How wireless Electricity Theft Detection Can Assist in Reducing The theft or Stealing of Electricity

Author & Presenter: S. Tshikomba B-Tech Power Eng. BSc. MOT - Chief Engineer R.P.O. (Acting Deputy Director) of City of Tshwane Metro.

Abstract

South African Utilities are struggling to collect revenue due to electricity theft; therefore, there is a need for researchers to look at wireless communication technique. This paper will cover electrical power theft detector via wireless technology. The electrical power theft detector will assist in detecting an unauthorized tapping on distribution lines via transmission and receiving technique. The uniqueness of this system is that it recognizes the common act of stealing electricity via tempering with the meter box. In the market, there are several types of wireless system or PLC, s, to avoid complexity of the study only ZIGBBE (PLC) will be discussed.

This system ensures the accurate billing of the electricity consumed hence to provide the best way to prevent from the electricity theft. The supply cut by this system can only be reset by the authorized person of the Utility Section making it best method to reduce the manual error and provide an excellent way to detect the bypassing of the energy meter. The ZIGBEE is preferred on this study because it provide major advantages such as low power consumption and the low cost of the ZIGBEE module.

1 Introduction

Power theft is the most worrying factor in all South African Utility companies. Electricity fraud is a dishonest or illegal use of electricity equipment or service with the intention to avoid billing charge [1]. Losses encountered due to stealing of electricity is called energy losses, divided into Technical and non-technical losses of which no-technical losses are uncontrollable and affects collection of revenue in Utility companies. This paper discusses the technology of wireless electricity theft detector in curbing stealing of electricity. Bypassing of energy meter is common and energy meter is known to be the easiest reachable part of the infrastructure in terms of tempering. The wireless theft detector system is preferred in such areas. The use of the power grid for data transmission is very commercially attractive to Utilities as having the lowest operational costs. The research efforts focused for years on developing a cheap bi-directional technology that would enable power line communication (PLC) for application such as remote meter reading power grid control and maintenance, telemetry and others [2].
This paper will cover Effects of electricity theft, types of techniques, and ZIGBEE technology overview.

2 Effect of electricity theft

Electricity theft is a major contributor for non-technical loss and it now reached a stage where it is not easily controllable. Electricity theft can be considered as interference of the system in the way to adulterate its measurements by total or partial bypassing of metering system Theft or Pilferage of energy is mainly due to two types of consumers, non-consumers and bonafide consumers. Power theft can be measured Accurate estimation of theft is possible by conducting through analysis of power system. Analysing transmission and distribution losses can give clear indication of the power theft.
Electricity theft affects generated units hence causing load shedding because the Utility do estimations in advance looking at that present moments to prevent disturbance during peak loads. The utility companies mostly transfer the economic losses that are caused by stealing of electricity on honest and legal consumers in terms of increase in tariff [3].
The following activities experienced from customer side can be considered as an electricity theft [3-4].

- Tempering with energy meter
- Bypassing electric meter
- Evading payment (non-payment of bills, billing irregularities)
- Magnets, reversing the current direction by changing the terminals were used in analog disc type energy meter
- Radio frequency devices employed to temper electronic meter
- Intermittent and opportunistic theft by well off
- Illegal customers disconnect neutral from the return path. In such a case energy meter assumes that voltage between live wire and the new neutral is zero, which implies total energy consumed is zero.

3 Types of Techniques

Two types of techniques are used to deliver the information to the authorised agency to control the theft of the electricity via bypassing the energy meter; [5];

3.1 wired techniques

- Electrical cables
- Coaxial cable
- Optical fiber

3.2 wireless technique

- ZIGBEE technology
- GSM technique
- WI-FI
- Infrared
- Wi-max
- Bluetooth

4 ZIGBBE technology overview

This ZIGBEE technology is utilised because it can limit all the problems that are associated with the installations such as rural areas where it is really very much difficult to install the wired system to convey the information. The ZIGBEE module provides an efficient way to convey the information to the authorized official at low cost as compared to that of the GSM Modem and utilises a cell phone to send the message to the officials having a long battery life. The other wireless techniques such as Bluetooth, infrared etc. are having the limitation of range and of the efficiency. The wireless system based on GSM/GPRS is well known but the fee is needed to utilise it and the cost of hardware system is very high. In this regard, the ZIGBEE technology which works in international free frequency band and access self-organisation function is adapted to solve the problem in the wireless electricity theft detection system.
The ZIGBEE standard provides network security and application support services. Employing a suit of technologies, it enables scalable, self-organising, self-healing networks that can manage various data traffic patterns. ZIGBEE is a low cost, low-power wireless mesh-networking standard. The low cost allows the technology to be widely deployed in wireless control applications. The low power usage allows longer life with smaller batteries, while the mesh network provides high reliability and larger range of operations. ZIGBEE can meet the growing demand for capable wireless networking between various low power-consuming devices.
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 For ZIGBEE network model refer to figure 1 below [5].

4.1 ZIGBEE devices

The ZIGBEE consists of the three following devices [5].

4.1.1 ZIGBEE Coordinator device

- It is the devise of ZIGBEE, which starts the signal. It coordinates the signal at the transmitting time in which signals are easily transmitted.
- The is one and only one coordinator per ZIGBEE network
- This devise has the unique responsibility network tree and might bridge to other networks.
- There is exactly one ZIGBEE coordinator in each network.
- It is able to store information about the network, including acting as the repository for security keys.

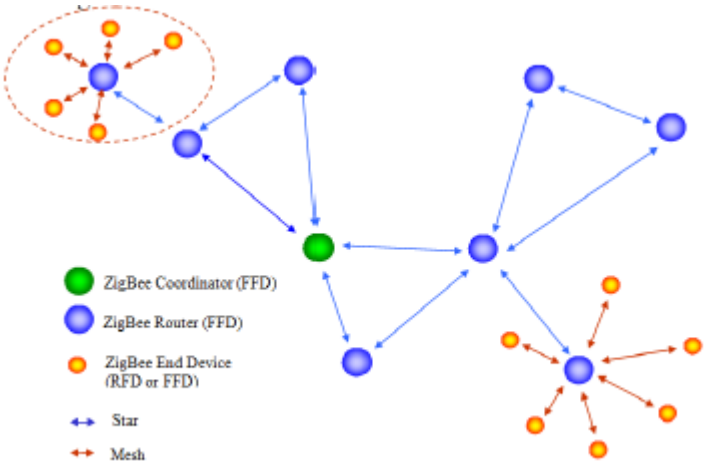
4.1.2 ZIGBEE Router device

- It is provided 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.
- Routers can act as an intermediate router, passing data from other devices.

4.1.3 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.
- Then nodes in a star network are all end devices except for the coordinator.
- It is used for 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.
- I requires the least amount of memory, and therefore can be less expensive to manufacture than a ZR or ZC.

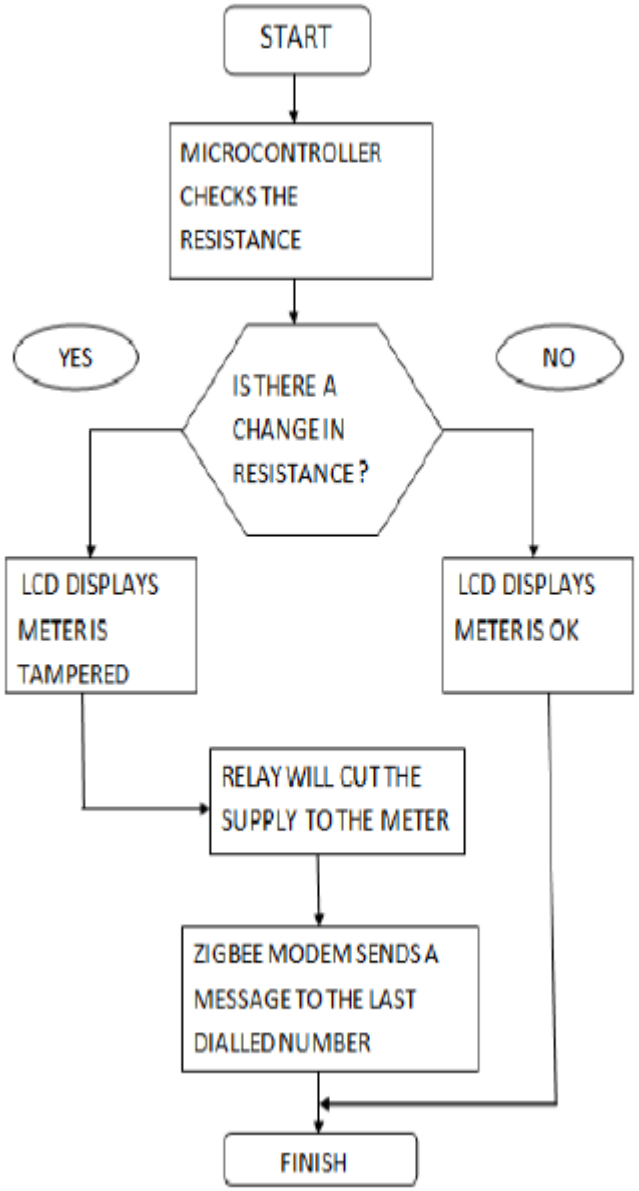
Figure 1: ZIGBEE Network Model



4.2 How ZIGBBE function

The flow chart shows how the system is used to prevent the electricity theft that is 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 is tempered. To operate the microcontroller via the relay there is a need for amplifier circuit because no direct access of the relay to the microcontroller. When the microcontroller switches off the load, the ZIGBBE Modem sends the results to the authorised official. The system will not allow the consumer to reset, meaning it will only allow the person from authorised agency to reset. The microcontroller will convey the information to the relay and switch from ON to OFF and the power supply to the meter will be cut down by the system. Then the LDC will display the message “Meter tempered” and this message will be conveyed to the official. Figure 2 below summarise the process [5].

Figure 2: Shows the process flow of ZIGBEE



5 Conclusions

The wireless ZIGBEE technique based system is preferred to detect the stealing of electricity worldwide, to control the revenue losses. The grid infrastructure was not initially designed to handle communication traffic, high performance signal processing is critical to ensure two-way communication. The theft of bypassing meters is the most popular across the Country when comparing to the other techniques used to steal electricity. This system ensures the accurate billing of the electricity consumed. It also provide the best way to prevent electricity theft. The advantages are that it can reduce manual errors, provide an excellent way to detect the bypassing of the energy meter. ZIGBEE is a wireless communication technology that uses low cost and low power consumer technique and provides long battery life to use because it uses cellphone to send information. The wireless system gives much better results at short haul but the concern of the long haul depends upon the service employed by the network. The research in looking into improving this system is still in pipeline. The missing link is to improve the communication part of it in long haul.

Acknowledgement

The author would like to thank the AMEU and my Organisation City of Tshwane to afford me this opportunity to attend the Conference and share my knowledge with Engineers from different parts of the Country and not to forget all my colleagues who contributed towards assisting me in compiling this paper.

References

[1] Nagi J. Yap K.S., Nagi F., “NTL Detection of electricity theft and abnormalities for large power consumers in TNB Malaysia”, IEEE Power Engineering Journal, 2010
[2] Druta S. Cassin-Delauriere A., “S-FSK and OFDM on a single platform – low cost PLC implementation made real”
[3] Hashmi U., “Anti-theft energy metering for smart electrical distribution system” IEEE International Conference on Industrial Instrumentation and Control, May 2015
[4] Nizar A.H., Dong Z.Y., Jalaluddin M., “Load profiling method in detecting non-technical loss activities in a power utility”, IEEE First International Power and Energy Conference PEC, 2006
[5] V. Pandey, S. Singh Gill, A Sharma, “Wireless electricity theft Detection System Using ZIGBEE Technology”, Volume 1, Issue 4, March 2013