [154]. The encryptions are called: AES-128, AES-192, or AES-256 etc. AES encryption-decryption procedure is that the system shall go through 10 cycles for 128-bits keys, 12 cycles for 192-bits keys, and 14 cycles for 256-bits keys to produce the last cipher-text or to get the original plain-text. AES permits 128 bits of data size to be divided into four basic working blocks. The basic blocks array matrix of 4x4 are called state. The first stage of the algorithm is AddRoundKey stage. This process before getting to the final round it goes through nine main rounds, where each of the following transformations are performed [156].

- Sub-bytes.
- Shift-rows.
- Mix-columns.
- Add round Key.

The AES-128 encryption consists of ten rounds. After the first key is added at round 0 the initial 9 rounds are similar, the only difference is the final round. The first 9 rounds are made up of 4 alterations. The last round does not have MixColumns change. There are four straightforward steps called layers that are executed on the incoming data while performing the encryption process and these are: ByteSub, ShiftRow, MixColumn and AddRoundKey.

The AES algorithm flowchart is illustrated by Figure 4.9. The illustration shows how plain text is turned into cipher text by running encryption process and then decryption from cipher text back to plain text.

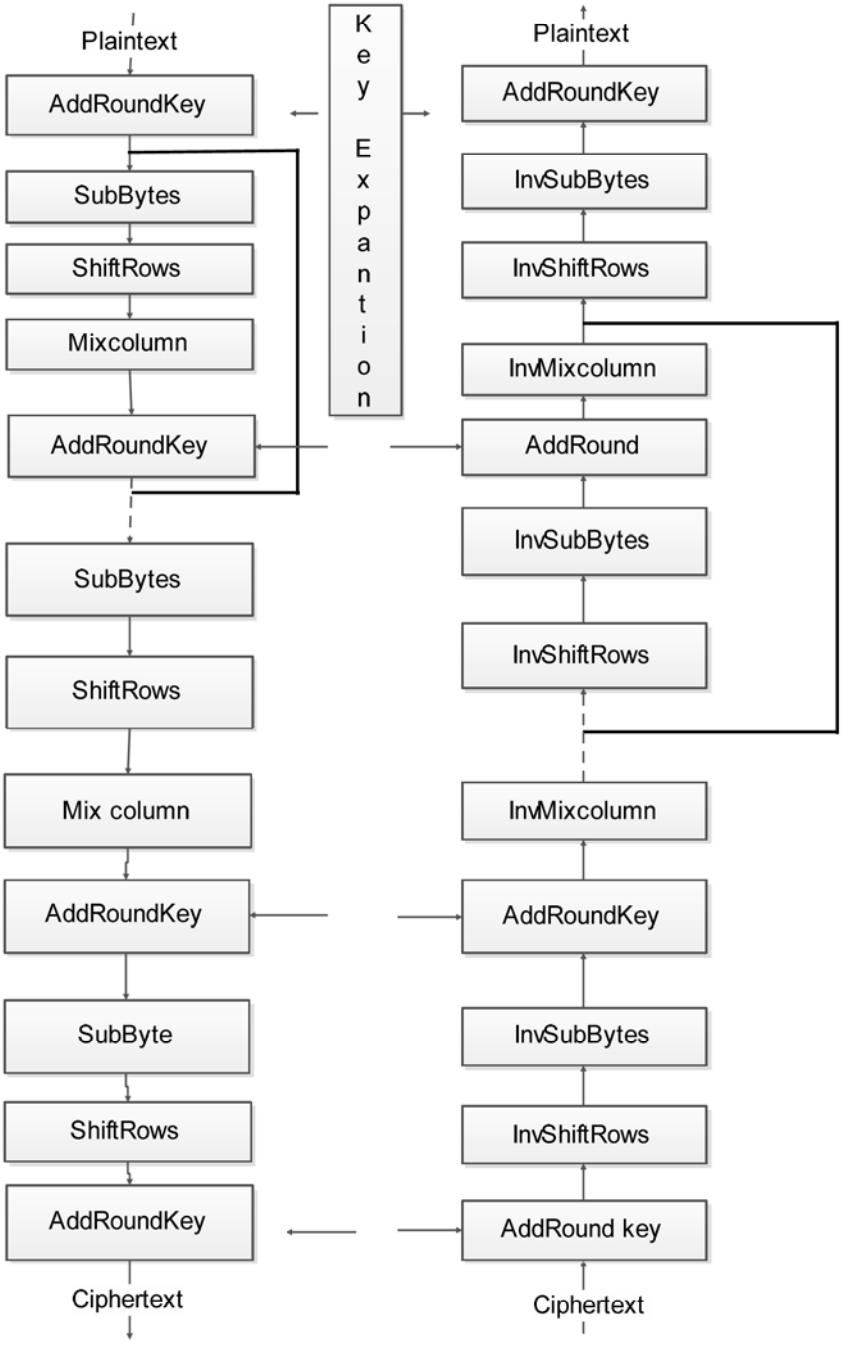


Figure 4-9 Flowchart of AES Algorithm [157]

- **Substitute Byte**

AES make use of 128 bits block of data. This data block has 16 bytes in each block. In sub-byte conversion, each byte of data block is converted by making use of 8-bit substitution box. The substitution box is well-known as Rijndael Sbox. The substitution of byte operates is depicted in Figure 4.10.

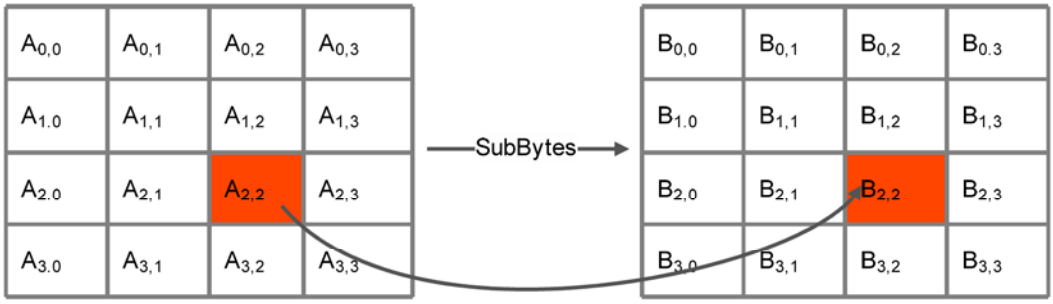


Figure 4-10 Substitute Byte [158]

- **Shift Rows**

Shift Rows is a byte switch. The bytes of the bottom three rows of the state are cyclically shifted. On the second row, one byte moves left hence the shift is performed. For the third and fourth row, two-bytes and three-bytes move left and shifts left respectively. The shift row operates of AES algorithm is depicted in Figure 4.11.

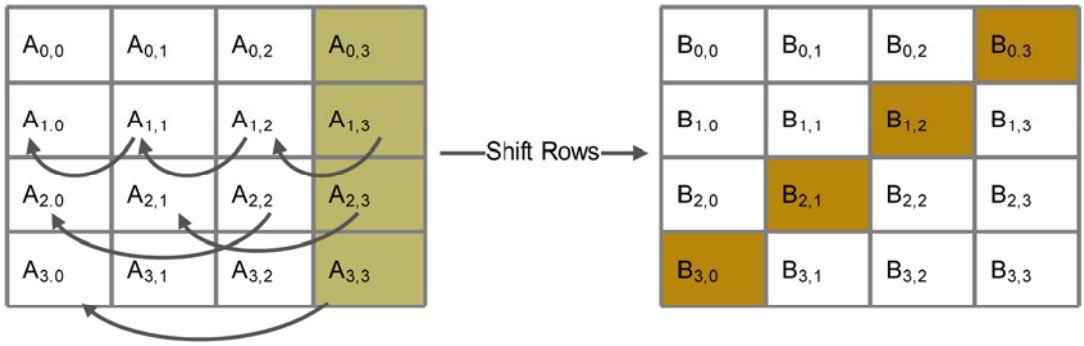


Figure 4-11 Shift Rows [158]

- **Mix Columns**

Mix column round is the same with matrix duplication of each column of the states. The matrix are multiplied with each vector. In this process, the bytes are used as polynomials rather than numbers.

The MixColumn operates of AES algorithm is depicted in Figure 4.12.

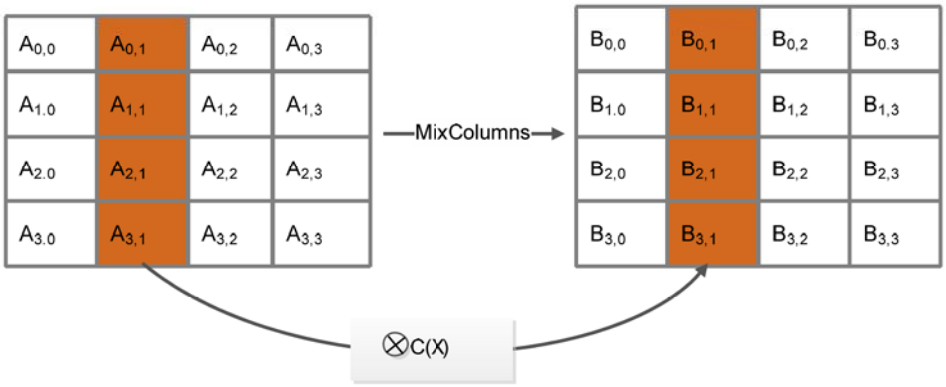


Figure 4-12 Mix Columns [158]

- **Addroundkey**

The Addroundkey is a bit XOR between the 128 bits of the current state and 128 bits of the round key. This alteration has its own inverse. The shift row operates of AES algorithm is depicted in Figure 4.13.

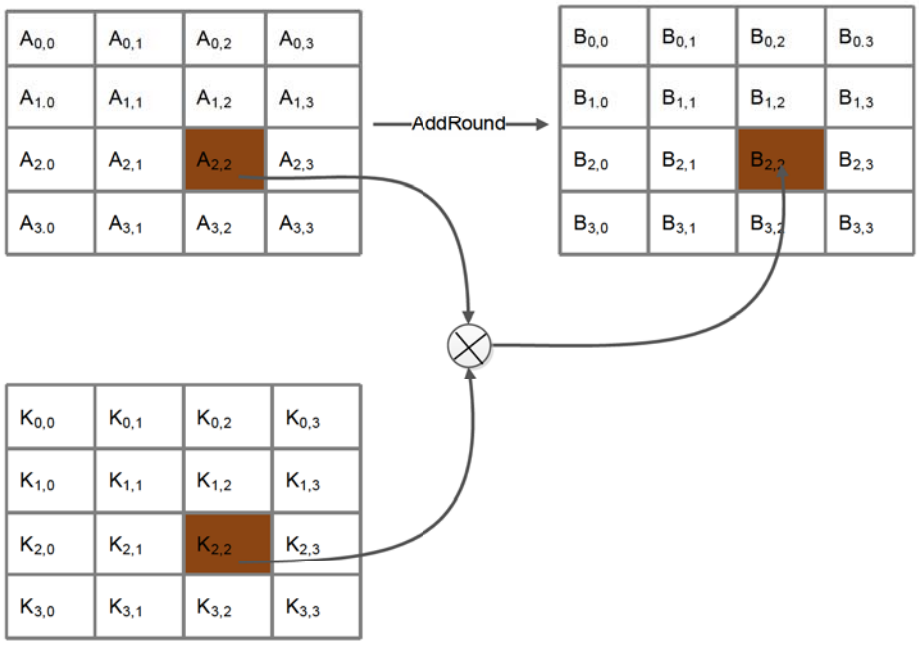


Figure 4-13 AddRoundkey [158]

The flowchart of modified AES algorithm is depicted in Figure 4.14. This flowchart gives a run-down of new modification from the plain text encryption to cipher text and from cipher decryption back to plain text.

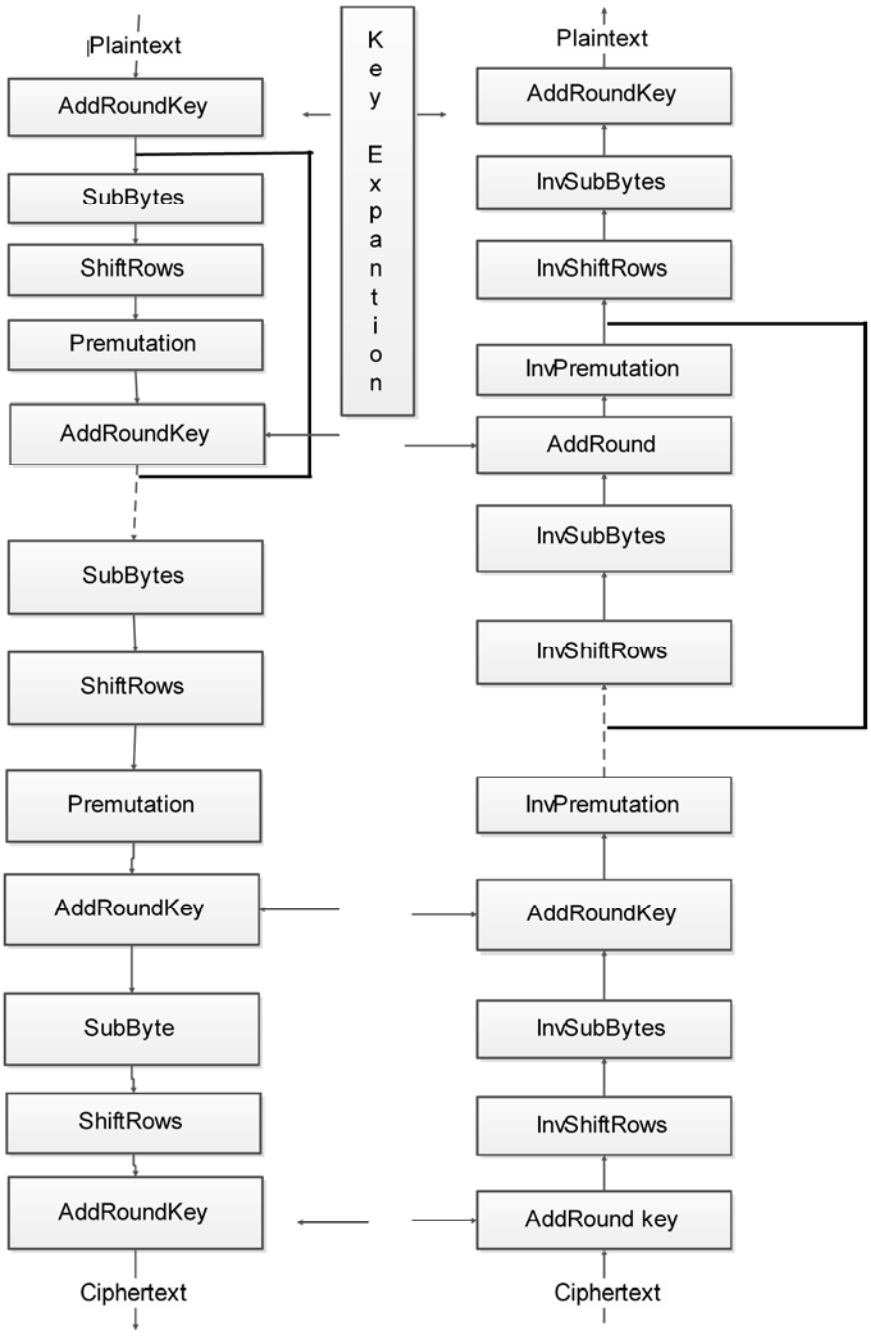


Figure 4-14 Flowchart of Modified AES Algorithm [157]

The key length number of rounds and the required number of keys for different key length 128 bits, 192 bits and 256 bits is depicted in Table 4.4.

Table 4-4 Summary Table for Key Length No. Rounds and Keys

Key length	Number of rounds	Number of keys
128	10	11
192	12	13
256	14	14

4.6.5 AES Modification to Enhance Speed

To minimise more calculation the AES was analysed and modified, to lessen the calculation time of encryption and decryption [159]. Lessening the calculation of the algorithm will improve the encryption performance. This led to the development of a modified AES [160].

It is emphasised that the aim is to lessen computation time but not compromise the security of data. Modified AES algorithm provides improved encryption speed. AES has the block length and the key length. The three alternatives are: 128, 192, or 256 bits. We selected 128 bits key since it is the most applied in encryption of PLC. To defeat big calculation on encryption process the MixColumn step is skipped and the permutation is implemented. The other three junctures remain unchanged [161], [162].

4.6.6 AES Results and Analysis

Java NetBeans 8.0.2 compiler is used to verify the efficiency of the modified AES encryption. Using this test analysis it is shown that the modified AES is faster than the original AES.

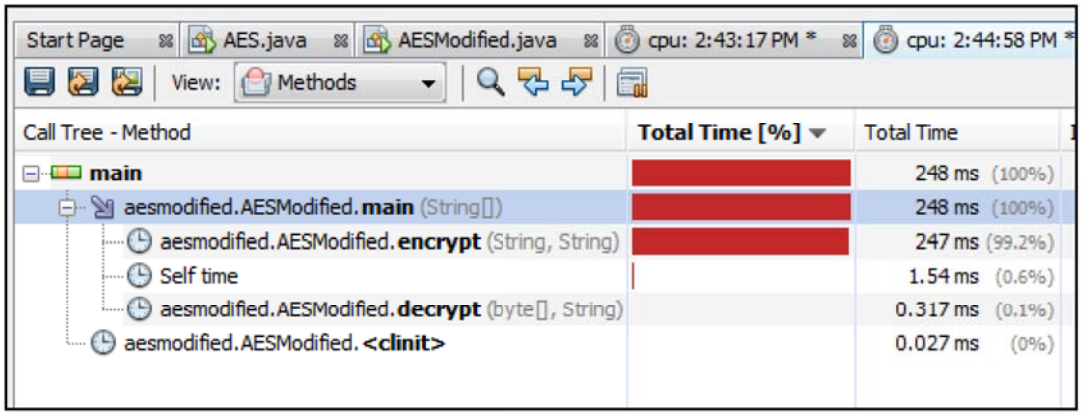


Figure 4-15 AES Java Compiler Simulation

A few data sizes were simulated using AES and Modified AES shown in Figure 4-15 and the results are tabulated and compared in Table 4.5.

Table 4-5 Encryption Process Time

File size	AES (ms)	Modified AES (ms)	Efficiency (ms)
16 bit	290	247	43

4.6.7 Comparison of AES Cryptosystem with DES

Both AES and DES use block cipher scheme. The AES and DES uses symmetric cryptosystems. Both encryption scheme make use of substitution tables called S-boxes. AES and DES encryption and decryption process are similar [161]. Despite these resemblances of AES and DES, there are essential and important differences between their algorithms. The DES algorithm is based on the Feistel cipher arrangement. DES uses 64-bits block size and 56-bits key length and it is attacked a lot as its key is too short to provide robust security [162]. The AES algorithm on the other hand does not use Feistel cipher. AES has three layers, each with its own function. The AES also uses 128-bits block which is twice the length used by DES and is represented by 4 x 4 array of bytes. Another difference between these two is the amount of rounds required. DES needs 16 rounds whereas the AES needs 10, 12 or 14 rounds. For a 128-bits block and a 128-bits key, no attacks have been reported to have exceeded more than six rounds. Three extra rounds, and last round, were added for data security enhancement on AES [163]. The comparison of various encryption schemes are shown on Table 4.6.

Table 4-6 Encryption Comparison Table [163]

FACTORS	AES	DES	3DES	MARS	RSA	SERPANT	TOW FISH
Length	128,192,256 bits	56 bits	126-445 bits	128-2048 bits	1024 bits	256 bits	256 bits
Cipher block	Symmetric	Symmetric	Symmetric	Symmetric	Asymmetric	Symmetric	Symmetric
Block size	128,192,256 bits	64 bit	64 bit	128	512	128	128
Developed	2000	1977	1978	1999	1978	1998	1998
Crypto re-sistance	Very Strong	Vulnerable to cryptanalysis	Vulnerable to cryptanalysis	Strong to cryptanalysis	Brute force and oracle attack	Strong to cryptanalysis	Strong to cryptanalysis
Security	Considered secure	Week	Only one weak to DES	Strong	Least secured	Strong	Strong
Speed	Fast	Moderate	Moderate	Fast	Slower	Slower	Slower

4.6.8 Proposed Modifications

Decreasing the number of rounds of AES algorithm will make it weak as well as prone to attack. Our aim is to work-out a computationally efficient as well as highly restricted ciphering PLC data encrypting algorithm [164]. In addition, increasing the security level through enhancing the key schedule operation [165]. The details of the suggested modifications are discussed in the following subsections. The reduction on AES algorithm calculation will also improve performance. MixColumn step has a large amount of calculations contrast with other steps of AES. Therefore, it is herein proposed to skip the MixColumn execution and instead replace it with permutation step. The latter will decrease computations process therefore reducing the time taken to perform encryption. The other juncture of AES algorithm remains unchanged [166].

4.7 Java NetBeans 8.0.2

The Java Runtime Environment (JRE) is contained on the Java software. The JRE contains Java Virtual Machine (JVM), Java classes and Java environment libraries. The JRE is what one needs to run in the web browser. The Java Plug-in software is a part of JRE. The JRE allows applets inscribed in the Java language to be executed within numerous browsers. The Plug-in is not a standalone program and will not work by itself [167].

A compiler is a program or an application that runs code inscribed in a particular programming language. This code is then turned into a machine code that a computer uses. For an example a programmer writes code of statements in a language like Java using an editor. The file created is called the source code. In fact, the output of the compilation is called the object code [167]. The object code is the code that is utilized by a processor to execute an instruction at a time. The Java language was derived from C and C++ syntax, but it contains less low-level facilities than C and C++.The Java NetBeans 8.0.2 compiler was selected to write the code due to the security and academic background to use the language. The original Java AES code will be modified to suit the PLC data encryption standard. The modified code will be used to compile the code of the Advanced Encryption Standard that will be used for data encryption [168].Modified code and new flowcharts will be created and the code will be written. The original code will then be run on 128 bit data and 128 bit key and see how long it takes to encrypt and decrypt data. The modified code will also be tested on 128 bit data and 128 bits key and see how long it takes to encrypt and decrypt data. The Java code and flowcharts are on the appendix A pages 96 and 97.

4.8 Summary Conclusion

The AES algorithm is the enhancement security over the DES and other cryptosystem. It offers a great level of security efficiency. Though it will need improvement to keep up with current threat it seems as if it will still be strong for some time. Due to its flexibility and variable length block of 128, 192 or 256 bits it is likely that in future, the AES block size can be stretched beyond 128, 192 and 256 bits length [169]. It is also a current block cipher and it provides brilliant long term security against brutal force attacks. It generally is effective in software and hardware. In concluding, it is recommended as the best solution for PLC security. Comparing the above mentioned algorithms it is clear why Rijndael algorithm was selected as an Advanced Encryption Standard. We also realised that it has a lot of advantages over its competitors. AES is the best with regards to speed software and hardware [169]. AES is twice faster than DES. The RC6 is suitable for smart cards like 8051utilization. RC6 cannot be equated with Rijndael or Twofish due to its key scheduling. The smart card application requires an execution of key schedule for every processing block so that the memory is saved to keep the extended key. For this reason, it is required for key schedule to be appropriate for fly key to be generated. The key scheduling design idea for the key scheduling disturbs the performance significantly, and the algorithms has a heavy key scheduling disadvantage for smart card application. Finally, we report the performance of AES best algorithm for the future [170].

5 Resilience and Robustness of PLC System

5.1 Introduction

In this section, we explore resilience, robustness and the efficiency of PLC system as well as physical layer security as there is an interrelationship and dependence among these three. Our focus is on data security resilience and robustness of the PLC's physical layer. This security is referred to as Physical Layer Security (PLS). PLS has been sufficiently investigated on wireless communication but not on PLC environments. For this reason, we pay more attention to what has already been done in this regard in the wireless physical layer. The PLC channel is explored and its performance compared to that of wireless channel in terms of data transmission secrecy. The Home Plug AV (HPAV) is a baseline of the physical layer requirement in IEEE P1901 standard [171]. The privacy of data can be implemented at the upper layers or the bottom physical layer of the ISO/OSI reference model. The first technique involves cryptographic based on algorithms such as AES as detailed on the previous chapter four. The second one involves the physical medium. The PLS can be implemented to enhance the security provided by cryptography. PLS concepts are information security and the complexity of security. The information method assumes that the intruder has all computational resources hence requirement of safeguarding is necessary and no data is released to the intruder. The complexity of cryptography assumes that the intruder has no computation power. Thus it is difficult for an intruder to observe an encrypted messages and to decode them. The information method to private communication is known as the firmest concept of security. PLC use tree topologies where wires are shared amongst communication links. The purpose of this chapter is to investigate the challenges of securing physical layer communication. A comparison with the wireless is done and results are reported [172].

5.2 Smart Meter IP Addressing to Enhance Security

5.2.1 Background

The Internet Protocol (IP) address is a unique number that is assigned to a device in this case to a SM. This IP address is a unique number that serves as an ID of the connection. It works like a street address. IP address is used to route information on the network to its destination. The IP is the way of ensuring the unique identity of the device on the network [173]. There are different ways to address the SMs, one of them is by the use of IP address. If the SM is connected serially

it can be addressed differently to its communication link using serial RS232 or RS485. For serial communication, the communication address number can be used instead of IP address [174].

5.2.2 Robust Addressing Requirements

An addressing scheme of a SM must meet the following requirements: robustness, resilience multiplatform compatibility and flexibility [175].

The network addressing scheme must be able to handle data during transmission. PLC SG must have an algorithm that has the ability to continue operating despite abnormalities on the network. Robust security network, the network must be self-healing in the event of abnormalities. The data must be transmitted in a secure manner. The encryption and authentication shall take place at a high speed [176]. Latency issues due to cartographic process will not be acceptable.

Resilience-The PLC network must be able to provide acceptable service level despite faults and challenges. To increase the resilience of a communication network, the challenges and threats have to be identified and suitable resilience methods have to be well-defined for the service to be secure [176].

Flexibility-The addressing scheme must be able to be dynamic in the load management environment where by introduction of new equipment on the network can be done without problems and changes on the equipment hardware or software are not required [176].

Multiplatform-The main communication network of this research is PLC network but the SMs must be addressed in order for them to be able to communicate on other networks with other devices. This means that data must be able to come from SMs and be able to travel on other networks rather than PLC network before reaching the utility [176].

5.3 Software Diversity Requirements

A common hack system uses buffer overflow. The intruder can attack and manipulate addresses on the stack to execute a programme. Stack cookies are values located amongst function's variables return addresses. The values have to be checked for alteration prior to the return address [177]. This check is to verify if a buffer overflow had interfered with the return address. If the return address is altered, there is a huge possibility that the canary have been altered. The stack or canaries are predominantly vulnerable in eight to sixteen bit architectures. This is common in SMs since they are predictable. The fields of information structures can be randomized to avoid this problem but this does not guarantee permutations against continuous probing. The solution to this can be the introduction of the Address Space Layout Randomization (ASLR), it makes it challenging to guess the address [178]. SMs are poorly suitable to support other arrangement of attacks techniques

such as stack frame padding. The protection against code injection is the non-executable bit. The non-executable bit can be set on a program to prevent malicious code from being executed [178].

5.3.1 Firmware Diversity

The firmware must be capable of defeating the compromise of SMs. The return address encryption is recommended in this regard. This return address will protect addresses on the canaries that can be executed using binary writing.

5.3.2 Address Encryption

It is suggest that the addresses be encrypted before they are stored in the stack and decrypt them before they are utilised. If an attacker overwrites an address without the decryption key, the decryption procedure will crush the attacker's address into a random number.

5.4 Communication Protocols for AMI

SMs send data via the communication channels through IP, GSM, GPRS, PLC, ZigBee etc. to the data concentrators, and these data concentrators communicate with the servers at the control centre [179]. The protocols used on the channel are very important for the implementation of security rules since SMs do not have much security build on them set by the manufacturer. If the protocol is well designed in aspect of security, the data travelling on the channel will be more secured due to the security rules implemented for example: authentication, encryption and decryption.

The SM transmits data over to the data concentrator and this data is forwarded to the Metering Data Management Centre (MDMC). The data is then used for metering purposes and various operations are executed [179]. The metering data is also used for the calculation of the cost of energy used up by the customers, for billing purposes. Since metering devices have a distinctive design and the data formats is different, it requires a special communication protocol that will ensure that the data received is not compromised or tampered with during data transmission [180].

This research looked at the best secure protocols that provides the security and integrity of the data. Java NetBeans 8.0.2 and OPNET simulation tool were used to test and prove the claimed credibility. The communication model is the same as client-server design, where SM acts as a clients, while the data concentrator acts as the server [180]. The data exchange take place when the data concen-

trator sends a request to the SM. The variations in the protocol used and type of network infrastructure available is chosen by each energy provider. A cheap alternate method is the use of the power lines themselves for data communication. Thus PLC is chosen for data transmission.

5.5 Smart Meter Design

A SM consists of three major modules as follows:

- Communications.
- Microcontrollers (MCUs).
- Sensors module.

This system is used to measure the consumption of energy. The Communication medium to the SM can be either wired or wireless. SM system may have an additional option of the LCD display that displays the consumption and messages from the utility. The illustration of a SM architect is depicted in Figure 5.1.

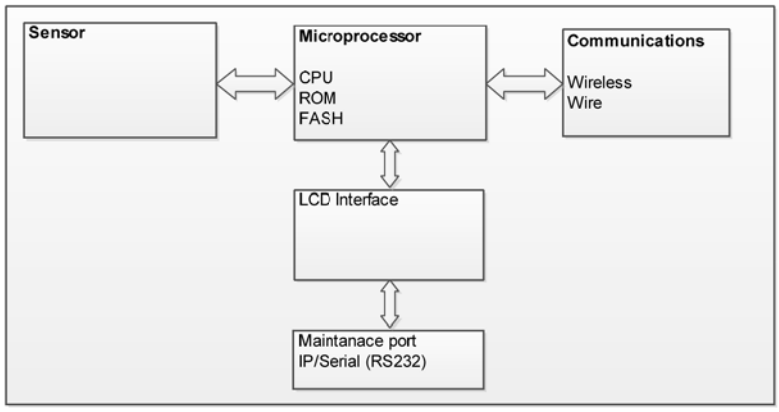


Figure 5-1 Smart Meter Design [181]

This study considers the current hardware limitations of the SM. Adding new hardware or modifying an existing SM with the purpose of improving security would be very costly for two reasons. Firstly, a great number of SMs have already been installed around the world therefore, recalling these devices and re-installing them will be costly. Secondly, the price of SMs will increase due to the powerful processors necessary to improve the computing power and memory. The proposed scheme will protect privacy without the necessity of adding new hardware that provides high computing and memory.

5.6 Smart Meter Communication

AMI standards have been developed in some countries one of the standards example is the Wireless Personal Area Network (ZigBee) that is designed and recommended for low-rate transmission in SMs like PLC [182]. The standard offers security methods that protects the network and application layers. It has been suggested that in symmetric cartography, encryption key used is the same for encrypt and decrypt of data. In asymmetric cartography, two keys are utilised which are public and private keys. The public key is used for encryption algorithm and private key is used for decryption algorithm. The public key encryption algorithm computation is exhaustive and is not very efficient. AES Counter Cipher Block Chaining Message Authentications Code (CCM) can be applied at the network layer to guarantee authenticity and privacy. ZigBee has several advantages including it being an open standard, support of mesh network hence making it possible for SMs to communicate directly with each other [182] [183].

In this work, not only the cost efficiency is considered, but also the protection of consumers' privacy by securing the communication between the SMs and the utility. The ZigBee could be applied to other techniques of encryption to achieve both cost efficiency and privacy; however, the current implementation achieves only cost efficiency. ZigBee has several issues including channel interferences, address conflict, and weakness in ASE repudiation. The cause of the weakness in ASE is asymmetric key encryption [183]. As a result, the two nodes should exchange the key before they communicate; consequently during key exchanges any adversary can potentially eavesdrop and obtain the key. The adversary can then simply use the key in order to compromise the nodes. Actually, the NIST and technology has considered that AES-128 encryption will be secure until 2036. Furthermore, symmetric key encryption has issues with key management when the number of nodes becomes huge. Asymmetric authentication and key exchange can solve this problem but asymmetric algorithms are slower and costly [184]. The advantages of using ECC are scalability and non-repudiation, while ECC uses one key instead of many. Additionally, ECC has advantages over the traditional public key system which are faster computations and less significant key size. Due to improved security in standard protocol, IEEE 802.15.4 and ZigBee Alliance that uses SKKE are a recommended protocol for key establishment and management [184].

However, this research aims to discover a secure communication algorithm in order to protect the privacy of the consumer as long as it maintains cost efficiency. Several approaches have been provided to secure a communication channel between SMs and utilities collectors. However, these approaches have concerns either in the security or cost efficiency. Firstly the issue of security means that the approach has been shown insecure or broken. Secondly cost efficiency means that the approach might be secure, but requires adding of some functionality that increases the cost of SMs rather significantly. Unlike the above mentioned approaches, the proposed scheme achieves both privacy and cost efficiency [185].

5.7 Smart Meter Data Privacy

The SM's functionality is to read the consumption of energy and send it via the communication channel to the utility. Since it has important information about consumers' energy consumption, it could be used to explore the consumers' energy activities. Some pertinent findings on data privacy are discussed in [186].

Data can be used to identify the activities of the consumer since the SM data can easily be linked to the householder location by observing the sender of data. Consequently an adversary is able to analyse the data frequently.

In order to prevent this problem the data must be encrypted. The SM sends data anonymously; in other words, without associating the data with the real identity of the SM that refers to the identity of the householder. It instead uses an anonymous identity. The utility collects the data from the SM with an anonymous identity and then authenticates the data. The service must be a trusted party between the consumer and the utility provider. It only blocks the identities of the consumers, preventing the adversary from linking the usage with identified consumers [186].

When an adversary continues to observe the usage of a small group of SMs over a long period of time, it is possible to link the data. This work protects privacy, including the usage, by applying the encryption technique that prevents an adversary from observing the identity and the usage. The proposed solution is to protect privacy on the communication channel between the SM and the utility collector. The adversary who eavesdrops the messages must not be able to distinguish be-

tween the usages of each SM [186]. This means that each SM sends the usage data to neighbourhood SM and uses encryption to protect the data, and then transfers the data results to the next SM continuously, until the data reaches the collector.

As a result, only the utility collectors are able to identify the usage of each SM; yet an adversary may still capture the sum of the total data for SMs in a neighbourhood. The accurate data from SMs, assumes that physical security must be improved in order to prevent fabricated data [189].

5.8 Smart Grid System Self-healing

One of the objectives of this research is to provide a solution for a SG to be self-healing. In particular, a PLC SG is exposed to faults created by natural and environmental factors such as wind, weather and rain. Some other factors include cyber-attacks and equipment or operator failures. If a fault occurs in a SG network, the system should quickly isolate the malfunctioning components from the rest of the network. A power failure caused by storms or cable theft on the network can cause disruption on the data transmission [190]. Protection schemes must detect faults and disconnect faulted components. Protective devices can isolate components and may also provide automated backup to sensitive data [190].

A power system that is compromised due to lack of security and integrity cannot serve its intended purposes. An intelligent adversary can introduce many types of attacks to breach security. Most existing systems are designed for use with standalone communication networks without the added technologies that ensure their security and system self-healing [191]. The SG concept has millions of automated SMs in homes and industries. A SG can potentially address the problems of an unstable power grid. The SG should be agile and capable of dynamically routing and re-routing power to optimal paths that deliver power and data on the network [191].

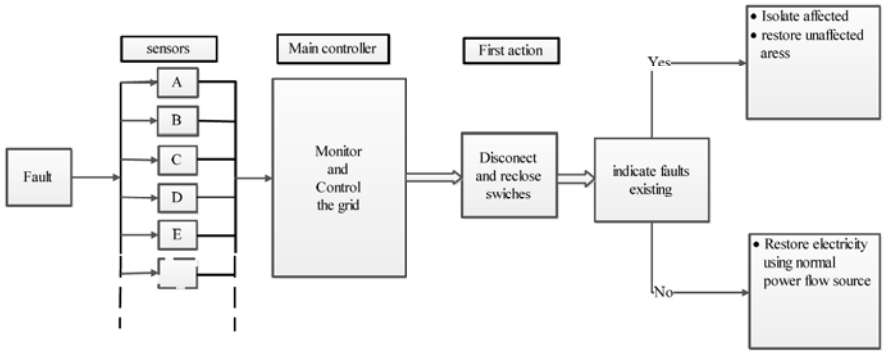


Figure 5-2 Self-healing Protection Network Block Diagram [191]

Using SG technology enables intelligent through line sensors and switches to create a self-healing network. Self-healing systems employ devices that restore power and network automatically when there is a fault in the line. Self-healing reduces the number of consumers affected by power outages. The self-healing systems consist of sensors and IEDs. These devices improve the performance of real-time information to main controller. In case of a fault, signals are sent by disconnected lines. Measurements can be collected in real-time using PMUs or IEDs linked to installed sensors [192]. The first stage in a self-healing is localizing the fault area. The second stage is sending information to monitor the network. The third stage is isolating faulty sensors from the grid and restoring electricity and SG communications. This self-healing process reduces cost, time and the duration of outages, therefore increasing the efficiency of the power grid [192].

5.9 Summary Conclusion

The Physical Layer Security (PLS) in PLC SGs networks and other methods which enhance PLC devices as well as network resilience and robustness have been discussed. The tamper free methods were discussed to prevent meter tampering. The solution was the implementation of tamper seals. The tamper seal can be physical or digital. When the seal is broken, the meter reports tamper alarm. We also elaborated on physical connection on the meter for maintenance purposes and proposed authentication to prove identity of the personnel executing maintenance or firmware upgrade. It was also clear that the resilient network should be flexible, and be multiplatform with software diversity. IP addressing the meter and IP address encryption was also introduced to prevent SM IP address spoofing. The data security is profoundly dependent on the channel data transmission physical layer security and other built-in security features. We discussed physical security problems on SG PLC network and described how they are tackled in the next generation of PLC. The main problem is that the attacker can try to add devices on the network with fake identity that is called meter spoofing. The meters on the network have to be authenticated for identity or perform some other physical check. With this proposition, we ensure resilience in PLC System. The introduction of self- healing capabilities to the grid also help reduce cost, time and the duration of outages, therefore increasing the efficiency of the power grid.

6 Modelling and Simulation (AMI)

6.1 Introduction

This section reviews the basis of the PLC network model. The PLC network was modelled in Chapter 2. Using Java NetBeans 8.5.2 compiler and MATLAB simulation AES encryption was tested and the PLC channel was modelled and simulated to prove that the SG will be secure and robust. In this chapter OPNET is used to simulate the PLC transmission channel. When designing a system it is important that the model created is analysed and tested. Modelling and analysis help the designer to prove that the system will work or not judging by results obtained. If the results are nor satisfactory and do not meet the design's needs, it has to be adjusted and some parameters remodelled and re-simulated. The block diagram depicted in Figure 6.1 shows a summarised AMI network. The data management centre sends the information to the PLC network, then to SMs via other types of network such as fibre and GPRS [193]. When the data concentrator receives the messages, it sends them through to the SMs. It is assumed that other networks that are interconnecting on AMI system are deemed to be working well on the system. The only problem anticipated is on PLC network. For this reason, the emphasis rests on the modelling of the PLC network between the concentrator and SM which is the PLC network in this case. [194]

Figure 6-1 Load Management System Block Diagram

6.2 System Model and Design Goals

6.2.1 Background

We commence this section by detailing our network modelling of the PLC network, as well as defining the design goals. Modelling is performed on the following: channel bandwidth, data speed, data packets queueing delay and data throughput. The design goals are: secure resilient, robust and fast data speed on PLC network.

6.2.2 Queuing Model

The data on the SG can be classified into different classes. For an example, data on remote is classified into low-priority class, while the data from the control centre and messages such as the outage notifications are classified as critical class. The queuing model is used to study the scheduling time of each class and the total scheduling time for the AMI scheduler [195]. The queuing model consists of several queues and one scheduler is involved in our study. The queuing model in SG scheduler assumes that the scheduler provides classes of traffic with different priorities, with smaller class number corresponding to a higher priority [195].

If the assumption is made that the scheduler provides class C of traffic with different priorities, then the smaller class numbers can be assigned to correspond to a higher priority. The traffic of class C (C =1, 2, 3….C) is characterized by four parameters:

1. The arrivals of the class C requests modelled as a Poisson process with average arrival rate of λ_c requests/second.

2. The average request size F_c Kbytes is specified by the size of each request.

3. The upper bound of scheduling time τ_c in seconds.

4. The possibility p_c that an arriving request belongs to class C.

The queuing model illustration diagram is depicted in Figure 6.2.

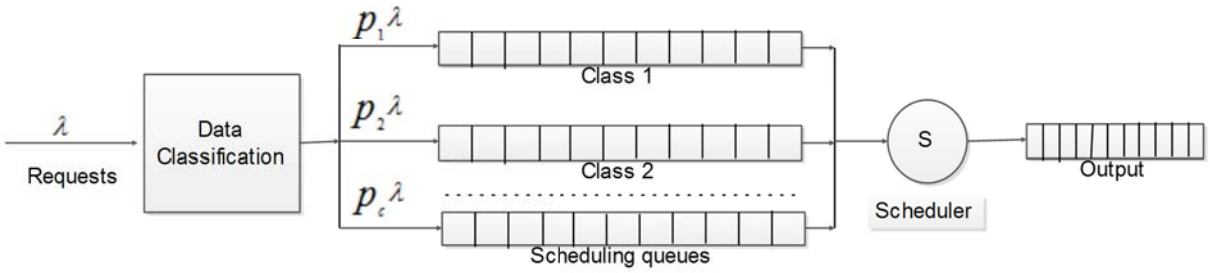


Figure 6-2 Queuing Model [196]

In order to simplify the queuing model, we assume that the model consists of queues connecting to a scheduler, and each queue is used to hold the traffic of the corresponding class. Requests can be

served immediately at the scheduling rate by the scheduler. In this research, we employ the pre-emptive priority service scheme [196].

In the queuing model, the scheduling rate for class C is denoted as $S_{sch}^{(c)}$. We have $S_{total} = \sum_{c=1}^{C} S_{sch}^{(c)}$ The average size of requests of class c- is F_c . Thus, the scheduling time for class-C traffic flows is assumed to follow a Poisson distribution with mean time of ($F_c/S_{sch}^{(c)}$). In accordance with the composition property of Poisson Process, the arrivals of task requests in class-C follow a Poisson process with arrival rate $\lambda_c = p_c\lambda$ and the total arrivals of all requests follow a Poisson process with average arrival rate $\lambda = \sum_{c=1}^{C} \lambda_c$. In a pre-emptive priority M/M/1 queuing system, the mean scheduling time for class- data flow is given by; [197]

$$T_{sch}^{(c)} \frac{(F_c/S_{sch}^{(c)}}{1-\beta_{sch}^{(c-1)}} + \frac{\sum_{j-1}^{c} p_c \lambda F_j^2 / S_{sch}^{(j)^2}}{(1-\beta_{sch}^{(c-1)})(1-\beta_{sch}^{(c)})} p_1 \lambda \tag{53}$$

where,

$$\beta_{sch}^{(c)} = \sum_{j=1}^{c} \frac{p_j \lambda F_j}{S_{sch}^{(c-1)}}.$$

To ensure the scheduling queue is stable, $\beta_{sch}^{(c)} = \sum_{j=1}^{c} \frac{p_j \lambda F_j}{S_{sch}^{(c-1)}} < 1.$ should be satisfied

6.2.3 Performance of Queuing System

To measure the performance of the queuing system it is important to understand the properties of the incoming flow of requests, service times and service disciplines. The arrival process can be characterized by the distribution of the inter-arrival times of the data expressed by;

$$A(t) = P(interarrival\ time < t) \tag{54}$$

In queuing theory, these inter-arrival times are assumed to be independent and identically distributed random variables. And called service request, its function is denoted by (t) , that is

$$B(x) = P(service\ time < x) \tag{55}$$

The arrangement of service and service discipline indicate to us the number of servers and the capacity of the system. If maximum number of customers are staying in the system, the service discipline determines the rule according to the next customer is selected. The rules used are

- FIFO - First In First Out.
- LIFO - Last Come First Out.
- RS - Random Service.

For simplicity consider first a single-server system, let traffic intensity, to be defined as;

$$Traficc\ intercity \frac{mean\ service\ time}{mean\ inter\ arriving\ time} \tag{56}$$

Assuming an infinite data packets system arrival intensity λ which is reciprocal of the mean inter-arrival time, and let the mean service be denoted by $1/\mu$. If traffic intensity > 1 then the systems is overloaded since the requests arrive faster than they are served. It shows that more servers are needed.

6.2.4 System Model

The system was modelled to ensure the robustness between the SMs and the data concentrator and from the data concentrator to data management centre. OPNET was used over other simulation tools such as OMMET++ because it offers flexibility to develop a detailed model.The model of the network was divided into four categories as follows:

- Model design.
- Applying statistics.
- Run simulation.
- View and analyse the results.

The simulation is executed in the OPNET platform using editor's tools. Key OPNET editors are as follows:

- *Project editor*: is used to create a network model. The OPNET network project model comprises of subnets, nodes, protocols, transmission links and the simulation and analysis and be executed here.
- *Node editor*: is used to create node models. Node models represent transmitters, receivers, switches etc.

- *Process editor:* is used to create process models. A process model within a device such as a personal computer could represent transmission and reception of packets on a network card.
- *Link editor*: is used to create, edit and view network link models. The transmission ink features can be defined using the editor.
- *Packet Format editor*: is used to create packet format models.
- *PDF (Probability Density Function) editor*: PDF is used to control certain events such as frequency of packet generation in a model.
- *Probe editor*: Used to specify what simulation results should be collected.
- *Analysis editor*: For analysing simulation results. Advanced statistical analysis functions are available.

Further descriptions of these editors can be found from the OPNET help tool. There are several advanced editors but those will not be used in these laboratory sessions. If the results are not satisfactory, then the network has to be re-modelled and then new statistics be implemented [198] [199]. The basic workflow of OPNET model is shown in Figure 6.3.

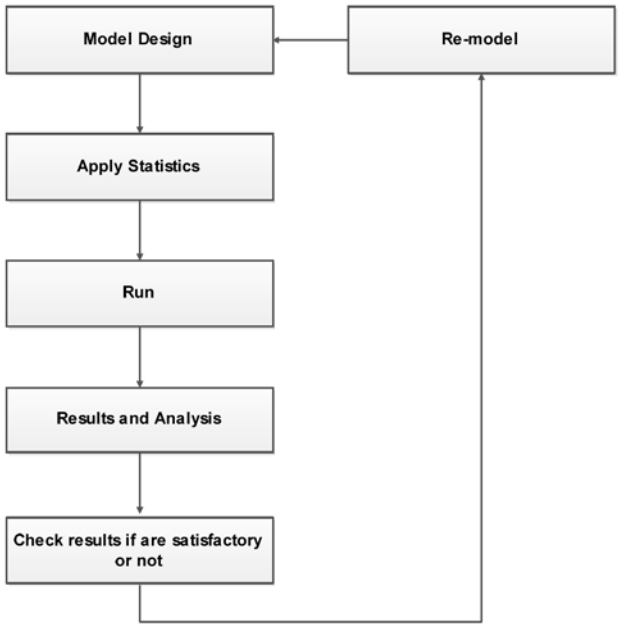


Figure 6-3 Workflow with OPNET [200]

The SM reports usage data and it provides unsophisticated functions such as sending an alarm and interacting with smart appliances at home. In this design, the SM actively monitors the power consumed by electrical devices and forwards the data to the utility provider [200]. A load management system model screenshot set up that was developed to run simulation is depicted in Figure 6.4. This setup has a power management centre, a router, connected to WAN. All SMs are connected to a data concentrator. The data concentrator communicates with the control centre. In that way the SM information is sent to control centre for billing purposes.

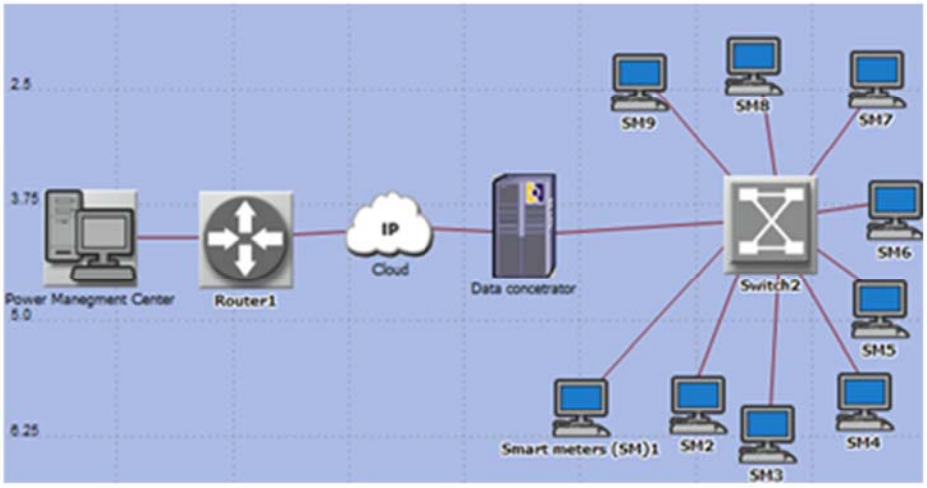


Figure 6-4 Load Management System Developed Simulation Screen Shot.

The utility provider manages the entire network. The utility collector collects all usage data from every SM in a neighbourhood via the star network model and then transmits the data to the utility billing system. The SM communicates through two-way communication to transfer and receive data to the utility; each SM can send and receive the data only from neighbours with a low-rate PLC. After transferring the data from each SM to the utility collector, each SM will resend the data from the neighbourhood meter until the packages reach the utility collector. All communications and routing in the network is driven by the utility provider [201].

6.3 Design Goals

The design goals are to improve the security and privacy in SMs by developing a new set of security rules that will enhance PLC network. Implementing AES protocol ensures data integrity. In addition, intrusion detection scheme will be necessary in order to avoid a SM compromise attack. The requirements of the best protocol to meet the design goals are as follows:

- Low data rate communication but secure to protect privacy.
- The protocol must be cost effective.
- Provide privacy of consumer data in a communication channel.
- Confidentiality, integrity, authentication, and non-repudiation with acceptable data latency must be guarantee.

6.4 Simulation

Simulation of AMI network was performed using OPNET and the simulation of encryption performed using Java NetBeans 8.5.2. Since many SMs are connected in the PLC network, it is important to choose a suitable communication bandwidth to enable real-time two-way information exchange [202]. There are two types of communication link channel speed which have to be analysed in this research These communication channel speeds are simulated in order to determine throughput and data propagation delay on the network.

6.4.1 Bandwidth Analysis of PLC Network

Bandwidth is the speed that a network element can forward traffic. Both physical and available bandwidths are independent of both ends host and protocol type [203]. The bandwidth of the PLC network channel shall not be a limiting element in SM network for AMI. The figure that shown how bandwidth is structured is depicted in Figure 6-5.

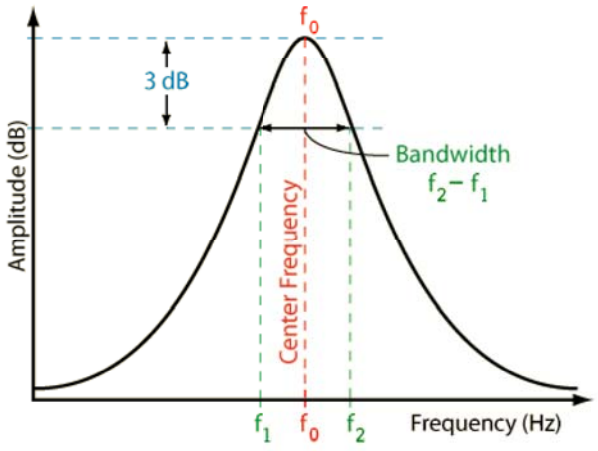


Figure 6-5 Bandwidth [203]

Some terms that are mostly used in this section are defined as follows.

- Maximum Burst Size (MBS) - is the maximum number of bytes transmitted sequential from a source to a destination on the network at certain period without dropping any data packets.
- Bandwidth - is the speed that a network can forward traffic without backing data due to size.
- Throughput - is amount of data successfully sent from a source to destination via a network. It is determined by hardware and software.
- Utilization - is the percentage of the capacity on a link currently being used by traffic.
- Available bandwidth - is the band capacity minus traffic over a given time.

A high bandwidth communications network is essential to allow excellent communication between SM and the utility [204]. The equation to calculate bandwidth can be expressed as:

$$Bw = \frac{f_r}{Q} \tag{57}$$

Or

$$Bw = f_2 - f_1 \tag{58}$$

where

BW=Bandwidth

f_r=resonating frequency

f_2=Upper cut off frequency

f_1=Lower cut off frequency

The available bandwidth is calculated by using;

$$\begin{aligned} A(t_s, t_e) &= Capacity - Trafic \\ &= C \times (1 - U) \\ &\neq A(T_{window}) \\ T_{window} &= (t_s - t_e) \end{aligned} \tag{59}$$

where,

t_s =time when measurement started

t_e =time when measurement ended

The communications arrangement that facilitates fast and secure data flow is mandatory for SM network. The communication speeds from 10 Mbps to 100 Mbps is required and it is proposed for the near future. SM networks require a robust network to transfer data control of devices and data collection. The data must be visible at real time. The real time processing is very critical as part of future distribution systems and data management.

6.4.2 Smart Meter Representation in OPNET

A SM is a device that is installed on a customer's premises to collect data and relay this back to the utility. It can be connected to a switch or hub on the network by a duplex link in order to transmit and receive information. It collects data and dispenses it to the utility. The data packets are transferred through the Ethernet switch, router, and firewall to the server (control centre). Since there is no SM device on the OPNET libraries, hereby we represent it by using a computer work-station derived from the package library SM [205], [206].

6.5 Network Modelling and Simulation

Two different models were developed and once again relying on OPNET to analyse network performance.

The simulation statistics were defined using required network parameters from the OPNET tools settings. The statistics are as follows:

- Application configuration.
- Profile configuration.
- Virtual Private Network configuration (VPN).
- Server.
- Nodes.

6.5.1 Application and Profile Configuration

The following statistics were set on the applications attribute: FTP, HTTP, Email and Database query. Medium and heavy browsing were used to specify the required applications in the simulation models of the SM network [207].

The profile configuration statistics that are used are: FTP, HTTP Database Email. Heavy and medium browsing were used to create user profiles and these profiles can be defined on different nodes of the network design to generate the traffic on the network.

6.5.2 Virtual Private Network (VPN) Configuration

VPN offers a secured transfer of information over the PLC network. VPN can also be used on the simulation to increase data packet latency. Encryption and decryption are done by this application, as well as wrapping and unwrapping the data packets.

6.5.3 Server (Control Centre) and Nodes

The server runs and monitors all applications using TCP/IP protocol. The services supported and used can be defined in the server. The profiles may support FTP, HTTP, database and email medium as well as heavy browsing.

Workstation nodes include SMs, Ethernet switches, Ethernet hubs, routers, and firewalls running on the network. In this case, workstation is represented by the SM on the network.

6.5.4 Apply Statistics of Smart Meter Network

There are two types of statistics that are essential to design a model on OPNET. The statistics are as follows:

- Global statistics.
- Object statistics.

Global statistics are gathered from the entire design of the network model and the object statistics could be gathered on individual nodes. Global statistics are: Data Base (DB) query, email response time, FTP response time and HTTP response time. Object or node statistics for the client are: client DB, client DB entry, client DB queue, client FTP, client email, client HTTP, server CPU utilization, server DB, server FTP, server email and server HTTP. The link statistic are queuing delay, throughput, and utilization [208].

6.6 Modelling and Analysis of Smart Meter Network

To model the PLC SM network two scenarios were considered. The illustration of an OPNET network model for scenario one is shown as in Figure 6.6. The model was developed on personal computer and the firewall added to enhance data security.

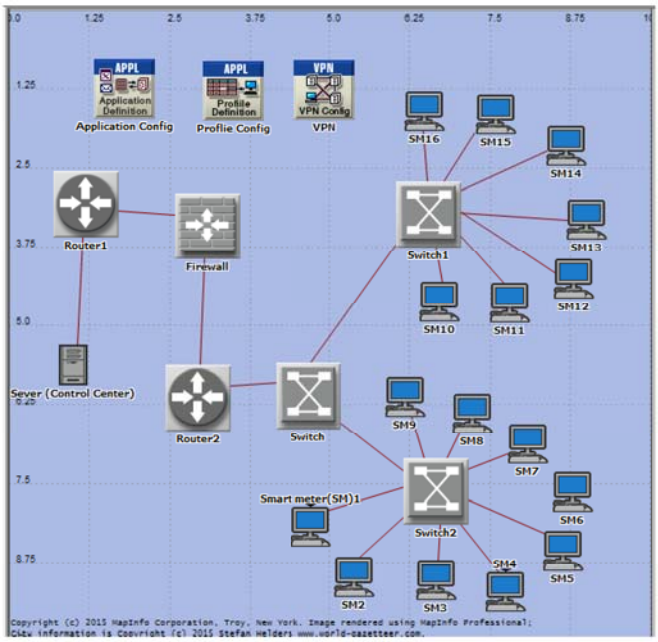


Figure 6-6 Screen Snapshot of OPNET Smart Meter Network with Firewall.

6.6.1 Network Model Scenario 1

In scenario one, network devices model for simulation was created. The model has SMs together with the network, Ethernet switch, router, firewall and server. The model was configured with a communication link of 10Mbps. The data base query response time was analysed. The database query response is the time elapsed when the request is sent to the server and a response is received. It is observed that the response time of the SM on communication channel running at 10 Mbps link is 0.2 ms with slight spike at 0.22 ms and the data query response is 0.18 ms on the 100 Mbps communication link. It has also been discovered that the reaction time appears to level off with time at 100Mbps which means that the network becomes more stable at bigger bandwidth network.

The bandwidth becomes more efficient when it has capacity. The efficient bandwidth can be expressed as:

$$\eta B = \frac{C}{B} - \log(1 - {}^{S}/_{N}) \tag{60}$$

where,

C=Chanel capacity

B=Bandwidth

S/N= Signal to noise ration

The robustness of the networks was analysed using data transmission delays propagation delay and data throughput. Transmission delay is a function of the packet's length and has nothing to do with the distance between the two nodes. This delay is proportional to the packet's length in bits, and it is:

$$T_{trans}^{cs} = \frac{D}{R} \tag{61}$$

Where

D is data

R is transmission rate

$$\left\lceil {}^{D}/_{(L-A)} \right\rceil = 4 \tag{62}$$

$$T_{trans}^{PS} = 4 * A/R + D/R$$

$$T_{trans}^{pkt} = L/R$$

Where

L is packet size

A is header size

Propagation delay T_{prop} is the time that a transmitted bit needs to travel from one end of a link to the other end. The end-to-end propagation delay is calculated using:

$$T_{prop}^{e2e} = (T_{prop}^{A\to 2} + T_{prop}^{1\to 2} + T_{prop}^{2\to B}) \tag{63}$$

Roundtrip delay equation is.

$$T_{prop}^{rt} = 2T_{pro}^{e2e} \tag{64}$$

Adding all together, we come up with a one formula to calculate the data packets delay as;

$$Delay^{data\ pkt} = T_{prop}^{e2e} + 3\left(T_{Proc} + T_{trans}^{pkt}\right) + \left(T_{queue}^{1} + T_{queue}^{2} + T_{queue}^{3}\right) \quad (65)$$

To prevent packets loss, the data packets data should be sent to bandwidth less or equal to the receiving rate which should also be equal to sending rate. The receiving rate can be expressed as:

$$R_{rev} = \frac{\sum_{i-2}^{n} PT_i}{\left(\sum_{i-2}^{n} PT_i\right) + \sum_{i-2}^{n} PT_i} xC_p \quad (66)$$

$$\frac{PT}{PT + XT} xC_p = \frac{R_{snd}}{R_{snd} + R_{xt}} = xC_p$$

$$R_{xt} = \frac{R_{snd}}{R_{rev}} xC_p - R_{snd}$$

$$A_{bw} = C_p = R_{st} - \left(\frac{R_{snd}}{R_{rev}} x\ C_p - R_{snd}\right)$$

$$R_{snd} - C_p\ x\left(\frac{R_{snd}}{R_{rev}} - 1\right)$$

Where

A_{bw} is available bandwidth

C_p is capacity of path

XT is cross traffic

PT is probe traffic

R_{snd} is sending rate

R_{rev} is receive rate

R_{rev} is cross traffic flow rate

It is vital to identify these statistics since there are many data packets coming from the SMs. If the network is not well planned to suit the data traffic, it can bring a substantial challenge. Some of the

data packets can be lost. Using the OPNET model facilitates easy development of larger network models and analysis to prove the model's functionality [209] [210].

6.6.2 Simulation Database Query Response Time of the Network

The graph of Figure 6.7 shows the results obtained from the OPNET simulation. It is established from the graph that the response time has increased significantly with respect to the increased bandwidth. The data base query response time line graph for 10 and 100Mbps network is depicted Figure 6.7. The time response at 100Mbps gives us better time at 0.18 ms which is less than 0.2 ms at 10Mbps.

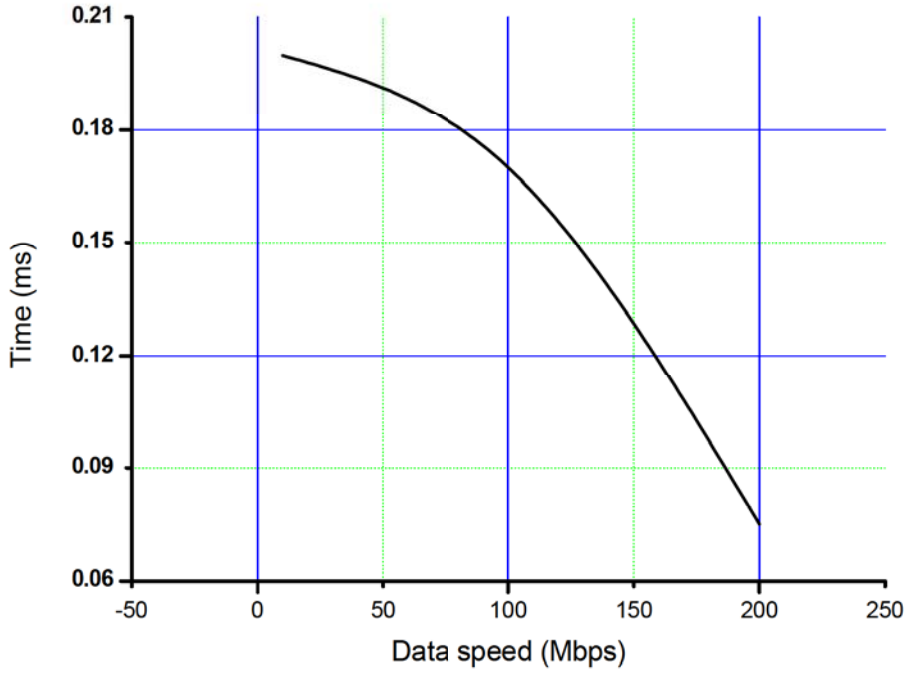


Figure 6-7 Data Base Query Response Time Line Graph

6.6.3 Simulation Results—Data Throughput from Router to Server

Figure 6.8 presents the data throughput point-to-point from router to server where the units are bits/sec. The data throughput with 10 Mbps and 100 Mbps communication link are compared from the simulation results. The data throughput of 10Mbps link is 11000 bits/sec as compared to that of 100Mbps that is 14000 bits/sec. It is evident from results analysis that the data throughput is greater with the bigger bandwidth. Throughput load (bits/second) line graph of analysis for both 10 and 100 Mbps is depicted in Figure 6.8.

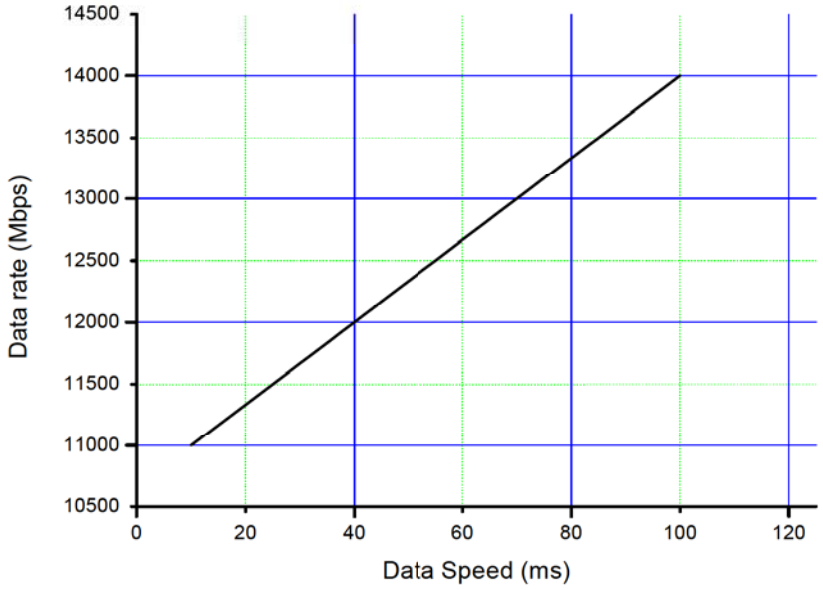


Figure 6-8 Mbps Throughput Load (bits/second) Line Graph of Analysis

6.6.4 Scenario 2

A secured and resilient AMI network is very important in order to run electricity data management system [73]. In order to attain good security, the firewall is used to provide basic security when internal and external users try to obtain unauthorised access to the SM network.

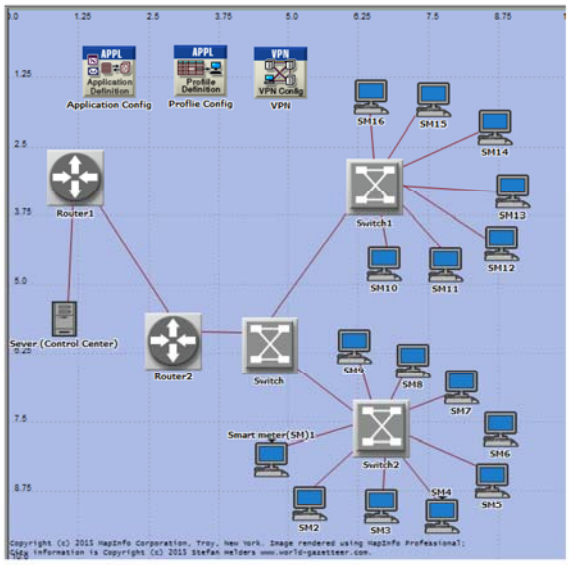


Figure 6-9 Smart Meter Network Without Firewall

Firewall configuration can be set in such a way that it is able to reject the transmission of data packets from certain IP addresses. The firewalls are essential to have on the network to protect the network from malicious and unauthorised access to the network but it adds data processing delay [211]. An OPNET network model of SM network without firewall is depicted in Figure 6.9. The analysis of the SM network with the firewall network slightly increases CPU usage and increase the data delay time. Since the firewall increases the data security and integrity of the network it is imperative that the firewall be introduced despite its data propagation delays [212] [213]. Figure 6.9 has the firewall removed to prove the process delay caused by the existence of the firewall on the network. It is observed that after the firewall was removed delay improve. Table 6.1 tabulates the times for 10Mbps and 100Mbps obtained from simulation results.

Table 6-1 Summary of Simulation Results with 10 and 100 Mbps Network

Scenarios	Data base query (ms)		Throughput Bits/sec		Server utilization (%)	
	10 Mbps	100 Mbps	10 Mbps	100 Mbps	10 Mbps	100 Mbps
Scenario 1 Smart meter network consisting of 16 smart meters, three switches , two routers, firewall and the server	0.21	0.18	11000	14000	20	16
Scenario 2 Smart meter network consisting of 16 smart meters, three switches, two routers and the server	0.2	0.17	11000	14000	22	17

6.7 Simulation Results and Analysis

The SM networks scenarios obtained during simulation depicted in Table 6.1 were used to analyze the database query response time, throughput and server utilization. Table 6.1 gives a summary of simulated outcomes of database query response time, throughput router to the server and server utilization using communicating link of 10 Mbps and 100 Mbps on the networks. The graph representation and interpretation of the simulation is portrayed in Figure. 6.10. Looking at the graph Figure 6.10 the response time in *ms* is better for 100Mbps. The data query response is 0.17 for 100Mbps. Changing the link capacity or decreasing it to 10Mbps it is seen that the data query response increase to 0.2 that is an increase in delay due to link capacity decrease.

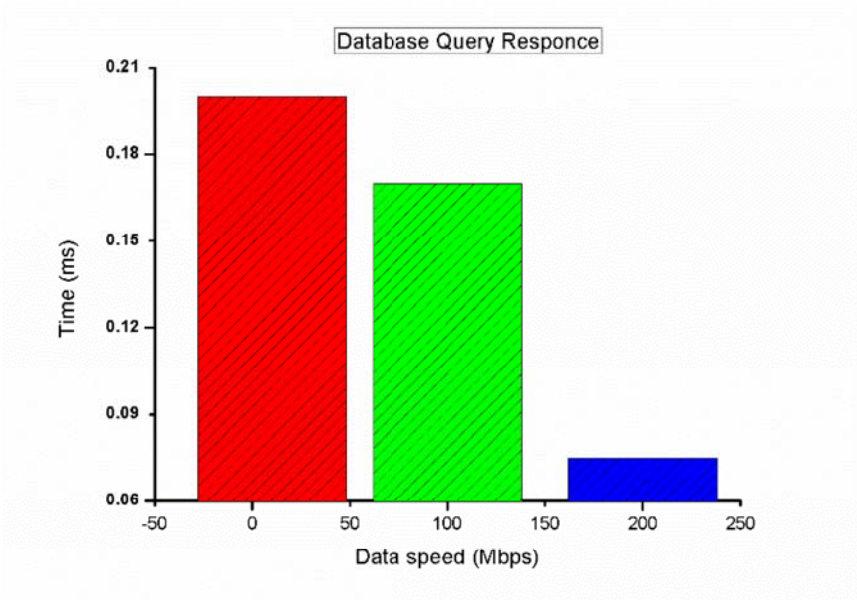


Figure 6-10 Data Query Response

The CPU utilization with respect to data speed is depicted in Figure 6.11. It is observed from the graph that the less the speed the high is the CPU utilization. In order to use less of the CPU in the saver it is required that the data speed used increased to 100Mbps. This gives the CPU more space to execute instruction faster. This results in CPU processing instruction as they sent. If there is less speed in getting to the CPU, then this slowly causes the CPU to be busy executing instruction all the time.

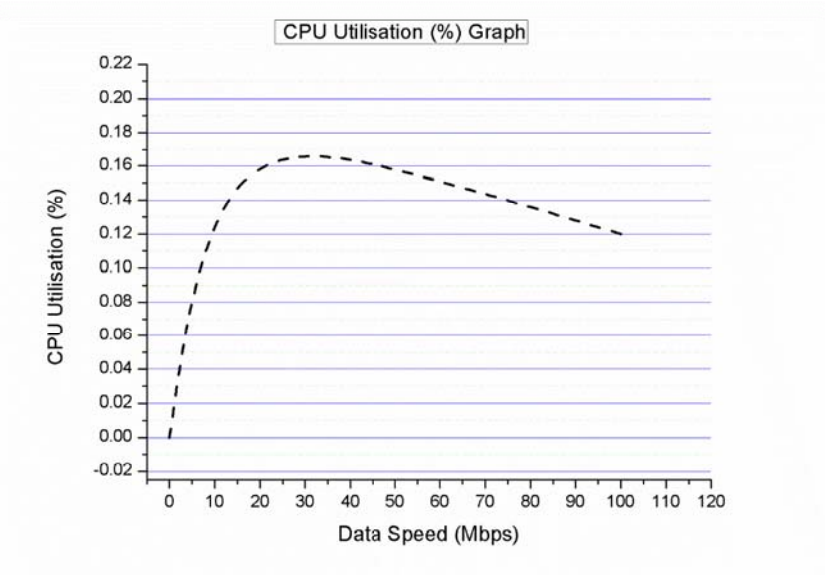


Figure 6-11 CPU Utilization

Figure 6.12 shows the simulated result of data throughput with respect to link bandwidth. With the increase in bandwidth, there is an increase in data throughput. From 10Mbps to 50 Mbps it is observed in the graph that the data throughput is 11000 bits/s. The throughput increased when the bandwidths is increased and it is evident in the graph that from 65Mbps to 120 the data throughput increased. In particular, the data throughput at 100Mbps is 14000 Mbps.

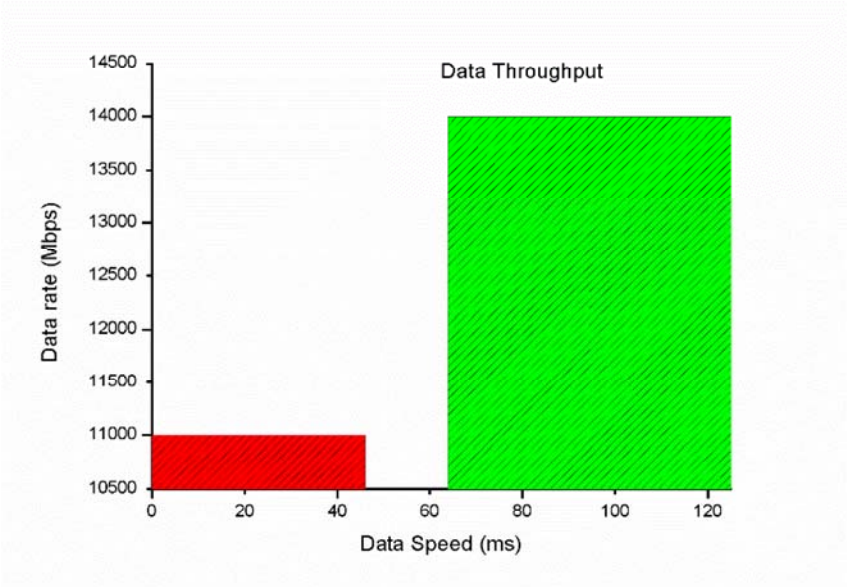


Figure 6-12 Data Throughput

It can be concluded that from the simulation graphical analysis that with an increase in bandwidth, the network parameters will react as follows:

- With an increase in bandwidth, the data base query response increases.
- With an increase in bandwidth, the data throughput also increases.
- With an increase in bandwidth, the server utilisation decreases.

Using the results above, it can be concluded that for a fast and a reliable network we require our SG network with a highest data speed of 100Mbps. The lowest speed of 10 Mbps can also be used in a low traffic SG network. On 100Mbps network, the AES encryption works well to protect the data against malicious attacks.

6.8 Summary Conclusions

In this chapter OPNET is used to simulate the PLC transmission channel. Both the modelling and simulation has helped us demonstrate that the PLC system when implemented, will function as per our set performance objectives.

With the help of an appropriate queuing model we were able to ascertain the required bandwidth to support the desired data speed in the PLC network .The simulation results were either graphed or tabulated and analysis carried out. The latter show a relative improved performance in comparisons with what is reported elsewhere in literatures.

Specifically we note that as per achieved simulation results we note that an increase in bandwidth will increase supportable data rates at the same time improving the response times. With an increase in bandwidth, the data throughput will also increase. However, an increase in bandwidth reciprocates the server utilisation in that it tends to decrease. The results demonstrate the feasibility of operating existing PLC communication infrastructures at 100Mbps which will facilitate practical realisation of SGs. All the same low speeds of up to 10MBps can still sustain an SG. At 100Mbps speed operation, the AES encryption effectively protects the data against malicious attacks.

7 Discussion and Conclusion

7.1 Discussion

Energy efficiency is important as it is a pillar of economic growth. This is the reason a number of countries around the world have been focusing on energy efficiency. Environmentally friendly SG is required to alleviate the strain on the grid and threats of blackouts. SG have a sophisticated network arrangement which may be exploited to access private information and sensitive data. This therefore spells the need for it to be secured. Energy theft and the metering information are amongst the biggest challenges related to the SG application.

Based on simulation results and analysis, the AES algorithm has proven to be the best to encryption and decrypt data on SG network. The modification proved that the AES can even be faster to encrypt and decrypt data packets, and that was proven by Java compiler when comparing the original AES to modified AES. OPNET helped in proving which bandwidth was required to run PLC network for SG. This research recommended a 100Mbps network but 10 Mbps can also be used for low data rate PLC such as narrow band PLC.

PLC network was chosen for data transmission from the meter to utility control centre. PLC uses the existing power lines to transmit data. The information is transferred on a conductor that is simultaneously used for carrying Alternate Current (AC) power to consumers. PLC uses existing electrical power grid infrastructure because it is less costly and more popular. The communication channel between customers and the utility should have confidentiality which protects consumers' privacy. A survey was conducted on PLC technologies such as obsolete X-10 and other protocols such as LonWorks, CEBus and HomePlug. The communication techniques were investigated to establish the better and secure communication algorithm. The authentication protocols and algorithm schemes were also investigated.

In this thesis, we addressed securing data on load management system over PLC network. The focus was mostly on data encryption, authentication and physical security. The investigation also examined all types of encryption algorithms and their challenges. The survey on power line technologies possible attacks and threats were also executed. After the research was executed on securing the smart metering, the AES algorithm was presented as the most effective and fastest on hardware and software to secure SG for utility data load management. The AES algorithm was

modified to handle data packets faster during encryption and decryption. Through simulation of the modified AES algorithm, it is proven that modified AES will best serve a better security for SG.

7.2 Findings Summary

7.2.1 PLC Research

PLC was investigated to discover a robust technique to transmit data for SG efficiently. The study was conducted on PLC network and it was discovered that the PLC channel has attenuation level issue due to some channel factors such as coloured, narrow band, synchronous and impulsive noise. A survey on PLC was also conducted to discover what was done before and what improvement has been made on PLC and it was concluded that OFDM has to be used. The OFDM was implemented on PLC network to overcome PLC channel hash conditions.

The research addressed the objective

a) Based on the primary objectives of this research project the first objective was to survey security threats in PLC (SG) and possible solutions. The survey was conducted and it was found that there are high security threats for insecure SGs and the solution was to implement a secure algorithm to protect this network as presented in chapter 4.

b) The second objective was to identify an effective security framework for an SG network. The security framework was identified and was modified to suit the PLC network.

c) Thirdly, the study sought to explore a candidate encryption/decryption algorithm that ensures secure as well as minimal latency when implemented.

d) Fourthly, the study sought to ensure smooth data aggregation as well as safeguarding in a SG network all the above statement support the credibility of these findings.

7.2.2 PLC Protocols Implementations on SG

PLC implementations challenges in SG were executed to run the current energy demand. The PLC protocols, new and old, were surveyed such as X-10, CeBus, home plug, MAC Protocol and LON works. The protocols were compared using data transmission rate and data size. The robustness of the protocols were also investigated, specifically to establish how protocols can handle load management using SMs. The findings on data security of these protocols were that these protocols are

insecure and they do not have robust and adequate security for SG. X-10 has excessive attenuation between two live conductors and can only transmit one command at a time. X-10 is relatively slow and has low data rate. X-10 was only for control and command of electric appliances and therefore does not include security algorithm. Message Authentication Code (MAC) protocol is vulnerable and works on peer-to-peer protocol. The protocol does not have the authentication to verify self-reported identity, therefore MAC protocol is vulnerable to spoofing attack. Lon Works is a peer-to-peer communication; the data on the protocol is transmitted as a plain text. Lon Works use short key for authentication and has no mechanism to dispute the key. CEBus is a packet peer to per protocol and uses communication to application language known as CAL. CEBus has never considered data security. Home plug offers very little data security and very low data rate at a very low speed. To enhance security on all these protocols, a second security protocol is added such as AES.

7.2.3 Data Encryption and Decryption

Comparison of encryption and authentication protocols were executed to develop the algorithm to safeguard the SG. The data risk management and potential data attacks were implemented. Mitigation techniques were also put in place. The algorithms such as X509, DES, 3DES, AES, ABE, RSA, MARS, RC6, Serpent and Twofish were investigated by simulation and analysis. The table of comparison was formulated and AES emerged as the most effective algorithm for SG.

7.2.4 Advanced Encryption Standard (AES)

The comparison of AES with other encryption algorithms with respect to key length, cipher block, block size, crypto resistance, data security, data size and encryption / decryption speed was executed. Eventually, AES was selected as the most effective algorithm to efficiently secure PLC data and it was proposed algorithm for SG. Due to some additional requirements such as encryption speed enhancement, AES algorithm was modified by to lessen the encryption and decryption algorithm calculations time and to enhance speed when transmitting big data size. The modification was done on the code using Java. The MixColumn step was replaced by Permutation. The modification was meant to minimise algorithm encryption calculation to improve encryption decryption latency on 128 bits AES without compromising security.

7.2.5 Simulation

Java NetBeans 8.0.2 compiler was used to simulate the efficiency of modified AES. The simulation of the modified and unmodified (original) AES code was executed using a computer to change

code and simulate. The original Java code to encrypt and decrypt 16 bits data takes 290ms and modified takes 247ms. These results proved the efficiency of modified AES by 43ms on 16-bits file data size.

7.3 Conclusion

The Power Line Communication network does not employ security measures to secure data transmission on the PLC network. The problem with this network is the lack of data security in PLC and that exposes Advanced Metering Infrastructure to serious threats with very dangerous consequences such as SMs spoofing, eavesdropping, SM data manipulation, bringing down economy due to power being stolen. PLC has its own channel characteristic that make it unique and different to other communication mediums. PLC channel poses noise and high attenuation but was chosen because it already install and is the cheaper way to get house hold SMs.

This thesis provides a review of all PLC protocols that have been used before and currently and proposes the better protocol to secure PLC SG. The focus of the protocol requirements were as follows: Encryption Authentication, Robustness. The threat to PLC security was surveyed to generate a robust security algorithm.

To better understand PLC network the PLC channel was studied and simulated using MATLAB. The PLC protocols were also investigated such as X10, Lon Work, CeBus and Home plug. The encryption techniques were also investigated such as AES, DES, Tow Fish, RSA, Mars, 3DES. Eventually, AES was presented as the mostly effective encryption scheme for PLC SG, but due to latency issues, original AES was modified. Through simulation in chapter 6 it was proven that AES data security is credible.

Java NetBeans 8.0.2 compiler was used to modify the AES encryption and decryption code and to simulate the AES encryption. It was discovered that the modified AES performed better than the normal AES for this purpose of data encryption since the mix column stage was modified and replaced with a preamble that has less computations therefore reducing encryption time but not compromising its data security.

Few software packages were utilised such as MATLAB, Java and OPNET. The OPNET modeller was utilised to analyse the SM network. Several scenarios were investigated and the different simulation models were tested using 10 Mbps and 100 Mbps communication links. It was observed that the firewall imposed on the network increased propagation delay time. The simulated results

from diverse SM networks structure proves that the 100 Mbps link is most appropriate to run SM network. The data speed of 10 Mbps can still be used to implement PLC network because they do not carry more data than electricity utility data management.

7.4 Future Work

There is need for extensive research to be undertaken on the feasibility of two way communications for SG for better data security. The PLC network is the network of the future and one that has to be adopted for SG since it reaches almost all households that have electricity in urban and rural areas. A better PLC protocol should be calibrated that will cater for data transmission security. SG has the potential to solve energy crisis. SG can help the world to manage the electrical grid and avoid load shedding. It is therefore recommended that more research be intensified to emerge with a powerful security system and standards for PLC SG.

8 References

[1] S. Lee, "Review of System Architecture and Security Issues for Smart Grid," *International Journal of Advanced Science and Technology,* vol. 53, pp. 111-116, 2013.

[2] R. Tongia, "Can broadband over powerline carrier (PLC) compete? A techno-economic analysis," *Telecommunications Policy,* vol. 28, pp. 559-578, 2004.

[3] A. Mannan, D. Saxena, and M. Banday, "A Study on Power Line Communication," *International Journal of Scientific and Research Publications,* vol. 4, 2014.

[4] Y. Yan, Y. Qian, and H. Sharif, "A secure and reliable in-network collaborative communication scheme for advanced metering infrastructure in smart grid," in *Wireless Communications and Networking Conference (WCNC), 2011 IEEE*, 2011, pp. 909-914.

[5] M. Costache and V. Tudor, "Security Aspects in the Advanced Metering Infrastructure," 2011.

[6] R. E. Brown, "Impact of smart grid on distribution system design," in *Power and Energy Society General Meeting-Conversion and Delivery of Electrical Energy in the 21st Century, 2008 IEEE*, 2008, pp. 1-4.

[7] P. Chanyagom, I. Kopriva, H. H. Szu, and J. S. Landa, "Communication through narrowband powerline channel using underdetermined blind signal separation," *tC,* vol. 1, p. 1, 2003.

[8] M. A. Faisal, "Securing Advanced Metering Infrastructure (AMI) in Smart Grid using Intrusion Detection System (IDS)," Masdar Institute of Science and Technology, 2012.

[9] F. Zwane, *Power Line Communication Channel Modelling*: Citeseer, 2014.

[10] S. Galli, A. Scaglione, and Z. Wang, "For the grid and through the grid: The role of power line communications in the smart grid," *Proceedings of the IEEE,* vol. 99, pp. 998-1027, 2011.

[11] S. McLaughlin, D. Podkuiko, S. Miadzvezhanka, A. Delozier, and P. McDaniel, "Multi-vendor penetration testing in the advanced metering infrastructure," in *Proceedings of the 26th Annual Computer Security Applications Conference*, 2010, pp. 107-116.

[12] R. Rashed Mohassel, A. Fung, F. Mohammadi, and K. Raahemifar, "A survey on Advanced Metering Infrastructure," *International Journal of Electrical Power & Energy Systems,* vol. 63, pp. 473-484, 2014.

[13] S. Galli, A. Scaglione, and Z. Wang, "Power line communications and the smart grid," in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, 2010, pp. 303-308.

[14] K. Adak, J. Mohamed, and S. H. Darapuneni, "Advanced Metering Infrastructure Security," ed: Technical report, University of Colorado, Boulder, 2009.

[15] K. Alfaheid, "*A Secure and Compromised-Resilient Architecture for Advanced Metering Infrastructure*," University of Ontario Institute of Technology, 2011.

[16] M. Bauer, W. Plappert, C. Wang, and K. Dostert, "Packet-oriented communication protocols for smart grid services over low-speed PLC," in *Power Line Communications and Its Applications, 2009. ISPLC 2009. IEEE International Symposium on*, 2009, pp. 89-94.

[17] M. S. Yousuf, S. Z. Rizvi, and M. El-Shafei, "Power line communications: An overview-Part II," in *Information and Communication Technologies: From Theory to Applications, 2008. ICTTA 2008. 3rd International Conference on*, 2008, pp. 1-6.

[18] S. T. Mak, "TWACS, a power line communication technology for power distribution network control and monitoring," *IEEE Trans. Power Del.;(United States),* vol. 1, 1986.

[19] M. Gotz, M. Rapp, and K. Dostert, "Power line channel characteristics and their effect on communication system design," *IEEE Communications Magazine,* vol. 42, pp. 78-86, 2004.

[20] N. Sharma, T. Pande, and M. Shukla, "Survey of Power Line Communication," *IJCA, CSI-COMNET,* 2011.

[21] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on smart grid communication infrastructures: Motivations, requirements and challenges," *IEEE communications surveys & tutorials,* vol. 15, pp. 5-20, 2013.

[22] A. M. Tonello, A. Pittolo, and M. Girotto, "Power line communications: understanding the channel for physical layer evolution based on filter bank modulation," *IEICE Transactions on Communications,* vol. 97, pp. 1494-1503, 2014.

[23] S. M. Amin and B. F. Wollenberg, "Toward a smart grid: power delivery for the 21st century," *IEEE power and energy magazine,* vol. 3, pp. 34-41, 2005.

[24] Y. Yan, Y. Qian, and H. Sharif, "A secure and reliable in-network collaborative communication scheme for advanced metering infrastructure in smart grid," pp. 909-914, 2011.

[25] X. Fang, S. Misra, G. Xue, and D. Yang, "Smart grid—The new and improved power grid: A survey," *IEEE communications surveys & tutorials,* vol. 14, pp. 944-980, 2012.

[26] D. Niyato, L. Xiao, and P. Wang, "Machine-to-machine communications for home energy management system in smart grid," *IEEE Communications Magazine,* vol. 49, 2011.

[27] S. S. S. R. Depuru, L. Wang, and V. Devabhaktuni, "Smart meters for power grid: Challenges, issues, advantages and status," *Renewable and sustainable energy reviews,* vol. 15, pp. 2736-2742, 2011.

[28] H. Meng, S. Chen, Y. Guan, C. Law, P. So, E. Gunawan, *et al.*, "A transmission line model for high-frequency power line communication channel," in *Power System Technology, 2002. Proceedings. PowerCon 2002. International Conference on*, 2002, pp. 1290-1295.

[29] H. Meng, S. Chen, Y. Guan, C. Law, P. So, E. Gunawan, *et al.*, "Modeling of transfer characteristics for the broadband power line communication channel," *IEEE Transactions on power delivery,* vol. 19, pp. 1057-1064, 2004.

[30] T. Esmailian, F. R. Kschischang, and P. Glenn Gulak, "In-building power lines as high-speed communication channels: channel characterization and a test channel ensemble," *International Journal of Communication Systems,* vol. 16, pp. 381-400, 2003.

[31] L. Lampe and A. J. H. Vinck, "On cooperative coding for narrow band PLC networks," *AEU - International Journal of Electronics and Communications,* vol. 65, pp. 681-687, 2011.

[32] R. Devi, "Channel estimation and modeling of power line communication," 2013.

[33] N. R. Parhyar, M. A. Shah, and M. M. Lodro, "SIMULATION AND MATHEMATICAL MODELLING OF POWER LINE COMMUNICATION CHANNEL FOR HIGH DATA TRANSFER RATE," *ENGINEERING, SCIENCE & TECHNOLOGY,* p. 13.

[34] D. Wang, Z. Tao, J. Zhang, and A. A. Abouzeid, "RPL based routing for advanced metering infrastructure in smart grid," in *Communications Workshops (ICC), 2010 IEEE International Conference on*, 2010, pp. 1-6.

[35] S. Barmada, A. Musolino, and M. Raugi, "Innovative model for time-varying power line communication channel response evaluation," *IEEE journal on selected areas in communications,* vol. 24, pp. 1317-1326, 2006.

[36] J. Zhou, R. Q. Hu, and Y. Qian, "Scalable distributed communication architectures to support advanced metering infrastructure in smart grid," *IEEE Transactions on Parallel and Distributed Systems,* vol. 23, pp. 1632-1642, 2012.

[37] S. Robson, A. Haddad, and H. Griffiths, "Simulation of power line communication using atp-emtp and matlab," in *Innovative Smart Grid Technologies Conference Europe (ISGT Europe), 2010 IEEE PES*, 2010, pp. 1-8.

[38] V. C. Gungor, B. Lu, and G. P. Hancke, "Opportunities and challenges of wireless sensor networks in smart grid," *IEEE transactions on industrial electronics,* vol. 57, pp. 3557-3564, 2010.

[39] V. C. Güngör, D. Sahin, T. Kocak, S. Ergüt, C. Buccella, C. Cecati, *et al.*, "Smart grid technologies: communication technologies and standards," *Industrial informatics, IEEE transactions on,* vol. 7, pp. 529-539, 2011.

[40] K. W. Ackerman, "Timed power line data communication," University of Saskatchewan Saskatoon, 2005.

[41] K. Bhargavi, S. Hiremath, and C. Sowmya, "Power Line Communications Based Control and Monitoring of Industrial Parameter Using Wi□ Fi Technology."

[42] A. A. Atayero, A. Alatishe, and Y. A. Ivanov, "Power line communication technologies: Modeling and simulation of PRIME physical layer," in *World Congress on Engineering and Computer Science*, 2012, pp. 931-936.

[43] A. C. Brooks, S. J. Hoelzer, T. L. Stewart, and I. S. Ahn, "Design and Simulation of Orthogonal Frequency Division Multiplexing (OFDM) Signaling," *Electronic Publication: Digital Object Identifiers (DOIs),* pp. 1-4, 2001.

[44] R. E. Brown, "Impact of smart grid on distribution system design," in *Power and Energy Society General Meeting-Conversion and Delivery of Electrical Energy in the 21st Century, 2008 IEEE*, 2008, pp. 1-4.

[45] N. Chiotellis and P. G. Cottis, "Simulation of a Narrowband Power Line Communications System over Medium Voltage," *Applied Sciences,* vol. 6, p. 90, 2016.

[46] G. Bumiller, "System architecture for power-line communication and consequences for modulation and multiple access," in *7 th International Symposium on Power-Line Communications and its Applications (ISPLC2003), Kyoto, Japan*, 2003.

[47] S. Galli and O. Logvinov, "Recent developments in the standardization of power line communications within the IEEE," *IEEE Communications Magazine,* vol. 46, 2008.

[48] G. Bumiller, L. Lampe, and H. Hrasnica, "Power line communication networks for large-scale control and automation systems," *Communications Magazine, IEEE,* vol. 48, pp. 106-113, 2010.

[49] S. Galli and T. Lys, "Next generation narrowband (under 500 kHz) power line communications (PLC) standards," *China Communications,* vol. 12, pp. 1-8, 2015.

[50] B. Rajkumarsingh and N. S. Poonye, "Modeling Of Power Line Communication Channel For Automatic Meter Reading System With LDPC Codes," *GSTF Journal of Engineering Technology (JET),* vol. 3, p. 61, 2014.

[51] M. H. Chan and R. W. Donaldson, "Amplitude, width, and interarrival distributions for noise impulses on intrabuilding power line communication networks," *IEEE Transactions on Electromagnetic Compatibility,* vol. 31, pp. 320-323, 1989.

[52] A. Ghadrdanizadi, "Security and Feasibility of Power Line Communication System," in *Global Security, Safety and Sustainability: Tomorrow's Challenges of Cyber Security: 10th International Conference, ICGS3 2015, London, UK, September 15-17, 2015. Proceedings*, 2015, p. 244.

[53] J. E. Gilley, "Bit-error-rate simulation using Matlab," *Transcrypt International, Inc,* pp. 1-7, 2003.

[54] B. Hydro, *Smart Metering & Infrastructure Program Business Case*: BC Hydro, 2010.

[55] M. Katayama, T. Yamazato, and H. Okada, "A mathematical model of noise in narrowband power line communication systems," *IEEE Journal on Selected areas in Communications,* vol. 24, pp. 1267-1276, 2006.

[56] J. J. Lee, C. S. Hong, J. M. Kang, and J. W. K. Hong, "Power line communication network trial and management in Korea," *International journal of network Management,* vol. 16, pp. 443-457, 2006.

[57] M. Lee, R. E. Newman, H. A. Latchman, S. Katar, and L. Yonge, "HomePlug 1.0 powerline communication LANs—protocol description and performance results," *International Journal of Communication Systems,* vol. 16, pp. 447-473, 2003.

[58] M. K. Lee, R. E. Newman, H. A. Latchman, S. Katar, and L. Yonge, "HomePlug 1.0 powerline communication LANs?protocol description and performance results," *International Journal of Communication Systems,* vol. 16, pp. 447-473, 2003.

[59] D. Li, Z. Aung, J. R. Williams, and A. Sanchez, "Efficient authentication scheme for data aggregation in smart grid with fault tolerance and fault diagnosis," in *Innovative Smart Grid Technologies (ISGT), 2012 IEEE PES*, 2012, pp. 1-8.

[60] Y. Ma, P. So, Y. Guan, E. Gunawan, K. See, S. Chen, *et al.*, "Evaluation of MAC Protocols for Broadband PLC Networks," in *Proc. 6th International Power Engineering Conference (IPEC2003)*.

[61] T. Van Dam and K. Langendoen, "An adaptive energy-efficient MAC protocol for wireless sensor networks," in *Proceedings of the 1st international conference on Embedded networked sensor systems*, 2003, pp. 171-180.

[62] M. Nassar, A. Dabak, I. H. Kim, T. Pande, and B. L. Evans, "Cyclostationary noise modeling in narrowband powerline communication for smart grid applications," in *Acoustics, Speech and Signal Processing (ICASSP), 2012 IEEE International Conference on*, 2012, pp. 3089-3092.

[63] J. Desbonnet and P. M. Corcoran, "System architecture and implementation of a CEBus/Internet gateway," *IEEE Transactions on Consumer Electronics,* vol. 43, pp. 1057-1062, 1997.

[64] P. M. Corcoran, J. Desbonnet, and K. Lusted, "CE-Bus Network Access via the World Wide Web," *IEEE Trans. Consumer Electronics,* 1996.

[65] V. Clement, R. Mouret, and N. Saint Paul, "Network interfacing system with modules for administrating various protocol layers for a plurality of OSI models," ed: Google Patents, 1998.

[66] S. Panchadcharam, "Performance evaluation of information and communications technology infrastructure for smart distribution network applications," Brunel University School of Engineering and Design PhD Theses, 2012.

[67] H. Zimmermann, "OSI reference model--The ISO model of architecture for open systems interconnection," *IEEE Transactions on communications,* vol. 28, pp. 425-432, 1980.

[68] N. Pavlidou, A. H. Vinck, J. Yazdani, and B. Honary, "Power line communications: state of the art and future trends," *IEEE Communications Magazine,* vol. 41, pp. 34-40, 2003.

[69] G. Ren, S. Qiao, H. Zhao, C. Li, and Y. Hei, "Mitigation of periodic impulsive noise in OFDM-based power-line communications," *Power Delivery, IEEE Transactions on,* vol. 28, pp. 825-834, 2013.

[70] W. Rhee and J. M. Cioffi, "Increase in capacity of multiuser OFDM system using dynamic subchannel allocation," in *Vehicular Technology Conference Proceedings, 2000. VTC 2000-Spring Tokyo. 2000 IEEE 51st*, 2000, pp. 1085-1089.

[71] J. Serrao, A. Fakih, R. Khatik, S. Afzal, and C. Ravindra, "TRANSMISSION OF DATA USING POWER LINE CARRIER COMMUNICATION SYSTEM," *International Journal of Electronics Communication and Computer Technology (IJECCT),* vol. 2, pp. 280-283.

[72] Y.-S. Son, T. Pulkkinen, K.-D. Moon, and C. Kim, "Home energy management system based on power line communication," *IEEE Transactions on Consumer Electronics,* vol. 56, 2010.

[73] T. E. Sung and A. Bojanczyk, "POWER-LINE COMMUNICATIONS AND SMART GRID," *Convergence of Mobile and Stationary Next-Generation Networks,* pp. 317-348, 2010.

[74] B. Tan and J. Tompson, "Powerline communications channel modelling methodology based on statistical features," *arXiv preprint arXiv:1203.3879,* 2012.

[75] M. Tlich, A. Zeddam, F. Moulin, and F. Gauthier, "Indoor power-line communications channel characterization up to 100 MHz—part I: one-parameter deterministic model," *IEEE Transactions on Power delivery,* vol. 23, pp. 1392-1401, 2008.

[76] S.-G. Yoon, D. Kang, and S. Bahk, "OFDMA CSMA/CA protocol for power line communication," in *Power Line Communications and Its Applications (ISPLC), 2010 IEEE International Symposium on*, 2010, pp. 297-302.

[77] M. Zimmermann and K. Dostert, "A multipath model for the powerline channel," *Communications, IEEE Transactions on,* vol. 50, pp. 553-559, 2002.

[78] P. Mlynek, M. Koutny, and J. Misurec, "OFDM model for power line communication," in *Proc. 4th Int. Conf. on Comm. & Info. Tech., CIT10, Greece*, 2010.

[79] W. Zhu, X. Zhu, E. Lim, and Y. Huang, "State-of-Art Power Line Communications Channel Modelling," *Procedia Computer Science,* vol. 17, pp. 563-570, 2013.

[80] M. Zimmermann and K. Dostert, "An analysis of the broadband noise scenario in powerline networks," in *International Symposium on Powerline Communications and its Applications (ISPLC2000)*, 2000, pp. 5-7.

[81] O. Grigoriadis and H. S. Kamath, "Ber calculation using matlab simulation for ofdm transmission," in *Proceedings of the International MultiConference of Engineers and Computer Scientists*, 2008.

[82] I. Ali, "Bit-error-rate (BER) simulation using MATLAB," *International Journal of Engineering Research and Applications,* vol. 3, pp. 706-711, 2013.

[83] T. Pollet, M. Van Bladel, and M. Moeneclaey, "BER sensitivity of OFDM systems to carrier frequency offset and Wiener phase noise," *IEEE Transactions on communications,* vol. 43, pp. 191-193, 1995.

[84] V. P. Singh, "Analysis of Power Line Communication Channel Model Using Communication Techniques," *Circulation,* vol. 701, p. 8888, 2013.

[85] J.-J. Van de Beek, M. Sandell, and P. O. Borjesson, "ML estimation of time and frequency offset in OFDM systems," *IEEE transactions on signal processing,* vol. 45, pp. 1800-1805, 1997.

[86] P. G. Lin, "OFDM simulation in MATLAB," 2010.

[87] X. Li and L. J. Cimini, "Effects of clipping and filtering on the performance of OFDM," in *Vehicular Technology Conference, 1997, IEEE 47th*, 1997, pp. 1634-1638.

[88] D. Sharma and P. Srivastava, "OFDM Simulator Using MATLAB," *International Journal of Emerging Technology and Advanced Engineering,* vol. 3, pp. 493-496, 2013.

[89] M. Zimmermann and K. Dostert, "Analysis and modeling of impulsive noise in broad-band powerline communications," *IEEE transactions on Electromagnetic compatibility,* vol. 44, pp. 249-258, 2002.

[90] T. M. Schmidl and D. C. Cox, "Robust frequency and timing synchronization for OFDM," *IEEE transactions on communications,* vol. 45, pp. 1613-1621, 1997.

[91] S. Ghorpade and M. S. Sankpal, "Behavior of OFDM system using MATLAB simulation," *IJITR,* vol. 1, pp. 249-252, 2013.

[92] R. Amoah, "Formal security analysis of the DNP3-Secure Authentication Protocol," Queensland University of Technology, 2016.

[93] J. Liu, Y. Xiao, S. Li, W. Liang, and C. Chen, "Cyber security and privacy issues in smart grids," *Communications Surveys & Tutorials, IEEE,* vol. 14, pp. 981-997, 2012.

[93] B. Vaidya, D. Makrakis, and H. T. Mouftah, "Authentication and authorization mechanisms for substation automation in smart grid network," *IEEE Network,* vol. 27, pp. 5-11, 2013.

[94] S. Uludag, K.-S. Lui, W. Ren, and K. Nahrstedt, "Secure and scalable communications protocol for data collection with time minimization in the smart grid," 2014.

[95] M. A. Faisal, Z. Aung, J. R. Williams, and A. Sanchez, "Securing advanced metering infrastructure using intrusion detection system with data stream mining," in *Intelligence and Security Informatics*, ed: Springer, 2012, pp. 96-111.

[95] S. Miadzvezhanka, "Protocols for Secure Communication and Traitor Tracing in Advanced Metering Infrastructure," The Pennsylvania State University, 2011.

[96] Y. Zhang, L. Wang, W. Sun, R. C. Green, and M. Alam, "Distributed intrusion detection system in a multi-layer network architecture of smart grids," *Smart Grid, IEEE Transactions on,* vol. 2, pp. 796-808, 2011.

[97] R. Berthier, W. H. Sanders, and H. Khurana, "Intrusion detection for advanced metering infrastructures: Requirements and architectural directions," in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, 2010, pp. 350-355.

[98] M. A. Faisal, Z. Aung, J. R. Williams, and A. Sanchez, "Data-stream-based intrusion detection system for advanced metering infrastructure in smart grid: A feasibility study," *Systems Journal, IEEE,* vol. 9, pp. 31-44, 2015.

[99] R. Jiang, R. Lu, Y. Wang, J. Luo, C. Shen, and X. S. Shen, "Energy-theft detection issues for advanced metering infrastructure in smart grid," *Tsinghua Science and Technology,* vol. 19, pp. 105-120, 2014.

[100] P. Kadurek, J. Blom, J. Cobben, and W. L. Kling, "Theft detection and smart metering practices and expectations in the Netherlands," in *Innovative Smart Grid Technologies Conference Europe (ISGT Europe), 2010 IEEE PES*, 2010, pp. 1-6.

[101] S. Shokooh, T. Khandelwal, F. Shokooh, J. Tastet, and J. Dai, "Intelligent load shedding need for a fast and optimal Solution," *IEEE PCIC Europe,* pp. 1-6, 2005.

[102] K. Wu, R. Karri, G. Kuznetsov, and M. Goessel, "Low cost concurrent error detection for the advanced encryption standard," in *Test Conference, 2004. Proceedings. ITC 2004. International*, 2004, pp. 1242-1248.

[103] R. Jiang, R. Lu, Y. Wang, J. Luo, C. Shen, and X. S. Shen, "Energy-theft detection issues for advanced metering infrastructure in smart grid," *Tsinghua Science and Technology,* vol. 19, pp. 105-120, 2014.

[104] P. Kadurek, J. Blom, J. Cobben, and W. L. Kling, "Theft detection and smart metering practices and expectations in the Netherlands," in *Innovative Smart Grid Technologies Conference Europe (ISGT Europe), 2010 IEEE PES*, 2010, pp. 1-6.

[105] S. Salinas, M. Li, and P. Li, "Privacy-preserving energy theft detection in smart grids," in *Sensor, Mesh and Ad Hoc Communications and Networks (SECON), 2012 9th Annual IEEE Communications Society Conference on*, 2012, pp. 605-613.

[106] C. Efthymiou and G. Kalogridis, "Smart grid privacy via anonymization of smart metering data," in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, 2010, pp. 238-243.

[107] W. Li and X. Zhang, "Simulation of the smart grid communications: Challenges, techniques, and future trends," *Computers & Electrical Engineering,* vol. 40, pp. 270-288, 2014.

[108] D. Li, Z. Aung, J. R. Williams, and A. Sanchez, "No peeking: privacy-preserving demand response system in smart grids," *International Journal of Parallel, Emergent and Distributed Systems,* vol. 29, pp. 290-315, 2014.

[109] D. Mashima and A. A. Cárdenas, "Evaluating electricity theft detectors in smart grid networks," in *International Workshop on Recent Advances in Intrusion Detection*, 2012, pp. 210-229.

[110] S. Salinas, M. Li, and P. Li, "Privacy-preserving energy theft detection in smart grids: A P2P computing approach," *IEEE Journal on Selected Areas in Communications,* vol. 31, pp. 257-267, 2013.

[111] W. Wang and Z. Lu, "Cyber security in the Smart Grid: Survey and challenges," *Computer Networks,* vol. 57, pp. 1344-1371, 2013.

[112] H. Alanazi, B. Zaidan, A. Zaidan, H. A. Jalab, M. Shabbir, and Y. Al-Nabhani, "*New Comparative Study Between DES, 3DES and AES Within Nine Factors*," *arXiv preprint arXiv:1003.4085,* 2010.

[113] J. Blömer and J.-P. Seifert, "Fault based cryptanalysis of the advanced encryption standard (AES)," in *International Conference on Financial Cryptography*, 2003, pp. 162-181.

[114] A. Hahn, "Cyber security of the smart grid: Attack exposure analysis, detection algorithms, and testbed evaluation," 2013.

[115] G. Bertoni, L. Breveglieri, I. Koren, P. Maistri, and V. Piuri, "Error analysis and detection procedures for a hardware implementation of the advanced encryption standard," *IEEE transactions on Computers,* vol. 52, pp. 492-505, 2003.

[116] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A Survey on Cyber Security for Smart Grid Communications," *IEEE Communications Surveys and tutorials,* vol. 14, pp. 998-1010, 2012.

[117] Y. F. Chung, Z. Y. Wu, and T. S. Chen, "Unconditionally secure cryptosystems based on quantum cryptography," *Information Sciences,* vol. 178, pp. 2044-2058, 2008.

[118] P. B. Andersen, E. B. Hauksson, A. B. Pedersen, D. Gantenbein, B. Jansen, C. A. Andersen, *et al.*, "Smart Grid Applications, Communications, and Security," 2012.

[119] S. Gueron, "Intel® Advanced Encryption Standard (AES) New Instructions Set," *Intel Corporation,* 2010.

[120] F. M. Cleveland, "Cyber security issues for advanced metering infrasttructure (AMI)," in *Power and Energy Society General Meeting-Conversion and Delivery of Electrical Energy in the 21st Century, 2008 IEEE*, 2008, pp. 1-5.

[121] C. Adams, S. Farrell, T. Kause, and T. Mononen, "Internet X. 509 public key infrastructure certificate management protocol (CMP)," 2070-1721, 2005.

[122] D. Chadwick, A. Otenko, and E. Ball, "Role-based access control with X. 509 attribute certificates," *IEEE Internet Computing,* vol. 7, pp. 62-69, 2003.

[123] J. Benoit, "An Introduction to Cryptography as Applied to the Smart Grid," *Cooper Power Systems,* 2011.

[124] I. Bestak and M. Orgon, "The use of Encryption Algorithms In PLC Networks," *Simulation,* vol. 3, p. 168, 2012.

[125] P. Chown, "Advanced encryption standard (AES) ciphersuites for transport layer security (TLS)," 2070-1721, 2002.

[126] J. Daemen and V. Rijmen, *The design of Rijndael: AES-the advanced encryption standard*: Springer Science & Business Media, 2013.

[127] A. W. Dent, "Choosing key sizes for cryptography," *Information Security Technical Report,* vol. 15, pp. 21-27, 2010.

[128] G. N. Ericsson, "Cyber security and power system communication—essential parts of a smart grid infrastructure," *IEEE Transactions on Power Delivery,* vol. 25, pp. 1501-1507, 2010.

[129] H. Nicanfar, P. Jokar, K. Beznosov, and V. Leung, "Efficient authentication and key management mechanisms for smart grid communications," *Systems Journal, IEEE,* vol. 8, pp. 629-640, 2014.

[130] R. Gustavsson, "Security Issues and Power Line Communication," in *the Proceedings of the 5th International Symposium on Power-Line Communications and its Application (ISPLC)*, 2001.

[131] J. Thakur and N. Kumar, "DES, AES and Blowfish: Symmetric key cryptography algorithms simulation based performance analysis," *International journal of emerging technology and advanced engineering,* vol. 1, pp. 6-12, 2011.

[132] S. Hameed, F. Riaz, R. Moghal, G. Akhtar, A. Ahmed, and A. G. Dar, "Modified Advanced Encryption Standard For Text And Images," *Computer Science Journal,* vol. 1, 2011.

[133] S. D. Rihan, A. Khalid, and S. E. F. Osman, "A performance comparison of encryption algorithms AES and DES," *International Journal of Engineering Research and Technology,* vol. 4, pp. 151-4, 2015.

[134] G. Singh and A. Supriya, "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security," *International Journal of Computer Applications,* vol. 67, pp. 33-38, 2013.

[135] M.-L. Akkar and C. Giraud, "An implementation of DES and AES, secure against some attacks," in *International Workshop on Cryptographic Hardware and Embedded Systems*, 2001, pp. 309-318.

[136] R. C.-W. Phan, "Impossible differential cryptanalysis of 7-round Advanced Encryption Standard (AES)," *Information processing letters,* vol. 91, pp. 33-38, 2004.

[137] S. Heron, "Advanced encryption standard (AES)," *Network Security,* vol. 2009, pp. 8-12, 2009.

[138] S. Ju, M. Choi, C. Kim, and Y. Lim, "Security Architecture for Advanced Metering Infrastructure," *Advances in Computer Science: an International Journal,* vol. 2, pp. 71-75, 2013.

[139] M. Nagendra and M. C. Sekhar, "Performance improvement of Advanced Encryption Algorithm using parallel computation," *International Journal of Software Engineering and Its Applications,* vol. 8, pp. 287-296, 2014.

[140] S. H. Kamali, R. Shakerian, M. Hedayati, and M. Rahmani, "A new modified version of advanced encryption standard based algorithm for image encryption," in *Electronics and Information Engineering (ICEIE), 2010 International Conference On*, 2010, pp. V1-141-V1-145.

[141] S. Kaplantzis and Y. A. Sekercioglu, "Security and smart metering," in *European Wireless, 2012. EW. 18th European Wireless Conference*, 2012, pp. 1-8.

[142] S. Yu, "Data sharing on untrusted storage with attribute-based encryption," Faculty of the WORCESTER POLYTECHNIC INSTITUTE In partial fulfillment of the requirements for the Degree of Doctor of Philosophy in Electrical and Computer Engineering July 2010 Approved: Professor Wenjing Lou Professor Kaveh Pahlavan ECE Department ECE Department Dissertation Advisor Dissertation Committee Professor Berk Sunar Professor Jie Wang ECE Department CS Department, UMASS Lowell, 2010.

[143] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proceedings of the 13th ACM conference on Computer and communications security*, 2006, pp. 89-98.

[144] B. Padmavathi and S. R. Kumari, "A survey on performance analysis of DES, AES and RSA algorithm along with LSB substitution," *Int. J. Sci. Res,* vol. 2, pp. 170-174, 2013.

[145] Z. M. Fadlullah, N. Kato, R. Lu, X. Shen, and Y. Nozaki, "Toward secure targeted broadcast in smart grid," *IEEE Communications Magazine,* vol. 50, 2012.

[146] A. Nadeem and M. Y. Javed, "A performance comparison of data encryption algorithms," in *Information and communication technologies, 2005. ICICT 2005. First international conference on*, 2005, pp. 84-89.

[147] P. Kawle, A. Hiwase, G. Bagde, E. Tekam, and R. Kalbande, "Modified Advanced Encryption Standard," *International Journal of Soft Computing and Engineering (IJSCE),* vol. 4.

[148] B. Schneier and D. Whiting, "A Performance Comparison of the Five AES Finalists," in *AES Candidate Conference*, 2000, pp. 123-135.

[149] H. Khurana, M. Hadley, N. Lu, and D. A. Frincke, "Smart-grid security issues," *IEEE Security & Privacy,* pp. 81-85, 2010.

[150] S. Kim, E. Y. Kwon, M. Kim, J. H. Cheon, S.-h. Ju, Y.-h. Lim, *et al.*, "A secure smart-metering protocol over power-line communication," *Power Delivery, IEEE Transactions on,* vol. 26, pp. 2370-2379, 2011.

[151] Y.-J. Kim, M. Thottan, V. Kolesnikov, and W. Lee, "A secure decentralized data-centric information infrastructure for smart grid," *Communications Magazine, IEEE,* vol. 48, pp. 58-65, 2010.

[152] U. Kretzschmar, "AES128–AC Implementation for Encryption and Decryption," *TI-White Paper,* 2009.

[153] M. Tunstall, D. Mukhopadhyay, and S. Ali, "Differential fault analysis of the advanced encryption standard using a single fault," in *IFIP International Workshop on Information Security Theory and Practices*, 2011, pp. 224-233.

[154] J. Liu, Y. Xiao, S. Li, W. Liang, and C. P. Chen, "Cyber security and privacy issues in smart grids," *IEEE Communications Surveys & Tutorials,* vol. 14, pp. 981-997, 2012.

[155] D. L. K. D. A. Reddy and S. Jilani, "Implementation of 128-bit AES algorithm in MATLAB."

[156] P. McDaniel and S. McLaughlin, "Security and privacy challenges in the smart grid," *IEEE Security & Privacy,* pp. 75-77, 2009.

[157] P. Abhijith, M. Goswami, S. Tadi, and K. Pandey, "Optimized Architecture for AES," *IACR Cryptology ePrint Archive,* vol. 2014, p. 540, 2014.

[158] A. R. Metke and R. L. Ekl, "Security technology for smart grid networks," *Smart Grid, IEEE Transactions on,* vol. 1, pp. 99-107, 2010.

[159] C.-C. Lu and S.-Y. Tseng, "Integrated design of AES (Advanced Encryption Standard) encrypter and decrypter," in *Application-Specific Systems, Architectures and Processors, 2002. Proceedings. The IEEE International Conference on*, 2002, pp. 277-285.

[160] H. Mohan and A. R. Reddy, "Performance analysis of AES and MARS encryption algorithms," *IJCSI International Journal of Computer Science Issues,* vol. 8, pp. 1694-0814, 2011.

[161] S. Raza, N. S. Malik, A. Shakeel, and M. I. Khan, "Implementation and Comparative Analysis of the Fault Attacks on AES," *Int. Arab J. Inf. Technol.,* vol. 10, pp. 625-634, 2013.

[162] V. Rijmen and J. Daemen, "Advanced encryption standard," *Proceedings of Federal Information Processing Standards Publications, National Institute of Standards and Technology,* pp. 19-22, 2001.

[163] M. Ebrahim, S. Khan, and U. B. Khalid, "Symmetric algorithm survey: a comparative analysis," *arXiv preprint arXiv:1405.0398,* 2014.

[164] M. B. Sagar and K. Venkatesh, "SECURITY ISSUES OF POWER LINE MULTI-HOME NETWORKS FOR SEAMLESS DATA TRANSMISSION," 2013.

[165] L. Scripcariu and M. Frunza, "Modified Advanced Encryption Standard," in *11th international conference on development and application systems, Romania*, 2012, pp. 87-90.

[166] D. Selent, "Advanced encryption standard," *Rivier Academic Journal,* vol. 6, pp. 1-14, 2010.

[167] S. M. Seth and R. Mishra, "Comparative Analysis Of Encryption Algorithms For Data Communication 1," 2011.

[168] R. Shankar and P. Dananjayan, "Security enhancement with optimal qos using eap-aka in hybrid coupled 3g-wlan convergence network," *arXiv preprint arXiv:1007.5165,* 2010.

[169] A. A. Shtewi, B. E. M. Hasan, and A. Hegazy, "An efficient modified advanced encryption standard (MAES) adapted for image cryptosystems," *IJCSNS International Journal of Computer Science and Network Security,* vol. 10, pp. 226-232, 2010.

[170] A. Sterbenz and P. Lipp, "Performance of the AES Candidate Algorithms in Java," in *AES Candidate Conference*, 2000, pp. 161-165.

[171] R. Newman, S. Gavette, L. Yonge, and R. Anderson, "Protecting domestic power-line communications," in *Proceedings of the second symposium on Usable privacy and security*, 2006, pp. 122-132.

[172] C. Bekara, T. Luckenbach, and K. Bekara, "A privacy preserving and secure authentication protocol for the advanced metering infrastructure with non-repudiation service," *Proc. of ENERGY,* 2012.

[173] G. Kalogridis, C. Efthymiou, S. Z. Denic, T. Lewis, and R. Cepeda, "Privacy for smart meters: Towards undetectable appliance load signatures," in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, 2010, pp. 232-237.

[174] H. Li, S. Gong, L. Lai, Z. Han, R. C. Qiu, and D. Yang, "Efficient and secure wireless communications for advanced metering infrastructure in smart grids," *IEEE Transactions on Smart Grid,* vol. 3, pp. 1540-1551, 2012.

[175] L. F. Montoya, "Power Line Communications Performance Overview of the Physical Layer of Available protocols," *ref. http://latchman. list. ufl. edu/~ montoya/index. html,* 1998.

[176] K. Moslehi and R. Kumar, "A Reliability Perspective of the Smart Grid," *IEEE Transactions on Smart Grid,* vol. 1, pp. 57-64, 2010.

[177] A. R. Naik and L. B. Damahe, "Enhancing Data Security and Access Control in Cloud Environment using Modified Attribute Based Encryption Mechanism," *International Journal of Computer Network & Information Security,* vol. 8, 2016.

[178] A. Narayanan, "The Emerging Smart Grid: Opportunities for Increased System Reliability and Potential Security Risks," 2012.

[179] J. Yan, "Modelling and analysis on smart grid against smart attacks," University of Rhode Island, 2013.

[180] S. Elyengui, R. Bouhouchi, and T. Ezzedine, "The Enhancement of Communication Technologies and Networks for Smart Grid Applications," *arXiv preprint arXiv:1403.0530,* 2014.

[181] G. Singh, "A study of encryption algorithms (RSA, DES, 3DES and AES) for information security," *International Journal of Computer Applications,* vol. 67, 2013.

[182] K. H. Zuberi, "Powerline carrier (plc) communication systems," *Stockholm, Royal Institute of Technolog,* 2003.

[182] D. Mashima and A. A. Cárdenas, "Evaluating electricity theft detectors in smart grid networks," in *International Workshop on Recent Advances in Intrusion Detection*, 2012, pp. 210-229.

[183] M. Winanda, A. Satriawan, and Y. S. Gondokaryono, "Smart grid secure data transmission for high voltage grid," in *Information Technology Systems and Innovation (ICITSI), 2014 International Conference on*, 2014, pp. 70-75.

[184] G. A. Pagani and M. Aiello, "Power grid complex network evolutions for the smart grid," *Physica A: Statistical Mechanics and its Applications,* vol. 396, pp. 248-266, 2014.

[185] J.-J. Van De Beek, O. Edfors, M. Sandell, S. K. Wilson, and P. O. Borjesson, "On channel estimation in OFDM systems," in *Vehicular Technology Conference, 1995 IEEE 45th*, 1995, pp. 815-819.

[186] S. Fries, H. J. Hof, T. Dufaure, and M. G. Seewald, "Security for the Smart Grid–Enhancing IEC 62351 to Improve Security in Energy Automation Control," *International Journal on Advances in Security Volume 3, Number 3 & 4, 2010,* 2010.

[187] L. Thomas, A. Burchill, K. Samarakoon, Y. He, J. Wu, J. Ekanayake, *et al.*, "Control of electricity networks using smart meter data," 2012.

[188] S. M. Wadi and N. Zainal, "Rapid Encryption Method based on AES Algorithm for Grey Scale HD Image Encryption," *Procedia Technology,* vol. 11, pp. 51-56, 2013.

[189] S. M. Wadi and N. Zainal, "High Definition Image Encryption Algorithm Based on AES Modification," *Wireless Personal Communications,* vol. 79, pp. 811-829, 2014.

[190] S. B. Ghosn, P. Ranganathan, S. Salem, J. Tang, D. Loegering, and K. E. Nygard, "Agent-oriented designs for a self healing smart grid," in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, 2010, pp. 461-466.

[191] Q. Zhu and T. Ba°ar, "Robust and resilient control design for cyber-physical systems with an application to power systems," in *Decision and Control and European Control Conference (CDC-ECC), 2011 50th IEEE Conference on*, 2011, pp. 4066-4071.

[192] M. Ouyang, L. Dueñas-Osorio, and X. Min, "A three-stage resilience analysis framework for urban infrastructure systems," *Structural safety,* vol. 36, pp. 23-31, 2012.

[193] F. Aalamifar, A. Schlögl, D. Harris, and L. Lampe, "Modelling power line communication using network simulator-3," in *Global Communications Conference (GLOBECOM), 2013 IEEE*, 2013, pp. 2969-2974.

[194] J. Anatory, M. Kissaka, and N. Mvungi, "Channel model for broadband power-line communication," *IEEE transactions on power delivery,* vol. 22, pp. 135-141, 2007.

[195] S. A. B. Bakr, "Design, simulation, and emulation of a residential load management algorithm utilizing a proposed smart grid environment for the mena region," *CU Theses,* 2012.

[196] J. Li, Y. He, Y. Tie, and L. Guan, "Optimal resource allocation for LTE uplink scheduling in smart grid communications," *International Journal of Wireless Communications and Mobile Computing,* pp. 113-118, 2013.

[197] S. Sadeghi, M. H. Yaghmaee Moghddam, M. Bahekmat, and A. Heydari Yazdi, "Modeling of Smart Grid traffics using non-preemptive priority queues," in *Smart Grids (ICSG), 2012 2nd Iranian Conference on*, 2012, pp. 1-4.

[198] S. S. Rezaie, S. A. Hoseini, and H. Taheri, "Implementation of Extensible Authentication Protocol in OPNET Modeller."

[199] M. Panteli and P. Mancarella, "The grid: Stronger, bigger, smarter?: Presenting a conceptual framework of power system resilience," *IEEE Power and Energy Magazine,* vol. 13, pp. 58-66, 2015.

[200] S. McLaughlin, D. Podkuiko, and P. McDaniel, "Energy theft in the advanced metering infrastructure," in *International Workshop on Critical Information Infrastructures Security*, 2009, pp. 176-187.

[201] D. Cao and I. Andonovic, "Research on backbone communication network in smart grid by using OPNET," in *Smart Measurements for Future Grids (SMFG), 2011 IEEE International Conference on*, 2011, pp. 130-134.

[202] M. Padmaraj, V. Venkataraghavan, and S. Nair, "Simulation of Network Security Protocols," *Proceedings of OPNET WORKS,* 2002.

[203] F. Guo, L. Herrera, R. Murawski, E. Inoa, C.-L. Wang, P. Beauchamp, *et al.*, "Comprehensive real-time simulation of the smart grid," *IEEE Transactions on Industry Applications,* vol. 49, pp. 899-908, 2013.

[204] A. Bharathan and J. McNair, "An OPNET Modeler Simulation Study of the VISA Protocol for Multi-Network Authentication," in *Proceedings of the OPNET Network Modeling and Simulation Conference (OPNETWORK'03)*, pp. 1-5.

[205] G. F. Lucio, M. Paredes-Farrera, E. Jammeh, M. Fleury, and M. J. Reed, "Opnet modeler and ns-2: Comparing the accuracy of network simulators for packet-level analysis using a network testbed," *wseas transactions on computers,* vol. 2, pp. 700-707, 2003.

[206] R. Kaparti, "OPNET IT Guru: A tool for networking education," *REGIS University,* 2011.

[207] H. Kellerbauer and H. Hirsch, "Simulation of powerline communication with OMNeT++ and INET-Framework," in *Power Line Communications and Its Applications (ISPLC), 2011 IEEE International Symposium on*, 2011, pp. 213-217.

[208] C. H. J. Wu and T. Liu, "Simulation for intrusion-resilient, DDoS-resistant authentication system (IDAS)," in *Proceedings of the 2008 Spring simulation multiconference*, 2008, pp. 844-851.

[209] A. Kuki, "Modeling computer networks by the help of OPNet tools."

[210] H. Meng, Y. L. Guan, and S. Chen, "Modeling and analysis of noise effects on broadband power-line communications," *IEEE Transactions on Power delivery,* vol. 20, pp. 630-637, 2005.

[211] Y. Bi, J. Zhao, and D. Zhang, "Research on power communication network and power quality monitoring using OPNET," in *Industrial Electronics and Applications, 2007. ICIEA 2007. 2nd IEEE Conference on*, 2007, pp. 507-511.

[212] H. Lin, S. S. Veda, S. S. Shukla, L. Mili, and J. Thorp, "GECO: Global event-driven co-simulation framework for interconnected power system and communication network," *IEEE Transactions on Smart Grid,* vol. 3, pp. 1444-1456, 2012.

[213] X. Sun, Y. Chen, J. Liu, and S. Huang, "A co-simulation platform for smart grid considering interaction between information and power systems," in *Innovative Smart Grid Technologies Conference (ISGT), 2014 IEEE PES*, 2014, pp. 1-6.

9 Appendix A

AES Modified Encryption and Decryption Code

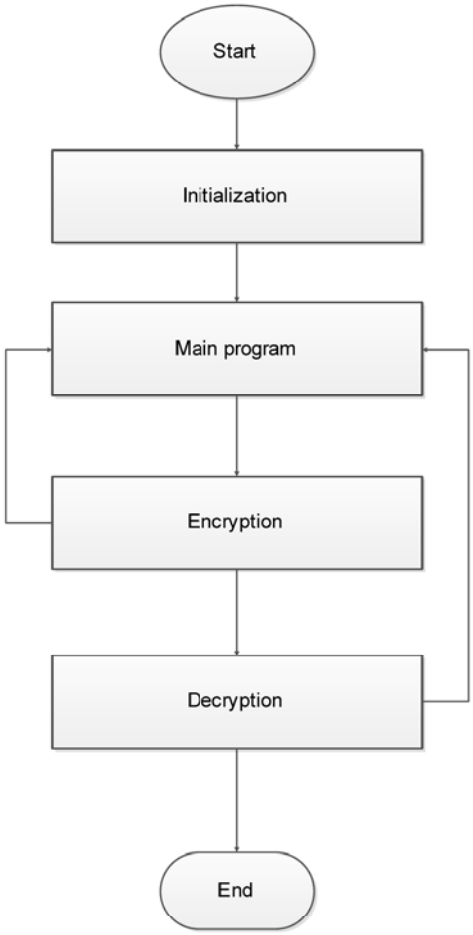
```
package aesmodified;
/* AES Java code
   Author ZP Khumalo
   Student No 20250262
   This code will encrypt and decrypt data using AES algorithm.
*/

import javax.crypto.Cipher; //Algorithm parameters specification initialization
import javax.crypto.spec.IvParameterSpec;//Algorithm parameters specification initialization
import javax.crypto.spec.SecretKeySpec;//Algorithm parameters specification initialization
/**
 *
 * @author KhumaloPK
 */
public class AESModified
{
  static String IV = "AAAAAAAAAAAAAAAA"; // 16 bit String
  static String plaintext = "test text ABC\0\0\0"; //String to be encrypted
  static String encryptionKey = "0123456790abcdef"; // This is a 128 bit encryption key

  // Main Program
  public static void main(String [] args)
  {

      System.out.println("Start program");
  // Errow hangling code
    try
    {

      System.out.println("==Java==");
      System.out.println("plain: " + plaintext);

      byte[] cipher = encrypt(plaintext, encryptionKey);// Generating cyper text
```

```
      System.out.print("cipher:  ");// Print cypher
      for (int i=0; i<cipher.length; i++)
        System.out.print(new Integer(cipher[i])+" ");
      System.out.println("");//Print a line

      String decrypted = decrypt(cipher, encryptionKey);//Decrypt the cypher

      System.out.println("decrypt: " + decrypted); //Print the results

    } catch (Exception e) {
      e.printStackTrace();
    }

  }
// Cypher encryption
  public static byte[] encrypt(String plainText, String encryptionKey) throws Exception
  {
    Cipher cipherblock = Cipher.getInstance("AES/CBC/NoPadding", "SunJCE");

    SecretKeySpec key = new SecretKeySpec(encryptionKey.getBytes("UTF-8"), "AES");

    cipherblock.init(Cipher.ENCRYPT_MODE, key,new IvParameterSpec(IV.getBytes("UTF-8")));

    return cipherblock.doFinal(plainText.getBytes("UTF-8"));
  }
//Cipher decryption
  public static String decrypt(byte[] cipherText, String encryptionKey) throws Exception
  {
    Cipher cipher = Cipher.getInstance("AES/CBC/NoPadding", "SunJCE");
    SecretKeySpec key = new SecretKeySpec(encryptionKey.getBytes("UTF-8"), "AES");
    cipher.init(Cipher.DECRYPT_MODE, key,new IvParameterSpec(IV.getBytes("UTF-8")));
    return new String(cipher.doFinal(cipherText),"UTF-8");
  }
```

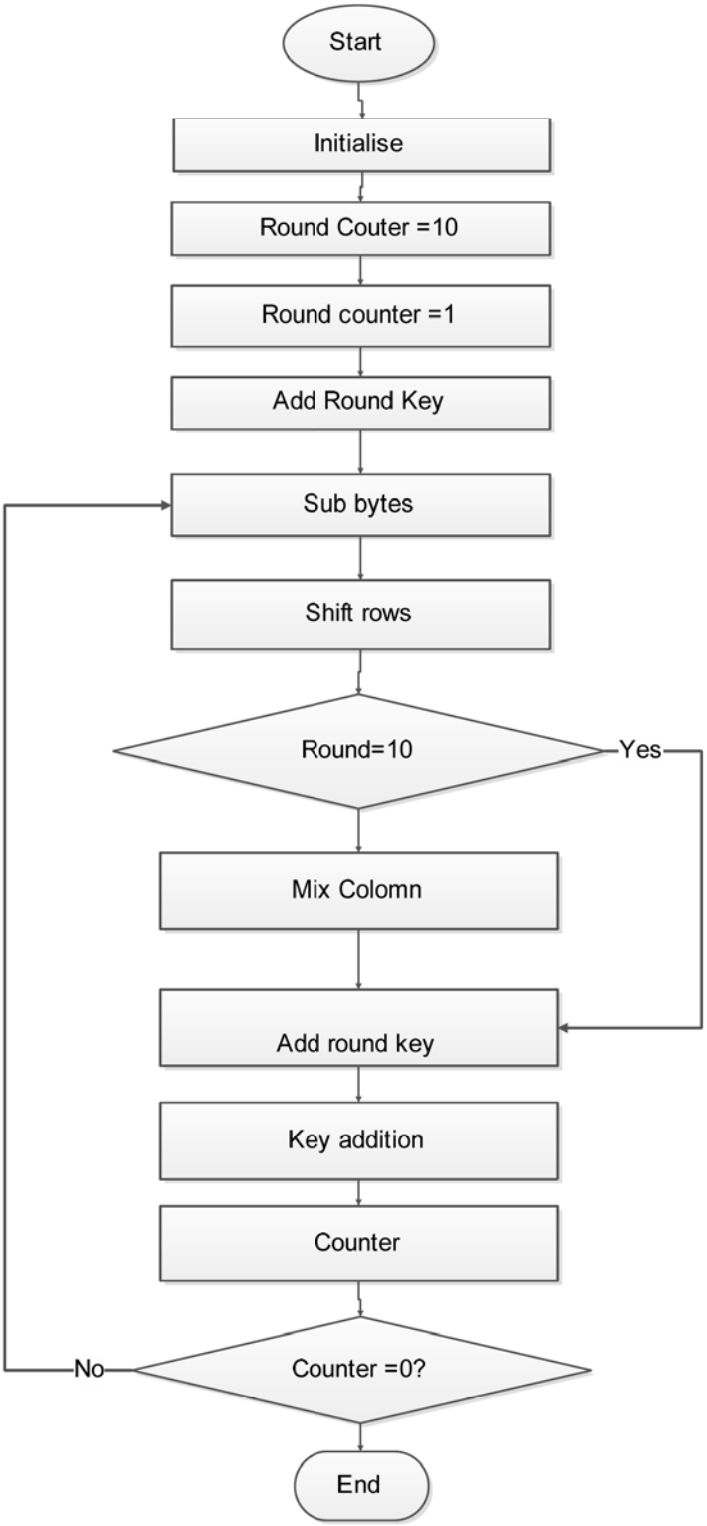
10 Appendix B

Modified AES Flowcharts

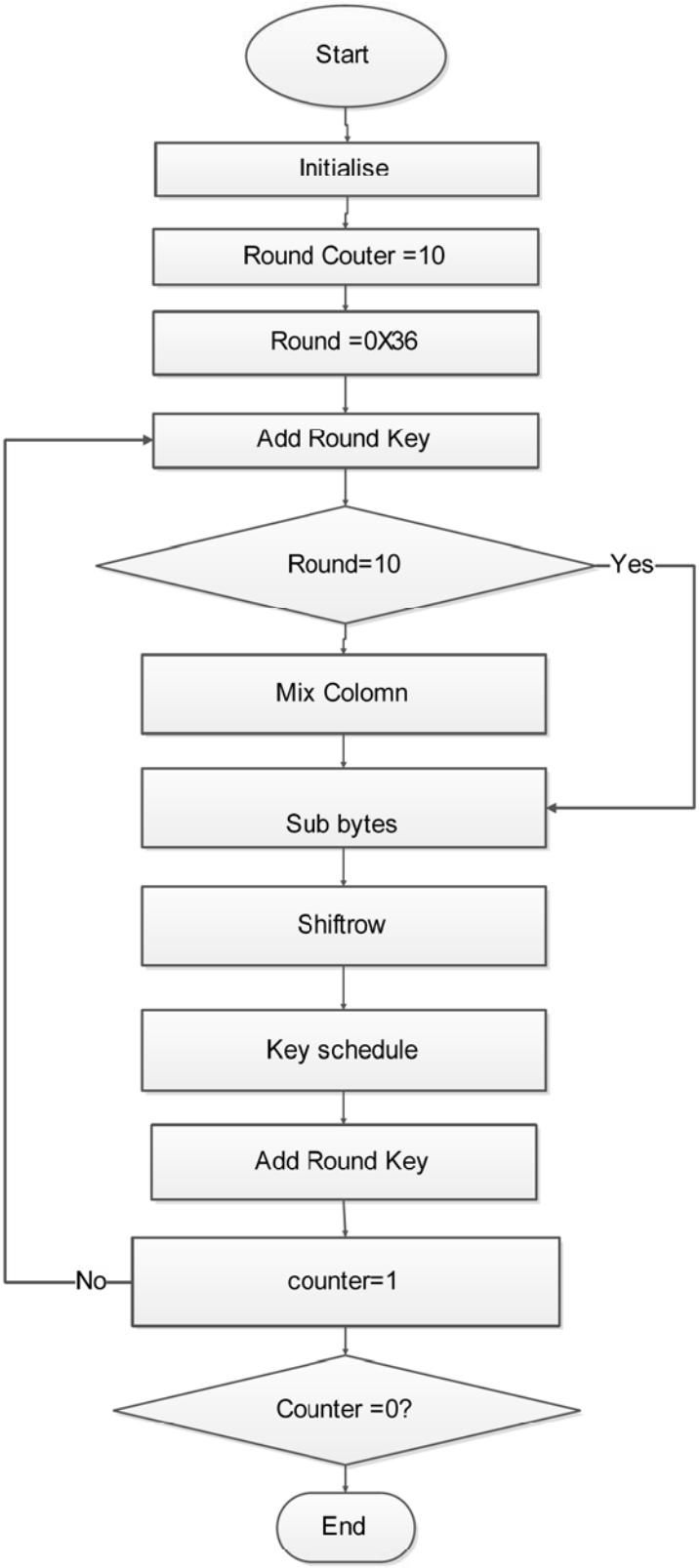
AES Main Program



AES Encryption Subroutine



AES Decryption Subroutine



11 Appendix C

MAT LAB CODE for Bit Error Rate Simulation

```
N = 10^6 % number of bits or symbols
rand('state',100); % initializing the rand() function
randn('state',200); % initializing the randn() function
% Transmitter
ip = rand(1,N)>0.5; % generating 0,1 with equal probability
s = 2*ip-1; % BPSK modulation 0 -> -1; 1 -> 1
n = 1/sqrt(2)*[randn(1,N) + j*randn(1,N)]; % white gaussian noise, 0dB variance
Eb_N0_dB = [-3:10]; % multiple Eb/N0 values
for ii = 1:length(Eb_N0_dB) % Noise addition
y = s + 10^(-Eb_N0_dB(ii)/20)*n; % additive white gaussian noise
% receiver - hard decision decoding
ipHat = real(y)>0; % counting the errors
nErr(ii) = size(find([ip- ipHat]),2);
end
simBer = nErr/N; % simulated ber
theoryBer = 0.5*erfc(sqrt(10.^(Eb_N0_dB/10))); % theoretical ber
% plot close all figure
semilogy(Eb_N0_dB,theoryBer,'b.-');
hold on
semilogy(Eb_N0_dB,simBer,'mx-');
axis([-3 10 10^-5 0.5]) grid on legend('theory', 'simulation');
xlabel('Eb/No, dB');
 ylabel('Bit Error Rate');
title('Bit error probability curve for BPSK modulation');
```

12 Appendix D

Publications

[1] Z.P Khumalo, B. Nleya, "Secured Smart Grid Network for Advanced Metering Infrastructure (AMI)", *SAIEE/ Smart Grid Conference Proceedings*, ESKOM Training centre,Midrand JHB, 25-27 Feb,,. ISBN no. 978-0-620-71202-6.

[2] Z.P Khumalo,B. Nleya. Renewable Energy Technology for Saving and Generating Pollution Free Energy in South Africa. *SAUPEC Proceedings*, Three River Lodge (VUT) Johannesburg.26 to 28 January 2016, ISBN no. 978 1 77012386.

[3] Z.P Khumalo, B. Nleya,"Data Re-Sequencing Delays in Smart Grids". *Proceedings of the IEEE's 3rd international conference on advanced computing and Communication Engineering.* Coastland Hotel, Durban28 to 29 November 2016. ISBN-987-1-5090-2576-6.

[4] Z.P Khumalo, B. Nleya, "A Review of Energy Efficiency Considerations in Optical Backbone Supported Clouds",*Proceedings of SAIEE's Conference on SMART GRIDs*, ESKOM Training centre Midrand JHB, 19-21 Sept, 2017.

[5] Z.P Khumalo, B. Nleya, "System Architecture and Security Overview for Smart Grids", *Proceedings of SAIEE'sConference on SMART GRIDs*, ESKOM Training centre, Midrand JHB, 19-2 Sept., 2017

[6] Z.P Khumalo and B. Nleya, "Secure Power Line Communication Based Network for Advance Metering Infrastructure",*SAUPEC Conference Proceedings*, Protea Hotel , Stellenbosh, 30 January, 01 February 2017.

[7] ZP Khumalo, Green Energy for Energy for Rural Area of South Africa. *JGED Journal of Green Economy and Development. Salt Rock Hote,* North Coast, 13-15 July, 2016.

[8] Z.P Khumalo, "Long Term Evolution LTE and Green Technology for Public Safety", *JGED Journal of Green Economy and Development*.,Salt Rock Hotel, North Coast,13- 15 July, 2016.

[9] Z. P Khumalo and Bakhe Nleya, "Secured Smart Grid Network for Advanced Metering Infrastructure (AMI)", Research Publications (Engineering and Built Environment),DUT, February, 2016.

[10] Z. P Khumalo and B .Nleya, "Sleep-Mode/Traffic Grooming versus Device Reliability Overview., " *To appear in IEEE International Conference on Advances in Big Data, Computing and Data Communication Systems (***icABCD 2018***)*, Durban,6-7 August, 2018.

[11] Z. P Khumalo and B .Nleya, "A Survey of Energy Efficient Optical Backbone Network Approaches for Supporting Cloud Computing", *To appear in IEEE International Conference on Advances in Big Data, Computing and Data Communication Systems (***icABCD 2018***)*, Durban,6-7 August, 2018.

END