International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 08 Issue: 02 | Feb 2021 www.irjet.net p-ISSN: 2395-0072

# Industrial Power Theft Monitoring and Control with Zigbee Communication

**Sornamurugan[1], Muthurajan[2], Balamurugan[3]**

*[1,2]Student,[3]Lecturer, Department. of Electrical and Electronics Engineering,*
*Lakshmi Ammal Polytechnic college, Tamilnadu, India*

---

**Abstract -** *Power Demand is one among some huge problems in the present situation. Steps are taken in various aspects to face the situation. Many Generating units are planned to construct and many new technologies are in the verge to implement to meet out the challenge. In this paper it is planned to monitor as well as to control power theft. Here the loads that involve in power theft are only industrial loads. The concept on explaining short and crisp, when an industry consumes power in an illegal manner which is considered to be theft then supply to the particular load is tripped off automatically from the station. Only the load that involves in theft alone will get tripped and other loads remains unaffected. Moreover any load can be disabled as well as enable right from the EB station by means of Zigbee communications. In this method the distributed and the consumed current is compared and measured with a micro controller. A minimum tolerance value is set to consider the natural losses that occur in the transmission lines. When the difference value between the two measured values go beyond the tolerance value then it is considered that there occurred a power theft and according to that the particular load is identified by the station by means of unique zigbee id. It leads to the tripping off the load by means of relay which is connected between the transmitted and received ends.*

***Key Words***: zigbee communication, Power theft, Load, EB station.

## 1.INTRODUCTION

Power demand is one among the major problem that prevails in the present situation, also which leads to further inconvenience because of load shedding. By this time many methods and techniques are also growing faster to meet out the situation. But some consumers in advance move to another step by consuming the normal amount of power and sometimes more than normal, but without paying money for it, which is termed as power theft. This unnoticed problem is emphasized in our project and it is taken into serious consideration because, when thinking of the existing situation of power demand and load shedding it is also necessary to think of other consumers as well as E.B. Stations both in technical and economical ways. It do not matter when a single consumer involves in power theft, but what if when all the consumers began to start it with assuming that only they are involved in that and hence there will not be any adverse effects. Hence we developed this innovative project to meet out this problem. There are ways to identify the region of power theft, but in addition to that apart from identifying the location of power theft, the power flow is continuously monitored and steps are taken spontaneously from the E.B. Station automatically by tripping off the particular load involved in stealing the power. Apart from that manual control to enable and disable any load directly which are connected to the station. The important matter to note is that the loads and consumers that are mentioned here are only industrial and not domestic consumers.

## 2. BLOCK ARRANGEMENT

The overall circuit is divided into two blocks of components. They are apart from specific blocks such as power supply circuit, CTcircuit, Precision rectifier circuit, zigbee circuits, etc…Such overall circuit is divided into the following two blocks, which are listed as

- Transmitter block
- Receiver block

Generally the transmitting circuits are placed in the load or industrial consumer and the receiving circuit is placed in the E.B. station side. In between the communication link is provided by means of the Zigbee protocol or zigbee communication.

## 2.1 TRANSMITTER CIRCUIT

The Transmitter circuit consists of two current transformers or any devices used for measuring a small amount of current for comparing purposes. A Relay is connected between the two CTs. One CT is connected at the distributed end and the one near the load which measures the consumed current as per the readings of the meter. All the components are connected to the microcontroller which compares the 2 current values. When the difference between the 2 values exceeds the tolerance value it is transmitted through the Zigbee transmitter.

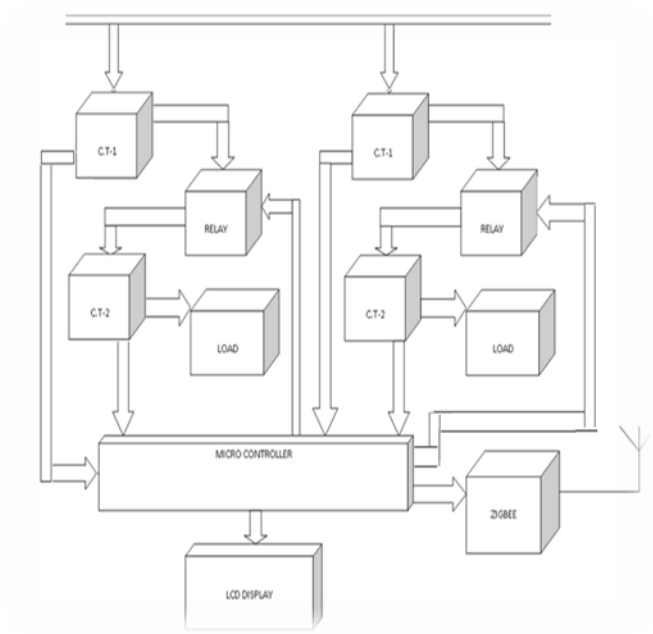


Fig-1: Transmitting circuit

## 2.2 RECEIVER CIRCUIT

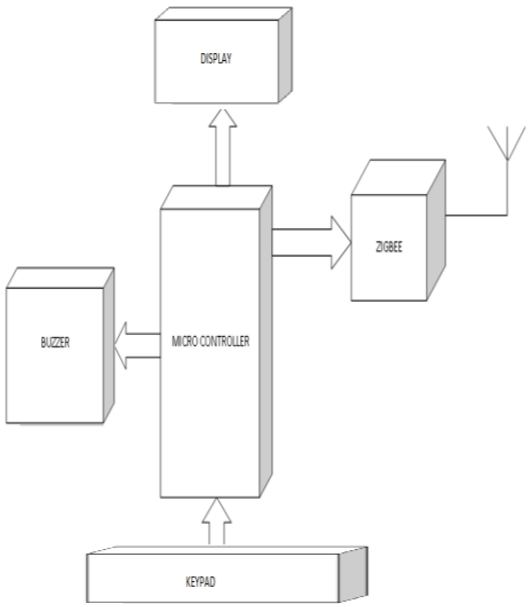


Fig-2: Receiver circuit

The receiver circuit receives the transmitted signal and according to that the particular load which involves in theft will be tripped by means of another zigbee component in the station.

## 3. COMPONENTS.

- Power supply unit
- Current transformer
- Precision rectifier setup
- Micro controller kit
- Relay circuit
- Zigbee circuit
-

### 3.1 Power supply unit

This circuit by means of Step down transformers, Rectifiers, Filter circuit and a regulator IC to feed with regulated DC voltage to enter into the circuit and its components

### 3.2 Current transformer – precision rectifier setup

The current Transformer is used to measure the current from the small value taken from the actual value of current to be measured. Moreover it is also used as a protection instrument. The precision rectifier is used to sense the very small value of current fed out from the current transformer.

### 3.3 Microcontroller kit

The microcontroller compares the current values and communicates by means of corresponding I/O ports for communication.

### 3.4 Relay circuit

The Relays which in normal are in NC and to trip off the load it is connected as NO.

### 3.5 Zigbee circuit

The Zigbee circuits by the way it means the transmitting and receiver circuits. They are used for communication purposes. The communication here mentioned means the connection between the transmitter and the receiver.

## 4. ZIGBEE PLATFORM

The ZigBee standard is supported by a consortium of over 200 companies grouped under the name of ZigBee Alliance. The goals driving the ZigBee Alliance are the creation of a reliabzle, low-cost, low-power, open global standard for low data rate wireless solutions, while allowing multi-hop routing of data. The ZigBee standard through mesh network capability and AES 128-bit encryption provides support for self-healing and high security. **Figure** describes a ZigBee network topology which typically includes three types of devices or nodes.

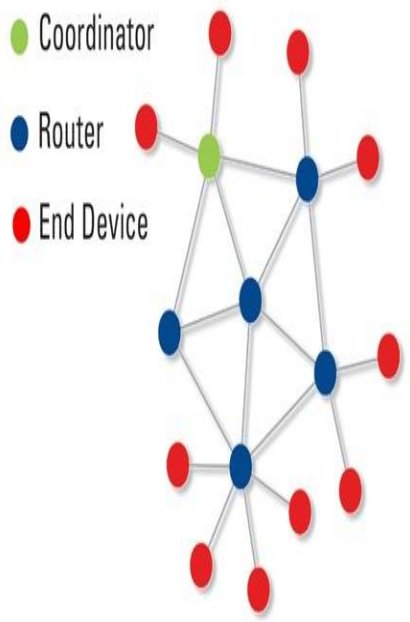


Fig-3: ZigBee Network Topology

### 4.1 Coordinator

One coordinator exists in each network. It starts the network and handles management functions as well as data routing functions. These functions require that the coordinator always be powered. Therefore, this type of node is recommended to be main-powered.

### 4.2 Routers

In most cases, routers are also main-powered. They help carry data across multi-hop ZigBee networks including a variable number of routers and, in some cases, are without routers, thus, transforming the network into a point-to-multipoint.

### 4.3 End Devices

These are devices that are battery-powered due to their low-power consumption. They sleep most of the time and wake up regularly to collect and transmit data. Devices such as sensors are configured as end devices. They are connected to the network through the routers.

## 5. OSI MODEL

We have built is a simple transmission system based on the Zigbee routing and networking protocol. Data networks (and transmission systems) are typically divided into various layers based on functionality. This is sometimes called a protocol stack (in our case, we are using a Zigbee stack). Essentially, the lower the layer, the closer we are to worrying about actual physical electrons flying around. Conversely, the higher the layer, the less we are worrying about physical constraints and the more abstract the data structures are that we are dealing with and manipulating.

| OSI Model | | | |
|---|---|---|---|
| | Data unit | Layer | Function |
| Host layers | Data | 7. Application | Network process to application |
| | | 6. Presentation | Data representation,encryption and decryption |
| | | 5. Session | Interhost communication |
| | Segments | 4. Transport | End-to-end connections and reliability,Flow control |
| Media layers | Packet | 3. Network | Path determination and logical addressing |
| | Frame | 2. Data Link | Physical addressing |
| | Bit | 1. Physical | Media, signal and binary transmission |

Fig-4: OSI Model

### 5.1.1 PHYSICAL LAYER

The physical layer's job is to move individual digital bits from one place to another. The protocols in this layer depend on the actual physical medium. For example, in a wireless system, the actual physical medium is simply the atmosphere.

### 5.1.2 LINK LAYER

A network's link layer routes a series of bits (sometimes called a datagram) from one node in a network to another. This can happen through a series of intermediate switches (or routers). Protocols at this layer provide more robust and full-featured services than protocols at the physical layer. WiFi is one example of a link-layer protocol.

### 5.1.3 NETWORK AND TRANSPORT LAYERS

Again, since these layers are higher in the model, protocols at this layer typically are more full-featured than protocols at the link or physical layers. Protocols at these layers use the link layer's routing capabilities to move the aforementioned datagram's between nodes in a network. The Internet Protocol (IP) is probably the most famous network layer protocol, while the Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP) are two examples of well-known and widely-used transport-layer protocols. Certain higher-level functionality is more prevalent in these two layers than in lower levels. For example, flow control controlling the transmission rate between nodes in order to lower congestion on the network (realizing that even just a two-node transmission system can be considered a network) and reliable transmission (ensuring that a packet is actually received) are two features commonly implemented in the network and transport layers.

### 5.1.4 SESSION, PRESENTATION AND APPLICATION LAYERS

These layers are essentially the end-result of a networking protocol stack. For example, a web browser resides in the application layer. These layers make use of all of the lower layers to send data between nodes on a network, and then use their own protocols for manipulating that data. A web browser renders HTML but uses lower-level protocols to send HTML between nodes in a network.

## 6. CONCLUSIONS

The zigbee used here has many advantages when compared with other technologies such as Wi-Fi, GSM. It has longer life with very low price. Its efficiency is high because of its very high speed. It also has a major disadvantage of distance. Hence it needs to be required in a large manner, but no matter because of low price. The current transformers and other current measuring instruments cost not much. Anyhow, they are all used in normal transmission and distribution systems. Here the microcontroller in the E.B.Station can be fixed as one in number and for any increase in the number of consumers it can be added by means of the unique zigbee ID. More importantly the control from the station can be done either by means of hardware switches or also by means of using compute. Shortly the cost of this project will not exceed the cost caused due to the power theft; hence it can be applicable for the present situation.'

## REFERENCES

[1] T.B. Smith, "Electricity theft- comparative analysis," Energy Policy, vol. 32, pp. 2067–2076, Aug. 2003M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

[2] A. A. Chauhan, "Non-technical losses in power system and monitoring of electricity theft over low-tension poles," in Proc. Second Int. Conf. on Advances in Computing and Communication Engineering, India, 2015, pp. 280-284.

[3] N.P.Wandhare, S.D.Kondra, K.H. Gulhane and K.J.Dave, "Automatic Load Balance and Theft Detection System",International Journal of Application or Innovation in Engineering & Management(IJAIEM).

[4] international Conference and Exhibition on Electricity Distribution, Prague, Czech Republic, June 2009, pp. 1–4

[5] J. R. Galvan, A. Elices, A. Munoz, T. Czernichow, and M. A. Sanz-Bobi, —System for Detection of Abnormalities and Fraud in Customer Consumption‖ in Proc. of the Electric Power Conference, Nov. 1998. [JRG 1998].

## BIOGRAPHIES

**S.Balamurugan,** Lecturer, Department Of Electrical & Electronics Engineering, Lakshmi ammal polytechnic college, Tamilnadu, India

**B.MUTHURAJAN** Second year, Department of Electrical & Electronics Engineering, Lakshmi ammal polytechnic college, Tamilnadu, India

**A.SORNAMURUGAN** Second year, Department of Electrical & Electronics Engineering, Lakshmi ammal polytechnic college, Tamilnadu, India