EVALUATION ON THE IMPACT OF TOPOLOGICAL VARIATION ON ENERGY EFFICIENCY IN ZIGBEE NETWORKS

BY

TAFADZWA MASARIRA

A DISSERTATION SUBMITTED TO THE UNIVERSITY OF ZAMBIA IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTER OF ENGINEERING IN INFORMATION AND COMMUNICATION TECHNOLOGY

THE UNIVERSITY OF ZAMBIA

LUSAKA

2022

COPYRIGHT DECLARATION

DECLARATION

I declare that this research proposal is my own work. Where collaboration with other people has taken place or material generated by other researchers is included, the parties and/ or materials are explicitly stated with references as appropriate.

This work is being submitted for Master of Engineering in Information and Communication Technology at the University of Zambia. It has not been submitted to any other university for any other degree or examination.

Name **Date**

Supervisor **Date**

CERTIFICATE OF APPROVAL

This dissertation by Tafadzwa Masarira is approved as fulfilling the partial requirements for the award of the degree in Master of Engineering in ICT of the University of Zambia.

Internal Examiner 1	**Signature**	**Date**
Internal Examiner 2	**Signature**	**Date**
Internal Examiner 3	**Signature**	**Date**
Chairperson **Board of Examiners**	**Signature**	**Date**

DEDICATION

To my wife Tariro Masarira and daughter Jemimah, I say thank you for your support and inspiration. I certainly appreciate the guidance of my supervisor and the lecturers in the department. Grateful to all that contributed directly or indirectly to this work. Above all may Glory be to God, the giver of life.

ABSTRACT

A Wireless sensor network (WSN) is a fast-developing technology which can monitor, calculate, and communicate wirelessly thereby finding it’s place in areas such as defence, home automation, medical care and environmental sciences which demands better security, throughput, energy efficiency and cost effectiveness. One of the leading WSN is Zigbee as it offers greater range than its counterparts of 10 – 100 metres with proven methods to extend, has low power consumption and can also connect to 64000 nodes which is far greater than its counterparts. The year 2020 saw an increase in the use of networks as governments all over the world enforced lockdowns to limit the movement of people in order to contain COVID 19 pandemic. There was tremendous increase in use of networks, and this resulted in more traffic or unprecedented use of networks. Thereby making it necessary to testing and validating the QoS i.e. throughput, packet loss, end to end delay. In previous research work, QoS has been of paramount importance. Growth in traffic and network size has shifted focus from QoS to energy efficiency and security. Therefore, key in this research is the need to improve energy efficiency.

Different scenarios were simulated using different parameters. Topologies examined were star , tree and mesh. Focus was on QoS , Energy Efficiency and Security based on topological variation. QoS the focus was on throughput and data sent. MATLAB was then used to analyse results obtained from simulations.

Performance evaluations show that the ZigBee can only be use for low-data rate and low-power smart grid applications not having very high reliability requirements and real-time deadlines. Star performed the best on small networks of ten (10) or less nodes. As the network get bigger i.e. more than 20 nodes tree and mesh perform better depending on parameters.

This research analysed several QoS factors in different topologies. However, it is observed that decision on topology to implement should be based on the priorities of QoS and the three have different strengths and weaknesses. Mesh and Tree topologies perform well on energy efficiency depending on the parameters. Mesh is also very resilient when attacked as it proved to be secure. The researcher is confident that this work would benefit other researchers and/or ICT professionals in enhancing QoS , energy efficiency and security through topological variation of ZigBee networks.

Table of Contents

LIST OF FIGURES

LIST OF TABLES

LIST OF ACRONYMS

IoT: Internet of Things

IEEE: Institute of Electrical and Electronics Engineers

QoS: Quality of Service

ETD: End to End Delay

WSN: Wireless Sensor Network

WPAN: Wireless Personal Area Network

LR-WPAN: Low Rate - Wireless Personal Area Network

FFD: Full Function Device

RFD: Reduced Function Device

RSSI: Received Signal Strength Indicator

OPNET: Optimized Network Engineering Tools

OMNET: Objective Modular Network Testbed

Wi-Fi: Wireless Fidelity

NWK : Network

APL : Application

IoT : Internet of Things

FHSS: Frequency Hopping Spread Spectrum

OSI: Open system Interconnection

MAC: Media Access

ZC: Zigbee Coordinator

ZED: Zigbee End Device

ZR: Zigbee Router

NS-2: Network Simulator version 2

NS-3: Network Simulator version 3

AES-CCM: Advanced Encryption Standard – Counter with Cipher Block Chaining Message Authentication Code

CHAPTER 1 - INTRODUCTION

1.0 Background

ZigBee is a wireless, open, mesh networking standard with the application of home, office automation and pervasive computing. In a distributed networking environment, ZigBee devices work together for a higher networking compatibility as the communication medium. ZigBee is a secure standard in WSNs for its low-cost, reliability, wirelessly monitoring capability and less energy consumption applied mostly in large-scale implementation. [1]

IEEE 802.15.4 supports three types of network topology i.e., star, tree, cluster tree and mesh topology. Each of these topologies has its strengths and limitations which can be used to advantage in different situations.[2] While there are mainly assumptions which have been made over time about these topologies, results could be different based on parameters. Hence, there is need to simulate or test any proposed approach before it is adopted.

The Internet of things (IoT) is quickly becoming a reality and WSNs being widely deployed. Their use is increasing exponentially, and the slowdown of the growth is not foreseeable yet.[3]Moreover, WSNs play an important role in IoT and are considered as an emerging technology with a wide range of applications in many areas. Critical factors and goals are changing with the fast progress of their implementation. Therefore, security and energy efficiency in these networks has become of paramount importance.[4] Regulatory authorities are no longer satisfied by the claim that a certain technology has low consumption but want it measured and reduced to the lowest possible level.

In the past years most, researchers focused on WSN with the view to improve performance. This led to works that focuses on performance analysis of different topologies supported by the IEEE802.15.4/ZigBee standard were compared based on throughput, data traffic sent, and data traffic received parameters using Riverbed modeler simulator[5] [6] [7] [5] . After 2020, we're seeing a shift in focus from just performance but achieving the best possible performance while networks are energy efficient. More and more Zigbee applications have entered the market and represent important enablers in the deployment of networks of interconnected devices. As network and spatial device densities grow, energy efficiency and consumption are becoming an important aspect[8].

Zigbee has so far been a main stay for home automation, but with the increased use of this technology there is more use in industrial and/or commercial setup. Therefore, it means that issues of security which were not of much importance are now critical as hackers have interest in commercial activities for gain.

1.1 Problem Statement

ZigBee technology as a wireless sensor and control network is one of the most deployed wireless technologies in recent times as results of its attractive features to the users such as open standard lightweight, low-cost, low-speed, low-power, interoperability protocol, among others.[9] It is built on existing IEEE 802.15.4 protocol and therefore combines the IEEE 802.15.4 features and its own new features which are progressively being added to meet the rising demand of other functionalities thereby finding applications in wide variety of wireless personal area networked systems.[10]

These advantages outlined above may not remain the same as the network size grow. Hence there is need to simulate and evaluate how QoS changes as the network size grow. The drawing card when users opt for Zigbee is energy consumption. This leads us to the need to calculate the energy consumption and track how it varies as network parameters changes. Though the energy consumption is low, user still wants the best possible energy efficiency without compromising on QoS.

Knowledge of energy consumption also helps in detecting attacks.[11] Unfortunately, these networks are prone to a huge range of security attacks and their improvement will be limited in the absence of proper premeditated security solutions to monitor networks. As the Zigbee technology gets more popular this also increase its vulnerability to attacks. Most security impediments also make an effect to energy consumptions which is easy to pick even for non-technical users. QoS, Energy and Security challenges highlighted are all affected by topology of the network. This makes topological variation central in this research.

1.2 Aim

To develop a model that would help to test energy efficiency of a Zigbee network using different topologies considering security and prioritising relevant QoS according to use case before implementation.

1.3 Research Objectives

The main objective of this study is to develop and implement a Zigbee model that is energy efficient taking into account the appropriate topology.

The specific objectives are to:

1. Examine effects of Zigbee topological variation in relation to QoS as network size increases.
2. Evaluate effects of Zigbee topological variation and network size to energy efficiency.
3. Assess the impact of wormhole attack to energy efficiency.

1.4 Research Questions

In this research, we will address some questions regarding QoS, security and energy loss challenges experienced in Zigbee networks in relation to topological variation. The fundamental questions at the core of this research are:

1 How does QoS vary by Zigbee topologies? What are the effects of network size on different topologies to QoS?

2 Quantify the energy efficiency by different topologies? Find the best topology for Zigbee network?

3 What is the effect of wormhole attack to the QoS of Zigbee network? How significant is a wormhole attack to energy efficiency?

1.5 Significance of Study

The use of WSN in particular Zigbee has been evolving over the years. The factors below highlight the relevance and importance of the proposed research are highlighted below:

1.5.1 Remote Working

COVID 19 is a health pandemic which struck the world in 2020. The virus could spread easily through the air and this prompted many governments throughout the world to encourage and in some cases enforced working from home to limit the spread of the virus. Remote working made the case of automation stronger than ever before. Professionals had to work from home at least for some days and for business to go on as usual some tasks had to be automated. There was a great acceleration in the use of technology, digitization, and new forms of working. Company executives reported that they moved 20 to 25 times faster than they thought possible on things like automation of business processes, improving data security, and increasing the use of advanced technologies in operations.[12]

COVID-19 crisis has brought about years of change in the way companies in all sectors and regions do business. Companies have accelerated the digitization of their customer and supply-chain interactions and of their internal operations by three to four years. The share of digital or digitally enabled products in their portfolios has accelerated by a shocking seven years.[13] The health pandemic forced most if not all companies to automate. This has significantly increased the use of WSN especially Zigbee to the effect that though it is by nature energy efficient there is need to test or simulate how it can be improve through topological variation. Therefore this research is of importance to companies who have or are in the process of adopting remote working.

1.5.2 Exponential Growth Industry 4.0

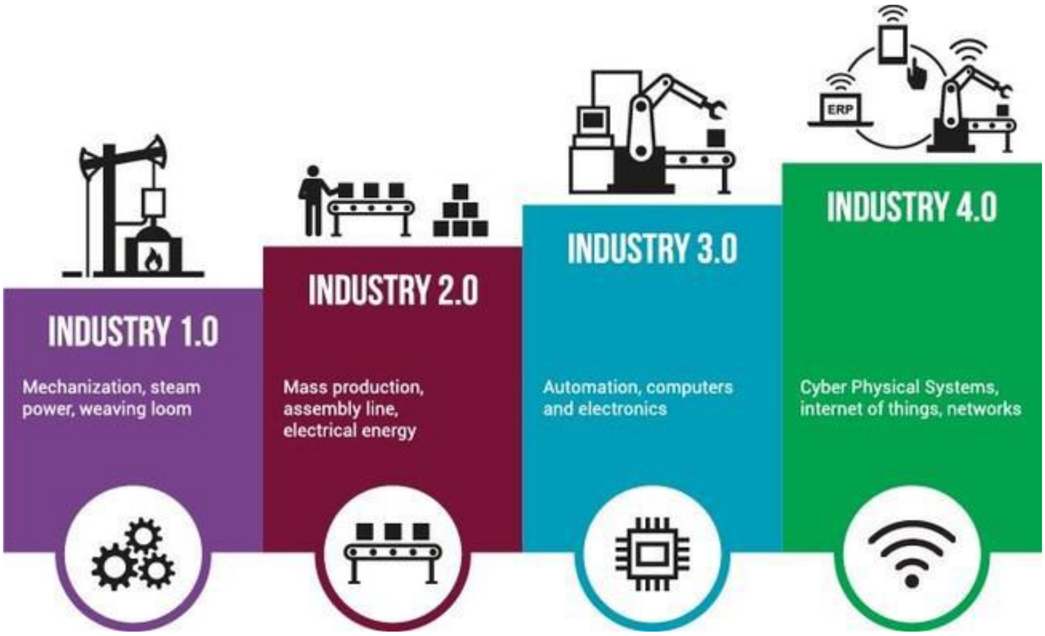

ERP
INDUSTRY 1.0
Mechanization, steam power, weaving loom
INDUSTRY 2.0
Mass production, assembly line, electrical energy
INDUSTRY 3.0
Automation, computers and electronics
INDUSTRY 4.0
Cyber Physical Systems, internet of things, networks

Figure 1.1 : Industry 4.0 revolution [14]

The current industrial revolution is the industry 4.0. One of its main aims is the replacement of old communication that uses wired links with new communication that is wireless communication. The main reason to move to wireless communication is to improve the mobility, reduce the deployment cost, reduce cable damage and to improve the scalability. To do this, the type of industrial application needs to be taken into consideration. The current industrial revolution is the 4.0 industrial revolution which combines different technologies such as Internet of Things (IoT), robotics, virtual reality and artificial intelligence.[14] It also seek to connect devices to IoT so as to improve the accessibility of the industry from anywhere in the world.

The proposed protocol to be used is ZigBee communication protocol along with the IoT service. IoT connect anything on the internet using a specified protocol with sensors, devices, equipment to transfer the information and communicate among devices intelligently to achieve smart monitoring and administration. While Zigbee is the leading choice on energy efficient WSN, the scale of its use in industry 4.0 may suffer diminishing return on strengths it is selected for. It is therefore imperative to test or simulate effect of growth and topological variation to energy efficiency in Zigbee networks.

1.5.3 Security

Internet of Things (IoT) has become increasingly popular in the past few years. Subsequently, the security of the IoT devices becomes crucial, especially many devices have access to highly personalized and sensitive data. WSN’s provide endless opportunities and at the same time pose formidable challenges due to the existence of enormous number of sensor nodes which are by default insecure, hence places few challenges on the network. Zigbee is one of the most widely used standards for wireless communication between different IoT devices and has been adopted by many major companies, like Samsung and Philips. [15]

Even in the case of the recent attack on the wireless ZigBee light bulbs by Philips [16] that allowed the attackers to take control of these devices, they could use their ZigBee radio transmitter to contaminate other bulbs or eventually jam the radio communications.[17] Even though Zigbee was designed with the importance of security in mind, there have been trade-offs made to keep the devices low-cost, low-energy and highly compatible. Some parts of the standard's security controls are poorly implemented, which inevitably lead to security risks. While focus of this research was on energy efficiency, efforts were made to evaluate the effects of a wormhole attack to Zigbee network .

1.6 Scope of the Project

This research is limited to Zigbee. Specifically, the researcher will focus on energy efficiency. On QoS focus shall be on throughput and data sent . Security is also another broad subject and in this study focus shall be on a wormhole attack. Topologies shall also be restricted to the main ones which are Star , Tree and Mesh.

1.7 Plan of Development

The remainder of research work is organized as follows:

Chapter Two :	Provides detailed literature reviews on Zigbee network. IEEE 802.15.4 standard has been discussed.
Chapter Three :	Describes the proposed research methodology process paying attention to simulators and scenarios that will be simulated. Parameters of the OPNET simulation are well articulated and the Mathematical Analysis that was done in MATLAB.
Chapter Four :	Details the results from OPNET simulation and MATLAB Analysis. This has been done through use tables and graphical representation.
Chapter Five :	Gives the summary of the research, its conclusion, and some recommendations, based on the simulations and the experimental results obtained. Finally, some potential future work is also proposed.

1.8 Chapter Summary

This chapter has introduced research on the effects of topological variation on energy consumption. Using simulations, we can find out how the real time system will work before building or implementing it. Simulations do not only shorten the time for designing but also reduce the production failures. Decision making can be improved as it reduces the risk of implementing a network that is not best suited for a particular scenario. While focus will be energy efficiency, the research shall also look at the effects to QoS and Security. This will also lead to improvement in the performance. The research objectives, scope and problem statement have been outlined.

CHAPTER 2 – LITERATURE REVIEW

2.0 Chapter Introduction

This section contains different literature reviewed from various sources like journals, conference papers, reports, textbooks, government documents coupled with selected items from the internet. Special attention has been given to WSN standards with focus on QoS, energy and security.

2.1 The Standard

IEEE 802.15 is a group of the institute of electrical and electronics engineers (IEEE). IEEE 802.15 standards committee specifies wireless personal area network (WPAN) standards. IEEE 802.15 is further divided into various groups that are working on different projects of WPAN like IEEE 802.15.1 specifies the standards for Bluetooth communication, IEEE 802.15.2 gives the traffic management rules for coexistence of 802.15(WPAN) and 802.11(Wi-Fi) and IEEE 802.15.3 specifies the standards for high data rate WPAN.

2.2 Wireless Sensor Network

WSNs are massive-scale sensor networks that were enabled due to the continuous improvements in wireless networking, embedded microprocessors, and integration and micro-fabrication. These networks can be adjusted to fit appropriately for a series of commercial and military applications. In general, WSNs consist of multifunctional wireless sensing devices positioned over a wide geographical area. These devices form a distributed communication network which can collect data about the surrounding environment and collaborate effectively to process the collected data. Modern WSNs consist of a large number of sensing devices that are cheap and linked together using low power communications such as IEEE 802.15.4 or ZigBee.[18]

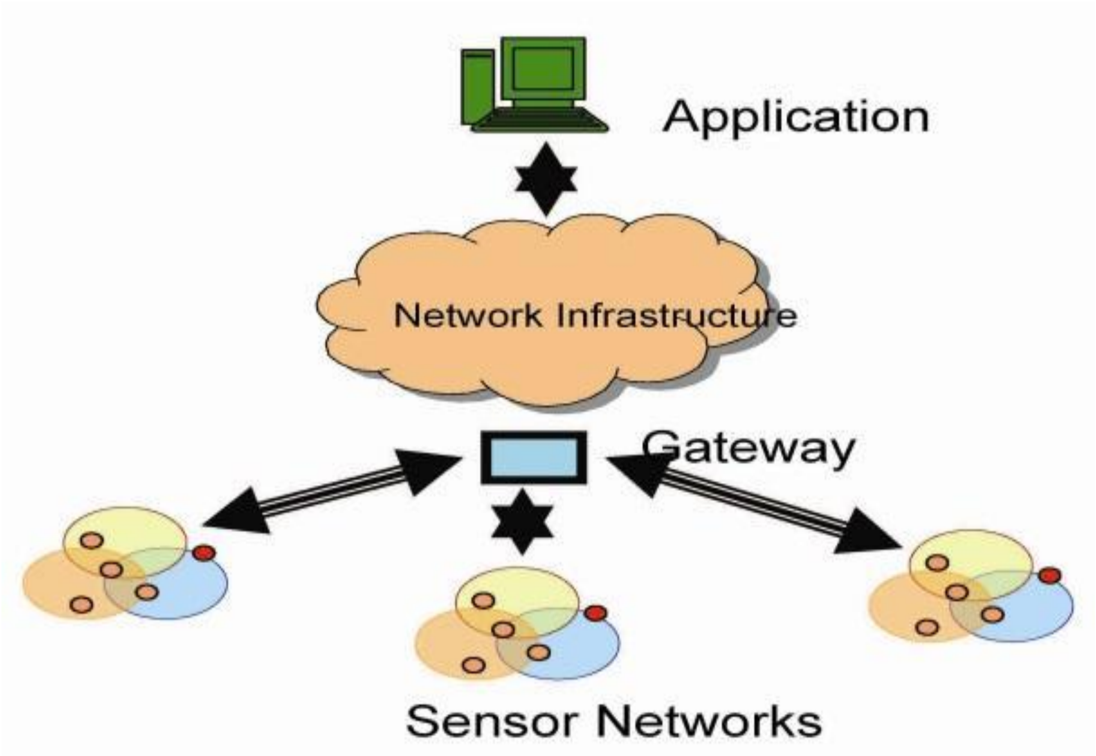


Figure 2.1 WSN schematic diagram [9]

WSNs differentiate functionally from the usual collection of sensing devices by its network capabilities, which enable cooperation, coordination, and collaboration between sensing assets. Additionally, instead of sending the raw data to the nodes responsible for the fusion, sensing nodes use their processing capabilities to perform simple local computations and transfer only the required and partially processed data.

In general, WSNs represent an important topic of study where many researchers tried to benefit from it to build various systems where control, tracking, or monitoring are involved such as smart grid[19] , smart buildings[20] , track cycling[21] , localization [22], smart alarm[23], energy monitoring, control, and management [24], health care[25], agriculture[26], and many other applications.

WSN is one of the systems that has been developed for exchanging information quickly and accurately. Wireless technology has been widely implemented in all aspects of life from a large sector of industry automation to small sectors such as home automation.[27]

2.2.1 WSN Transmission Protocol

Basically, there are three main technologies used for WSN and there are Zigbee, Wifi and Bluetooth. As the applications of WSNs are increasing, different protocols and standards are being researched and created to enhance the efficiency of the network. The decision to select a particular standard/protocol over the other is determined by the target application requirements and some other factors such as network size, network environment and network duration. Once the application requirements are set, then the engineer will select the technology which satisfies these requirements.[9] Below is an overview of each and then a table showing how these technologies compare:

2.2.2 Bluetooth

Bluetooth is a robust, low power, low cost, short-range wireless communication technology intended to replace cables in wireless personal area networks (WPANs). Initially created by Ericsson Microelectronics in 1994, its specifications are driven by a consortium that was founded by Ericsson, Nokia, Toshiba, IBM and Intel. The IEEE standard for Bluetooth (WPAN) is called The IEEE Project 802.15.1 and is based on the Bluetooth v 1.1 Foundation. It allows product differentiations because some of its core specifications are optional. It can communicate (pass and synchronize data) between up to seven devices using 868MHz, 915MHz and 2.4GHz radio bands at 1GHz per second using frequency-hopping spread-spectrum (FHSS) and up to a range of 10 meters . Bluetooth only supports star topology, uses master-slave based MAC protocol and full duplex transmission through the use of time-division duplexing. The simplified version of Bluetooth was released to the public in 2006 and is called Bluetooth Low Energy Technology. Designed to be more efficient (about 15 times than existing Bluetooth). However, it interoperate with existing Bluetooth. This efficiency is achieved by improvement on number of packets transmitted during connection, node discovery and the size of each individual packet .

In WSNs, applications of Bluetooth technology are increasing drastically. Bluetooth technology finds application in smart home, automation, health and fitness, mobile telephony, PC and peripherals etc.[9]

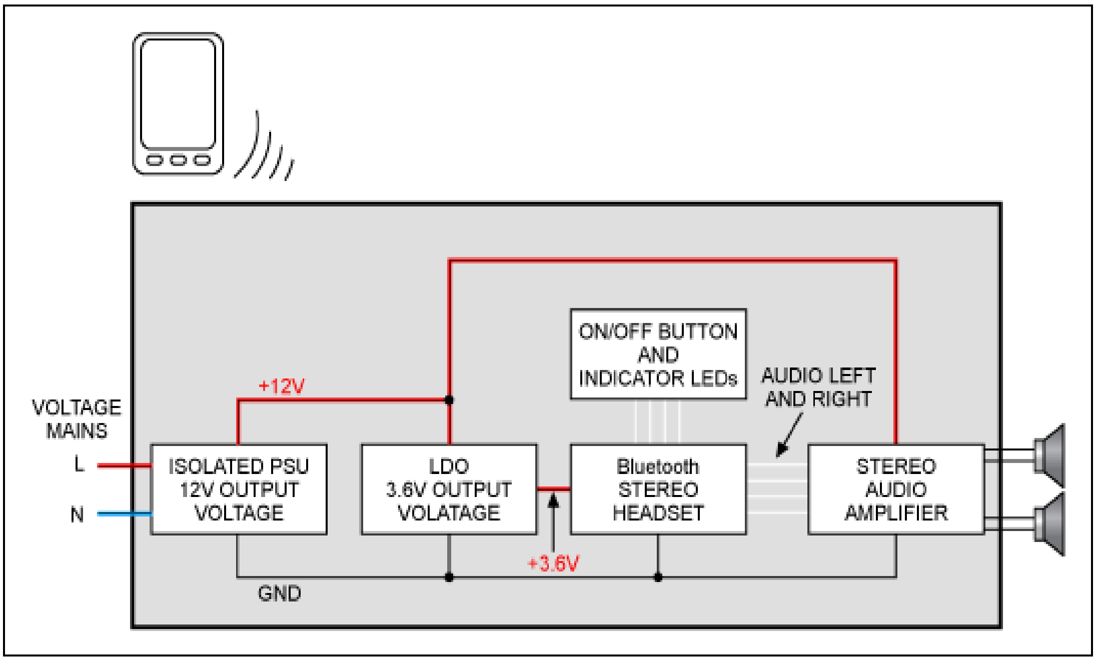


Figure 2.2 Block diagram of wireless Bluetooth stereo audio system.[28]

2.2.3 Wi-Fi

Based on IEEE 802.11 standards, Wi-Fi is a WLAN technology that allows electronic devices to exchange data over a network such as internet and uses a radio band of 2.4GHz. Wi-Fi is robust, easily expandable and cost effective. Wi-Fi data transfer rate is up to 300Mbps depending on the standard and has about 100 to 150Mbps through-put. It also has a broad coverage area, some non-line-of-sight (NLOS) transmission capacity, small disturbance of links, and supports mesh networking. A Wi-Fi-based WSN is a combination of traditional WiFi mesh network and WSN and hence possesses both the features of Wi-Fi mesh network and WSN. Therefore, it is both network-centred and data-centred. Wi-Fi-based WSNs are used in smart grid, smart agriculture and intelligent environment protection. Also because of Wi-Fi high bandwidth, fast transmission rate, long transmission distance and NLOS, Wi-Fi-based WSN is being deployed in video monitoring which requires data transition and good-real time.[9]

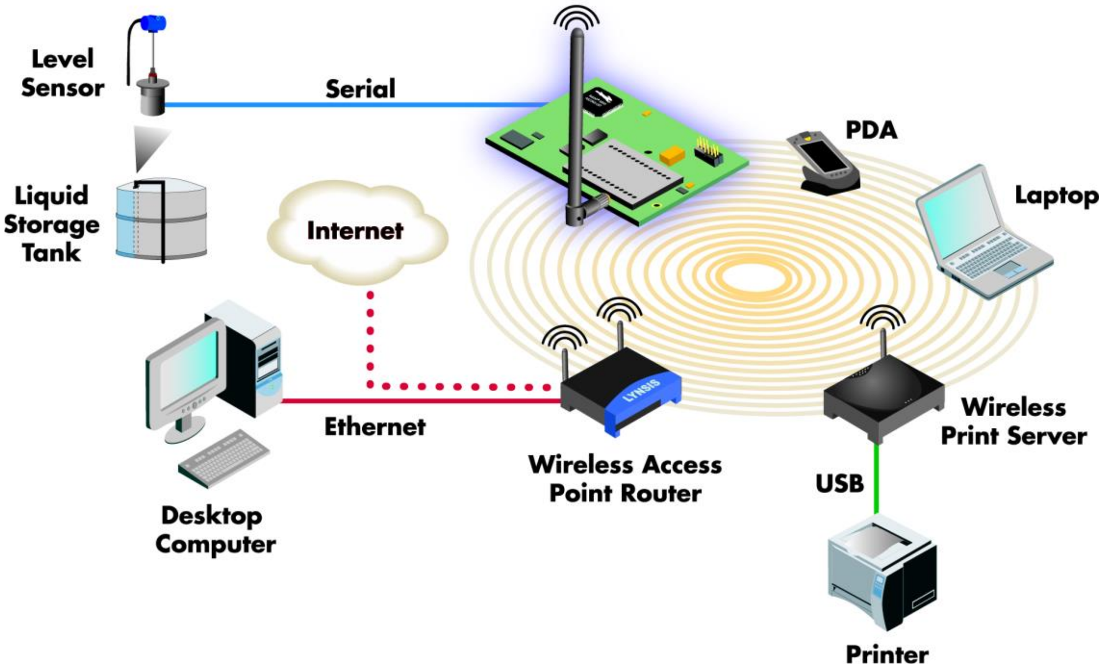


Figure 2.3: Wireless Local Area Network Connected to the Internet [28]

2.3 ZigBee Technology

ZigBee is a new open-standard wireless protocol developed by ZigBee Alliance (consisting of over 270 companies). ZigBee is particularly targeted at low-power, low-cost and low data rate wireless sensor and control networks, aimed at interoperability, it is easy to implement and can support up to 65,000 nodes depending on the type of topologies used [8]. ZigBee has a transmission range of 10 - 100metres. Comparing ZigBee with WiFi and Bluetooth, ZigBee stack is lighter weighted (about 120 KB). It has a maximum throughput of 250Kbps while Bluetooth (except 802.11n) and Wi-Fi transmit at 3Mbps and 54Mbps respectively. While WiFi devices (e.g. WiFi VoIP phones) are reported to have 8 – 12hours of battery lives and Bluetooth devices with a battery life of a few days, many ZigBee devices can boast of a battery life of up to 5years. The huge power saving resulted from relatively short-range of transmission, low data transfer rates and simple protocol stack of ZigBee.[9]

Below are the characteristics of Wi-Fi, Bluetooth and ZigBee

Comparison between ZigBee, Wi-Fi, Bluetooth

Performance	**ZigBee**	**Wi-Fi**	**Bluetooth**
Operating Frequency	2.4 GHz, 868/915 MHz	2.4 GHz	2.4 GHz
Communication Range	10 - 100m	100m	10m
Operating Voltage (Volts)	3	3.3	1.8
IEEE Standard	802.15.4	802.15.1	802.11 a,b,g
Battery Life (days)	100 to >1000	1 to 7	1 to 5
Max Network Nodes	>64000	32	8
Wake-up time	30ms	3s	10s
Bandwidth	2MHz	22MHz	1MHz
Success Parameter	Reliability, Robust, Low Power Consumption	Speed, Flexibility	Cost Convenience

Table 2.1: Comparison between ZigBee, Wi-Fi, and Bluetooth Performance – [29]

Based on the statistics given above Zigbee maybe the technology of choice. Although, the data rate for ZigBee is low, this is acceptable for short range communication and maybe taken as a strength as it results in low power consumption. Moreover, Wi-Fi and Bluetooth have 32 and 8 network nodes respectively, while ZigBee has 16 address lines for communication which means that we can have a maximum of 65536 nodes as shown in the table above. ZigBee signal response time is the shortest at 30ms, since it is used mostly in monitoring and control applications where data reliability, power-efficiency, and affordability are crucial. ZigBee Technology is simpler and cheaper than other WPANs such as Wi-Fi and Bluetooth.

2.3.1 History of Zigbee

It is now over two (2) decades since Zigbee was conceived and over the year it has evolved to be the most coveted network for home automation. This does not discount its usefulness in industry. Below we give the timelines of how it has evolved over the years[30] .

1999 - ZigBee-style networks began to be conceived around 1999, when many installers realized that both Wi-Fi and Bluetooth were going to be unsuitable for many applications. In particular, many engineers saw a need for self-organizing ad-hoc digital radio networks. The real need for mesh has been cast in doubt since that, in particular as mesh is largely absent in the market[30].

2003 - The IEEE 802.15.4-2003 standard was completed in May 2003 and has been superseded by the publication of IEEE 802.15.4-2006. In the summer of 2003, Philips Semiconductors, a major mesh network supporter, ceased the investment. Philips Lighting has, however, continued Philips' participation, and Philips remains a promoter member on the ZigBee Alliance Board of Directors[30].

2004 - The ZigBee Alliance announced in October 2004 that the membership had more than doubled in the preceding year and had grown to more than 100 member companies, in 22 countries. The ZigBee specifications were ratified on 14 December 2004[6]. The first stack release is now called ZigBee 2004. The ZigBee 1.0 specification was ratified on 14 December 2004 and is available to members of the ZigBee Alliance[3].

2005 - By April 2005 membership had grown to more than 150 companies, and by December 2005 membership had passed 200 companies. The ZigBee Alliance announced availability of Specification 1.0 on 13 June 2005, known as ZigBee 2004 Specification[11].

2006 - ZigBee 2006 Specification was announced. In 2007, ZigBee PRO, the enhanced ZigBee specification was finalized. The second stack release is called ZigBee 2006, and mainly replaces the MSG/KVP (Message/Key Value Pair) structure used in 2004 with a ”cluster library”. The 2004 stack is now more or less obsolete[31].

2007 - ZigBee 2007, now the current stack release, contains two stack profiles, stack profile 1 (simply called ZigBee), for home and light commercial use, and stack profile 2 (called ZigBee PRO). ZigBee PRO offers more features, such as multi-casting, many-to-one routing and high security with Symmetric-Key Key Exchange (SKKE), while ZigBee (stack profile 1) offers a smaller footprint in RAMand flash. Both offer full mesh networking and work with all ZigBee application profiles. ZigBee 2007 is fully backward compatible with ZigBee 2006 devices: A ZigBee 2007 device may join and operate on a ZigBee 2006 network and vice versa. Due to differences in routing options, ZigBee PRO devices must become non-routing ZigBee End-Devices (ZEDs) on a ZigBee 2006 network, the same as for ZigBee 2006 devices on a ZigBee 2007 network must become ZEDs on a ZigBee PRO network. The applications running on those devices work the same, regardless of the stack profile beneath them. Most recently, the ZigBee 2007 specification was posted on 30 October 2007. The first ZigBee Application Profile, Home Automation, was announced 2 November 2007[32].

2.3.2 ZigBee Alliance

ZigBee is organized under the control of the organization called ZigBee Alliance. ZigBee alliance is an organization of companies working together to define an open global standard for making low power wireless networks[33] . The intentional outcome of ZigBee alliance is to make a description that defines how to build altered network topologies with features of data security and interpretable application profiles. This organization has more than 150 members out of which seven are the promoter. A big challenge for the ZigBee alliance is to make the interoperability to work among different products[34]. For solving this problem, ZigBee Alliance has defined profiles which depends on the category of the product to which it belongs to. For example, there is a profile called the home lightning which defines how altered brands of home lightning-products should communicate to each other.[20]

2.4 Zigbee Applications

ZigBee module is a wireless data terminal of Internet of things, which provides users with wireless data transmission function by using ZigBee network. The product adopts high performance industrial-level ZigBee scheme and provides SMT and DIP interface, which can directly connect TTL interface device and realize data transparent transmission function. Low power design, the minimum power consumption is less than 1mA, 6 channels of I/O are provided to realize digital input/output and pulse output; Among them, 3 channels of I/O can also realize the functions of analog quantity collection and pulse counting. Suitable for applications of ZigBee technology usually have low equipment cost, small data transmission, a wide range of communication coverage required, and there are many devices in the network, but only for monitoring or controlling the environment.[35]

Typical applications of ZigBee technology are as follows:

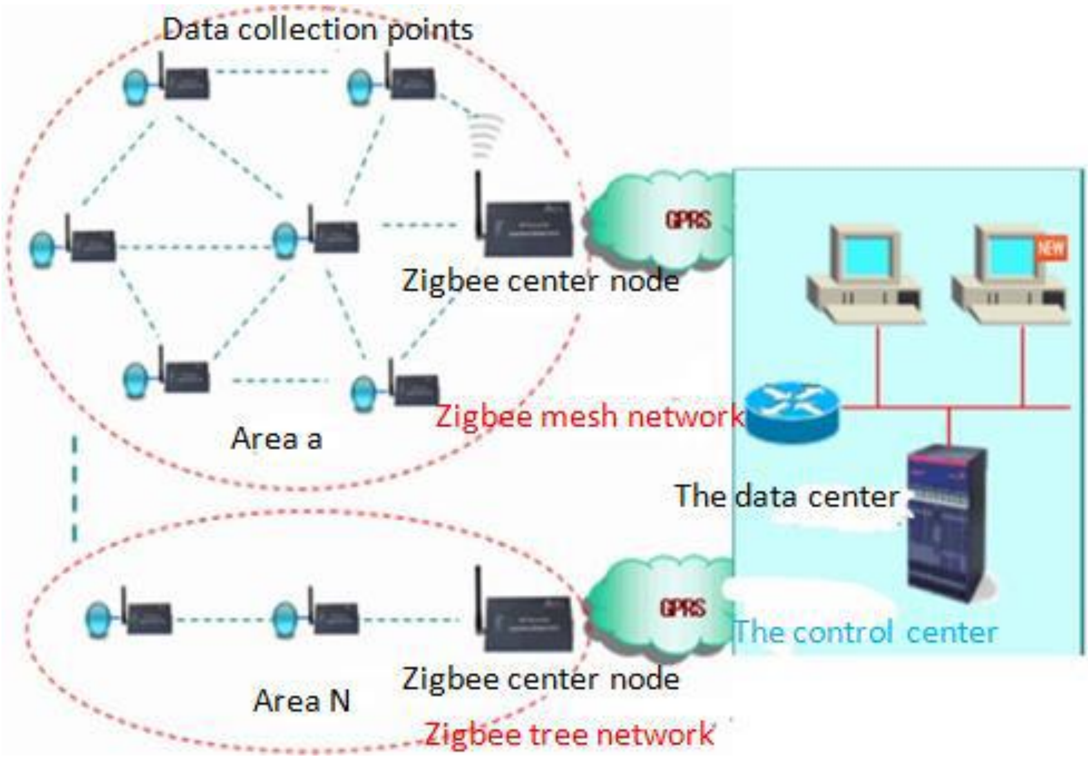


Figure 2.4: Combining ZigBee and GPRS for wireless data transmission[35]

Using GPRS wired network transmission based on Zigbee wireless sensor node data complete wireless network design, network USES the star or wake Zigbee module MESH network topology and the demand of communication mode, effectively reduce the per of Zigbee sensor node power consumption, reducing the sensor nodes to the sink node to report the data when the probability of collisions, and use the GPRS network transmission of the sink node data, changed the traditional wireless sensor networks need to rely on the limitation of public network for data transmission cable, the network has very significant advantages. The remote management center realizes remote communication with Zigbee network through GPRS and other public channels, and obtains relevant information collected through GPRS
network to realize effective control and management of the site.[35]

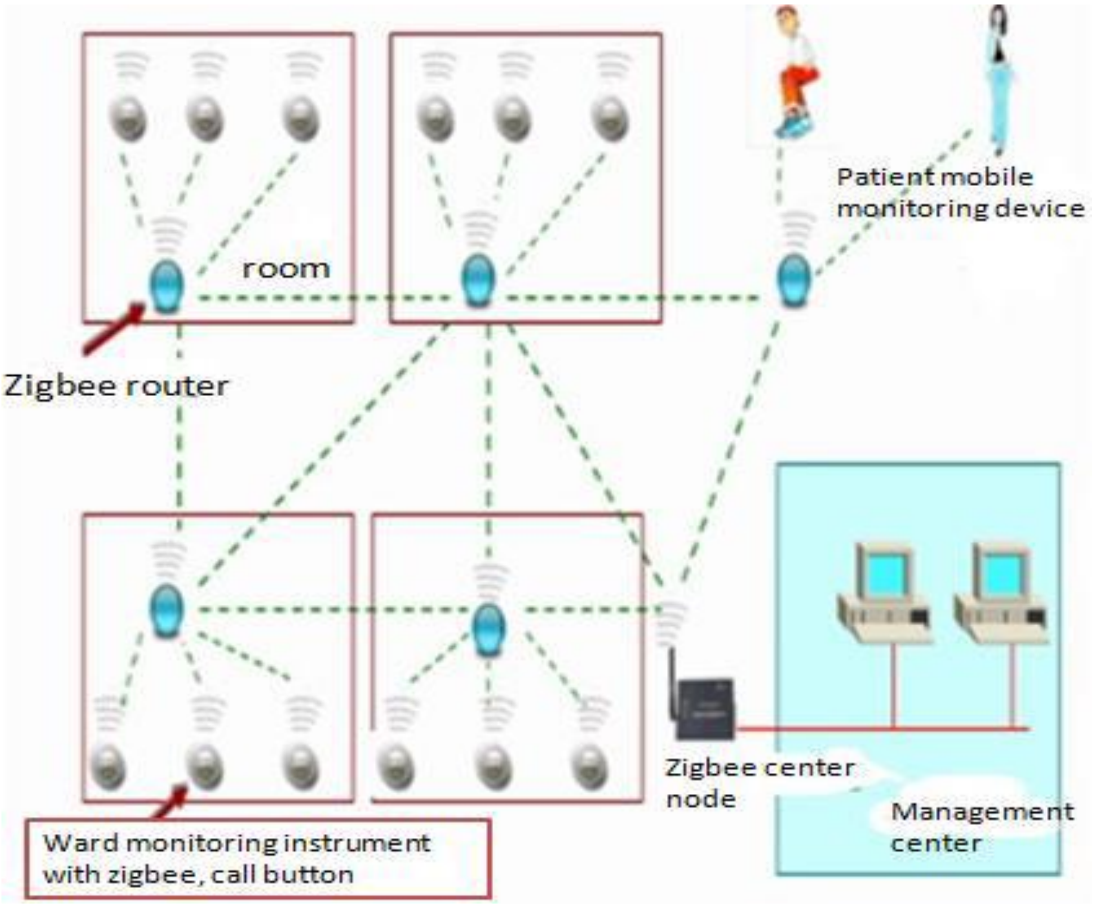

room
Zigbee router
Patient mobile monitoring device
Zigbee center node
Management center
Ward monitoring instrument with zigbee, call button

Figure 2.5: Medical Monitoring System [35]

Zigbee technology is used to form a mesh routing network. Appropriate routing nodes are set up in the corridor for data transfer. Call nodes in the room are connected by star network. All Zigbee routers form a cellular network, and then connect with the Zigbee centre node, which is set in the management centre to build a complete Zigbee wireless network, which is a very reliable network structure for communication.

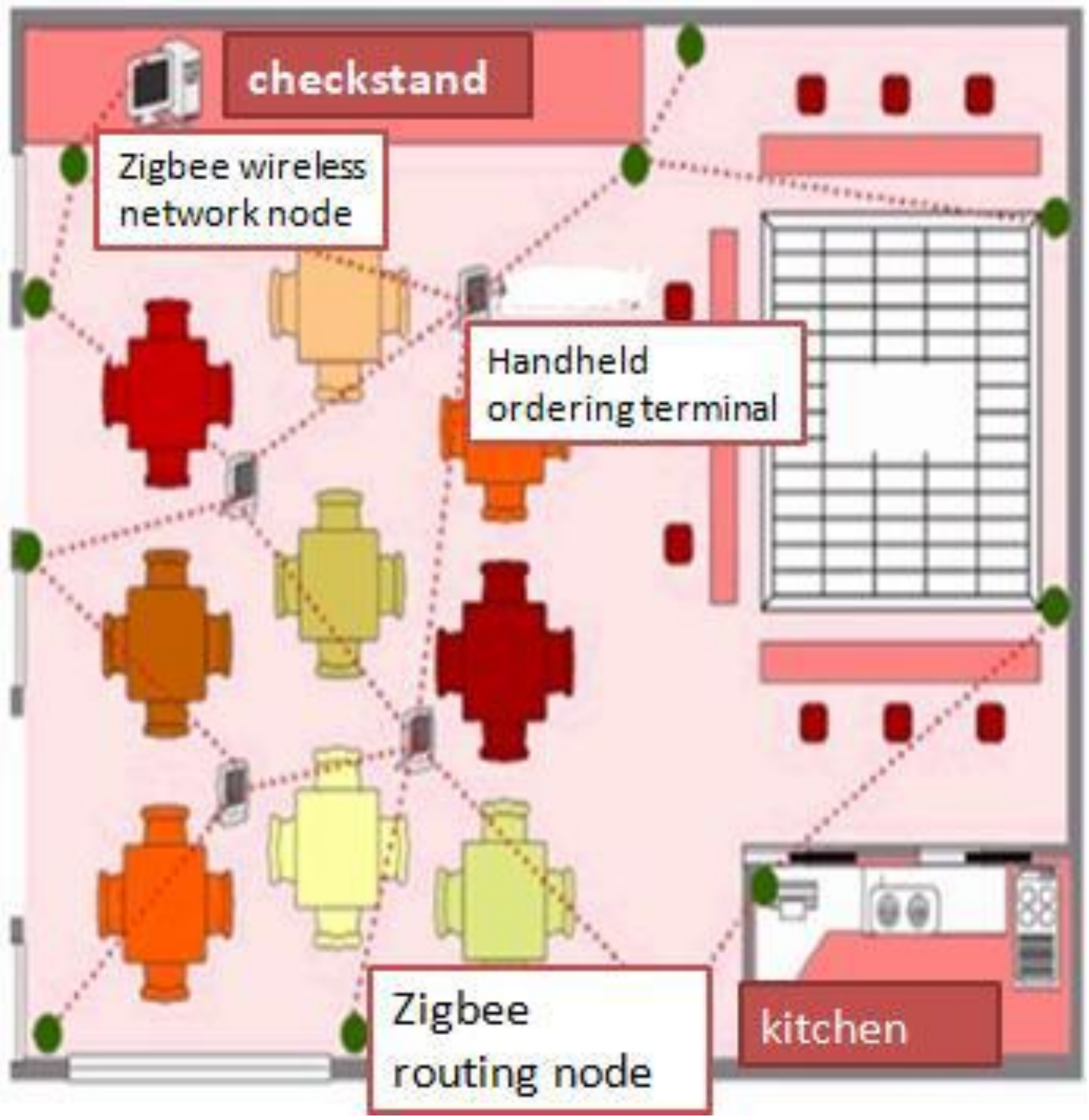


Figure 2.6: Wireless Ordering System[35]

Restaurant ZigBee wireless node network, through the deployment of ZigBee node equipment in the restaurant, bar, kitchen, cashier, processing center to form a complete wireless communication network, to achieve the automation of information processing; The waiter order through hand-held terminals to handle the customer's order, the user orders through the terminal and hall of ZigBee network automatically uploaded to the kitchen and the checkout counter, ZigBee center node of the wireless communication system, wireless ZigBee order routing and wireless terminal, enough to constitute a cellular communication network, any node to realize communication more adjustable way. Any one of the ZigBee routers is responsible for connection with the central network and data relay forwarding. All ZigBee routers form a cellular network and connect with ZigBee center nodes, which are set at the general service desk to build a complete ZigBee wireless network, which is a very reliable network structure for communication.

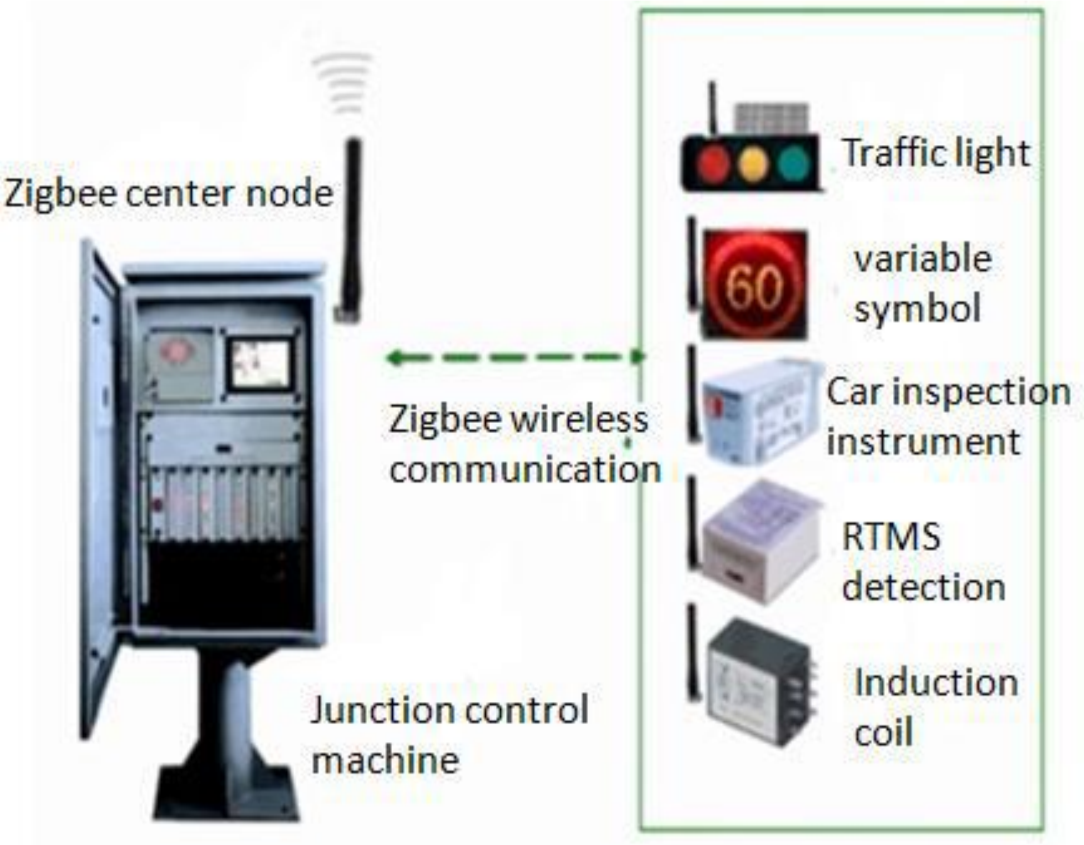


Figure 2.7: Intelligent Traffic Control System[35]

Using Zigbee and wireless control system combined solar energy, do not need to dig the road layout control circuit, to realize automatic wireless network connection between the equipment, which decrease the system installation costs, more important is to avoid the traditional installation method for the economic loss brought by the traffic interfered, but also avoided because of the fast urban development, road development, such as changes to the original embedded line interference.

2.5 Protocol Architecture of Zigbee

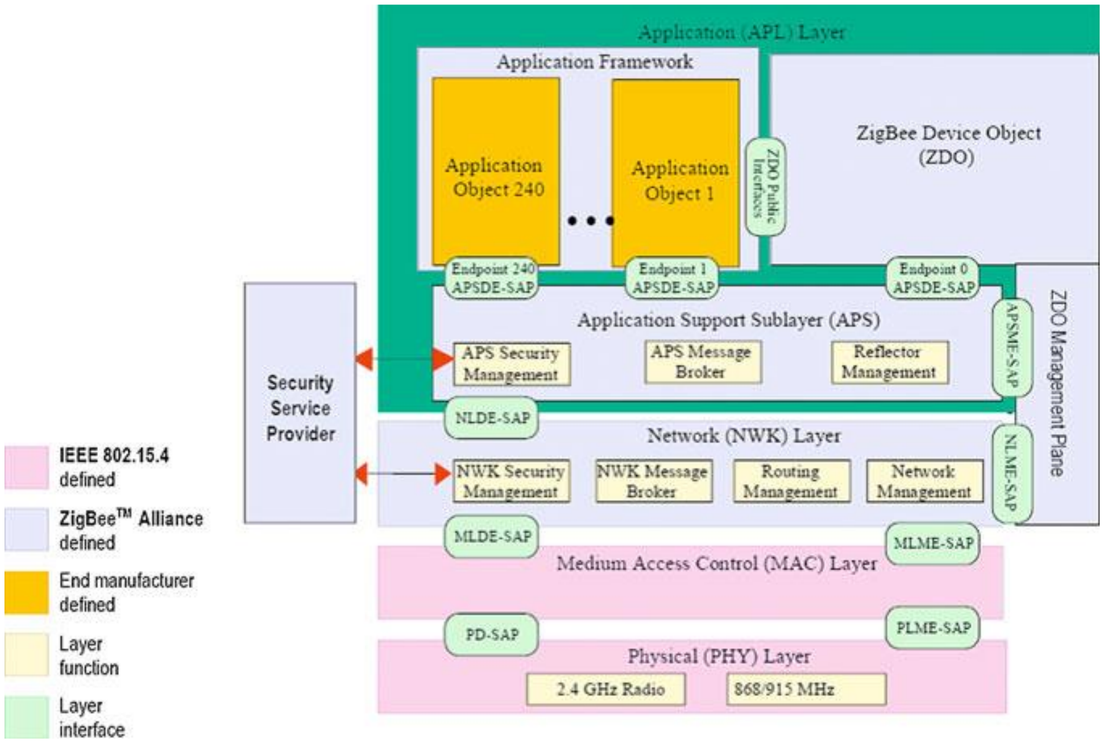


Figure 2.8: ZigBee Architectural Stack [2]

ZigBee standard enhances the feature of IEEE 802.15.4 standard by adding the network, security, and application framework layer over it [36] .Zigbee protocol has inherent security services such as providing encryption, data integrity check and identity authentication. These functions utilize AES-128 encryption technology to ensure the privacy of MAC, NWK and APS layer [37].

The IEEE standard defines the characteristics of PHY and MAC layers. ZigBee builds upon IEEE 802.15.4 standard defines the network layer specifications and provides a framework for application programming at the application layer. ZigBee follows the standard OSI (Open system Interconnection) reference model. Protocol stack of ZigBee has a layered structure. The first two layers, PHY (physical) and MAC (media access) are defined in the standard IEEE 802.15.4 as shown in the figure. The layers above to the physical and MAC are defined by the organization called ZigBee Alliance.[20]

2.5.1 Physical Layer

The physical layer of the standard IEEE802.15.4 is the nearest to the hardware, that controls and communicates directly with the radio transceiver. It controls all tasks like access to the ZigBee hardware, initializing the hardware, selection of channel, energy detection measurement, link quality estimation and clear channel assessment to assist the channel selection. Next in the upward direction there is the Media access control that is MAC layer.

2.5.2 Medium Access Control

MAC layer is an interface between the physical and the network layer. The function of MAC layer is to generate beacons and synchronize the devices to the beacon signal, in a network which is beacon enabled. It also performs the connect and disconnect function. The IEEE 802.15.4 MAC has defined four types of frame structures: A beacon frame which is used by a coordinator to transfer beacons. The beacon frame awakes the client devices, which hear for their address and sleep again when they receive it. A data frame is used for all transmissions of data. The data frame provides up to 104 bytes of payload. An acknowledgment frame is used to confirm successful reception of frame. It sends feedback from receiver to the sender and confirms that the packet has received without any error. A MAC command frame is used to handle all MAC peer operation control transfers. MAC command frame provides a method for remote control and layout of client nodes. MAC layer provides collision avoidance mechanism and is responsible for validating frames, frame delivery, network interface and secure services[7] .

2.5.3 Network Layer

Network layer comes under the ZigBee specification. Network layer is an interface between the application layer and the MAC Layer. Functions of this Layer are formation of network and routing. This layer helps the low power devices to increase their battery life. The Network layer connects or disconnects devices by using the network coordinator that implements security and forward frames to their destination. Network layer of the coordinator starts a new network and assigns an address to newly connected devices. Multiple network topologies are supported by the network layer like star, tree, and mesh as shown in figure.

2.5.4 Application Layer

The application Layer is the upper most layer of the protocol stack and it holds the application objects. ZigBee specification divides the APL layer into three discrete sub layers:

- Application support sub layer
- ZigBee device objects, and
- Application framework which contains manufacturer defined objects.

2.5.5 The application objects (APO)

Application objects are responsible to control and manage the layers in ZigBee devices. It is a type of software that controls the hardware. Each application objects allots a specific end point number that other APOs may use an addition to the network device address for interaction. There could be approximately up to 240 application objects into one ZigBee device.

2.5.6 Zigbee Device Object

The key description of ZigBee is the ZigBee device object, that performs three main functions: security, service discovery & binding. The function of discovery is to find out nodes and ask about the MAC address of the coordinator or router by using the unicast messages. The discovery also facilitates the procedure for finding some services through their profile identifiers. The security services in the ZigBee device object are responsible to authenticate and derive the required keys for data encryption. The role of binding manager is to bind the nodes to recourses and applications also bind the devices to channels. Application support sub layer: The APS sub layer is an interface between the Network layer and the APL layers. The APS sub layer processes incoming and outgoing frames to securely receive/transmit the frames and establish or manage the cryptographic keys[38].

2.6 Zigbee Components

ZigBee Coordinator (ZC) or Gateway (GW) one for each ZigBee Network initiates and configures network formation; acts as an IEEE 802.15.4 Personal Area Network (PAN) Coordinator; acts as ZigBee Router (ZR) once the network is formed. Full Functional Device (FFD) implements the full protocol stack if the network is operating in beacon-enabled mode, the ZC will send periodic beacon frames that will serve to synchronize the rest of the nodes. In a tree network all ZR will receive beacon from their parents and send their own beacons to synchronize nodes belonging to their clusters.

ZigBee Router (ZR) participates in multi-hop routing of messages in mesh and cluster-tree networks (in the latter case they are also called Cluster Heads (CHs)); associates with ZC or with previously associated ZR in cluster-tree topologies; acts as a local IEEE 802.15.4 PAN Coordinator; is a Full Functional Device (FFD) implements the full protocol stack.

ZigBee End Device (ZED) contains just enough functionality to talk to the parent node (either the Coordinator or a Router) it cannot relay data from other devices. This relationship allows the node to be asleep a significant amount of the time thereby giving long battery life. A ZED requires the least amount of memory, and therefore can be less expensive to manufacture than a ZR or ZC[30].

2.7 Topologies

“Topology” refers to the configuration of the hardware components and how the data is transmitted through that configuration.[6] They describe the physical and logical arrangement of the network nodes. Topology structures depending upon the position of devices, such as Coordinator, Router and end devices, has been depicted in the figures below. [32] There are three network topologies i.e. Star topology, Mesh topology, Tree topology.

2.7.1 Star Topology

Its structure is very simple so it can be easily configured. It can support up to 6000 devices. But still there are some disadvantages: If centrally positioned coordinator fails to work due to some technical fault, then whole network fails because all traffic go through the center of the star. Also due to this reason, traffic can be easily bottleneck at the coordinator, so this topology does not provide reliable transmission[39].

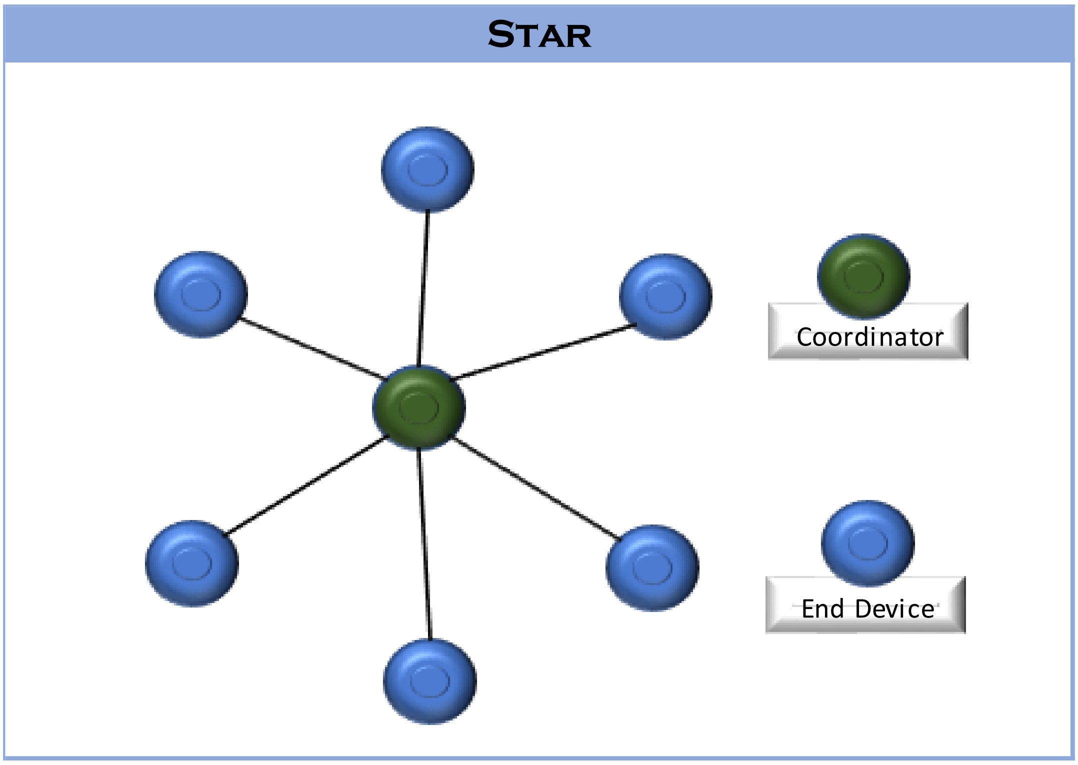


Figure 2.9: Star Topology

This topology is moderate on power saving because only end nodes can communicate to the coordinator or routers in activate mode and can go to sleep mode when there is no traffic. There are low overheads as packets are transited only between coordinator and end devices.

Collision is low when number of devices are at certain level and increase rapidly when no. of devices increases. Due to low collision, packet delivery ratio is high therefore maximum number of packets reach their destination. Reliability is considered low because if coordinator fails whole network fail. All end devices connect to one coordinator leaving users with little or no options for scalability. Only coordinator of capability of relaying message. Fading may be high because it operates in line of sight and due to obstacles in path of transmission. There is no alternate path to mitigate some of these challenges which may occur.Some of its advantages are but not limited to easy configuration, low complexity, less number of hop count, suitable for small and simple network

2.7.2 Tree Topology

In tree topology, Coordinator is positioned at the root of the network as shown in figure 2.10. Number of routers and end devices can be connected to coordinator and number of end devices can be connected to routers as children. Only routers and coordinator can act as parent nodes not end devices because end devices have no ability to relay message. When any node want to send message to other node then it send message to its parent node which is one

level higher than it, then that message is relayed higher and lower until it reach to its destination. This is not much reliable because a message can take only one potential path. Due to this if any router fails to work then its children (end devices) also stop working.[32]

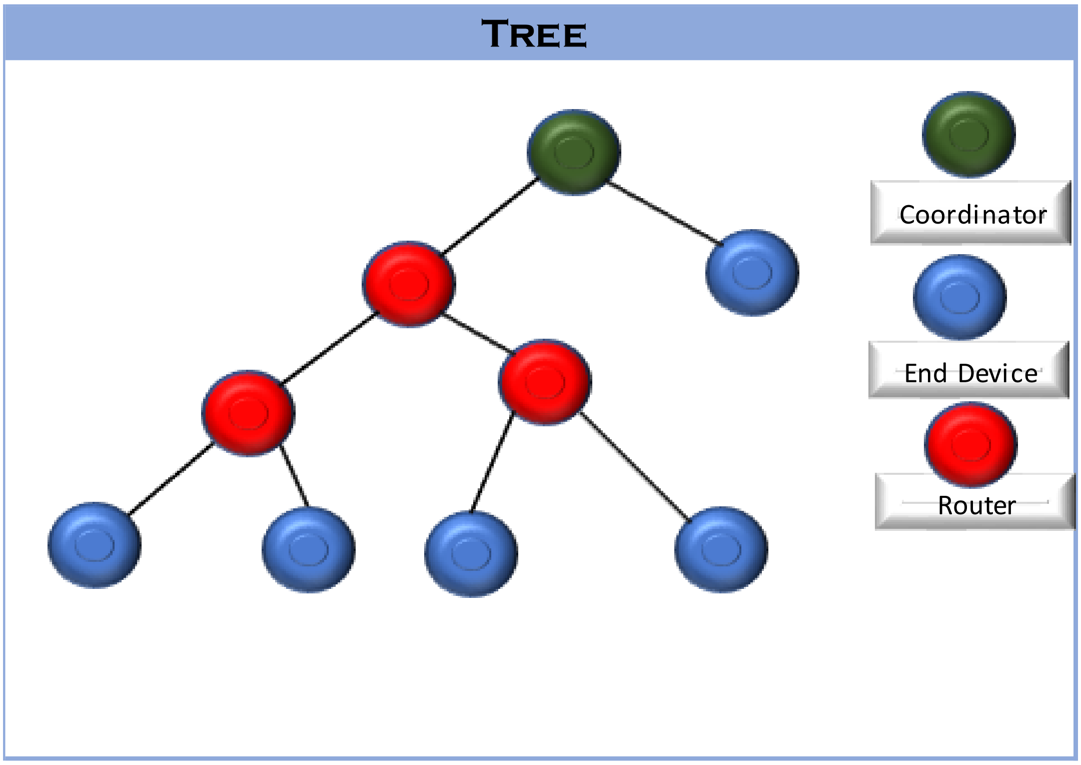


Figure 2.10: Tree Topology

Power saving is moderate because only end nodes can communicate to the coordinator or routers in activate mode and can go to sleep mode when there is no traffic. The minimum number of hops is 2 and the number increases depending on the depth of the tree network. Collision is moderate and increases sharply when number of devices increases. This also has an effect of reducing the Packet Delivery Ratio – PDR.

Duplication of packets is low because all packets go through parents(routers) which check if it is a duplicate and if it is discarded by router. Reliability is moderate if router fail all its children cut off from the network. However, this does not affect the rest of the network. The structure of this topology makes it highly scalable as there can be a number of routers and end devices in parent child relationship. Overheads are high because there can be number of routers and end devices in parent child relationship. There is no alternate path and fading may be high when it operates in line of sight and due to obstacles in path of transmission. It provides high scalability and suitable for large networks.

2.7.3 Mesh Topology

Mesh (decentralized) networking is a type of network topology in which a node (device) transmits its own data as well as serves as a relay for other nodes. In other words, all nodes cooperate in the distribution of data in the network[40] . It is not a new concept at all, as it had emerged from the Multiple Ad Hoc Networks in the 70s from Packet Radio Network (PRNET) created by The Defense Advanced Research Projects Agency (DARPA) of the U.S. Department of Defense. Later in the 90s, many other civil solutions had also been proposed and created for different uses such as mesh routers form a mesh of self-configuring, self-healing links among themselves[41].

This is the most flexible and reliable topology because there are number of potential paths for a message. If any router fails to work then ZigBee’s self-healing mechanism search for another path and message can be relayed through other path[32].

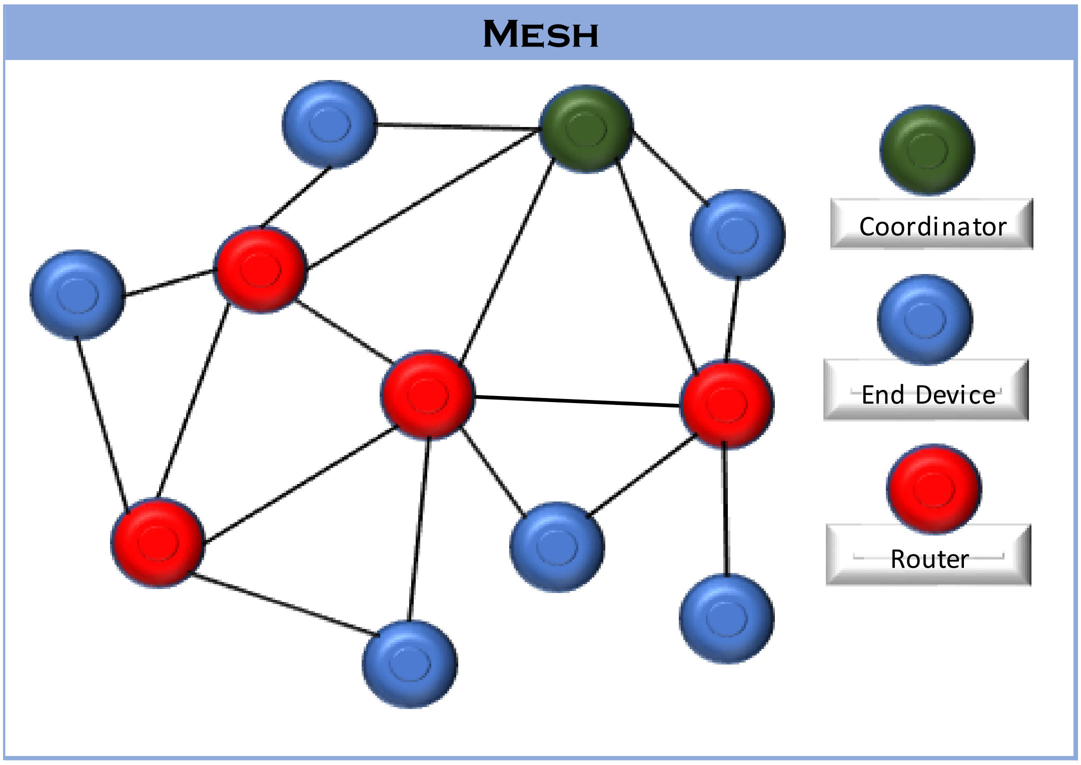


Figure 2.11: Mesh Topology

Power saving is high because all devices communicate in active mode and all devices are allowed to sleep to save the power in sleep mode. Collision is high due to multipath and increases sharply when number of devices increases decreases sharply due to excessive collision, but it is slightly more than tree because of its multi-hop nature. Duplicate packets are high due to multi-hop and collision. Reliability is high because if one device fails only that device cut off from the network. Scalability is high because there can be number of routers and end devices at any place. Overheads depends upon number of end devices between sender and receiver. Fading is low because when it operates in line of sight and due to obstacles in path of transmission an alternate path can be utilised. It is most reliable topology. It reduces fading, provide mobility and scalability and save much power.

2.8 Mobility in Zigbee

Mobility plays important role in ZigBee network. All the devices in ZigBee are mobile and static. Static devices do work in static state and remain in same state but mobile devices can move.

In Tree topology, Routing of mobile end devices rely on its parent. If child end device moves outside the range of its parent and come in the range of different parent then new address is allocated to the child. Transmission interrupted till the end device does not acquire the new address and resumes transmission after route discovery and device discovery process triggered. All the children depend upon its parent router, if router move and connect to new parent then it acquire new address but as well as its all children also have to change their address. Sometimes it faces inconsistency and device discovery process faces much difficulty in recovery [42] .

In Mesh topology, if end device move out of its router range and come in new router's range then it acquires new address. Transmission interrupted for the time when devices loss its old address and get new address. Then device discovery process triggered and transmission resumes. In mesh topology routers have in built capability of route recovery and only acquire -new address if routing table runs out of its capacity [43].

2.9 WSN Challenges

WSNs face several challenges that need to be considered during the design and deployment of WSNs. Most of these challenges are related to communication protocols used in WSNs. The most important challenges are as follows:

2.10.1 Energy - Efficiency (Limited Power Resources)

Most of the WSNs are battery powered, which limits power resources and thus requires ways to maximize the average lifetime of the nodes in a WSN, especially in those applications where deployed nodes are hard to reach in case of battery failure. Many researches were carried out to find ways to maximize battery powered WSNs and to efficiently manage power resources mainly focusing on how to reduce power consumption of the communication protocol used in the WSN which dissipates most of the power during Tx/Rx of data such as in where Gharghan, Nordin & Ismail proposed an energy-efficient transmission method known as the sleep/wake algorithm for a bicycle torque sensor node[44]. The study aimed to emphasize the trade-off between energy efficiency and the communication range between the cyclist and coach. It conducted two experiments where ZigBee (XBee S2) protocol was utilized in the first experiment, and the Advanced and Adaptive Network Technology (ANT) protocol based on the Nordic nRF24L01 radio transceiver chip was used in the second experiment. Also, ANT current consumption was measured and simulated as well as comparing it to the XBee S2 based torque sensor node.[45]

2.9.2 Noisy Channels, Co-Interference, and Network Coverage

Wireless protocols operate in different channel environments, which can be noisy and represent a challenge for WSN robustness in such channel conditions, especially in the harsh indoor channel environment where AWGN, Rayleigh, and Rician multipath fading is a critical issue to overcome. Another challenge is the cochannel interference due to other devices operating in the same frequency band, especially the popular 2.4 GHz band which is mostly used by WSNs and other devices. These challenges mainly affect the performance of the WSN and reduce the overall system coverage. Most of the wireless protocols cannot correct errors, and thus some research were carried out to solve this problem. In [10] Zhan et al. proposed to combine forward error correction (FEC) within the media access control (MAC) layer of the IEEE 802.15.4 standard for packets transmission. They aimed to avoid the time and energy consuming mechanism (namely the automatic repeat request (ARQ) mechanism) used by WSNs in the noisy wireless channel scenarios within the smart building environment. They have investigated the performance of convolutional codes (CCs), Reed-Solomon (RS) codes, and their concatenated codes in terms of bits error rate (BER) and packets error rate (PER) using the developed CPS simulation platform and was applied to different code rates and packet lengths. The achieved results showed that in most cases CCs proved to be superior compared to other codes. They also found that for longer packet RS codes with larger symbol length are preferred.

Furthermore, the result also showed that RS and CCs concatenated codes are good candidates. As future work, they suggest considering the non-line-of-sight wireless channel and the pulse interference from other devices. Also, in [38] Romia, Ali & Abdalla proposed to incorporate a recursive least square (RLS) based adaptive linear equalizer (ALE) to the physical layer of the receiver side aiming to improve the ZigBee performance in harsh transmission channel effects. They investigated the performance of the system for different multipath fading channels, including Rayleigh and Rician. Moreover, they proposed a methodology for deciding design parameters of the RLS based ALE’s where these parameters are chosen to obtain the best performance in terms of BER and convergence response time. The design procedure is based on solving multiple objectives optimizing function using genetic algorithms.

Finally, for verification purposes, the designed system was also modeled and tested in MATLAB Simulink as well as comparing the performance of the RLS adaptation algorithm with the least mean square (LMS) one. According to the achieved results, they found that the RLS based ALE was able to remove the inter-symbol interference and recover the original signal efficiently with least BER concluding that the RLS algorithm offers the best ZigBee performance with least BER and fast convergence compared with the LMS technique. Aiming to reduce the packet drop rate, energy consumption and collisions in the buffer constraint sensor devices in [39] Sahoo, Pattanaik & Wu designed a new channel access mechanism which includes a new frame structure, a new superframe structure, and a modified superframe structure with a new retransmission opportunity. These designs lead to

1) avoiding collision due to the hidden terminal problem,
2) mitigating the problems due to Wi-Fi and ZigBee interference, and
3) reducing the collisions and retransmission delay with high reliability respectively.

According to the performance evaluation and validation of their design, they indicated that significant improvements could be achieved in terms of throughput, packet drop rate, energy consumption, reliability, and average delay of the nodes.

2.9.3 Quality of Service (QoS)

QoS is an important parameter that specifies the overall performance in any WSN in terms of different factors such as response time, packet drop rate, packet delivery ratio, transmission delay, and throughput. Therefore, analyzing QoS parameters represents a challenging task in WSN design which is directly related to other constraints and challenges that affects the system performance. Where aiming to analyze the QoS parameters in ZigBee network, authors in [52] implemented a ZigBee Network based on node priority, which demonstrates a method to generate a new priority of devices with respect to their existing priority and zones' priority as well. They analyzed QoS based on the new priority status for task preference purposes. The results were obtained by performing a simulation study. The achieved results showed that the QoS of the network is more conspicuous than the non-priority based network. Authors in [9] proposed a smart distribution power grid architecture with Cyber-Physical System (CPS) enabled micro-grids that meet almost all smart distribution power grid functional requirements. They have also presented a six-tier communication topology derived from the architecture for a smart distribution power grid for an easy transition to an optimal communication architecture.

2.9.4 Localization and Distance Accuracy

For location-based WSN applications, localization accuracy represents a significant challenge that has gained attention from various researchers. Thus, aiming to improve localization and distance measurement accuracy of WSN used in track cycling applications proposed two soft computing localization techniques (Neural Fuzzy Inference System (ANFIS) and Artificial Neural Network (ANN) which was hybridized individually with three optimization algorithms namely Particle Swarm Optimization (PSO), Gravitational Search Algorithm (GSA), and Backtracking Search Algorithm (BSA)). These two techniques emphasis on the received signal strength indicator (RSSI) measurement carried out from the three ZigBee anchor nodes scattered throughout the track cycling field. They aimed to estimate the distance between bicycles moving on the cycle track for outdoor and indoor velodromes.

The achieved results showed that the hybrid GSA-ANN performance is the best compared to other methods in terms of accuracy localization and distance estimation accuracy as well as achieving a mean absolute distance estimation error of 0.02 m and 0.2 m for outdoor and indoor velodromes respectively. The results indicate that GSA-ANN is appropriate in both indoor and outdoor environments and applicable to any static or mobile WSN node.

However, the study has a drawback, which lies in the possibility of implementing such a technique in real time where ANN requires a considerable amount of memory. To solve this issue, a microcontroller with high speed and large memory size like Arduino Due is required which results in high power consumption, large size, and extra weight, all of which are considered critical issues in bicycle sensor nodes. They expect that these challenges can be avoided in the future once quantum computing is in place.[45]

2.9.5 WSN Related Security Threats

Adversary can easily exploit the confidential information that IS being transmitted wirelessly in WSNs. A signal from a legitimate wireless sensor can be captured by an illegitimate wireless sensor to achieve the desired goals. "In wireless sensor network communications, an adversary can gain access to private information by monitoring transmissions between nodes. For example, a few wireless receivers placed outside a house might be able to monitor the light and temperature readings of sensor networks inside the house, thus revealing detailed information about the occupants' personal daily activities".[46]

Identifying the behaviour of data transmitted within the WSN can also be very helpful for an adversary to plan the strategy of attack. If we think from an adversary's mind, the first step we will think of is to monitor how the targeted WSN is working. And for that reason, we'll first try to listen to the wireless data and see what sort of encryption is involved, what is the structure of each packet, what kind of data each mote is transmitting, and ultimately figuring out which mote worth more and which one is less worthy for us. "Different advantages for the attacker result from eavesdropping data. On one hand, the attacker can sniff potentially confidential data. On the other hand, it enables the attacker to perform statistical traffic analysis for deducing which motes pose the most worthwhile targets" [47].

If the adversary is intended on affecting the performance of the WSN, the simpler way would be to put extra load on the network. This can be done by adding a node into the network which pretends to be a legitimate one and then it starts sending false data continuously to the neighbour nodes until they get exhausted. Another way would be to interfere the transmission and dropping the data of the packet a legitimate node transmits. "A further threat to WSNs is dropping data which can be considered as Denial of Service (DoS) in a broader sense. A simple and effective attack is to jam the wireless channel. Nodes trying to send under this attack[46].

Subuh Pramono et al, conducted RSSI analysis to measure how strong the signal is for each node placement and to analyze whether it is related to the quality of service (QoS) results obtained. This model used in that research is ZigBee protocol that supports star topology and mesh topology. [27]

Helmy Fitriawan et al, paper reports the performance analysis of developed ZigBee based WSN. Several QoS parameters are considered in the analysis, i.e. throughput, packet delay and packet loss. [48]

As shown, above research on QoS such as throughput, packet loss and ETD are common. However, more use of ZigBee networks has presented more challenges. Power challenges and initiatives like smart rural have made the battery-powered sensing nodes become a necessity. Methods for conserving their internal power to extend the lifespan and maintain the coverage of the overall network have become increasingly important especially after the world was hit by a health pandemic of Covid 19 in the year 2020 and the public was being encouraged to stay at home. [49]

Kompal Gupta et al , proposed future work that is associated with the study of energy-efficiency and reliability of all these topologies separately, i.e. emphasis will be placed on developing protocols that would continue the battery life, as well as access to the source code of the network and the application layers. [36]

Currently most of security modes of ZigBee still stay in theory stage. Most researchers focus on the applications of ZigBee . [37]

2.10 ZigBee Challenges

While Zigbee fall under the WSN family, there are some challenges which are unique to it. However, there is need to focus on the challenges and gaps as detailed below:

2.10.1 Zigbee Vulnerabilities

Many efficient and secure enhancements have been done to the ZigBee standard since the first version of 2004; its low computing power would make it more susceptible to network attacks though. As discussed in the previous section, ZigBee is characterized in a few built-in security

services and features, however; its applications are still vulnerable to network attacks as in sniffing the network key which is sent in plaintext for instance. Consequently, it is vital to value network and security threats on ZigBee standard, evaluate their severity impact, and later to suggest proper security controls and countermeasures. As with any wireless sensor network (WSN), threats can be identified by how attacks are accomplished, what layer of the communication stack these attacks are recognized in, whether the intended malicious node is part of the network or not, and finally to which part of the network the attack is targeting. [50]

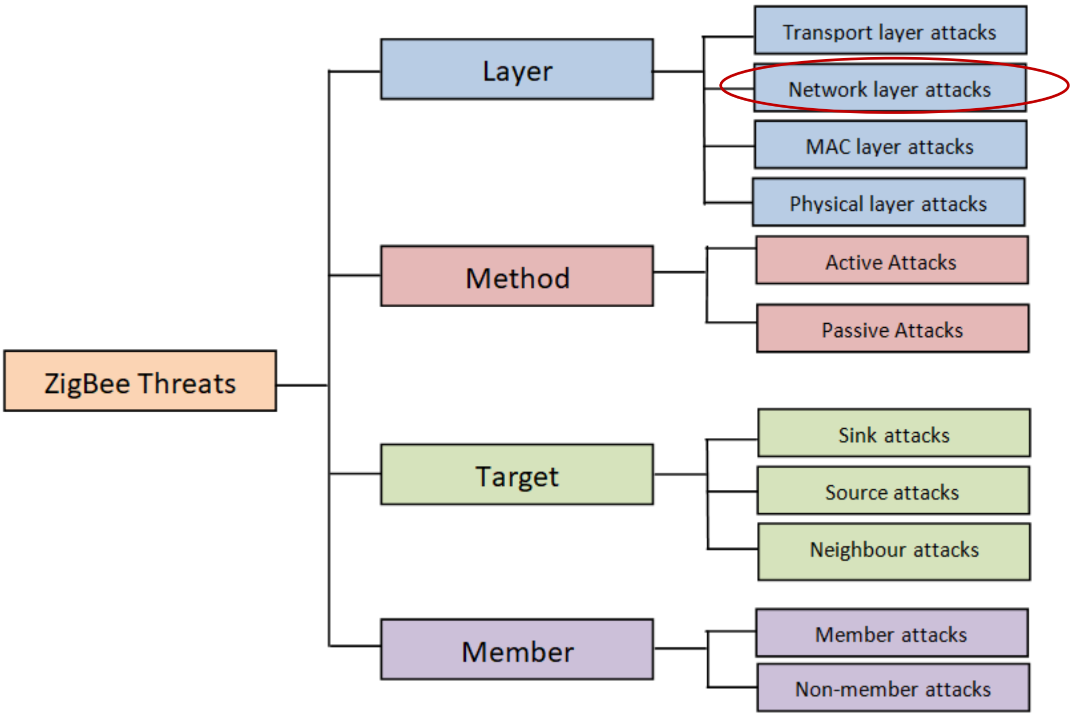


Figure 2.12: ZigBee possible threats and attacks[51]

The figure above illustrates ZigBee possible threats and attacks through adopting the WSN threat model. Attacks may vary from eavesdropping the radio channel of ZigBee network so that to add malicious contents or to replay old packet, to more sever attacks as in adding a malicious node to the network to overwrite the memory of normal deployed node. As depicted in Figure 2.12, attacks on ZigBee can be categorized into the following:

Layers Attacks

1. Transport Layer Attacks: This layer is utilized to support communication links for sensors newly joining the network. Attacks might include flooding and desynchronization; where the targeted node is flooded by a numerous number of invalid connection establishment requests (flood attack), and forging packets to one or both ends of connection so that host requests to
retransmit the missed packet frames (de-synchronization attack)[52].

2. Network Layer Attacks: This layer is responsible for routing process and network traffic as well. ZigBee nodes are always assigned in no man's land, so we often meet with nodes invalidation, destroyed or captured. It’s necessary for us to update and change network nodes. Attackers always tap the communication of nodes by assigning some malice ones or joining a large number of false messages to make the network paralysis. There are some typical types of insider network attacks such as sinkholes, sybil, wormholes and selective forwarding attacks.[53]

In the wormhole attack, there should be two malicious nodes that are located on different hops of the network. When a sender node transmits a data frame, one malicious node tunnels this data to the other malicious node and by which it will send it to the neighbouring nodes in turn. Consequently, the sender node is tricked that malicious nodes are close by one or two hops where these two malicious nodes might be out of range.[51]

3. MAC Layer Attacks: It incorporates the MAC header that helps the receiver to know the length of the packet, retransmits of frames in case of errors, and allocates resources for newly joined nodes. Link layer jamming is one example of MAC layer attacks that is launched to
create DoS by interrupting messages exchange between transmitting and receiving nodes. This would degrade and reduce the performance of the network consequently [54].

4. Physical Layer Attacks: Attacks are mainly exploiting the common radio signal by jamming to either eavesdrop or tamper the data packet frames [50].

Method Attacks

1. Active Attacks: This attack requires an actual interception of the network where the adversary can modify the data, inject fault data frames, consequently; the network performance is negatively affected. Moreover, data integrity and confidentiality are compromised [55].

2. Passive Attacks: Unlike active attacks, no actual interception of the real communication stream, but rather attacker monitors the data traffic without affecting its integrity. However; the confidentiality of information is exposed as sensitive information can be collected for

some other malicious intent [55].

Target Attacks

1. Sink Attacks: Sinkhole or simply the sink attack can take place when a malicious node announces a route to be the shortest path. And since all routing algorithms o select the shortest path, it will attract more network traffic to be tunnelled toward it. Usually, this attack is combined with wormhole attack[56] .

2. Source Attacks: In these attacks, the adversary compromises one legitimate node to act as a black hole node; a node that selectively drops received packets or all received packets to trick other neighbouring nodes to search for another rout as the previous one has failed [57].

3. Neighbour Attacks: This type of attack exploits the process of discovering other neighbouring nodes by broadcasting HELLO message. A malicious node sends HELLO message with a high transmission power, and hence the receiving nodes consider this node as its neighbour and will send the sensed packet data in return. Consequently, a huge amount of energy will be wasted, and congestion might occur consequently [58].

4. Member Attacks: Sometimes are referred as outcast and insider attacks. In the case of outcast attacks; the attacker node is not part (non-member) of the network but authorized to threat the network. On the other hand, the insider (member) attack takes place when a malicious node is part of the network either by compromising it or the attacker has loaded a fake profile
and asked to join the network[59].

5. Energy Depletion Attack (Ghost Attack): attacker sends faked messages to lure node to intentionally to deplete that node's energy by redundant security-related computations. This will cut back the node's lifetime and enable the attacker to launch several after-depletion attacks as in Denial of Service (DoS) and reply attacks accordingly [60].The sequential freshness is obtained by preventing message replay in IEEE 802.25.4. The receiver rejects those frames in which the counter value is equal to less than the last received counter value. This replay protection mechanism can lead to Denial-of-Service attack as the attacker sends a number of frames containing large

but different counter values. The receiver on receipt of these frames sets the counter of the last received frame to these exceptionally large values and thus when it receives legitimate frames with a reasonably sized counter value, the frame is discarded by the receiver for the purpose of replay protection and thus leading to denial of service[30].

2.10.2 Challenges and Gaps in Security

Security is a critical concern in many IoT applications [1] [49] [36] .The IEEE 802.15.4 standard addresses the security requirements through a medium access control (MAC) layer package, providing fundamental security services ranging from data confidentiality, data integrity to replay protection [8]. Despite these basic services, several security challenges and pitfalls, especially pertaining to the initialization vector management, key management and integrity protection. More attacks on the physical and MAC sub-layers, including jamming, capture and tampering, exhaustion, collision and unfairness [61].

Besides, today off-the-shelf attack toolkits [62] such as KillerBee are available that can be leveraged even by a novice adversary to explore and exploit the security of ZigBee networks. Using KillerBee and an IEEE 802.15.4 compatible radio interface, an adversary can carry out several attacks ranging from surreptitious eavesdropping to traffic injection with a little or no effort[63] . This shows that there is great need for more research work on security issue with the view to improve it.

2.10.4 IoT Worm Hack on Philips Hue Light Bulbs

In November 2016, a paper was published to explain the attack targeted on Philips Hue Light Bulbs that implemented with Zigbee standard. The researchers used a drone to target Philips Hue Light Bulbs and infected the light bulbs with a worm/virus that gives the attackers the ability to turn them on and off. Interestingly, the attackers controlled the lights to a Morse code "SOS" message[64]. This attack exploited the hard-coded symmetric keys on the light bulbs to control them through the Zigbee network. The worm was able to attack a light bulb from up to 400 meters away and then spread to nearby bulbs because Zigbee uses hard-coded skeleton keys. In more details, the worm tricked Philips into release an automatic update for the bulbs and bypassed the built-in security safeguards against unauthorized remote access. Then, the attackers were able to easily decrypt the AES-CCM key that is used in all Hue light bulbs.

The worm can then spread to close-by bulbs using the Zigbee wireless network thereby affecting the network layer as highlighted in figure 2.12 [62]. After publishing the paper about the attack, Zigbee quickly issued a response. They claimed that the vulnerability was not part of Zigbee standard, but rather an internal implementation error made by Philips. From this attack, we can see that even though Zigbee Alliance tries its best to ensure the security of its standard, they do not have complete control over how other companies implement the protocol and some erroneous implementation could lead to security weaknesses.[65]

2.10.5 Challenges and Gaps in Energy Efficiency

Kompal Gupta et all, noted that future work should be associated with the study of energy- efficiency and reliability of all these topologies separately, i.e. emphasis will be placed on developing protocols that would continue the battery life, as well as access to the source code of the network and the application layers[36] . This shows the need for more research in the area of energy efficiency. This cannot be over emphasised as our energy (electrical power) deficit as our country(Zambia) is facing load shedding.

Battery-powered wireless sensor nodes are also fast becoming the most popular sensor components in wireless home security systems, therefore significant attention is being given to developing efficient methods for extending the battery life of sensors, and thus the lifespan of the overall network [49].

2.11 Related Works

In [6] ,the paper analysed the ZigBee/IEEE 802.15.4 standard using three possible topologies in ZigBee WSN Networks. In this work we provided a versatile analysis of the characteristics of the IEEE 802.15.4 topology formation process and the significant impact on the overall network performance using different parameters like throughput, MAC Delay, No. of Hops, Network Load etc. The results show that tree topology outperforms among all other topologies. We performed an extensive simulation analysis, combined with a topological variation parameter related ZigBee wireless sensor network i.e. WPANs. The analysis is usable to configure IEEE 802.15.4/ZigBee procedures and in selecting the related parameters of ZigBee PAN Network. Overally, the performance evaluations demonstrated that the ZigBee can only be use for low-data rate and low-power smart grid applications not having very high reliability requirements and real-time deadlines.

In [66] .the appropriate network topology that will support the architecture in such a way as to reach a very high-performance level. The network architecture of a street lighting control system has a series of specific characteristics: it is of the long-thin type, it may incorporate up to a few hundred nodes distributed on a wide geographical area and it has a central sink node that collects all the data. In light of the above essential factors, the objective of this paper is to assess the performance of the mesh and tree network topologies that can be implemented within a street lighting control system based on a ZigBee communication protocol. As far as the end-to-end delay is concerned, both types of simulated network topologies behave similarly. When employing the tree network topology, the network load is divided among the coordinator and the local routers, thus reducing collisions and the number of lost packages. Therefore, the performance of the tree network topology far outbalances the benefits of a mesh topology. The number of hops performed in a mesh network is much higher than that of a tree topology. This particular characteristic may equate a lower power consumption than that required by tree network topologies if the nodes are battery-powered. The tree topology performs highly better than mesh topologies when implementing a street lighting control system.

In [56],an evaluation on the performance of wireless sensor network with wormhole attack is carried out. Wormhole attack is a prominent attack that forms a serious threat in a wireless Network. Detecting and eliminating such an attack is a very challenging task till now. It is to be noted that the results obtained and analyzed here are specific to particular scenarios. On analyzing the simulation results it is observed that the average end to end delay in the scenario with attack is increased by 9%. Similarly the data dropped also shows a significant increase of 50%. From the simulation results it is evident that the performance of the sensor network under study with wormhole attack is getting degraded. It is obvious that the load offered on the network with an attacker is more compared to the network without an attacker.

2.12 Chapter Summary

This chapter has outlined the exponential growth of WSN. While there are a number of technologies under WSN, focus of this research is on Zigbee. Though it is generally low in energy consumption, there is need to calculate the energy efficiency and how it is affected by the topology implemented. In this chapter, we listed some of the challenges related to energy, QoS and security have been reviewed in detail.

CHAPTER 3 – METHODOLOGY

3.0 Chapter introduction

This chapter looks at how the research was done, step by step to answer the research questions which were presented in chapter one. First, we will look at the research design which briefly outlines the methods which were used to answer the research questions. Detailed step by step approach taken to undertake the research are then outlined using the research methodology process.

3.1 Research design

This study is quantitative and specifically adopts simulations to implement Zigbee model design. It is meant to develop a decision support model that would help ICT professional to test the energy efficiency in relation to topology of a Zigbee network before it is deployed.

3.2 Research Methodologies

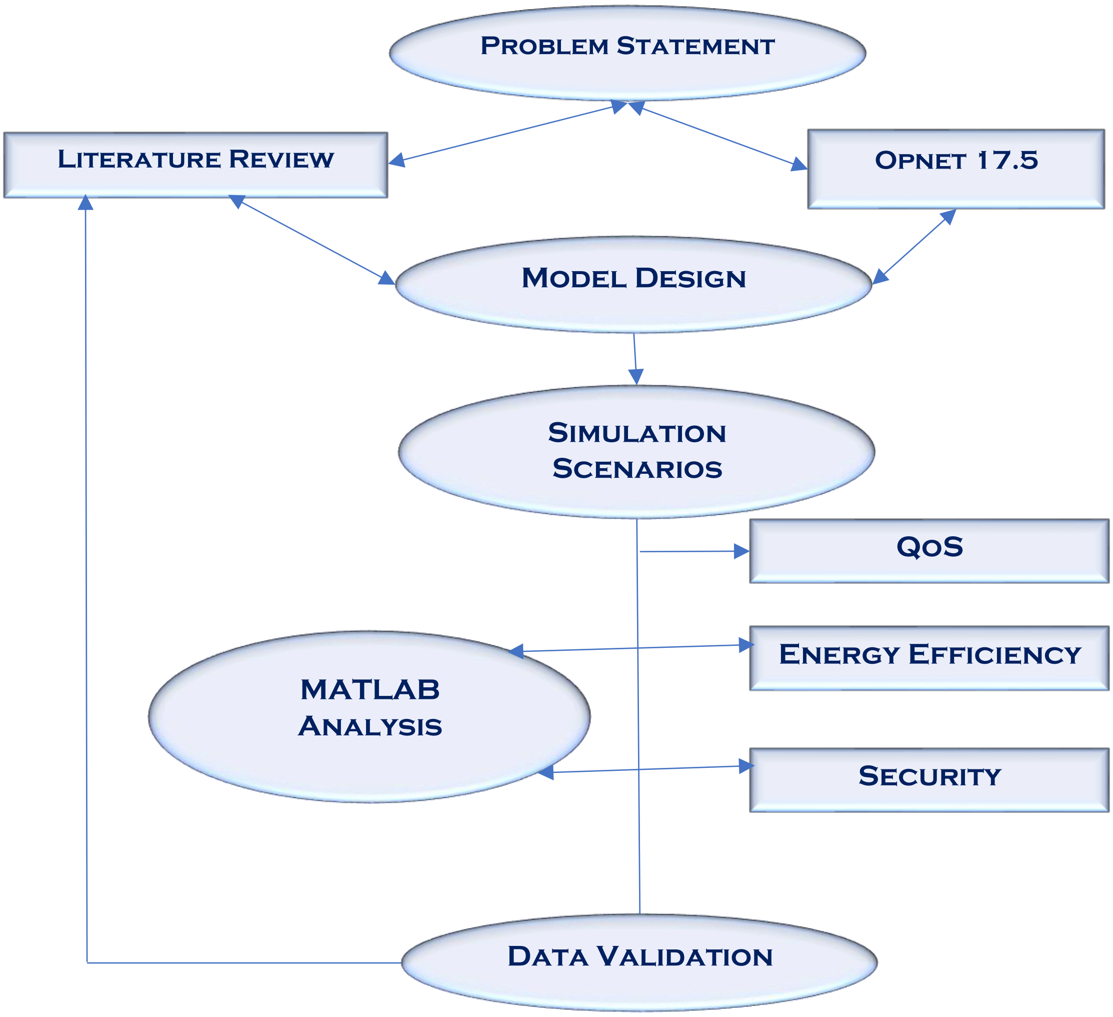


Figure 3.1: Research Methodology Process

Simulation can be described as a method of designing a model of a real system under investigation and performing experiments to understand the behaviour and response of the system under different conditions and changing parameters (Banks 1999). For the simulations to be useful, the behaviour of the model is expected to closely mimic the response of the system being observed. Discrete event simulation is the most widely used tool to study the behaviour of communication networks and also to predict the behaviour of complex stochastic dynamic systems modelling real world applications of practical interest.

3.3 Modelling WSNs Using Simulators

With the development of the information era, existing networks become larger and larger and their structures become more and more complex. Before upgrading existing networks, building new networks, or testing new protocols, the performance of the whole network shall be analysed and evaluated effectively and objectively. When planning and designing networks, developers not only need to develop a new network protocol but also need to build a network algorithm. When building networks, network experts shall use existing resources efficiently to get the optimal network performance. Traditional network design and planning mainly depend on experience and scientific methods such as analysis and experiment. Analysis aims at the preliminary analysis of research objects and the dependent network system.

Based on certain limiting conditions and reasonable assumptions, the research objects and system are described; the mathematical analysis model of research objects is abstracted and is then used to solve problems. The experimental method is to design a reasonable hardware and software configuration environment, build a test bed and lab, and research the protocol, behaviour, and performance of the real network. When the network becomes larger and larger, it is difficult to design the network using experience and mathematical analysis only. And it is difficult to guarantee accuracy. The experimental method is seldom used because its cost is high, and it can be easily influenced by environmental factors. Therefore, a new network planning and design method is increasingly needed for network design. As an objective and reliable network planning and design technology, network simulation emerges at the right moment. Network simulation can verify several different design plans at the same time and obtain quantitative network performance forecast data, which offers a reliable basis for verifying and comparing plans. Therefore, it is becoming a more and more popular method in network planning, design, and research[3].

Simulation is a very powerful and flexible tool. Many system configurations can be controlled to study the complexity and reality that can be achieved by the simulation model. The objectives of a simulation are to draw conclusions that are meaningful, and of practical importance. The actual definition of what aspects of the system under investigation should be included in the simulation model and the required level of detail are the central design choices constraining the quality of the final output and of the derived conclusions.

3.3.1 Simulator: Selection Criteria

This research involves the discrete-event simulations of the performance of ad hoc wireless sensor networks, including the use of energy which determines the life of the network. Therefore, there is a need for selection criteria for the type of simulator that will be required. Different simulators, either open source or commercial have many modules that are essential for our research e.g. the energy model, while others that don't have the required models or are only available as purchasable modules. The simulator needs to be customisable as it may also be required to run the simulations with some of the trace options turned on while others trace options switched off e.g. if the packet delivery is only being monitored at the MAC layer, then there is no need for the traces of packet handling at network and transport layer.

In some cases, we may only want to monitor the network energy consumption, then we will not be interested in the rest of the OSI reference model, and hence the trace support for them modules can be switched off (even though all those events would be taking place, but to reduce the size of the trace file, and to increase the speed of the simulation, they will not be recorded). Another key advantage is to have a simulator that can run on multiple platforms, e.g., Windows and Linux. Many simulators are written for Linux OS as they are open source and can easily be modified and execute much faster in that environment as compared to when they are transported in Windows OS. Many network simulators come with some sort of topology creation tools that allow the researcher to create large network topologies using simple script or configuration languages. As the simulation networks become larger, we will require the use of such tools to create large topologies, hence having such support in the simulator will enhance our work.

3.4 Network Simulators Considered

The networks , which satisfy most of the characteristics mentioned above are Omnet++ , OPNET, MATLAB and NS3.

3.4.1 Omnet ++

OMNET++ (Object-oriented modular discrete event simulator)3 is a modular discrete event simulator implemented in C++. Getting started with it is quite simple, due to its clean design. OMNET++ also provides a powerful GUI library for animation and tracing and debugging support. Its major drawback is the lack of available protocols in its library, compared to other simulators. However, OMNET++ is becoming a popular tool and its lack of models is being cut down by recent contributions. For instance, a mobility framework has recently been released for OMNET++, and it can be used as a starting point for WSN modeling. Additionally, several new proposals for localization and MAC protocols for WSN have been developed with OMNET++ under the Consensus project, and the software is publicly available. Nevertheless,

most of the available models have been developed by independent research groups and don’t share a common interface, which makes it difficult to combine them.

Advantages of OMNET++:

- Strong structured.
- Extremely modular.
- Not limited to network protocol simulation.
- Source code is openly available.
- Simulation model for internet, IPV6, mobility is also accessible.

Disadvantages Omnet++:

- It does not offer a great variety of protocols.
- Users with significant background work.
- Poor analysis and management of typical performance.
- The mobility extension is comparatively incomplete.

3.4.2 OPNET

It is the leading network technology development environment in the industry at present. An object-oriented modeling method and graphical editor are used to effectively reflect the actual network structures and network components. An actual system can be visually mapped onto the model.

OPNET was created by two Massachusetts Institute of Technology researchers in 1986. Subsequently, as the tool of high-tech network planning, simulation, and analysis, it was acknowledged and used widely in the fields of communication, national defense, and computer networks. Nowadays, OPNET has entered the fields of military science, education, banking, and network operation. Business circles (such as Cisco) and operators (such as AT&T) use OPNET to carry out diversified simulations and debugging. After entering China in 1998, OPNET research and its application developed rapidly.

At present, many colleges and research institutions are using it, including Peking University, Beijing University of Posts and Telecommunications, Research Institute of Telecommunications Transmission of MIIT, China Academy of Telecommunication Research of MIIT, etc. Furthermore, Huawei Technologies Co., Ltd., Zhongxing Telecommunication Equipment Corporation, and Datang Mobile Communications Equipment Co. Ltd., also use OPNET as simulation software to optimize network performance and enhance the usability of network communications as far as possible[67].

OPNET Modeler Advantages

- Fast discrete event simulation engine
- Set of element library with source code
- Object-oriented modeling
- Hierarchical modeling environment
- Scalable wireless simulations support
- Customizable wireless modeling
- Discrete Event, Hybrid, and Analytical simulation
- Grid computing support

OPNET Modeler Disadvantages

- Complex GUI operation.
- It does not permit a set of nodes within a single connected device.
- Exactness of results is limited by the sample resolution.
- Simulation is incompetent if nothing happens for long periods.

3.4.3 MATLAB

MATLAB (Matrix Laboratory) is a fourth-generation, high-level programming language

for numerical computation, visualization, and programming, which can interact with the environment [68]. MATLAB was developed by MathWorks. MATLAB's power lies in the fact that it is used for every facet of computational mathematics. Some of the mathematical calculations that are commonly used are: Matrices Calculations, Array Processing , Multi-Dimensional Plotting, Curve Fitting ,Linear Algebraic Calculations ,Statistical and Data Analysis[68].

MATLAB is one of the nonstandard state languages. A collaborative environment for iterative investigation, the outlining of roles as well as critical thinking is provided by MATLAB. MATLAB optimizes a design to meet a custom objective and creates custom plots for devices.

MATLAB's modifying interface improves devices by enhancing code, model practicality, and by boosting execution.

Amongst its many uses is Signal Processing, Communications System , Image Processing, Video Processing, Control Systems, Testing, Measurement, Computational Finance, and Computational Biology

MATLAB Advantages

- Implement and test your algorithms easily
- Develop the computational codes easily
- Debug easily
- Use a large database of built in algorithms
- Process still images and create simulation videos easily
- Symbolic computation can be easily done
- Call external libraries

- Perform extensive data analysis and visualization
- Develop application with graphics user interface

MATLAB Disadvantages

- MATLAB is interpreted language and hence it takes more time to execute than other compiled languages such as C, C++.
- It is expensive than regular C or Fortran compiler. Individuals find it expensive to purchase.
- It requires fast computer with sufficient amount of memory. This adds to the cost for individuals willing to use it for programming.
- It is difficult to develop real time applications using MATLAB as it sits "on top" of windows.
- It is not free and hence users need to obtain licensed version from MathWorks, Inc.

3.4.4 NS3

NS-3 is a discrete-event network simulator, targeted mainly for research and learning use. Ns-3 is open software, licensed under the GNU GPLv2 license, and is publicly accessible for research, enlargement, and use. NS-3 is a C++ library which provides a set of network simulation models implemented as C++ objects and wrapped through python. The users usually interact with this library by writing a C++ or a python application which instantiates a set of simulation models to set up the simulation scenario of importance, enters the simulation main loop, and exits when the simulation is done[69].

NS3 Advantages:

- The system has been modularized
- To allow for modular libraries
- Individual modules contains with directory structure
- To allow the node to use external routing

NS3 Disadvantages:

- Ns3 suffers from lack of credibility
- Modules, component based on ns2

- Ns3 needs lot of maintainers
- Active maintainers are required

3.5 Selected Simulators

After reviewing four simulation software state above, the researcher selected OPNET and MATLAB for use in this research. OPNET was used to Zigbee network topologies and matlab was used to calculate energy consumption using QoS statistics obtained from scenarios simulated in OPNET.

OPNET

After reviewing several simulators, OPNET has been chosen as the best tool to carry out this

research. The selection of OPNET has been based on several factors as listed below:

Popularity : First and foremost is that OPNET is the most popular network simulator. It is widely used by the mobile and ad hoc research community and is also the most trusted among all the network simulators. OPNET is also considered by some researchers as a reference simulator and has much larger scientific acceptance .

Available on different platforms: Another great feature of OPNET is that it is free to download and can run on different platforms and has nearly all the pre-built components, incorporates modularity, scalability, and modifiability with all the source code unlike OPNET and QualNET that come along very heavy licensing fees. However the learning curve of OPNET is slightly steep and requires ability to program in C++.

Community : OPNET has got a very large online research and developer's community that is readily available via the free mailing list.

Easy deployment: OPNET have excellent graphical user interface for easy deployment of simulation networks, the core source code is not provided, and hence the inbuilt models cannot be modified as compared to NS3, which provides the code for all the modules.

MATLAB

After reviewing several simulators, MATLAB has been chosen as the best tool to carry out this

research. The selection of MATLAB has been based on several factors as listed below:

GUI: The graphical output is optimized for interaction. You can plot your data very easily, and then change colours, sizes, scales, etc, by using the graphical interactive tools.

Functionality: MATLAB's functionality can be greatly expanded by the addition of toolboxes.

3.6 OPNET Simulation SetUP

In this study, a wireless sensor network was designed by using different ZigBee topologies such as Star, Tree and Mesh. The goal is to simulate the evaluation and the analysis of the system designed and to be able to predict whether the real system results would be correct, the Riverbed (OPNET) Modeler Academic Edition 17.5 has been used as a simulation tool. Riverbed is a company that purchased the Opnet Company. This version of the program not only enables the development of robust network communication and various system models, but also communication between the administrator, the PAN coordinator, routers and end devices. [70]

In this study, a performance analysis of wireless sensor network topologies has been conducted using the ZigBee standard. Toward this end, four (4) different scenarios have been considered. The first three scenarios are based on topology, that is , star, tree, and mesh topologies were compared with respect to criteria like end-to-end delay, throughput, Mac load and traffic received.

The parameters used in the simulations are as below:

Parameters	Star	Mesh	Tree
No. of Sensor Nodes	10 | 20 | 30 | 40	10 | 20 | 30 | 40	10 | 20 | 30 | 40
Number of Retransmissions	5	5	5
Minimum Backoff exponent	3	3	3
Maximum Backoff exponent	4	4	4
Packet power Threshold	-80	-80	-80
Mesh Routing	Disabled	Enabled	Disabled
Transmission band (MHz)	2450	2450	2450
Transmit power	0.4	0.4	0.4
Transmit power(coordinator)	0.5	0.5	0.5
Packet size (bytes)	128	128	128
Packet inter arrival time(sec)	1	1	1
Data Rate (Kbps)	250	250	250

Table 3.1: Simulation Parameters

Scenario 1 : Star Topology

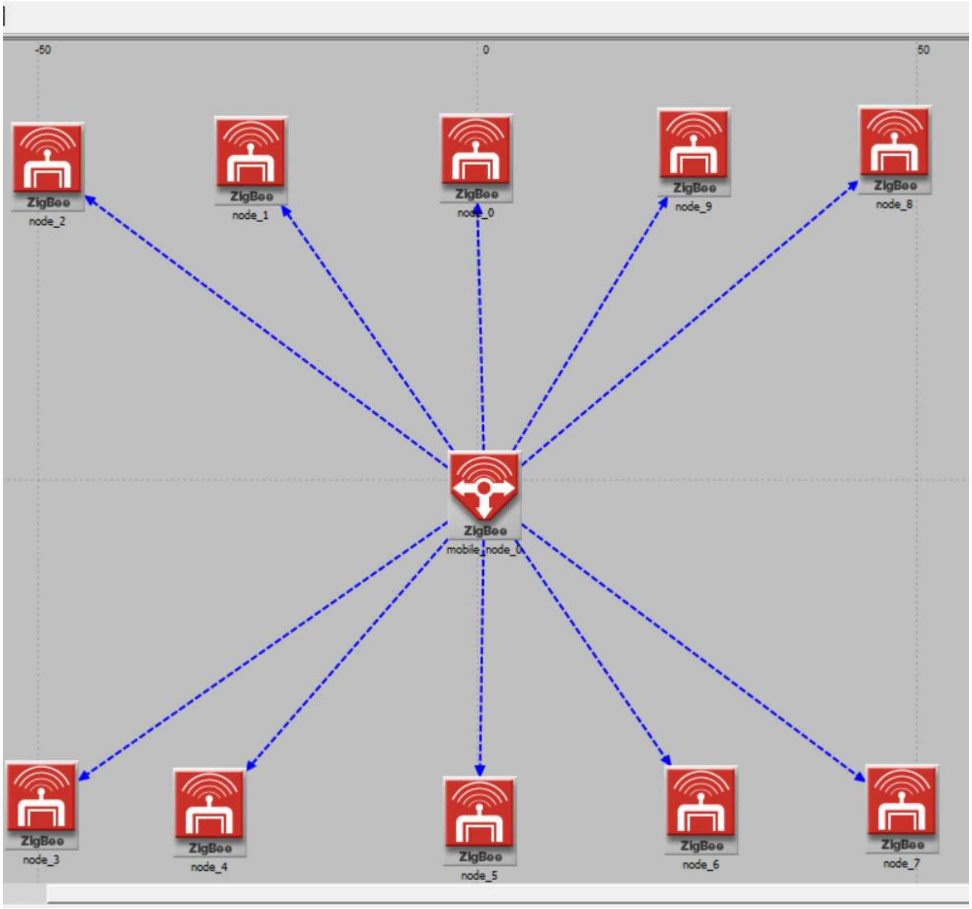


Figure 3.2: Scenario 1 – Star topology

This scenario was set up using the parameters in table 3.1 under the column labelled Star. The simulations were done using different number of node, that is , 10, 20 , 30 and 40. In this case the coordinator was communicating directly with the end devices. This topology does not have routers. The duration for each run was 30minutes.

Scenario 2 : Tree Topolgy

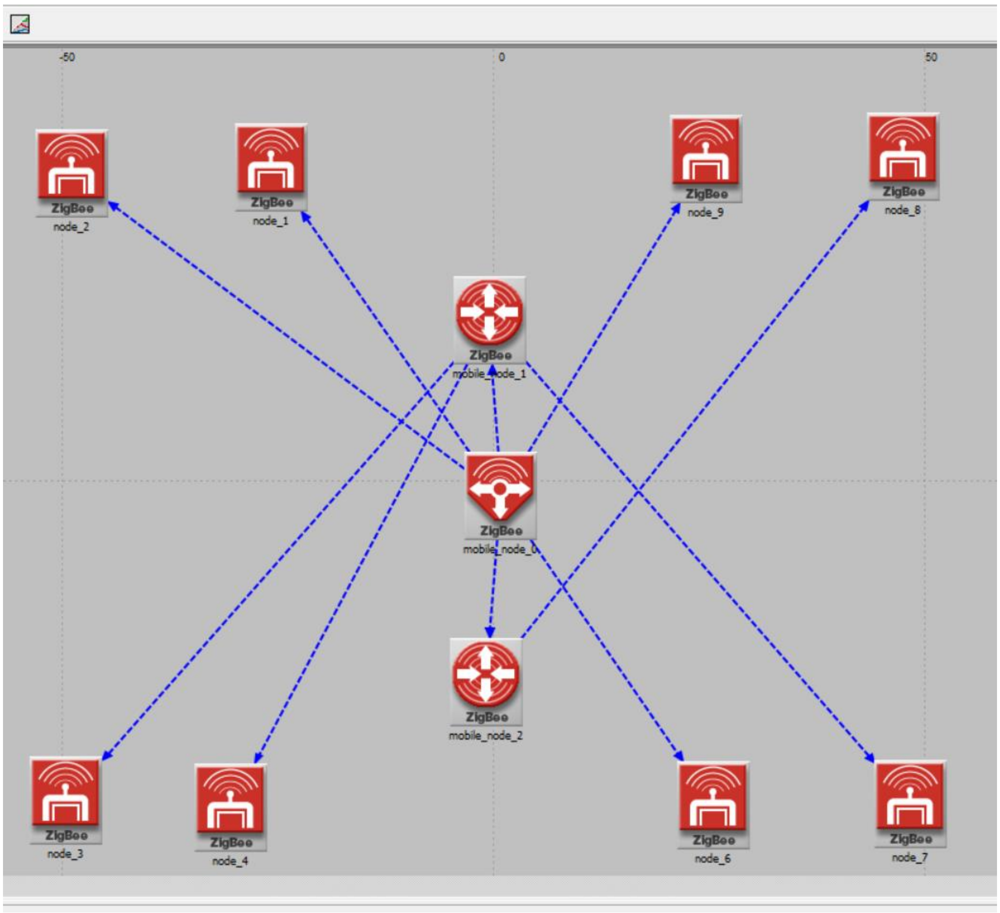


Figure 3.3: Scenario 2 – Tree topology

This scenario was set up using the parameters in table 3.1 under the column labelled tree. The simulations were done using different number of node, that is , 10, 20 , 30 and 40. In this case the coordinator could communicate directly with the end devices or through the router. The duration for each run was 30minutes.

Scenario 3: Mesh Topology

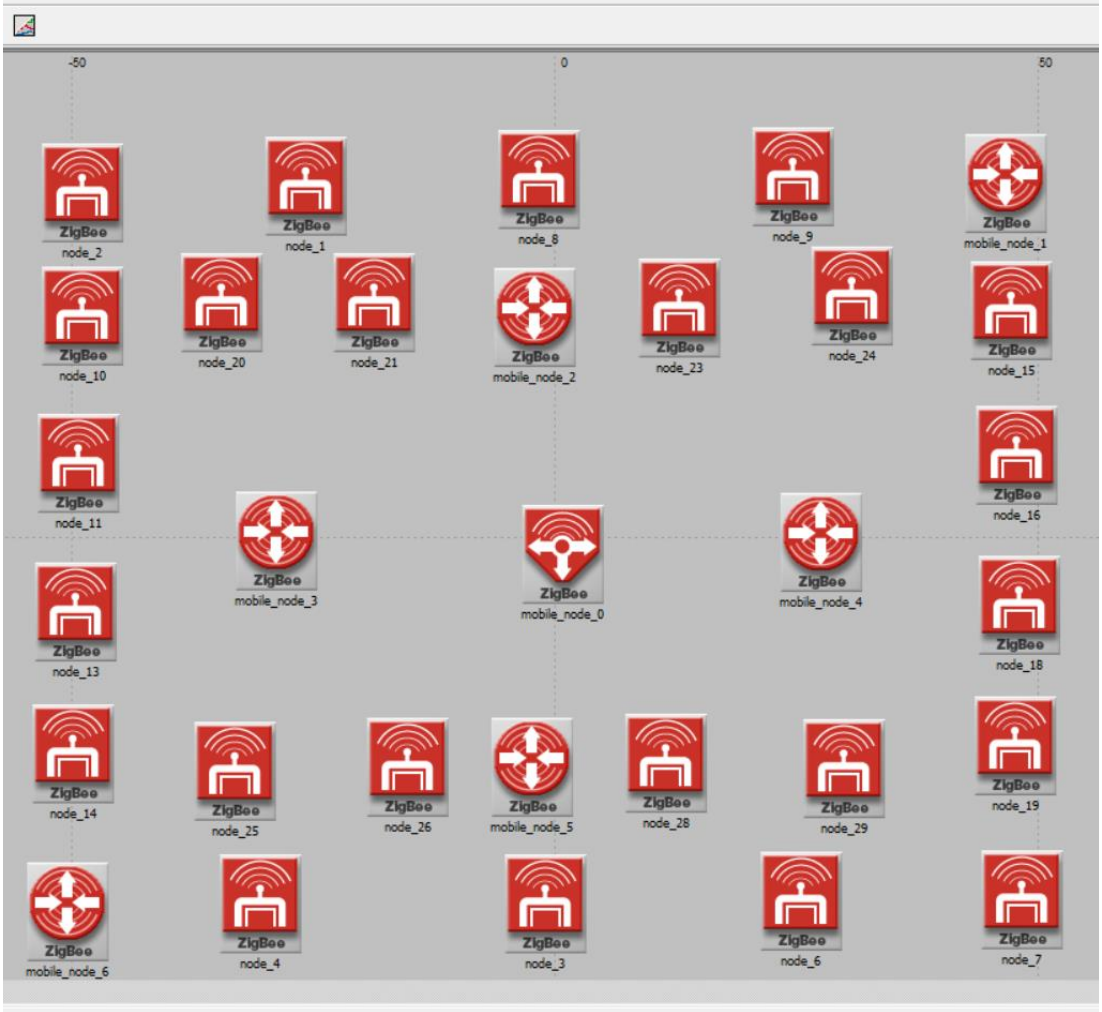


Figure 3.4: Scenario 3 – Mesh topology

This scenario was set up using the parameters in table 3.1 under the column labelled Mesh. The simulations were done using different number of node, that is , 10, 20 , 30 and 40. In this case the coordinator could communicating directly with the end devices or through routers. Packets can also use different routes from the coordinator to the end devices. The duration for each run was 30minutes.

Scenario 4: Wormhole Attack

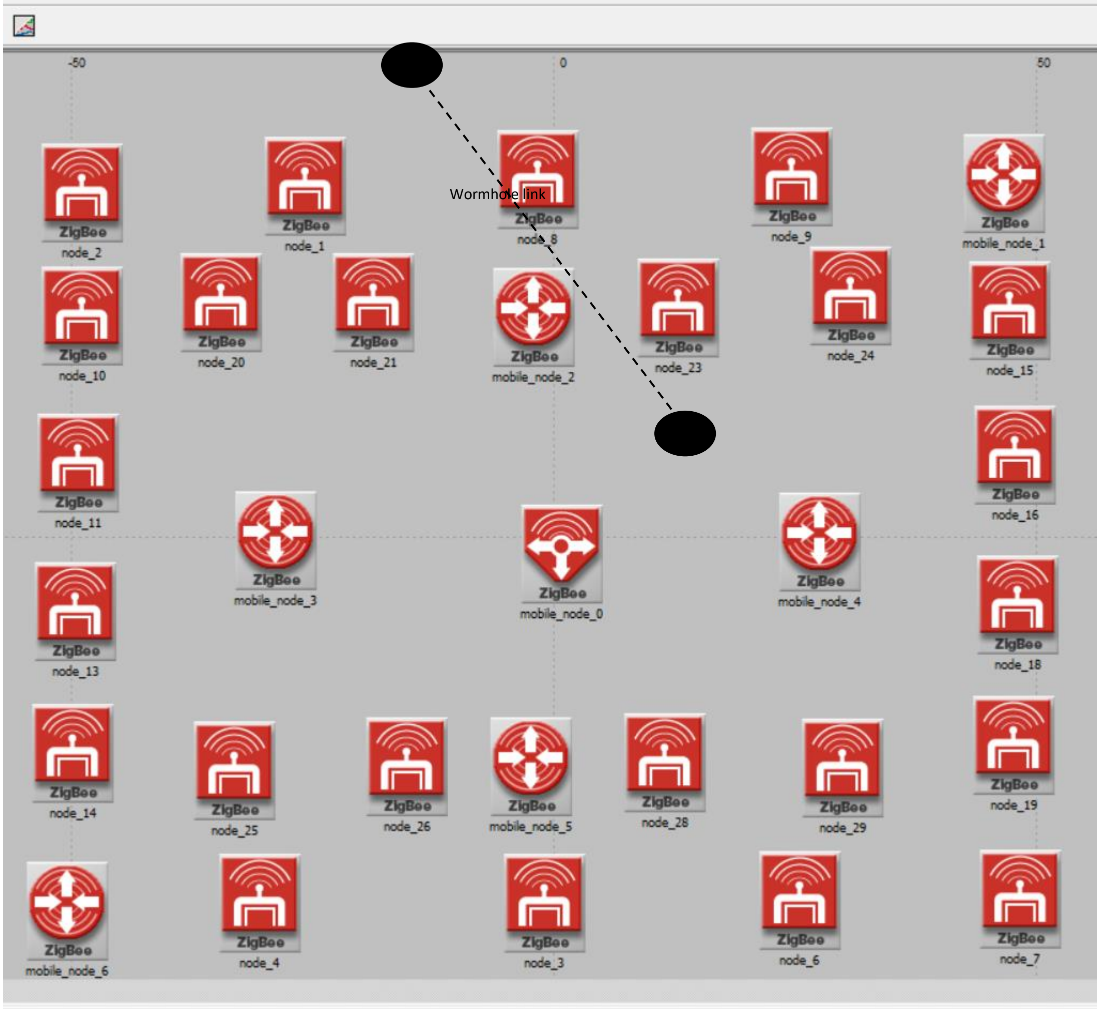


Figure 3.5: Scenario 4 – Wormhole Attack

This scenario was set up using the parameters in figure 3.1 under the column labelled Tree and Mesh. Focus on this scenario was on the effect of a wormhole attack to both Tree and Mesh topology. The simulations were done using 30 nodes. The duration for each run was 30minutes.

3.7 Mathematical Analysis in MATLAB

The data collected from OPNET were incorporated into a MATLAB program implementing Equations 3.1 to 3.8 discussed in the methodology to obtain the energy consumed by the system over the given simulation duration taking into account the node contention as well as retransmissions due to collisions and interference.[71]

This section briefly reviews the methodology used in calculating the energy consumption and throughput of a WSN. The approach used in calculating the energy consumed by wireless sensor nodes in a WSN, regardless of the wireless standard deployed and the topology of the network, is based on the following equation 3.1 [72] :

$$\mathbf{E_{total} = V \times \Sigma_i\, I_i \times t_i} \quad \textbf{(3.1)}$$

Where:

E – Energy Consumed

V – Voltage

i – Operating State

I_i – Corresponding voltage consumed for each operating state

t_i – Corresponding time for each operating state

According to Equation (1), the energy consumed by a WSN is comprised of three components: a constant operating voltage (V), a current (I_i) consumed by the node at different operation states and the corresponding time (t_i) for each operation state. In Equation (1), the subscript *i* denotes the four different operation states: transmission, reception, idle and sleep. These four states occur every cycle, where a cycle denotes the inter-arrival time between packets.

First State: Transmission

The first state is transmission during which both the processor and the radio component are active, processing and transmitting bits. Similarly, both the processor and the radio component are active in the reception state to receive packets, waiting for acknowledgements or to scan the medium to perform channel assessment. It is based on following equation 3.2 [73]

$$\mathbf{T_{Tx} = (Payload + Overhead) / Data\ Rate} \quad \textbf{(3.2)}$$

Second State: Receiving

The second operational state is the reception state where the radio component, in addition to the processor, is also functional throughout reception listening to the medium in order to receive packets, to wait for acknowledgments or to scan the medium for channel assessment. It is based on following equation 3.3 [71]

$$\mathbf{T_{rx}} = \sum_{i=0}^{M} \alpha^{i}(1 - \alpha^{i}) \times (i + 1) + \alpha^{M+1} \times (M + 1) \quad \textbf{(3.3)}$$

Where :

T – time

Rx – receiving state

M - maximum number of retry

n - number of nodes

α - probability of the medium being busy. It is derived using equation 3.4 [73]

$$\alpha = \frac{(\boldsymbol{n}-\mathbf{1}) \times (\mathbf{1}-\boldsymbol{P_{loss}}) \times \boldsymbol{E}[\Gamma] \times (\boldsymbol{T_{cca}} + \boldsymbol{T_x} + (\mathbf{2} \times \boldsymbol{T_{tr}}) + \boldsymbol{T_{ACK}}}{\left(\frac{\mathbf{1}}{\boldsymbol{\lambda}}\right) + \boldsymbol{E}[\boldsymbol{\Gamma}] \times \boldsymbol{E}[\boldsymbol{D_{HoL}}]} \qquad \mathbf{(3.4)}$$

$$\mathbf{E[D_{HOL}]} = \sum_{\mathbf{v=0}}^{\mathbf{M}} \boldsymbol{\alpha}^{\mathbf{v}}\mathbf{(1 - \alpha)} \left\{\sum_{\mathbf{i=0}}^{\mathbf{v}} \frac{\mathbf{W_i-1}}{\mathbf{2}} \times \boldsymbol{\sigma} + \mathbf{(v+1)} \times \mathbf{T_{CCa}}\right\} +$$

$$\boldsymbol{\alpha}^{\mathbf{M+1}} \left\{ \sum_{\mathbf{i=0}}^{\mathbf{M}} \frac{\mathbf{W_i-1}}{\mathbf{2}} \times \boldsymbol{\sigma} + \mathbf{(M+1)\ X\ T_{CCa}} \right\} \qquad \mathbf{(3.5)}$$

Equation 3.5 [72]**Where:**

P_{loss} – packet loss probability

CCA – Clear Channel Assessment

$E[D_{HoL}]$ – Duration for Head of Line

Third State: Idle

During the third operational state, idle current is consumed only by the processor, which processes the sensed data. It is worth noting that during the idle interval, the radio component is OFF. It calculation is based on the following equation 3.6 .[73]

$$\textbf{Idle Time} = \mathbf{E[D_{HoL}]} - \textbf{Total CCA} \qquad \mathbf{(3.6)}$$

Fourth State: Sleep

The fourth operational state is the sleep state during which both the radio component and the processor are OFF [12]. It is worth mentioning that, before a node goes into the sleep or idle state, it sets a timer to be able to determine the exact duration over which the radio component remains OFF. When the timer elapses, the radio component is turned ON once again to prepare for the transmission or reception state. The main reason that the radio component needs to be turned OFF, when it is not neither transmitting nor receiving is to reduce power consumption. As the radio component constitutes the main source of energy consumption, turning it off while it is not being utilized presents an approach to enhance energy efficiency of a node. It is derived using the following equation 3.7 [71].

$$\text{Sleep Time} = \text{Cycle Time} – \text{Idle Time} - \text{NCCA} - T_{Tx} \qquad (3.7)$$

Goodput per Joule

The focus of the study was on the assessment of the wireless communication protocols taking into account data drops and data retransmissions as a result of collisions in an interference-free environment. Consequently, a figure of merit was introduced to offer a fair comparison metric between the studied wireless standards emphasizing the trade-off between correct data transmission and energy consumption. The figure of merit, known as the Goodput per Joule, is shown in equation 3.8 [72]:

$$\text{Goodput per Joule} = \text{Useful Data Sent} / \text{Total Energy Consumed} \qquad (3.8)$$

where *Useful Data Sent* is the successfully transmitted data from transmitter to receiver excluding the headers added by each protocol. Furthermore, *Useful Data Sent* does not account for the number of retransmissions performed by each protocol till a successful transmission. For example, if a sensor node sends a particular frame 5 times till it receives an acknowledgment packet, only 1 frame is considered useful for the network[74]. Conversely, *Total Energy Consumed* accounts for the energy consumed in the 5 attempts, taking into consideration energy consumed during transmission, reception, and sleep.

3.8 Chapter Summary

This chapter has described in detail the simulation process and analysis carried out in regard to energy efficiency in Zigbee networks. Furthermore, attention has also been given to other characteristics closely related such as QoS and security. Simulators which were considered for this research have been discussed. Factors which led to the selection of OPNET and MATLAB as the tools of choice for this research has been given. Key amongst those factors was functionality and familiarity by most engineers in this field.

CHAPTER 4 – DATA COLLECTION AND ANALYSIS

4.0 Chapter Introduction

This study is meant to find out which of the three Zigbee topologies provides the best performance. In this research we focus is on energy efficiency, QoS and security. One of the important factors which make it the first choice is low energy consumption hence the need to be more specific in measuring energy efficiency considering how it is affected by network size and topology.

4.1 Throughput

Figure 4.1 below show the results of a network throughput obtained from OPNET simulation. On the x-axis we have number of node and the labels in the bars represent throughput in bytes per second. Generally, Mesh has the highest level of throughput followed by Tree and then Star. However, it is noteworthy that at times Tree perform better than Mesh.

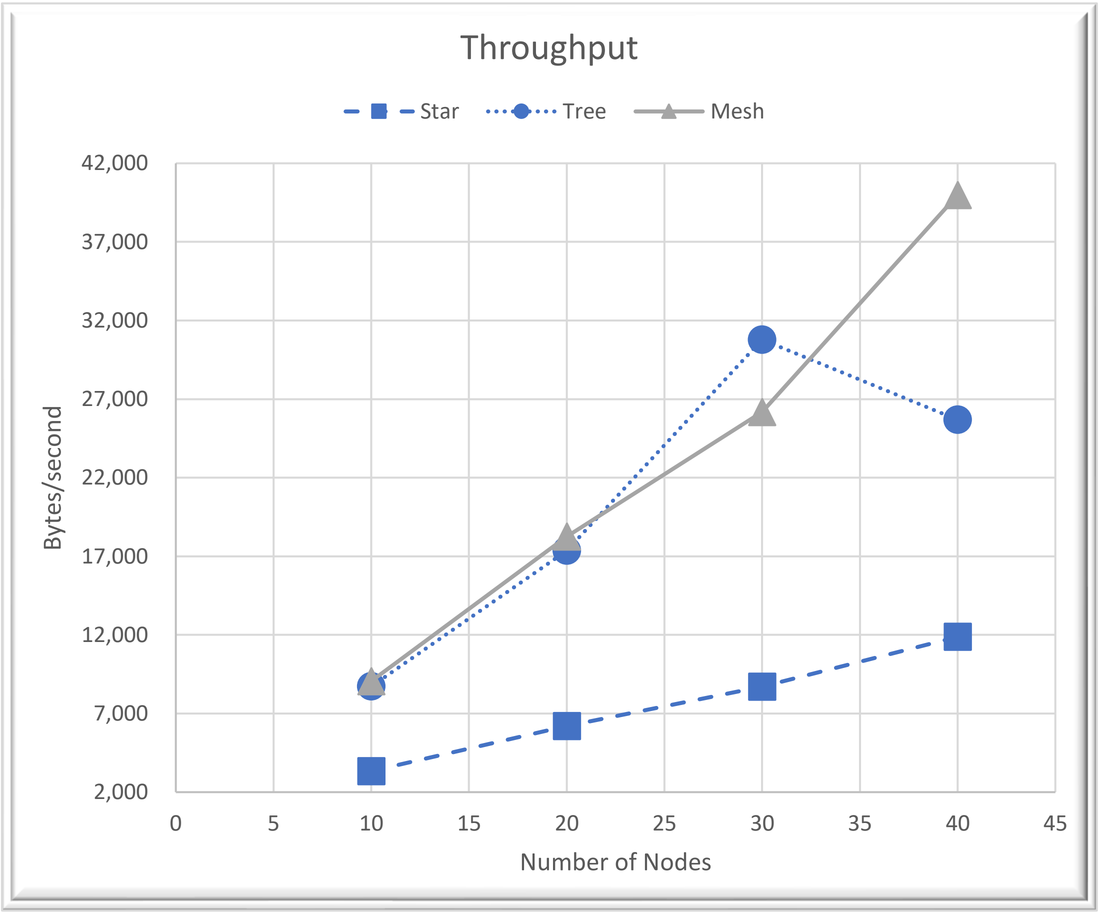


Figure 4.1: Throughput in bytes/sec

4.2 Data Sent

Figure 4.2 below show the data sent in bytes per second with each topology depicting the data sent as number of nodes increase. The difference between Throughput and Data Sent is Data Dropped. Generally, Tree topology has the best figures for data sent. However, from a different standpoint Star has the least data dropped.

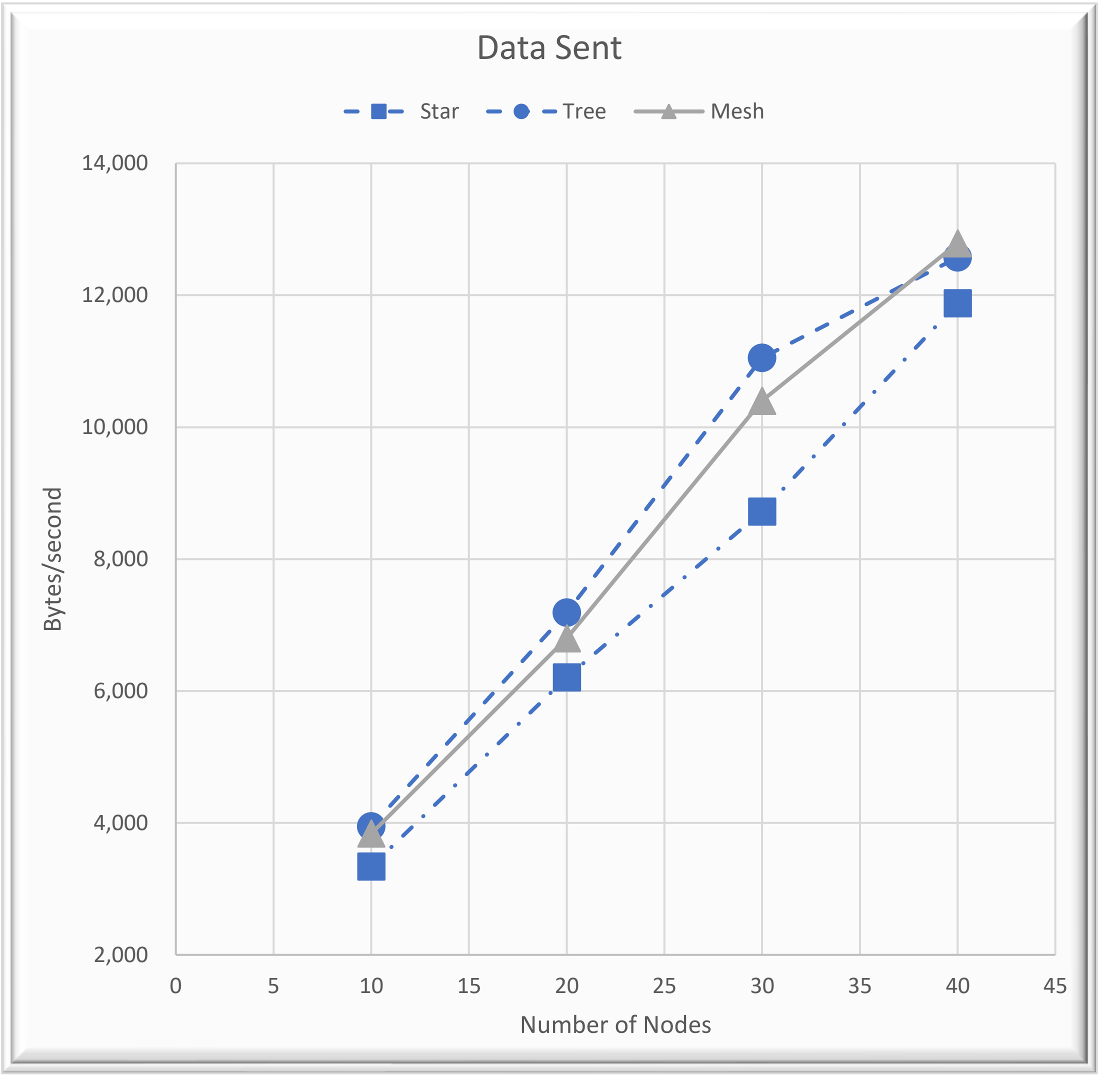


Figure 4.2: Data Sent in bytes/sec

4.3 Goodput per Joule

This is a figure of merit which gives a fair comparison metric between Zigbee network emphasizing the trade-off between correct data transmission and energy consumption. Based on this study, Tree topology has the highest or rather the best goodput per joule and Star being the least. However, there are some instances where Mesh performs the best.

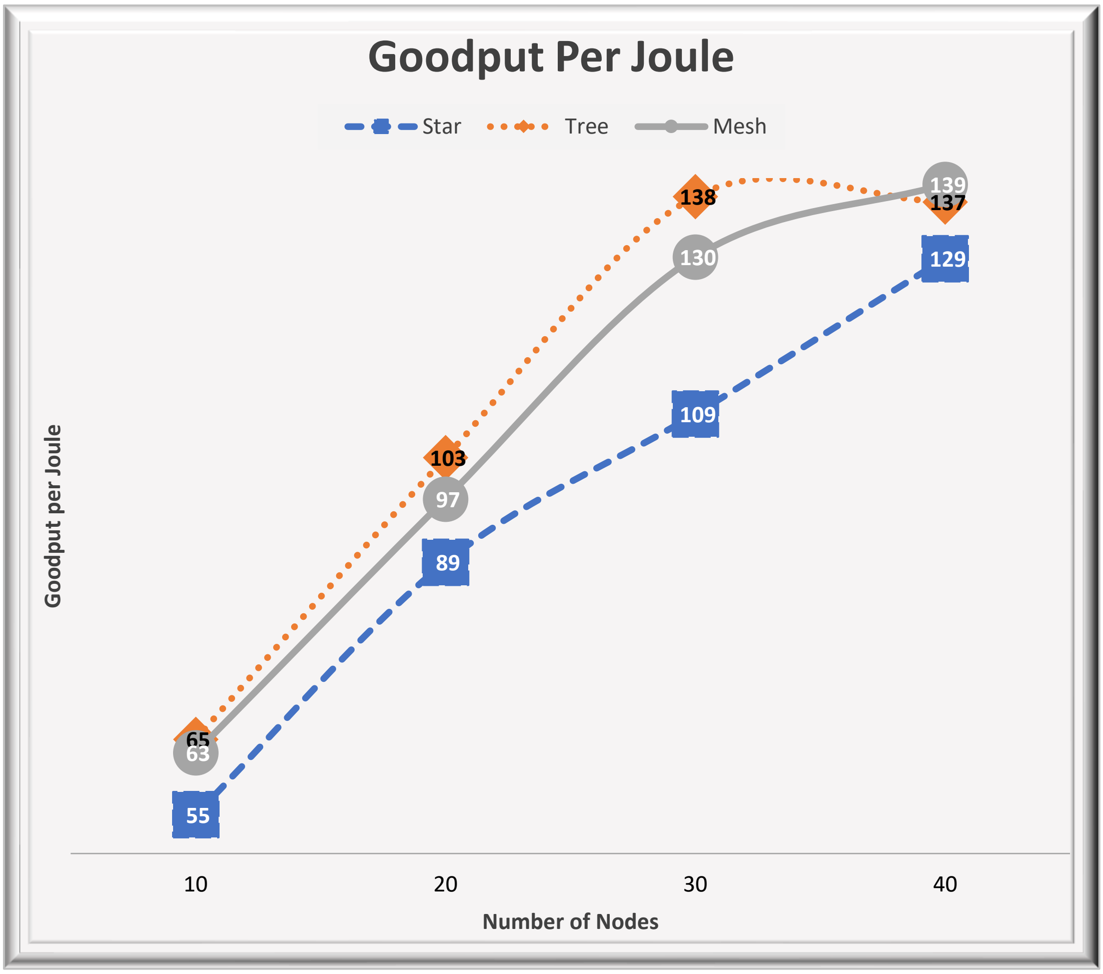


Figure 4.3: Goodput/Joule

4.4 Goodput per Joule – Wormhole Attack

Figure 4.4 depicts the goodput per joule for a network with an attack and another one without a wormhole attack. The other statistic of interest was the percentage difference between an attack and a network without attack. Tree topology had a percentage change of 82% and Mesh topology had a percentage difference of 14%.

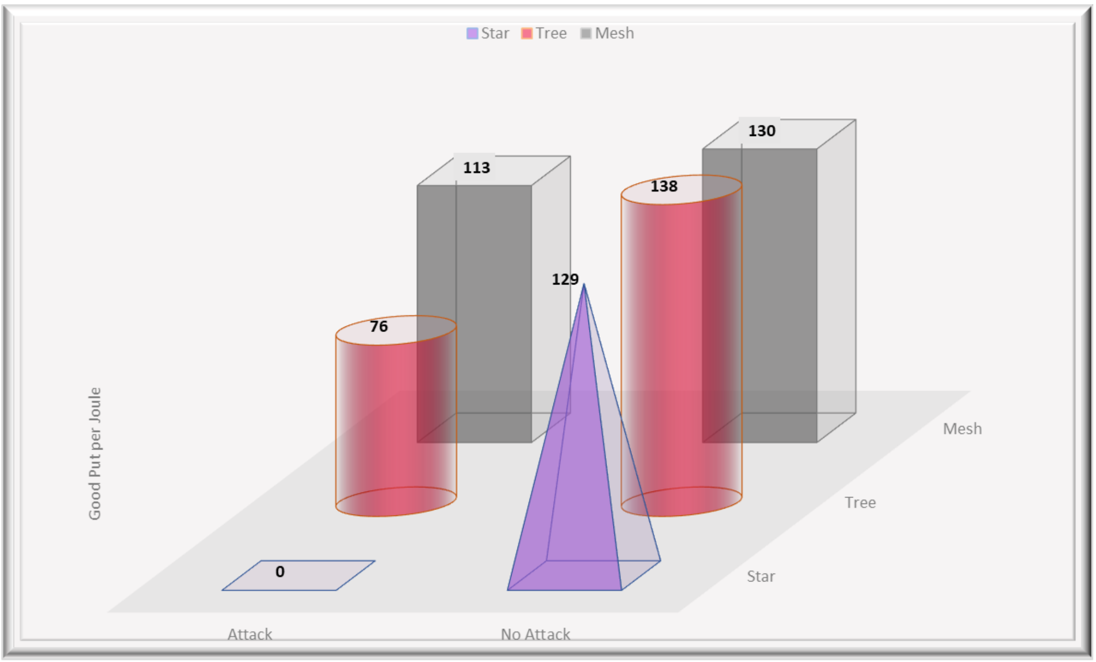


Figure 4.4: Goodput Per Joule – Wormhole Attack

4.5 Chapter Summary

In this chapter different aspects of Zigbee protocol have been simulated using OPNET and analysed in MATLAB. The aspect or characteristics are energy efficiency, QoS and security. The results of these experiments were described in each section and where applicable compared with each other. The results showed that either tree or mesh topology can be the most energy efficient depending on parameters of a specific scenario. However, generally star topology always trails behind. It is also noteworthy that in case of a wormhole attach mesh topology is affected the least.

CHAPTER 5 – DISCUSSION AND CONCLUSION

5.1 Chapter Introduction

In order to fulfill the research objectives by providing adequate answers to the research question, simulation and analysis has been carried out. Simulation of the Zigbee network was done using OPNET with well-defined parameters. The results where then analysed using MATLAB. Therefore, this chapter gives a conclusion, implications of research and recommendations for further study.

5.2 Conclusion

Topologies are important in ZigBee. Whole network performance depends upon the topology, so it is necessary to consider that which topology fit best in which case. The principal objective of this research was to find out more on the effects of topological variation to energy efficiency. Attention was also given to QoS, Wormhole Attacks (Security) while measuring the energy efficiency inform of goodput per joule.

5.2.1 Quality-of-Service

Most papers consider Mesh as the best topology. Based on simulation we can conclude that tree topology performs better than mesh in some instances. After consistently trailing behind in most simulations, we have concluded that the Star topology is not ideal when you require good performance.

5.2.2 Energy Efficiency

After a series of scenarios, were Mesh and Tree would alternate in taking the lead on energy efficiency, we came to a conclusion that they are at the same level when it comes to energy efficiency.

5.2.3 Security- Wormhole Attack

Mesh has proved to be strong when attacked by wormhole as it had a decrease in performance of fourteen percentage. However, the downside is that in a case may breach privacy, it is difficult to tell from the performance of Mesh topology that it has been attacked. Star and Tree topologies are easy to tell from performance that they could be under attack. Based on this study Mesh is more secure than Tree and Star.

5.3 Recommendations

Energy efficiency techniques such as energy-efficient routing , sleep/wake-up approaches, radio optimization and data reduction approaches have received great attention from researchers. We recommend that in an effort to implement all these approaches, topological variation is also taken into consideration as it may bear fruit without must cost implications compared to other techniques which may require additional software and hardware from the usual components.

5.3.1 Quality-of-Service

The most recommended topology by researchers is Mesh. Based on our study we recommend that users who implement Zigbee should simulate or test how their applications will perform under different topologies using their desired parameters as Tree outperformed Mesh in some scenarios. While widely held industry opinions may be used as a baseline, most scenario are unique or not the same. There are also scenarios where self-healing is a priority, then mesh will be the best but if that feature is not a priority, then users may have to go by tree when it performs the best.

5.3.2 Energy Efficiency

Based on this study we recommend Star topology is not considered when energy efficiency is a priority as it consistently trailed behind. However, one cannot draw a line between Mesh and Tree topology based on energy efficiency as we consider them on the same level based on this study. However, we further recommend simulation or testing of tree and mesh topology to find out the best for their scenario.

5.3.3 Security- Wormhole Attack

The cost of implementing security measures is increasing as networks get more sophisticated and hackers also devising new ways to attack. We therefore recommend, monitoring of energy consumption/ efficiency as it can give you an early sign of an attack on the network. However, the is need for caution when using the Mesh topology as a security breach may cause little (15% or less) decline in efficiency.

5.4 Future Work

The advancement of technology requires an equal measure in research in order to reap full benefits. Based on literature reviewed and research carried out, the star topology is less energy efficient . Unfortunately, it also receives less attention when it comes to research but is widely implemented especially in homes because it is less expensive than the other topologies. In a nutshell, there is need for more research on how to improve energy efficiency in Zigbee networks which are implemented using star topology. Its simplicity in nature may be an indication that energy efficient approaches for this topology may be achieved with less research efforts that the other topologies.

This research focused of the network layer regarding security. A lot of research work can also be earmarked for other layers of the Zigbee Architectural Stack.

References

[1] N. Islam, M. J. H. Biddut, A. I. Swapna, and S. Asaduzzaman, "Improved Quality of Service in ZigBee network with statistical modeling," *Proceedings of 2015 3rd International Conference on Advances in Electrical Engineering, ICAEE 2015*, pp. 174–177, 2016, doi: 10.1109/ICAEE.2015.7506824.

[2] S. Tennina *et al.*, *IEEE 802.15.4 and ZigBee as Enabling Technologies for Low-Power Wireless Systems with Quality-of-Service Constraints*, vol. 1. 2013.

[3] M. Chen, Y. Miao, and I. Humar, *OPNET IoT Simulation*. 2019. doi: 10.1007/978-981-32-9170-6.

[4] W. Razouk, "Zigbee Security within the Framework of IoT," pp. 265–265, 2014, doi: 10.1109/soca.2014.57.

[5] P. Mounika, "Performance analysis of wireless sensor network topologies for Zigbee using riverbed modeler," *Proceedings of the 2nd International Conference on Inventive Systems and Control, ICISC 2018*, no. Icisc, pp. 1456–1459, 2018, doi: 10.1109/ICISC.2018.8399050.

[6] L. Jaiswal, J. Kaur, and G. Singh, "Performance Analysis of Topological Variation in Personal Area Network using ZigBee Wireless Sensors," *Networks*, vol. 8491, pp. 706–711, 2012.

[7] S. K. Nath, S. Aznabi, N. T. Islam, A. Faridi, and W. Qarony, "Investigation and performance analysis of some implemented features of the ZigBee protocol and IEEE 802.15.4 Mac Specification," *International Journal of Online Engineering*, vol. 13, no. 1, pp. 14–32, 2017, doi: 10.3991/ijoe.v13i01.5984.

[8] E. Zanaj, G. Caso, L. de Nardis, A. Mohammadpour, Ö. Alay, and M.-G. di Benedetto, "Energy Efficiency in Short and Wide-Area IoT Technologies—A Survey," *Technologies*, vol. 9, no. 1, p. 22, 2021, doi: 10.3390/technologies9010022.

[9] Omojokun. G.Aju , "A Survey of ZigBee Wireless Sensor Network Technology: Topology, Applications and Challenges," *International Journal of Computer Applications*, vol. 130, no. 9, pp. 47–55, 2015, doi: 10.5120/ijca2015907130.

[10] P. Malhotra, P. Dhillon, and H. Sadawarti, "ZigBee Technology (802.15. 4): A Survey," *International Journal of Engineering Research & Technology*, vol. 2, no. 11, pp. 1939–1944, 2013, [Online]. Available: http://www.ijert.org/browse/volume-2-2013/november-2013-edition?download=6394:zigbee-technology-802154--a-survey&start=280

[11] N. C. D. Sudhir Kumar Sharma,Bharat Bhushan, Raghvendra Kumar, Aditya Khamparia, *Integration of WSNs into Internet of Things*, 2021

[12] L. LaBerge, C. O'Toole, J. Schneider, and Kate Smaje, "How COVID-19 has pushed companies over the technology tipping point-and transformed business forever," *McKinsey Global Publishing*, no. October, pp. 1–9, 2020, [Online]. Available: https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/how-covid-19-has-pushed-companies-over-the-technology-tipping-point-and-transformed-business-forever

[13] S. Singhal and K. Sneader, "The next normal arrives: Trends that will define 2021 — and beyond," *McKinsey&Company*, no. January, 2021, [Online]. Available: https://www.mckinsey.com/featured-insights/leadership/the-next-normal-arrives-trends-that-will-define-2021-and-beyond

[14] S. S. Mahmood and P. Sharma, "Industrial automation using zigbee communication protocol," *International Journal of Recent Technology and Engineering*, vol. 8, no. 3, pp. 7240–7243, 2019, doi: 10.35940/ijrte.C6294.098319.

[15] X. Fan *et al.*, "Security Analysis of Zigbee," *MWR InfoSecurity*, no. May, pp. 1–18, 2017, [Online]. Available: http://ieeexplore.ieee.org/document/7940247/%0Ahttps://courses.csail.mit.edu/6.857/2017/project/17.pdf%0Ahttps://www.mwrinfosecurity.com/assets/Whitepapers/mwri-zigbee-overview-finalv2.pdf

[16] P. Morgner, S. Mattejat, Z. Benenson, C. Müller, and F. Armknecht, "Insecure to the touch: Attacking ZigBee 3.0 via touchlink commissioning," *Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks, WiSec 2017*, pp. 230–240, 2017, doi: 10.1145/3098243.3098254.

[17] P. Ciholas, A. Lennie, P. Sadigova, and J. M. Such, "The Security of Smart Buildings: a Systematic Literature Review," pp. 1–50, 2019, [Online]. Available: http://arxiv.org/abs/1901.05837

[18] H. A. H. Alobaidy, J. S. Mandeep, R. Nordin, and N. F. Abdullah, "A review on zigbee based WSNs: Concepts, infrastructure, applications, and challenges," *International Journal of Electrical and Electronic Engineering and Telecommunications*, vol. 9, no. 3, pp. 189–198, 2020, doi: 10.18178/ijeetc.9.3.189-198.

[19] R. Martinez-Sandoval, A. J. Garcia-Sanchez, F. Garcia-Sanchez, J. Garcia-Haro, and D. Flynn, "A comprehensive WSN-based approach to efficiently manage a smart grid," *Sensors (Switzerland)*, vol. 14, no. 10, pp. 18748–18783, 2014, doi: 10.3390/s141018748.

[20] Netalkar, "Zigbee Based Wireless Sensor Networks for Smart Campus\n," *International Journal of Computer Science and Information Technologies*, vol. 5, no. 6, pp. 55–62, 2014.

[21] S. K. Gharghan, R. Nordin, and M. Ismail, "Statistical validation of performance of ZigBee-based wireless sensor network for track cycling,"

2015 International Conference on Smart Sensors and Application, ICSSA 2015, pp. 44–49, 2015, doi: 10.1109/ICSSA.2015.7322508.

[22] S. K. Gharghan, R. Nordin, M. Ismail, and J. A. Ali, “Accurate Wireless Sensor Localization Technique Based on Hybrid PSO-ANN Algorithm for Indoor and Outdoor Track Cycling,” *IEEE Sensors Journal*, vol. 16, no. 2, pp. 529–541, 2016, doi: 10.1109/JSEN.2015.2483745.

[23] N. K. Suryadevara, S. C. Mukhopadhyay, S. D. T. Kelly, and S. P. S. Gill, “WSN-based smart sensors and actuator for power management in intelligent buildings,” *IEEE/ASME Transactions on Mechatronics*, vol. 20, no. 2, pp. 564–571, 2015, doi: 10.1109/TMECH.2014.2301716.

[24] M. Zhan, J. Wu, H. Wen, and P. Zhang, “A Novel Error Correction Mechanism for Energy-Efficient Cyber-Physical Systems in Smart Building,” *IEEE Access*, vol. 6, no. c, pp. 39037–39045, 2018, doi: 10.1109/ACCESS.2018.2854794.

[25] V. Subrahmanyam, M. A. Zubair, A. Kumar, and P. Rajalakshmi, “A Low Power Minimal Error IEEE 802.15.4 Transceiver for Heart Monitoring in IoT Applications,” *Wireless Personal Communications*, vol. 100, no. 2, pp. 611–629, 2018, doi: 10.1007/s11277-018-5255-y.

[26] C. T. Kone, A. Hafid, and M. Boushaba, “Performance Management of IEEE 802.15.4 Wireless Sensor Network for Precision Agriculture,” *IEEE Sensors Journal*, vol. 15, no. 10, pp. 5734–5747, 2015, doi: 10.1109/JSEN.2015.2442259.

[27] S. Pramono, A. O. Putri, E. Warsito, and B. S. Basuki, “Comparative analysis of star topology and multihop topology outdoor propagation based on quality of service (QoS) of wireless sensor network (WSN),” *2017 IEEE International Conference on Communication, Networks and Satellite, COMNETSAT 2017 - Proceedings*, vol. 2018-Janua, pp. 152–157, 2017, doi: 10.1109/COMNETSAT.2017.8263591.

[28] R. Design, T. Circuit, S. Bom, and M. K. Jun, “Simple Wireless Bluetooth Stereo Audio System for Outdoor Use Putting the Bluetooth Audio System Together Determining the Output Power,” pp. 1–11, 2012.

[29] Z. Qadir, V. Tafadzwa, H. Rashid, and C. Batunlu, “Smart Solar Micro-Grid Using ZigBee and Related Security Challenges,” *2018 18th Mediterranean Microwave Symposium (MMS)*, pp. 299–302, 2018.

[30] C. Wang, T. Jiang, and Q. Zhang, *ZigBee Network Protocols and Applications*. 2016. doi: 10.1201/b16619.

[31] P. Ajgaonkar, L. Wang, and M. Alam, “Simulation studies on ZigBee communications for home automation and networking,” *AUTOTESTCON (Proceedings)*, pp. 329–334, 2010, doi: 10.1109/AUTEST.2010.5613588.

[32] Manpreet and J. Malhotra, “ZigBee technology: Current status and future scope,” *2015 International Conference on Computer and Computational*

Sciences, ICCCS 2015, pp. 163–169, 2015, doi: 10.1109/ICCACS.2015.7361343.

[33] T. Zillner, “ZigBee Exploited - The Good, the Bad and the Ugly,” *Cognosec*, vol. 16, no. 2, p. 6, 2015.

[34] C. Peng and K. Qian, “Development and Application of a ZigBee-Based Building Energy Monitoring and Control System,” *Scientific World Journal*, vol. 2014, 2014, doi: 10.1155/2014/528410.

[35] S. Long and F. Miao, “Research on ZigBee wireless communication technology and its application,” *Proceedings of 2019 IEEE 4th Advanced Information Technology, Electronic and Automation Control Conference, IAEAC 2019*, no. Iaeac, pp. 1830–1834, 2019, doi: 10.1109/IAEAC47372.2019.8997928.

[36] K. Gupta, R. Vohra, and R. Singh Sawhney, “Envisaging Performance Metrics of ZigBee Wireless Sensors by Topology Variations,” *International Journal of Computer Applications*, vol. 121, no. 3, pp. 33–36, 2015, doi: 10.5120/21523-4502.

[37] F. M. Sun *et al.*, “A ZigBee based multi-hop health monitoring system: Design and performance evaluation,” *Proceedings - IEEE 38th Annual International Computers, Software and Applications Conference Workshops, COMPSACW 2014*, pp. 673–677, 2014, doi: 10.1109/COMPSACW.2014.113.

[38] T. J. Bihl, K. W. Bauer, and M. A. Temple, “Feature Selection for RF Fingerprinting with Multiple Discriminant Analysis and Using ZigBee Device Emissions,” *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 8, pp. 1862–1874, 2016, doi: 10.1109/TIFS.2016.2561902.

[39] J. J. D. Gifty and K. Sumathi, “ZigBee Wireless Sensor Network simulation with various topologies,” *Proceedings of 2016 Online International Conference on Green Engineering and Technologies, IC-GET 2016*, 2017, doi: 10.1109/GET.2016.7916714.

[40] S. K. Ibrahim, “Performance Evaluation of Zigbee Coordinator Fails Node with Different Topologies,” *Journal of Computer Science & Systems Biology*, vol. 08, no. 05, pp. 292–295, 2015, doi: 10.4172/jcsb.1000203.

[41] T. L. Indrek Taal, “Security Risk Analysis of Wireless Mesh Network for Emergency Networks,” 2020.

[42] A. A. Anasane and R. A. Satao, “A Survey on Various Multipath Routing Protocols in Wireless Sensor Networks,” *Procedia Computer Science*, vol. 79, no. 12, pp. 610–615, 2016, doi: 10.1016/j.procs.2016.03.077.

[43] T. Nimi and P. Samundiswary, “Comparative Performance evaluation on Priority based ZigBee Network with tree and mesh routing,” *2018 4th International Conference on Electrical Energy Systems (ICEES)*, pp. 691–695, 2018.

[44] S. K. Gharghan, R. Nordin, and M. Ismail, “An ultra-low power wireless sensor network for bicycle torque performance measurements,” *Sensors (Switzerland)*, vol. 15, no. 5, pp. 11741–11768, 2015, doi: 10.3390/s150511741.

[45] H. A. H. Alobaidy, H. N. Abdullah, and T. M. Salman, “Implementation and Performance Evaluation of WSN for Energy Monitoring Application,” *Eng. &Tech.Journal*, vol. 33, no. 7, pp. 1555–1568, 2015.

[46] A. A. Alsahli and H. U. Khan, “Security challenges of wireless sensors devices (MOTES),” *2014 World Congress on Computer Applications and Information Systems, WCCAIS 2014*, pp. 1–9, 2014, doi: 10.1109/WCCAIS.2014.6916650.

[47] N. Aschenbruck, J. Bauer, J. Bieling, A. Bothe, and M. Schwamborn, “A security architecture and modular intrusion detection system for WSNs,” *9th International Conference on Networked Sensing Systems, INSS 2012 - Conference Proceedings*, 2012, doi: 10.1109/inss.2012.6240521.

[48] H. Fitriawan, M. Susanto, A. S. Arifin, D. Mausa, and A. Trisanto, “ZigBee based wireless sensor networks and performance analysis in various environments,” *QiR 2017 - 2017 15th International Conference on Quality in Research (QiR): International Symposium on Electrical and Computer Engineering*, vol. 2017-Decem, no. 1, pp. 272–275, 2017, doi: 10.1109/QIR.2017.8168495.

[49] C. C. Chang and Y. H. Hsu, “Reducing energy consumption by a low-current real-time clock on a ZigBee networking device,” *Proceedings of 4th IEEE International Conference on Applied System Innovation 2018, ICASI 2018*, pp. 750–753, 2018, doi: 10.1109/ICASI.2018.8394368.

[50] Y. M. Amin, A. T. Abdel-hamid, and S. Member, “Layer Attacks,” *2016 International Conference on Selected Topics in Mobile & Wireless Networking (MoWNeT)*, pp. 74–79, 2016.

[51] M. A. bin Karnain and Z. bin Zakaria, “A review on ZigBee security enhancement in smart home environment,” *2015 IEEE 2nd International Conference on InformationScience and Security, ICISS 2015*, 2016, doi: 10.1109/ICISSEC.2015.7370969.

[52] Y. M. Amin, A. T. Abdel-hamid, and S. Member, “Layer Attacks,” *2016 International Conference on Selected Topics in Mobile & Wireless Networking (MoWNeT)*, pp. 74–79, 2016.

[53] N. Sugirtham and R. S. Jenny, “An Evaluation on the Performance of Wireless Sensor Network with Wormhole Attack,” vol. 6, no. 1, pp. 11–18, 2015.

[54] L. Jaiswal, J. Kaur, and G. Sandhu, “Performance Analysis of Backoff Exponent Behaviour at MAC Layer In ZigBee Sensor Networks,” *International Journal of Computer Applications*, vol. 57, no. 22, pp. 58–64, 2012, doi: 10.5120/9425-3863.

[55] F. Delaveau, A. Evesti, J. Suomalainen, R. Savola, and N. Shapira, “Active and Passive Eavesdropper Threats within Public and Private Civilian Wireless Networks - Existing and Potential Future Countermeasures - An overview,” *Wireless Innovation Forum - European Conference on Communications Technologies and Software Defined Radio (SDR-WInnComm-Europe)*, no. June, pp. 1–36, 2013.

[56] N. Sugirtham and R. S. Jenny, “An Evaluation on the Performance of Wireless Sensor Network with Wormhole Attack,” vol. 6, no. 1, pp. 11–18, 2015.

[57] I. Vaccari, E. Cambiaso, and M. Aiello, “Remotely Exploiting at Command Attacks on ZigBee Networks,” *Security and Communication Networks*, vol. 2017, 2017, doi: 10.1155/2017/1723658.

[58] J. Govindasamy and S. Punniakodi, “Energy efficient intrusion detection system for ZigBee based wireless sensor networks,” *International Journal of Intelligent Engineering and Systems*, vol. 10, no. 3, pp. 155–165, 2017, doi: 10.22266/ijies2017.0630.17.

[59] L. Nachabe, M. Girod-Genet, and B. el Hassan, “Unified Data Model for Wireless Sensor Network,” *IEEE Sensors Journal*, vol. 15, no. 7, pp. 3657–3667, 2015, doi: 10.1109/JSEN.2015.2393951.

[60] X. Cao, D. M. Shila, Y. Cheng, Z. Yang, Y. Zhou, and J. Chen, “Ghost-in-ZigBee: Energy Depletion Attack on ZigBee-Based Wireless Networks,” *IEEE Internet of Things Journal*, vol. 3, no. 5, pp. 816–829, 2016, doi: 10.1109/JIOT.2016.2516102.

[61] M. Yadav, P. Brar, and P. Kaur, “Comparitive analysis of different modes of operation for Zigbee mac with variation in network size and traffic,” *2014 International Conference on Electronics, Communication and Computational Engineering, ICECCE 2014*, pp. 148–152, 2014, doi: 10.1109/ICECCE.2014.7086649.

[62] C. Marghescu, M. Pantazica, and P. Svasta, “Simulation of a Wireless Sensor Network Using OPNET,” pp. 249–252, 2011.

[63] X. Cao, D. M. Shila, Y. Cheng, Z. Yang, Y. Zhou, and J. Chen, “Ghost-in-ZigBee: Energy Depletion Attack on ZigBee-Based Wireless Networks,” *IEEE Internet of Things Journal*, vol. 3, no. 5, pp. 816–829, 2016, doi: 10.1109/JIOT.2016.2516102.

[64] X. Fan *et al.*, “Security Analysis of Zigbee,” *MWR InfoSecurity*, no. May, pp. 1–18, 2017, [Online]. Available: http://ieeexplore.ieee.org/document/7940247/%0Ahttps://courses.csail.mit.edu/6.857/2017/project/17.pdf%0Ahttps://www.mwrinfosecurity.com/assets/Whitepapers/mwri-zigbee-overview-finalv2.pdf

[65] Y. Zhuang and L. Ma, “An energy-efficient and low-collision IEEE 802.15.4-based MAC for data gathering in wireless sensor networks,” *Proceedings -*

2012 International Conference on Computer Science and Service System, CSSS 2012, pp. 1244–1247, 2012, doi: 10.1109/CSSS.2012.315.

[66] A. Lavric, V. Popa, C. Males, and I. Finis, “A performance study of ZigBee wireless sensors network topologies for street lighting control systems,” *2012 International Conference on Selected Topics in Mobile and Wireless Networking, ICOST 2012*, pp. 130–133, 2012, doi: 10.1109/iCOST.2012.6271280.

[67] R. Ware, M. K. Mukerjee, S. Seshan, and J. Sherry, “Beyond Jain’s Fairness Index,” pp. 17–24, 2019, doi: 10.1145/3365609.3365855.

[68] J. M. C. Dac-Nhuong Le, Abhishek Kumar Pandey,Sairam Tadepalli,Pramod Singh Rathore, *Network Modeling, Simulation and Analysis in MATLAB*. 2019.

[69] A. Kaur, J. Kaur, and G. Singh, “An efficient hybrid topology construction in Zigbee sensor network,” *International Conference on Recent Advances and Innovations in Engineering, ICRAIE 2014*, 2014, doi: 10.1109/ICRAIE.2014.6909171.

[70] S. Vançin and E. Erdem, “Design and Simulation of Wireless Sensor Network Topologies Using the ZigBee Standard,” *International Journal of Computer Networks and Applications (IJCNA*, vol. 2, no. 3, pp. 135–143, 2015.

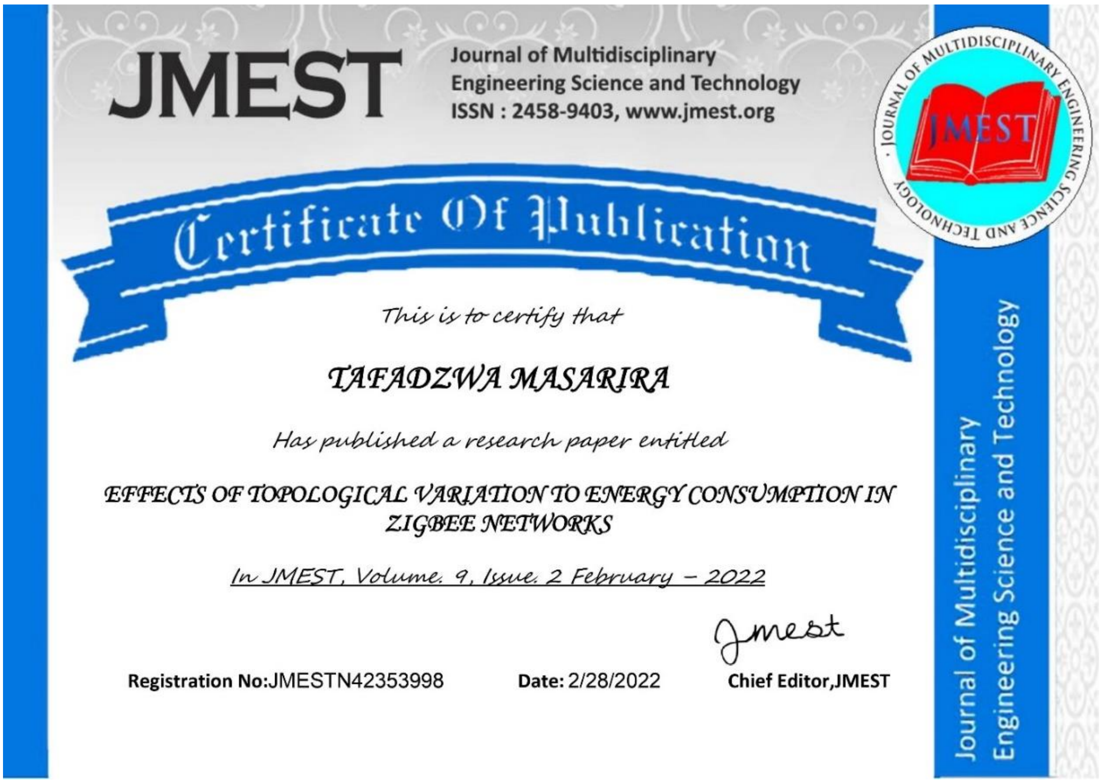
[71] A. Kenawy *et al.*, “WSN goodput and energy consumption for various wireless communication standards,” *2013 The International Conference on Technological Advances in Electrical, Electronics and Computer Engineering, TAEECE 2013*, no. I, pp. 40–45, 2013, doi: 10.1109/TAEECE.2013.6557192.

[72] A. Betzler, C. Gomez, I. Demirkol, and J. Paradells, “A holistic approach to ZigBee performance enhancement for home automation networks,” *Sensors (Switzerland)*, vol. 14, no. 8, pp. 14932–14970, 2014, doi: 10.3390/s140814932.

[73] M. Onsy *et al.*, “Performance of WSNs under the Effect of Collisions and Interference,” *Wireless Sensor Network*, vol. 06, no. 06, pp. 93–103, 2014, doi: 10.4236/wsn.2014.66010.

[74] S. S. Mahmood and P. Sharma, “Iot Based Industrial Automation using Zigbee Communication Standard,” *International Journal of Innovative Technology and Exploring Engineering*, vol. 9, no. 4, pp. 379–383, 2020, doi: 10.35940/ijitee.d1402.029420.

Appendix 1: Certificate of Publication



JMEST Journal of Multidisciplinary Engineering Science and Technology
ISSN : 2458-9403, www.jmest.org

JOURNAL OF MULTIDISCIPLINARY ENGINEERING SCIENCE AND TECHNOLOGY
JMEST

Certificate Of Publication

This is to certify that

TAFADZWA MASARIRA

Has published a research paper entitled

EFFECTS OF TOPOLOGICAL VARIATION TO ENERGY CONSUMPTION IN ZIGBEE NETWORKS

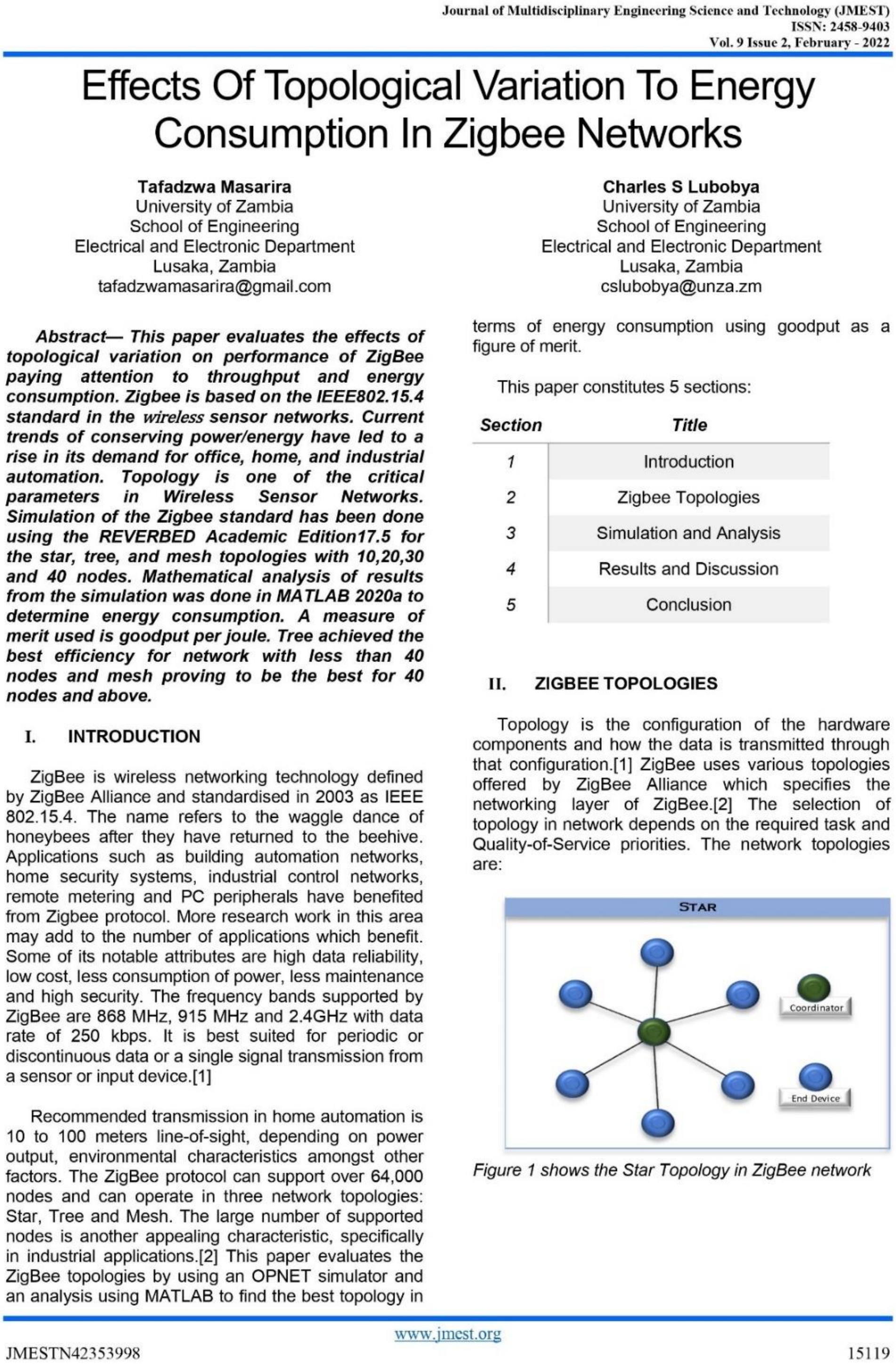
In JMEST, Volume. 9, Issue. 2 February – 2022

Jmest

Registration No:JMESTN42353998 Date: 2/28/2022 Chief Editor,JMEST

Journal of Multidisciplinary Engineering Science and Technology

Appendix 2: Published Journal



Journal of Multidisciplinary Engineering Science and Technology (JMEST)
ISSN: 2458-9403
Vol. 9 Issue 2, February - 2022

Effects Of Topological Variation To Energy Consumption In Zigbee Networks

Tafadzwa Masarira
University of Zambia
School of Engineering
Electrical and Electronic Department
Lusaka, Zambia
tafadzwamasarira@gmail.com

Charles S Lubobya
University of Zambia
School of Engineering
Electrical and Electronic Department
Lusaka, Zambia
cslubobya@unza.zm

Abstract— This paper evaluates the effects of topological variation on performance of ZigBee paying attention to throughput and energy consumption. Zigbee is based on the IEEE802.15.4 standard in the wireless sensor networks. Current trends of conserving power/energy have led to a rise in its demand for office, home, and industrial automation. Topology is one of the critical parameters in Wireless Sensor Networks. Simulation of the Zigbee standard has been done using the REVERBED Academic Edition17.5 for the star, tree, and mesh topologies with 10,20,30 and 40 nodes. Mathematical analysis of results from the simulation was done in MATLAB 2020a to determine energy consumption. A measure of merit used is goodput per joule. Tree achieved the best efficiency for network with less than 40 nodes and mesh proving to be the best for 40 nodes and above.

I. INTRODUCTION

ZigBee is wireless networking technology defined by ZigBee Alliance and standardised in 2003 as IEEE 802.15.4. The name refers to the waggle dance of honeybees after they have returned to the beehive. Applications such as building automation networks, home security systems, industrial control networks, remote metering and PC peripherals have benefited from Zigbee protocol. More research work in this area may add to the number of applications which benefit. Some of its notable attributes are high data reliability, low cost, less consumption of power, less maintenance and high security. The frequency bands supported by ZigBee are 868 MHz, 915 MHz and 2.4GHz with data rate of 250 kbps. It is best suited for periodic or discontinuous data or a single signal transmission from a sensor or input device.[1]

Recommended transmission in home automation is 10 to 100 meters line-of-sight, depending on power output, environmental characteristics amongst other factors. The ZigBee protocol can support over 64,000 nodes and can operate in three network topologies: Star, Tree and Mesh. The large number of supported nodes is another appealing characteristic, specifically in industrial applications.[2] This paper evaluates the ZigBee topologies by using an OPNET simulator and an analysis using MATLAB to find the best topology in terms of energy consumption using goodput as a figure of merit.

This paper constitutes 5 sections:

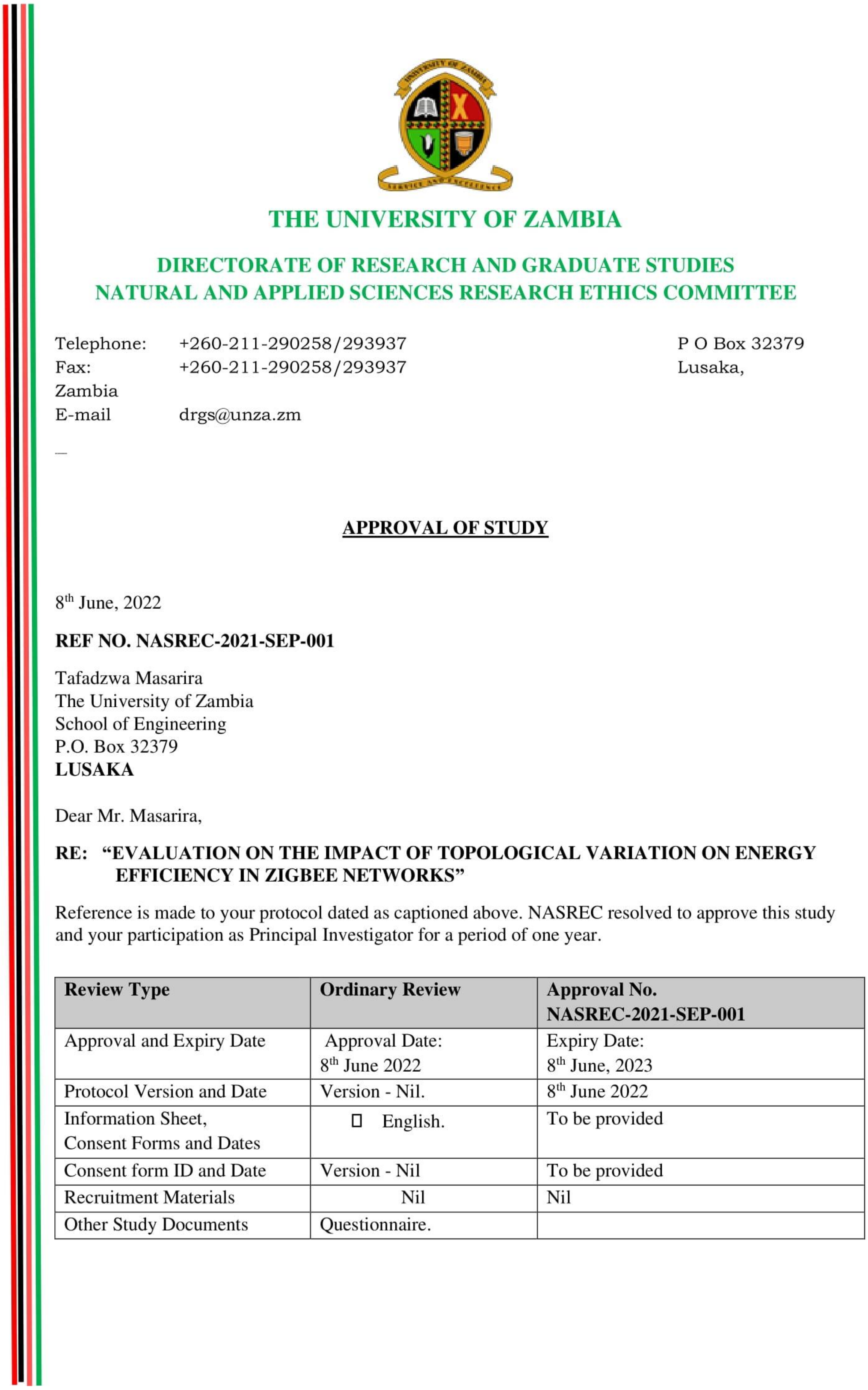
Section	*Title*
1	Introduction
2	Zigbee Topologies
3	Simulation and Analysis
4	Results and Discussion
5	Conclusion

II. ZIGBEE TOPOLOGIES

Topology is the configuration of the hardware components and how the data is transmitted through that configuration.[1] ZigBee uses various topologies offered by ZigBee Alliance which specifies the networking layer of ZigBee.[2] The selection of topology in network depends on the required task and Quality-of-Service priorities. The network topologies are:

Figure 1 shows the Star Topology in ZigBee network

Appendix 3: Ethics Approval Letter



THE UNIVERSITY OF ZAMBIA

DIRECTORATE OF RESEARCH AND GRADUATE STUDIES
NATURAL AND APPLIED SCIENCES RESEARCH ETHICS COMMITTEE

Telephone: +260-211-290258/293937 P O Box 32379
Fax: +260-211-290258/293937 Lusaka,
Zambia
E-mail drgs@unza.zm

_

APPROVAL OF STUDY

8th June, 2022

REF NO. NASREC-2021-SEP-001

Tafadzwa Masarira
The University of Zambia
School of Engineering
P.O. Box 32379
LUSAKA

Dear Mr. Masarira,

RE: "EVALUATION ON THE IMPACT OF TOPOLOGICAL VARIATION ON ENERGY EFFICIENCY IN ZIGBEE NETWORKS"

Reference is made to your protocol dated as captioned above. NASREC resolved to approve this study and your participation as Principal Investigator for a period of one year.

Review Type	**Ordinary Review**	**Approval No.** **NASREC-2021-SEP-001**
Approval and Expiry Date	Approval Date: 8th June 2022	Expiry Date: 8th June, 2023
Protocol Version and Date	Version - Nil.	8th June 2022
Information Sheet, Consent Forms and Dates	□ English.	To be provided
Consent form ID and Date	Version - Nil	To be provided
Recruitment Materials	Nil	Nil
Other Study Documents	Questionnaire.	

Specific conditions will apply to this approval. As Principal Investigator it is your responsibility to ensure that the contents of this letter are adhered to. If these are not adhered to, the approval may be suspended. Should the study be suspended, study sponsors and other regulatory authorities will be informed.

Conditions of Approval

- No participant may be involved in any study procedure prior to the study approval or after the expiration date.

- All unanticipated or Serious Adverse Events (SAEs) must be reported to NASREC within 5 days.

- All protocol modifications must be approved by NASREC prior to implementation unless they are intended to reduce risk (but must still be reported for approval). Modifications will include any change of investigator/s or site address.

- All protocol deviations must be reported to NASREC within 5 working days.
- All recruitment materials must be approved by NASREC prior to being used.

- Principal investigators are responsible for initiating Continuing Review proceedings. NASREC will only approve a study for a period of 12 months.

- It is the responsibility of the PI to renew his/her ethics approval through a renewal application to NASREC.

- Where the PI desires to extend the study after expiry of the study period, documents for study extension must be received by NASREC at least 30 days before the expiry date. This is for the purpose of facilitating the review process. Documents received within 30 days after expiry will be labelled “late submissions” and will incur a penaltyfee of K500.00. No study shall be renewed whose documents are submitted for renewal 30 days after expiry of the certificate.

- Every 6 (six) months a progress report form supplied by The University of Zambia Natural and Applied Sciences Research Ethics Committee as an IRB must be filled in and submitted to us. There is a penalty of K500.00 for failure to submit the report.

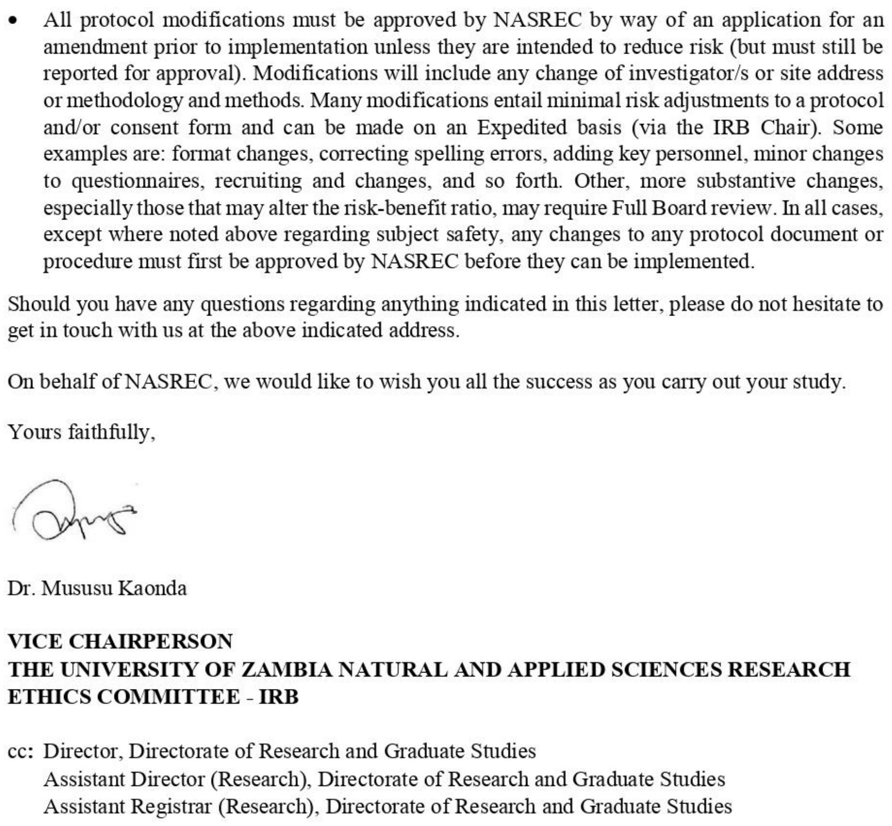
- When closing a project, the PI is responsible for notifying, in writing or using the Research Ethics and Management Online (REMO),both NASREC

- and the National Health Research Authority (NHRA) when ethics certification is no longer required for a project.

- In order to close an approved study, a Closing Report must be submitted in writing or through the REMO system. A Closing Report should be filed when data collection has ended and the study team will no longer be using human participants or animals or secondary data or have any direct or indirect contact with the research participants or animals for the study.

- Filing a closing report (rather than just letting your approval lapse) is important as it assists NASREC in efficiently tracking and reporting on projects. Note that some funding agencies and sponsors require a notice of closure from the IRB which had approved the study and can only be generated after the Closing Report has been filed.

- A reprint of this letter shall be done at a fee.



- All protocol modifications must be approved by NASREC by way of an application for an amendment prior to implementation unless they are intended to reduce risk (but must still be reported for approval). Modifications will include any change of investigator/s or site address or methodology and methods. Many modifications entail minimal risk adjustments to a protocol and/or consent form and can be made on an Expedited basis (via the IRB Chair). Some examples are: format changes, correcting spelling errors, adding key personnel, minor changes to questionnaires, recruiting and changes, and so forth. Other, more substantive changes, especially those that may alter the risk-benefit ratio, may require Full Board review. In all cases, except where noted above regarding subject safety, any changes to any protocol document or procedure must first be approved by NASREC before they can be implemented.

Should you have any questions regarding anything indicated in this letter, please do not hesitate to get in touch with us at the above indicated address.

On behalf of NASREC, we would like to wish you all the success as you carry out your study.

Yours faithfully,

Dr. Mususu Kaonda

VICE CHAIRPERSON
THE UNIVERSITY OF ZAMBIA NATURAL AND APPLIED SCIENCES RESEARCH ETHICS COMMITTEE - IRB

cc: Director, Directorate of Research and Graduate Studies
Assistant Director (Research), Directorate of Research and Graduate Studies
Assistant Registrar (Research), Directorate of Research and Graduate Studies

Appendix 4: MATLAB Code

```
% close all;
% clear all;
% clc;
W_min=2^3;
W_max=2^5;
for j=0:5
    W_j(j+1)=min(2^j*W_min,W_max);
end
syms a;
syms vect2;
syms A;
syms B;
syms NCCA;

Tcca=0.25;
M=5;
sigma=0.32;
sum1=0;
vect1=zeros(1,6);
%vect2=zeros(6,1);
for v=0:M
    temp=a^v-a^(v+1);
    sum2=0;
    for i=0:v
        sum2 = sum2 + ( (W_j(i+1)-1)*0.5 ) * sigma + (v+1)*Tcca;
    end
    sum1 = sum1 + temp*sum2;

end
A = sum1;
sum3 = 0;
for i = 0:M
    sum3 = sum3 + ( (W_j(i+1)-1)*0.5 ) * sigma + (M+1)*Tcca;
end

B = sum3*a^(M+1);

E_D_HOL = vpa((A + B),5);

%Equation 3
Pd = 25;
Oh = 31;
Dr = 250;
T_turn=0.192;
Tack = 0.352;
Tx = (Pd + Oh) / Dr;
T_con=(Tx) * (2 * (T_turn)) + Tack;
```

```
%below is Equation 4....
lambda=0.01;
n=40;
%syms E_D_HOL;
syms den;
syms num;
syms P1;
syms poly;

P1 = lambda*((E_D_HOL)+ T_con);
rho=vpa(P1,5);
%%%Equation 5%%
in_E_Gamma=1-rho;
%%Equation 6%%
a_con=(n-1)*T_con*lambda;
den=in_E_Gamma+lambda*E_D_HOL;
num=a_con*(1-a^(M+1));
poly=num - a*(den);
poly_disp=vpa(poly,5);
alpha_all=solve(poly_disp,a);
%%%Equation 7 Finding NCCA%%%
alpha=alpha_all(2);
sum_alp=0;
for i=1:5
    sum_alp=sum_alp+ alpha^i*(1-alpha)*(i+1)+alpha^(M+1)*(M+1);
end
NCCA=sum_alp;

%%Equation 8%%
V = 3;
Itx = 32;
Irx = 25;
Iidle = 10;
Isl = 3;
Ct = 0.5;
a=alpha;
V_E_D_HOL=subs(E_D_HOL);
Totalcca = NCCA * Tcca;
Tidle = V_E_D_HOL - Totalcca;
Tsl = Ct - Tidle - NCCA - Tx ;
% Finding the power%%%%%
Etx = V * Itx * Tx;
Erx = V * Irx * NCCA;
Eidle = V * Iidle * Tidle;
Esl = V * Isl * Tsl;
Etotal = Etx + Erx + Eidle + Esl;
```