**Republic of Iraq**
**Ministry of Higher Education**
**and Scientific Research**
**University of Babylon**
**College of Engineering**
**Department of Electrical Engineering**


# Design and Implementation of Wireless Home Smart Meter for Power Distribution Network

**A Thesis**

**Submitted to the College of Engineering / University of Babylon in Partial Fulfillment of the Requirements for the Degree of Master in Engineering/ Electrical Engineering / Industrial Electronics**

**By**

**Farqad Mohammad Naser Ghalib**

**Supervised by:**

**Prof. Dr. Kasim Karam Abdalla**

**Assistant Prof. Dr. Shamam Alwash**

*2022 A.D.* *1444 A.H.*

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

إِنَّ رَبَّكُمُ اللَّهُ الَّذِي خَلَقَ السَّمَاوَاتِ وَالْأَرْضَ فِي سِتَّةِ أَيَّامٍ ثُمَّ اسْتَوَى عَلَى الْعَرْشِ يُغْشِي اللَّيْلَ النَّهَارَ يَطْلُبُهُ حَثِيثًا وَالشَّمْسَ وَالْقَمَرَ وَالنُّجُومَ مُسَخَّرَاتٍ بِأَمْرِهِ أَلَا لَهُ الْخَلْقُ وَالْأَمْرُ تَبَارَكَ اللَّهُ رَبُّ الْعَالَمِينَ

صدق الله العلي العظيم

الاعراف (٥٤)

# Examining committee certificate

We certify that we have read this thesis entitled **"Design and Implementation of Wireless Home Smart Meter for Power Distribution Network"** and as an examining committee, examined the student **Farqad Mohammad Naser Ghalib** in its content and that in our opinion it meets standard of a thesis for the degree of master in engineering/electrical engineering / Industrial Electronic .

Signature:
**Name: Prof. Dr.**
**Ibrahim A. Murdas**
(Chairman)
Date: / / 2022

Signature:
**Name: Asst. Prof. Dr.**
**Ahmed Q. ALdhahab**
(member)
Date: / / 2022

Signature:
**Name: Asst. Prof. Dr.**
**Moneer Ali Lilo**
(member)
Date: / / 2022

Signature:
**Name: Prof. Dr.**
**Kasim Karam Abdalla**
(supervisor)
Date: / / 2022

Signature:
**Name: Asst. Prof. Dr.**
**Shamam F. Alwash**
(supervisor)
Date: / / 2022

Signature:
**Name: Prof. Dr.**
**Hatem Hadi Obeid**
(Dean of College of Engineering)
Date: / /2022

# Supervisor certification

I certify that this thesis entitled **"Design and Implementation of Wireless Home Smart Meter for Power Distribution Network"** was prepared by **Farqad Mohammad Naser Ghalib** under my supervision at the department of electrical engineering, college of engineering, university of Babylon, as partial fulfillment of the requirements for the degree of master in engineering /electrical engineering /Industrial Electronic **.**

**Supervisors**

Signature :

**Name: Prof. Dr. Kasim Karam Abdalla**

Date: / /2022

Signature **:**

**Name: Asst. Prof .Dr. Shamam F. Alwash**

Date: / / 2022

In view of the above recommendation, I am forward this thesis for discussion by the Examination Committee .

**Head of Electrical Department**

Signature **:**

**Name: Asst. Prof .Dr. Shamam F. Alwash**

Date: / / 2022

# *Dedication*

*To*

*My support in life… my parents*

*My source of energy… my wife*

*My happiness in life … my children*

*My friends*

*I dedicate this work*

*Farqad*
*Sep. 2022*

# *Acknowledgment*

**In the name of Allah, Most Gracious, Most Merciful**

First and above all, I praise ALLAH, the almighty for providing me this opportunity and granting me the capability to proceed this thesis

I submit my highest appreciation to my thesis advisors, Prof. Dr. Kasim Karam Abdalla and Assistant Prof. Dr. Shamam Alwash, for their constant help, encouragement, guidance, patience and support through this research

I would like to thank my friends and colleagues for their assistance, collaboration and friendship. I also thank the faculty and staff of the Department of Electrical Engineering for their kind support

I am expressing my deepest gratitude to all those who gave me helpful hand through this study

**Finally**, I would like to express my deep gratitude to my family for their patience and endurance throughout my studies and for their continuous support, their love and encouragement enabled me to complete this work**.**

*Farqad*
*Sep. 2022*

# *Abstract*

Nowadays, the biggest challenge is to preserve electrical energy from the losses that occur as a result of technical losses (TLs) or non-technical losses (NTLs). The TLs are happened due to the energy dissipated in system equipment, whereas the NTLs are due to the two major problems, the electrical energy theft (EETh) problem, and the billing non-payment (BNP) problem.

The traditional system used to collect bills or detect electrical power thefts is done manually and entirely manpower-dependent, meaning that the consumers cannot be forced to pay the bills and most electrical power thefts cannot be detected. Therefore; the energy unit price (tariff) will rise for the consumer to cover these losses by the electrical energy companies which constitutes a heavy financial burden on the consumers.

As a result, the proposed system is designed and implemented to solve the NTLs problems to be a smart system has the ability to be a prepaid billing and energy theft detection system. On the other hand, the proposed system has the ability to locate the EETh weather was in consumer energy meter or at the feeder of transformer that supplied these consumers meters. The proposed system also can reduce the candidate area for energy theft testing by the specialist team from a large city containing hundreds of transformers feeder to a unique feeder and a small group of houses attached to that feeder.

The proposed system was designed and implemented practically by using simple components with low cost and few sensors compared with the other works and build a local network without depending on the internet or telecommunication companies.

The proposed system has been tested, calibrated and proven to be an accurate and highly efficient to achieve the required thesis aims.

# Table of Content

# List of Tables

# List of Figures

# List of Abbreviations

| Abbreviation | Definition |
|---|---|
| AC | Alternative Current |
| ADC | Analogue to Digital Converter |
| API | Application Programming Interface |
| AT | Application Transparent |
| BNP | Billing Non Payment |
| BLA | Block light LED Anode |
| BLK | Block light LED Cathode |
| CE | Coordinator Enable |
| CN | CONSUMER NODE |
| CSMA-CA | Carrier Sense Multiple Access Collision Avoidance |
| CT | Current Transformer |
| CU | Communication Unit |
| DH | Destination address /High part |
| DL | Destination address /Low part |
| DSN | Distributed Sensor Networks |
| DSP | Digital Signal Processing |
| E | Enable |
| ECG | Electro Cardio Gram |
| EEPROM | Electrically Erasable Programmable Read Only Memory |
| EETh | Electrical Energy Theft |
| EPROM | Electrically Programmable Read Only Memory |
| FPGA | Field Programmable Gate Array |
| ft | Foot |
| GHZ | Giga Hertz |
| GND | GROUNG |
| GPRS | General Pocket Radio Service |
| GPU | General Processing Unit |
| GSM | Global System Mobile |
| GUI | Graphical User Interface |
| I/O | Input / Output |
| ID | Identification number |
| IDE | Arduino Integrated Development Environment |
| IEEE | Institutes of Electrical and Electronic Engineers |
| IOT | Internet Of Thing |

| | |
|---|---|
| IQD | IRAQI DINAR |
| ISO | International Organization for Standardization |
| JV | Channel Verification |
| Kbps | Kilo Bit Per Second |
| KHz | Kilo Hertz |
| KWh | Kilo Watt Hour |
| LCD | Liquid Crystal Display |
| LED | Light emitting display |
| MAC | Medium Access Control |
| MCU | Microcontroller |
| MHZ | Mega Hertz |
| MISO | Master In Slave Out |
| MOSI | Master Out Slave In |
| MPU | Microprocessor Unit |
| NI | Node Identifier |
| NTLs | Non-Technical Losses |
| OSI | Open Systems Interconnection |
| PAN | Personal Area Network |
| PU | Processing Unit |
| RF | Radio Frequency |
| RFID | Radio Frequency Identification |
| ROM | Read Only Memory |
| Rx | Receiver |
| Rs | Register select |
| Rw | Read/ Write |
| SAR | Successive Approximation Converter |
| SD | Single Data |
| SM | Sleep mode |
| SDA | Serial data line |
| SCK | Serial clock |
| SMP | Sensor Management Protocol |
| SMS | Short Message Service |
| SMP | Sensor Management Protocol |
| SN | SERVER NODE |
| SO | Sleep Option |
| SoC | System on a Chip device |
| SP | Spent Sleeping |
| SPIN | sensor protocol for information via negotiation |

| | |
|---|---|
| SU | Sensing Unit |
| SWSN | Static Wireless Sensor Network |
| TLs | Technical Losses |
| TN | Transformer Node |
| Tx | Transmitter |
| Wi-Fi | Wireless Fidelity |
| WSN | Wireless Sensor Network |

# List of symbols

| Item | Description | unit |
|---|---|---|
| $t_o$ | Time interval | second |
| $V_s$ | step value | volt |
| $V_{p-p}$ | peak to peak voltage | volt |
| $2^m$ | quantization level | unitless |
| $m$ | number of levels | unitless |
| $\mathbf{I_T}$ | total consumers current | unitless |
| $n$ | number of consumers. | unitless |
| $I_i$ | current for consumer i | Ampere |
| $\mathbf{I_1}$ | Consumer node 1 current | Ampere |
| $\mathbf{I_2}$ | Consumer node 2 current | Ampere |
| $\mathbf{I_{TN}}$ | measured current at transformer node | Ampere |
| $\mathbf{I_T}$ | calculated total current consumed by consumer nodes CNs. | Ampere |
| $\boldsymbol{\alpha}$ | threshold value that represents the consumed currents | unitless |
| $A$ | mean average of consumer current. | unitless |
| $x_i$ | is the $i^{th}$ measured current value. | Ampere |
| $i$ | counter from first reading (1) to $n^{th}$ readings. | Ampere |
| $I_m$ | measured current value. | Ampere |
| $\boldsymbol{\mu}$ | threshold value for devices currents | unitless |

# Chapter One

# Introduction

# Chapter One

# Introduction

## 1.1 Overview

Power systems suffer from many losses. These losses pose serious economic problems to the electricity supply companies and the consumer. Power systems have two types of losses which are technical losses (TLs) and non-technical losses (NTLs) [1]. TLs represent energy dissipated in system components while NTLs are due to electrical energy theft and the non-payment of electrical energy bills. Annually, electrical power companies all over the world are losing about 89.3 billion U.S. dollars as NTLs [2]. Thus, the NTLs are considered as a financial onus on the electrical power companies, and due to that losses, these companies have added an extra costs to the electricity unit price (tariff) that have to pay by consumers [3]. Therefore, the main and important solutions to get rid of this onus is the solution of the problem of the bills non-payment (BNP), and the electrical energy theft (EETh) problem.

The electric power system is consisting of three parts which is the generation part, the transmission part and distribution part [4]. NTLs are appeared in the distribution part ( consumption part) since these two parts are next to utilities, the violation is easy to implement and inexpensive.

It is important to take these problems seriously by designing and implementing a smart system capable of solving the problems of NTLs with low-cost, high-efficiency. This system consists of several parts, the most important of which is the smart energy meter, which transmits the required data wirelessly through the ( Wireless Sensor Network) WSN between the parts of the system for the purpose of detecting theft as well as filling the meter without human intervention. Thus, the cost will fluctuate and the people's lives will save

from tampering with electricity. Here, the two main problems of non-technical losses will be highlighted.

### 1.1.1 Bills Non-Payment (BNP)

Electrical energy bills can be paid by using three payment methods which are manual payment, prepaid payment, and post-paid payment [5]. The manual payment is a traditional method of payment that relies on manpower. It seems to cost a lot of money to collect the data from electrical energy meters manually and enter them into the company billing system to issue bills. Thus, the salary of the required manpower is considered another burden to increase the tariff. Moreover, this method does not provide the ability to force the consumer to pay the electrical energy bills, and consequently it cannot contribute to reduce the problem of the BNP. On the other hand, the prepaid payment system has the ability to reduce the problem of the BNP by forcing the consumer to pay before energy consumptions, using a smart system. In this system, an energy meter is used to measure and display the electrical energy data which is periodically sent to the company accounts management system by using a bidirectional communication approach [6]. In the case of the post-paid payment method, a smart system similar to previous method is utilized. However, the payment is done after the energy is consumed within a certain period of time. Thus, the last two methods have advantages over the traditional method by reducing the required manpower and the problem of the BNP, consequently reducing electricity tariff.

Accordingly, most researchers focus on prepaid and post-paid payment methods which are feasible either by modifying the traditional system so that it includes an electromagnetic energy meter, or by implementing a smart system that includes an electronic energy meter. Moreover, the recent development of the electronic meter has brought these systems forward including the accuracy,

performance, ease of use, and compatibility with different communication approaches [7], which can be either wired or wireless. However, the wireless communication is better than the wired form due to the wire's issues like complexity, cost, and maintenance [8].

### 1.1.2 Electrical Energy Theft (EETh)

The economic progress of developing countries is closely related to the consumption of electric energy in terms of the large number of factories and industries, and consequently, the lack of this energy significantly affects the progress of these countries [9].

Nowadays, the biggest challenge is to preserve the electrical energy from the loss that occurs as a result of technical (TL) or non-technical losses (NTL) [10]. EETh is major part of the NTLs and can be defined as the process of obtaining electrical energy without paying any sums or paying small amounts much less than the amounts of the energy consumed. This process is done without the knowledge of the Ministry of Electricity or the owner company [11]. In short, it means the illegal consumption of electrical energy, regardless of the method of consumption [12]. Yearly, the EETh loss costs the electric power supply companies about £19 billion over the world [13]. As a result, the energy unit price (tariff) will rise for the consumer to cover this loss by the electrical energy companies.

In traditional meters or non-smart energy systems, the EETh is detected only by the company crews or by the meter reader staff. The process of checking the EETh is done manually by the specialist person via looking only and examining the wires which input and output to the meter only, whether there is a jumper operation for the meter or not. Therefore, it is not possible to detect many thefts that occur in this way, which require a lot of manpower and associated costs such as salaries, transportation, and others. Hence, it has become necessary

to build a smart system that doesn't rely on manpower and can detect and treat the EETh problem at the same time.

## 1.2 Literature Survey

Researchers have tried in various ways to address NTLs problems that negatively affect consumers. The following is a review of studies and research that attempted to solve the BNP problem and the EETh problem.

### 1.2.1 BNP Literature Review

Several researches have been developed for dealing with the BNP problem as the following.

**J.K. Mishra et al**.,**2018 [14]**, proposed a prepaid energy billing system based on a modified traditional electromechanical meter by using a light sensor that counts the number of LED flashes. Each 3200 flashes equal one consumption unit, and then the microcontroller handles that data. This method may not produce accurate readings due to inconsistent lighting circumstances in the surrounding environment. The communication between the consumer and the utility center is done by manpower only.

**P. Pramod Kumar** and **K. Sagar, 2020 [15]** developed a post-paid smart energy billing system based on implementing an electronic energy meter. The consumption readings in this system are directly updated to the server every minute by using GSM/SMS technology, which is a costly process but accurate.

**N. Mahfuz et al., 2020 [16]** suggested a smart energy meter that depends on GSM/SMS technology and avoided the large number of SMSs sent to the server by saving the consumption readings onto single data (SD) card, then send these data to the utility center by SMS which means depending on telecommunication companies policy.

**B.M. Waheib et al., 2021 [17]** introduced a smart energy meter by using two SIM cards, in transmitting and receiving parts depending on GSM technology. However, the consumer in this system is informed about all important details such as the value of the bill to be paid, and activation or

warning messages through an SMS received on cell phone or through a web page, which imply extra costs and more complexity. It is worth mentioning that the accuracy of energy billing systems based on GSM/SMS technology is subjected to the policy and service continuity of telecommunications companies.

**P.S. Vaidya et al., 2020, [18]** developed a Post-paid billing energy systems based on the Internet of Things (IOT). The energy consumption readings in these systems are sent to the cloud using Wi-Fi technology, while bills are emailed to the consumer.

**V.V. Gavhane et al., 2021 [19]** suggested a Post-paid billing energy systems based on the Internet of Things (IOT) by using Wi-Fi technology. The bills are displayed on the meter LCD. However, these system assumed that the internet service is available, which cannot be achieved for all consumers

**G. M. Jasim** and **K. K. Abdalla, 2021 [20]**, proposed a prepaid energy system based on the RFID and Wi-Fi technologies. The RFID technology in this system is used to recharge the energy meter while the Wi-Fi technology is used to transmit the consumption energy and the necessary information to the central unit. This is rather cost and hasn't the ability to coordinate in a network and high power consumption comparing with the proposed system.

**S.J Danbatta** and **A. Varol**., **2019 [21]** found that although the system avoided the problem of using the internet, it has many drawbacks due to the use of the Wi-Fi technology, such as high cost implementation and high power consumption in the nodes.

**S.S. Chowdary et al., 2020 [22]** suggested a new system by using IOT/Zigbee technologies. The consumption data is collected from meters via Zigbee technology and sent to the cloud via Wi-Fi technology. However, internet availability is still required. The main drawbacks of this system is still using Wi-Fi technology which means high power consumption and also the internet, while the proposed system depends on Zigbee technology only which is low power consumption and without depending on the internet.

On the other hand, there are several methods developed for recharging the energy meter balance.

**K.N. Shaikh** and **I. Mustafa., 2021 [23]** proposed two methods to recharge the energy meter balance. The first method is using the RFID card, while the recharging can be done in second method by sending a scratched card number to the utility center through SMS and check the validity of that card to recharge the energy meter.

**D. Zangmo et al., 2020** [24], suggested two methods for meter recharging. The first one uses a recharging card via SMS to check its validity. The second method is online recharging, which deals with a bank online to send out a notification to the utility center to recharge the meter.

### 1.2.2 EETh Literature Review

Several researchers have attempted to solve the EETh problem by proposing an smart system using several techniques that try to find out when and where the energy theft occurred, and some went so far as to find out how much energy was stolen.

**A. Bin Halabi et al., 2019** [25] Introduce a smart system that compares the measured transformer power supplied to consumers with the consumed power measured by consumer power meters using a specific algorithm. If there is a difference between the two measurements, it means that it is a case of theft. In this case, the utility center will shut down a consumer meter once a time to check the different states and so on to find the illegal consumer. Therefore, by using this algorithm the system can detect whether the EETh is at the consumer meter or in the distribution line. In this system, wired communication is used here with lab conditions only. Furthermore, the regular consumer is extinguished to identify the thief, and this is sometimes unacceptable.

**N.K. Mucheli et al., 2019 [26]** imposed a method based on the comparison between the supplied current and the actual current for each

consumer. A distribution box has been placed on certain poles to distribute the electrical energy through this box to the consumers' meters, where a current sensor is placed for each consumer in the distribution box. Moreover, another current sensor is placed at each consumer meter. This method is also assumed to take the coordinates of each distribution box as well as for each consumer's meter when it is installed for the first time by using GSM/GPRS technology and stored in a database. However, if there is a difference between the currents at the two sensors, that means it is a theft state and will inform the utility center by the saved location of the illegal consumer. The use of many sensors means additional cost, maintenance, and complexity. In addition, the communication between the system is done by GSM technology. The proposed system uses much less sensors which mean low cost and doesn't depending on GSM technology.

**J.Y. Kim et al**., **2019 [27]** imposed a method to divide the electrical distribution networks into smaller and independent networks to monitor the flow of energy by installing a middle system monitoring meters for each network that calculates the electrical energy supplied to each independent network and detects theft that occurs. An algorithm has been found to detect these thefts. Using a lot of middle meters added an extra cost to the system.

**M.B. Shahid et al., 2019 [28]** developed a smart energy theft detection system based on a machine learning technique that depends on consumer load profile (that contains the consumer meter data). In the case of theft detection, each consumer's consumption is compared to its load profile, if there is a certain difference above the threshold level, the illegal consumer is identified by its ID. On the other hand, if it turns out that all consumers are legal, that means the theft is in the distribution line. So, all the legal consumers have forced shutdown and the high voltage will be injected into the distribution line as a penalty to the illegal one by changing the transformer tap changer. This method is rather risky.

**W.Li. Longintheran., 2019 [29]** used the machine learning method to solve the EETh problem which means create a data base according to consumer consumption and expect the energy consumption behavior. After that, compare the consumed energy that expected with the true consumption to know the theft. Unfortunately, this methods are considered a virtual study, in addition, it is a rather complex method.

**R. Punmiya** and **S. Choe, 2019 [30]** used the gradient boosting method as a machine learning to detect energy theft. This method is considered a weak classifier that depends on a decision tree which is un similar to the random forest method which deals with many classifiers.

**J. Tao** and **G. Michailidis, 2019 [31]** developed statistical techniques that solve the problem of theft if the meter data is changed so that the thief can reduce his power consumption data and add the difference to the power consumption data of other consumers. Such thefts are difficult to detect because they conserve the same amount of power supplied in distribution transformers when compared to the power consumed by customers, so the only victim of this problem is the legal consumers.

**M. Uvais , 2020 [32]** imposes a mathematical model with simulation to determine the EETh at the distribution line only by comparing the supplying current for all consumers with the summation of the consumers' actual currents. Then, by calculating the line's impedance in case of theft, the length of the theft distance from the distribution transformer can be determined. This study has not been applied in practice.

Due to the development in smart energy meters, the methods of stealing electrical energy have also evolved from traditional thefts, as in the previous methods, to more complex methods by targeting electrical energy consumption data.

**S.O. Tehrani et al.,2020 [33]** demonstrated the new classification of energy theft can be categorized into two types. The first type is physical energy theft by

tampering with meters or distribution lines and the second type is energy theft by cyber and data attacks by changing the measured data and tampering with the programs of smart meters or communication links.

As previewed before most researchers found a suitable solution to detect the EETh in distribution line and others found a solution to detect EETh at consumer meter but with high cost and depending on the internet or telecommunication companies.

## 1.3 Problem Statement

The legal consumer loses a lot of money because of the high energy unit price (tariff), which covers the losses of electricity companies due to the theft of electric energy and the non-payment of bills by most consumers. As a result, the need has arisen to find an smart system that handles these losses**.** The following are most of the problems that were dealt with in the event of non-payment of bills or theft of electrical energy.

### 1.3.1 BNP Problem Statement

The bill non-payment (BNP) problem of the electric energy system is one of the important non-technical losses (NTL) problems that must be taken into consideration, which occurs as a result of the traditional collection system followed in most countries which has the following drawbacks:

- The traditional system depends on the manpower to read and collect the consumption of electrical energy, and record and send them on paper to the main center to the extent of billing each consumer separately.
- The traditional process is manually done which means it costs a lot and wastes time.
- It is also a non-accurate system which leads to many errors occurring either because of the workers themselves or the absence of most consumers near their meters when the meter reader comes. That leads to

recording false consumption readings that negatively affected either the company or the consumer.

- In the traditional system, there is no possibility of forcing the consumer to pay the electrical energy bills. Moreover, it can communicate with the utility center through manpower only.

As a result, researchers have tried to solve the (BNP) problem by using a variety of methods. All these methods examine three mechanisms for building a billing system. The first mechanism is how to collect the energy consumption of the consumer's meter. The second is how to communicate between the consumer meter and the server, and the last is how to fill the meter with the balance to be either prepaid or postpaid payment.

However, most of these researches have many drawbacks such as high-cost implementation, assuming the Internet is available to all users as well as working under the terms of the communication companies.

### 1.3.2 EETh Problem Statement

The EETh problem is considered also one of the important NTLs at electrical energy system which must be solved for many reasons:

- The EETh is dangerous and deadly to humans
- The EETh generates fires resulting from the tampering that takes place and thus causes huge human and material losses
- The EETh directly affects the balance of electrical loads in the electrical system, which negatively affects the performance of the electrical power system
- EETh incurs electricity companies heavy losses, which leads to a rise in the tariff price for consumers to offset these losses.

### 1.4 Thesis Objective

This thesis has two main objectives :

1. Finding a solution of the BNP problem by design and implement a smart energy billing system with low cost, high performance and accuracy able to achieve enforcing the consumer to pay based on new utilized smart meter.

2. Finding a solution to the EETh problem by designing and implementing a smart theft detection system with low cost, high performance and to find a solution for EETh problem based on detecting the location and the power amount that theft. In addition, enhance the accuracy of the developed system with reduced cost compared with other works.

## 1.5 Thesis Organization

This thesis offers the proposed system for design and implementation a smart system that dealing with the distribution lines losses, especially the NTLs as (BNP) problem and (EETh) problem by using the Wireless Sensor Networks (WSNs) as communication system. This thesis contains five chapters as following:

- Chapter One includes the overview of the NTLs in distribution system, both of the BNP problem and the EETh problem, the literature review for the two NTLs problems, the problem statement, the thesis objectives, and the thesis organization.
- Chapter two demonstrates the theoretical concepts that associated with the energy, the communication systems, the smart meter via the traditional meter, and sensing concepts.

- Chapter three includes the proposed system design and implementation with configuring the WSNs element and demonstrate the system operation. It is also show the GUI Interfacing.
- Chapter four displays the obtaining results and compare these results with another standard meter as calibration in BNP state, also the results for the EETh state.
- Chapter five shows the conclusion and the future work that can add a good development for both the NTLs problems.

# Chapter Two

# Theoretical Concepts

# Chapter Two

# Theoretical Concepts

## 2.1 Introduction

The electricity sector suffers from many problems as a result of NTLs represented in the electrical energy theft (EETh) problem, as well as the problem of the bills non-payment (BNP) problem. In this chapter, the most important techniques that used in the desired system are reviewed, as well as the reasons for choosing these techniques over others.

In this chapter, two parts have been discussed, the first part is the electrical power and energy. Limp a little on the smart meter and its advantages over the traditional meter in terms of the possibility of paying electric energy consumption bills, as well as the possibility of detecting electrical energy theft. The second part is the communication system that used with the energy consumption and how to communicate to send these energies values to the utility center to deal with them.

## 2.2 Electric Power and Energy

The Electrical power is defined as the rate at which energy is received or delivered from one circuit to another circuit [34]. In mathematical expression power is :

$$\boldsymbol{P = dw/dt} \tag{2.1}$$

The electrical power can be written as

$$\boldsymbol{P = \frac{w}{t}} \tag{2.2}$$

where : $P$ is the power and its unit is Joules per second(J/sec ) or Watt (W)

$w$ is the energy in Joules.

$t$ is the time in seconds.

The Energy can be defined as the capacity to do work as the following equation

$$\boldsymbol{w = \int_{t_o}^{t} P dt} \tag{2.3}$$

where $t_o - t$ is the time interval

The energy that supplied to the consumers is rated the term of kilowatt hour (KWh). One kWh can be defined as the electrical power of 1 KW consumed in an 1 hour, as the following expressed

$$\boldsymbol{E = P * t} \tag{2.4}$$

where: $E$ is the electrical energy ( KWh),

$P$ is the power (KW),

and $t$ is the time in ( hour ).

## 2.3 Energy Measurements

The electric energy meter is the equipment that count and display the consumed electrical energy [35]. Two types of energy meters are there, the traditional energy meter and the digital energy meter.

### 2.3.1 Traditional Electrical Energy Meter

It is also called the conventional or electromechanical energy meter which has been used since 19$^{th}$ century. It simply consists of rotating disk made of copper or aluminum attached to clock mechanism through a gear mechanism and a display as shown in Figure 2.1.

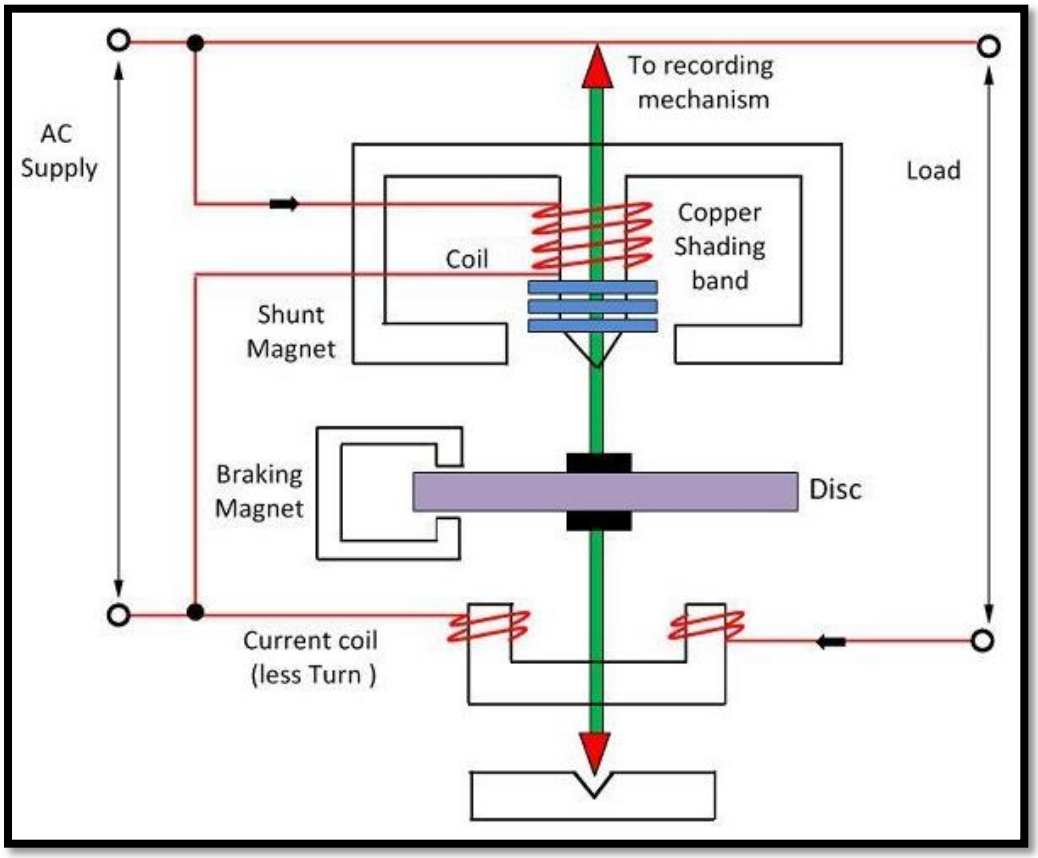



Fig. 2.1 Single phase electromechanical meter

### 2.3.2 Digital Energy Meter

It is an electronic device that depends on electronic sensors ( current sensor, voltage sensor) to calculate the electrical energy consumption by using a microcontroller, then display the consumption on the meter display as shown in the block diagram at Figure 2.2.

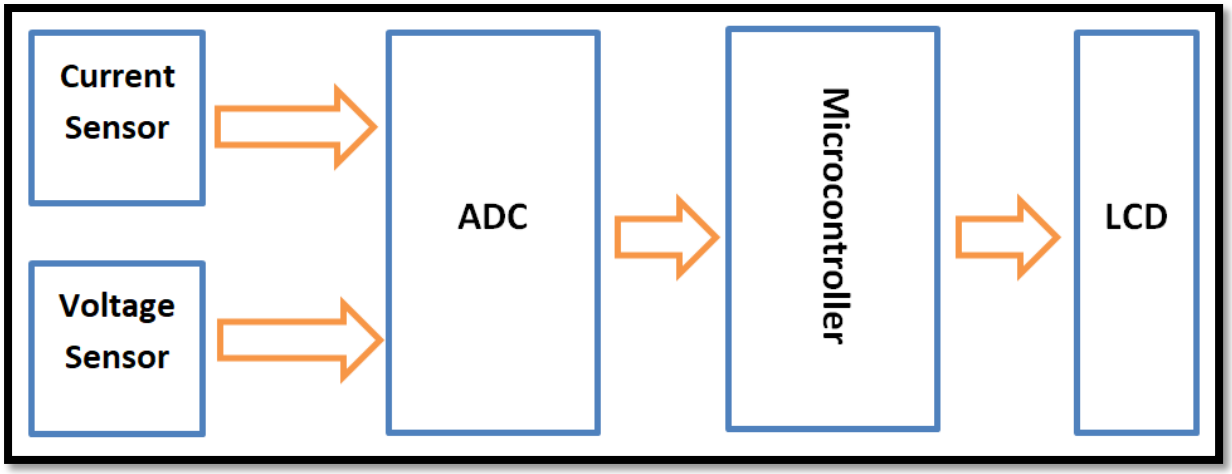



Fig. 2.2 Block diagram of digital energy meter

### 2.3.3 Smart Meter Motivation

In conventional meter the process of energy payment and communication totally depends on man power. In other words, the manual payment and manual communication is used in these meters. It seems to cost a lot of money to collect the data from electrical energy meters manually by human and enter them into the company billing system to issue bills. Also, most of the time, inaccurate readings by the relevant employee. Thus, the salary of the required manpower is considered another burden to increase the consumption unit price (tariff).

Moreover, this meter does not provide the ability to force the consumer to pay the electrical energy bills, and consequently it cannot contribute to reduce the first problem of the Non-Technical Losses (NTLs) in distribution systems, the Bills Non Payment( BNP) problem. On the other hand, the traditional meter, doesn't detect and solve the second problem of the NTLs which is the Electrical Energy Theft problem (EETh).

The invention of the electronic or digital meter greatly contributed to the construction of the smart meter. The smart meter has the ability to do many things such as:

- communicate in bidirectional way
- be an electronic prepaid or postpaid energy payment
- change the tariff automatically
- Work automatically without human intervention
- Can be Full control with consuming load

## 2.4 Communication System

In the late ninth century, the language of communication between people developed greatly when electricity was invented and then the telegraph, telephone and radio were invented [36] which greatly contribute in electronic communication. The electronic communication leads to share information between people in easy and reliable way. As known any communication system consists of three parts, the transmitter which send the specific information via the channel or medium, and then the receiver which pick up that information and dealing with it as shown in Figure 2.3.

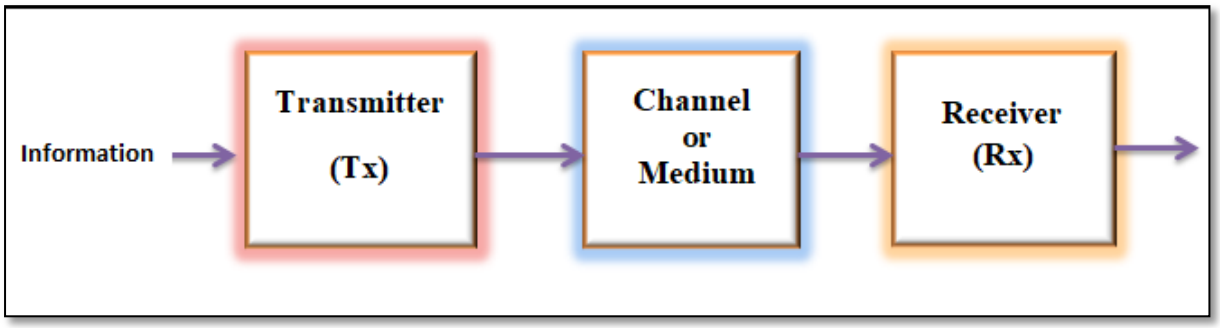



Fig. 2.3 Communication system

Communication system can be categorized to wire communication such as optical fiber, coaxial cable, twisted pair, etc. and wireless communication. Due to many wired communication problems such as high maintenance and high cost due to long distances, researchers have preferred to use wireless communication.

One of the most advantages in wireless communication is that no need for physical wires to communicate. In Smart system, there are many technologies to transmit and receive the required data wirelessly through the WSN.

## 2.5 Wireless Sensor Network ( WSN ) Concept

The WSN is a group of nodes including sensors that organized in wireless communication network. These nodes are small size, low power, low cost and have the ability to communicate, coordinate and cooperate to achieve the

requirement application [37] and due to the fixed location of the nodes sometimes referred to WSNs as Static Wireless Sensor Network (SWSN) [38].

As is known, the requirements of military defense are always an important motive for the study of many systems and the conduct of many types of research that serve these requirements.

The WSNs have been developed during the beginning of Cold War when there was a need to develop a system of acoustic sensors at the bottom of the seas and oceans capable of tracking Russian submarines. However, recent studies began in the 1980s with work on Distributed Sensor Networks (DSN), which contributed significantly to the development of WSN systems [39].

The importance of a WSN becomes clear when there is a certain environment that cannot be accessed by a human being, in which intervention in it poses a danger for life or in a place that is difficult to reach in many medical, military, technological and other fields. It is highly expected that in the future the WSNs will be an integral part as well as a necessary aspect of human life and all indications confirm that [37].

The WSNs are directly linked to the physical phenomenon that turns it directly into an understandable language that can be dealt with and the various systems can be managed through it [40].

### 2.5.1 WSNs Parts

WSN is mainly consists of two parts, the nodes and the wireless communication protocol.

**1) WSN Node**

Each node consists of three parts, as shown in Figure 2.4. The sensing unit which senses the physical circumstances, the processing unit which process the sensing data, the communication unit that transmit and receive the processing data wirelessly. It contains a power source as a battery or solar cell, etc. [41].

The sensing unit is consisting of a sensor and Analog to Digital Converter (ADC) that generates a digital signal from analog signal. While the processing unit is consisting of a microcontroller and memory to control the process. The communication unit which consists of the transceiver has the ability to transmit and receive the required data [42].

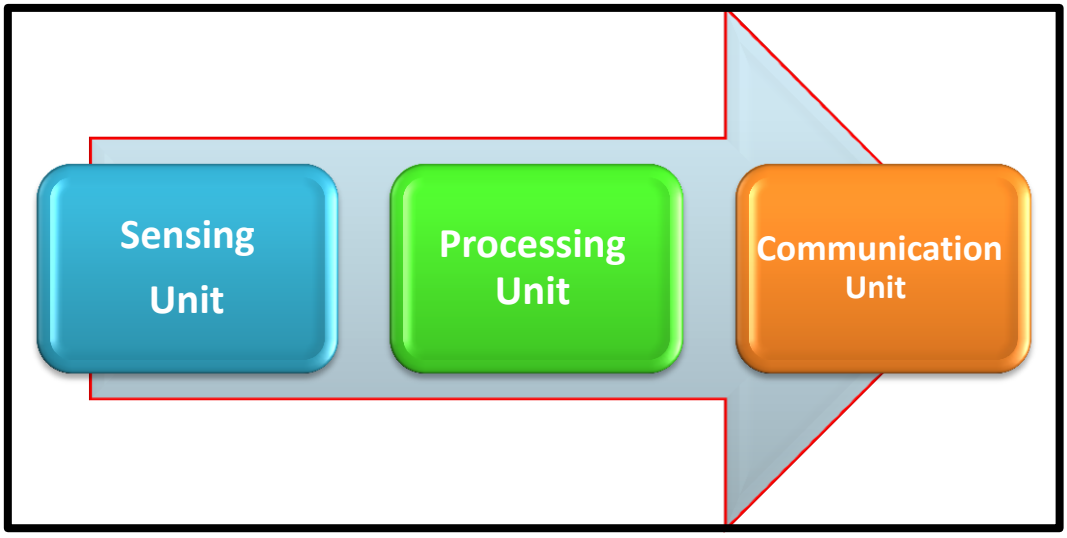



Fig. 2.4 WSN node

**a) Sensing Unit (SU)**

The sensing unit responsible for detecting the physical environment through the sensor and changing it to a digital signal through the analog to digital converter (ADC).

**i. Sensors**

The sensor technology supports daily human life in many fields to make it more easier and convenient. The sensor can be denoted as a device that can detect the changes in the physical environment and translate these changes into a suitable reaction such as electrical signals. These changes include movement, temperature, humidity, mass, weight, light, motion, pressure, and many more. There are many applications that depend on sensor technologies such as medical applications as health care, fitness, etc. and military applications as radars or others, in addition to all industries where sensor technologies are used. Figure 2.5 illustrate the sensor's operation.

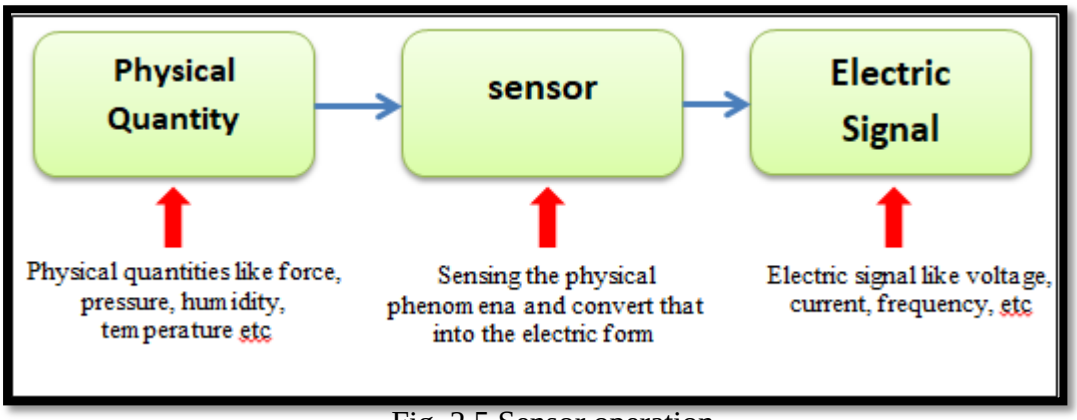



Fig. 2.5 Sensor operation

Many researchers have classified sensors into several categories, depending on the type, or the need for an external power source, or how they operate. Some of researchers classify the sensors into two groups, the active sensors and the passive sensors [43]. The active sensors require an external power signal or excitation to operate and produce the wanted response, while the passive sensors doesn't need any external exciting signal to operate. Another classification is used, the analogue and digital sensors according to their mission such as the electromechanical sensors, the location sensors, energy sensor, etc.[44]

**ii. Analog to Digital Converter (ADC)**

Most physical changes in nature give analog values, temperature, pressure or weight and therefore their values are many and not easy to deal with.

The ADC has the ability to convert an input analog signal into digital signal that is easy to deal by the processing unit [45] as shown in Figure 2.6.

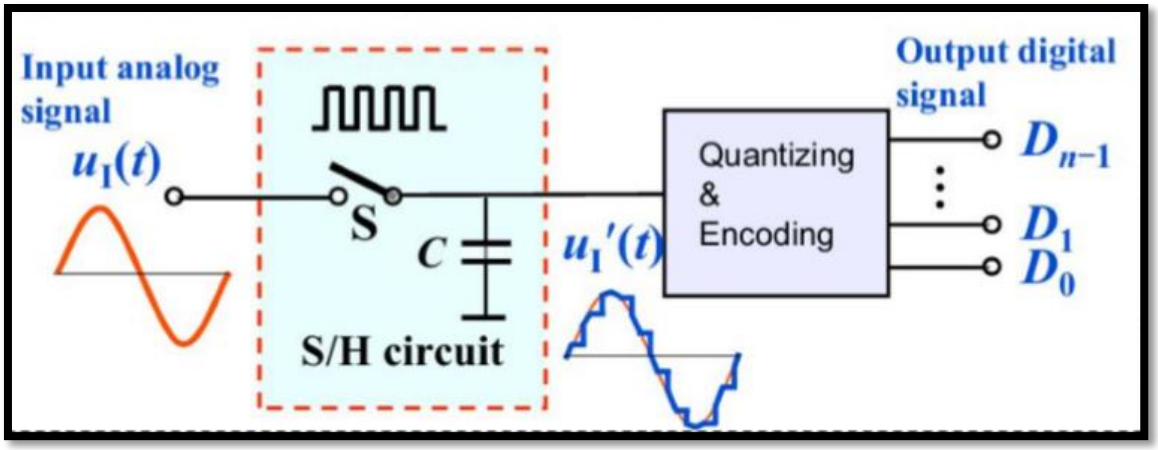



Fig. 2.6 ADC principle [46]

There are many types of ADC according to the purposed and the required system such as flash, pipeline, counter type, successive approximation converter (SAR) [46].

The accuracy of the ADC can be improved by increasing the resolution and increasing the sampling rate that lead to increase the maximum frequency as shown in Figure 2.7.

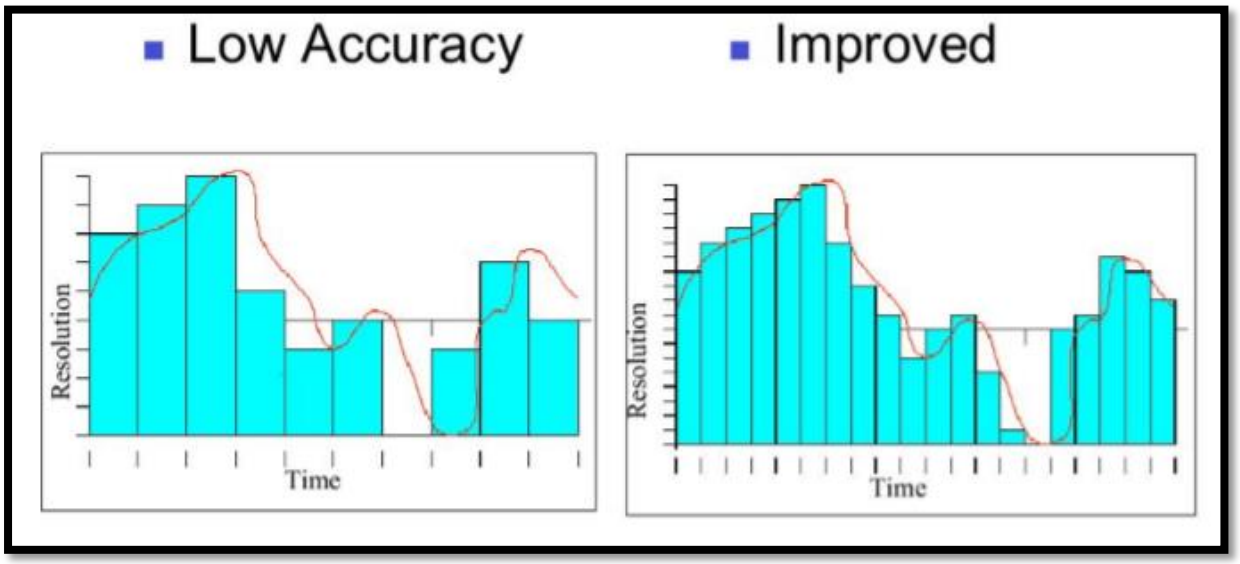



Fig. 2.7 ADC accuracy improvement[46]

The ADC resolution can be illustrated as equation 2.5 [47]

$$V_s = \frac{V_{p-p}}{2^m} \quad (2.5)$$

where: $V_s$ is step value in volt ,

$V_{p-p}$ is peak to peak voltage in volt,

$2^m$ is the quantization level, and $m$ is the number of levels.

**b) Processing Unit (PU)**

The main part of the processing unit is the microprocessor which may be a microcontroller unit (MCU), general processing unit (GPU), digital signal processor (DSP), field programmable gate array (FPGA) or system on a chip device (SoC) [48]. The purposes of choosing the MCU over the others is the

low power consumption, low cost, easy compatible with other devices, and small size. All this features is suitable for the WSNs. Moreover, the easy programming with C or C++ language add a good advantage for using the MCU.

- **Microcontroller (MCU)**

The MCU is a small computer has inputs and outputs (I/O) ports to connect all the necessary external devices such as sensors, transceivers, LCDs, etc. The MCU works as a brain for human and does all the required computation and coordinates all the external components works. It is an integrated circuit that has the following parts as shown in Figure 2.8

- Microprocessor Unit (MPU)
- Memory for data storage for instruction code
- I/O ports
- Timer
- ADC
- Serial I/O

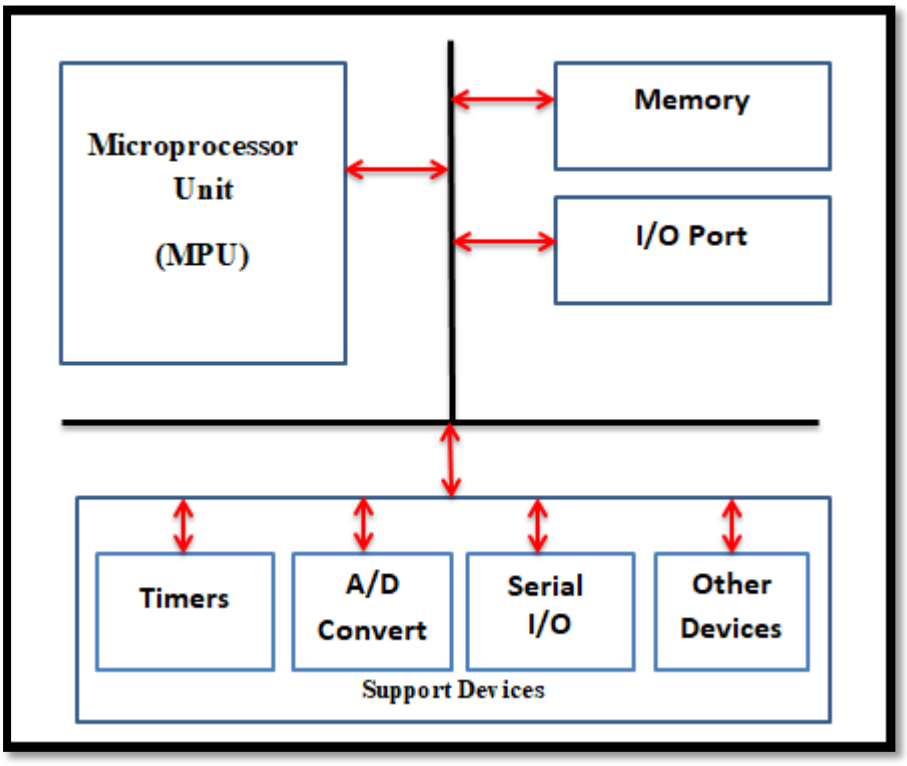



Fig. 2.8 MCU parts

**c) Communication Unit (CU)**

Communication unit consists of the wireless transceiver and the antenna which is used to transmit and receive required data depending on the (PU). The CU is managed by PU in case of turning on or off to keep the power consumption.

**i) Transceiver**

In most communication circuits, the system needs to transmit and receive data in a bidirectional manner, and that need a transmitter device and the receiver device and this is achieved by one device called the transceiver [49].

**ii) Antenna**

The antenna It is the mediator between the transmitter and the free space on the one hand, and between the free space and the receiver on the other hand [36].

## 2) WSN protocol

The International Organization for Standardization (ISO) distinguishes the inner functions of a communication system by separating it into abstraction layers in an imaginary model called Open Systems Interconnection (OSI).

The WSNs communication protocol should save the life of the sensor network as well as achieve low power consumption. The WSNs protocols contains the following layers [50, 51] and shown in Figure 2.9:

**a) Physical Layer**

This layer is responsible for saving the life time of sensor node by reducing power consumption

**b) Data Link Layer**

This layer is responsible for a Well Designed Medium Access Control (MAC) protocol. The MAC protocol have to adjust with network topology in case of node failure.

**c) Network Layer**

The mission of this layer is verifying that only the active nodes which receives data will consume the battery power by using the sensor protocol for information via negotiation (SPIN). The SPIN protocol will block the unwanted data and reduces the power consumption. This layer is responsible for network security, network structure, and network routing.

**d) Transport Layer**

This layer is responsible for founding a packets loss retrieval technique

**e) Application Layer**

This layer is responsible for sensor node movement, also turning it on and off and monitors the data collection rules based on the software operation system introduced by the Sensor Management Protocol (SMP).

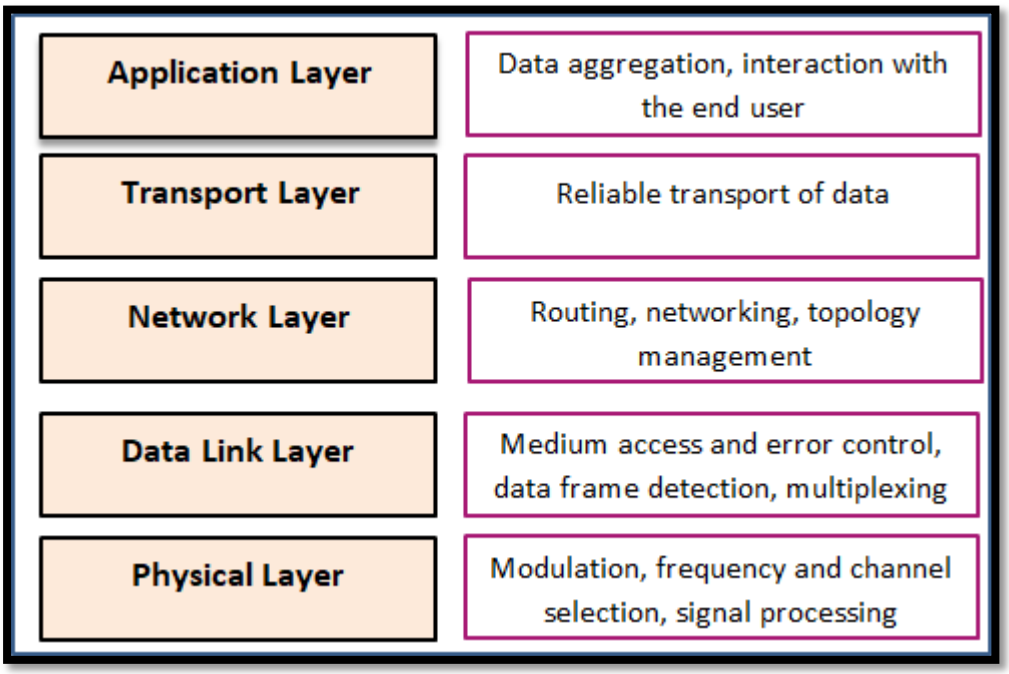
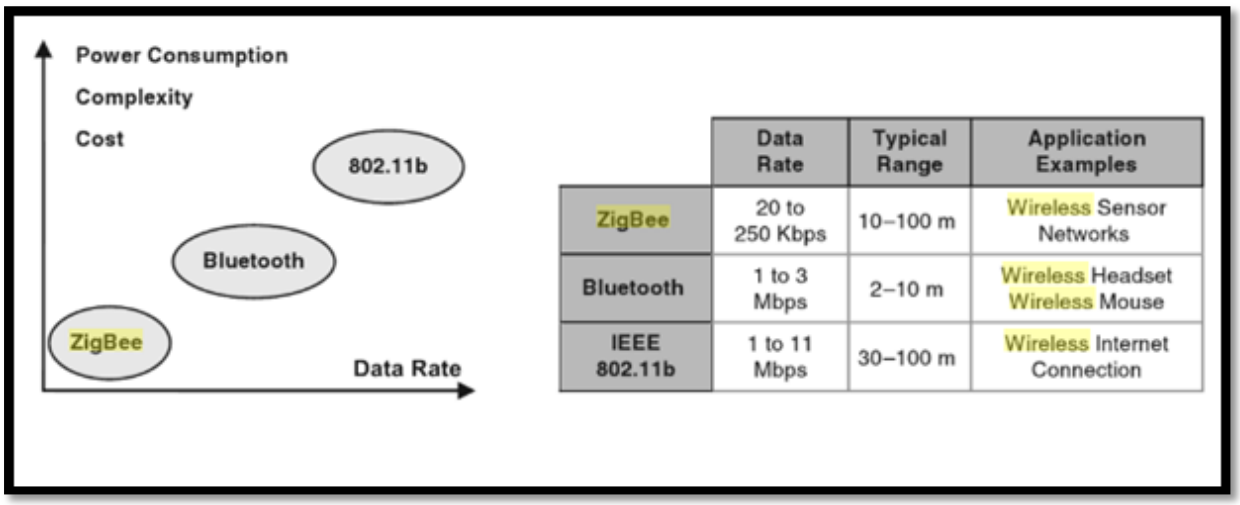



Fig. 2.9 WSNs protocol layers

### 2.5.2 WSN Features

- Low power consumption
- Low data rate
- High reliability
- Low cost
- Application of sensing
- Ability to self-organized

Recently, a lot of wireless communication standard protocol have been developed such as Wi-Fi, Zigbee, Bluetooth, etc. [52]. Figure 2.10 shows a simple comparison between these technologies, and as shown in the figure, it turns out that Zigbee is one of the best technologies in WSN, because it is a low power consumption, low cost, less complexity, and low data rate and that is very important in the WSNs [53].




| | Data Rate | Typical Range | Application Examples |
|---|---|---|---|
| ZigBee | 20 to 250 Kbps | 10–100 m | Wireless Sensor Networks |
| Bluetooth | 1 to 3 Mbps | 2–10 m | Wireless Headset Wireless Mouse |
| IEEE 802.11b | 1 to 11 Mbps | 30–100 m | Wireless Internet Connection |

Fig. 2.10 Comparison between Zigbee, Bluetooth, and 802.11b [53]

### 2.5.3 WSNs Application

The WSN is one of the most important studies that has contributed very effectively in all life fields. As shown in Figure 2.11, these applications can be summarized to main six categories as following [54] :

- **Military Fields** : such as battlefield observation, enemy detection, monitor the movements of the enemy's fighting trucks, tanks, missiles, aircraft, and others.
- **Health Care Application and Medical Services** : such as monitoring the electrocardiogram (ECG) for the patient, or any medical conditions sensors that indicates the vital signs for human can be placed to monitor it continuously
- **Environment Fields** : such as air, water, wind, gas, etc. monitoring , and emergency where it is possible to avoid natural disasters such as earthquakes, volcanoes, forest fires or tsunamis, or reduce their risks by monitoring their activity through WSNs.
- **Urban Fields** : which means smart cities, smart home, the transportation system, monitor the bearing of buildings, bridges, traffic jam monitoring, etc.
- **Plants and Animals application**: WSNs are very important in the fields of agriculture and livestock development in terms of creating the appropriate conditions for their upbringing and constantly monitoring these conditions.

- **Industrial Fields :** The WSNs intervenes in all areas of industry in terms of monitoring machines, organizing their work, giving important notifications about the work of systems, enabling the observer to know their malfunctions, as well as providing logistical support. It is worth noting the importance of WSN occur in various industries, such as gas and oil leaks, or nuclear site problems, in addition to voltage problems, etc.

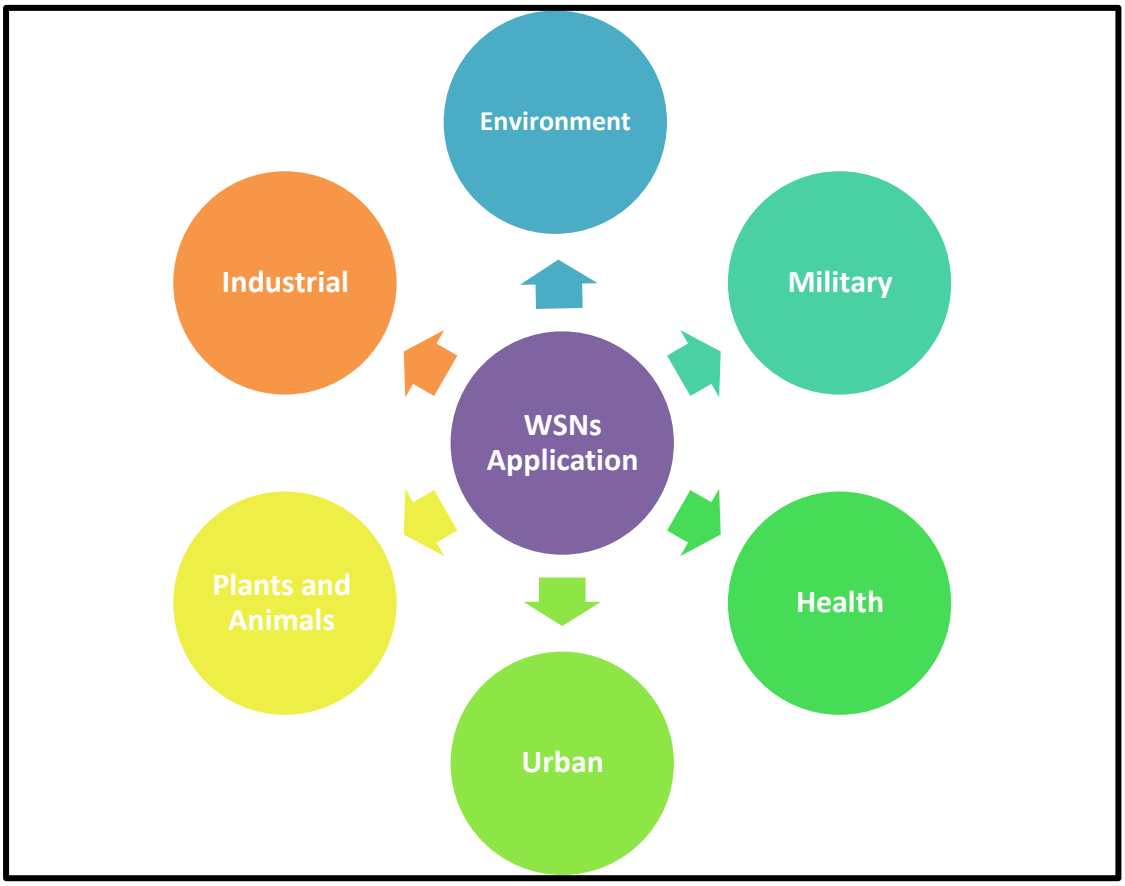



Fig. 2.11 WSNs application

## 2.6 Zigbee Technology

Zigbee technology is one of the most important WSNs technology which belongs to wireless personal area networks (PAN) that uses the standard of IEEE 802.15.4. [55]. It is used for transmitting and receiving data wirelessly through a certain specifications. The name Zigbee was created according to the method of flight of bees which is usually flying in a zigzag path in search of flower nectar and transmit information about food locations and directions to the rest of the hive, hence the name Zigbee is come from. Then the name Zigbee is given to this technique by Institutes of Electrical and Electronic Engineers (IEEE) [56].

Zigbee technology was designed for providing the following features [57] :

- low power consumption, which positively affects the long battery life.
- Reliable and self-healing
- advance encryption

- secure system
- high accuracy
- simple protocol
- low data rate
- low cost.
- Global implementation

Zigbee was initially designed for commercial, industrial, monitoring and controlling purposes and developed to be a high level WSNs.

Zigbee technology uses the Carrier Sense Multiple Access Collision Avoidance ( CSMA-CA) to increase the reliability by regulating the times of sending and receiving information in order to avoid obtaining corrupt data. That mechanism has the ability to ensure that the channel is not busy for transmitting and receiving data, exactly when someone is waiting for his turn in talking.

Moreover, the Zigbee technology uses the 16 bit (cyclic redundancy check codes) CRC for each packet (which is a number of bits that transmitted with each other with a certain format) to ensure the data bit is correct [58].

Three operating frequency bands are used at IEEE 802.15.4 with 27 radio channels. These bands are 868MHz, 915MHz, and 2.4GHz as shown in Figure 2.12. Channel 0 at a frequency of 868.0 or 868.6MHz, provides a data rate of 20 kbps. Channels 1 to 10 operate at a frequency of 902.0 to 928.0 MHz and each channel provides a data rate of 40 kbps. Channels 11 to 26 are located in the frequency 2.4 or 2.4835 GHz and each channel provides a data rate of 250 kbps [59].

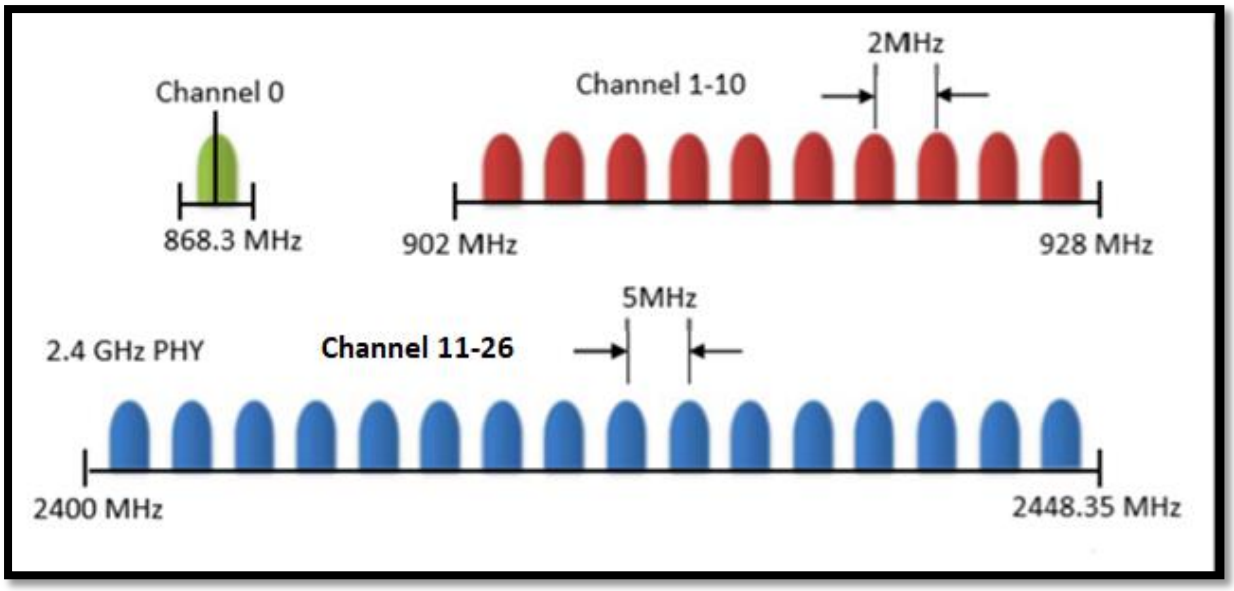



Fig. 2.12 Operating frequency [59]

### 2.6.1 Zigbee Devices

Depending on the task of Zigbee standard has three types of devices, the Coordinator, the Router, and the End device [60]. Each one of these devices has a different setup and different mission as the following :

1) **Coordinator (C):**

It is the device responsible for starting the network and is considered the kernel of the Zigbee network, which has only one coordinator. Each network should be managed by one coordinator [61]. A coordinator is like a portal with the outside world and it is responsible for many things :

- Configuring and initiating the network.
- Choosing an unused channel to operate the network (unique PAN ID).
- Determining the security policy for the network.
- Creating a profile for the network.
- Allocating the address to enable the routers and the end devices to join the network.
- Selecting a route for data packet.
- Communicating with all the network devices.

2) **Router (R):**

A Router is perfect node which is considered the link between the parts of the network, in other words, it is intermediate node and transfers the readings of the sensors in the nodes to the coordinator and also transfers the orders from coordinator to these nodes [53]. When the router joins the Zigbee network, it stills connect to the same PAN ID and on the same channel until forced to leave.

The router is responsible for transmitting and receiving information from the coordinator to the user (end device) and vice versa, and stating whether or not it has been received [62]. The router has the following features :

- secures the transmission and receiving information between far nodes and the coordinator.
- Must powered on all the time
- Can rout the information in the network
- Allow the new devices to join the network with specific setting.
- Might have many routers according to the network topology.

**3) End- Device (E):**

It is the device that responsible for collecting diverse information from sensors and send it to the parents ( coordinator or router). This device has the following features :

- Can send and receive information.
- Can save power consumption by entering the sleep mode while not active and therefore long battery life.
- Needs the parents either the coordinator or the router to communicate.

### 2.6.2 Zigbee Network Topology

Three types of networks are depended in Zigbee technology, star, cluster tree, and mesh topologies [61]. The number of routers and end devices rely on the network topology [63].

#### 1) Star Network Topology

In this topology, the nodes communicate directly with the coordinator as shown in Figure 2.13 . It consists of one coordinator and a lot of end device and there isn't any router device. Each end device is physically separate from the other end device and cannot communicate between them. It is the simplest and the most limited network [61].

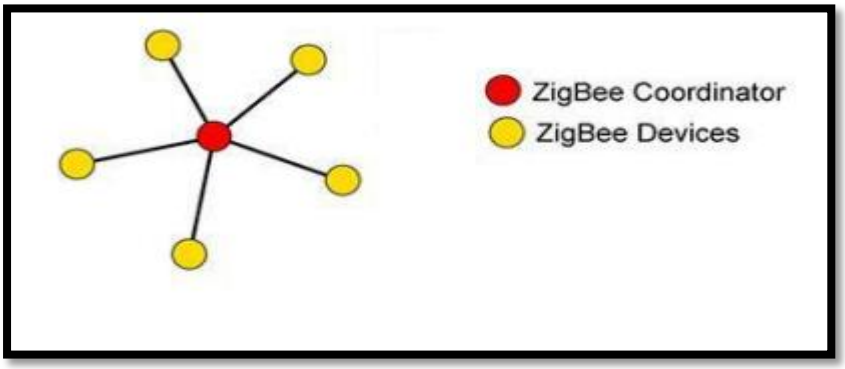



Fig. 2.13 Star network [61]

#### 2) Cluster Tree Network Topology

The coordinator like the root of the tree, end device can directly connect with the coordinator or across the router as shown in Figure 2.14. It is more reliable than the star topology because of the multipath to coordinator.

The network operates in a hierarchical fashion, the source nodes must pass messages to their parents (the first node above the source node) which then relays their messages up the tree until they reach the coordinator or until they reach a router that can forward the message down the tree to the intended target

destination. One of the disadvantages of this topology is that if the router fails for any reason, the end device will not be able to deliver the information, in other words lost the data [61].

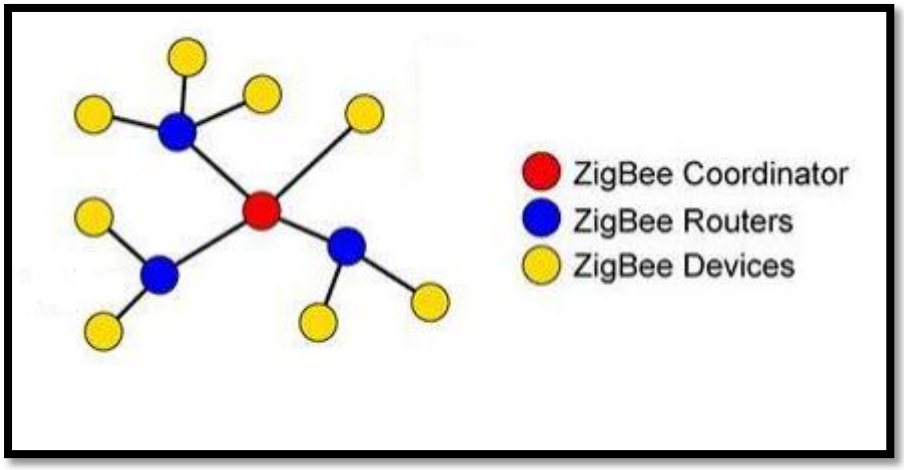



Fig.2.14 Cluster tree network [61]

### 3) Mesh Network Topology

Mesh network also called peer to peer network [64]. It is the most reliable network in Zigbee network topologies. The mesh network architecture provides multiple paths for messages within the network; which makes room for more flexibility from other topologies. If a particular router fails, the network can rebuild an alternate route through another network routers. Each node can connected with other close node and cooperate to transfer the data to the coordinator or across the router [61].

If any router stop suddenly or fail to operate, the coordinator will rebuild another path for the nodes. This network has one coordinator and a lot of routers and end devices as shown in Figure 2.15.

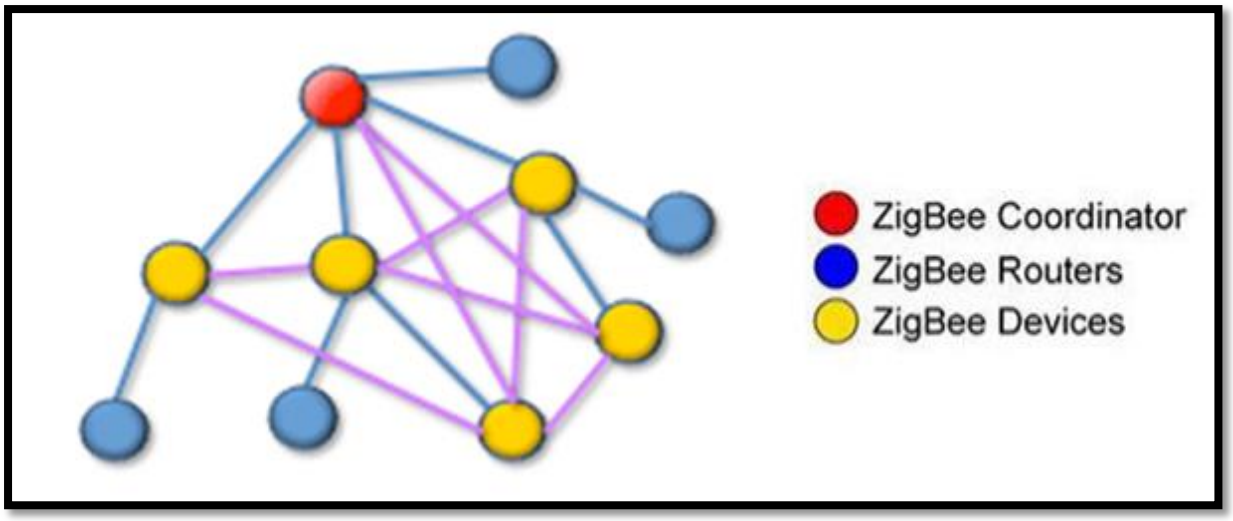



Fig.2.15 Mesh network

In mesh networking, since many nodes are there in the mesh network that can pass on the data, it doesn't matter the distance between two nodes. When a node wants to connect to another, the network automatically calculates the best path. A mesh network is also reliable and provides redundancy. If a node can no longer function, for example because it has been removed from the network or because of a barrier preventing it from communicating, the rest of the nodes can still communicate with each other, either directly or through intermediate nodes.

## 2.7 Comparison Between Network Topologies:

Each networks type has some Pros and Cons [59] as shown in table 2.1. The choosing of any network is depending on the requirements. A mesh network topology has been used because of the need to more reliable, low delay, and multipath network.

Table 2.1 Pros and Cons of the Networks

| | Advantages | Disadvantages |
|---|---|---|
| **Star Network** | • Simple network<br>• Easy to install<br>• Low power operation<br>• Very low delay<br>• Easy to synchronize | • Small range<br>• Don't have the ability to communicate with each other just with the coordinator. |
| **Cluster tree Network** | • Low routing<br>• Allow multi-hop communication | • High delay |
| **Mesh Network** | • Low delay network<br>• Multipath network<br>• High reliability<br>• Robust network<br>• High range | • More complex than the other networks |

## 2.8 Mesh Network Features [61]

There are many features that a Mesh Network has which gives high flexibility to send and receive data with high reliability

### 2.8.1 Routing :

That means the message is hopping from node to another node until arrive to required destination.

### 2.8.2 Ad-hoc Network Creation :

It means that no human intervention in the network, in other words it is an automated process.

### 2.8.3 Self-healing :

This feature means that the mesh network has the ability to reconfigured even though some nodes are missing or fail to operate.

## 2.9 How the Zigbee Communicate

There are three general types of communication topologies, the unicast, the multicast, and the broadcast mechanism [65].

- **Broadcast** means that the transmitting process for all nodes with the same data, in other word, these transmissions are propagated throughout the entire network so that all possible nodes receive the transmission data .
- **Multicast** means the data is delivered to a specific group of devices in a network .
- **Unicast** means that the data is delivered to specific device as shown in Figure 2.16

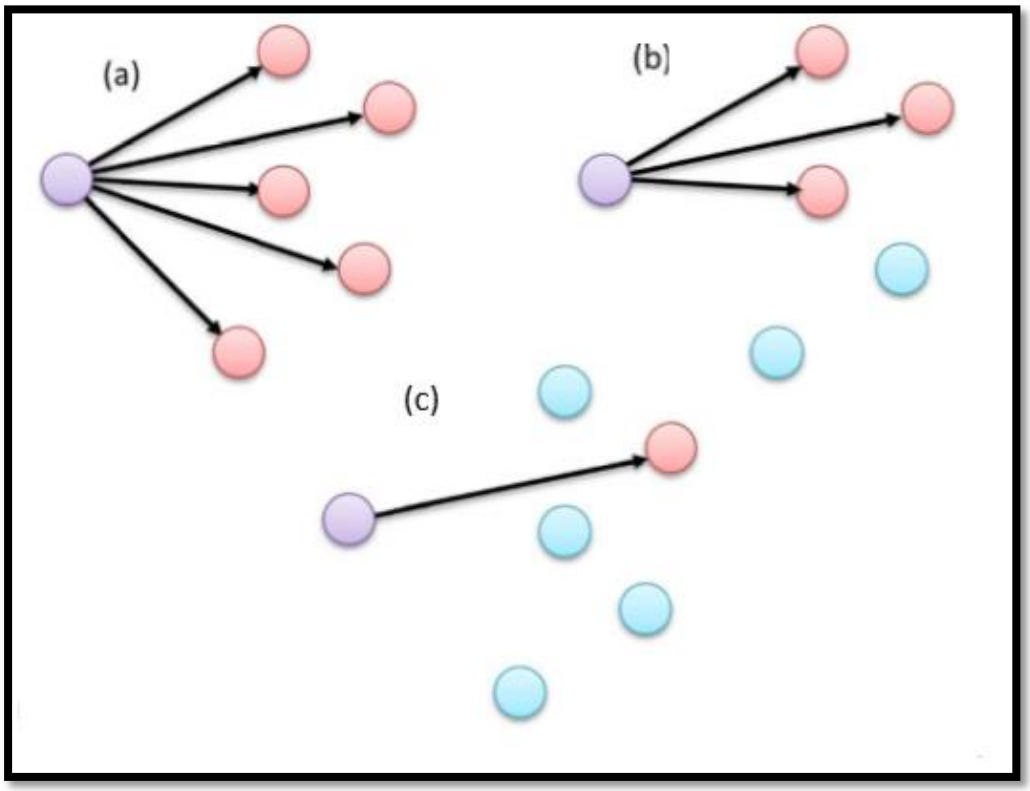



Fig.2.16 communication mechanism

(a)Broadcast (b) Multicast (c) Unicast

## 2.10 XBee

The XBee is a trademark of Zigbee Alliance. It is a cost-effective, stand-alone modular component that uses radio frequency (RF) to transmit and receive data between XBee units [66]. The XBee is the commercial type of Zigbee as shown in the Figure 2.17.

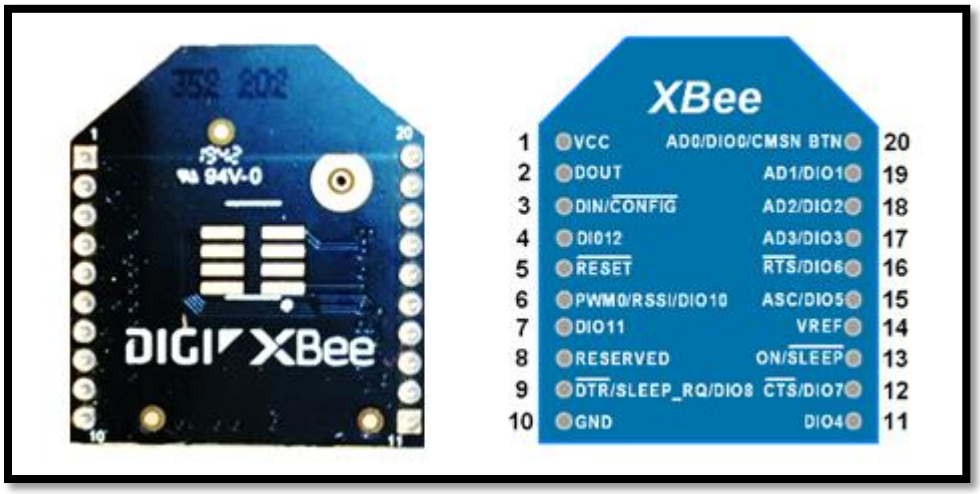



Fig.2.17 XBee pin out

The XBee has two types of communication, the serial communication and wireless communication as shown in Figure 2.18

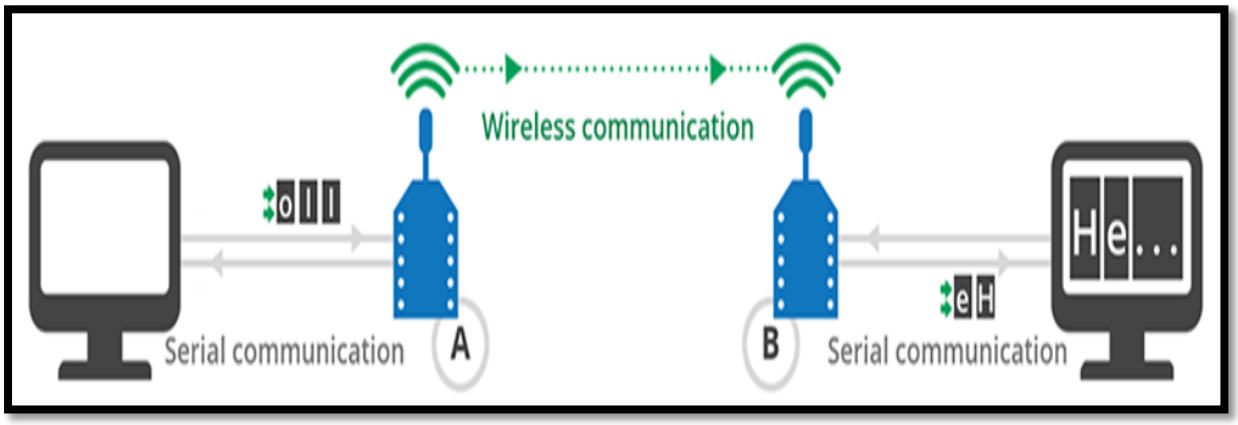



Fig.2.18 XBee communication types [61]

### 2.10.1 Wireless Communication:

This communication is happened between two Xbee or more has the same radio frequency and they are part of Zigbee network. If these conditions are existing, then the wireless communication is valid.

### 2.10.2 Serial Communication :

This communication takes place between the Xbee and another device such as computer through the serial interface.

The XBee can be configured as **Coordinator, Router,** and **End-device** by using the Digi XCTU program which is an official configuration program for configuring the XBee [61]. It is a free cross-platform application compatible with Windows, MacOS and Linux operating systems. The XCTU has two operation modes, the Application Transparent ( Transparent Mode) (AT) or the Application Programming Interface (API) [67]. The XBee 3 is used in the entire system which has a high range (about 200 ft indoor and 4000 ft outdoor) [68]. For more details, see Appendix (A).

## 2.11 Proposed System Theory

### 2.11.1 Arduino Mega 2560

The Arduino is an advanced electronic board with a microcontroller based on AT mega 2560 and an open-source electronic circuit that is programmed by a computer. The importance of arduino lies in its ease of using and programming in wide area so that the arduino has many shields which makes it more compatible with the other systems. Furthermore, it is convenient and easy to use in programming with Arduino IDE ( Arduino Integrated Development Environment ) and C++ languages, which are commonly used at the present time [69, 70]. Figure 2.19 shows the inputs and outputs pins diagram of the Arduino.

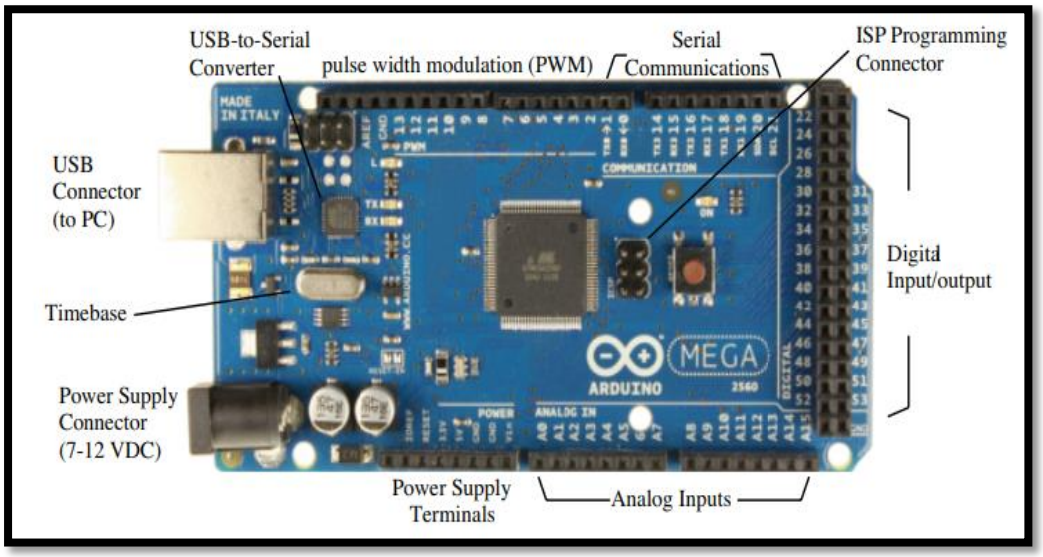



Fig.2.19 Arduino mega 2560 pin out [69]

### 2.11.2 Arduino Shield

The arduino shield is an extra piece that gives an additional function to the arduino board and it can be simple or complex according to the specific mission. The purpose of using the Arduino shield is to reduce the wiring complexity because it has the same position of the pins like the arduino pin and to decrease the processing time. As a result, it is necessary to connect the arduino shield carefully with the suitable pins of arduino to avoid the damaged that happened due to wrong supplying voltage and current to the pins. There are many types of shields, the GSM arduino shield, the Wi-Fi arduino shield, the prototype shield, the micro SD shield, etc.

The Xbee shield is one of the most important shield which supports low power consumption and connects the Zigbee to the arduino circuit. Figure 2.20 shown the XBee arduino shield.

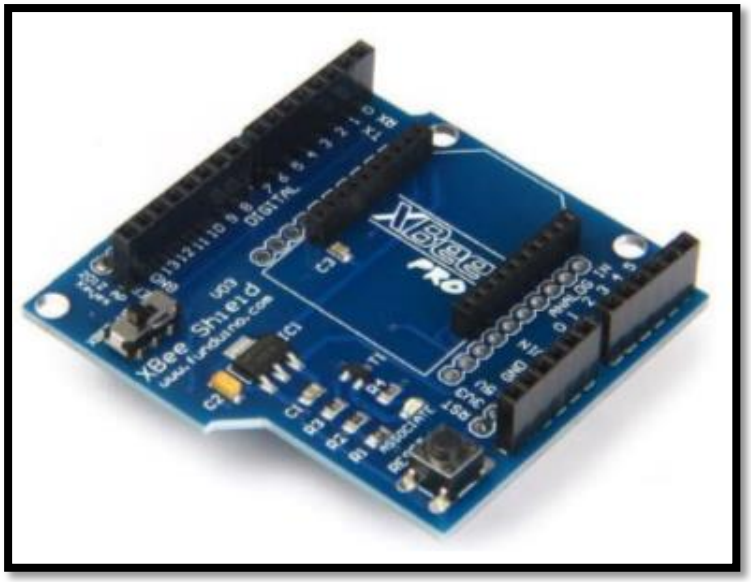
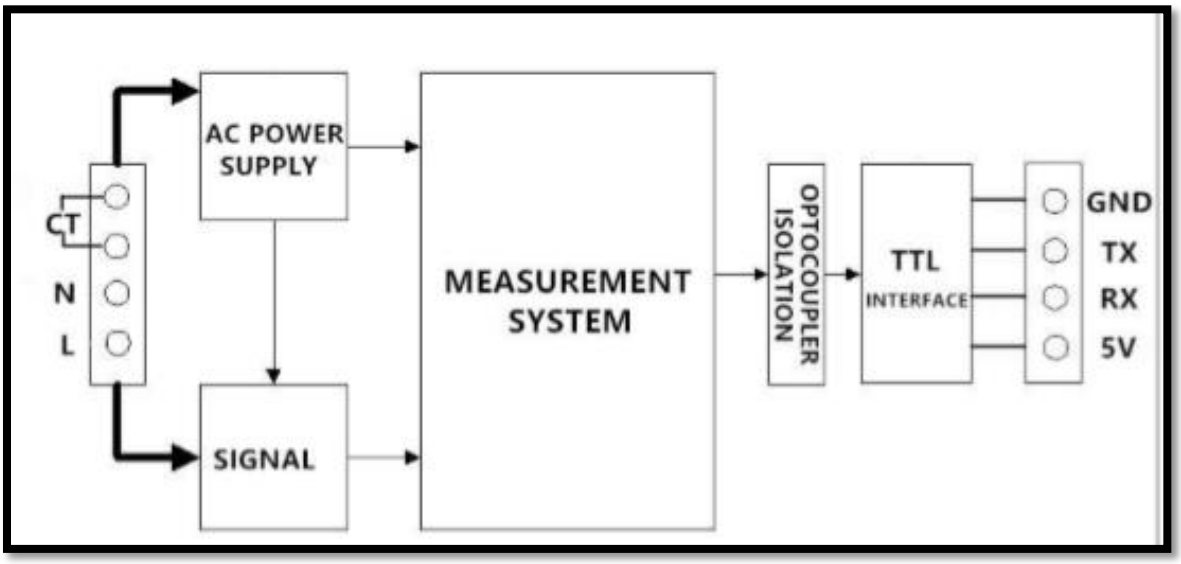



Fig. 2.20 XBee shield [69]

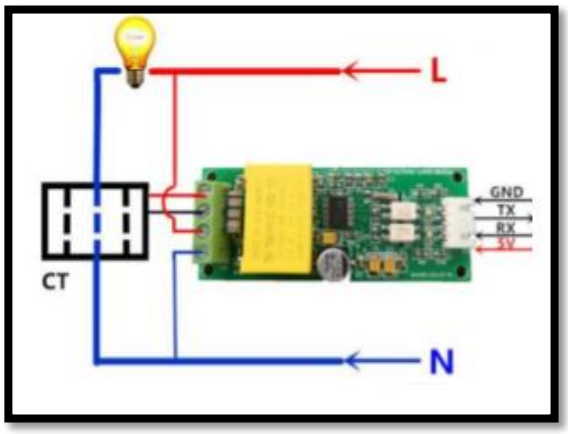
### 2.11.3 Energy Sensor:

The energy sensor (PZEM-004T-100A) is used to measure the AC voltage (V), AC current (I), the active power (P), the power factor(Pf), the frequency (f), and the active energy (E). This sensor has the ability to measure and store the above measurements and display data through the interfacing TTL because this sensor has not display unit. This sensor uses an alternative current (AC) power source and measures the above parameters by passing the load wire through the current transformer (CT).

The reasons for using this sensor is its high accuracy, low cost, easy to programmable and low power consumption which means long battery life for whole system and it is easy to communicate with serial communication by using only two terminals (Tx and Rx) [71]. Figure.2.21 shows the block diagram, wiring and shapes for the energy sensor. More details are shown in appendix (B).




(a)




(b) (c)

Fig. 2.21(a) PZEM004T block diagram, (b) ) PZEM004T wiring

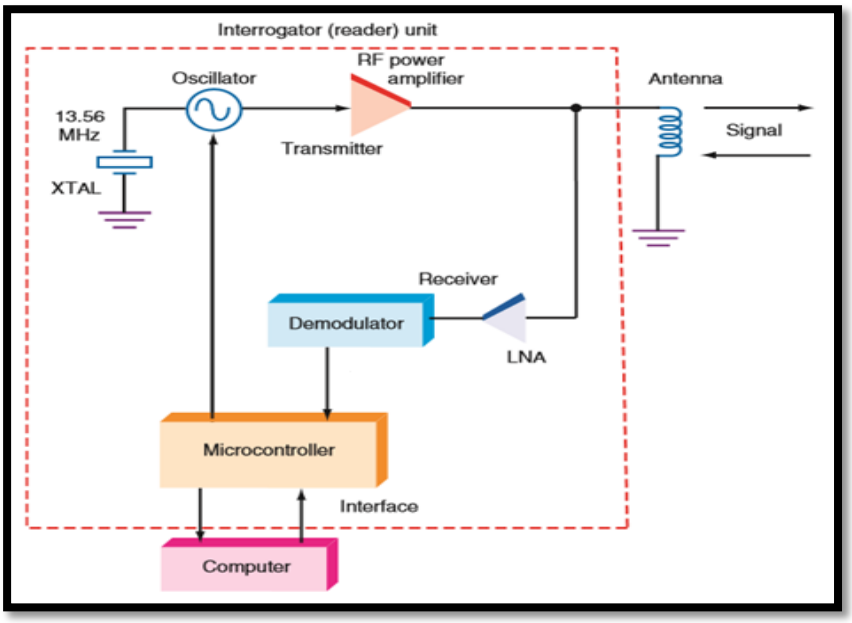
(c) PZEM004T shape

## 2.11.4 Radio Frequency Identification ( RFID)

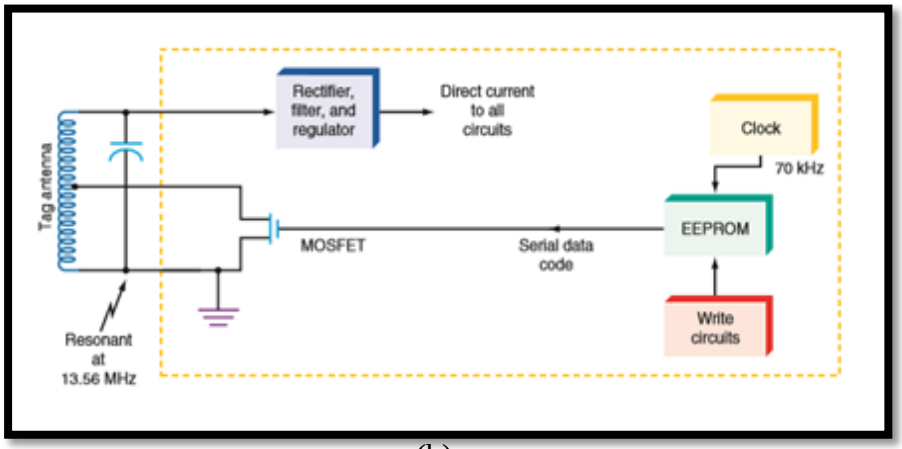
Determining the identity of things has become one of the necessary and important things in daily life activities, such as allowing the entry of one person without another, or tracking the transporting and storing goods in ports, also in marketing fields, medicine fields, automation field as well as collecting the required fees [72].

The RFID is one of the best technology for identifying objects through radio waves. Although RFID technology has been widely used in recent times, its discovery dates back to World War II. This technique was used for the first time for the purpose of distinguishing friendly from enemy aircrafts.

The RFID consists of two devices, the first part which carry the required information is called the transponder or tag as shown in Figure 2.22 b, while the second part which capture and transfer the information is called interrogator or reader as shown in Figure 2.22 a [73].




(a)




(b)

Fig. 2.22 RFID (a) Interrogator (b) Transponder [73]

**The RFID tags** can be classified according to the power source into three types [74] as shown in Figure 2.23:

- Passive tags which hasn't any battery to operate the its circuit, the operation power signal come from the interrogator.
- Semi passive/Semi Active tag has a battery to power the tag , but still need the interrogator power signal to communicate.
- Active tag is already has battery to power up the transponder to send a required data signal to the interrogator.

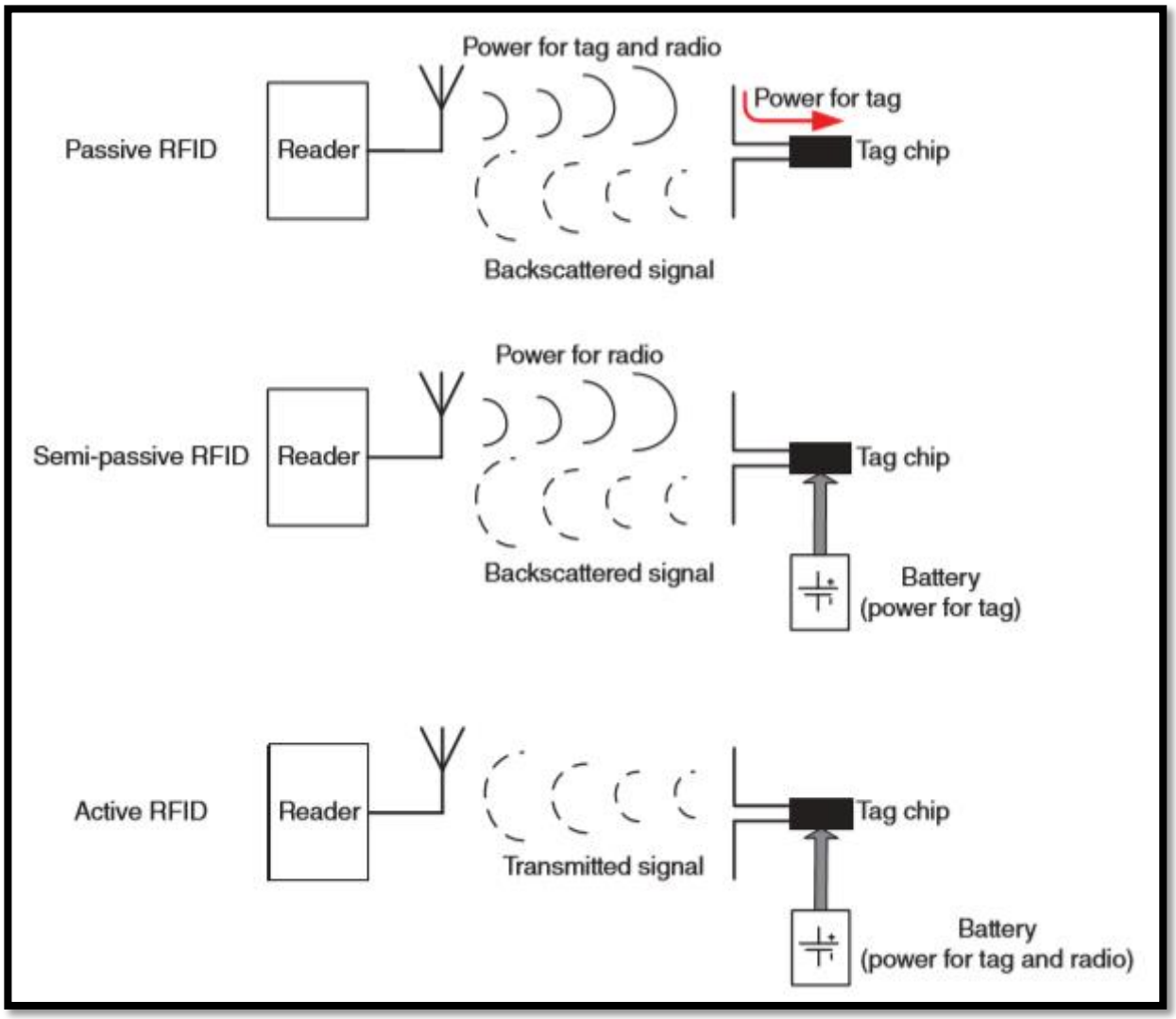



Fig. 2.23 RFID tag classification [74]

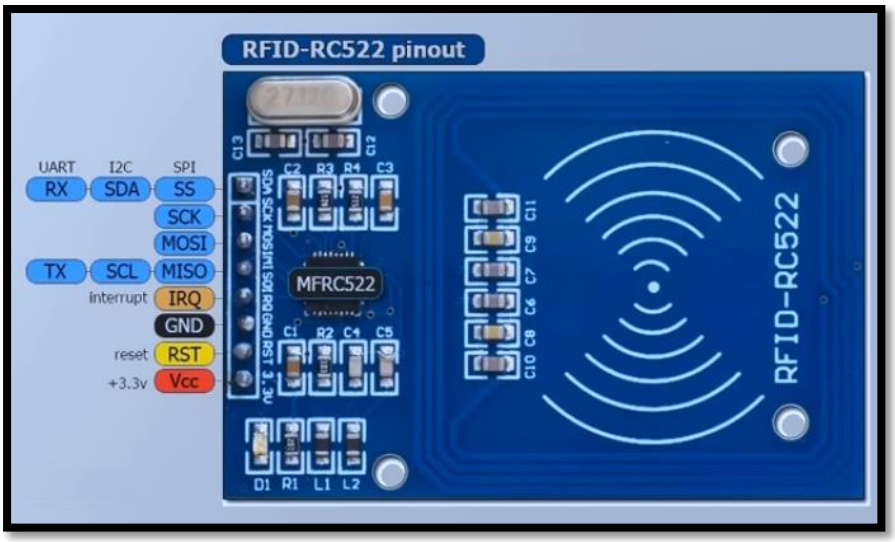
**The RFID works** on different frequencies [74] according to specific application as shown in Table 2.2.

Table 2.2 RFID Frequencies [74]

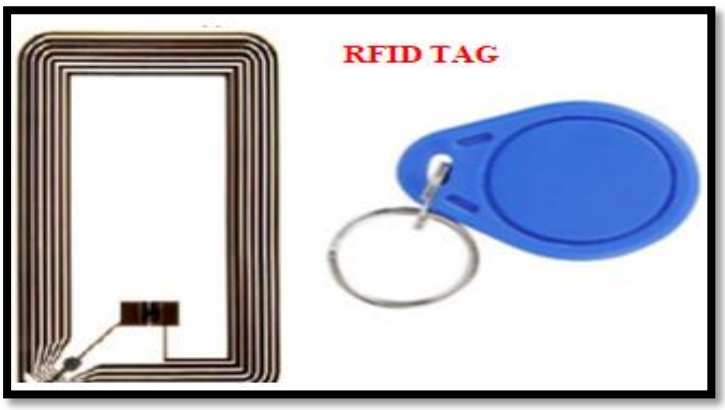
| | **(LF)** | **(HF)** | **(UHF)** | **Microwave** |
|---|---|---|---|---|
| **Frequency** | (125-134) KHz | 13.56MHz | 860-960 MHz | 2.45-5.8GHz |
| **Read Range** | 1 m | 1 m | 3 m | 4.5 m |
| **Data Rate** | 1 kbps | 10kbps | 50-150 kbps | Not specified |

- **RFID-RC522**

The passive tag will be used as the RFID-RC522 model in this thesis which operate at high frequency with 13.56 MHz . The reason for using RC-522 model is the good features like low consumed power, cheap, and small size which is compatible with the idea of proposed system [75, 76]. as shown in Figure 2.24




(a)




(b)

Fig. 2.24 (a) RC-522 tag pin out (b) RC 522 tag shape

1) **Principle Operation of RFID/RC-522**

- The interrogator sends an electromagnetic radio wave power signal to the transponder which receives this signal to charge its capacitor.
- When the capacitor reaches to the threshold value, the RFID transponder circuit switched on and transmit a modulated signal to the transponder.
- Lastly, the transponder will demodulate the tag signal to get the required information. The basic operation can be shown in Figure 2.25.

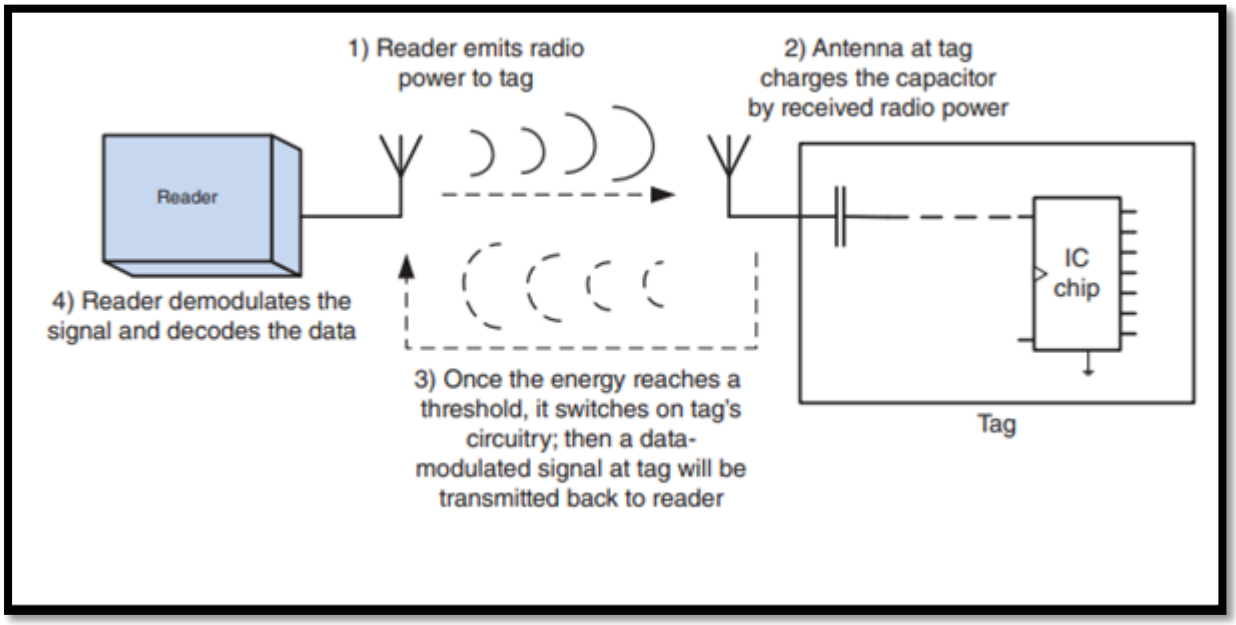



Fig. 2.25 Basic operation for RFID

### 2.11.5 Led Crystal Display (LCD)

The display devices provide a visual display of symbols, numbers or letters due to electrical inputs, and act as components of an electronic display system [77]. The LCD is made of liquid crystals which is a special crystals that interact with the electricity [78]. It is characterized as very low power consumption device [79] which is very useful in the desired system. The 128*64 LCD 7920ST module has been used in the system.

## 2.12 Graphical Unit Interface (GUI)

User interface is the concept of human-computer interaction for planning and designing an interface that meets people's needs in effective ways so that it is a language understandable to the user and helps in analyzing data and information [80]. The user interface is a part of computer software and of the computer itself. The user interface consists of two main parts: input and output.

In other words, the GUI is an environment that allows the user to know what is going on in the system without having to know the programming languages and their complexities as shown in Figure 2.26.

### 2.12.1 GUI Features

There are many features for GUI such as

- Easy to use and understand by the user
- Can have multitask

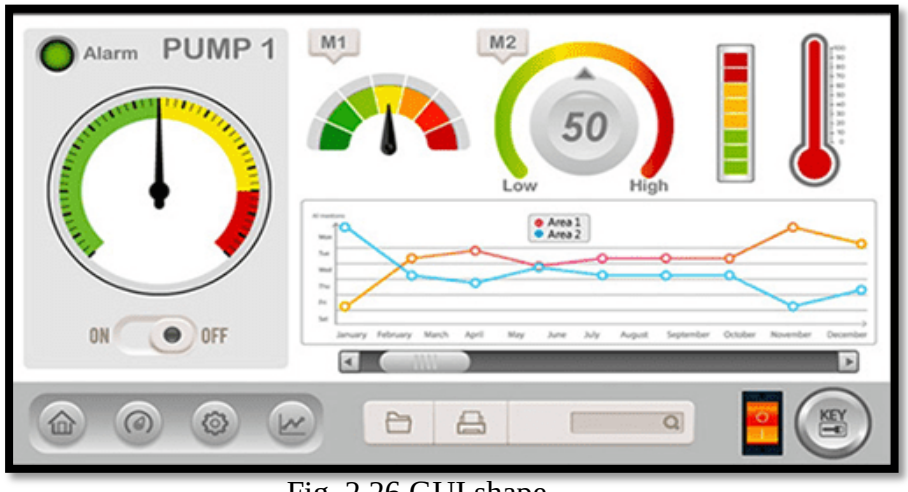



Fig. 2.26 GUI shape

# Chapter Three

# Design and Implementation

# Of

# The Proposed System

# Chapter Three

# Design And Implementation Of The Proposed System

## 3.1 Introduction

This chapter presents the design and implementation of a smart energy system able to be a prepaid billing and theft detection system in the same time with slight differences in some components and big difference in system operations idea. The communication in the proposed system is based on a wireless sensor network (WSN) as Zigbee network technology and radio frequency identification (RFID) technology (that used in prepaid billing system) without depending on telecommunication companies or the internet, as the most of the researchers did. This system is implemented by using arduino C/C++ language used in consumer nodes and transformer node, while C sharp language used in server node and GUI . The idea of proposed system is illustrated in Figure 3.1.

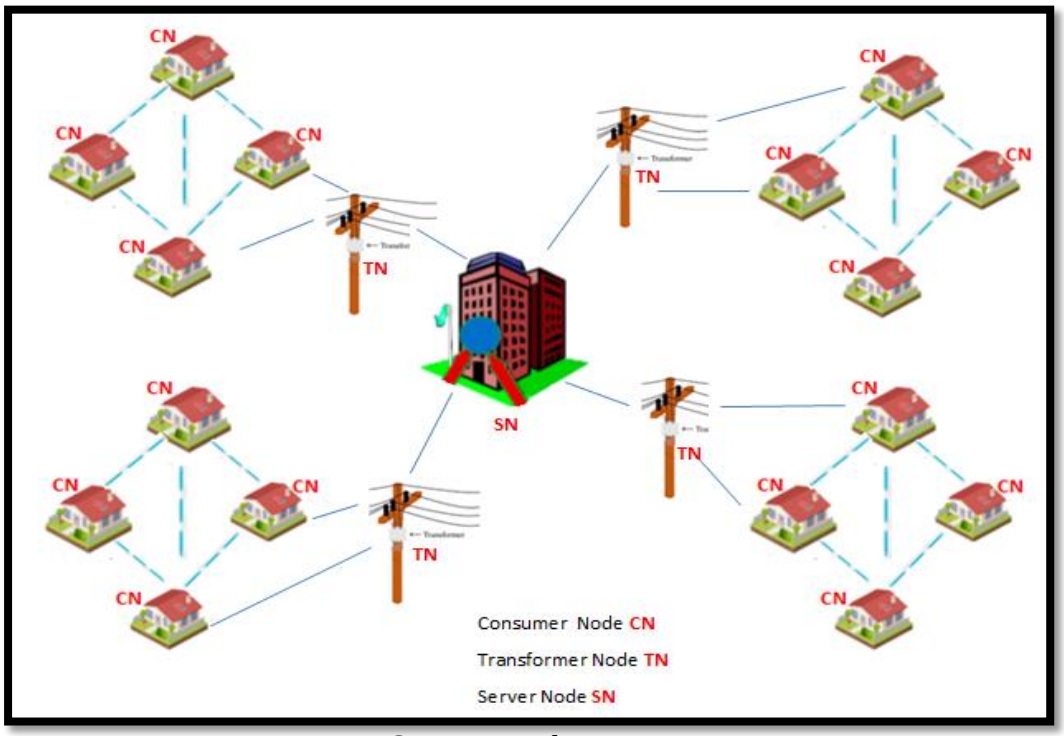



Fig.3.1 Proposed system

## 3.2 Overall System Description

The proposed system has three types of nodes, as shown in Figure 3.2. The first type is the consumer node, the second is the transformer node which supplies electrical power to the consumers, and the third type is the server node which controls all of the system.

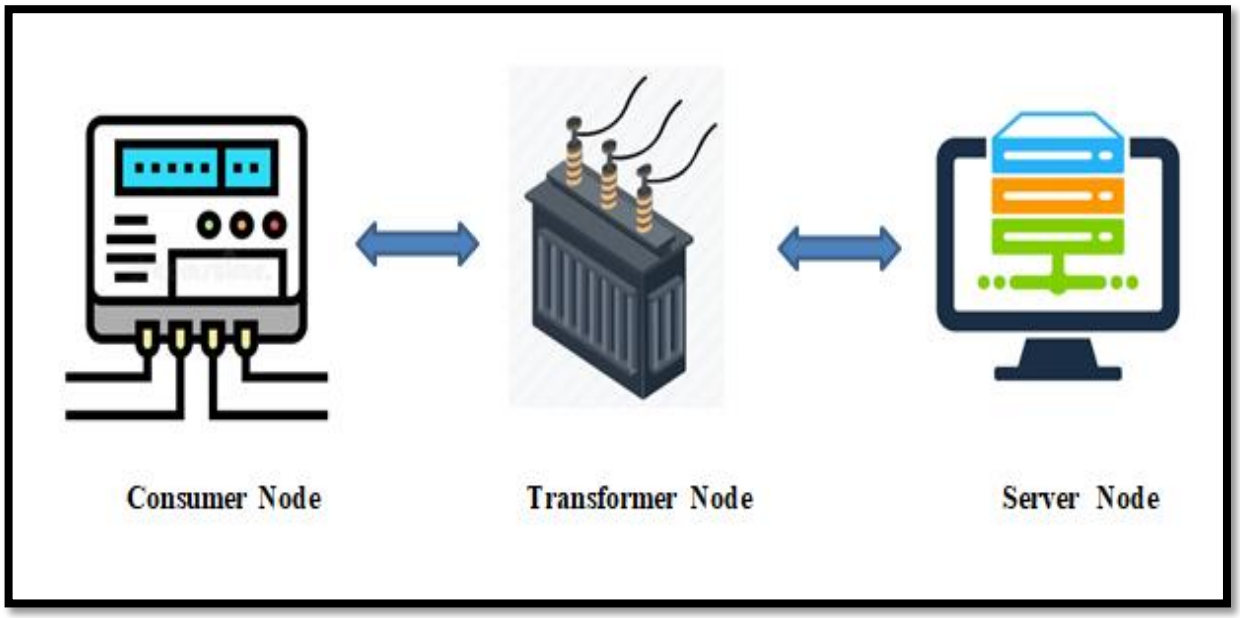



Fig. 3.2 Proposed system nodes

## 3.3 Proposed System Operation

In this section, we will explain the hardware and the software operations which solve both the BNP and the EETh problems by using a simple, low cost and high performance components with the simple and more effective technologies.

### 3.3.1 Proposed system for Billing Non Payment (BNP) problem

The purpose of building this system which is shown in Figure 3.3 is to solve the BNP problem of electrical energy. It proposes a prepaid system which guarantees the rights of both the consumer and the electricity company. The proposed system displays the consumed the electrical energy by the consumer in

(KWh), as well as the amount of the RFID tag which refers to the balance that has been filled out by the consumer. It also displays the remaining balance and notifies the consumer if the balance is close to running out, which requires filling it again.

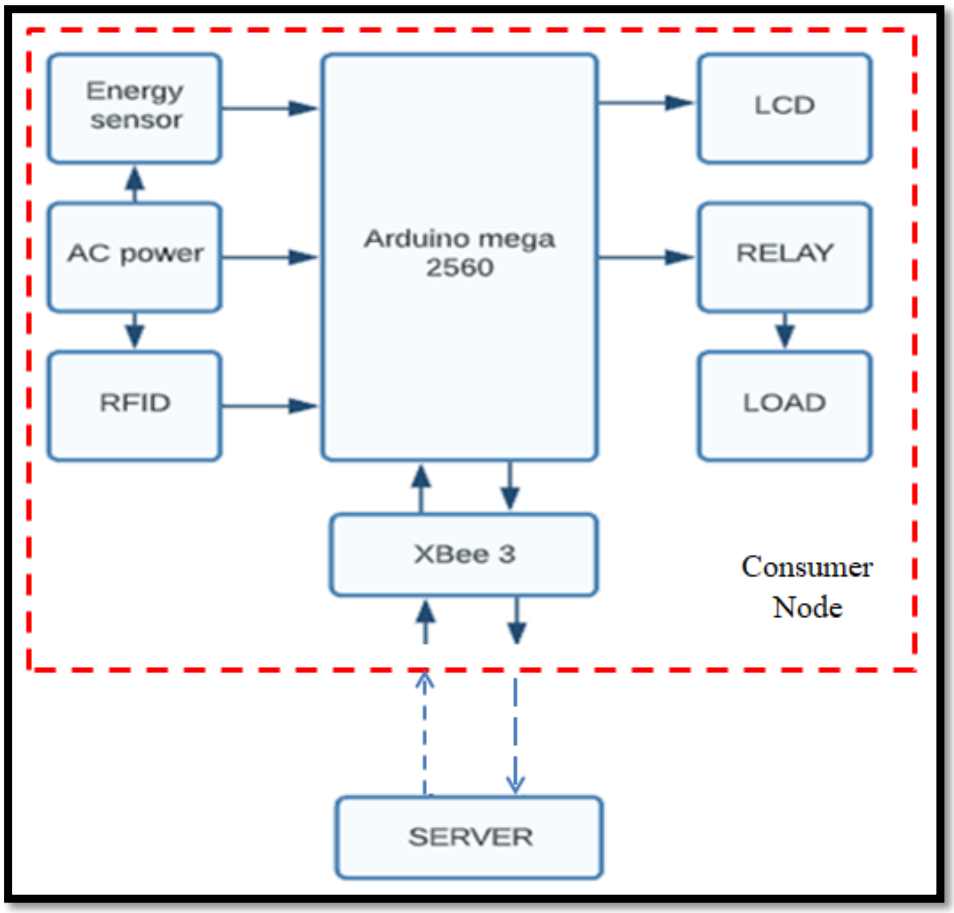



Fig. 3.3 Proposed system for BNP block diagram

1) **System Operation**

When the RFID interrogator reads the tag amount, the system sends its code to the server for checking the validity of that card. The meter will be charged if the card is valid and shows the total balance on the LCD, otherwise no message will be shown and the meter will wait for a valid card.

It is assumed that the amount will be 25000 Iraqi Dinar (IQD) and the energy consumption unit price (tariff) is assumed to be 10 IQD/KWh for residential consumer, taking into account that the card amount represents 100% as a

balance. Equation 3.1 shows the formula which calculates the remaining balance for the prepaid meter of the consumer.

$$\boldsymbol{C = |EB - E * T|} \quad (3.1)$$

where, $C$ is the remaining balance for the consumer's meter,

$EB$ is the existing balance,

$E$ is the energy consumed by load which measured by the energy sensor,

$T$ is the unit price (tariff).

When the remaining KWh reaches a low level equal to 10% of the balance, a warning is sent out to alarm the consumer to recharge the meter with new balance. If the energy balance reaches zero, the microcontroller sends a signal to the relay for powering off the load. In this case, the consumer has to recharge the energy balance to reclose the relay circuit again for powering the consumer's load. Figure 3.4 shows the flowchart of the system's algorithm.

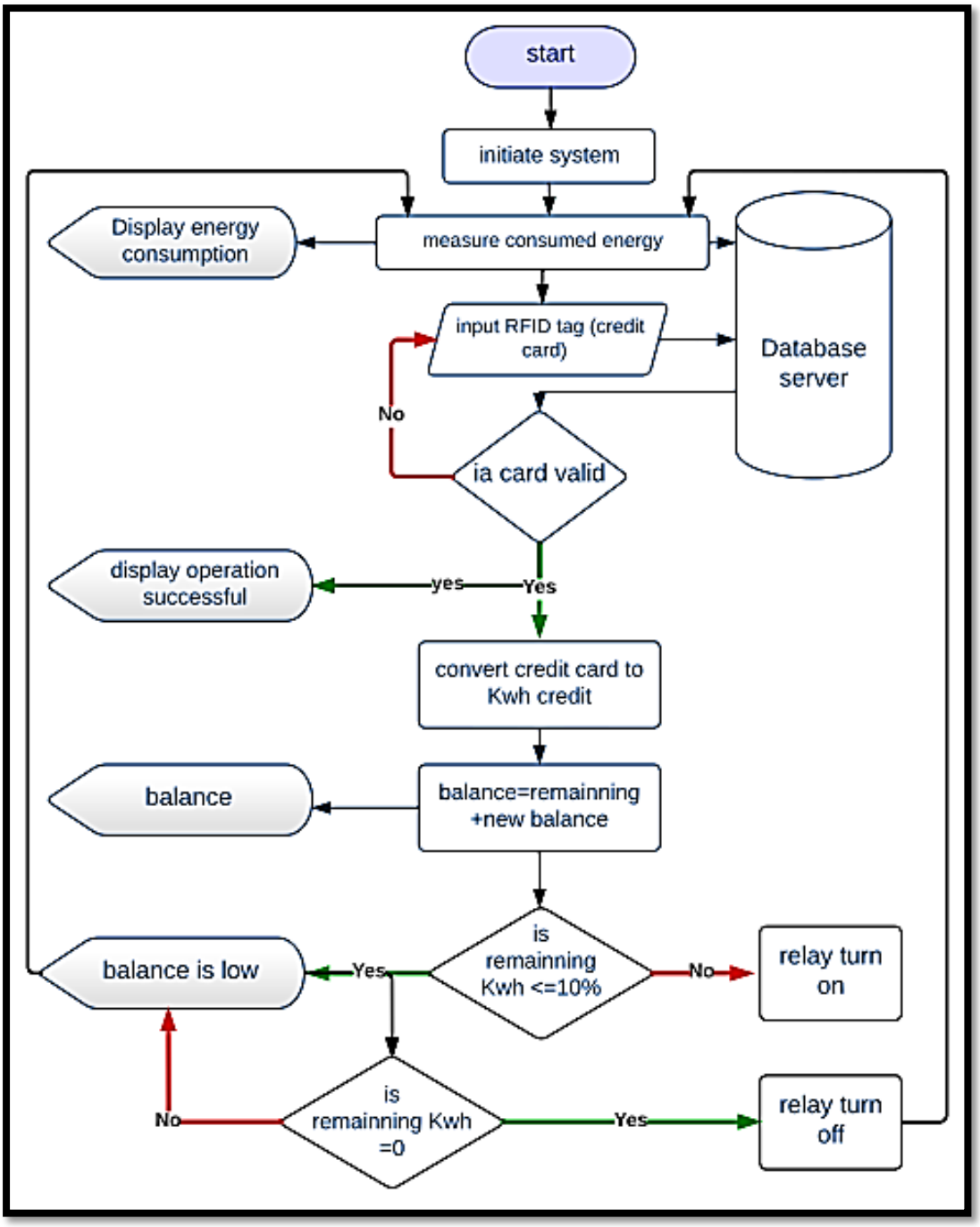



Fig. 3.4 Proposed system operation for BNP problem

### 3.3.2 Proposed System for Electrical Energy Theft (EETh) problem

This system is designed for EETh detection and implemented in simple components with high quality designing as shown in Figure 3.5. In fact, this system is able to detect electricity thefts by using wireless communication (Zigbee mesh network). This system is unlike traditional meters in which the

theft can only be detected by the intervention of roving teams that detect thefts through inspection overall network.

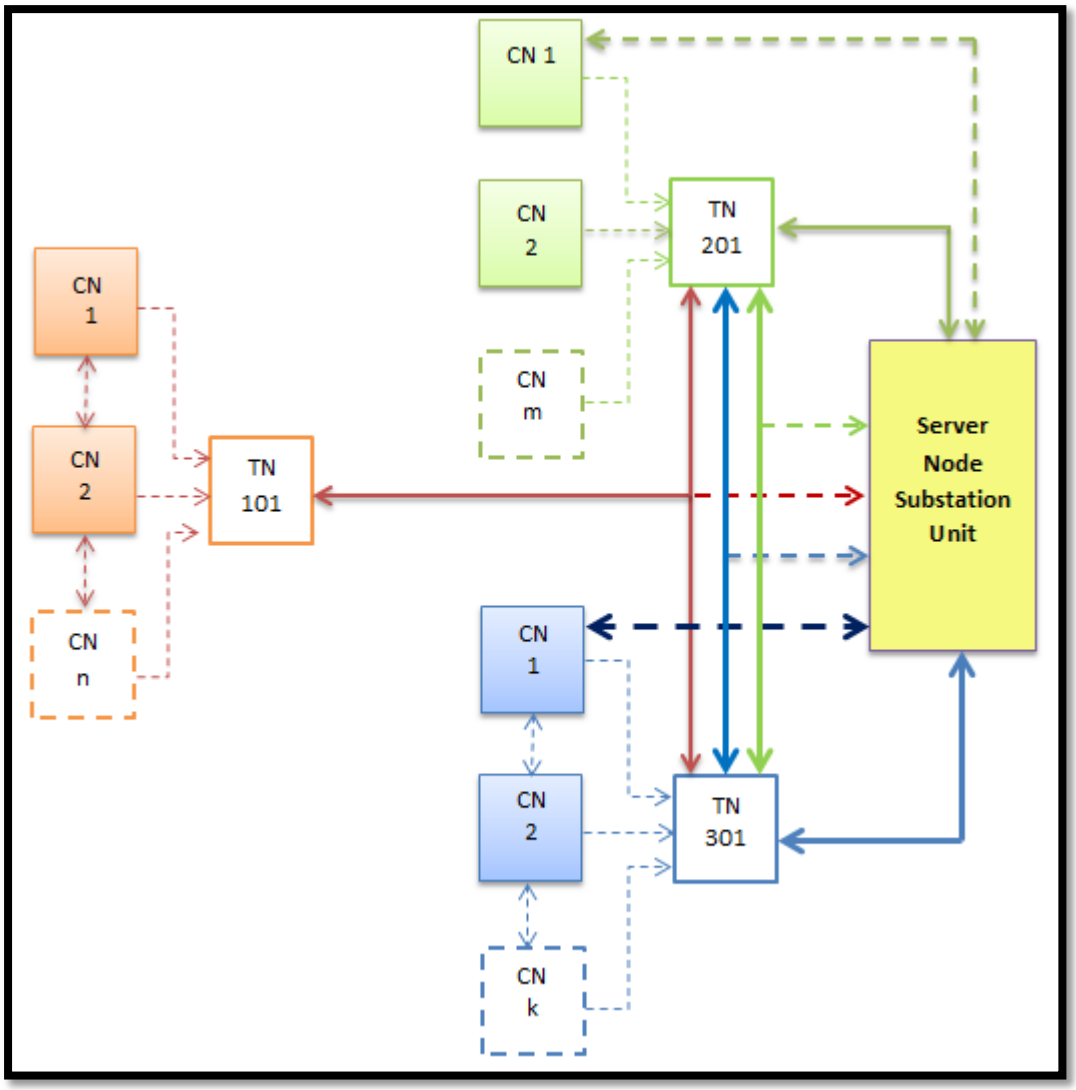



Fig. 3.5 Proposed system block diagram for EETh problem

The contribution of the proposed system is the ability to detect the EETh at the distribution line (TN) and identify the candidate consumer energy meter (CN) that may be an illegal consumer to locate the area that may be the energy theft is happened.

### 1) System Operation

The solution of the EETh problem has three parts, the first part is the solution for the EETh problem that appears at CN (consumer energy meter ), while the

second part is the solution for the EETh problem that appears at the distribution line (TN). The third part is candidating the CN that possible to be the illegal CN.

**A. EETh Problem Detection at CN**

The cases of tampering that occur inside the meter by the illegal consumer are numerous, such as :

- Tampering with the magnet of the meter
- Bypassing the phase line
- Bypassing the neutral line
- Bypassing the whole meter
- Illegal tapping ( underground cables)

So, as a solution for the energy theft at the consumer meter , the components of the proposed meter are placed inside a sealed box with screws, and even the inlet and outlet cables are fixed inside. In the event of an attempt to open the meter, the controller turns off the consumer's load, and send indication of tampering action to the server.

consequently, we could prevent tampering that could happen inside the meter and avoid the EETh at consumer node.

**B. EETh Detection at (TN ) Distribution line**

The detection of electrical energy theft that occurs in distribution lines is one of the important things to address this problem. In this section The EETh detection can be summarized in the following steps as shown in Figure 3.6 :

- Firstly, after initiate all the system make sure that all the devices are working properly and all nodes are in work state.
- Then the CN1 will measure the load current and send it wirelessly to another node down to the server. This currents denoted as $I_1$.
- After that the CN 2 will also measure the load current and send it wirelessly to another node down to the server. This currents denoted as $I_2$.

- The TN has current sensor that can measure the current supplied to the line for CN1 and CN2. Then TN current will also transmit to the SN wirelessly by Zigbee network. It is denoted as $I_{TN}$ .
- Then we will calculate the total current which represents the summation of transmitted CN 1 current, CN 2 current, … CN n current, where n is the number of the Consumers Nodes ( CNs) as shown in the following equation:

$$I_T = \sum_{i=1}^{n} I_i \tag{3.2}$$

where : $I_T$ is the total current of the consumers currents CN1 and CN2,…etc. ,

$n$ is the number of consumers,

$I_i$ is the current for consumer $i$, $i$ = 1,2,3,…., n.

- The SN will make a comparison between the $I_T$ and the $I_{TN}$ as shown in the following equation :

$$\mathbf{I_{TN} - I_T} \leq \boldsymbol{\alpha} * \boldsymbol{I_{TN}} \tag{3.3}$$

where : $\mathbf{I_{TN}}$ is the measured current at TN.

$\mathbf{I_T}$ is the calculated total current consumed by consumer nodes CNs.

$\boldsymbol{\alpha}$ is the threshold value that represents the consumed currents for the system devices. Take into account ($\mathbf{0.01 \leq \alpha \leq 0.05}$)

- If the condition is valid that means no theft detection and the system will continuously check again for energy theft.
- If the condition is not valid, the SN will indicates that there is an EETh detection at TN which represents the supplier for the distribution line that feeds the CNs.

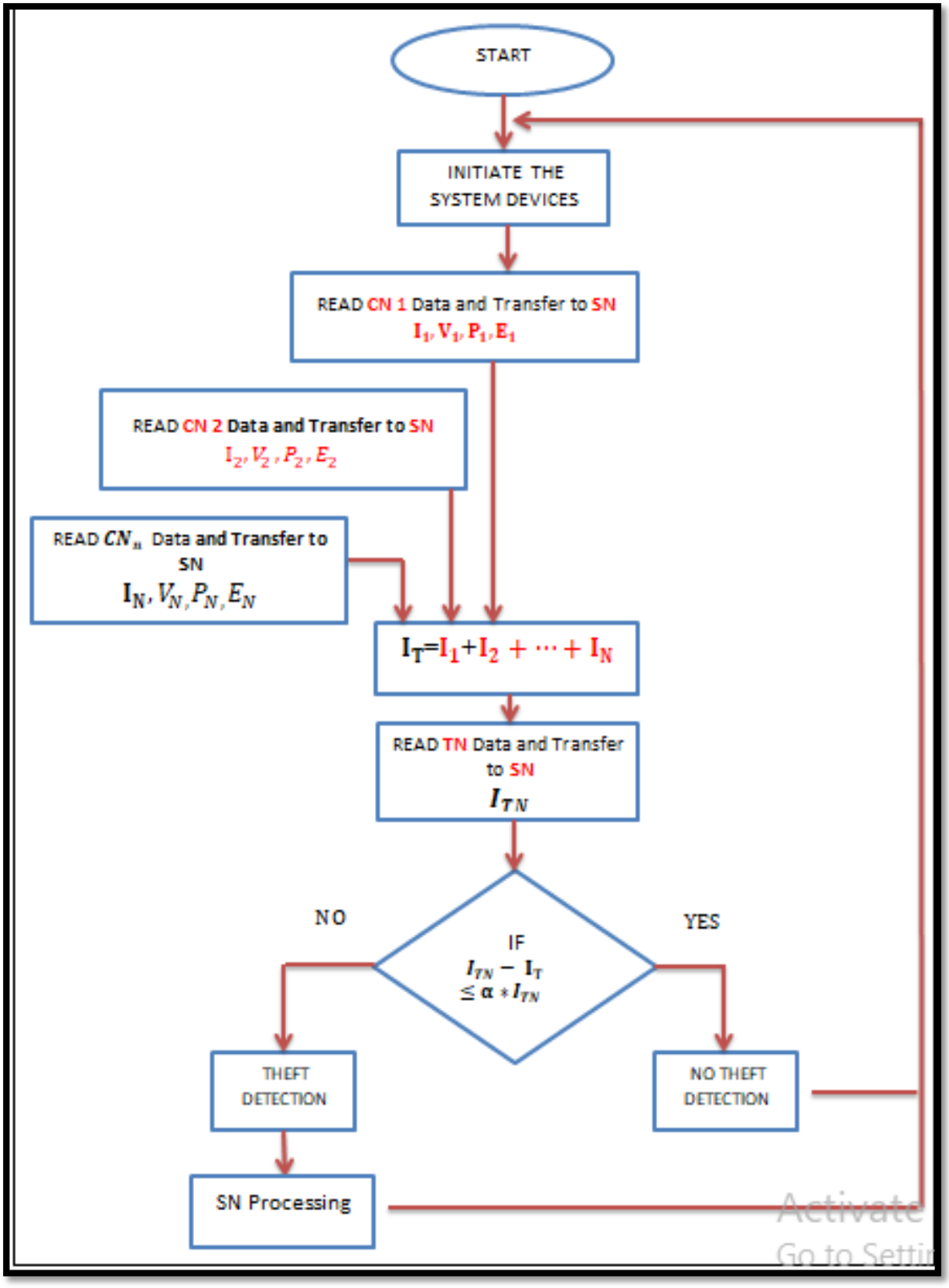



Fig.3.6 Proposed system EETh operation

### C. EETh Nodes Candidate

In the previous section, it was able to determine the location of EETh in which TN is located. As a result, it is able to limit the energy theft from a large city in which there are many distribution lines and electrical power transformers to a small area. This small area does not exceed around twenty houses are connected to one transformer feeder. In other words, system is detecting the illegal TN. Hence, it became possible to send the specialized team to look for illegal consumers in this small area.

To facilitate the task of this team in the search for theft of electrical energy, the proposed methods are capable for determining CN that it is possible to be the illegal consumers for many cases.

- **Case One**: If the illegal consumer turns all the CN load into theft case, that means the transmitted data to the SN shows that the load current become zero for that CN . The proposed system will indicate that this node may be a candidate energy theft state and inform the specialist team . When the proposed system operates, all transmitted data of the system nodes will be saved in Excel sheet represents the load file for each node. This load file shows the date and time for energy theft case as shown in results at chapter four.
- **Case Two**: In the event that the consumer turns off the load and leaves the house, the data that transmitted to the server will indicate that the house current has become zero, but it does not indicate a case of theft of electrical energy by this consumer because the calculated currents are identical to the transmitted currents and there is no theft case.
- **Case Three** : In the case of detecting theft in TN, the server will candidate the illegal node by comparing the current measured in the node that transmitted to the server with the average current (which shown in equations (3.4 and 3.5) of this node, therefore this node candidates to be illegal consumer.

$$A = \frac{\sum_{i=1}^{n} x_i}{n} \quad (3.4)$$

$$A - I_m \geq \mu \quad (3.5)$$

Where : $A$ is the mean average of consumer current,

$x_i$ is the $i^{th}$ measured current value,

$i$ is a counter from first reading (1) to $n^{th}$ readings,

$n$ is number of readings,

$I_m$ is the measured value,

μ is the threshold value determined by the electricity company according to the load type ( residential, commercial, industrial,…, etc.)

- If the condition in equation (3.5) is valid, this means that this node is candidate to be an EETh.
- If the condition is not valid, that means there is no candidate nodes.

As a result, the proposed system was able to obtain the candidate nodes that could be theft of electrical energy, and thus it will be very useful in making a small search area for the specialist team to be more accessible and effective.

### 3.4 Proposed System Parts (Practical Test)

As mentioned before, the proposed system is consisting of three nodes, the Consumer Node ( CN ), the Transformer Node (TN), and the Server Node (SN) as shown in Figure 3.7.


Fig. 3.7 Practical proposed system nodes

### 3.4.1 Consumer Node (CN)

This node represents the smart meter. In the proposed system two consumer nodes were built in a simple design and implementation. as shown in Figure 3.8. Each CN consists of the following parts:

- The Arduino mega 2560 as microcontroller
- The power sensor pzem004t / 100A as power sensor
- The RFID / RC-522 as payment unit
- The LCD 64*128 ST 7920 as a display
- The Zigbee module / Xbee3 as a communication unit
- Relay
- Power supply

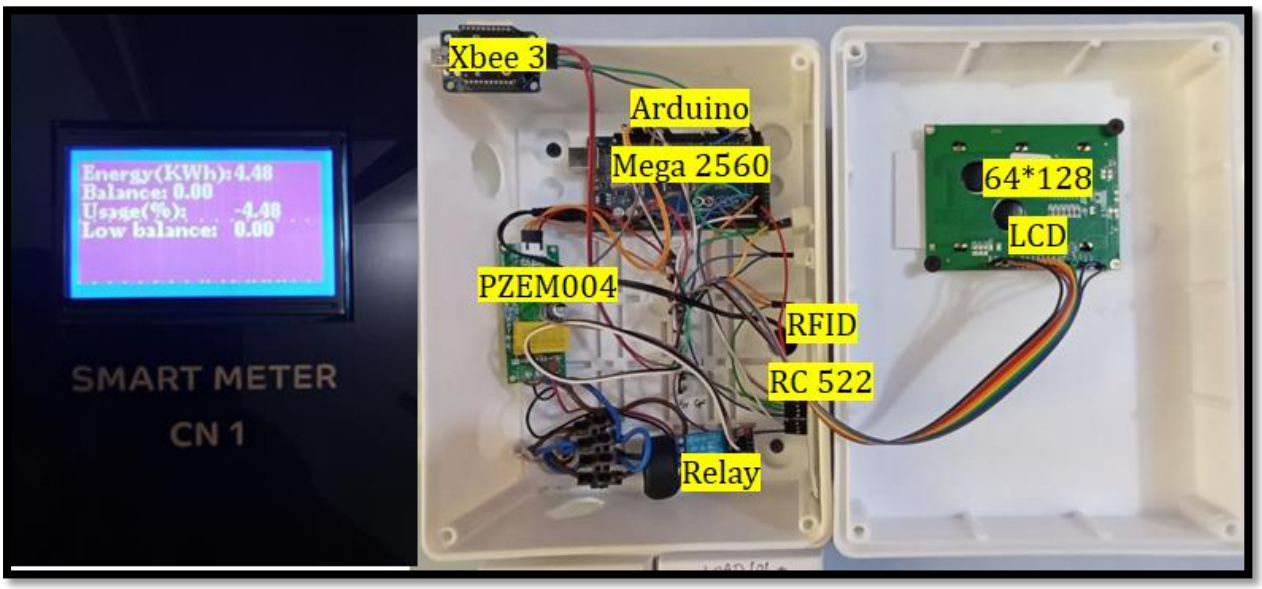



Fig. 3.8 Consumer node (CN)

### a) Consumer Node Tasks

The consumer node which is a smart meter has the following duties:

- Measures the load parameters such as, the voltage, current, power, power factor, and consumed energy.
- Calculates, the entire energy balance which is filled by the RFID and compares it always with the consumed energy.
- Doesn't allow to open the meter to prevent theft of electrical energy. In the event that the meter is opened, the system will send the case of energy theft to the server, as well as cut off the electrical power to the consumer.
- Behaves End Devices node in the Mesh Network.
- Fills in the electrical energy balance on site by using RFID.
- Sends wirelessly the requested data via other nodes to the server.
- Displays the necessary information on the meter LCD to be understandable by the consumer.

### 3.4.2 Transformer Node (TN)

The transformer node which supplies electrical energy to the consumers. The Transformer Node consists of the following parts as shown in Figure3.9.

- The power sensor PZEM004T/100A
- The microcontroller ( Arduino Mega 2560)
- The communication Unit Zigbee / Xbee3
- Power supply

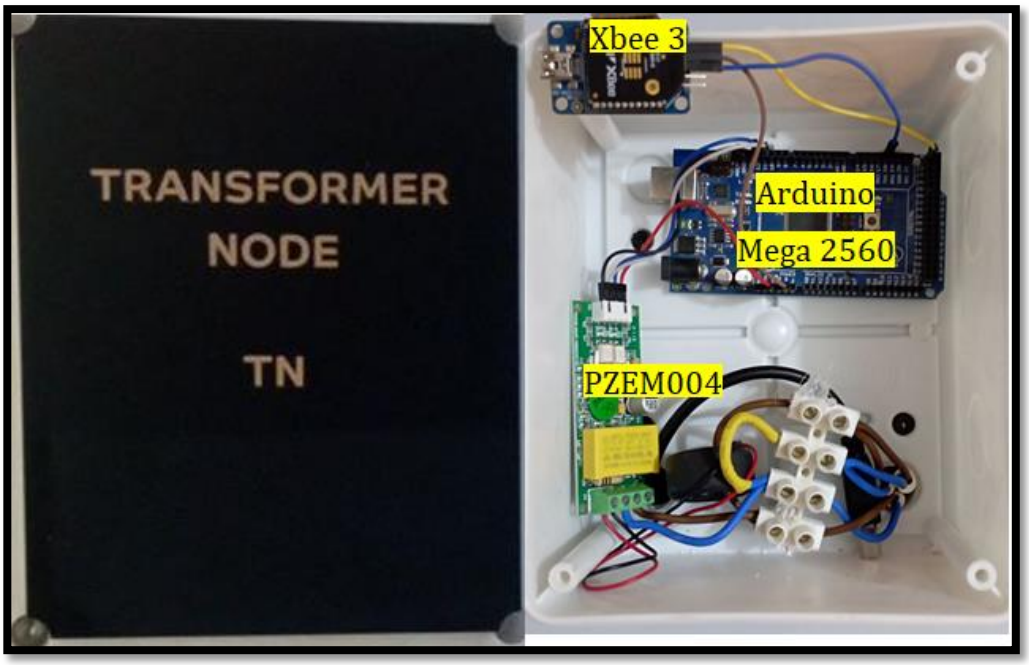



Fig.3.9 Transformer node (TN)

**a) Transformer Node Tasks**

The Transformer node has many tasks as following :

- Works as an intermediate node represented in Router node
- Works as a transceiver between consumers nodes and the server node.
- Collects all the consumers' data and sends it to the Server or to another Router down to the Server.
- Receives the necessary commands and send them to the consumers' nodes ( End Device).

- Measures the total consumed energy in the consumers meters, and also the total drawn current.

### 3.4.3 Server Node (SN)

This node represents the which is the Mastermind that organizes all the system. It consists of the following parts as shown in Figure 3.10.

- The Zigbee / Xbee3 with adapter (coordinator)
- Laptop


Fig. 3.10 Server node

### A. Server Node Tasks

The Server Node has many duties as following:

- Consider as *a Coordinator* and control all the system operation.
- Manage the BNP and EETh operation
- Receive all nodes data
- Consist of all consumer's data arranged in the database as a load file for each consumer.
- compare the power consumption and current of the consumer node with transformer node data as EETh detection.

## 3.5 Proposed System Components Connections

The proposed system wiring connection can be shown in figure below

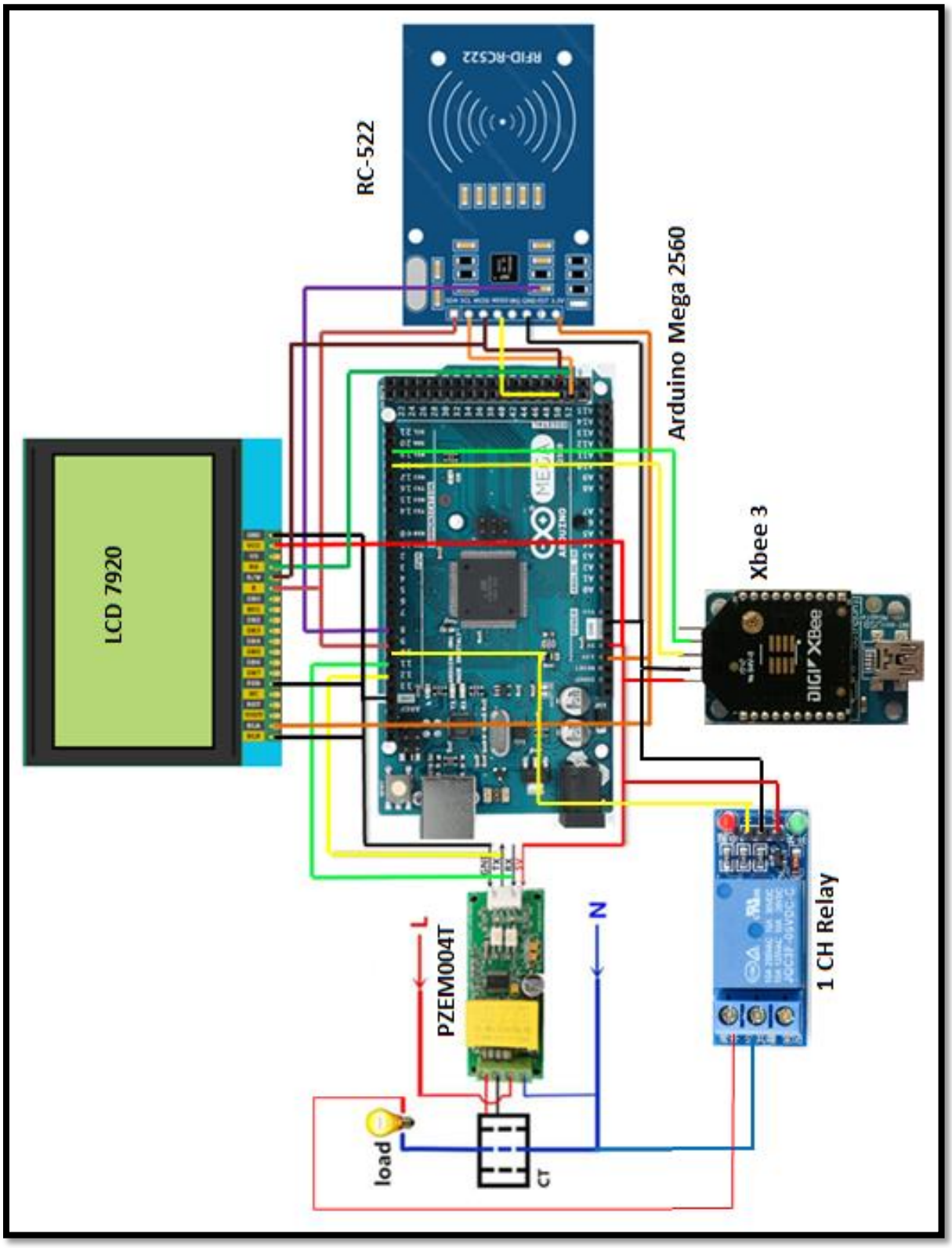



Fig. 3.11 The proposed system wiring

### 3.5.1 Arduino Mega 2560:

The Arduino is a Mastermind for all the system. It connects all the system components represented in power sensor (PZEM004T), payment device (RFID RC-522), communication device (Xbee3), Relay and the LCD. The software operation was programmed with Arduino IDE ( Arduino Integrated Development Environment) and C++ languages (as shown in Figure 3.12) which are commonly used at the present time. The Arduino has many tasks as following:

- Initiate all the system components to operate.
- Communicate between system nodes.
- process the data incoming from the energy sensor and displays the required information on the LCD.
- perform the prepaid payment management process in terms of sending the RFID tag code to the server to indicate its validity, as well as calculating the remaining balance for the consumer and displaying this information in an understandable way to the consumer.


Fig. 3.12 Arduino IDE

### 3.5.2 Power Sensor ( PZET004T)

This sensor has the ability to measure the load voltage, current, power, power factor, and store energy - as explained in chapter two. This sensor uses an alternative current (AC) power source to measure the above parameters.

Table 3.1 shows the pin wiring for this sensor, and Figure 3.13 shows its circuit connection.

Table 3.1 PZEM pin out

| Pins details | Connection with the arduino mega 2560 |
|---|---|
| **5V** | Connecting to pin 5V at arduino |
| **Rx** | Connecting to pin 12 at arduino |
| **Tx** | Connecting to pin 11 at arduino |
| **GND** | Connecting to pin GND at arduino |

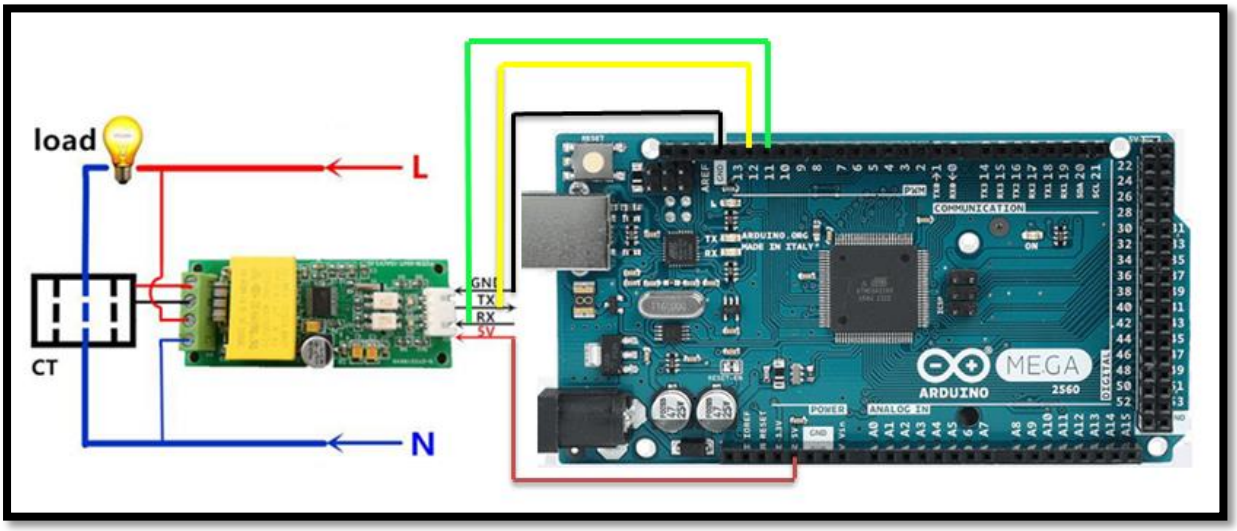



Fig. 3.13 PZEM004T/100Acircuit diagram

### 3.5.3 RFID / RC-522

The RFID / RC-522 considered one of the most important technique that used in variable applications as mentioned in chapter two. It is connected to the Arduino to activate the prepaid system as the consumer charges power to the home with this RFID card. When the RFID transponder has been brought close to the interrogator, the later sends the code to the Arduino for checking the card's validity. Then the Arduino checks this tag's validity, if it is valid, the meter will

be filled out with a new balance and shows a message on the meter LCD that the process is true. Table 3.2 shows the RC-522pins out and Figure 3.14 shows the wiring connections.

Table 3.2 RC-522 pin out

| The RC-522 pins Details | Connection with the arduino mega 2560 |
|---|---|
| **SDA** | Connecting to pin 9 at arduino |
| **SCK** | Connecting to pin 52 at arduino |
| **MOSI** | Connecting to pin 51 at arduino |
| **MISO** | Connecting to pin 50 at arduino |
| **IRQ** | No connection |
| **GND** | Connecting to pin GND at arduino |
| **RST** | Connecting to pin 8 at arduino |
| **3.3 v** | Connecting to pin 3.3v at arduino |

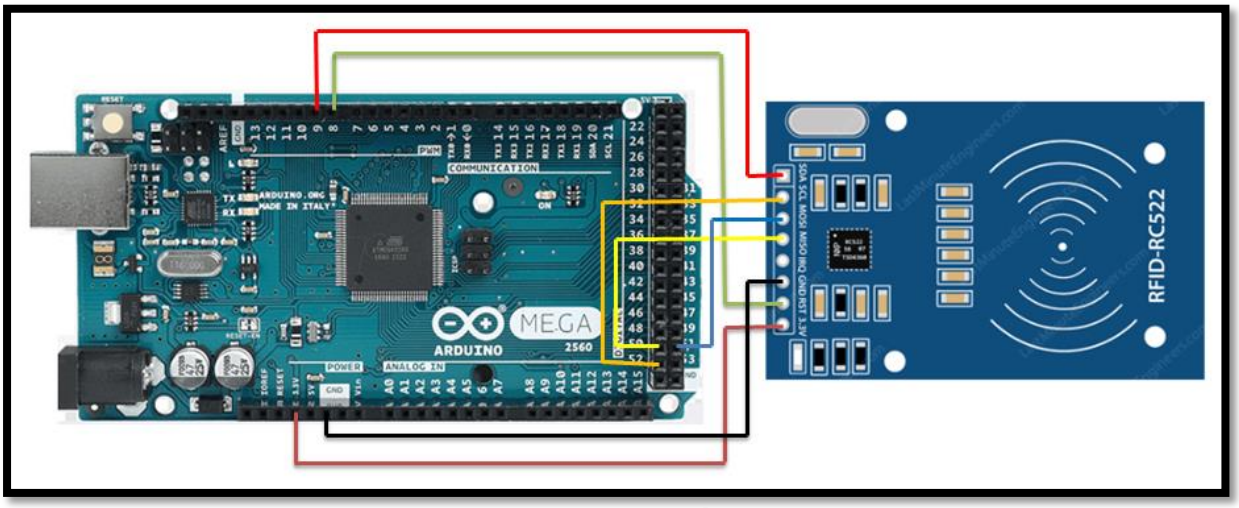



Fig. 3.14 RC-522 circuit diagram

### 3.5.4 Liquid Crystal Display ( LCD )

This part is necessary to display the required information to the consumers, such as the consumed energy in (KWh), the energy meter Balance, the rest balance, and another messages. The 128*64 7920ST model is used to be compatible with the low power consumption concept for the proposed system.

It is useful for the consumers to know whether the balance has been filled or whether the balance will run out and this requires recharging. The LCD also displays the state of electrical energy theft, as shown in the next chapter. The LCD connection to the Arduino shown in Figure 3.15 and the Table 3.3 shows the pins out.

Table 3.3 LCD pin out

| The LCD pins Details | Connection with the arduino mega 2560 |
|---|---|
| **BLK** | Connecting to pin GND at arduino |
| **BLA** | Connecting to pin 3.3v at arduino |
| **PSB** | Connecting to pin GND at arduino |
| **E** | Connecting to pin 52 at arduino |
| **RW** | Connecting to pin 51 at arduino |
| **RS** | Connecting to pin 53 at arduino |
| **VCC** | Connecting to pin 5v at arduino |
| **GND** | Connecting to pin GND at arduino |

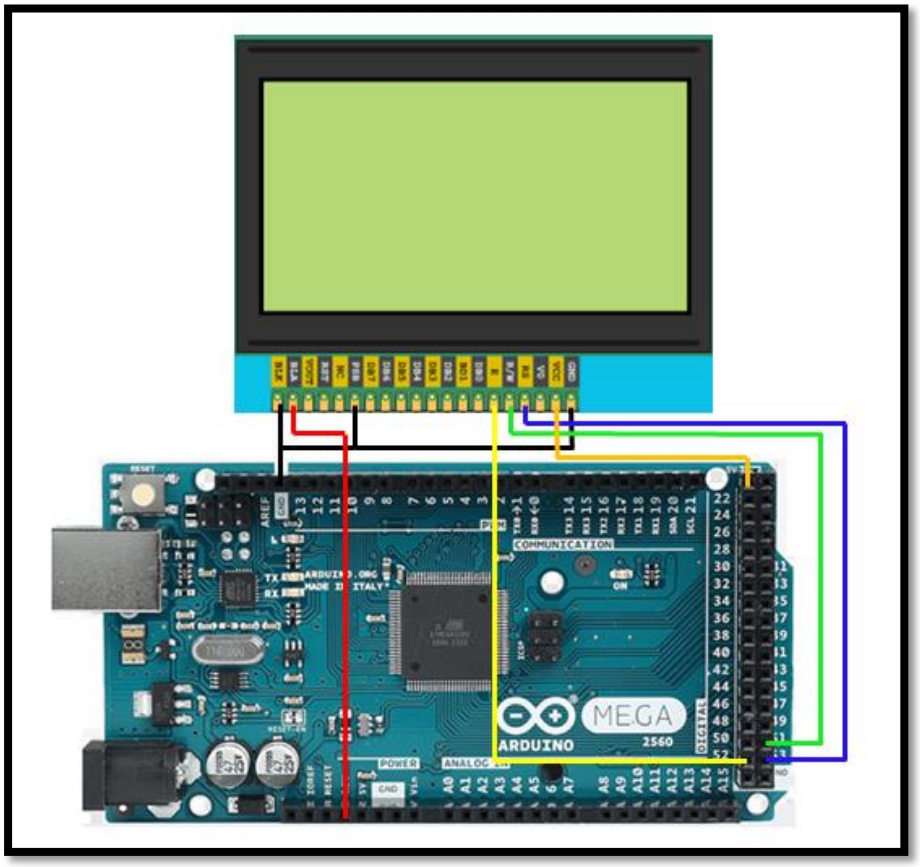



Fig. 3.15 LCD circuit diagram

### 3.5.5 Wireless Communication System by using Zigbee / XBee3

The means of communication used in the proposed system is WSNs represented in Zigbee technology, which is characterized by low power consumption, low cost, low data rate, high security, high reliability and high performance as reviewed in the previous chapter. This module has the ability to communicate in mesh network and to ensure that, the Zigbee (XBee3) has been programmed in XCTU (which is the official configuration program for the Xbee). Table 3.4 shows the Xbee3 pinout and Figure 3.16 demonstrate the Xbee3 wiring circuit with the USB adapter which connecting to Arduino.

Table 3.4 XBee3 pin out

| The xbee3 with adapter pins Details | Connection with the arduino mega 2560 |
|---|---|
| **5v** | Connecting to pin 5v at arduino |
| **GND** | Connecting to pin GND at arduino |
| **Tx** | Connecting to pin Tx1 at arduino |
| **Rx** | Connecting to pin Rx1 at arduino |

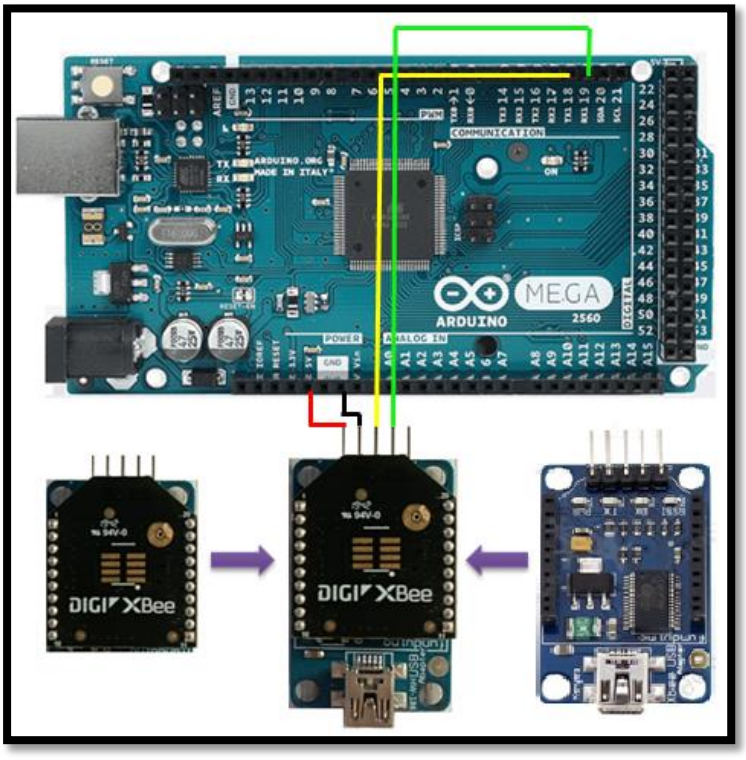



Fig. 3.16 XBee3 circuit diagram

## 3.6 XCTU Configuration

The XCTU considered the official configuration program for the Xbee. The XBee support two types of operation modes, the AT mode and the API mode as reviewed in chapter two. To communicate wirelessly between XBee modules, each one must be part of the same network. The XCTU configuration /AT mode has been used to configure the XBee modules in the proposed system. The major settings can be seen in the following Table and Figure.

Table 3.5 XBee setting

| Parameters | XBee 1 | XBee2 | XBee3 |
|---|---|---|---|
| **ID** | 2015 | 2015 | 2015 |
| **JV** | Default value | Enable [1] | Enable[1] |
| **CE** | Enable [1] | Default value | Default value |
| **DH** | Default value | 0 | 0 |
| **DL** | Default value | 0 | 0 |
| **NI** | Coordinator | Router | End device |
| **SP** | 1F4 | 1F4 | 1F4 |
| **SM** | Default value | Default value | Cyclic sleep [4] |
| **SO** | Default value | Default value | 2 |

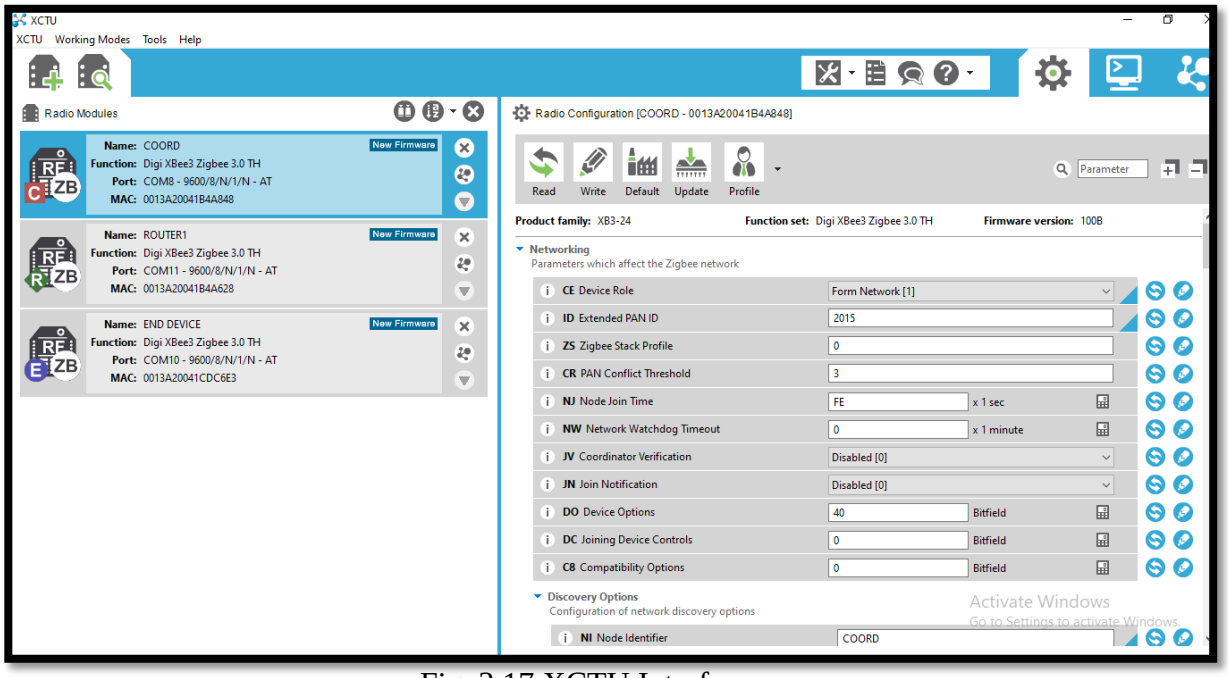



Fig. 3.17 XCTU Interface

As shown in table above, many major settings can be explained as following:

- PAN ID (ID) : This ID is define the network and must be the same for all network devices.
- Channel Verification ( JV) : This setting means that there is a coordinator in the network by set JV=1 for Routers and End devices only.
- Coordinator Enable (CE) : Set 1 for coordinator only
- Scan channel (SC) : Every node must have the same SC value.
- Sleep mode (SM) : it is useful to set SM for End devices to have a temporary sleep state and turn themselves off to save battery life.
- Node Identifier ( NI) : it is define the nodes to be easy to deal with.
- Destination address /High part ( DH)
- Destination address /Low part ( DL)
- Spent Sleeping (SP) : It is the time duration of sleep in hexadecimal.
- Sleep Option (SO) : It is set sleep option and means set the XBee awake during the period.

### 3.6.1 XCTU Configuration Steps:

- Open the XCTU program and search for XBee Module
- Select the required USB serial port then click "finish"
- After found the XBee modules, the selected modules have been added
- Configure each XBee module according to its type, coordinator, Router, or End device as reviewed before.
- After complete the Xbee modules configuration, the XBees are ready to communicate and transmit or receive data.

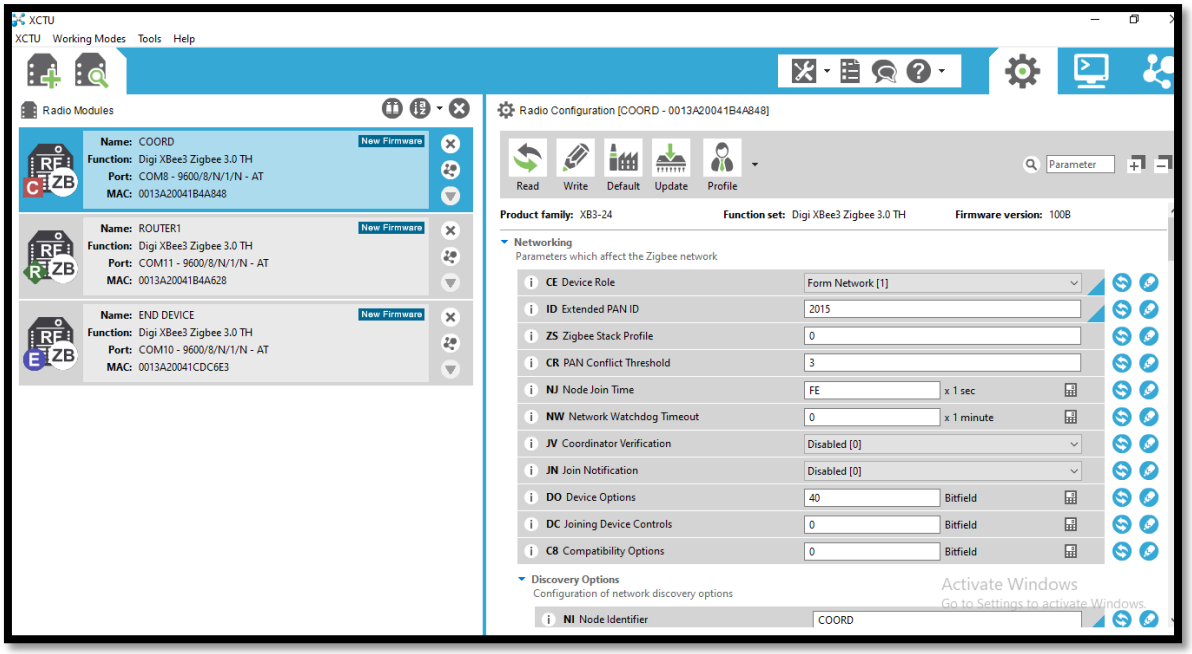



Fig. 3.18 XCTU setting

## 3.7 Graphical User Interface GUI

The GUI was built to be understandable by the persons who observe the system at the utility center. The interface consists of many parts, the security login, the received data part for CN1, CN2,and for the TN. It shows, the required information for the SN for each consumer such as consumed energy, voltage , current, power, and balance ) as shown in Figure 3.19.

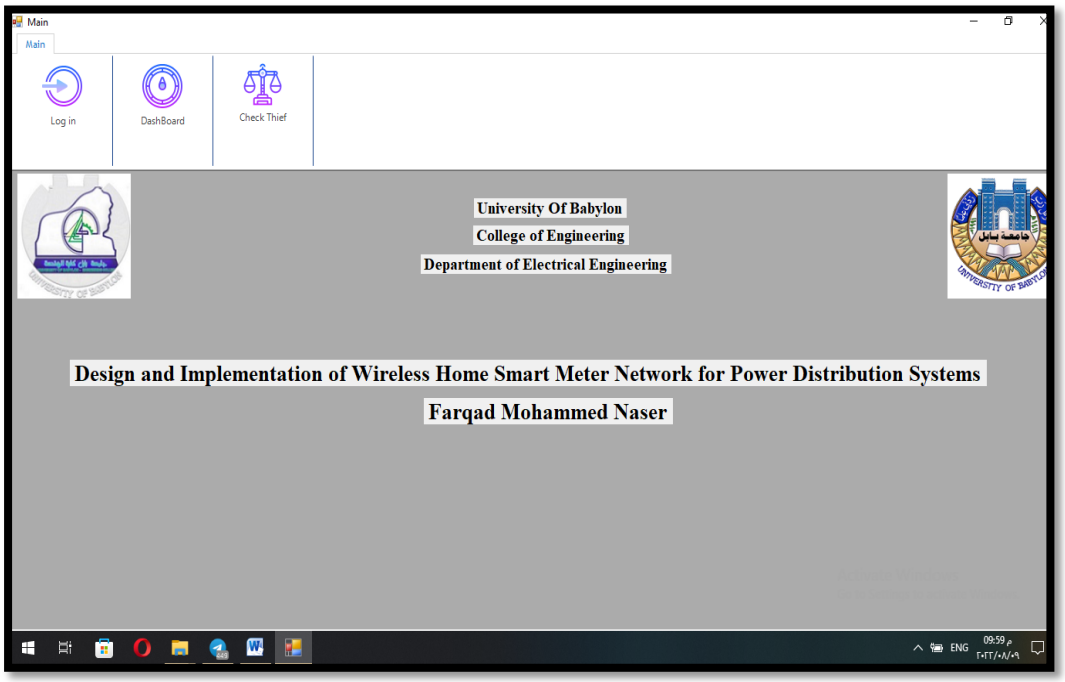



Fig. 3.19 GUI system

# Chapter Four

# Results And Discussion

# Chapter Four

# Results And Discussion

## 4.1 Introduction

The proposed system included design and implementation of two systems, the prepaid system and the anti-theft energy system with wireless data transfer system.

In practice three parts were designed and implemented. The first part is design and implementation of a smart energy meter has the ability to measure the consumed electrical energy and other parameters with high accuracy and performance and can communicate wirelessly with the other system nodes.

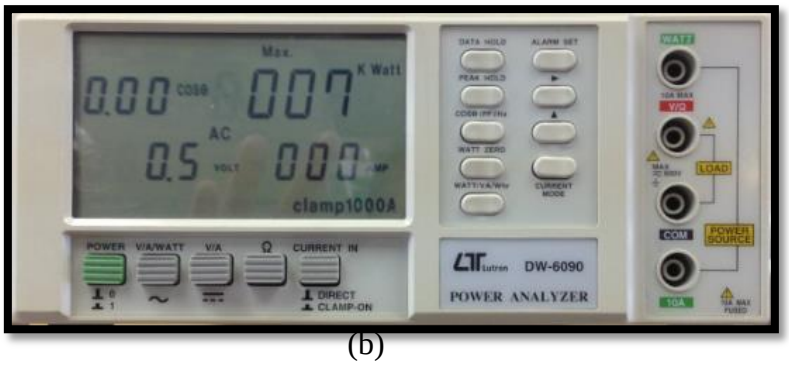
The second is the Communication part between all nodes and the third part is the Utility Center (Server).

In this chapter, we will review the most important results that were obtained as a result of applying these systems.

### 4.2 Smart Energy Meter

The smart energy meter was built in simple, low cost, high accuracy component. This meter has the ability to measure load voltage, current, frequency, power, power factor, and energy. All these measured values compared with power analyzer (LUTRON DW- 6090) which is multi-measurement as shown in Figure 4.1. For more details, show appendix (C).


(a)




(b)

(Fig.4.1 (a) Proposed smart meter (b) Power analyzer

### 4.2.1 Measured Values

The measured parameters that received by SN which are transmitted from the CN ( proposed smart meter) are the same values tested with many types of loads ( Resistive loads, Inductive loads, and Capacitive loads) as shown below with many values for each load type. The calibration is done with the power analyzer (LUTRON DW- 6090) and the percentage error was determined according to the following formula .

$$\text{percentage error} = \frac{\textbf{approximate value} - \textbf{exact value}}{\textbf{exact value}} \quad \ldots\ldots\ldots\ldots\ldots\ldots \quad (4.1)$$

In this section, the measured parameters are shown in details.


Fig. 4.2 The Proposed system test with resistive, inductive, and capacitive loads

### a) Voltage Measurements

The measured voltage by the proposed system at SN is calibrated with the power analyzer (LUTRON DW- 6090) with various loads for resistive loads, inductive loads, and capacitive loads.

- For resistive load show Table. 4.1 with percentage error.

Table 4.1 Voltage measurements for resistive load

| LOAD TYPE | LOAD VALUE | POWER ANALYZER VOLTAGE (V) | PROPOSED SYSTEM **CN** VOLTAGE (v) | PROPOSED SYSTEM **SN** VOLTAGE (v) | ERROR SN with POWER ANALYZER READINGS |
|---|---|---|---|---|---|
| **RESISTIVE LOAD** | 70 Ω | 231.3 | 232.7 | 232.7 | 0.00605 |
| | 80 Ω | 231.5 | 232.8 | 232.8 | 0.0056 |
| | 100 Ω | 230 | 231 | 231 | 0.0043 |
| | 150 Ω | 230 | 230.4 | 230.4 | 0.0017 |

- For inductive load the voltage measurements can be shown in Table 4.2

Table 4.2 Voltage measurements for inductive loads

| LOAD TYPE | LOAD VALUE | POWER ANALYZER VOLTAGE (V) | PROPOSED SYSTEM **CN** VOLTAGE (v) | PROPOSED SYSTEM **SN** VOLTAGE (v) | ERROR **SN** with POWER ANALYZER READINGS |
|---|---|---|---|---|---|
| **INDUCTIVE LOAD** | 708 mH + 150 Ω | 231.9 | 231.7 | 231.7 | 0.00086 |
| | 550 mH + 150 Ω | 231.9 | 231.9 | 231.9 | 0 |
| | 376 mH + 150 Ω | 231.7 | 231.8 | 231.8 | 0.00043 |
| | 193 mH + 150 Ω | 231.7 | 231.1 | 231.1 | 0.0026 |

- For capacitive load the voltage measurements can be shown in Table 4.3

Table 4.3 Voltage measurement in capacitive loads

| LOAD TYPE | LOAD VALUE | POWER ANALYZER VOLTAGE (V) | PROPOSED SYSTEM **CN** VOLTAGE (v) | PROPOSED SYSTEM VOLTAGE **SN** (v) | ERROR SN with POWER ANALYZER READINGS |
|---|---|---|---|---|---|
| **CAPACITIVE LOAD** | 84 µF + 150 Ω | 230.3 | 230.7 | 230.7 | 0.001737 |
| | 70 µF + 150 Ω | 229.9 | 230.2 | 230.2 | 0.001305 |
| | 56 µF+ 150 Ω | 232.5 | 232.2 | 232.2 | 0.00129 |
| | 49 µF+ 150 Ω | 229.7 | 230.8 | 230.8 | 0.00489 |
| | 28 µF + 150 Ω | 233.3 | 233.5 | 233.5 | 0.000857 |
| | 7 µF + 150 Ω | 234.3 | 234.1 | 234.1 | 0.000854 |

All the measured values by the energy sensor is root mean square (r.m.s) values. So the load type doesn't effect on the sensor measurements, because the later deals with the load magnitude only, and this fact applying for all the measurements. The error in all tables is calculated according to the formula 4.1 and it is due to the devices accuracy in all the proposed system. Taking into account, the percentage error is rather small compared with the standard meter which mean the reliability of the proposed system.

### b) Current Measurements

The currents that measured in SN were tested with resistive, inductive, and capacitive loads. It is also calibrated with the power analyzer (LUTRON DW-6090).

- For resistive load the currents measurements can be shown in Table. 4.4.

Table 4.4 Current measurements for resistive load

| LOAD TYPE | LOAD VALUE | POWER ANALYZER CURRENT (A) | PROPOSED SYSTEM **CN** CURRENT (A) | PROPOSED SYSTEM **SN** CURRENT (A) | ERROR SN with POWER ANALYZER READINGS |
|---|---|---|---|---|---|
| **RESISTIVE LOAD** | 70 Ω | 3.005 | 3.002 | 3.002 | 0.000998 |
| | 80 Ω | 2.62 | 2.62 | 2.62 | 0 |
| | 100 Ω | 2.068 | 2.07 | 2.07 | 0.000967 |
| | 150 Ω | 1.58 | 1.59 | 1.59 | 0.006329 |

- For inductive load the currents measurements can be shown in Table. 4.5.

Table 4.5 Current measurements for inductive load

| LOAD TYPE | LOAD VALUE | POWER ANALYZER CURRENTS (A) | PROPOSED SYSTEM **CN** CURRENT (A) | PROPOSED SYSTEM **SN** CURRENTS (A) | ERROR SN with POWER ANALYZER READINGS |
|---|---|---|---|---|---|
| **INDUCTIVE LOAD** | 708 mH + 150 Ω | 0.78 | 0.79 | 0.79 | 0.01282 |
| | 550 mH + 150 Ω | 0.93 | 0.94 | 0.94 | 0.010753 |
| | 376 mH + 150 Ω | 1.16 | 1.16 | 1.16 | 0 |
| | 193 mH + 150 Ω | 1.42 | 1.43 | 1.43 | 0.00704 |

- For capacitive load the currents measurements can be shown in Table 4.6.

Table 4.6 Current measurements for capacitive load

| LOAD TYPE | LOAD VALUE | POWER ANALYZER CURRENTS (A) | PROPOSED SYSTEM **CN** CURRENT (A) | PROPOSEDS YSTEM **SN** CURRENTS (A) | ERROR SN with POWER ANALYZER READINGS |
|---|---|---|---|---|---|
| **CAPACITIVE LOAD** | 84 µF + 150 Ω | 1.53 | 1.54 | 1.54 | 0.006536 |
| | 70 µF + 150 Ω | 1.5 | 1.51 | 1.51 | 0.006667 |
| | 56 µF+ 150 Ω | 1.48 | 1.49 | 1.49 | 0.006757 |
| | 49 µF+ 150 Ω | 1.43 | 1.44 | 1.44 | 0.006993 |
| | 28 µF + 150 Ω | 1.26 | 1.26 | 1.26 | 0 |
| | 7 µF + 150 Ω | 0.49 | 0.49 | 0.49 | 0 |

### C) Active Power Measurements

The active power that measured in SN were tested with resistive, inductive, and capacitive loads. It is also calibrated with the power analyzer (LUTRON DW- 6090).

- For resistive load the active power measurements can be shown in Table . 4.7.

Table 4.7 active power measurements for resistive load

| LOAD TYPE | LOAD VALUE | POWER ANALYZER POWER (W) | PROPOSED SYSTEM **CN** POWER (W) | PROPOSED SYSTEM **SN** POWER (W) | ERROR SN with POWER ANALYZER READINGS |
|---|---|---|---|---|---|
| **RESISTIVE LOAD** | 70 Ω | 703 | 701.5 | 701.5 | 0.002133 |
| | 80 Ω | 616 | 615 | 615 | 0.001623 |
| | 100 Ω | 482 | 482 | 482 | 0 |
| | 150 Ω | 366 | 366.8 | 366.8 | 0.002185 |

- For inductive load the power measurements can be shown in Table. 4.8.

Table 4.8 power measurements for inductive load

| LOAD TYPE | LOAD VALUE | POWER ANALYZER POWER (W) | PROPOSED SYSTEM **CN** POWER (W) | PROPOSED SYSTEM SN POWER (W) | ERROR SN with POWER ANALYZER READINGS |
|---|---|---|---|---|---|
| **INDUCTIVE LOAD** | 708 mH + 150 Ω | 101 | 103 | 103 | 0.019802 |
| | 550 mH + 150 Ω | 139 | 142.1 | 142.1 | 0.023.2 |
| | 376 mH + 150 Ω | 206 | 209.3 | 209.3 | 0.016019 |
| | 193 mH + 150 Ω | 305 | 306.8 | 306.8 | 0.005902 |

- For capacitive load the power measurements can be shown in Table. 4.9.

Table 4.9 power measurements for capacitive load

| LOAD TYPE | LOAD VALUE | POWER ANALYZER POWER (W) | PROPOSED SYSTEM **CN** POWER (W) | PROPOSE DSYSTEM **SN** POWER (W) | ERROR SN with POWER ANALYZER READINGS |
|---|---|---|---|---|---|
| **CAPACITIVE LOAD** | 84 µF + 150 Ω | 224 | 230.7 | 230.7 | 0.029911 |
| | 70 µF + 150 Ω | 335 | 330.3 | 330.3 | 0.014229 |
| | 56 µF+ 150 Ω | 329 | 323.1 | 323.1 | 0.017933 |
| | 49 µF+ 150 Ω | 309 | 304.3 | 304.3 | 0.01521 |
| | 28 µF + 150 Ω | 238 | 230.5 | 230.5 | 0.031513 |
| | 7 µF + 150 Ω | 38 | 34.4 | 34.4 | 0.094737 |

### d) Frequency Measurements

In table 4.10 the frequency was measured by the proposed smart meter and the power analyzer (LUTRON DW- 6090) for resistive, inductive, and capacitive load.

Table 4.10 Frequency measurement

| LOAD TYPE | LOAD VALUE | POWER ANALYZER FREQUENCY (HZ) | PROPOSED SYSTEM **CN** FREQUENCY (HZ) | PROPOSED SYSTEM **SN** FREQUENCY (HZ) | ERROR SN with POWER ANALYZER READINGS |
|---|---|---|---|---|---|
| **RESISTIVE** | 70 Ω | 50 | 49.5 | 49.9 | 0.002 |
| **INDUCTIVE** | 708 mH +150 Ω | 50 | 50 | 50 | 0 |
| **CAPACITIVE** | 84μF + 150 Ω | 49.9 | 49.9 | 49.9 | 0 |

**e) Power factor Measurements**

The power factor (PF) that measured in SN were tested with resistive, inductive, and capacitive loads. It is also calibrated with the power analyzer (LUTRON DW- 6090) as shown in Table 4.11.

Table 4.11 Power factor measurement

| LOAD TYPE | LOAD VALUE | POWER ANALYZER PF | PROPOSED SYSTEM **SN** PF | ERROR SN with POWER ANALYZER READINGS |
|---|---|---|---|---|
| **RESISTIVE** | 70 Ω | 1 | 1 | 0 |
| **INDUCTIVE** | 708 mH +150 Ω | 0.55 | 0.56 | 0.018182 |
| **CAPACITIVE** | 84μF + 150 Ω | 0.97 | 0.97 | 0 |

**f) Energy Consumption Measurements**

The consumed energy measurement is different from the other measurements, because it is cumulative while the other measured values are not cumulative, they represent the current readings only. The energy that measured in SN were tested many load types as shown in Table 4.12.

Table 4.12 Energy measurement

| Time ( hour ) | POWER ANALYZER ENERGY (KWh) | PROPOSED SYSTEM **CN** ENERGY (KWh) | PROPOSED SYSTEM **SN** ENERGY (KWh) | ERROR SN with POWER ANALYZER READINGS |
|---|---|---|---|---|
| **0** | 0 | 0 | 0 | 0 |
| **1.23** | 1 | 1 | 1 | 0 |
| **2.31** | 2 | 2.001 | 2.001 | 0.005 |
| **4** | 3 | 3.003 | 3.003 | 0.001 |
| **5.33** | 4 | 4.012 | 4.012 | 0.003 |
| **6.05** | 5 | 5.006 | 5.006 | 0.0012 |
| **8.13** | 6 | 6.031 | 6.031 | 0.05167 |
| **9.24** | 7 | 7.002 | 7.002 | 0.002857 |

### 4.2.2 Test Calibration

All the results that obtained at SN is exactly the same results that measured by the proposed smart meter which is very close to the power analyzer measurements (LUTRON DW- 6090) . These measurements are ( voltage, current, active power, power factor, frequency, and energy).

This great convergence in the results gives us an indication of that the proposed smart meter has high accuracy and efficiency, as well as the success of wireless transmission. It is possible to adopt this system in measuring the consumption of electric energy and other parameters by the competent electricity companies.

## 4.3 Utility Center ( Server ) GUI Results

As noticed in previous sections, all the results that obtained from the proposed smart meter (CN) which transmitted wirelessly to the (SN) by Zigbee mesh network are exactly the same values at both transmitting and receiving sides.

The utility center (SN) GUI which shown in Figure 4.3 is designed to show the received data from all system nodes and detect the EETh case so that the system alerts in a case of theft.

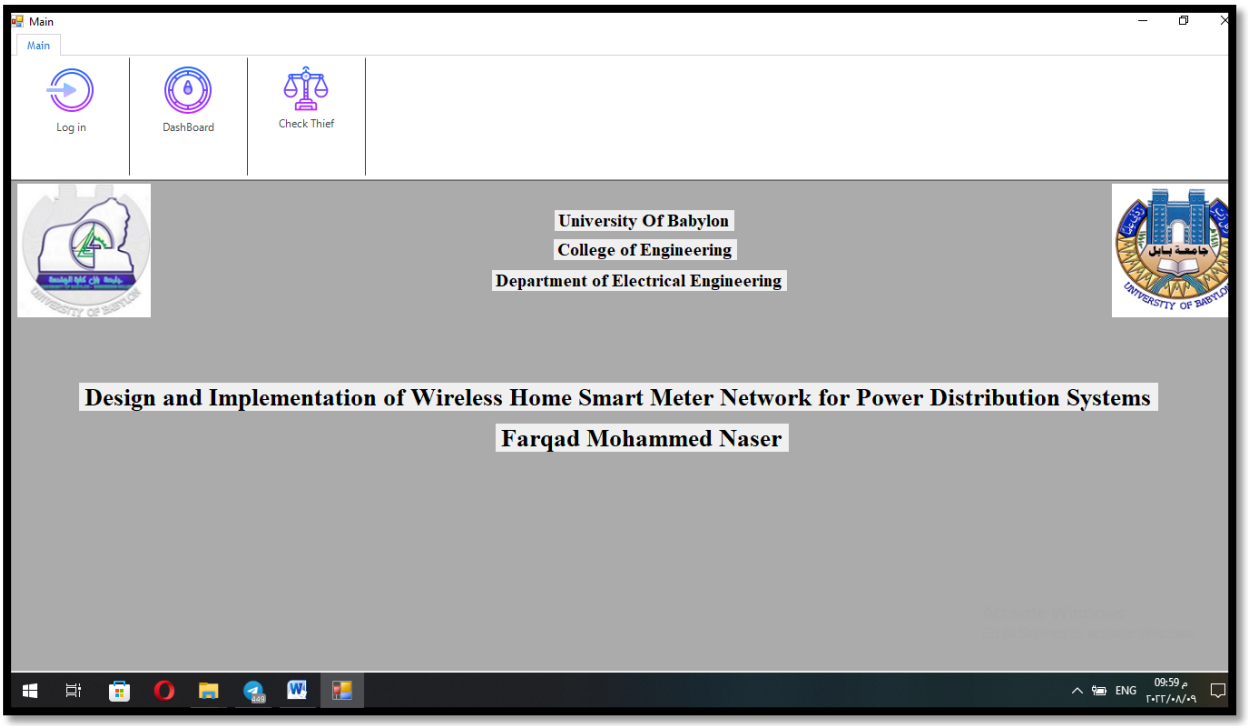



Fig. 4.3 GUI for main system

This interface is protected by a user name and password and can only be accessed by authorized persons as shown in Figure 4.4.

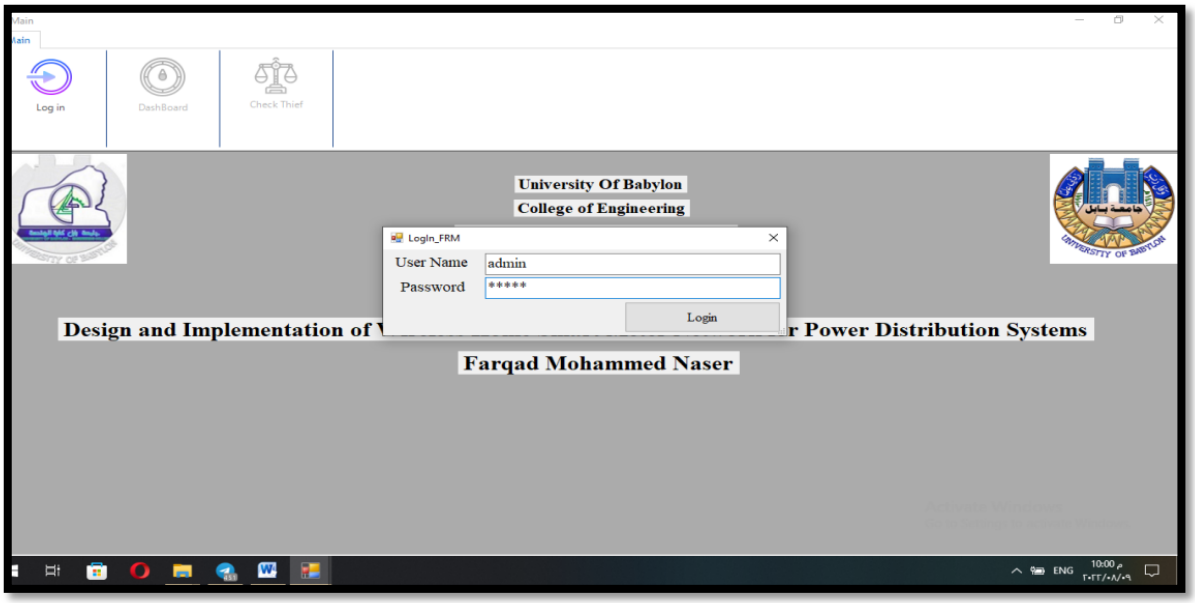



Fig. 4.4 GUI protection

### 4.3.1 Nodes Data

The Server Node (SN) contains data base includes the data for each Consumer Node (CN) in addition to the Transformer Node (TN) data that supplies the electrical power for these consumers. These data can be (voltage, current, active power, frequency, balance and energy) which were sent wirelessly to the SN by Zigbee mesh network.

- For consumer node (node 100), the data is received as shown in Figure 4.5.

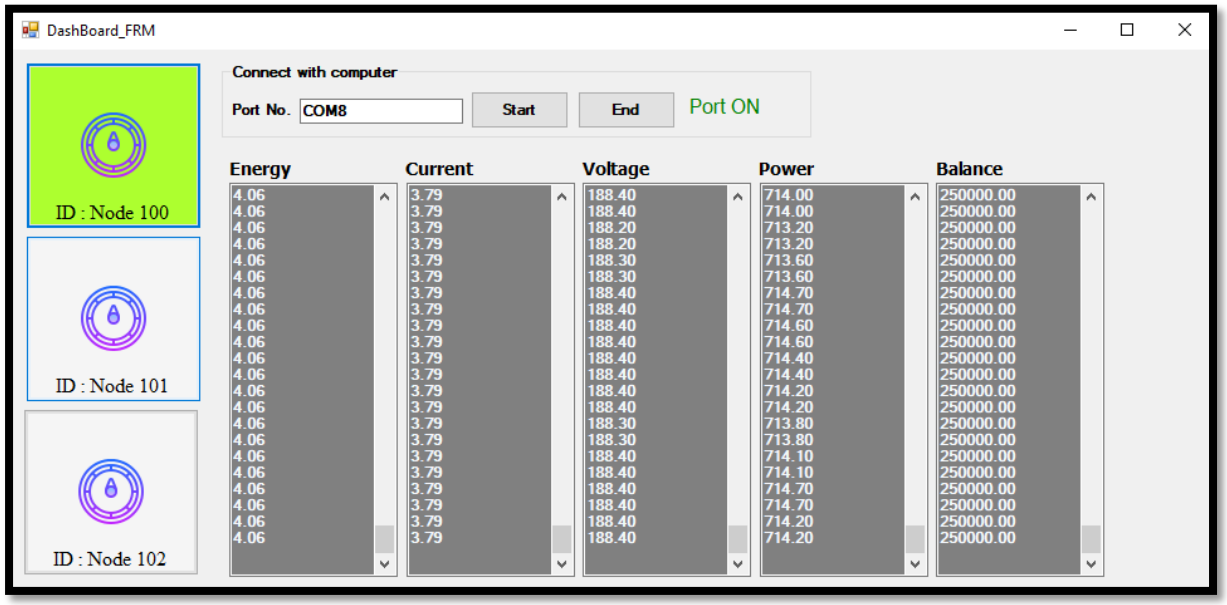



Fig. 4.5 GUI for node 100

The CN 100 transmitted data was verified with the data received by the SN and it was found that they are 100% identical, which indicates the accuracy and efficiency of the proposed system as shown before.

- For another consumer node (node 102), the data is received as shown in Figure 4.6

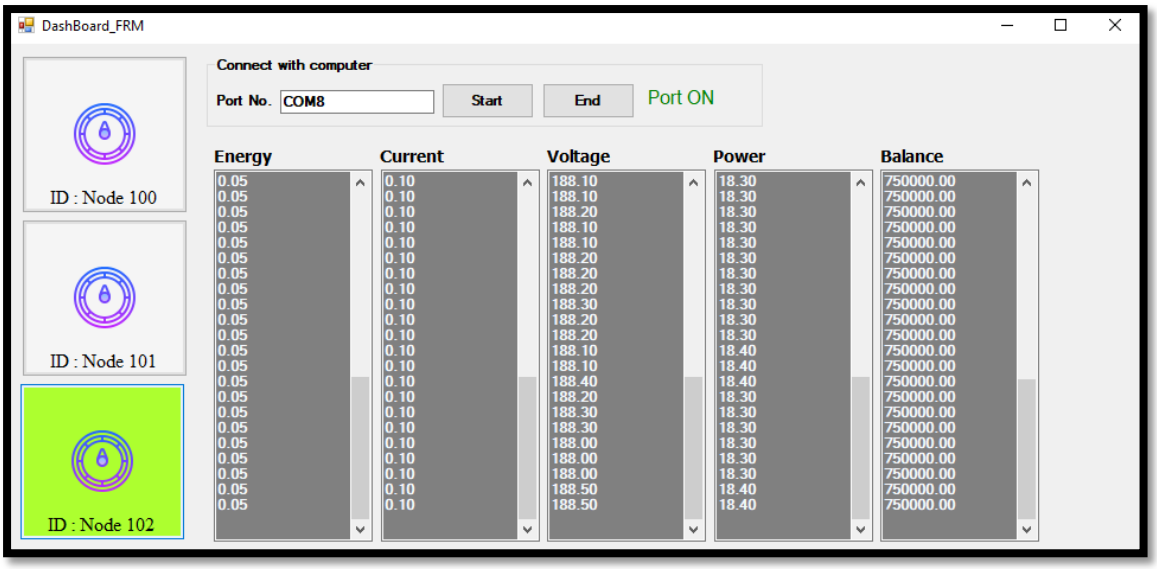



Fig. 4.6 GUI for node 102

The CN 102 transmitted and received data is also 100% identical which means that the process of transferring data between the nodes took place correctly as shown in previous article.

- The transformer node (node 101) data represents the total currents, active power and energies for all the CNs that supplied with electrical energy from this transformer as shown in Figure 4.7. Taken into account the TLs which is the devices losses ( $I^2 R$) which appears at the total amounts of currents, active power, and energies.

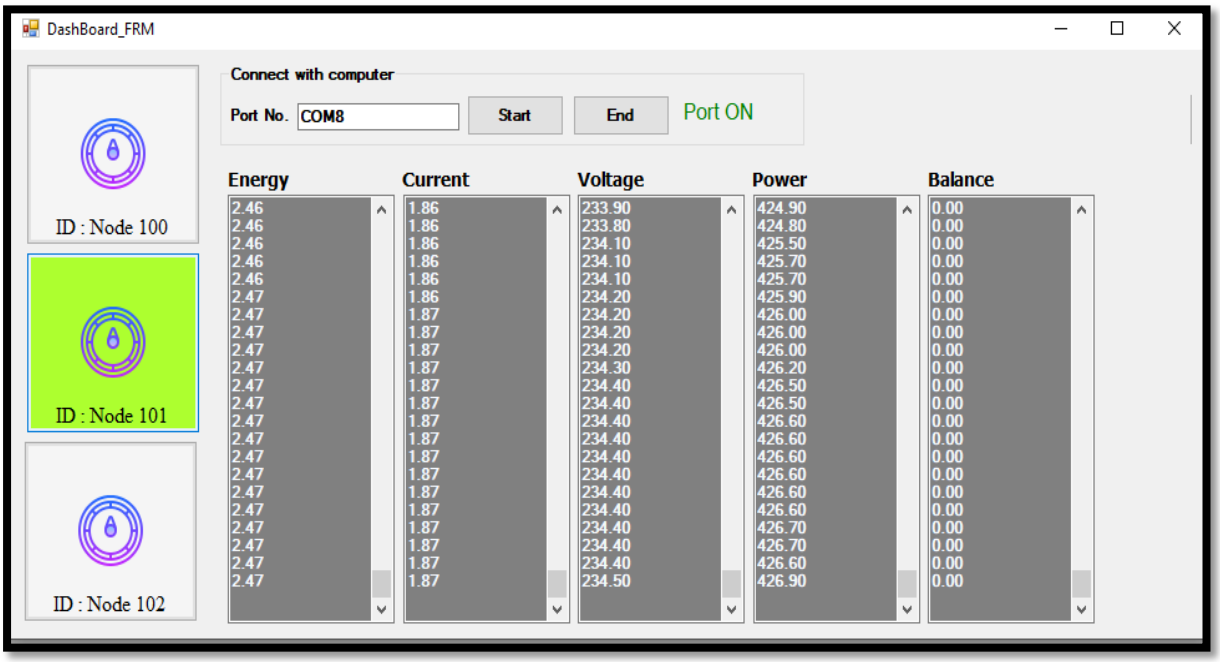



Fig. 4.7 GUI for node 101

### 4.3.2 EETh Detection

In the proposed system, it became possible to know the theft of electrical energy that occurs in the distribution line and the theft that may be occurs in each CN to be a candidate theft node after receiving all the necessary data as shown before.

**a) EETh Detection in Distribution Line TN**

After receiving and checking that all nodes data are received correctly as shown in previous section, it has become easy to detect the EETh and can determine on which distribution line (TN) did the theft take place.

As we reviewed before in chapter three, the method for detect the theft energy which is depending on the comparison between the currents. Here we will discuss two cases:

- **No Energy Theft Case** :

The difference in TN current (which represents the total currents for all consumers) comparing with the CNs currents is less than the threshold value ( which mentioned before in chapter three) that mean there is no theft detection as shown in Figure 4.8

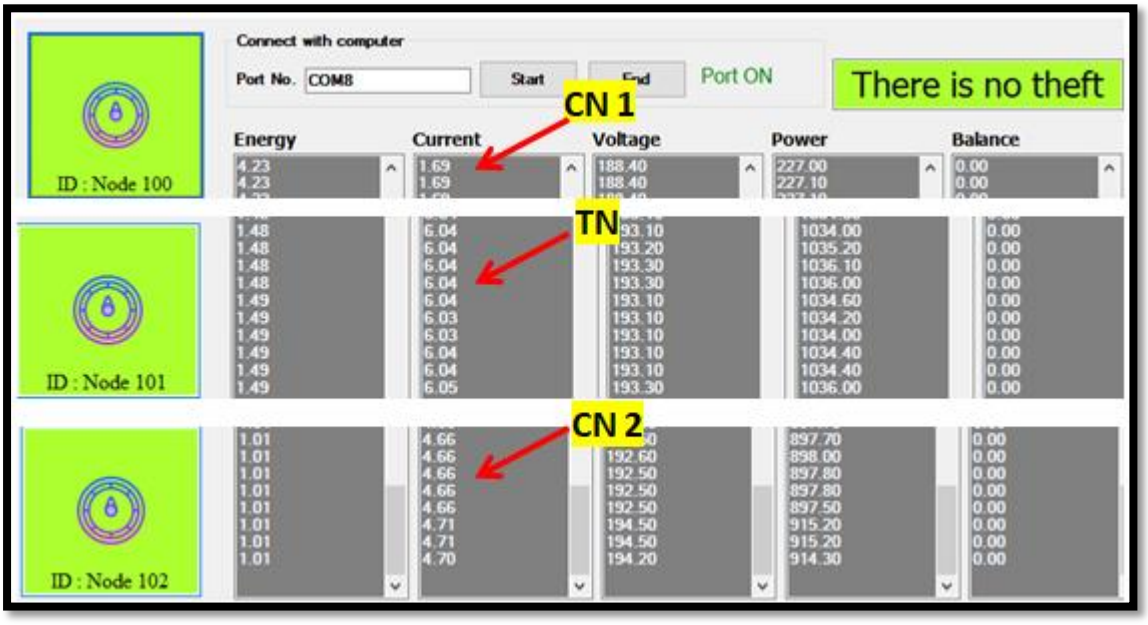



Fig. 4.8 No EETh case at TN distribution line

- **Energy Theft Case**:

The difference in TN current comparing with the CNs currents is higher than the threshold value which means there is an energy theft. When an illegal consumer steals electricity, the system senses this theft depending on the consumes current, and therefore the theft is detected. In other words, when the EETh happened ,the TN current still the same reading as no theft case , but it is captured at Utility Center. This detection is known when a comparison is made between the transmitted TN current and transmitted CN currents and then with the total currents of these transmitted data as shown in Figure 4.9.

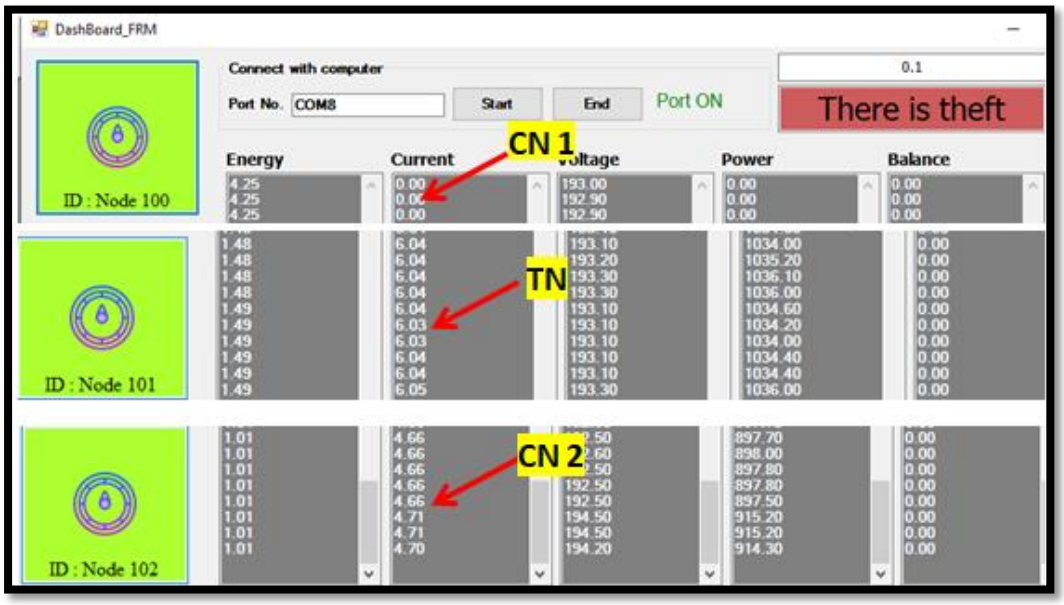



Fig. 4.9 EETh Case at TN distribution line

As shown above, the EETh detected in distribution line which is can be divided in many zones and named at server as TN 101, TN 201,TN 301, …etc.

Table 4.13 shows the EETh currents for resistive, inductive, and capacitive loads that tested and calibrated with the standard meter(LUTRON DW- 6090).

Table 4.13 The EETh test calibration

| LOAD TYPE | LUTRON DW- 6090 EETh CURRENTS (A) | PROPOSED SYSTEM SN EETh CURRENTS (A) | ERROR |
|---|---|---|---|
| **RESISTIVE** | 1.12 | 1.101 | 0.016964 |
| **INDUCTIVE** | 1.1 | 1.1 | 0 |
| **CAPACITIVE** | 1.12 | 1.11 | 0.08929 |

It is clear from the Table 4.13 that the percentage error is small, and therefore the system is able to detect thefts with high efficiency and accuracy.

**b) EETh detection for a candidate consumer node CN**

After it was discovered that the EETh occurred in any distribution line TN, it became possible to candidate the CN that may be in EETh state. In other words, in which consumer node it occurred when the current is changed.

**Case one** : when the illegal consumer turns his entire load into a theft, its data that transmitted to SN shows that the load current has become zero, the system will detect that there is an EETh state as shown in Figure 4.10

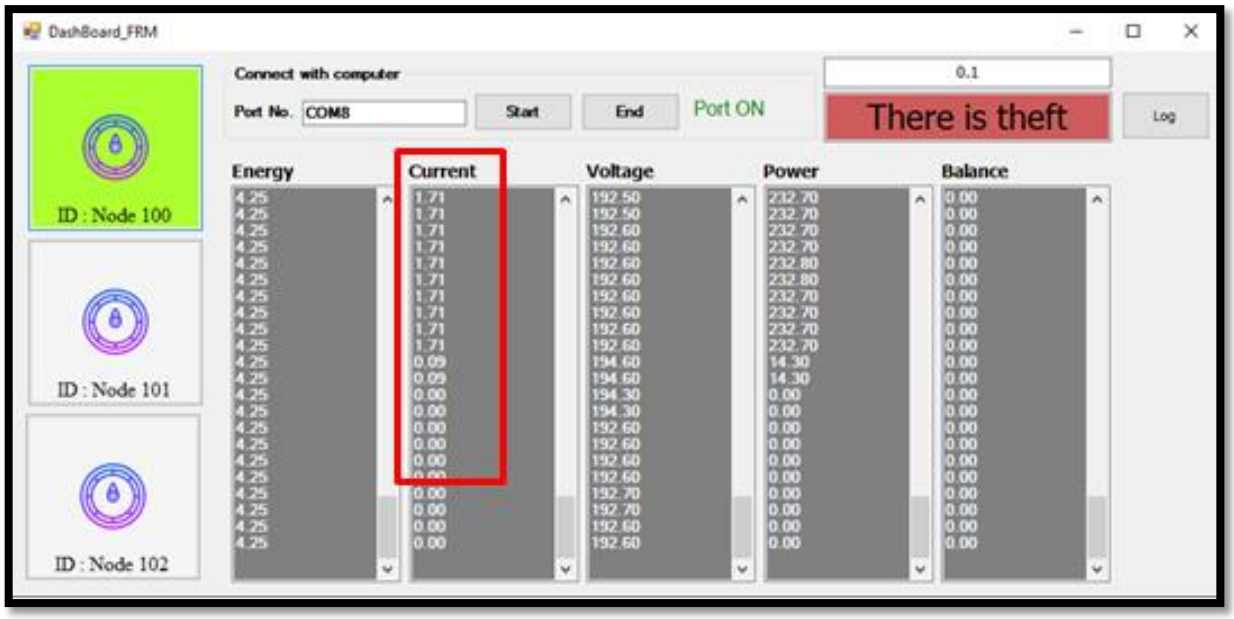



Fig. 4.10 EETh detection in CN

And The Utility center will candidate the energy theft CN as shown in Figure 4.11.

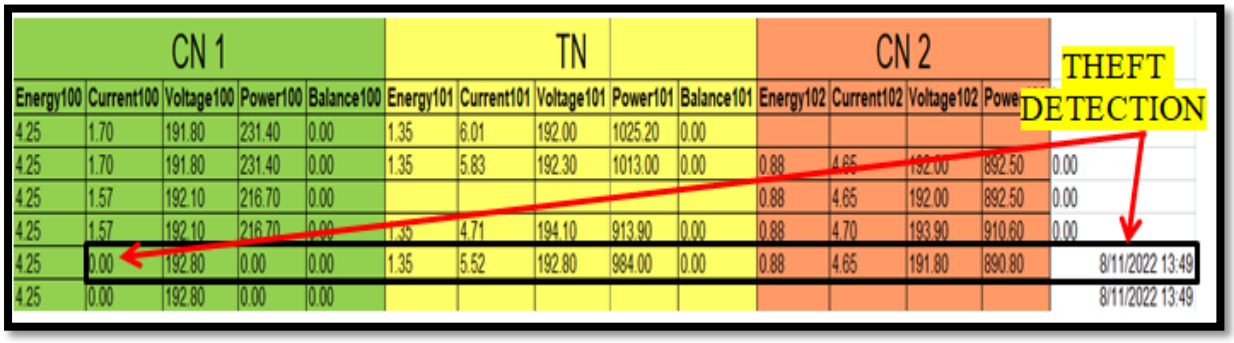



Fig. 4.11 Candidate EETh in CN1

**Case two** : when the consumer leave his house and turn off the load, the system will not decide that there is a theft state as shown in Figure 4.12


Fig. 4.12 No EETh detection in CN1

### 4.3.3 BNP System Results

This system is designed and implemented as prepaid payment by using the RFID technology.

- At the beginning, the smart meter read the energy consumption, the filled balance of that meter and the usage of that balance with comparing with

the consumed energy (as reviewed in chapter three) as shown in Figure below

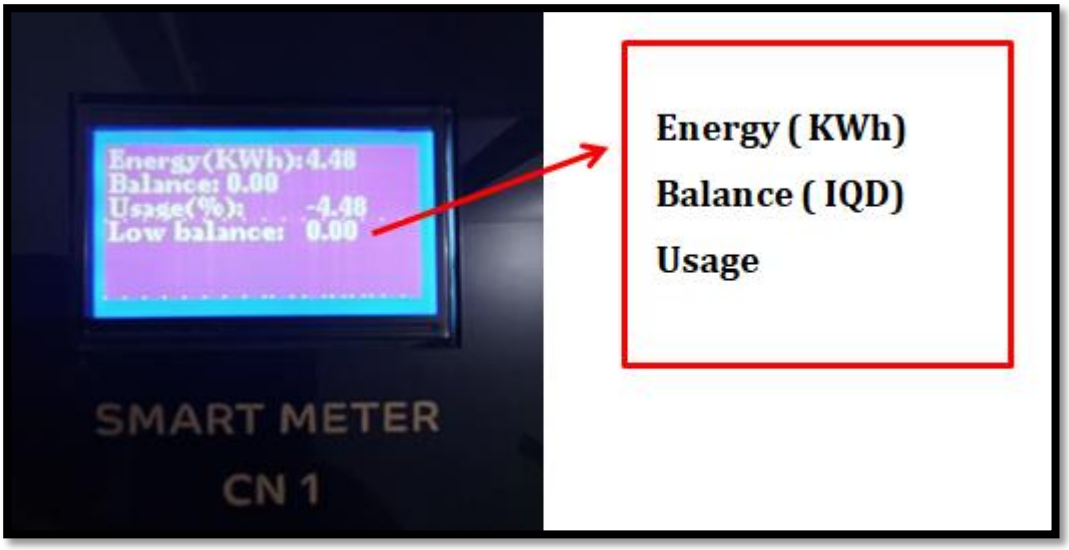



Fig. 4.13 Smart meter LCD data

The system calculate the usage until reaches to 10% of the balance, the system warns the consumer that the " **balance is low**" and requires recharging as shown in Figure 4.14.


Fig. 4.14 Low balance case

If the consumer recharge the balance, the meter displays the statement "operation successful" if the card is valid, as shown in Figure 4.15.

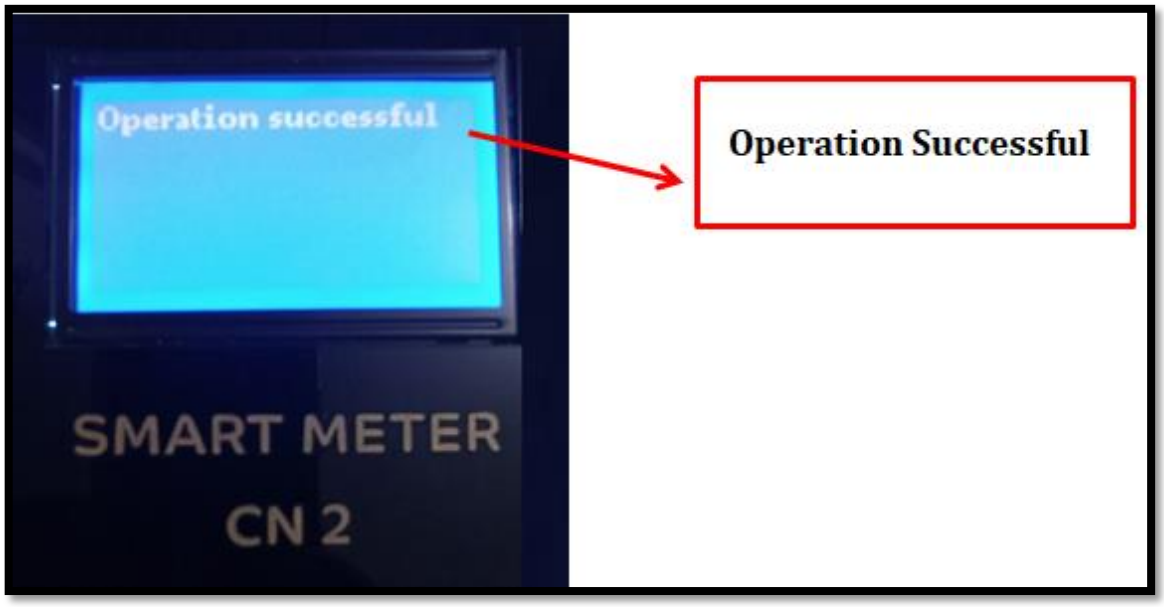



Fig. 4.15 Payment operation

## 4.4 Discussion

- The proposed system consists of three parts, the first part is design and implementation of a smart energy meter, the second part is the solution of the BNP problem, and the third part is the solution for the EETh problem.
- The smart meter was designed and implemented in low cost components with high accuracy and performance according to the obtained results and the percentage error.
- Tables 4.1 to 4.11, showed that the measured parameters by the consumer node are received at the server node without any error and calibrated with a standard meter. take into account that all the measured values are r.m.s values.
- Figures 4.7 to 4.12 shows the proposed system that solve the EETh problem.
- The proposed system for EETh uses a few sensors compared with the sensors used in reference [26] and [27].

- The proposed system for EETh uses a local network and doesn't depend on the internet or the telecommunication companies compared with almost researches.
- Figures 4.13 to 4.15 shows the proposed system that solve the BNP problem.
- The proposed system for BNP uses a local network and doesn't depend on GSM compared with references [15][16][17], and doesn't depends on the internet compared with references [19][22].
- In the proposed system the AT is used as xbee3 mode, but if the network be larger the API mode is better to use to avoid the noise.
- The system is tested and calibrated with standard meter (LUTRON DW-6090) with attendance of the supervisors.

# Chapter Five

# Conclusions And Future Works

# Chapter Five

# Conclusions And Future Works

## 5.1 Conclusions

This thesis can be summarized into the following aspects :

- The proposed system is designed and implemented to solve the non-technical losses (NTLs) problems, the billing non-payment (BNP) problem and the electrical energy theft (EETh) problem.
- The proposed system greatly contributed to finding a solution to the EETh problem occurring in the distribution line (TN) and candidate this energy theft in which the CN occurred.
- The proposed system enabled the Electricity Corporation to limit the areas of electrical energy theft from a large city to a small area that does not exceed two streets, in other words, from a large area containing hundreds of transformers feeding electrical energy to one transformer in which electrical energy theft occurred.
- All operations of the proposed system were done automatically without human intervention, which significantly reduced the percentage of errors that were occurring as a result of traditional systems in collecting meter readings and organizing payment bills, as well as thefts that occur on the electrical network.
- The proposed system was designed and implemented in low cost components with high accuracy. The CN costs about 90 US dollar, the TN costs about 65 US, while the SN costs about 50 US dollar without the computer price.
- The proposed system was implemented using few sensors compared to other works that used many sensors to achieve the same purpose.

- The system GUI is secured and easy to use by the authorized with the ability to save the data in the form of an excel file.
- The proposed system is depending on WSNs only without rely on the internet or the telecommunication companies which gives powerful advantages over the previous researches.
- The system is secured and hard to attack by the hackers because the system is not connected to the Internet, and considered as a local network.
- The proposed system is designed so that data cannot be lost without access to the server, and this is one of the advantages of the Zigbee mesh network.

## 5.2 Future Works

- Design and implementation a three phase smart energy meter able to be a prepaid and theft detection meter.
- Improving the electrical distribution networks to be suitable for detecting and locating the irregular consumer and adding an immediate fine to deter violators
- Design and implementation a smart power system capable of optimal management of consumer loads in case of the electrical energy lack.

# References

## References


[1] M. S. Saeed, M. W. Mustafa, N. N. Hamadneh, N. A. Alshammari, U. U. Sheikh, T. A. Jumani, *et al.*, "Detection of Non-Technical Losses in Power Utilities—A Comprehensive Systematic Review," *Energies*, vol. 13, no.18, pp.1-25, 2020.

[2] F. d. S. Savian, J. C. M. Siluk, T. B. Garlet, F. M. do Nascimento, J. R. Pinheiro, and Z. Vale, "Non-technical losses: A systematic contemporary article review," *Renewable and Sustainable Energy Reviews*, vol. 147, pp. 1-13, 2021.

[3] X. Lei, A. Khan, W. Xie, S. Aftab Qureshi, M. Ilyas, J. Lin, *et al.*, "Designing and Modeling of Automated Anti-theft Electricity Distribution System," *MATEC Web of Conferences*, vol. 160, pp. 1-5, 2018.

[4] A. J. Pansini, *Power transmission and distribution*: River Publishers, 2020.

[5] R. Raju, P. Madhumathy, and G. Pavithra, "A Comparison of Smart Electricity Billing Systems," in *2020 International Conference on System, Computation, Automation and Networking (ICSCAN)*, pp. 1-5, 2020.

[6] N. Baloyi, S. D. Chowdhury, J. Mnisi, and T. Mashee, "Design of GSM Based Energy Meter: A Review," *6th IEEE International Energy Conference (ENERGYCon)*, pp. 836-840, 2020.

[7] G. Peter and S. Bin Iderus, "Design of enhanced energy meter using GSM prepaid system and protective relays," *Materials Today: Proceedings*, vol. 39, pp. 582-589, 2021.

[8] G. A. Naidu and J. Kumar, "Wireless Protocols: Wi-Fi SON, Bluetooth, ZigBee, Z-Wave, and Wi-Fi," vol. 65, pp. 229-239, 2019.

[9] L. Duarte Soares, A. de Souza Queiroz, G. P. López, E. M. Carreño-Franco, J. M. López-Lezama, and N. Muñoz-Galeano, "BiGRU-CNN Neural Network Applied to Electric Energy Theft Detection," *Electronics*, vol. 11, p. 693, 2022.

[10] X. Kong, X. Zhao, C. Liu, Q. Li, D. Dong, and Y. Li, "Electricity theft detection in low-voltage stations based on similarity measure and DT-KSVM," *International Journal of Electrical Power & Energy Systems,* vol. 125, p. 1-11, 2021.

[11] P. Semwal, S. Palit, S. Indulkar, and S. Senthilmurugan, "Smart Metering in Smart Grid," *International Journal of Engineering and Advanced Technology (IJEAT) ISSN,* vol. 8, no. 4, pp. 1020-1027, 2019.

[12] C. H. Park and T. Kim, "Energy theft detection in advanced metering infrastructure based on anomaly pattern detection," *Energies,* vol. 13, no. 13,pp. 1-10, 2020.

[13] A. Althobaiti, A. Jindal, A. K. Marnerides, and U. Roedig, "Energy Theft in Smart Grids: A Survey on Data-Driven Attack Strategies and Detection Methods," *IEEE Access,* vol. 9, pp. 159291-159312, 2021.

[14] J. K. Mishra, S. Goyal, V. A. Tikkiwal, and A. Kumar, "An IoT Based Smart Energy Management System," in *2018 4th International Conference on Computing Communication and Automation (ICCCA)*, , pp. 1-3, 2018.

[15] P. Pramod Kumar and K. Sagar, "A Proficient and Smart Electricity Billing Management System," vol. 3, pp. 156-160, 2020.

[16] N. Mahfuz, M. Nigar, and N. Ulfat, "Smart Energy Meter and Digital Billing System for Bangladesh," in *2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, pp. 1-4,2020.

[17] B. M. Waheib and N. I. Abdulkhaleq, "A global system for mobile communications-based electrical power consumption for a non-contact smart billing system," *International Journal of Electrical & Computer Engineering (2088-8708),* vol. 11, no. 6, pp 4659-4666,2021.

[18] P. S. Vaidya, C. S. Kature, S. G. Waghmare, and M. S. Dhumane, "IoT Based Energy Meter Billing System," *International Journal of*

*Advance Scientific Research and Engineering Trends*, vol. 4,no. 5, pp. 4-6, 2020.

[19] V. V. Gavhane, M. R. Kshirsagar, G. M. Kale, S. Katangle, S. Deosarkar, and S. Nalbalwar, "IoT based Energy Meter with Smart Monitoring of Home Appliances," in *2021 6th International Conference for Convergence in Technology (I2CT)*, pp. 1-5,2021.

[20] G. M. Jasim and K. K. Abdalla, "Single phase energy smart meter system design and implementation using RFID and based on IoT," in *IOP Conference Series: Materials Science and Engineering*, vol. 1090, no. 1,2021.

[21] S. J. Danbatta and A. Varol, "Comparison of Zigbee, Z-Wave, Wi-Fi, and bluetooth wireless technologies used in home automation," in *2019 7th International Symposium on Digital Forensics and Security (ISDFS)*, pp. 1-5,2019.

[22] S. S. Chowdary, M. A. Abd El Ghany, and K. Hofmann, "Iot based wireless energy efficient smart metering system using zigbee in smart cities," in *2020 7th International Conference on Internet of Things: Systems, Management and Security (IOTSMS)*, pp. 1-4,2020.

[23] K. N. Shaikh and I. Mustafa, "Design and Implementation of RFID and GSM based Smart Prepaid Energy Meter," *International Journal of Electrical Engineering & Emerging Technology*, vol. 4, pp. 33-36, 2021.

[24] D. Zangmo, C. Dem, S. Thinley, and R. Chhetri, "Feasibility Study of Prepaid Energy Meter in Bhutan.", vol. 3, no. 4, pp. 1-4, 2020

[25] A. Bin-Halabi, A. Nouh, and M. Abouelela, "Remote detection and identification of illegal consumers in power grids," *IEEE Access*, vol. 7, pp. 71529-71540, 2019.

[26] N. K. Mucheli, U. Nanda, D. Nayak, P. Rout, S. Swain, S. Das, *et al.*, "Smart power theft detection system," in *2019 Devices for Integrated Circuit (DevIC)*, pp. 302-305,2019.

[27] J. Y. Kim, Y. M. Hwang, Y. G. Sun, I. Sim, D. I. Kim, and X. Wang, "Detection for non-technical loss by smart energy theft with intermediate monitor meter in smart grid," *IEEE Access*, vol. 7, pp. 129043-129053, 2019.

[28] M. B. Shahid, M. O. Shahid, H. Tariq, and S. Saleem, "Design and development of an efficient power theft detection and prevention system through consumer load profiling," in *2019 International Conference on Electrical, Communication, and Computer Engineering (ICECCE)*, pp. 1-6,2019.

[29] W. Li, T. Logenthiran, V.-T. Phan, and W. L. Woo, "A novel smart energy theft system (SETS) for IoT-based smart home," *IEEE Internet of Things Journal*, vol. 6, pp. 5531-5539, 2019.

[30] R. Punmiya and S. Choe, "Energy theft detection using gradient boosting theft detector with feature engineering-based preprocessing," *IEEE Transactions on Smart Grid*, vol. 10, pp. 2326-2329, 2019.

[31] J. Tao and G. Michailidis, "A statistical framework for detecting electricity theft activities in smart grid distribution networks," *IEEE Journal on Selected Areas in Communications*, vol. 38, pp. 205-216, 2019.

[32] M. Uvais, "Controller based power theft location detection system," in *2020 International Conference on Electrical and Electronics Engineering (ICE3)*, pp. 111-114,2020.

[33] S. O. Tehrani, M. H. Y. Moghaddam, and M. Asadi, "Decision tree based electricity theft detection in smart grid," in *2020 4th International Conference on Smart City, Internet of Things and Applications (SCIOT)*, pp. 46-51,2020.

[34] M. A. Salam and Q. M. Rahman, *Fundamentals of electrical circuit analysis*: Springer, 2018.

[35] S. Muralidhara, N. Hegde, and P. Rekha, "An internet of things-based smart energy meter for monitoring device-level consumption of energy," *Computers & Electrical Engineering*, vol. 87, p. 1-10, 2020.

[36] Frenzel Jr, L. E. (2008). *Principles of Electronic Communication Systems, pp.504, 2008.*

[37] S. R. Jondhale, R. Maheswar, and J. Lloret, "Fundamentals of Wireless Sensor Networks," in *Received Signal Strength Based Target Localization and Tracking Using Wireless Sensor Networks*, ed: Springer, pp.1-19,2022.

[38] A. Pang, F. Chao, H. Zhou, and J. Zhang, "The method of data collection based on multiple mobile nodes for wireless sensor network," *IEEE Access*, vol. 8, pp. 14704-14713, 2020.

[39] N. Heydarishahreza, S. Ebadollahi, R. Vahidnia, and F. J. Dian, "Wireless Sensor Networks Fundamentals: A Review," in *2020 11th IEEE Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, pp. 0001-0007,2020.

[40] M. Naghibi and H. Barati, "EGRPM: Energy efficient geographic routing protocol based on mobile sink in wireless sensor networks," *Sustainable Computing: Informatics and Systems*, vol. 25, p. 1-10, 2020.

[41] D. Kandris, C. Nakas, D. Vomvas, and G. Koulouras, "Applications of wireless sensor networks: an up-to-date survey," *Applied System Innovation*, vol. 3, p. 14, 2020.

[42] K. Gulati, R. S. K. Boddu, D. Kapila, S. L. Bangare, N. Chandnani, and G. Saravanan, "A review paper on wireless sensor network techniques in Internet of Things (IoT)," *Materials Today: Proceedings*,pp. 1-5 2021.

[43] B. Chander and G. Kumaravelan, "Outlier detection strategies for WSNs: A survey," *Journal of King Saud University-Computer and Information Sciences*,pp. 1-23, 2021.

[44] M. Javaid, A. Haleem, S. Rab, R. P. Singh, and R. Suman, "Sensors for daily life: a review," *Sensors International*, vol. 2, p. 100121, 2021.

[45] S. Ratnaparkhi, S. Khan, C. Arya, S. Khapre, P. Singh, M. Diwakar, *et al.*, "Smart agriculture sensors in IOT: A review," *Materials Today: Proceedings,*pp. 1-6, 2020.

[46] F. Ohnhäuser, *Analog-digital converters for industrial applications including an introduction to digital-analog converters*: Springer, 2015.

[47] Z. Yin, Y. M. Wang, and E. R. Fossum, "Low bit-depth adcs for multi-bit quanta image sensors," *IEEE Journal of Solid-State Circuits,* vol. 56, pp. 950-960, 2021.

[48] W. Dargie and C. Poellabauer, *Fundamentals of wireless sensor networks: theory and practice*: John Wiley & Sons, 2010.

[49] M. Maheepala, M. A. Joordens, and A. Z. Kouzani, "Low power processors and image sensors for vision-based iot devices: a review," *IEEE Sensors Journal,* vol. 21, pp. 1172-1186, 2020.

[50] N. Mukherjee, S. Neogy, and S. Roy, *Building wireless sensor networks: theoretical and practical perspectives*: CRC Press, pp.5, 2017.

[51] K. Al-Ani, A. Abdalkafor, and A. Nassar, "An overview of wireless sensor network and its applications," *Indonesian Journal of Electrical Engineering and Computer Science,* vol. 17, pp. 1480-1486, 2020.

[52] S. Prakash, "Zigbee based wireless sensor network architecture for agriculture applications," in *2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT)*, pp. 709-712, 2020.

[53] H. Landaluce, L. Arjona, A. Perallos, F. Falcone, I. Angulo, and F. Muralter, "A review of IoT sensing applications and challenges using RFID and wireless sensor networks," *Sensors,* vol. 20, p. 2495, 2020.

[54] H. Haque, K. Labeeb, R. B. Riha, and M. N. R. Khan, "IoT based water quality monitoring system by using Zigbee protocol," in *2021 International Conference on Emerging Smart Computing and Informatics (ESCI)*, pp. 619-622, 2021.

[55] E. Kabalcı, Y. Kabalcı, and P. Siano, "Design and implementation of a smart metering infrastructure for low voltage microgrids," *International Journal of Electrical Power & Energy Systems,* vol. 134, p. 107375, 2022.

[56] M. S. Gomes, R. L. de Paula, and J. C. Leite, "Development of an Intelligent Mobile Robot Prototype for Indoor Material Transportation." vol. 11, issue 10, pp.56-86, 2021.

[57] A. S. Mustafa, M. M. Al-Heeti, and M. M. Hamdi, "A new approach for smart electric meter based on Zigbee," *Bulletin of Electrical Engineering and Informatics,* vol. 11, 2022.

[58] D. Gislason, *Zigbee wireless networking*: Newnes, 2008.

[59] M.-S. Pan and Y.-C. Tseng, "ZigBee and their applications," in *Sensor Networks and Configuration*, ed: Springer, pp. 349-368,2007.

[60] S. Shrestha and S. Shakya, "Technical analysis of ZigBee wireless communication," *Journal of trends in Computer Science and Smart technology (TCSST),* vol. 2, pp. 197-203, 2020.

[61] R. Faludi, *Building wireless sensor networks: with ZigBee, XBee, arduino, and processing*: " O'Reilly Media, Inc.", 2010.

[62] G.,Shi, & K, Li (2017). Signal interference in WiFi and ZigBee networks. Cham, Switzerland: Springer International Publishing. (pp. 9-27), 2017.

[63] V. M. Mishra and A. Kumar, "Zigbee internode communication and FPGA synthesis using mesh, star and cluster tree topological chip," *Wireless Personal Communications,* vol. 119, pp. 1321-1339, 2021.

[64] T. Kumar and P. Mane, "ZigBee topology: A survey," in *2016 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT)*, pp. 164-166, 2016.

[65] S. Farahani, *ZigBee wireless networks and transceivers*: newnes, pp. 81-82, 2011.

[66] C. Bell, *Beginning Sensor Networks with XBee, Raspberry Pi, and Arduino*: Springer, 2020.

[67] G. Kanagachidambaresan, "Introduction to Wired and Wireless IoT Protocols in SBC," in *Role of Single Board Computers (SBCs) in rapid IoT Prototyping*, ed: Springer, pp. 99-120, 2021.

[68] M. Nekrasov, R. Allen, I. Artamonova, and E. Belding, "Optimizing 802.15. 4 outdoor IoT sensor networks for aerial data collection," *Sensors*, vol. 19, p. 3479, 2019.

[69] S. F. Barrett, "Arduino I: Getting Started," *Synthesis Lectures on Digital Circuits and Systems*, vol. 15, pp. 1-222, 2020.

[70] J. Cicolani and J. Cicolani, *Beginning Robotics with Raspberry Pi and Arduino*: Springer, 2018.

[71] G. Stefanov and V. Cingoski, "WI-FI Smart Power Meter," 2021.

[72] K.-K. Duan and S.-Y. Cao, "Emerging RFID technology in structural engineering–A review," in *Structures*, pp. 2404-2414,2020.

[73] A. Lozano-Nieto, *RFID design fundamentals and applications*: CRC press, 2017.

[74] Zheng, F., & Kaiser, T. (2016). *Digital Signal Processing for RFID*. John Wiley & Sons, 2016.

[75] A. Elizarov, S. Bashkevich, I. Lavrukhin, A. Larionov, and V. Karavashkina, "Development of intelligent RFID-system for logistics Processes," in *2019 Systems of signals generating and processing in the field of on board communications*, pp. 1-5,2019.

[76] S. Monk, *Hacking Electronics: Learning Electronics with Arduino and Raspberry Pi*: McGraw-Hill Education, 2017.

[77] T. E. Rani, R. Rao, and M. A. Rani, "A Novel Approach to Integrate Measuring Instruments onto Single SoC," *CVR Journal of Science and Technology*, vol. 1, pp. 41-44, 2011.

[78] A. Subero, "Display Interfacing," in *Programming Microcontrollers with Python*, ed: Springer, pp. 209-230,2021.

[79] M. Rodríguez Fernández, E. Zalama Casanova, and I. González Alonso, "Review of display technologies focusing on power consumption," *Sustainability*, vol. 7, pp. 10854-10875, 2015.

[80] W. O. Galitz, *The essential guide to user interface design: an introduction to GUI design principles and techniques*: John Wiley & Sons, 2007.

# Appendixes

## Appendix (A) Xbee3

## Appendix (B) PZEM-004T V3.0

## Appendix (C) Standard Meter (LUTRON DW- 6090)

# Appendix (A) Xbee3

# DIGI XBEE 3 ZIGBEE 3.0

## Easy-to-add connectivity in a compact, low-power, low-profile footprint

Digi XBee® 3 modules accelerate time to market for designers, OEMs and solution providers by quickly enabling wireless connectivity and easy-to-add functionality. Building on industry-leading technology, pre-certified Digi XBee 3 modules offer the flexibility to switch between multiple frequencies and wireless protocols as needed.

Digi XBee 3 Zigbee 3.0 offers a fully interoperable ecosystem covering all vertical markets including building automation, smart energy, digital health, intelligent lighting, and others.

With Digi Remote Manager®, Digi XBee 3 modules can be easily configured and controlled from a simple, central platform. Built-in Digi TrustFence® security, identity and data privacy features use more than 175 controls to protect against new and evolving cyberthreats. MicroPython and XCTU software tools simplify adding functionality, configuration and testing.

From edge computing to future migration, Digi XBee modules offer size, weight, power and performance advantages ideal for scalable device connectivity. A versatile addition to the expanding Digi XBee Ecosystem of wireless modules, adapters and software, the Digi XBee 3 Series is engineered to accelerate development and deployment.

### SIZE AND FLEXIBILITY

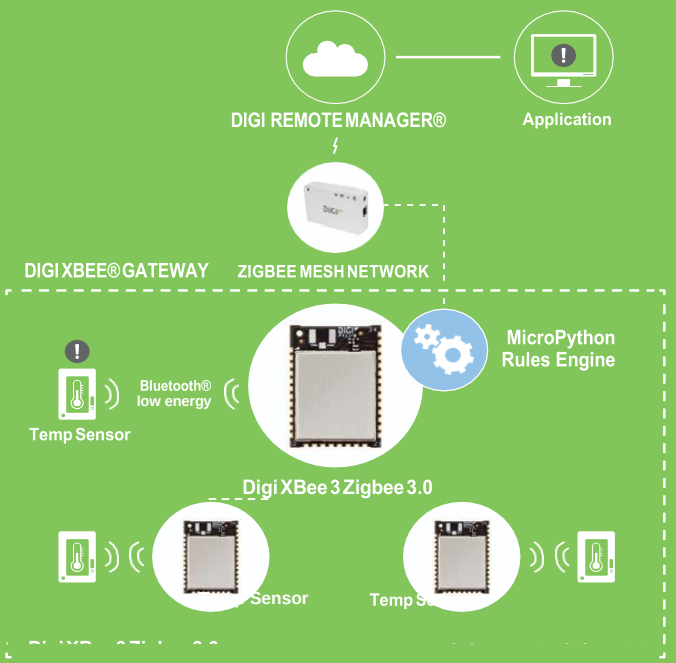
- At 13mm x 19mm, the new Digi XBee® 3 micro form factor allows for more compact and portable applications
- Digi XBee 3 is one module for all protocols including: Zigbee, 802.15.4, DigiMesh® and BLE, all configurable via Digi XCTU

### PROGRAMMABILITY

- Eliminate the need for an external microcontroller and create smart end nodes using MicroPython

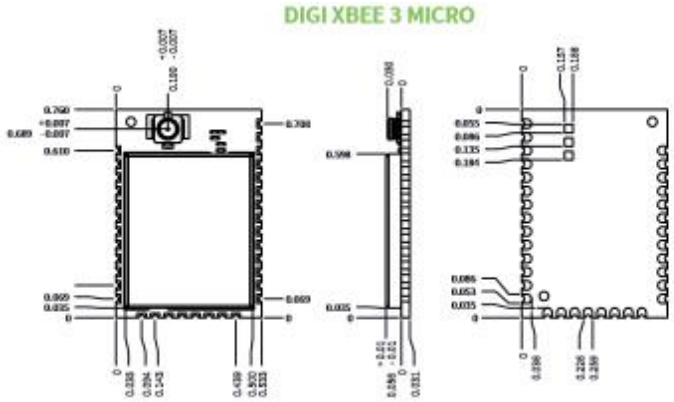
### SECURITY

### APPLICATION EXAMPLE




### RELATED PRODUCTS AND SERVICES

| PERFORMANCE | DigiXBee3Zigbee3.0 | DigiXBee3PROZigbee3.0 |
|---|---|---|
| TRANSCEIVER CHIPSET | Silicon Labs EFR32MG SoC | |
| DATA RATE | RF 250 Kbps, serial up to 1 Mbps | |
| INDOOR/URBAN RANGE* | Up to 60 m (200 ft) | Up to 90 m (300 ft) |
| OUTDOOR/RF LINE-OF-SIGHT RANGE* | Up to 1200 m (4000 ft) | Up to 3200 m (2 miles) |
| TRANSMIT POWER | +8 dBm | +19 dBm |
| RECEIVER SENSITIVITY (1% PER) | -103 dBm Normal Mode | |
| **FEATURES** | | |
| SERIAL DATA INTERFACE | UART, SPI, $I^2C$ | |
| CONFIGURATION METHOD | API or AT commands, local or over-the-air (OTA) | |
| FREQUENCY BAND | ISM 2.4 GHz | |
| FORM FACTOR | Micro, through-hole, surface mount | |
| INTERFERENCE IMMUNITY | DSSS (Direct Sequence Spread Spectrum) | |
| ADC INPUTS | (4) 10-bit ADC inputs | |
| DIGITAL I/O | 15 | |
| ANTENNA OPTIONS | Through-hole: PCB Antenna, U.FL Connector, RPSMA Connector<br>SMT: RF Pad, PCB Antenna, or U.FL Connector<br>Micro: U.FL Antenna, RF Pad, Chip Antenna | |
| OPERATING TEMPERATURE | -40º C to 85º C (-40º F to 185º F) | |
| DIMENSIONS (L X W X H) | Through-hole: 2.438 x 2.761 cm (0.960 x 1.087 in)<br>SMT: 2.199 x 3.4 x 0.305 cm (0.866 x 1.33 x 0.120 in)<br>Micro: 13 x 19 x 2 mm (0.533 x 0.76 x 0.087 in) | |
| **PROGRAMMABILITY** | | |
| MEMORY | 1 MB / 128 KB RAM (32KB are available for MicroPython) | |
| **NETWORKING AND SECURITY** | | |
| PROTOCOL | Zigbee® 3.0 | |
| ENCRYPTION | 128/256 bit AES | |
| RELIABLE PACKET DELIVERY | Retries/acknowledgements | |
| IDS | PAN ID and addresses, cluster IDs and endpoints (optional) | |
| CHANNELS | 16 channels | |
| **POWER REQUIREMENTS** | | |
| SUPPLY VOLTAGE | 2.1 to 3.6 V | |
| TRANSMIT CURRENT | 40 mA @ 8 dBm | 135 mA @ 19 dBm |
| RECEIVE CURRENT | 17 mA | |
| POWER-DOWN CURRENT | 2 micro Amp @ 25º C (77º F) | |
| **REGULATORY APPROVALS** | | |
| FCC, IC (NORTH AMERICA) | Yes | Yes |
| ETSI (EUROPE) | Yes | No |
| RCM (AUSTRALIA) | Yes | Yes |
| ANATEL (BRAZIL) | Yes | Yes |
| TELECK MIC (JAPAN) | Yes | No |
| KCC (SOUTH KOREA) | Yes | No |


| | |
|---|---|
| **XB3-24Z8RM-J** | Digi XBee 3 Zigbee 3.0, 2.4 GHz, Micro, RF Pad Ant, MMT |
| **XB3-24Z8UM-J** | Digi XBee 3 ZigBee 3.0, 2.4 GHz, Micro, U.FL Ant, MMT |
| **XB3-24Z8CM-J** | Digi XBee 3 ZigBee 3.0, 2.4 GHz, Micro, Chip Ant, MMT |
| **XB3-24Z8RM** | Digi XBee 3 PRO ZigBee 3.0, 2.4 GHz, Micro, RF Pad Ant, MMT |
| **XB3-24Z8UM** | Digi XBee 3 PRO ZigBee 3.0, 2.4 GHz, Micro, U.FL Ant, MMT |
| **XB3-24Z8CM** | Digi XBee 3 PRO ZigBee 3.0, 2.4 GHz, Micro, Chip Ant, MMT |
| **XB3-24Z8ST-J** | Digi XBee 3, 2.4 Ghz Zigbee 3.0, SMA Ant, TH MT |
| **XB3-24Z8UT-J** | Digi XBee 3, 2.4 Ghz Zigbee 3.0, U.FL Ant, TH MT |
| **XB3-24Z8PT-J** | Digi XBee 3, 2.4 Ghz Zigbee 3.0, PCB Ant, TH MT |
| **XB3-24Z8ST** | Digi XBee 3 PRO, 2.4 Ghz Zigbee 3.0, SMA Ant, TH MT |
| **XB3-24Z8UT** | Digi XBee 3 PRO, 2.4 Ghz Zigbee 3.0, U.FL Ant, TH MT |
| **XB3-24Z8PT** | Digi XBee 3 PRO, 2.4 Ghz Zigbee 3.0, PCB Ant, TH MT |
| **XB3-24Z8RS-J** | Digi XBee 3, 2.4 Ghz Zigbee 3.0, RF Pad Ant, SMT |
| **XB3-24Z8US-J** | Digi XBee 3, 2.4 Ghz Zigbee 3.0, U.FL Ant, SMT |
| **XB3-24Z8PS-J** | Digi XBee 3, 2.4 Ghz Zigbee 3.0, PCB Ant, SMT |
| **XB3-24Z8RS** | Digi XBee 3 PRO, 2.4 Ghz Zigbee 3.0, RF Pad Ant, SMT |
| **XB3-24Z8US** | Digi XBee 3 PRO, 2.4 Ghz Zigbee 3.0, U.FL Ant, SMT |
| **XB3-24Z8PS** | Digi XBee 3 PRO, 2.4 Ghz Zigbee 3.0, PCB Ant, SMT |

# APPENDIX (B) PZEM-004T V3.0

## PZEM-004T V3.0 User Manual

**Overview**

This document describes the specification of the PZEM-004T AC communication module, the module is mainly used for measuring AC voltage, current, active power, frequency, power factor and active energy, the module is without display function, the data is read through the TTL interface.

PZEM-004T-10A: Measuring Range 10A (Built-in Shunt)

PZEM-004T-100A: Measuring Range 100A (external transformer)

1.Function description

### 1.1 Voltage

1.1.1 Measuring range:80 ~ 260V

1.1.2 Resolution: 0.1V

1.1.3 Measurement accuracy: 0.5%

### 1.2 Current

1.2.1 Measuring range: 0 ~ 10A(PZEM-004T-10A); 0 ~ 100A(PZEM-004T-100A)

1.2.2 Starting measure current: 0.01A(PZEM-004T-10A); 0.02A(PZEM-004T-100A)

1.2.3 Resolution: 0.001A

1.2.4 Measurement accuracy: 0.5%

### 1.3 Active power

1.3.1 Measuring range: 0 ~ 2.3kW(PZEM-004T-10A); 0 ~ 23kW(PZEM-004T-100A)

1.3.2 Starting measure power: 0.4W

1.3.3 Resolution: 0.1W

1.3.4 Display format:

< 1000W, it display one decimal, such as: 999.9W

≥1000W, it display only integer, such as: 1000W

1.3.5 Measurement accuracy: 0.5%

**1.4 Power factor**

1.4.1 Measuring range: 0.00 ~ 1.00

1.4.2 Resolution: 0.01

1.4.3 Measurement accuracy: 1%

**1.5 Frequency**

1.5.1 Measuring range: 45Hz ~ 65Hz

1.5.2 Resolution: 0.1Hz

1.5.3 Measurement accuracy: 0.5%

**1.6 Active energy**

1.6.1 Measuring range: 0 ~ 9999.99kWh

1.6.2 Resolution: 1Wh

1.6.3 Measurement accuracy: 0.5%

1.6.4 Display format:

< 10kWh, the display unit is Wh(1kWh=1000Wh), such as: 9999Wh

≥10kWh, the display unit is kWh, such as: 9999.99kWh

1.6.5 Reset energy: use software to reset.

**1.7 Over power alarm**

Active power threshold can be set, when the measured active power exceeds the threshold, it can alarm

**1.8 Communication interface**

RS485 interface。

2 Communication protocol

**2.1 Physical layer protocol**

Physical layer use UART to RS485 communication interface

Baud rate is 9600, 8 data bits, 1 stop bit, no parity

**2.2 Application layer protocol**

The application layer use the Modbus-RTU protocol to communicate. At present, it only supports function codes such as 0x03 (Read Holding Register), 0x04 (Read Input Register), 0x06 (Write Single Register), 0x41 (Calibration), 0x42 (Reset energy).etc.

0x41 function code is only for internal use (address can be only 0xF8), used for factory calibration and return to factory maintenance occasions, after the function code to increase 16-bit password, the default password is 0x3721

The address range of the slave is 0x01 ~ 0xF7. The address 0x00 is used as the broadcast address, the slave does not need to reply the master. The address 0xF8 is used as the general address, this address can be only used in single-slave environment and can be used for calibration etc.operation.

### 2.3 Read the measurement result

The command format of the master reads the measurement result is(total of 8 bytes):

Slave Address + 0x04 + Register Address High Byte + Register Address Low Byte + Number of Registers High Byte + Number of Registers Low Byte + CRC Check High Byte + CRC Check Low Byte.

The command format of the reply from the slave is divided into two kinds:

Correct Reply: Slave Address + 0x04 + Number of Bytes + Register 1 Data High Byte + Register 1 Data Low Byte + ... + CRC Check High Byte + CRC Check Low Byte

Error Reply: Slave address + 0x84 + Abnormal code + CRC check high byte + CRC check low byte

Abnormal code analyzed as following (the same below)

- ☐ 0x01,Illegal function
- ☐ 0x02,Illegal address
- ☐ 0x03,Illegal data
- ☐ 0x04,Slave error

The register of the measurement results is arranged as the following table

| Register address | Description | Resolution |
|---|---|---|
| 0x0000 | Voltage value | 1LSB correspond to 0.1V |
| 0x0001 | Current value low 16 bits | 1LSB correspond to 0.001A |
| 0x0002 | Current value high 16 bits | |
| 0x0003 | Power value low 16 bits | 1LSB correspond to 0.1W |
| 0x0004 | Power value high 16 bits | |
| 0x0005 | Energy value low 16 bits | 1LSB correspond to 1Wh |
| 0x0006 | Energy value high 16 bits | |
| 0x0007 | Frequency value | 1LSB correspond to 0.1Hz |
| 0x0008 | Power factor value | 1LSB correspond to 0.01 |
| 0x0009 | Alarm status | 0xFFFF is alarm , 0x0000is not alarm |

For example, the master sends the following command (CRC check code is replaced by 0xHH and 0xLL, the same below)

0x01 + 0x04 + 0x00 + 0x00 + 0x00 + 0x0A + 0xHH + 0xLL

Indicates that the master needs to read 10 registers with slave address 0x01 and the start address of the register is 0x0000

The correct reply from the slave is as following:

0x01 + 0x04 + 0x14 + 0x08 + 0x98 + 0x03 + 0xE8+0x00 + 0x00 +0x08 + 0x98+ 0x00 + 0x00 + 0x00 + 0x00 + 0x00 + 0x00 + 0x01 + 0xF4 + 0x00 + 0x64 + 0x00 + 0x00 + 0xHH + 0xLL

The above data shows

- ☐ Voltage is 0x0898, converted to decimal is 2200, display 220.0V
- ☐ Current is 0x000003E8, converted to decimal is 1000, display 1.000A
- ☐ Power is 0x00000898, converted to decimal is 2200, display 220.0W
- ☐ Energy is 0x00000000, converted to decimal is 0, display 0Wh
- ☐ Frequency is 0x01F4, converted to decimal is 500, display 50.0Hz
- ☐ Power factor is 0x0064, converted to decimal is 100, display 1.00
- ☐ Alarm status is 0x0000, indicates that the current power is lower than the alarm power threshold

### 2.4 Read and modify the slave parameters

At present,it only supports reading and modifying slave address and power alarm threshold

The register is arranged as the following table

| Register address | Description | Resolution |
|---|---|---|
| 0x0001 | Power alarm threshold | 1LSB correspond to 1W |
| 0x0002 | Modbus-RTU address | The range is 0x0001~0x00F7 |

The command format of the master to read the slave parameters and read the measurement results are same(descrybed in details in Section 2.3), only need to change the function code from 0x04 to 0x03.

The command format of the master to modify the slave parameters is (total of 8 bytes):

Slave Address + 0x06 + Register Address High Byte + Register Address Low Byte + Register Value High Byte + Register Value Low Byte + CRC Check High Byte + CRC Check Low Byte.

The command format of the reply from the slave is divided into two kinds:

Correct Response: Slave Address + 0x06 + Number of Bytes + Register Address Low Byte + Register Value High Byte + Register Value Low Byte + CRC Check High Byte + CRC Check Low Byte.

Error Reply: Slave address + 0x86 + Abnormal code + CRC check high byte + CRC check low byte.

For example, the master sets the slave's power alarm threshold:

0x01 + 0x06 + 0x00 + 0x01 + 0x08 + 0xFC + 0xHH + 0xLL

Indicates that the master needs to set the 0x0001 register (power alarm threshold) to 0x08FC (2300W).

Set up correctly, the slave return to the data which is sent from the master.

For example, the master sets the address of the slave

0x01 + 0x06 + 0x00 + 0x02 + 0x00 + 0x05 + 0xHH + 0xLL

Indicates that the master needs to set the 0x0002 register (Modbus-RTU address) to 0x0005

Set up correctly, the slave return to the data which is sent from the master.

### 2.5 Reset energy

The command format of the master to reset the slave's **energy** is (total 4 bytes):

Slave address + 0x42 + CRC check high byte + CRC check low byte.

Correct reply: slave address + 0x42 + CRC check high byte + CRC check low byte.

Error Reply: Slave address + 0xC2 + Abnormal code + CRC check high byte + CRC check low byte

### 2.6 Calibration

The command format of the master to calibrate the slave is (total 6 bytes):

0xF8 + 0x41 + 0x37 + 0x21 + CRC check high byte + CRC check low byte.

Correct reply: 0xF8 + 0x41 + 0x37 + 0x21 + CRC check high byte + CRC check low byte.

Error Reply: 0xF8 + 0xC1 + Abnormal code + CRC check high byte + CRC check low byte.

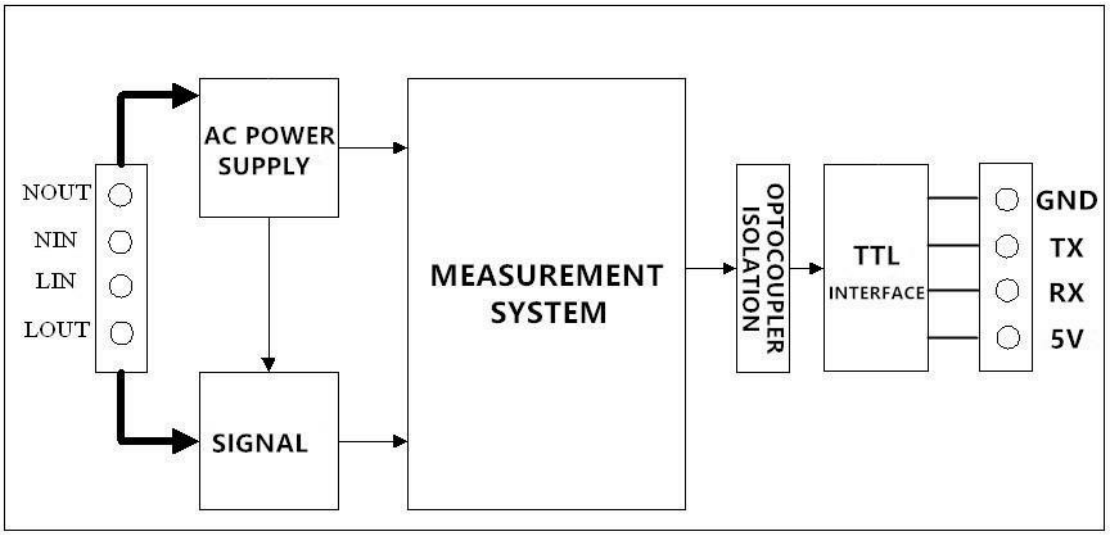
It should be noted that the calibration takes 3 to 4 seconds, after the master sends the command, if the calibration is successful, it will take 3 ~ 4 seconds to receive the response from the slave.

### 2.7 CRC check

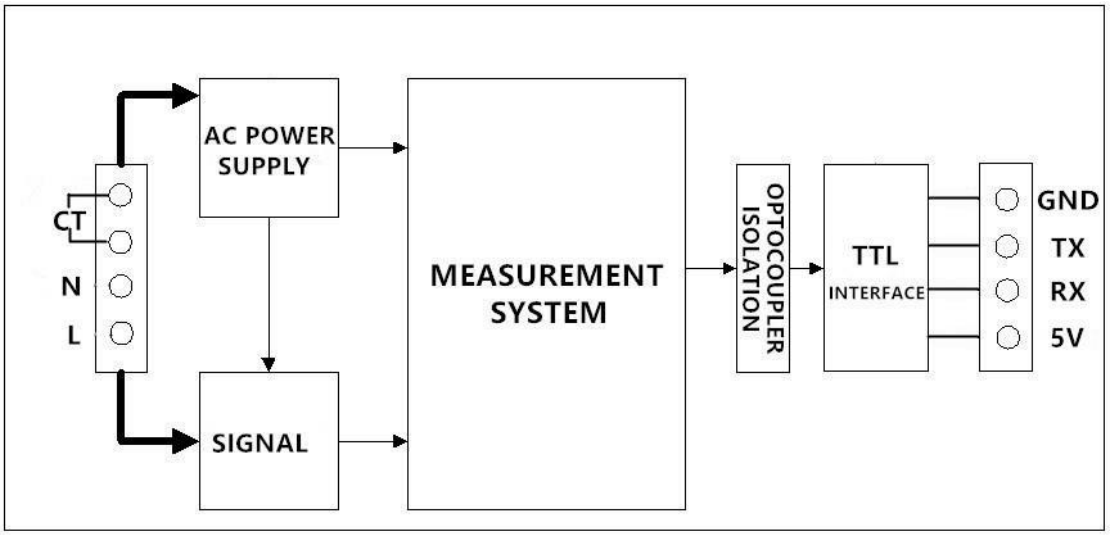
CRC check use 16bits format, occupy two bytes, the generator polynomial is X16 + X15 + X2 +1, the polynomial value used for calculation is 0xA001.

The value of the CRC check is a frame data divide all results of checking all the bytes except the CRC check value.

## 3 Functional block diagram

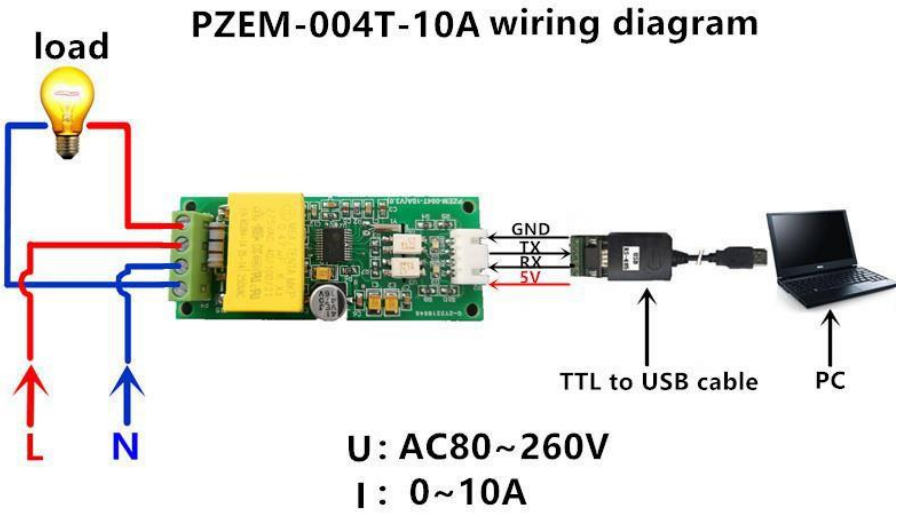



Picture 3.1 PZEM-004T-10A Functional block diagram

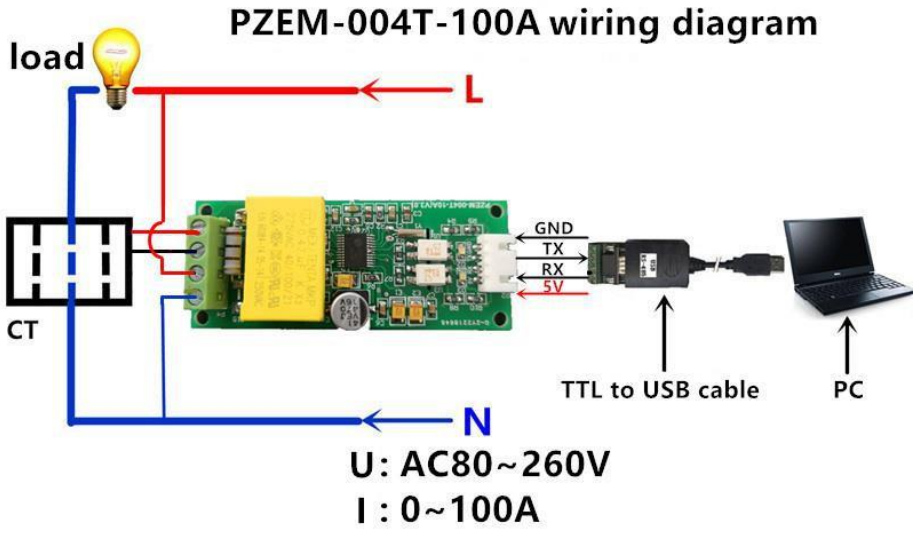



Picture 3.2 PZEM-004T-100A Functional block diagram

4 Wiring diagram




Picture 4.1 PZEM-004T-10A wiring diagram




Picture 4.2 PZEM-004T-100A wiring diagram

5 Other instructions

5.1The TTL interface of this module is a passive interface, it requires external 5V power supply, w hich means, when communicating, all four ports must be connected (5V, RX, TX, GND), otherwis e it cannot communicate.

5.2 Working temperature

-20’C ~ +60’C。

# Appendix (c) Standard Meter (LUTRON DW- 6090)

**Model : DW-6090** *ISO-9001, CE, IEC1010*

## 1. FEATURES

* Multi-functions : WATT, VA, Whr, COS θ ( Power factor ), ACV, ACA, DCV, DCA, Hz, ohm.
* True AC power( Watt ) & apparent power ( VA ) measurement.
* True rms display for ACV, ACA.
* 0.1 W resolution ( < 1000 W ), high precision an high resolution in the low wat range, good performance for low power LED lamp watt measurement.
* Supper large LCD, easy to read-out, display the Watt, Power factor, Voltage & Current value at the same time.
* Accept different kinds current input signal as direct input, inductive clamp probe or CT ( current transformer ).
* Auto range.
* Built-in peak hold & data hold function.
* Watt & VA measurement with Hi, low alarm setting capability.
* RS-232 output interface.
* Exclusive custom exclusive design LSI circuit, provides high accuracy, reliability and durability.
* Built-in over input indication.
* Power supply by batteries or AC to DC adapter.
* Built-in low battery indicator .
* Durable bench type housing plastic case with carrying handle.

## *2-1 General Specifications*

| | |
|---|---|
| Display | * 93 mm x 52 mm large LCD ( Liquid Crystal Display) display.<br>* Multi-display unit, show Volt, Ampere, Watt, Power factor or Hz at same time. |
| Measurement | WATT, VA, Whr,, Power factor, ACV, ACA, DCV, DCA, Hz, ohm. |
| Zero Adjustment | *Whr:*<br>External adjustment by push button. |
| | *DCV, ACV, DCA, ACA :*<br>Automatic adjustment. |
| Polarity | Automatic switching, "-" indicates reverse polarity. |
| Current input mode | Direct input, inductive clamp probe or CT. |
| Over input Indication | Indication of " - - - - " or " - - - - " . |
| Data Output | RS232 serial interface. |
| Sampling Time | *W, VA, ACA, ACV, COS θ , Hz :*<br>Approx. 1.5 Sec. |
| | *DCV, DCA, OHM :*<br>Approx. 1 Sec. |
| Operating Temp. | 0 to 50 ℃ ( 32 to 122 ℉ ). |
| Operating Humidity | Less than 80 % R.H.. |
| Power Supply | *Battery power :*<br>DC 9V, 1.5 V AA (UM-3) battery x 6 PCs. |
| | *AC power :*<br>AC to DC 9V adapter ( 500 mA ), optional. |
| Power Consumption | *Battery power :*<br>Approx. DC 55 mA |
| Dimension | 280 x 210 x 90 mm ( 11.0 x 8.3 x 3.5 inch ). |
| Weight | Approx. 1.6 Kg ( 3.52 LB ). |
| Standard Accessories | Test lead ( red & black )..... 1 pair.<br>Instruction Manual..... 1 PC. |

# الخلاصة

في الوقت الحاضر ، يتمثل التحدي الأكبر في الحفاظ على الطاقة الكهربائية من الخسائر التي تحدث نتيجة الخسائر الفنية (TLs) أو الخسائر غير الفنية (NTLs).

تحدث TLs بسبب الطاقة المشتتة في معدات النظام ، في حين أن NTLs ترجع إلى مشكلتين رئيسيتين ، مشكلة سرقة الطاقة الكهربائية (EETh) ، ومشكلة عدم دفع الفواتير (BNP).

النظام التقليدي المستخدم لتحصيل الفواتير أو الكشف عن سرقات الطاقة الكهربائية يتم يدويًا ويعتمد كليًا على القوى العاملة ، مما يعني أنه لا يمكن إجبار المستهلكين على دفع الفواتير ولا يمكن اكتشاف معظم سرقات الطاقة الكهربائية. وبالتالي؛ سيرتفع سعر وحدة الطاقة (التعريفة) للمستهلك لتغطية هذه الخسائر من قبل شركات الطاقة الكهربائية التي تشكل عبئًا ماليًا ثقيلًا على المستهلكين.

ونتيجة لذلك ، تم تصميم وتنفيذ النظام المقترح لحل مشاكل NTLs ليكون نظامًا ذكيًا لديه القدرة على أن يكون نظام دفع مسبق وكذلك له القدرة على كشف سرقة الطاقة الكهربائية. من ناحية أخرى ، يمكن للنظام المقترح تحديد موقع EETh في عداد طاقة المستهلك أو في وحدة التغذية بالمحول الذي يغذي عدادات المستهلكين.

يمكن للنظام المقترح أيضًا تقليل المساحة المرشحة لكشف سرقة الطاقة الكهربائية من قبل فريق متخصص من مدينة كبيرة تحتوي على مئات من المحولات المغذية إلى محولة تغذية واحدة ومجموعة صغيرة من المنازل الملحقة بهذا المغذي.

تم تصميم النظام المقترح وتنفيذه عمليًا باستخدام مكونات بسيطة بتكلفة منخفضة وقليل من المستشعرات مقارنـــــــــة بالأعمال الأخرى وبناء شبكة محلية دون الاعتماد على الإنترنت أو شركات الاتصالات.

تم اختبار النظام المقترح ومعايرته وإثبات دقته وكفاءته العالية لتحقيق أهداف الأطروحة المطلوبة.

جمهورية العراق
وزارة التعليم العالي والبحث العلمي
جامعة بابـل
كلية الهندسة
قسم الهندسة الكهربائية

# تصميم و تنفيذ عدادات طاقة ذكية لا سلكية لشبكة توزيع الطاقة الكهربائية

رسالة
مقدمة الى كلية الهندسة / جامعة بابل
كجزء من متطلبات نيل درجة الماجستير في الهندسة / الهندسة الكهربائية /الكترونيك صناعي

من قبل
فرقد محمد ناصر غالب
بأشـراف
أ.د. قاسم كرم عبدالله
أ.م.د. شمم فاضل علوش

1444 هـ
2022 م