Technical Analysis and Mitigation of Electricity Theft for Domestic and Commercial End Users

By

Salome Jiyane-Tshikomba

Student No: 21751239

A thesis submitted in fulfilment of the requirements for the Master of Engineering Degree in the Department of Electrical Power Engineering, Faculty of Engineering and the Built Environment

Durban University of Technology

Supervisor: **Prof. Innocent E. Davidson**

Co-supervisor: **Dr. Evans Eshiemogie Ojo**

August 2019

DECLARATION

I undertake that all materials presented in this thesis is my own work and has not been written for me, in whole or in part by any other person. I undertake that any quotation or paraphrase from the published or unpublished work(s) of another person, has been duly acknowledged in the work, which I now present for examination.

Mr/Ms/Ms Salome Jiyane-Tshikomba _____

Student Number: 21751239

Approved for submission

Supervisor: **Prof. Innocent E. Davidson** _____

Co-Supervisor: **Dr Evans Eshiemogie Ojo** _____

Durban, 30 September 2019

Acknowledgements

I thank Professor Innocent E. Davidson and Dr. Evans Ojo, supervisor and co supervisor respectively for their guidance and support in making this project possible and viable. I also thank all the sponsors who supported all the Durban University of Technology students including me.

I would also like to thank the engineering conference organizers of the following professional organizations: DUT Interdisciplinary Research Conference, SARPA Conference, AMEU Conference and COGTA learning session, where an opportunity was provided for me to present my research work and its outcomes.

I am not forgetting my family members, colleagues and employer who always supported me when I was busy with my studies.

Abstract

Utility services are experiencing common problem of power losses, which impose a big impact on their annual budget. Practically, power losses consist of technical losses and non-technical losses. Technical losses are due to operations and ageing of infrastructure, while non-technical losses (NTL) are due to non-metered energy. The focus is on managing non-technical losses using an automation wireless method. The wireless ZigBee technique is proposed and further investigated for communication failure over long distances, while solving the problem of stealing of electricity. Advance-metering infrastructure (AMI) technique and smart meters are feasible for system integration that is why they are chosen to be part of this study. The success of the study depends on quality data of the Utility, meaning the more accurate the data, the easier the analysis of outliers. The operation and planning of revenue protection contains large amount of data that needs to be worked on, so data mining assist in that regard. Then the load profiling method assist in illustrating the variation in demand/electrical load over a specific time. The wireless communication technique will be used as a viable solution in curbing electricity theft. The uniqueness of the proposed ZigBee system is that it recognizes the common act of stealing electricity through tempering with the meter box and tapping of the supply. The survey and the pilot project was utilized to achieve the goal of the study. The survey conducted is in tandem with the objective of the thesis. The research questions that were developed and tested provided a proven percentage score of positive responses to the questionnaire. Though some respondents were dodgy because they were still happy with the fact that they were still indulging in theft of electricity, therefore, they saw the thesis as an avenue to rob them of freedom to continue the pilferage of electricity without any legal penalties imposed on them. The cost associated with energy losses that are caused by illegal electricity connections will decrease by upgrading the infrastructure, installing the ZigBee technique, and by giving attention to the communication system and its problems. The wellness and workshops need to be conducted so that communities at least once a month will learn the basics of the danger associated with connecting electricity illegally. The pilot project also showed good results, whereby the cost of 3000 units (meters) piloted expense was R8.5Million but the return on investment was R24Million.The proposed ZigBee technique is feasible, and will improve revenue of the Utilities.

Table of Contents

Contents

List of Figures

List of Tables

List of Abbreviations

AMI	Advance Metering Infrastructure
AMR	Automated Meter Reader
GSM	Global System for Mobile Communication
RF	Radio Frequency
LPU	Large Power Users
SPU	Small Power Users
NPD	Network Development Plan
TOU	Time of Use
RTU	Remote Terminal Unit
HMI	Human Machine Interfaces
IED	Intelligent Electronic Device
PCS.	Process Control System
LMR	Land Mobile Radios
PLC	Power Line Communication
WLAN	Wireless Local Area Network
SCADA.	Supervisory Control and Data Acquisition System
PSC	Power System communication
IDS	Intrusion Detection System
SAS	Substation Automation System
VNP	Virtual Private Network
IPSec	IP Security
WSN	Wireless Sensor Network
IoT	Internet of Things
HIV	Human Immunodeficiency Virus
GDP	Gross domestic Product
T &D	Transmission and Distribution
ELP	Energy Loss Programme
BICA	Business Industry Commerce and Agriculture
NTL	Non-Technical losses
TL	Technical Losses

Chapter One

Introduction

1.1 Background

Provision of electricity is a basic need or an exercise of human right in South Africa. The main utility suppliers in South Africa are Eskom and municipalities. Eskom and municipalities have obligations to ensure that most of the citizens are supplied with electricity. This also includes rural areas, irrespective of the financial standing of anyone or the prevalence of poverty in households because the affordability of electricity in South Africa is a *sine qua non*.

Eskom is the largest generator of energy in South Africa but is the least distributor of energy to the end users, in some areas it shares the service delivery with municipalities which as well creates complex situations when service delivery problems arise. Electricity theft is a serious threat to Eskom and municipalities with overwhelming impact; it becomes difficult to sustain economic growth of South Africa, putting strain on the country's annual revenue that could be used for other critical developmental projects. Electrocution due to electricity theft through unsafe illegal connections and meter tempering causes many public fatalities every year. Innocent young children are the most victims. The consequence of electricity theft is higher tariffs for all. Other consequences include, power outages, production downtime, traffic street lights failure, household inconvenience, damaged to appliances etc.
Figures 1 and 2 show how illegal connections are arranged in electric poles and through the wall respectively in the figures.

Figure 1: Illegal connections at Stanger KwaZulu-Natal

Figure 2: Illegal connections at Gauteng, Pretoria

The objective of this study therefore is to aggregate and analyse the non-technical losses in the system and then utilize ZigBee technique as the tool for curbing and mitigating illegal electricity connections while bearing in mind the communication barrier over a long distance.

The structure of the dissertation is as follows: first, load profiling and data mining of the utility system, advance metering infrastructure (AMI), smart metering, global system for mobile communication (GSM) technique and ZigBee technique with its network communication.

1.2 Energy Losses Analysis

Utilities define energy loss as the difference between energy purchased as measured at the transmission networks and the energy sold to all customers. These losses are experienced in the form of technical and non-technical perspectives:

A Technical losses: is a loss that is inherent in the system and refers to the energy lost in the electrical networks due to the flow of current or energisation of the system [1] [2] [3].

Electricity and energy are lost from the distribution system. As electricity flows through substation conductors, heating occurs which energizes the transformer, and when transformers are energized, hysteresis/losses occur in the transformer core, all of which contributes to the loss of electrical energy [2] [4]. Long distribution lines also contribute to the technical losses: overloaded distribution lines contribute to losses as the lines or cables lose energy through heat generated [5]. Ageing distribution infrastructure due to short circuits can also bring about losses.

B Non-technical losses: These losses occur mostly due to electricity theft resulting from unlawful tapping from Utility's infrastructure, network, or bridging of the meters and incorrect billing or non-billing of the customers. [5] [6] [7]. There are factors that may lead to non-technical losses. On the customer data that is received from the municipality, there are business customers that are sitting on residential segmentation tariff. Those businesses are under-billed by paying residential tariffs instead of business tariffs because business tariff includes fixed charges, which are paid monthly without fail. The incorrect K- factor is another cause of revenue loss that can cause the municipality to lose revenue. In some municipalities, the billing data that was analysed, several industrial customers were registered with wrong K-factors, for example on 0.02, 0.04, 0.06, 0.08 and 0.12, in the billing system. The K- factors are based on the voltage ratio and current transformer ratio of the customer [6] [8].

A blanket meter audit of all customers is required to collect and rectify customer data and tariff segmentation. In most cases, the following will be determined:

- Voltage links removed on analogue meters.
- Main circuit breakers tripped on large power users.
- Current transformers short-circuited so that the current to the meter is zero.
- The voltage phases and current phases swopped to misguide meter readings.
- Mismatch of CT ratio on programmable meters.
- Communication cables cut inside the meter.

According to the national treasury report of South Africa, electricity losses in Metros for 2016 and 2017 were R7 193 903 and R6 547 689 respectively. For the financial year-end, 2015, the overall total losses were estimated at R4.7 billion, of which 46% was residential in nature and 54% was business related: industry, commerce and agriculture (BICA). For 2016 financial year end losses were estimated at approximately R4.88 billion, and 2017 financial year, the volume of energy losses experienced an extreme increase of 20 Billion and also the cost of electricity was increased at a higher rate which resulted in extreme loss of revenue due to failure to purchase units by the customers. The electricity theft do not only affects the developing countries, but also affects the developed countries like the United States of America, Britain and France. The total annual revenue of the United States range from 0.5% to 3.5%, whereas Bangladesh, India, Iran and Pakistan which come under the category of developing countries, has the percentage of NTL's average which ranges from 10% to 15% [9] [8].

The bulk of the residential areas where losses are generally higher than the acceptable average are found in all the nine provinces of South Africa. The problem is worse off in urban areas like Gauteng province. This is because the province has big townships like Soweto, Sebokeng, Orange Farm, Randfontein, Evaton, Vosloorus, Mamelodi, Itireleng and Phumulong thus skyrocketing an average percentage loss of over 40 %. Figures 3 and 4 depict a typical example of illegal tampering and connections of varying magnitudes. The biggest challenge in Gauteng province is the lack of political will and support by the local councillors. These leaders always stand on customer's side even when they are wrong. This often results in mass action when

illegal electric cable removal operations are conducted in these areas. Mpumalanga and Free State Provinces are also on the top of the list when compared to other South African Provinces.

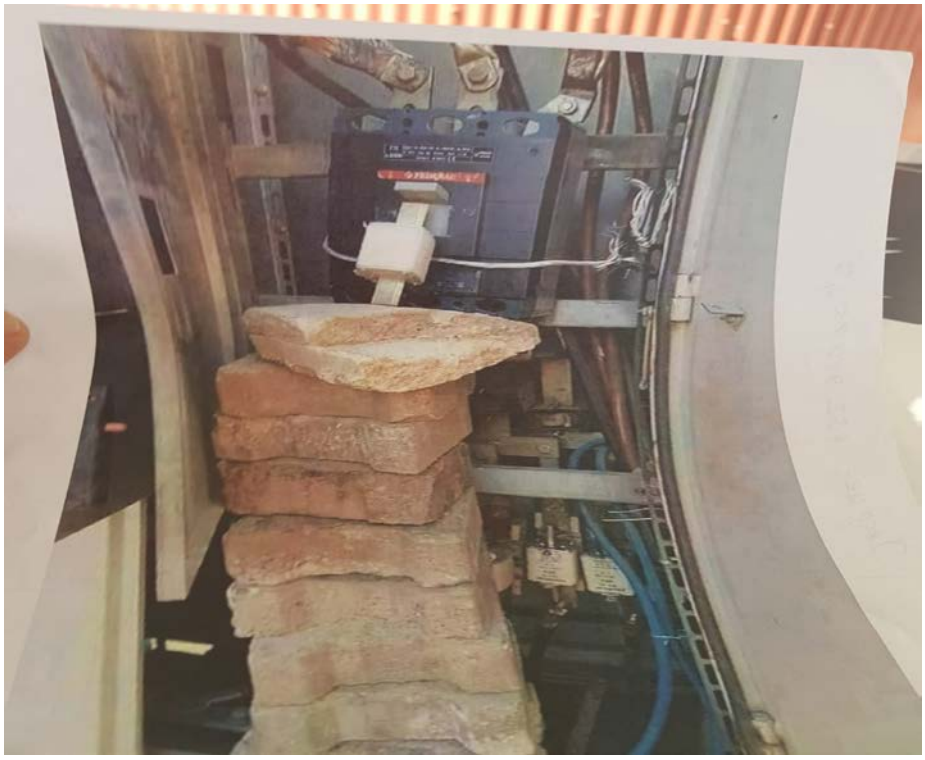


Figure 3: Gauteng Cullinan Plots, bricks are used to prevent tripping on a circuit breaker

Figure 4: Gauteng informal settlement: dangerous and illegal connection of electrical cable to a facility

1.3 Energy Loss Management Programme (ELP)

Eskom is one of the utility companies that tried to run a national energy losses management programme (ELP) with the primary objective of managing losses and the trends. The programme was addressing the energy losses problem holistically from technical, commercial and social perspectives. The strategic objectives of the ELP were to:

a) Arrest the current upwards energy loss trend
b) Manage the trend to an acceptable level
c) Ensure sustainability at an acceptable level [10].

In the past years, Eskom focussed on carrying out revenue protection audits, where customer-metering installations were inspected in order to detect theft or faults. Where faults were found, the meters were replaced and where tampering (theft) were detected, the customers involved were disconnected and only reconnected after tampering and reconnection fees were paid. The tampering fees were increased for customers who were found to have tampered with their meters more than once [10].

1.4 Major Challenges of Non-Technical Losses

- Tariffs that are non-cost reflective, customers are under billed while operating costs are more than revenue collections.
- The culture of defaulting leads to accumulation of very high bills, resulting in disconnection with high penalties. This aggravates electricity theft.
- House allocation backlog force the community to build tin houses in an unproclaim land which will automatically force them to tap from the high masts around them or any other electricity point.
- High rate of drug addict cripple the Utilities because the culprits cut parts of network like copper or steel, to sell them to feed their addictions.
- There is high unemployment rate, people are relying on grants, and lots of houses are run by the kids due to high HIV deaths of their parents.
- There’s a high number of houses that are unmetered or with stuck meters [11].

- Customers resist inspection of their meters.
- Low inspections, high customer base and extensive inducement to bribery and corruption [11].

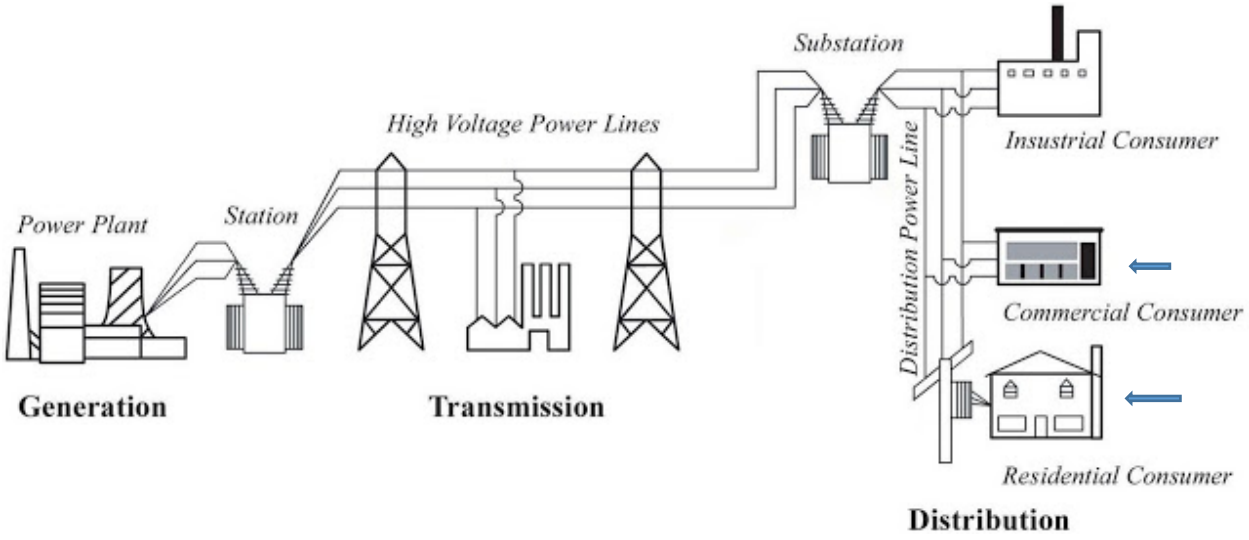


Figure: 5: Power System Network diagram [12]

1.5 Classification of Non-technical Losses amongst Countries

The level of non-technical losses varies according to the economic conditions of a country. In countries where GDP per capita is low, it is common to find higher levels of non-technical losses (pilferage). This is perhaps from the fact that the cost of electricity is relatively higher compared to the household incomes. In some countries, electricity supply has become non-regularized due to conflict of war or failure of government to maintain adequate controls on the supply of electricity and therefore pilferages have become endemic with high levels of tolerance within the community [13].

The countries of interest are ranked in the order of purchasing price parity (PPP per capita) as follows on the study that was conducted in 2007 by Indian Statistical Institute

Table 1: Relationship between Distribution Losses to Economic Prosperity of studied countries [13]

Country	Estimated losses	PPP per capita
India	NTL -20% to 40%	2,700
Philippines	NTL – 3.5% total losses 10%	3,300
Indonesia	NTL Unknown total losses 12%	3,400
Jordan	NTL – 3 to 5% total losses – 15%	4,700
Jamaica	NTL – 13.2% Total losses 23.2%	4,800
China	NTL – 10%	5,300
Thailand	NTL – 0.32% Total Losses – 5.69%	8,000
Brazil	0.5% to 25%	9,370
Turkey	NTL – 6% to 64%	9,400
Lebanon	Unknown	10,400
South Africa	NTL – 10%	10,600
Venezuela	NTL – 12.74%	12,800
Russia	Unknown but 10% +	14,600
UK, Australia, United States	NTL between 0.2% to 1%	>30,000

It can be seen from the case studies in table 1 that the non-technical loss mitigation practices in Philippines, Indonesia, Jamaica and Thailand are of particular interest; their non-technical losses are lower when compared to other Countries.

The fourth industrial revolution has introduced the automation system using wireless communication for electric system automation. When compared to conventional wired communication networks, wireless communication have potential benefits in order to remotely control and monitor substations and activities therein [14]. The vision of smart distribution grid is also due to growing recognition for electricity grid modernization to integrate, enable new electricity generation sources and consumption schemes [15].

Modern power grids need to be smarter in order to provide an affordable, reliable and sustainable supply of electricity. Smart distribution grid enables power utilities to carry out real time monitoring and controlling systems. Smart meters with effective communication medium and automated meter reading are necessary for effective energy management and energy accounting [16].

1.6 Research Problem

The South African municipalities are experiencing series of problems of energy losses of revenues due to technical and non-technical issues of electricity theft and pilferages. . Non-technical losses are contributing to more losses than technical losses. Hence, this study will focus on the challenges of non-technical losses and preferred mitigation measures. Utilities always waste finances in the constant repairs of equipment that are damaged due to theft of electricity, which also adversely affects low financial contribution towards other service deliveries. It becomes imperative to give attention to the analysis of these non-technical losses and to develop strategies to curbing and mitigating them.

1.7 Aim and Objectives of the study

The aim of the study is to analyze non-technical losses with their technical issues and implement wireless technique based on ZigBee to mitigate theft of electricity, taking into cognizance communication distance.

The objectives of this study are as follows:

- To reduce unplanned outages and ensuring more reliable services
- To reduce rate of vandalised infrastructure(s)
- To reduce network overload – less network trips, improve business and employ more people.
- To avoid load shedding – customer retention
- To protect human beings and animals from being electrocuted
- To increase revenue return for Eskom and municipalities

1.8 Research Questions

To what extent does electricity theft account for loss of revenue to public and private electric utilities (e.g. annual GWh lost expressed as a percentage of total GWh produced)?;

What are the costs associated with electricity theft and their overall economic impact? And

Will ZigBee wireless technique limit/combat electricity theft, to the domestic and commercial end users in South Africa?

1.9 Significance of the Study

The study will address the problem of illegal electricity connections ultimately. It will also look at technical challenges and possible solutions that will be of significant impact to the utilities companies as well as the end users in terms of revenue generation and collection. In solving these problems, utilities will be paid and thus revenue collection is improved upon. This eases the stress of annual high tariff structures, which the customers experience.

1.10 Limitations and Delimitations

The project is limited to domestic and commercial users. This involves single phase and three phase power users.

1.11 Project contribution

The project will geared towards the understanding of the technical glitches which the utility companies and municipalities encounter leaving them unable to collect generated revenue. It presents and install the wireless ZigBee system as a tool to mitigating and abating the research problems in this pilot study. The study evaluates the current technology of AMI and GSM, in order to solve the inherent problem of illegal connections or non-technical losses. By reducing non-technical losses, the revenue of utility companies and municipalities will improve and be more efficient and effective.

The study provides a better understanding of the technical and non-technical problems that cause poor revenue collection by Utilities. It presents the opportunities offered by installing wireless system that is ZigBee, to avoid running of cables that will be exposed to the human beings and end up being vulnerable as a point of tapping electricity illegally to consume electricity free of charge.

1.12 Thesis Outline

Chapter One: Introduction

The dissertation is made up of five chapters: Chapter one presents the background of the study, the research problem(s), aim and objectives of the research, research questions, and significance/justification of the study, limitations and delimitations of the study as well as contribution/impact of the study.

Chapter Two: Literature Review

This chapter looks at various literatures covering the entire study. The following topics were covered: technical analysis on losses, load profiling, AMR, GSM technologies and wireless ZigBee technology as the main problem mitigation strategy, and then the incursion on sensor networks and communication problems, which forms part of the study.

Chapter Three: Research Methodology/ Design

The standard form was formulated for survey purposes; ten (10) questions were tabulated with rating from 1 to 5 interpreted as strongly agree, agree, not sure, disagree and strongly disagree respectively. The results determine the questions: to and what extent electricity theft accounts for loss of revenue which will *ipso facto* affect end users and also will determine the viability of the mitigation tools. Data were collected on SAP (Systems, Applications and Products) for a small portion of town (Chiawelo) which were verified in tandem with information on customer side conducted by an audit. Costs associated with electricity theft and overall economic impact were determined using ZigBee technique, which was incorporated and installed into the existing system.

Chapter Four: Analysis and Discussion

Chapter four addresses the analysis of results obtained and interpretation thereof. Discussions of practical implication for implementing the results were articulated. There were comparisons with other available empirical studies.

Chapter Five: Conclusion

This chapter concludes the study with inferences and deductions from the results obtained, comparison with existing studies and publications and necessary evidence-based recommendations for implementation and future works.

Chapter Two

Literature Review

2.1 Introduction

This Chapter presents the study of several literature surveys conducted on electricity losses because of theft by the public, technical related issues and possible ways of mitigating against pilferage of electricity. The chapter also evaluated ways and strategies that could assist in ameliorating the challenges of non-technical losses as well what is already on the market in terms of mitigating tools, noting their advantages, disadvantages and improving on them in this study. The wireless system is the main technology that is proposed in this study although it also has some draw backs that need to be given more attention by the researchers, innovators and stakeholders.

The approach in this thesis is a comprehensive literature review on the following topics: load profiling and data mining, advance metering infrastructure, smart meter, GSM, ZigBee, communication and network security/cyber-attack. The purpose of studying load profiling and data mining is to present the best possible way(s) of arranging customer's data in order to meet minimum requirements of interfacing the proposed technique of mitigation electricity theft and pilferages with other possible tools.

Advanced metering infrastructure (AMI) can be interfaced with the new technology. Both technologies need to be well understood by any developer or researcher. For end users, it is also very important to study smart meters that already exists on site even with some attendant problems of communication part, which requires to be addressed as well. ZigBee technology is the main proposed technique but it cannot be complete without looking at its network communication and security components.

2.2 Load Profiling and data mining

An energy trend analysis of customer's load consumption pattern over a given period is load profiling, see figure 6 [4]. The monthly data analysis provides valuable information that will assist the Utility to understand the customer characteristics of low buy no buy power consumption, which helps to expose abnormal consumption behavior that is highly correlated with NTL activities [4].

2.2.1 Advantages of the load profiling technique

- It yields good results and is the cheaper approach compared to other existing techniques that can trend energy consumed.
- Assist Utility Companies in determining the next financial budget plan.
- It assist the power Utilities in reviewing marketing strategies, so as to improve efficiency.

2.2.2 Loading conditions

The need to evaluate and analyze loading conditions is crucial in ascertaining losses because different load conditions yield different load shapes from one customer to another. The loading conditions is as shown in Table 1.

Table 2: Loading conditions [4]

Loading conditions	**Items**
Type of customer	Domestic
	Commercial
	Industrial
Location	Urban
	Rural
Voltage level	Low Voltage
	Medium/High Voltage
Type of climate	Rainy/ windy
	Hot/Cold
Type of day	Week day
	Saturday (weekend)
	Sunday (weekend)
	Public holiday

2.2.3 Data selection

When choosing customers, it is very important to look at the following feature characteristics:

- Period of recorded invoices e.g. monthly.
- Geographical localization e.g. whether is Rural or Urban.
- Contractual tariff structure: Single phase domestic, three phase domestic, large power users and high tension users.
- Economic activity classification; if the area is well off in terms of business or there is high rate of unemployment which can cause high rate of NTLs.

2.2.4 Data Preprocessing

With respect to data cleaning, data cannot be rejected from a set where customers with less than six monthly register per year; and those with negative values on consumption attributes, can be eliminated. Normally, the consumption bills depend on the results of the consumption read which is not always the case in reality because if the company taking readings have no access to the premise where the meter are to be read, then estimation is possible based on historical consumption. Several and continuous differences between read data and billed data show abnormal behavior which keeps propping up [17].

2.2.5 Customer characterization and data mining analysis

Data mining consists of different steps with varying degree of complexities with different periods of time [4].

The representative load profiles gathered from the load-profiling module is a reference. In previous studies, most of the researchers rejected the untypical load profile due to insignificant behavior [18]. However, in the current study, the untypical load profile acts as a benchmark for investigation with outlier detection techniques.

The benchmarking has two types of load profiles, namely: abnormal behavior pattern and normal behavior pattern. Abnormal behavior pattern is a type of investigation that continues after detection. When gathered load profile compared with the new load profile, can be used as a reference to detect non-technical losses activities. The new load profile will be updated if no outlier found but if deviation detected, investigation will conducted using any outlier detection technique like statistical based, density based, distance based, model based and deviation based. If detected outlier is confirmed due to non-technical losses, then the new load

profile will be updated for an anomalous reference for forecasting purposes. Then this load profile represent a reference for forecasting non-technical losses activities for new load profile using forecasting techniques such as support vector machines (SVM) and time series , see figure 7 [4].

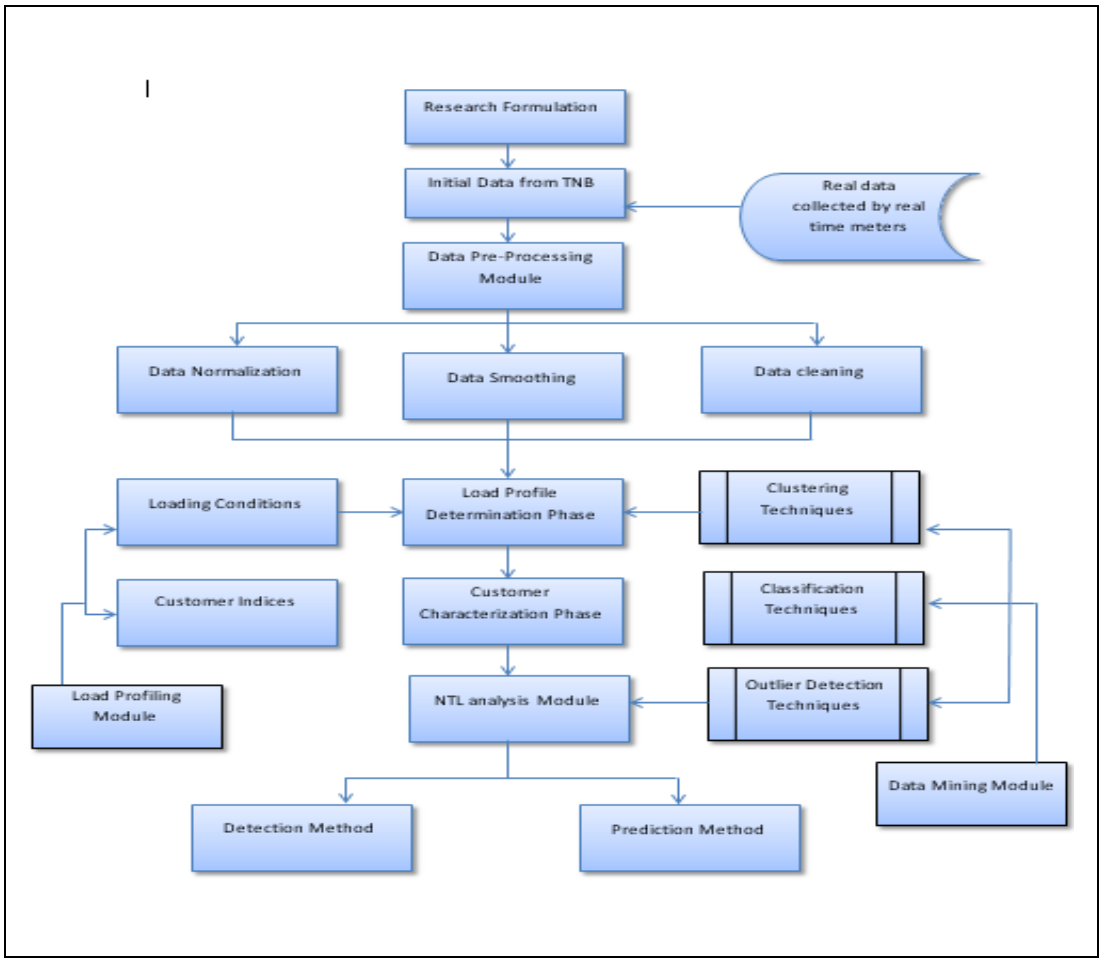


Figure 6: Load profiling based non-technical loss (CLPNTL) analysis framework [4]

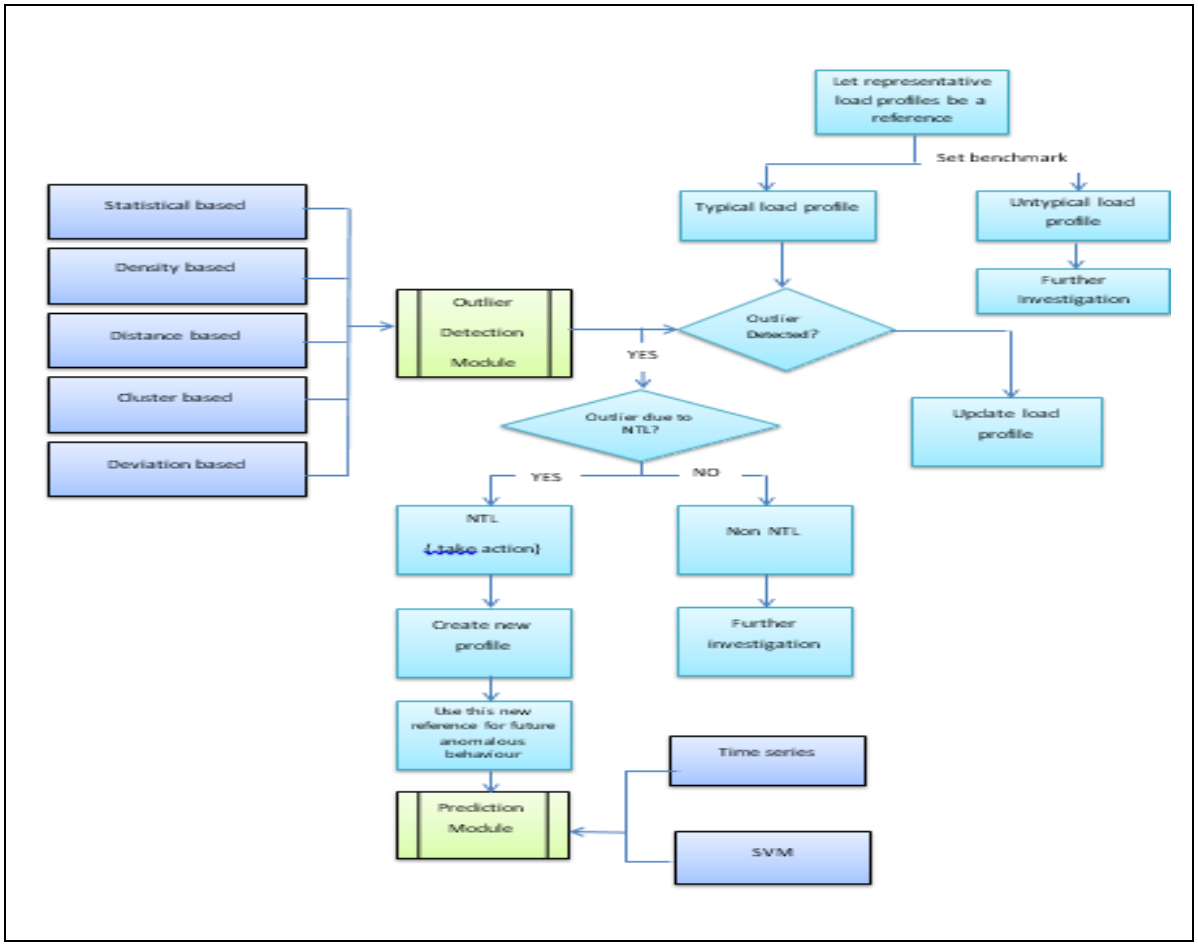


Figure 7: Data mining based non-technical loss detection framework (DMNTL) [4]

2.3. Advanced metering infrastructure (AMI)

Advanced metering infrastructure includes smart grid and contains a variety of operational and energy measures, smart appliances, smart meters, energy resources that are renewable. The smart grid is preferred because it is easily integrated with other new techniques that are capable of curbing the stealing of electricity. Smart grid system can also achieve the following factors [9] [15]:

a. Integration of distributed resources and deployment of distributed resources and generation along with renewable resources.

b. Usage of digital information will increase and control technology to increase security, reliability and electric grid's efficiencies.

c. Along with full cyber-security, the dynamic optimization of grid operations will take place.

d. Energy efficient resources, the resources of demand-side, and the demand response incorporated and developed.

e. Combination of the consumer devices and the smart appliances.

f. Providing the consumers with control options and timely information.

g. With the use of this smart technology, it can optimize consumer devices and other appliances physically. It records the communication concerns, its operations and automation of distribution.

h. The combination of advanced electrical storage and the techniques of peak-shaving technologies along with the plug-in electric and the hybrid electric vehicles deployed.

i. Progress in communication standards; operating process of the appliances and electric grid connected equipment along with servicing the infrastructures of the grid.

j. Gathering and lowering unnecessary barriers, will result in the adoption of smart grid technology, services and applications.

2.4. Importance of AMI

Advance metering infrastructure (AMI) is utilized by power Utilities because it can be redesigned and still perform the way it should be. The smart meter system is the integral part of AMI which cater for data collection and communication. Smart grid is feasible for monitoring of the delivered energy. It is a unique system that allow customers to monitor their own consumption via the computer program [9], [20].

AMI with Programmable logic controllers (PLC) when utilized simultaneously on the system can be viable for the two way communication between meter and central station remote

terminal unit (RTU), placed at nearby substation. It send an alarm signal to the central station in case of tempering of meters (sensors), long duration shut off meters. It has a kill button at central station for the meters; data logging capabilities and power line communication capabilities (sending, receiving, signature analysis) and lower cost [9], [5], [21].

2.5 Smart Meters

During outages, the smart meters detect and restore energy faster to the customers. Smart meters are capable of reducing the demand in energy supply which will automatically stop unnecessary projects of building new substations. The smart meter can also reduce greenhouse gas emission and other pollutions [9], 15].

2.6 GSM Technique for detecting power theft

GSM is a specialized modem, which operates with a SIM card, like a cellphone over a network, meaning it can be classified as a cellphone without a display screen. Utility services prefer it because it maximize the profit, one message can be used to collect the bill. Due to its automation properties, the duties are easily manipulated. It also eliminate problems of corruption for example closing of accounts unlawfully [22].

2.6.1. The function of GSM

Electrical power detection system detects unauthorized tapping of transmission lines. The system in real-time detects which line is being tapped. GSM is a wireless transmitter and receiver system, and can protect a distribution network from power theft by tapping on meters. [22],[23],[24].

2.6.2 Installation of GSM

GSM installation is carried out by using three poles during installation from P1 to P3. The middle pole (P2) carries master module and then P1 and P3 carry slave module. The microcontroller on P2 compares two currents of master and slave modules if the difference

between the two is greater than the predefined value, then the respective officer from the utility company receives the message of possible power theft or pilferage. It measures and communicates power consumed by consumer to the controlling sub-station. To avoid the short circuit on the system, it activates and implements temperature sensor system. [25] [22].

2.7 ZigBee Technology

The ZigBee technology is utilised because it can limit the problems associated with confined space in rural areas where it is challenging to install the wired system to convey the information. It uses a cell phone to send messages to officials. Other wireless techniques such as Bluetooth and infrared have limitation of range and efficiency. Utility companies pay a license fee to get access of GSM/GPRS, and the cost of hardware is very high. It uses unlicensed 2.4 GHz ISM band that is available worldwide. ZigBee has range between 10m to 2km and it works well with networks such as Wi-Fi, Ethernet and GPS. It also provides scalable networking solution that makes it suitable to controlling and monitoring applications [26], [27].

2.7.1. Types of Techniques

Two types of techniques are used to deliver information to an authorized agency to control theft of electricity via bypassing the energy meter; [14] [26] [28] [29];

2.7.1.1 Wired techniques

- Electrical cables;
- Coaxial cable; and
- Optical fiber.

2.7.1.2 Wireless technique

- ZigBee technology;
- GSM technique;

- WI-FI;
- Infrared;
- Wi-max; and
- Bluetooth.

2.7.2 What is wireless sensor network?

Wireless sensor network (WSN) is a group of sensors arrayed for monitoring and recording the physical conditions of the environment and organizing collected data at a central location. WSNs measure environmental conditions like temperature, sound, pollution levels, humidity, wind speed and direction, pressure, etc. [26] [29].

2.7.3 Operations of ZigBee?

ZigBee operates in the industrial, science and medical (ISM) radio bands, namely: 868 MHz in Europe, 915 MHz in the USA and Australia, and 2.4GHz worldwide [26].

2.7.4 ZigBee devices

The ZigBee consists of the three following devices [26]:

2.7.4.1 ZigBee Coordinator device

- ZigBee device kick-starts the signal. It coordinates the signal at the transmitting time, transmits signals easily;
- It is one and only coordinator per ZigBee network;
- This device has the unique responsibility network tree and can bridge other networks;
- There is exactly one ZigBee coordinator in each network; and
- It is able to store information about the network, including acting as the repository for security keys.

2.7.4.2 ZigBee Router device

- It provides the path to the signal at the signal transmitting time;
- A ZigBee is a logical device type that can route messages from one node to another; and
- Routers can act as an intermediate router, passing data from other devices.

2.7.4.3 ZigBee end device

- This ZigBee term indicates the device in question has no routing capability;
- It can only send and receive information for its own use;
- An end device functions as a leaf node in a cluster tree network;
- The nodes in a star network are all end devices except for the coordinator;
- It has long battery life;
- A complete mesh network would not contain any end devices, but in practice, a design may call for one or more of them;
- It is present at the end;
- It contains just enough functionality to talk to its parent node (either the coordinator or a router); it cannot relay data from other devices; and
- It requires the least amount of memory, and therefore can be less expensive to manufacture than a ZR or ZC.

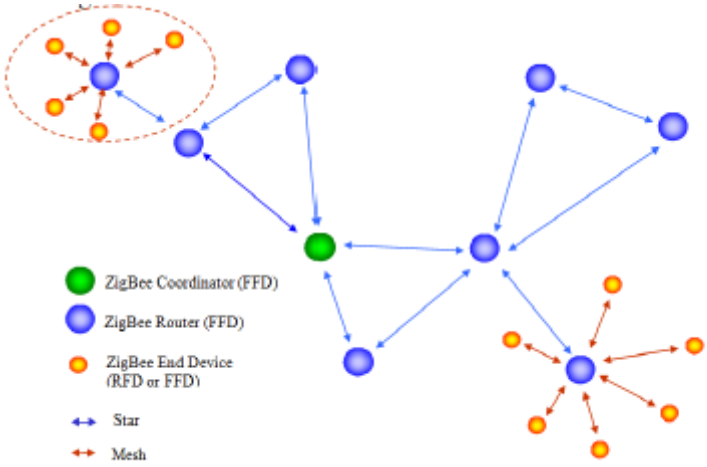


Figure 8: An Illustration/schematics of ZigBee

2.7.5 How ZigBee functions

The function of ZigBee is illustrated on figure 8, whereby it shows how three components of ZigBee that is Coordinator (FFD), Router and End Device work together for it to be feasible. The flow chart in figure 9 shows how the system works to prevent electricity theft or checkmate pilferages. Firstly, the microcontroller checks for the resistance and if there is change in the value of the resistance, the supply will cut off and the LCD will show that the meter has been tampered with. To operate the microcontroller via the relay, there is a need for amplifier circuit because no direct access of the relay to the microcontroller is possible. When the microcontroller switches off the load, the ZigBee modem (figure 8) sends the results to the authorized official. The system will not allow the consumer to reset, meaning it will only allow the person from authorized agency to do resetting. The microcontroller will convey the information to the relay and switch from ON to OFF and the power supply to the meter will switch off by the system itself. Then the LDC will display the message “meter tempered” and this message will reach the utility’s official (s). Figure 9 is a presentation of the summary or overview of the function sequence [26]. The research on other techniques was done and compared to ZigBee, see table 3 below.

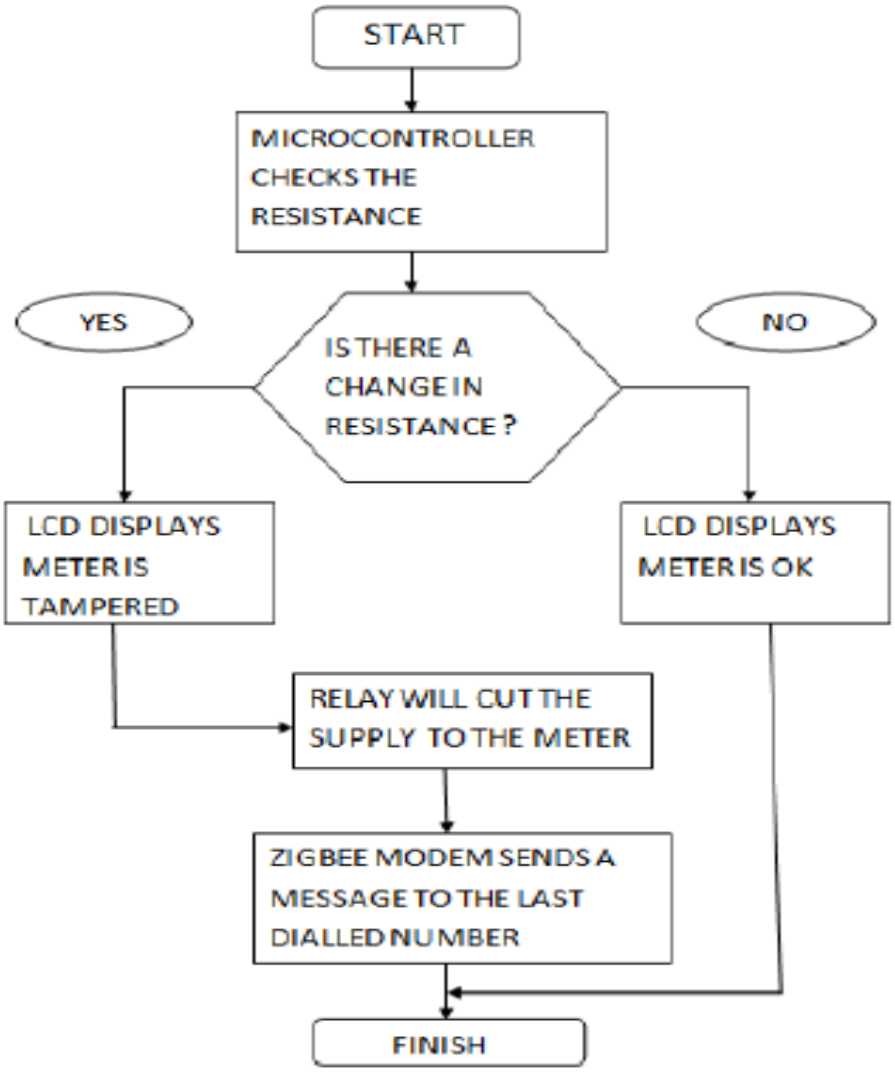


Figure 9: Process flow of ZigBee

Table 3: Comparison between ZigBee and other wireless technology [26] [30] [29]

DESCRIPTION	ZIGBEE	WIFI
Network type	WPAN (Wireless Personal Area Network)	WLAN (Wireless Local Area Network)
Network size	Up to 65536	32
Network Architecture	Star, Tree, Mesh	Star
Range (meters)	1 – 100+	1 – 100
Frequency Band	2.4 GHz and 868/915MHz	2.4 GHz and 5 GHz
Battery Life	Years	Hours
Application focus	Monitoring and Control	Web, Email, Video
Data rates (K bits/s)	250	11,000+

2.8 Power system communication

Electric system automation objective is to maintain uninterrupted power service to the end users. Power utilities find it difficult to supply reliable power without fail in both rural and urban areas because of unforeseen and natural catastrophes. The operational and commercial demands of electric utilities require faster and reliable network communication that can integrate or synchronise with existing equipment and planned operational equipment. The communication technologies consist of four classes as follows; power line, satellite, wireless and optical fiber communication [4].

This brings significant advantages for electric utilities, such as low up-front cost, easy network maintenance, robustness and reliable service coverage. For example , low power and low range wireless sensor can be utilised for urban areas, WiMAX technology which enables a fully connected communication network for electric system automation application, such as real-time grid and equipment monitoring and wireless automatic meter reading systems. Conventional desktop computers put severe constraints, since sensor nodes have limited processing ability, storage and energy, also wireless links have limited bandwidth, and security is important and even critical for many applications of sensor networks [14]. Another challenge is budget because they are expensive to operate in urban areas. The changing technology can be a challenge since a customer cannot buy network connections but lease it or obtain a license to operate on it for a certain period. Communication networks in rural and urban areas are crucial to electricity automation.

Communication capabilities have developed from narrow- band, low speed communication to high-speed broadband “highways” for all sorts of communication. Communication system typical for smart grids is shown in Figure 10 [31];

2.8.1. Real-time operational communication requirements

To maintain operation of electric power distribution systems, it is divided into real-time operational data communication and real-time operational speech communication. Real time operational data communication is also divided into tele-protection and power system control. The communication is characterized by the fact that interaction must take place in real time with hard time requirements. Real-time operational voice communication encompasses traditional telephony power system island operation. The actual possibility of having voice communication is, by the control center staff, considered as the most powerful tool for both normal and abnormal operation cases, which also includes facsimile for switching sequence orders.

Tele-protection – messages should be transmitted within a very short time frame, within the range of 12 to 20 ms, depending on the type of protection scheme. The requirement owes its origin to the fact that fault current disconnection shall function within approximately 100 ms.

Power system control – Mainly includes supervisory control of the power process on secondary or higher levels. These systems are of the kind SCADA/EMS. Measured values must not be older than 15 seconds (s), when arriving at the control center. Breaker information shall arrive no later than two (2) seconds after the event has occurred.

2.8.2 Administrative operational communication requirements

In addition to real-time operational communication information needed in more detail to support minor and major power system disturbances. The example is interactions with event recorders, disturbance recorders, and power swing recorders. The communication is characterized by the fact that it does not need to take place in real time. Time requirements are

usually moderate. Other examples are asset management, fault location, metering and transfer of settlement information, security system and substation camera supervision.

2.8.3 Administrative communication requirements

They includes voice communication and facsimile within the company (between the offices that are at different geographical locations), as well as to/from the company, where the communication has an administrative purpose.

2.9 Cybersecurity

Protection of computer systems from the theft and damage to their hardware, software or information, as well as from disruption or misdirection of services provided is called cybersecurity. A secure information system is very important in electric power industry systems. A more office-oriented information system can discontinue its service during a cyberattack. Secured South African information system is characterized by the following definitions [32] [33] [34]:

2.91 Cyber security consideration for the smart grid

However, it brings not only great performance benefit to the power industry, but also tremendous risks as well as arduous challenges in protecting the smart grid system from cyber security threats. Considering the vast scale of a smart grid, it is reasonable to expect that the cumulative vulnerability of the smart grid communication system might also be vast. The consequences of a smart grid cyber-security breach is enormous. New functions such as demand response introduce significant new cyber-attack vectors such as a malware that initiates massive coordinated and instantaneous drop in demand, potentially causing substantial damage to distribution, transmission and even generation facilities [35] [33].

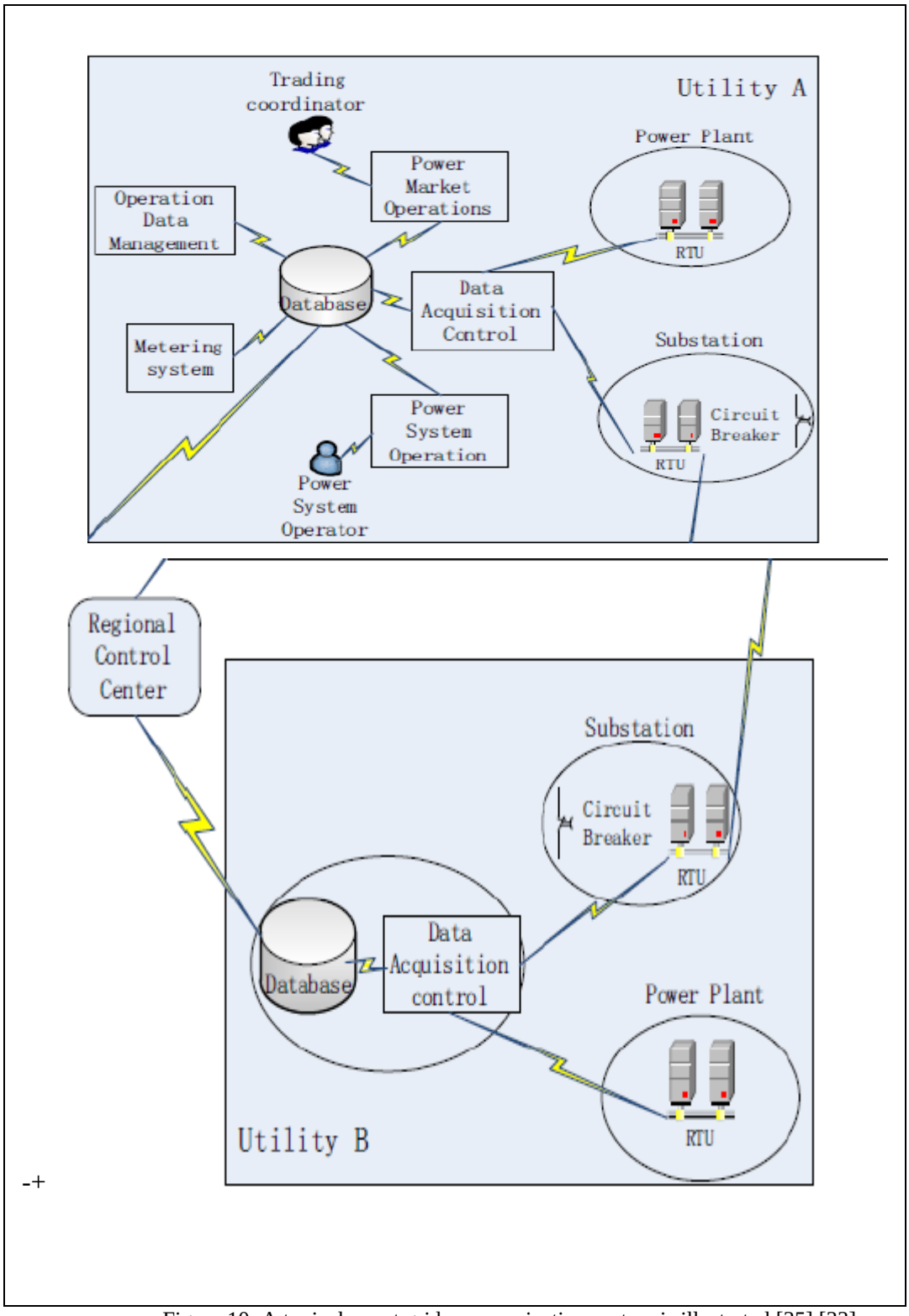


Figure 10: A typical smart grid communication system is illustrated [35] [33]

2.9.2 Cyber security issues

A. De-coupling between operational SCADA/EMS and admin IT, to secure operation: When existing SCADA/EMS systems are recently being refurbished or replaced, the information and IT security issues must be taken into account. If SCADA/EMS system is to be refurbished, the operational SCADA/EMS system part must be shielded from the administrative part, such that the operational part is protected from digital threats that are possible over the internet connection. If a SCADA/EMS system is to be replaced, it is then a good occasion to reconsider an overall system structure, and then incorporate IT security on all SCADA/EMS levels. A more secure state is to de-couple the operational SCADA/EMS system and the administrative IT system. Another alternative way is to secure the firewall configuration in between operational and administrative parts [31].

B. Threat and possibilities: The fact that SCADA system are recently being interconnected and integrated with external system creates new possibilities and threats [31].

C. SCADA system and SCADA security: The fact that SCADA system are recently to an extent based on off-the-shelf product, and increasingly being connected over internet for different purposes: remote access, remote maintenance; implies that SCADA systems are being exposed to the same kind of vulnerabilities as ordinary office PC solution based on Microsoft products. The use of SCADA system is cross-sectional and it has an impact on different parts of a society [31].

D. Governmental coordination in Sweden on SCADA security: Like in many other countries, the issue of securing CIIP system have been emphasized in Sweden. A governmental coordination action between different authorities and agencies started to focus on SCADA security. As a natural step, the SCADA security guidelines has been developed. Technical guidelines and administrative recommendations are developed which are available for free downloading, that supports the securing actions of the SCADA systems in the different areas of operation: power, water and transportation [31] [36].

E. Information security domains - CIGRE development: Since the SCADA/EMS systems became increasingly integrated; it also became more difficult to treat the system structure in terms of “parts” or “subsystem.” The physical realization of various functions is less evident from a user perspective. Instead, it becomes more natural to study a SCADA/EMS system in terms of” domains.” This concept in application was introduced to power systems as well. A domain is a specific area, wherein specific activities/business operations are going on and they can be grouped together. The following security domains are introduced:

- Public, supplier, maintainer domain;
- Power plant domain;
- Substation domain;
- Telecommunication domain;
- Real-time operation domain; and
- Corporate IT domain.

The purpose of the domain concept is to emphasize for everyone involved within a specific area the importance and handling of information security issues. When communicating across power utilities, organizations, and other companies, using communication networks, the security domains should be recognized, for example a power utility could define a security domain and related policies and procedures for its tele control activity to assure compliance with legislative or regulatory requirements [38] [31] [38].

2.9.3 Security objectives

Availability: It is essential to have availability of control in order to maintain the normal function of the power grid. For example this allows operators to restore power in case of outages (either by accident or by terrorist intent) [39] [32] [33].

Integrity: Availability on its own is not sufficient, as a hacker might take control of a substation and let the station pass wrong switchgear state data to the operator to mislead him to do the remote control. By using this method, the hacker can still perform the actions that were not granted to him directly by the SCADA system [39] [32] [33].

Confidentiality: confidentiality means in this context that nobody has access to data that he is not entitled to [39] [32] [33]. The table 4 below gives summary of availability, integrity, and confidentiality for different communication systems.

Table 4: Availability, integrity, and confidentiality for different communication systems [32]

Systems	**Availability**	**Integrity**	**Confidentiality**
Leased lines	High	Low	Low
Dialup lines	Normally high, but low in busy periods like New Year's Eve or during a disaster	Average	Low, see leased lines
Power Line Carrier (PLC)	High	Very good	Very good
Radio link	Low	Low	Mostly poor
Radio Network Communication systems	Low	Low	Low
Privately operated IP network	High	High	High
Public operated IP network, such as ADSL, SDSL, GPRS, UMTS	High	Low	Low
Linux or Windows based Substation Controller	High	Low	Low
Real time Operating System based Substation Controller	High	Low	Low
Bay Controllers and Intelligent Electrical Devices (IEDs)	High	High	Low, normally not addressing security
Station Bus in a Substation control System	High	Low protected by building	Low protected by building

2.9.4 Network *Challenges*

(i) Internetworking

The interconnected smart grid communication systems have several vulnerabilities that vary across networks due to lack of built-in security in many applications and devices. This should

not be the model for a network as important as the smart grid. Layers of the cyber security defense of smart grid should be built into solutions to minimize the threats from interruption, interception, modification, and fabrication. Keeping the network private, i.e. where all transport facilities are wholly owned by a utility, would greatly minimize the threats from intruders, as there would be no potential access from intruders over the internet [40] [33].

(ii) Security policy and operations

The reliability of a smart meter grid depends on appropriate operations of many components and the proper connectivity between them [41] [33]. To disrupt a smart grid system, an attacker might attempt to gain electronic access to a component and configure it to impersonate as another component and or report a false condition or alarm. One of the simplest types of attacks that an adversary might attempt is the DoS attack, where the adversary prevents authorized devices from communicating by consuming excessive resources on one device. Care must be taken by organizations to ensure that security policies and practices are not in conflict with those of other organizations with which they will need interoperability [33].

(iii) Security services

Managing and maintaining a secure smart grid will be as equally vital as developing, deploying and integrating a secure smart grid solution. Security services will help network operators to identify, control and manage security risks in smart grid communications. Every aspect of a smart grid must be secure. Cyber security technologies are not enough to achieve secure operations without policies, ongoing risks assessment, and training [33], [42].

A smart grid requires access to cost-effective, high-performance security services, including expertise in mobility, tailored per utility to best fit their needs and help them achieve their organizational objectives. Figure 11 illustrates a typical set of security services in smart grid communications [33]. It describes a framework that operationalizes cyber security across people, process, policy and technology foundations of each organization [33].

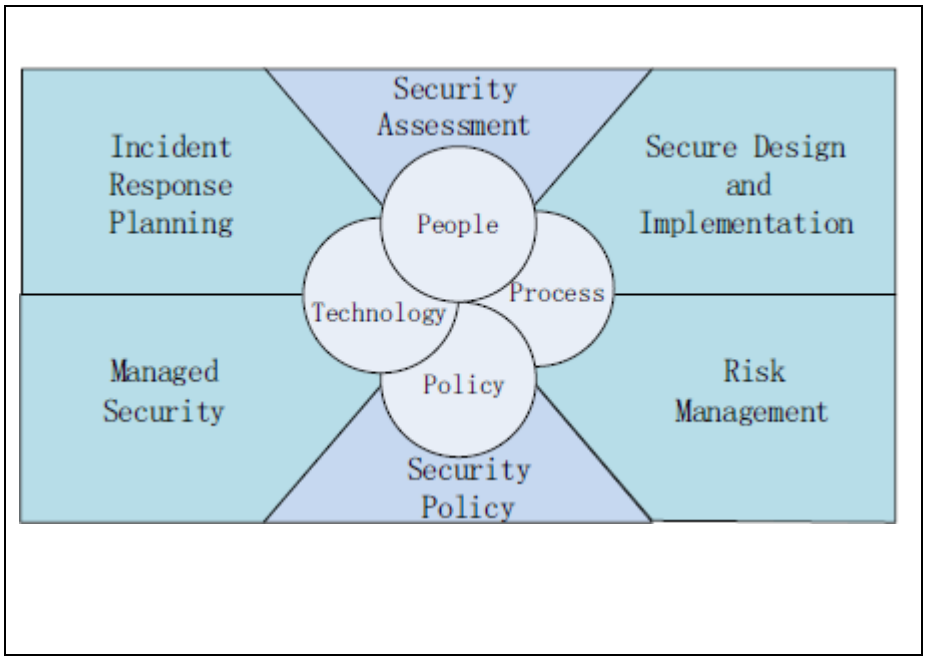


Figure 11: Illustrates a typical set of security services in smart grid communications [33]

(iv) Efficiency and scalability

Ensuring system availability is a high priority in critical systems like the smart grid, which requires that several key issues be addressed. First, the system must be efficient in its use of computation and communication resources so that resources do not become overwhelmed and all requests can be handled. Second, the system must have good error management built in to ensure proper handling of failures (e.g. those resulting from bad messages). Furthermore, the error management function must be fail-safe in nature so they do not lead to resource exhaustion even in the face of adversarial action. Third, the system must have adequate redundancy built into it so that, if sub-systems fail or are compromised, then the entire system do not collapse. The fourth, the system should support auxiliary security functions that may be deployed in the smart grid communication system to detect and respond to cyber-attacks [41] [33]

2.9.5 Differences between enterprise network and smart grid

There are three major differences between enterprise network and smart grid network security, namely:

2.9.5.1 Different security objectives

In enterprise network, the main objective is to protect data, ensure system reliability and protection of equipment and power lines [33].

2.9.5.2 Different security architecture

In enterprise networks, the data server resides at the center of the network and requires more protection than the edge nodes, which are used as an access points by end users. In smart grid networks, EMS sits at the center (in the control center) whereas RTU/PLCs sits at the edge. Usually, only devices such as re-closer, circuit breaker, which are controlled directly by RTU/PLCs, can do harm to human life, operation, or damage equipment and power lines. EMS/SCADA and data log servers cannot do any damage directly. Therefore, in smart grid communication systems, edge nodes need a subset of the controls used for central devices [33].

2.9.5.3 Different technology base

In enterprise network, windows, UNIX and Linux are widely used as operating systems, whereas Ethernet is used to connect all devices with IP-based protocols. Therefore, common security solutions are designed based on these common architectures. Thus, it is difficult to develop common host-based or network-based security solutions for smart grid applications [33]

2.9.6 Current solutions

- Firewalls and IDS

Since the most important threat to the SCADA network may come from malicious attackers via the internet, it is necessary to monitor the traffic flows from the Internet (IP network) to the SCADA network. It is proposed that firewalls and other intrusion detection system (IDS) be installed at the various ingress points (gateways) of the SCADA network to identify malicious traffic before it is allowed entrance. Although this will help to filter out some attacks, it may still be an inadequate defense action against attacks. Viruses and worms could swamp the

systems with huge volumes of attack traffic. Hence, having only firewalls attack and IDS at entry points may not suffice. This leads to the concept of the electronic perimeter [33].

- Electronic perimeter

It is proposed that a wider electronic perimeter be defined where cyber-attacks can be filtered and unwanted traffic stopped before it reaches the gateway of the SCADA network. This extends perimeter, as it would be possible to stop the attacks further away from the SCADA network. In addition, the IDS devices along the electronic perimeter could form an overlay network (i.e. a vital private network over the internet) and functions in a distribution and collaborative fashion, supporting one another in tackling the attacks more effectively. The setup can be viewed as an electronic fence or protective perimeter- barrier that allows only legitimate traffic to reach the gateway of the SCADA network.

- Domain-specific IDS

IDS devices, along the electronic perimeter, can establish a baseline profile of the normal system behavior. In addition, a perspective on an intrusion can be developed by analyzing the emerging characteristics of the data such as patterns, clusters and tradeoffs by looking for trends and cycles in the data flow. This would require domain-specific knowledge of the SCADA network and associated communication devices in order to construct the IDS attack signature database. Identifying these attack scenarios and generating signatures that correspond to these situations is a significant challenge in itself and would need extensive and detailed analysis of the various attacks in the context of interconnected grids. However, once this is achieved, the observed behavior needs to be correlated to detect potential intrusions and filter the attack traffic. The solution of domain-specific IDS overlay network, along an extended secure cyber-perimeter, which functions in a collaborative e manner, has the potential to tackle known cyber-attacks to date in a fairly effective manner. It would follow the principle, “Stop the attack even before it reaches you”

- Secure communication

The various communication links must be secured by adopting well-known security standards such as virtual private network (VPN) and IP security (IPSec) to provide authentication, data integrity and confidentiality for the data communication between the internet or corporate network and the SCADA network. In addition, DNS security must be deployed in all DNS

servers associated with the electric grid for validating the authentication and the integrity of DNS transactions.

- Best security practices

Security practices such as computer operation and network management policies must be defined according to the NERC guidelines. This is for procedures such as the choice of passwords and their expiry, use of a limited number of privileged computer accounts and disabling the rest, closure of unwanted communication ports and computers, enforcement of access control mechanisms, and frequent update of anti-virus signature database. It is useful to evaluate the extent to which the corporate and SCADA networks can be logically and physically separated without affecting any functionality, in order to prevent a vulnerability in one network from making the other network also vulnerable.

- Online vulnerability map tool

It is also useful to develop a vulnerability analysis tool, to test whether the servers, hosts, routers, and devices that are part of the SCADA network are vulnerable to known attacks. This tool performs host/network vulnerability analysis periodically (through port scanning and other mechanisms) and provides a visual map of the vulnerability that alerts the operators/engineers to take appropriate remedial actions. The tool has to be flexible so that new attacks can be added to the repertoire at any time. The tool acts as a security management technique, and complements the IDS techniques.

2.9.7 Deployments

Smart grid deployment must meet stringent security requirements. Strong authentication will be required for all users and devices, which may affect the operation of the grid. With the large number of users and devices affected, scalable key and trust management systems, customized to the specific needs of the energy service provider, will be essential. From years of deploying and operating large secure network communication system, it is now known that the effort required to provide symmetric keys into thousands of devices can be too expensive or insecure. The development of key and trust management system for large network is required; these systems can be leveraged from other industries, such as land mobile radio systems and association of public-safety communications officials (APCO) radio systems. Several (APCO) deployment systems provide state-wide wireless coverage, with tens of thousands of secure

devices. Trust management systems, based on public key infrastructure (PKI) technology, could be customized specifically for smart grid operators, easing the burden of providing security, which adheres to standards, and guidelines that are known to be secure [31].

Chapter Three

Research Methodology

3.1 Introduction

This chapter presents the methodology used in this research that addresses the concept of electricity theft as a technical problem to electricity providers such as Eskom and municipalities. The methodology presents research design, data collection method, research instruments before introducing the pilot study. In addition, issues around the sampling frame, the sample size and the data analysis approach are also discussed.

The methodology allows to appreciate at what extent electricity theft accounts for loss of revenue to electric utilities i.e. annual GWh lost expressed as a percentage of total GWh produced. The cost implication associated with electricity theft and their overall economic impacts are also evaluated, the impact of ZigBee wireless technique and capability to curbing electricity theft is explored. The outcome can give guidance on the effective technique or method that can be followed to mitigate stealing of electricity.

The starting point was load profiling and data mining technique where data were acquired from utility's SAP system which was thereafter analyzed and compared with site information in order to determine customer's behavior and responses.. This will assist in aligning the proposed wireless ZigBee system to the existing smart meter system. Another advantage of load profiling and data mining is that in some regions, Eskom and municipalities use shared network therefore it will assist in specifying the demarcation of the each marked area respectively. The proposed wireless ZigBee technique has an advantage of limiting all the problems associated with confined space when it comes to installation. It has low costs and long battery life. It also has disadvantage of failing at a long distance and vulnerable to cyber-attacks. This study also covers such problems to establish whether this can be improved.

The available data collected were analyzed, and then the survey was conducted amongst utilities' customers, local community, councilors and utility staff. Data were tabulated,

graphical representation was done for better interpretation, analyzed and outputs discussed in Chapter 4.

The outcome of the survey is showing positive results to the direction of the proposed technique in mitigating electricity theft thus resulting in increase in revenue generation and collection, thereby improving South African economy.

3.1.1 Research design

The purpose of this approach is to allow for collection and processing of data for research coherency. When data is gathered correctly, preserved and processed properly, naturally it leads to sound analysis and interpretation thereof, namely:

(A) ZigBee technique will be installed to the existing infrastructure in order to curb theft of electricity;

(B) Load profiling, AMI, smart meter will be discussed as they play important role in interfacing of ZigBee technique to the existing infrastructure;

(C) Pilot study will be discussed to assist in understanding the interfacing of ZigBee technique into the existing infrastructure;

(D) A survey questionnaire will be administered to respondents, which will assist in evaluating whether the project will be feasible or not and to identify out losses and cost associated;

(E) Communication failures will also be investigated.

(F) Apart from testing the research instruments and planning for data collection, the study seeks to limit personal interferences before, during and after collection of data. This researcher's commitment is to remain as objective as possible throughout this research; and

(G) The minimum time required for such as a study is two years full-time.

3.1.2 Research method

As indicated above, this is a quantitative study, and as such, it will make use of a survey questionnaire for data. Collection. Quantitative methods have a reputation of dealing with numbers, making interferences and adopting a more objective stance in garnering, processing, interpreting and even using data outputs where necessary.

Quantitative research also tests hypothesis, the null and the alternate hypothesis are used to test for significant differences. In the case of this study, the following hypothesis emanated from the literature surveyed:

(i) Power theft detector using wireless technology is effective in curbing cable theft and pilferages;
(ii) Power theft detector using wireless technology is not effective in curbing cable theft;
(iii) It is possible to mitigate electricity theft in domestic and commercial businesses;
(iv) It is not possible to mitigate electricity test in domestic and commercial businesses.
(v) It is possible to collect revenue thereby improving S.A. economy.
(vi) It is not possible to collect revenue thereby improving S.A. economy.

Qualitative research on the other hand is more about giving the voice to both the researcher and the ordinary population in what appears to be a subjective interpretation. Several qualitative methods are known to date. These include interviews (structured and non-structured, focus group, online and telephonic (Johnson and Christensen 2008). On the other hand, quantitative research in natural sciences and social science is defined as the systematic empirical investigation of observable phenomena using statistical, mathematical, or computational techniques. Any data that is numerical in nature form such as statistics, percentage, etc. Suffice to indicate that this study is quantitatively approached and therefore the qualitative paradigm is outside the scope of this study.

3.2 Research instruments

3.2.1 Survey

For this study, a questionnaire survey was developed and used to collect data. It used Likert scale type of questions. The significance of Likert scale is that the method makes it easier to analyze data and provide precise and concise information, which one can compute and study objectively.

3.2.1 1 Sampling frame and size

A survey consisting of 50 sheets of A4 paper with 10 questionnaires on each that was conducted to ensure that all targeted respondents are given an equal chance of taking part on a full set of observation objects. Part of the daily duty of the researcher was incorporated in assisting customers with electricity problems; part of the survey was conducted during same period and duty situation. The way and manner of selecting participants/respondents was by random sampling as there was no specific pattern followed. Conferences were also targeted because a mixed feedback of professionals and non-professionals will make the study pool more reflective and interesting. This will also assist in disseminating the study not only to Gauteng but also to the other provinces of South Africa.

3.2.1.2 Data analysis

Questions were counted per number ranging from 1 to 5; whereby in each number, strongly agree, agree, not sure, disagree and strongly disagree were counted and calculated, translated in percentages, put into tables and represented graphically per rating using combo chart. The combo chart assisted in comparing the five ratings of the survey. The data were turned into viable information that assisted in discussing the questionnaire results and drawing inferences.

3.2.2 Pilot study

A pilot study or pilot experiment is a small-scale preliminary study conducted in order to evaluate the feasibility, time, cost, adverse events, and improvements if necessary upon the study design prior to performance of a full-scale research project. This pilot study was conducted with the aim to identify areas that need improvement, clarity or novelty. The pilot study was conducted and it involved 10% of the targeted population of this study. Participants who took part in the pilot study did not participate again in the main study survey. The pilot study highlighted the flaws that needed amendment(s).

3.2.2.1 Smart meter case study

The smart meter project took place in 2016 from March to December. The project was initiated by the loss of revenue that took place within the period. The researcher was tasked to manage the project, which had 13000 smart meters around the city of Tshwane, installed for

commercial and middle class domestic users. There was a team of 5 electricians at work, 5 inspectors with their assistances, 5 administrators and 2 senior revenue protection officers. The approach was to start with load profiling and data mining and then followed by the technique of smart metering which already existed. This case study demonstrated the importance of load profiling and data mining before any technique can be utilized. The steps taken are expatiated in the following subsection:

3.2.2.2 Meter Audits

Low consumption report is normally drawn from the billing or vending system to identify customers that are subscribing to low units or not subscribing at all. The report normally guides the utility with customers that have tampered with their meters or have faulty meters to customers that have not been billed for a while. The latter customers are to be visited to audit the meters to verify their conditions whether functional or not. If the meter is faulty, the utility will be required to replace the meter immediately. If the meter is tampered with, the customer will have to be disconnected immediately by removing the concentric cable or switch-off the circuit breaker at the pole top box or in the pillar-box. The customer would be penalized by the utility by issuing a fine. The customer will have to pay the fine and be issued with proof of payment before he/she can be reconnected.

A blanket audit may also be conducted on all customers in a specific area to ensure that all the meters are in good conditions and they are all sealed. Blanket audit is quite an expensive exercise, but once it is carried out, the utility should expect electricity sales improvement.

3.2.2.3 Data Cleanup

A blanket meter audit assists with data cleanup as the existing data is collected from the field. Most of the utilities are struggling with complexity of cumbersomeness of data as faulty meters are replaced from the field with new meters. The new meters are not registered on the billing system and when a meter is not registered on the billing system, it becomes difficult to track the purchase history of that specific meter or the billing history thereof. Customers ends up not being billed as the new meter installed fails to be registered and thus linked to the customer. A field customer data needs to be collected so that it can be compared with the current data that

are stored on the billing system. Data cleanup exercise should be implemented to identify and remove old meters that are still registered and linked to the customers on the billing system. New installed meters identified, should be linked to the existing point of deliveries (PODs). Customers that were not billed due to a new meter being installed can be billed based on the current meter readings. Customers with calibration problem meters will requires a new meter to be installed in parallel with the faulty one and allowed to run for a period of three months to be able to do the meter reading comparison. If there are variances of more than 2.5 percent on the readings, a faulty meter can therefore be replaced immediately. The customer can be advised that they are under-billed at the time. The utility can implement a process of back charges to recover the lost revenue from the customer.

3.2.2.4 Power Line Carrier (PLC) Implementation technology to curb Non-technical losses

There are a number of revenue protection mechanisms available today. Each with its own pros and cons. A number of municipalities have already embarked on debt recovery drives, aggressive service suspension programs to AMR systems with very mixed results. In some cases, the investment turns out to be too high for the benefit, and in others, buy-in from the public becomes an obstacle where consumers reject measures adopted by the utility. The PLC system operates efficiently as the meters can be read and monitored remotely. The technology is based on low voltage network, which supplies residential and commercial customers. All meters are installed inside the kiosks within the transformer zone. The installed meters are split meters with the following components: customer interface unit (CIU) and energy measurement unit (EMU). The EMU is housed inside the kiosk or on the pole top box. The CIU is issued to the residential or commercial customers. Communication between the EMU and the CIU is through the mains cable using power line carrier (PLC) technology. The CIU is used for loading of tokens for prepaid customers, monitoring remaining credits and electricity consumptions. Postpaid customers use the CIU to read their meter readings and manage their electricity monthly consumption.

When electricity token is loaded through the CIU by punching the 20 digits on the receipt to the CIU, the token is pushed to the EMU through PLC technology. The EMU will receive and encrypt the token into the credits in kilowatt-hours. The EMU will be credited with electricity

units and the internal latch will switch into on-status. The customer will be able to receive electricity for usage until the credit is exhausted and can be recharged.

3.2.2.5 Data Concentrator Unit (DCU) and Check meter

The data concentrator unit (DCU) and the check meter should be housed inside the miniature substation or on the pole-mounted kiosk. Some data concentrators can also do the bulk metering function. The data concentrator unit communicates with all the meters every 30 minutes within the transformer zone. The communication of the DCU and the EMU's will be through the power line carrier. The purpose is to compile individual meter electricity profile. Meaning each customer with a meter will have electricity usage profile. The data concentrator will record any event that is happening on each meter within the transformer zone. If there is any alert or alarm signal coming from any meter, it will be pushed to the head end system. If there is a power failure from the transformer, the DCU will send an alarm signal to the head end system (HES) to report the power failure. Tampered meters will be reported to the HES through the DCU.

The Check meter functionality is to record all energy imports within the transformer zone. The check meter is also used to monitor energy demand within the transformer zone. It also assists the network planners to monitor the transformer load and be able to plan in case the load attains the transformer capacity. If there is any energy theft within the transformer zone, it is easy to identify the problematic zone. The utility will focus on that transformer zone instead of auditing all the area.

3.2.2.6 Head End System (HES)

The head end system functionality is to register all the meters installed within the transformer zone once the transformer zone is energized, see figure 12 below. Data concentrator will record all the meters within the transformer zone and sends the meter data to the HES. The utility will link all the registered meters accordingly with their stand numbers according to the billing system. All the meter profile data will be transferred to the HES by the data concentrator unit using GPRS modem on a daily basis. Tamper alarms and power failure alarms will be given high priority by the DCU to the HES. All meter alarms will be flagged by the system. The

system will be able to read all the meters remotely through the DCU. The system will be able to do on-demand meter reading on individual meters or on all the meters.

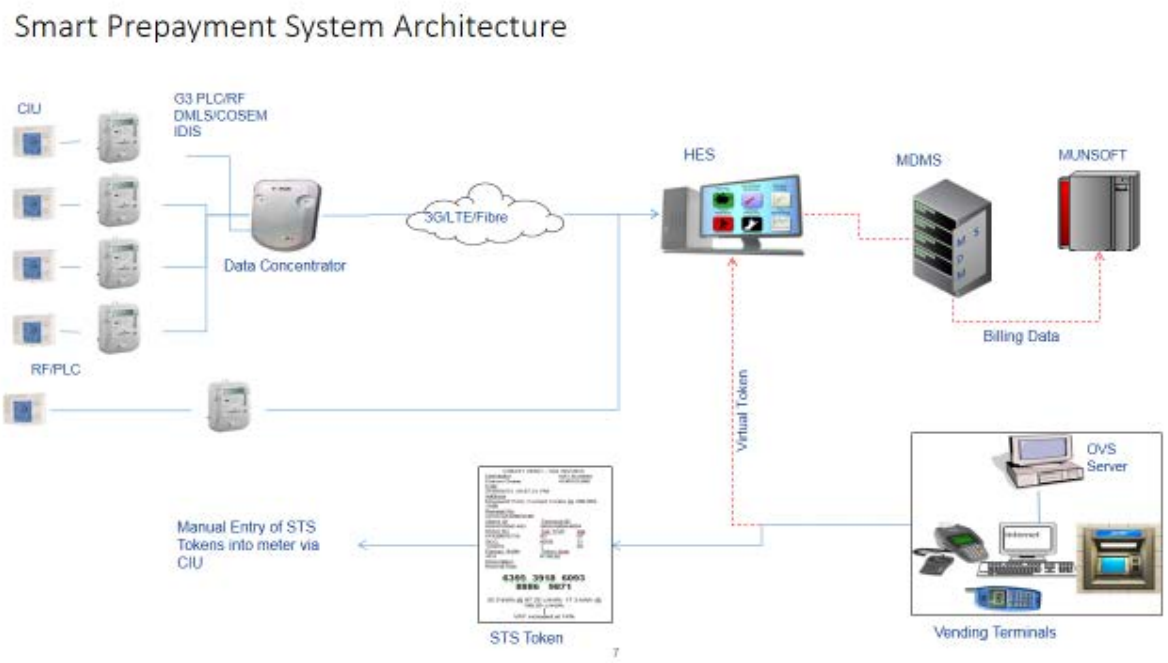


Figure 12: Illustrates HES

Remote connect and disconnect can be performed through the HES on customers that are on arrears. The head-end system can also be used to control the demand during peak periods by reducing the meter power limit on the latch during peak periods or by installing appliance control units on customers with swimming pools, under floor heating, geysers and air conditioners. The HES can be used as a SCADA to monitor the performance of LV network.

3.2.2.7 Energy Balancing and Feeder Balancing

Energy balancing can be performed through the HES for each transformer zone and the whole area that is on AMI. The system has a capability of consolidating all the check meter readings on all transformer zones and the main meter readings of the main feeders and flags the technical losses on the main feeders and be able to flag all the losses per transformer zone.

3.2.3 ZigBee Interface to existing AMI system

The proposed ZigBee technique is used in places where AMI system and AMR energy meters are already in place. ZigBee is proposed on this study to act as a sensor for detecting actions of theft of pilferage of electricity and send an alarm to the utility. It is used to monitor customer side, forms a node (ZigBee node) for apartment or particular area, and connect with GSM (global system for mobile) clients. The GSM connect with server and more clients depend on the customer site. The data sends automatically per 30 minutes and intimates the customer site through e-mail, SMS and billing; and the data will be stored in Microsoft access in the server. Due to this upgrade, power loss will be prevented and workforce to read the meters will be reduced [43].

3.2.3.1 Communication protocol

The data is transferred from energy meter to ZigBee, and from ZigBee to the GSM, The overall data is stored in PC server. Communication protocol is as follows [43]:

a. TCP/IP- Transfer Control Protocol/Internet Protocol;
b. UDP –User Datagram Protocol';
c. Ethernet Protocol; and
d. SNP – Simple Network Paging Protocol.

The TCP/IP is used to transfer data from server to the PC for sending e-mails to the customer site and data to be stored in a particular head of electricity board [43].

The UDP is used to communicate a short distance data to long distance data transfer. SNP is used to send SMSs for mobile communication to inform customer site via texts [43].

3.2.3.2 Software type

In this proposed technique, software is used as both front end and back end. The schematic drawing in Figure 13 shows ZigBee node connected with GSM node [43] thus:

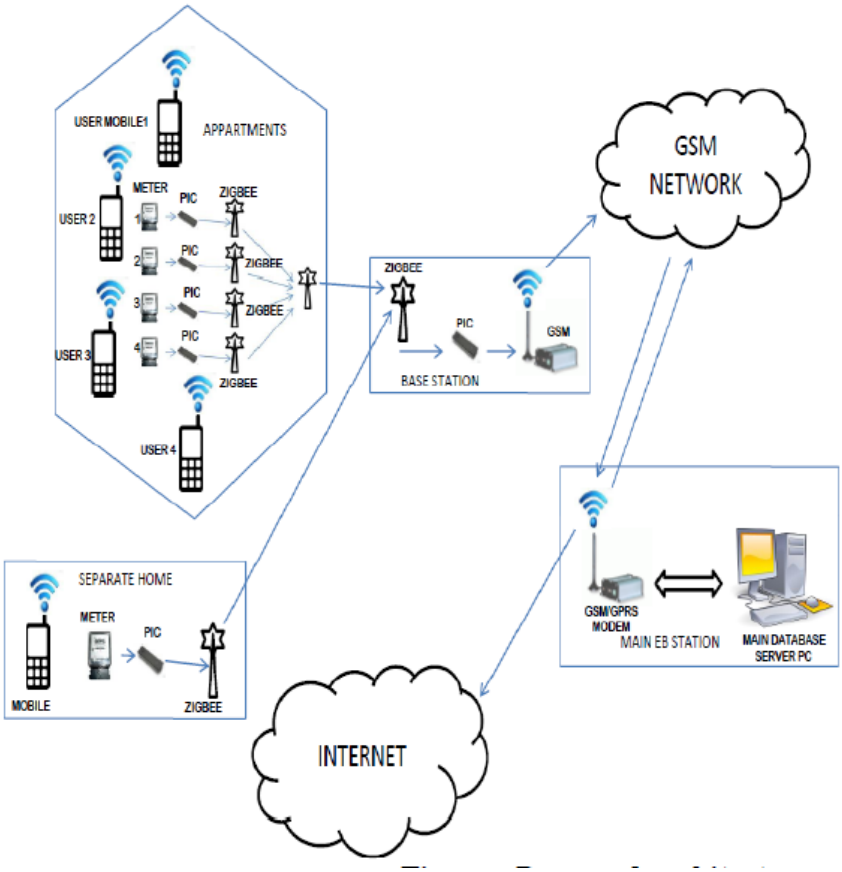


Figure 13: proposed architecture [43]

3.3 Cyber Security

Cyber security protects the system from unauthorized exploitation of systems, networks and technologies. Firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. It establishes the barrier between the trusted internal network and untrusted external network such as internet. Firewalls are often categorized as either network firewalls or host-based firewalls. Network firewalls filter traffic between two or more networks and run on network hardware. Host-based firewalls run on host computers and control network traffic in and out of those machines [44].

It is very important to put firewall into any head end system to protect the system from unauthorized exploitation of systems, networks and technologies.

3.4 Socio-economic conditions and marketing strategy

It is imperative to engage local councilors before implementing any of these monitoring and preventive utility projects. The community need to be engaged by organizing community meetings to share relevant information. A study needs to be carried out based on the living standard of the community. Implementing a project without a study may create a conflict with the community, for example, you may find that the goal of the project is to reduce the non-losses whereas the community is dependent on that illegality to survive due to high unemployment rate, number of pensioners and poverty of the poor. Such problems can be compensated by applying free basic electricity, skills training so that people can be employable or be able to create employment. Encouraging people to sell electricity using their cellphones can create other opportunities; they can even be utilized to assist in maintaining the system.

3.5 Marketing Strategy

Once the technology has been implemented, an educational campaigns need to be presented to teach people how to use electricity wisely. Engage the DoE to assist by supplying the community with solar geysers and energy saving lights. A campaign to educate the community on the benefit of such projects will be conducted by sponsoring different activities in the community. Safety campaigns can also be conducted to orient the community on the danger of connecting electricity illegally and the disadvantages of electricity thefts.

3.6 Case study analysis and outcomes

The city of Tshwane managed to collect 90 % of the overall income of the expected revenue using this initiative. The only smart meters that could not be accessed are the ones that were welded by the customers in which the city tasked the suppliers to collect on its behalf. Presently, the proposed wireless ZigBee system is beefing-up smart meters, to improve revenue collection. Table 5 illustrates the benefits of the project.

3.6.1 Benefit of the case study

Table 5: summary of the project - Decrease in energy losses

CUSTOMER	ASPIRATION	UTILITY
Control over consumption;	Control over illegal consumption;	Low/No revenue loss securing the financial sustainability of Utility
Fewer outages	Financial sustainability	High payment levels
Fewer safety incidents	Satisfied customers	Low /no outages due to overloading
Improved quality of supply	Customer controls energy consumption	Low maintenance costs;
Reliability of supply	Meter philosophy for all residential customers.(prepaid and/or smart meters)	High customer satisfaction index;
No estimations	Control over illegal consumption	High customer satisfaction index
No billing issues	Fairness to customers	Improved Operational Efficiencies.
Efficient use of electricity		

Chapter Four

Analysis and Discussion

4.1 Introduction

The Chapter is the analysis of the results and the discussions of the study; outcomes from the survey conducted are also presented. Tables formulated were used to describe and explain the ratings. The graphs elaborate more on the table ratings and their displays. Research questions were evaluated, answered and discussed, and thereafter survey conclusion recapped and summarized the overall survey exercise.

4.2 Data Gathering Process

Survey data were gathered by means of questionnaires, which were from the thesis objectives. The survey are composed of ten questions, with five ratings as applicable: strongly agree, agree, not sure, disagree and strongly disagree and ratings from 1 to 5 respectively. The survey was constructed manually because it was a combination of survey and interview whereby the participants were asked to elaborate on some questions to support responses where they are no clear meaning or understanding. The number of participants were 50 and were chosen randomly from across South Africa's power utilities customers and workers. Using an engineering conference as a contact platform, it was easier to reach out to participants from different provinces who were also part of the conference participants. The questions for the survey were as follows:

(A) Poor revenue collection is caused by high tariffs
(B) Connecting electricity illegally can affect human beings and environment.
(C) The stealing of electricity puts pressure on local municipalities' budget.
(D) Good collection of revenue improves service delivery.
(E) The impact of stealing of electricity hits hard on South Africa's economy.
(F) Wellness and workshops to the community can assist in understanding the danger of connecting electricity illegally.

(G) If the problem of stealing of electricity can persist, the loyal customers will end up resisting to pay their bills/buying of electricity.

(H) Strengthening up network security and protection can reduce stealing of electricity.

(I) Wireless technology can give good results in terms of curbing illegal consumption of electricity; and

(J) Solving communication problems on wireless system can decrease stealing of electricity, thereby increasing collection of revenue thereof.

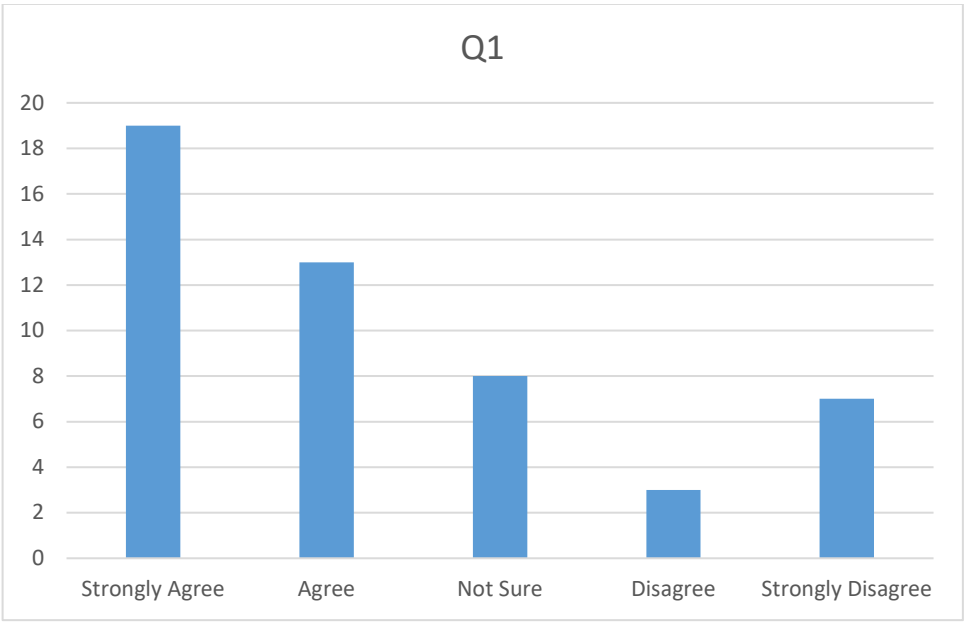
4.3 Survey Outcomes Discussion

(A) The outcome of question 1 gave positive response because out of the 50 participants, 19 agreed without doubt while13 agreed. The people are aware that losses incurred by utilities are caused by them and resulting in high tariffs. See table 6 and figure 14 for more details.

Table 6: Question 1 Outcome

RATINGS	Q1
Strongly Agree	19
Agree	13
Not Sure	8
Disagree	3
Strongly Disagree	7

Y



X

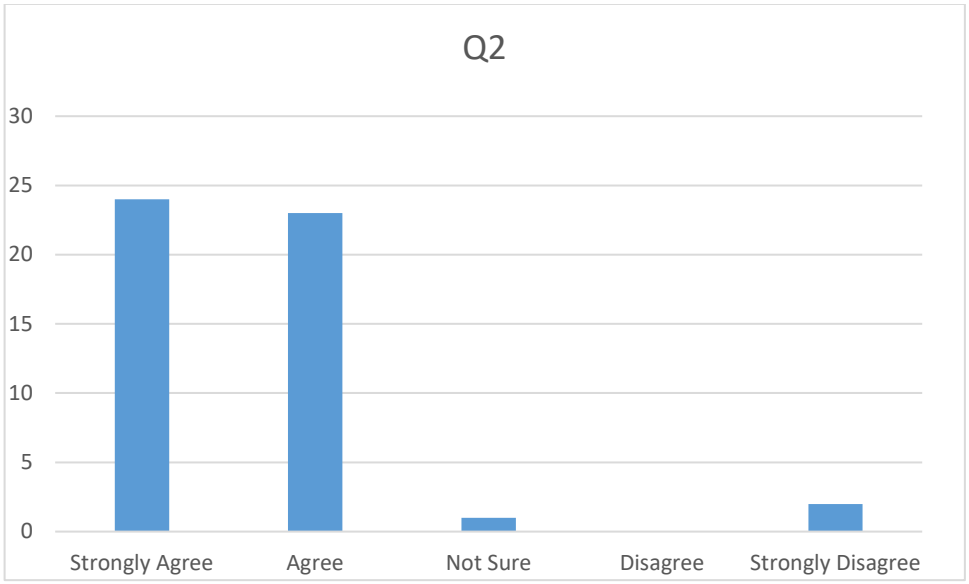
Figure 14: Question 1graph whereby X = Outcome, Y = Respondents

(B) Question 2 received 24 respondents on strongly agree terms while 23 respondents was on agree, which is positive. The interpretation is that the cost associated with losses are affecting the overall economy. Resources or funds that are allocated to cater for other service deliveries will be misdirected to pay unnecessary claims occasioned because of death caused by electrocution during electricity tampering and/or other such sundry claims of damages as a result of power in the area caused by short circuits of electrical power. See table 7 and figure 15 for more details.

Table 7: Question 2 Outcome

RATINGS	Q2
Strongly Agree	24
Agree	23
Not Sure	1
Disagree	0
Strongly Disagree	2

Y



X

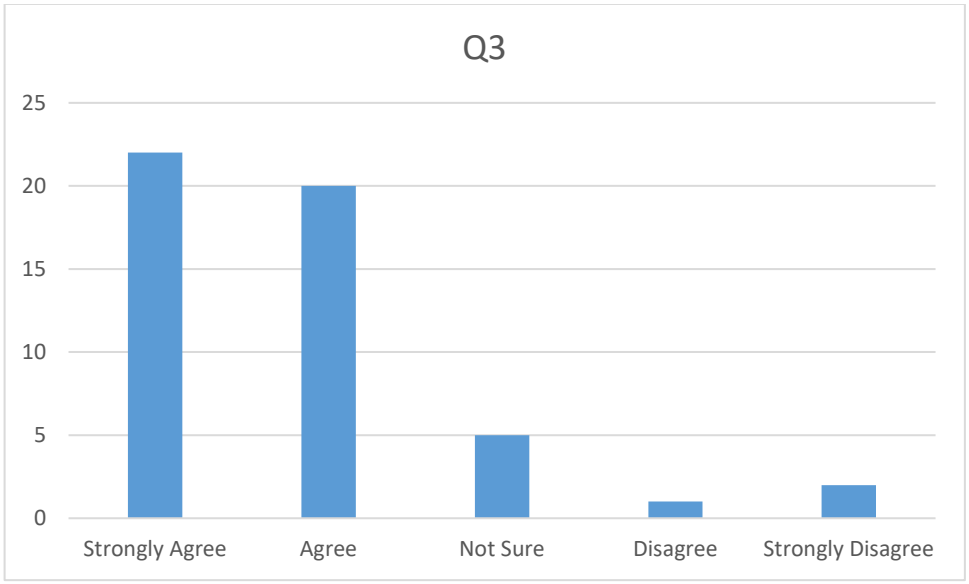
Figure 15: Question 2 graph whereby X = Outcome, Y = Respondents

(C) Responses on Question 3 on strongly agree, is 22 and on agree, is 20. It means that the people are very much aware of what damages are they causing by tampering with electricity illegally. Lack of knowledge of how these actions affects the municipality budget has been identified as main reason behind. See table 8 and figure 16 for more details.

Table 8: Question 3 Outcome

RATINGS	Q3
Strongly Agree	22
Agree	20
Not Sure	5
Disagree	1
Strongly Disagree	2

Y



X

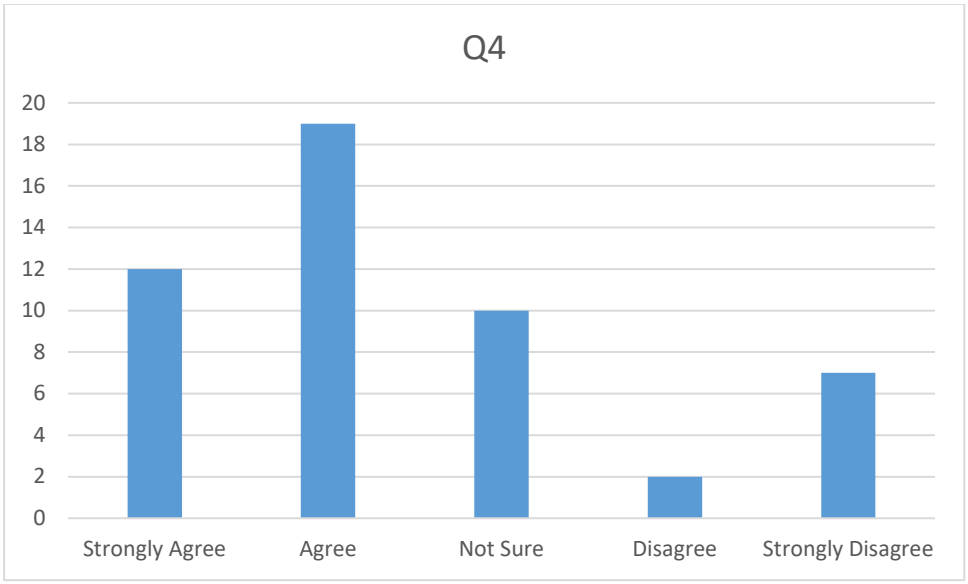
Figure 16: Question 3 graph whereby X = Outcome, Y = Respondents

(D) Question 4 received 12 strongly agree respondents and 19 agree respondents. This implies that a positive response has been achieved. The fact that unemployment rate is high may have induced people to resort to electricity thefts. This is a plausible reason deduced from the responses of question 4. Electricity theft by the people obviously increases the losses incurred. See table 9 and figure 17 for more details.

Table 9: Question 4 Outcome

RATINGS	Q4
Strongly Agree	12
Agree	19
Not Sure	10
Disagree	2
Strongly Disagree	7

Y



X

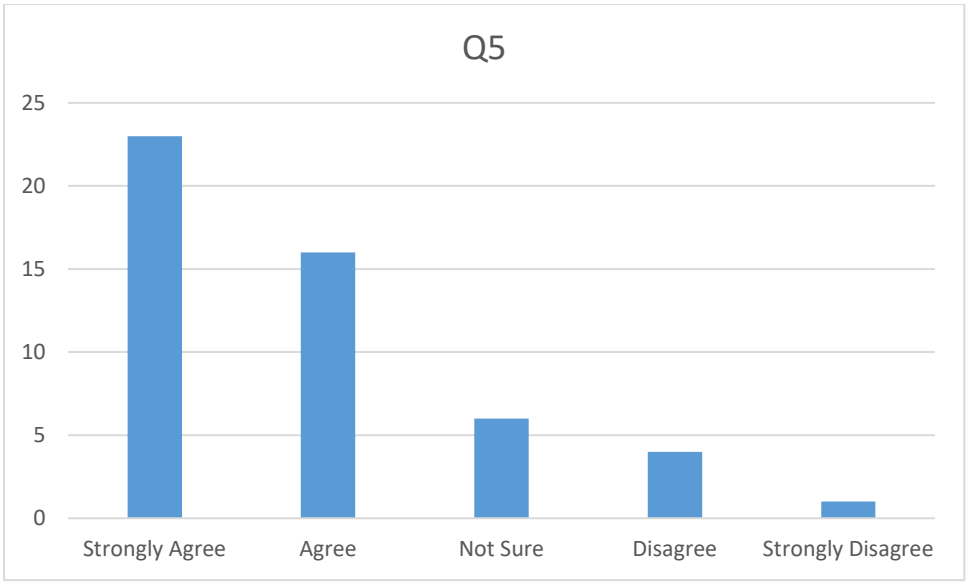
Figure 17: Question 4 graph whereby X = Outcome, Y = Respondents

(E) Question 5 is almost similar to question C. The only difference is that it specifies South African economy while the former refers to the municipality. Since it is known that the initial budget comes from the government, it is therefore important to remind the communities this fact, so that various acts of vandalizing facilities or collective infrastructures and networks be reconsidered and abruptly put to a stop. Reponses to this question got high number of strongly agree (23) and agree (16). See table 10 and figure 18 for more details.

Table 10: question 5 Outcome

RATINGS	Q5
Strongly Agree	23
Agree	16
Not Sure	6
Disagree	4
Strongly Disagree	1

Y



X

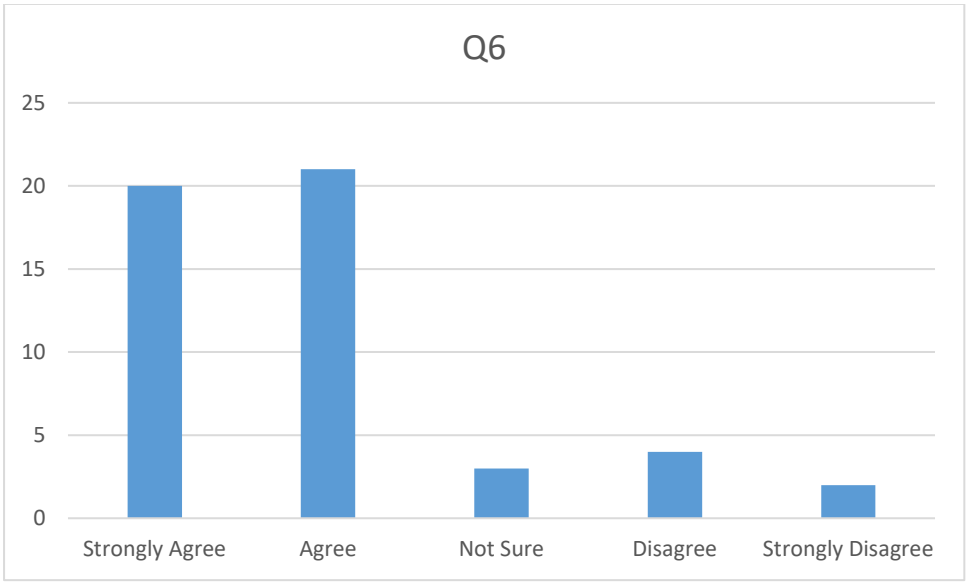
Figure 18: Question 5 graph whereby X = Outcome, Y = Respondents

(F) Question 6 got 20 strongly agree and 21 agree responses respectively. Some respondents opted not to answer the question. There was support for the hope that after the session, more knowledge will be acquired on how to handle electricity with care and on how to save it. With positive adherence to the knowledge acquired, users will reduce losses both on municipal and users side. It will also drastically reduce associated cost like claims, arrears and penalties. See table 11 and figure 19 for more details.

Table 11: question 6 Outcome

RATINGS	Q6
Strongly Agree	20
Agree	21
Not Sure	3
Disagree	4
Strongly Disagree	2

Y



X

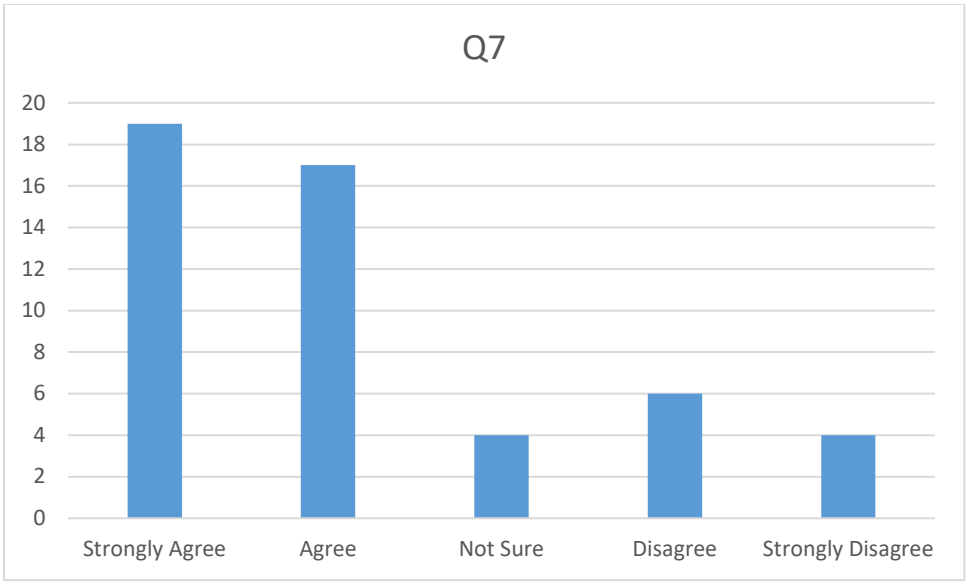
Figure 19: Question 6 graph whereby X = Outcome, Y = Respondents

(G) Question 7 also received positive response although not very satisfactory because strongly agree received 19 respondents and agree got 17. There were mixed responses to this question. Users who pay electricity end up defaulting as well. This was the response implication deduced from this question. Utilities are experiencing unnecessary losses of revenue because many people can afford to pay but default due to negligence of the need for constant offsetting of utility bills. See table 12 and figure 20 for more details.

Table 12: question 7 Outcome

RATINGS	Q7
Strongly Agree	19
Agree	17
Not Sure	4
Disagree	6
Strongly Disagree	4

Y



X

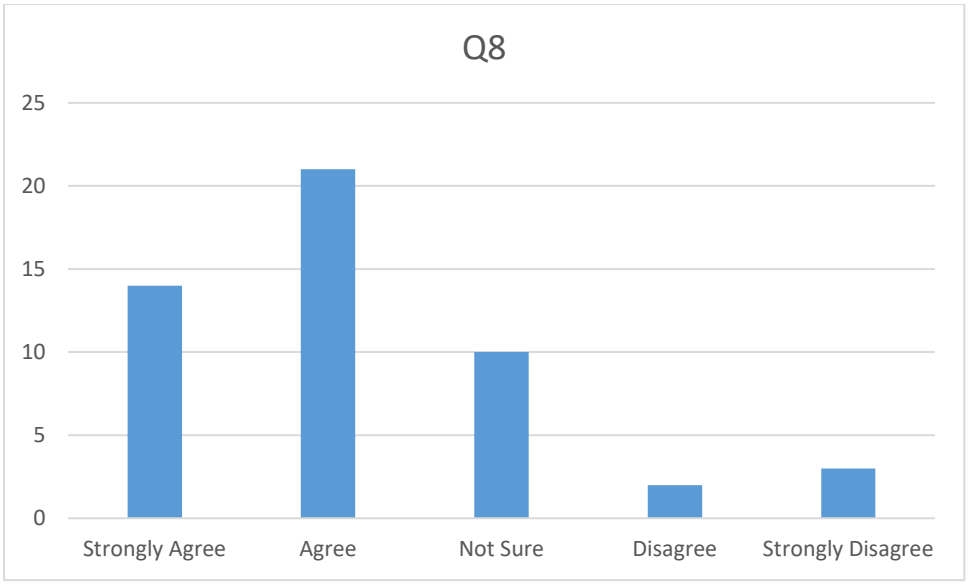
Figure 20: Question 7 graph whereby X = Outcome, Y = Respondents

(H) This question got 14 strongly agree and 21 respondents respectively. People are happy that they will be billed correctly and statements will reflect what they consumed unlike the current situation where they are over-charged by utility because of theft by others. See table 13 and figure 21 for more details.

Table 13: question 8 Outcome

RATINGS	Q8
Strongly Agree	14
Agree	21
Not Sure	10
Disagree	2
Strongly Disagree	3

Y



X

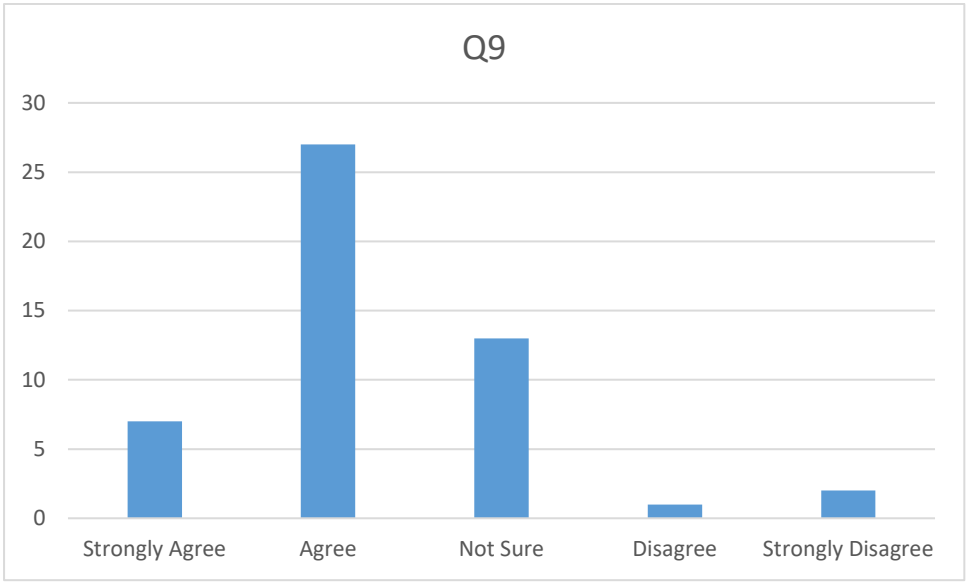
Figure 21: Question 8 graph whereby X = Outcome, Y = Respondents

(I) Question 9 got 7 strongly agree and 27 agree respondents respectively because the respondents were not familiar with the proposed systems. Nevertheless, detailed explanation of the proposed system, they were happy to learn and be aware of the benefits. The advantage to them is that there will be no more exposure of meters for tempering. It also requires no frequent maintenance and so will limit stranger's access into their compounds who come as meter readers. See table 14 and figure 22 for more details.

Table 14: question 9 Outcome

RATINGS	Q9
Strongly Agree	7
Agree	27
Not Sure	13
Disagree	1
Strongly Disagree	2

Y



X

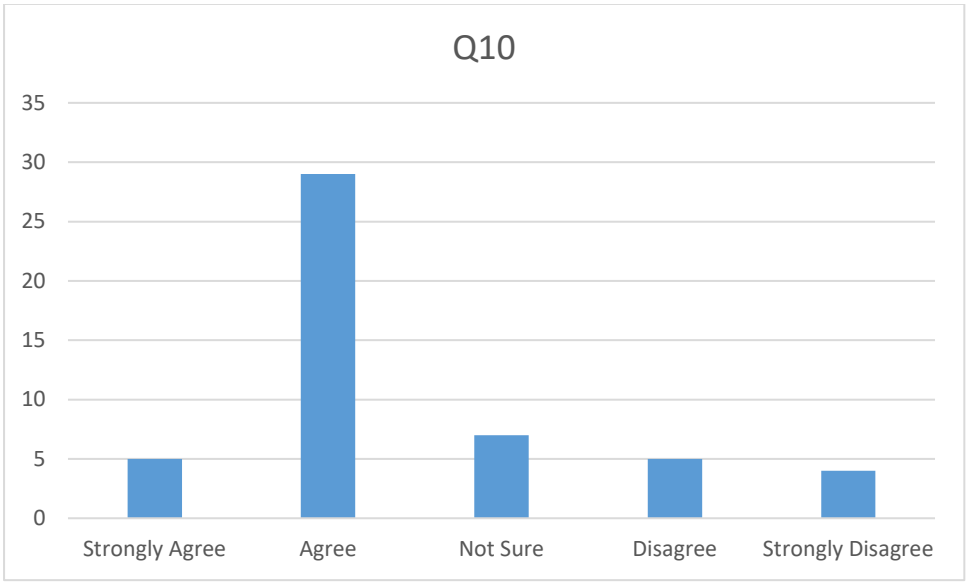
Figure 22: Question 9 graph whereby X = Outcome, Y = Respondents

(J) Question 10 got 5 strongly agree and 29 agree respectively. It also puzzled respondents because of their lack of knowledge. With detailed information on the workings of the system, there were thumbs up because even the current system have communication problems, which sometimes last for days leaving communities without electricity. See table 15 and figure 23 for more details.

Table 15: question 10 Outcome

RATINGS	Q10
Strongly Agree	5
Agree	29
Not Sure	7
Disagree	5
Strongly Disagree	4

Y



X

Figure 23: Question 10 graph whereby X = Outcome, Y = Respondents

Table 16: Outcome of survey per question

RATINGS	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10
Strongly Agree	19	24	22	12	23	20	19	14	7	5
Agree	13	23	20	19	16	21	17	21	27	29
Not Sure	8	1	5	10	6	3	4	10	13	7
Disagree	3	0	1	2	4	4	6	2	1	5
Strongly Disagree	7	2	2	7	1	2	4	3	2	4

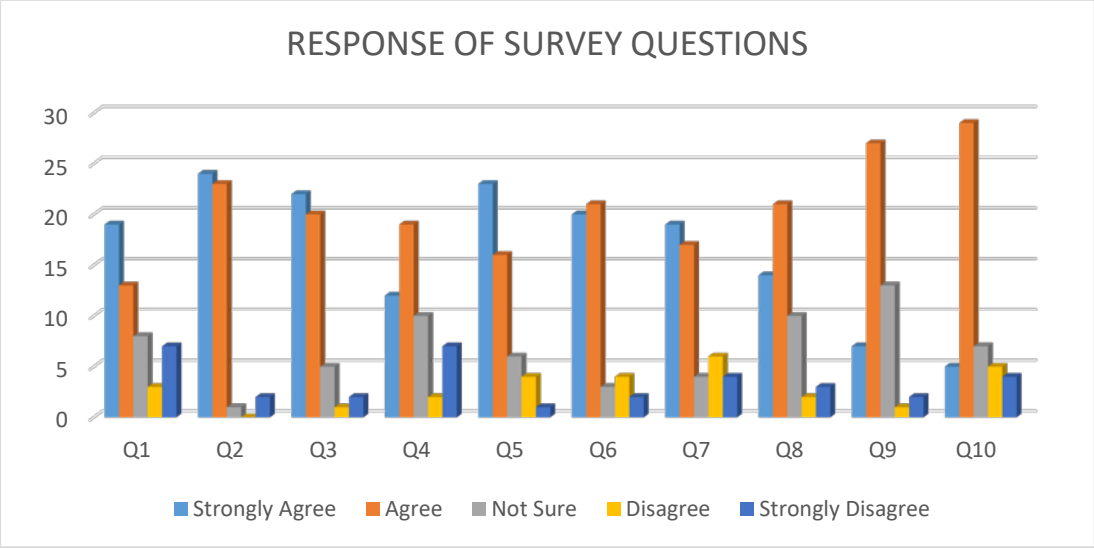
Table 17: Outcome of survey per question in percentage (%)

RATINGS	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10
Strongly Agree	38%	48%	44%	24%	46%	40%	38%	28%	14%	10%
Agree	26%	46%	40%	38%	32%	42%	34%	42%	54%	58%
Not Sure	16%	2%	10%	20%	12%	6%	8%	20%	26%	14%
Disagree	6%	0	2%	4%	8%	8%	12%	4%	2%	10%
Strongly Disagree	14%	4%	4%	14%	2%	4%	8%	6%	4%	8%

Graphical Presentation of Results

Results from the table to the graph are arranged as questions against number of people. The color light blue represents strongly agree, red represents agree, purple represents not sure, yellow represents disagree while royal blue represents strongly agree. Check figure 24 below where X axis represent number of respondents and y-axis represent survey questions 1 to 10.

Y



X

Figure 24: Graph of survey whereby X = Outcome, Y = Respondents

4.4 Survey Conclusion

It is concluded that the survey questionnaire served the purpose because a large number of respondents did support the thesis idea although it was clear that most of the end users lack knowledge about electricity infrastructures and the networks. A typical South African indigent citizen also called the poor of the poorest (POP) do not understand the importance of cash flow, that is the amount of money going into any organization and the amount which is coming out. The decision in doing this survey manually was taken with such reason in mind, so that if the customer do not understand, then the interviewer can assist a little bit to explain some of the

concept and attendant issues which the end users are not certain or aware of. The important situation that was noted is that, before interacting with the community, the first point of contact which cannot be omitted is to have access to local councilor whom they feel holds the responsibility to manage the affairs of the area because he/she was voted to bring service delivery to the people at all times.

The survey conducted is in tandem with the objective of the thesis. The research questions that were developed and tested provided proven percentage score of positive responses on the questionnaire. Though some respondents were not straightforward because they are still happy with the current situation of things wherein they still hope to indulge in theft of utilities and therefore saw the thesis as an avenue to rob them of freedom to continue the pilferage of electricity without any legal penalties imposed on them. The cost associated with energy losses that are caused by illegal electricity connections will decrease by upgrading the infrastructure, installing ZigBee technique and by giving attention to the communication system and its problems. The wellness and workshops need to be conducted so that communities at least once a month will learn the basics of the danger associated with connecting electricity illegally, tempering with government installed facilities and acquire knowledge on how to save energy. With these, the proposed technique is feasible, workable and implementable.

Chapter Five

Conclusion

5.1 Conclusion

Electricity theft is a growing problem nationally, and indigent people tend to make living out of it. Most fatalities occur in informal settlement, and incidents are not report to Law Enforcement. Electric cables lie across roads, railways, from one building to another in formal places, from one tin house to another. The electricity theft can be classified as an electricity theft pandemic. In some communities, there are kingpins – who build their own substation and supply to the community, at a fee every month. Imposing big fine to them showed no good results because of high unemployment rate, culprits tend to reconnect themselves due to failure to afford pay high penalties imposed to them and end up reconnecting themselves illegally.

The research study proposes wireless techniques (ZigBee), taking cognizance of communication constraints over long distances. The ZigBee technique is recommended technology solution that can mitigate electricity theft due to its characteristics of wireless and automated. It also comprises of star and mash network. It requires minimum staff.

In this pilot study, the techniques show good results for solution of curbing electricity theft but like in any other technique advantages and disadvantages exist. A constraint with ZigBee technology is that in very long distances it may have problems communicating clearly, 'The further you go, the lesser the communication". The causes being that, if long structures exists between router or radio or any other unforeseen interference then highly possible such failure will be experienced. The solution for the problem is to mount the ZigBee on top pole boxes, meaning it can work better when installed in upper structures, communication can improve over a long distance. The problem of cyber-attack on the network may be resolved by the monitoring of the network, tracking every action that is taking place in your network, and placing firewall into your head end system to protect the system from unauthorized exploitation of the system, network and technologies.

Electricity theft and its trend is growing very fast across the country of South Africa and indigent people tends to make a living out of it. Most fatalities associated with the tampering of electricity facilities happen in the informal settlement where this ugly situation happens. The most worrisome aspect of the intrigue is that these crimes are not reported to the law-enforcement agencies, the police and others. Unprotected and naked electricity wires and cables with currents passing through them are exposed to roads, railways and pathways or from one building to another in those settlements and locations and from one tin house or shacks to another. The electricity theft prevalence has therefore reached a crescendo. They are now being classified as a pandemic, which is ravaging the nation's economy in terms of revenue generation. Imposition of heavy fines and penalties on culprits may be the way to go but due to high unemployment rate, the situation can continue unabated if care and concrete strategy is not adopted. The miscreants tend to reconnect themselves due to failure of checks and in order to evade high penalties imposed on them, they end up reconnecting themselves illegally.

This study is proposing a wireless (ZigBee) techniques to mitigate this enigma but bearing in mind that wireless communication generally poses some problem over long distances. Wireless system networks (WSNs) measure environmental conditions like temperature, sound, pollution levels, humidity, wind speed and direction, pressure, sound, pollution levels, humidity, wind speed and direction, pressure and so on. The ZigBee technique is the technology that can mitigate the pilferages of electric power due to its characteristics of having the least amount of memory making it less expensive to manufacture. It also comprises of star and mash networks. It has long battery life with enough functions to talk to parent nodes; cannot relay data from other devices. Lastly, it requires less staff to manage the system. The ZigBee modem sends results to an authorized official who will act on them. The system will not allow the consumer to reset, meaning it will only allow the person from an authorized agency to reset or make changes. The microcontroller will convey the information to the relay and switch from ON to OFF and the power supply to the meter will switch off by the system. Then the LDC will display the message "meter tempered" and this message will automatically reach the utility's official.

In this study, the technique proposed and studies show good results as a solution to stopping the pilferage or theft. The major drawback of ZigBee technology is its application over a long distance. There could be problems of poor connectivity during transmission or communication of information. The further the distance, the lesser the connection. The principles behind this is simply interference; with barrier such as structures, buildings existing between system router or radio or any other unforeseen interference, then the likelihood of possible failure is high or even poor or no connectivity will be experienced. The solution albeit to install the ZigBee system on high altitude top pole boxes so as to overcome barriers. It therefore means that ZigBee system can work better when there are no barriers in between; communication can therefore improve over long distances. The problem of cyber-attack on network can be solved as well by monitoring the network, tracking every action that is taking place in your network, and lastly placing firewalls into head end systems in order to protect the system from unauthorized exploitation or access, network and technologies.

References

[1] T. B. Smith, "Electricity theft: a comparative analysis," *Energy policy*, vol. 32, no. 18, pp. 2067-2076, December 2004.

[2] I. E. Davidson, "Evaluation and effective management of non-technical losses in power networks," *The Transactions of the South African Institute of Electrical Engineers*, Vol. 94, No.3, pp. 39-42, September 2003.

[3] D. Gerbec, S. Gašperič, I. Šmon, F. Gubina, "Determining the load profiles of consumers based on fuzzy logic and probability neural networks," *IEE Proceedings-Generation, Transmission and Distribution*, vol. 151, no. 3, pp. 395-400, 2004.

[4] A. Nizar, Z. Dong, M. Jalaluddin, and M. Raffles, "Load profiling method in detecting non-technical loss activities in a power utility," in *2006 IEEE International Power and Energy Conference*, pp. 82-87, 2006.

[5] M. U. Hashmi and J. G. Priolkar, "Anti-theft energy metering for smart electrical distribution system," in *2015 International Conference on Industrial Instrumentation and Control (ICIC)*, pp. 1424-1428, 2015.

[6] J. Nagi, K. Yap, F. Nagi, S. Tiong, S. Koh, and S. Ahmed, "NTL detection of electricity theft and abnormalities for large power consumers in TNB Malaysia," in *2010 IEEE Student Conference on Research and Development (SCOReD)*, pp. 202-206, 2010.

[7] http://www.moneyweb.co.za/archive/eskom-customers-subsidise-huge-electricity-losses/ available on line, unpublished.

[8] P. Glauner, J. A. Meira, P. Valtchev, R. State, and F. Bettinger, "The challenge of non-technical loss detection using artificial intelligence: A survey," *arXiv preprint arXiv*:1606.00626, Jun 2, 2016.

[9] T. J. R. Ahmad and S. E. Reviews, "Non-technical loss analysis and prevention using smart meters," *Renewable and Sustainable Energy Reviews*, vol. 72, pp. 573-589, 2017.

[10] M. Maphaka, "Energy losses management programme", *60th AMEU Convention, Stellenbosch South Africa*, 2010.Unpublished.

[11] S.B. Tshikomba, "Illegal Connections and Tempering Offences in The city Of Tshwane," SARPA Convention, pp.1-5, 2013, unpublished.

[12] https://www.brainkart.com/article/Generation-Transmission-and-Distribution-of Electric-Power_12341/, 2017. Available on line.

[13] P. J. E. U. W. B. Antmann, "Reducing technical and non-technical losses in the power sector. Background Paper for the WBG Energy Strategy," pp. 1-34, 2009.

[14] V. C. Gungor and F. C. J. C. N. Lambert, "A survey on communication networks for electric system automation," vol. 50, no. 7, pp. 877-897, 2006.

[15] J.E. Calmeyer, "The role of smart metering in revenue protection," Strike Technologies, pp.32-34, August 2011.

[16] A. PM and D. J. Jeniba, "Electricity Theft Control Using Smart Prepaid Energy Meter." Unpublished.

[17] F. Biscarri, I. Monedero, C. León, J. I. Guerrero, J. Biscarri, and R. Millán, "A Mining Framework to Detect Non-technical Losses in Power Utilities," in *ICEIS (2)*, pp. 96-101, 2009.

[18] D. Gerbec, S. Gašperič, I. Šmon, F. Gubina, "Determining the load profiles of consumers based on fuzzy logic and probability neural networks," *IEE Proceedings-Generation, Transmission and Distribution*, vol. 151, no. 3, pp. 395-400, 2004.

[19] Report to NIST on Smart Grid Interoperability Standard Roadmap EPRI, Jun.17 2009 [online]. Available:http//www.nist.gov/smartgrid/InterimSmartGridRoadmapNISTestructure.pdf, unpublished.

[20] S. Druta and A. Cassin-Delauriere, “S-FSK and OFDM on a single platform – low cost PLC implementation made real,” unpublished.
[21] S.L. Narnaware, P.R. Mandape and L.R. Sarate, “Power theft prevention using smart meter with GSM technology,” *International Journal of Engineering Science and Research Technology*, pp.82-87, 28-29 November 2006.
[22] S. Patil, G. Pawaskar, K. Patil, “Electrical power theft detection and wireless meter reading," *International Journal of Innovative Research in Science, Engineering and Technology*, vol. 2, no. 4, pp. 1114-1119, 2013.
[23] A. Abdollahi, M. Dehghani, and N. Zamanzadeh, "SMS-based reconfigurable automatic meter reading system," in *2007 IEEE International Conference on Control Applications*, pp. 1103-1107: IEEE, 2007.
[24] M. Kumar, A. Kumar, A. Athalekar, P. Desai, and M. J. I. J. O. R. i. A. T. Nanaware, "Electrical Power Line Theft Detection," vol. 3, no. 5, pp. 46-50, 2015.[24] M. Maphaka, “Energy losses management programme,” AMEU Convention, pp.1-9, 2010.unpublished.
[25] V. Pandey, S. S. Gill, A. J. I. Sharma, "Wireless electricity theft detection system using ZigBee technology," *Computing and communication*, vol. 1, no. 4, pp. 364-367, 2013.
[26] H.-C. Chen and L.-Y. J. P. E. Chang, "Design and implementation of a ZigBee-based wireless automatic meter reading system," vol. 88, no. 1b, pp. 64-68, 2012.
[27] R. Rao, S. Akella, and G. Guley, "Power line carrier (PLC) signal analysis of smart meters for outlier detection," in *2011 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, pp. 291-296, 2011.
[28] A. Kulkarni, A. J. I. J. O. E. S. Patange, and Applications, "A review on zigbee, gsm, and wsn based home security by using embedded controlled sensor network," vol. 6, pp. 1-8, 2016.
[29] http://www.rfwireless-world.com/Terminology/zigbee-vs-wifi.html, 2003. Available on line, unpublished.
[30] G. N. Ericsson, "Cyber security and power system communication—essential parts of a smart grid infrastructure," *IEEE Transaction on Power Delivery*, vol. 25, no. 3, pp. 1501-1507, 2010.
[31] G. N. Ericsson, "Toward a framework for managing information security for an electric power utility—CIGRÉ experiences," *IEEE Transactions on Power Delivery*, vol. 22, no. 3, pp. 1461-1469, 2007.
[32] Y. Yan, Y. Qian, H. Sharif, D. Tipper, "A survey on cyber security for smart grid communications," *IEEE Communications Surveys & Tutorials*, vol. 14, no. 4, pp. 998-1010, 2012.[33] Information technology – code of practice for information security management 2000, ISO/IEC 17799, unpublished.
[34] S. Clements and H. Kirkham, "Cyber-security considerations for the smart grid," in *IEEE PES General Meeting*, pp. 1-5: IEEE, 2010.
[35] Swedish Civil Contingencies Agency, Guide to Increased Security in Process Control System for Critical Societal Functions {Online].Available: http://www.krisberedskapsmyndigheten.se/up-load/17915/SCADA_eng., 2008. Available on line.
[36] G. Dondossola, O. Lamquet, and A.Torkilseng, “Key issues and related methodologies in the security risk analysis and evaluation of electric power control system,” CIGRE Session, Paris 27, Aug. 1-2Sep. 2006.
[37] Common vulnerable and Exposures List [Online]. Available: http://www.cve.mitre.org/, 1999. Available on line.
[38] X. Du and H. H. Chen, "Security in wireless sensor networks," *IEEE Wireless Communications*, vol. 15, no. 4, pp. 60-66, 2008.
[39] H. Li, R. Mao, L. Lai, and R. C. Qiu, "Compressed meter reading for delay-sensitive and secure load report in smart grid," in *2010 First IEEE International Conference on Smart Grid Communications*, pp. 114-119, 2010.

[40] M. Jensen, C. Sel, U. Franke, H. Holm, and L. Nordström, "Availability of a SCADA/OMS/DMS system—a case study," in *2010 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT Europe)*, pp. 1-8, 2010.

[41] Y. Yan, Y. Qian, H. Sharif, D. Tipper, "A survey on cyber security for smart grid communications," *IEEE Communications Surveys & Tutorials*, vol. 14, no. 4, pp. 998-1010, 2012.

[42] C.-W. Ten, M. Govindarasu, and C.-C. Liu, "Cybersecurity for electric power control and automation systems," in *2007 IEEE International Conference on Systems, Man and Cybernetics*, pp. 29-34, 2007.

[43] S. Arun, S. J. I. J. o. A. R. i. C. S. Naidu, and S. Engineering, "Design and implementation of automatic meter reading system using GSM, ZIGBEE through GPRS," vol. 2, no. 5, 2012.

[44] htts://en.wikipedia.org/wiki/firewall, 2006.