ADVANCED ZIGBEE NETWORK WITH GREATER RANGE AND LONGEVITY

by

Tasneem Khan Shifa, B.Sc.

A thesis submitted to the Graduate Council of
Texas State University in partial fulfillment
of the requirements for the degree of
Master of Science
with a Major in Engineering
December 2021

Committee Members:

Harold Stern, Chair

Rich C. Compeau

William Stapleton

FAIR USE AND AUTHOR'S PERMISSION STATEMENT

Fair Use

Duplication Permission

DEDICATION

This thesis is dedicated to my parents, my mother and father. They have inspired who I am today and who I always want to be. They are main the motivation for everything I do in my life. Also, my little brother who always has my back and believes in me. Then my amazing husband who has been so instrumental in everything I have ever accomplished and I say that with so much pride. He has always inspired me to do better and believed in me even when I didn’t believe in myself. I am so grateful for him. Whatever I am today and whatever I will be is all because of these people.

ACKNOWLEDGEMENTS

I am really grateful to my thesis advisor Dr. Harold Stern, for his continuous motivation and support. The development of the thesis could not have been possible without the expertise of Dr. Harold Stern. His approach and suggestions have always inspired me. It is a genuine pleasure to work with him on this research.

Also, I am very thankful to my committee members Dr. William Stapleton and Dr. Rich C. Compeau for their excellent advice and suggestions during the proposal presentation. The research work could not have been possible without their validation and evaluation of the results of this research.

I would really like to appreciate Dr. Vishu Viswanathan for his continuous support throughout my journey as a graduate student at Texas State University.

Finally, I would like to dedicate all my accomplishments to my mother, father, brother, and my husband. They have always motivated me to do better. Whatever I am today and whatever I will be is all because of them. I am blessed and grateful.

TABLE OF CONTENTS

Page

LIST OF TABLES

Table **Page**

LIST OF FIGURES

Figure **Page**

ABSTRACT

With the rapid development of Internet of Things networks (IoT), a new type of wireless standard, ZigBee, has emerged in order to satisfy the demand of low power dissipation, low cost, and easy deployment among wireless communication devices. In the currently developed ZigBee system, all transmitters use a common spreading code which can result in a large number of message collisions. A promising new system using multiple spreading codes has previously been proposed to increase system throughput, reduce collisions, and increase energy efficiency or range, but it has only been evaluated with constant message lengths and single hop topology. Systems with such restrictions represent only a small subset of IoT networks. For our research, we aim to evaluate the system with variable message length and multiple hopping topology. We will consider a large network with many sensors which are out of the limited range of the coordinator but which can transmit messages through a router, which involves two hops. Therefore, our new proposed multiple hop system has larger range and longevity compared to the single hop proposed system and reduced collisions compared to the current ZigBee system.

We have implemented the code in MATLAB and run multiple simulations in terms of varying the amount of message traffic, message length and number of CAP slots. By comparing each data set and its graphical representation, the results show that our new proposed system has higher success rates than the current system. Our findings determine suitability for a much larger set of IoT systems and applications and may suggest protocol

changes that can produce further improvements to increase reliability and security, range, operating life, and throughput of ZigBee systems. This will be significant for enabling new applications and attracting more customers. So, with the design of high-performance ZigBee wireless communication networks, it will have a broad application space in real life.

1. INTRODUCTION

1.1 Problem Statement

In the present communication world, there are numerous high data rate communication standards available, but these standards are not optimal for many lower data rate applications involving sensors and control devices. The Zigbee technology is low-cost and low-power consumption, and its excellent characteristics make this communication best suited for various embedded applications, industrial control, instrumentation, and home automation. The Zigbee technology provides a maximum range for transmission distances from 10–100 meters based on the output of power as well as environmental characteristics. Zigbee communication is specially built for control and sensor networks, based on the IEEE 802.15.4 standard for wireless personal area networks (WPANs).

Zigbee is a complete IoT (Internet of Things) solution that allows smart objects to work together. Zigbee technology certified products can connect and communicate with each other by using the same IoT language. Also, in smart homes and buildings millions of Zigbee products already are deployed. [1]

All smart home appliances depend on connectivity with a device, app, or hub. For integrating a connected home, Wi-Fi is seen as a ubiquitous choice. Both Wi-Fi and ZigBee have their positive qualities, but they also have some negatives. Wi-Fi has higher bandwidth but it has greater power consumption and is more expensive than ZigBee. On

the other hand, ZigBee has longer battery life and lower cost but it has lower bandwidth and range than Wi-Fi. So, to make any decision based around budgets, power consumption and range, these tradeoffs are crucial to understand. In case of power consumption, ZigBee-based networks generally consume 25% less power than that of Wi-Fi networks. ZigBee's battery life is a major plus over Wi-Fi and needs to be strongly considered if devices' endpoints will run on batteries. [2] Also, with our proposed new ZigBee multiple hop system, we can have a greater range and longevity without having to spend more power.

In recent times, a promising new ZigBee system has been proposed which uses multiple spreading codes. [3] This new system has been developed to increase system throughput, reduce collisions, and increase energy efficiency. But the system has been evaluated by using only constant message lengths and single hop topology. In the present ZigBee system by using constant message lengths, there is little flexibility in the whole system and because of using single hopping, there is limited range and there are excessive collisions because nodes only contact with the coordinator but can't communicate with each other. Thus, the capacity is decreased along with waste of power and time in the system. So, these systems represent only a small subset of IoT networks because of different restrictions.

For our research, we aim to evaluate the proposed system with variable message length and multiple hopping topologies. With our developed ZigBee system, there will be fewer collisions and increases in throughput and range and these changes will save a lot of time and power for the whole system relative to the present system. We have developed simulations in MATLAB to evaluate our system. The results will be analyzed and

compared with the present system.

Our findings will determine suitability for a much larger set of IoT systems and applications and will suggest protocol changes that can produce further improvements to increase reliability and security, range, operating life, and throughput of ZigBee systems. This will be significant for enabling greater applications and it will bring more customers. So, with the design of high-performance ZigBee wireless communication networks, our system will have a broad application space in real life.

1.2 ZigBee on the Internet of Things

The Internet of Things (IoT) has not been around for very long, but over the past few years we have moved from disconnected systems into a world more completely linked and more in control at our fingertips. Smart home devices and similar technologies have progressed over the years. What once started with automation has now expanded into the Internet of Things (IoT).

As a concept, the Internet of Things wasn't officially named until 1999. The first example of an Internet of Things, which was from the early 1980s, was a Coca Cola machine at the Carnegie Melon University. By connecting the Internet to the refrigerated appliance, local programmers could check if drink was available, and, they could see if the drink was cold, before making the trip.

In simpler terms, it can be stated that the Internet of Things consists of any device with an on/off switch connected to the Internet. This includes a broad range of devices and applications, from cellphones to building maintenance to the jet engine of an airplane. It also includes medical devices, such as a heart monitor implant or a biochip transponder in a farm animal, so all these can transfer data over a network and are members of the IoT. So, theoretically if anything has an off/on switch, then it can be part of the system. The IoT consists of a gigantic network of internet connected "things" and devices.

Kevin Ashton, the Executive Director of Auto-ID Labs at MIT, was the first one to describe the Internet of Things. He believed one of the most important prerequisites for the Internet of Things was Radio Frequency Identification (RFID). He also concluded that all computers could manage, track, and inventory devices if they were all "tagged,". Through technologies such as digital watermarking, barcodes, and QR codes, the tagging of things has been achieved to some extent. Inventory control is one of the more obvious advantages of the Internet of Things. So, any device capable, can be interconnected with other devices. By the end of the year 2013, the Internet of Things had evolved into a system using multiple technologies, ranging from the Internet to wireless communication and from micro-electromechanical systems (MEMS) to embedded systems. IoT supports the automation of buildings and homes, wireless sensor networks, GPS, and control systems. [4]

Applications of Internet of Things (IoT) have developed rapidly, including communications networks, sensors, intelligent applications, centralized management, many control & monitoring systems like home and office automation, medical monitoring,

industrial automation, low power sensors, HVAC systems, fire extinguishers and wireless remote control.

Specifically, all the connected devices can share information with each other. All the devices can be controlled without the need to visit each thing individually. Similarly, devices manufactured by different companies are connected over a single network. Therefore, IoT requires a common language for its communication. That's where ZigBee contributes to the Internet of Things. [4]

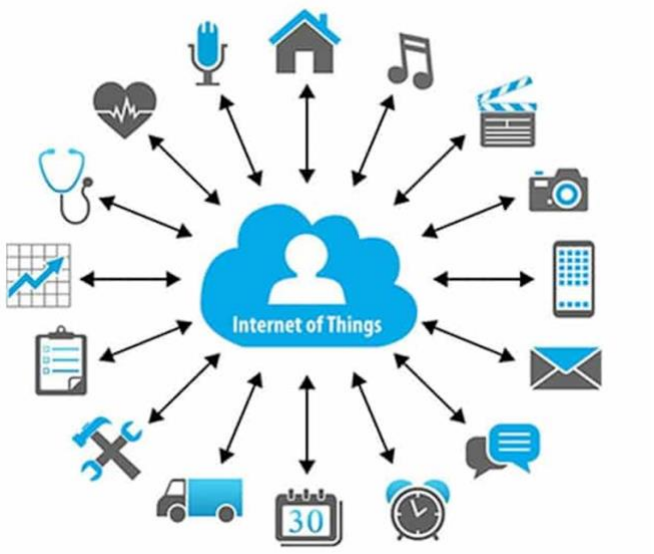


Figure 1.1. Internet of Things (IoT) [5]

Zigbee based technology is considered one of the major wireless communication breakthroughs in recent years. [6] It offers reliability, security, lower cost and easy deployment and support for multiple network topologies like star, tree, and mesh networks. The wireless technologies like Bluetooth and Wi-Fi provide streaming of high definition

content and are striving for even faster transmission speeds. But on the other hand, ZigBee is designed for low power applications and lower data rates and applications like controlling a series of simple devices such as LEDs or thermostats or sensors, and these devices can run for many years without the need for recharging.

ZigBee is popular for many IoT applications due to its extremely low power consumption and with multi hop networks, its long reach. Also, it can communicate with its peers as well as a smart hub. So, the smart devices can create their mini-internet and create a network where signals can be transmitted. There is a great economic advantage in this approach because no separate routers or networks are needed, which can be expensive. This type of configuration is called a mesh network and it is very useful for many wireless systems worldwide. [7]

The ZigBee standard incorporates the IEEE 802.15.4 physical radio specification. ZigBee operates in unlicensed bands including 2.4 GHz, 900 MHz, and 868 MHz. [8] For commercial ZigBee, the 2.4 GHz band is used worldwide. However, there are different devices that use different frequency bands like 686 MHz, 784 MHz and 915 MHz in Europe, China, and USA respectively. One of the main reasons for development of ZigBee technology is because of its use in wireless monitoring and control. [9]

In the currently developed ZigBee system, all transmitters use a common spreading code. Because of this, collisions occur and the transmitted messages cannot be successfully recovered. This affects the capacity and efficiency of the ZigBee systems. Also, in current

systems using single hopping topology, all nodes can't communicate with each other and can only communicate with a coordinator. So, a lot of interference occurs while transmitting messages. This wastes a lot of power and time.

A promising new system using multiple spreading codes has been proposed to increase system throughput, reduce collisions, and increase energy or range, but it has only been evaluated with constant message lengths and single hop topology. [3] But these are significant restrictions, so the proposed system works very well with subsets of IoT networks but may not at all fulfil the requirements of many other networks.

In our thesis, we analyze the proposed ZigBee system with variable length messages and multiple hop topology, so that there will be fewer collisions while transmitting messages. So, the need for retransmission or the loss of information will be less, and the energy that is wasted will be saved. The capacity of the system will increase. So, this design of ZigBee wireless communication will have a broader set of applications in real life.

1.3 ZigBee Applications in IoT

ZigBee technology is very popular for many IoT applications because of its multi hop networks, long range, extremely low power consumption and lower cost. Some of its applications are narrated in the following.

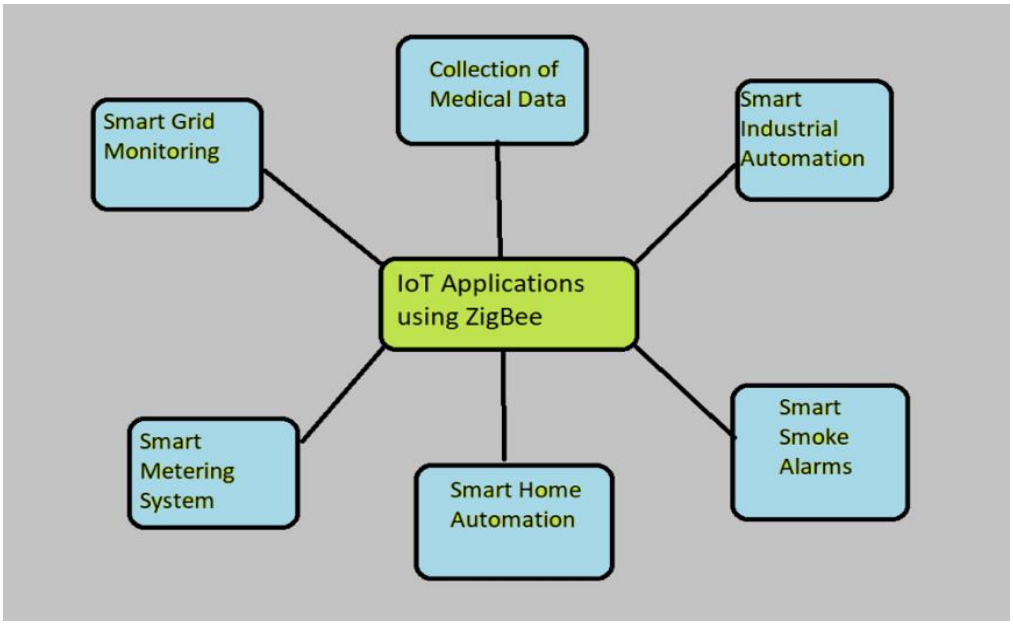


Figure 1.2. IoT Applications Using ZigBee [10]

- **Medical Data Collection:** This technology is used in home patient monitoring where a patient wears a Zigbee device which collects information like the pulse rate, the temperature of the body, blood pressure etc. Here the collection of medical data is very important and crucial.

- **Smart Industrial Automation:** In manufacturing and production industries, various parameters and critical pieces of equipment are monitored using a communication link. Because of ZigBee, cost is reduced and there is higher reliability.

- **Smart Smoke Alarms:** Smart smoke alarms are used for sensing fire or smoke and for issuing acoustic-optic alarm signals to alert people locally and send alarm notifications to user Apps remotely. So, this alarm has an advanced sensor, high stability, and super low power consumption.

- **Smart Home Automation:** Nowadays there are many home automation systems like Google Home, Amazon Alexa, and others. Zigbee wireless technology is perfectly suitable for controlling home appliances remotely as a surveillance system, lighting control system, appliance control system, or safety systems.

- **Smart Metering System:** ZigBee-based automatic meter reading (AMR) systems can create self-forming wireless mesh networks across residential complexes that link meters with utilities corporate offices, and they can provide the opportunity to remotely monitor a residence's electric, gas, and water usage. This eliminates the need for people visiting each residential unit on monthly basis. So, everything is getting easier for people because of smart metering systems.

- **Smart Grid Monitoring:** A smart grid involves all the stakeholders of power systems with the bi-directional flow of power and information from generation to consumption. Thus, communications technologies are a vital part of the smart grid and enable the utility to manage tasks like energy management in Home Area Networks (HANs), Neighbor Area Network (NANs), and Wide Area Network (WANs). These networks are expecting to provide sustainable and efficient energy services with advanced control and communications infrastructure in a smart grid environment. [10]

So, for these applications ZigBee is very popular in IoT. Also, along with the development of ZigBee, there are other numerous applications for ZigBee in present years.

1.4 Thesis Objective

With development of IoT networks, many promising new systems have been proposed. For our thesis, we plan to focus on improvements to collision avoidance in ZigBee systems. As proposed in reference [3], we will incorporate multiple spreading codes. Our innovation is that, unlike reference [3], we will adapt our system to allow variable length messages and to incorporate multiple hop network topology. Variable length messages will enable flexibility and additional applications and will require less time to transmit longer messages.

Reference [3] used single hopping, but there are vast applications for which multiple hopping topologies will work better. In single hopping, nodes only contact with the coordinator but can't communicate with each other. So, either range is limited or the system requires a lot of power to transmit messages. With multiple hopping, we are assigning certain nodes as routers. So, by using multiple hooping, the system will save a lot of power. Saving power means longer battery life and greater range for ZigBee. The capacity of the ZigBee system will be increased.

We have developed simulations in MATLAB to evaluate our system. We will show advantages from our proposed method in terms of reliability and security, throughput, range, and the operating life of the ZigBee system. This method will also reduce the collisions of simultaneous ZigBee signals; thus, it will make ZigBee more efficient. Evaluation with variable message length and multi-hop network topologies will be in

enabling a greater number of applications and it will bring more customers. So, with the design of a high-performance ZigBee wireless communication network, it will have broad application space in real life.

1.5 Organization of Thesis

The thesis is organized as follows:

Chapter 1 provides an introduction, starting with a problem statement followed by a short description of ZigBee on Internet of Things (IoT) and ZigBee technology development. Then IoT applications using ZigBee are discussed. Lastly, there is the main objective of this thesis along with its chapter organization. Then Chapter 2 provides a description of current ZigBee systems and gives an introduction to IEEE 802.15.4 and the ZigBee alliance and its protocol development. Chapter 2 then provides a discussion of current ZigBee devices as well as operating modes for ZigBee, followed by a brief discussion of different topologies defined in the ZigBee network. Chapter 2 concludes by providing more information about present ZigBee systems and how they work.

Chapter 3 describes the different layers of the ZigBee system along with the functions and operations of different layers. Also, different algorithms and techniques are described, like pseudorandom sequences (PN) and how they are used in the direct sequence spread spectrum (DSSS), the superframe structure of a data frame, and carrier sense multiple access (CSMA/CA) techniques. Chapter 4 provides a literature review, describes various previous research works with ZigBee systems, and also discusses scope for more reliable,

secure, and cost-efficient ZigBee systems.

Chapter 5 starts with our proposed solution. In this section the mathematical analysis and MATLAB simulation steps to design the proposed system are described. Also, a flowchart of the proposed solution is presented and explained. In chapter 6, we provide simulation results and analysis of our proposed system by varying different parameters. It gives a performance comparison between our new proposed ZigBee system and the current ZigBee system. Then chapter 7 concludes the whole thesis research and Chapter 8 provides suggestion for future research.

2. DESCRIPTION OF CURRENT ZIGBEE SYSTEMS

With the development of wireless sensor networks and current technology, ZigBee has gained a lot of attention. Based on protocol standard IEEE 802.15.4, the physical and datalink layers of Zigbee technology are generated. For wireless sensor networks, ZigBee has amazing features like low power consumption, low complexity, and high reliability. Also, ZigBee devices have very long battery life, low cost, and high security. Because of all these features, ZigBee is the best option for many WSNs (Wireless Sensor Networks). [11] In this chapter we will provide a description of the ZigBee alliance's protocol development and details of ZigBee architecture.

2.1 ZigBee and IEEE 802.15.4

ZigBee is a standard-based network protocol supported by the ZigBee alliance. The network and application layers are defined by Zigbee alliance (software) and the physical and media access control layers for low-rate wireless personal area network (LR-WPAN) are defined by IEEE802.15.4 (hardware) which is designed for short range, low power consumption, low cost, and low data rate wireless communication devices. All these are mainly targeted towards automation and remote-control applications. The IEEE 802.15.4 committee worked on a low data rate standard. Then after some time the ZigBee Alliance and the IEEE decided to join forces and ZigBee is the commercial name for this technology. [12]

ZigBee provides low cost and low power connectivity for equipment which needs battery life as long as several months to several years. But this equipment does not require data transfer rates as high as those enabled by Bluetooth. In addition, ZigBee can be implemented in tree and mesh networks larger than is possible with Bluetooth. ZigBee compliant wireless devices are expected to transmit 10-100 meters, depending on the RF environment and the power output consumption required for a given application. ZigBee works in the unlicensed RF worldwide (2.4GHz global, 915MHz Americas or 868 MHz Europe). The data rate is 250kbps at 2.4GHz, 40kbps at 915MHz and 20kbps at 868MHz. [10] Different multiple access techniques can be used in ZigBee. For ZigBee, a range up to 150 meters outdoor can be achieved by Direct Sequence Spread Spectrum (DSSS). It consumes less power than Frequency Hopping Spread Spectrum (FSSS). Since multiple hops are allowed ZigBee is capable of making a very large network covering large distances. [11]

IEEE and ZigBee Alliance have been working closely for many years to specify the entire protocol stack. At one hand, IEEE 802.15.4 focuses on the specification of the lower two layers of the protocol stack which are physical and data link layer. On the other hand, ZigBee Alliance aims to provide for the upper layers of the protocol stack from network to the application layer. It provides interoperable data networking, security services, a range of wireless home and building control solutions, interoperability, compliance testing, marketing of the standard, and advanced engineering for the evolution of the standard. Through these, consumers are assured to buy products from different manufacturers with confidence that the products will work together.

Now IEEE 802.15.4 is detailing the specification of PHY (Physical layer) and MAC (Mac layer) by offering building blocks for different types of networking known as star, mesh, and cluster tree which we will discuss in Section 2.4, “ZigBee Network Topologies”.

Network routing schemes are designed for power conservation, and low latency through guaranteed time slots. ZigBee network layer has a unique feature which is communication redundancy eliminating single point of failure in mesh networks. Also, the physical layer has key features which include energy and link quality detection, and clear channel assessment for improved coexistence with other wireless networks. [12]

2.2 Current ZigBee Devices

ZigBee is a wireless technology developed as an open global standard to address the unique needs of low-cost, low-power wireless IoT (Internet of Things) networks. Zigbee network is defined with three different device types, which are,

- Coordinator,
- Router and
- End Device.

The following diagram shows a generic ZigBee network.

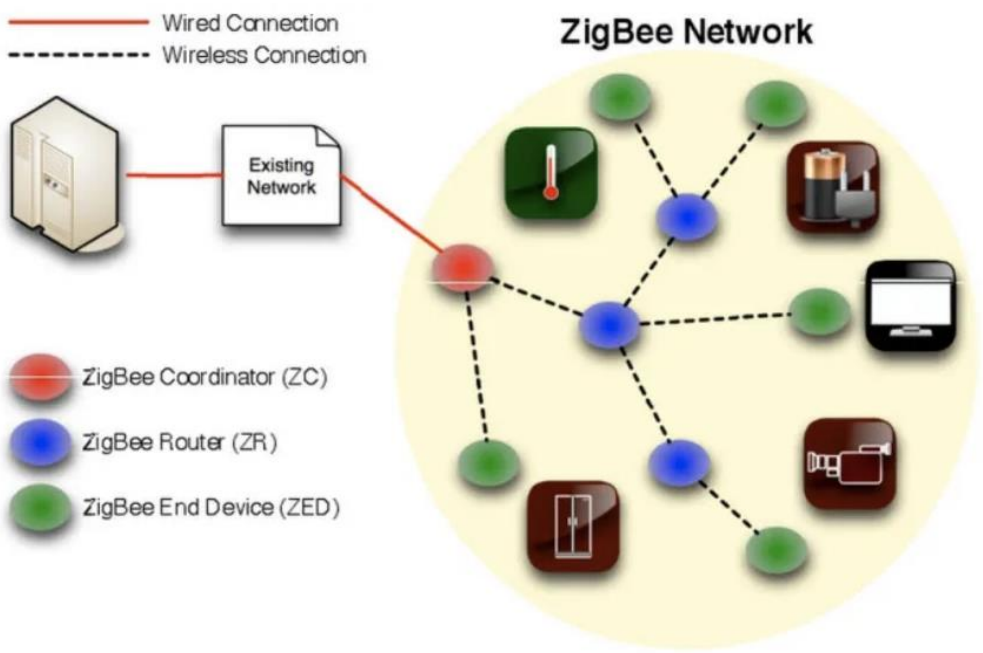


Figure 2.1. A Generic Zigbee Network [10]

2.2.1 Coordinator

Zigbee networks only have a single coordinator device, and this is the source of the network, the root of the tree that can bridge to other networks. The coordinator mainly stores information on the network, manages security keys and access and acts as the trust center.

The functions of the device are the following:

- Coordinator starts the network and selects the channel.
- For sleeping end device children nodes, it buffers wireless data packets.
- It manages the functions that will define the network & secure it and keep it healthy.
- The coordinator must be powered on all the time.

An example of a ZigBee coordinator would be the modems Assured Systems supply and USB ZigBee Coordinator AT and API.

2.2.2 Router

A router is a full-featured Zigbee node. Routers perform different functions within the network along with receive & forward data to and from other devices on the network.

The following are the functions of a router:

- Router can join existing networks and send, receive, & route information. Routing mainly involves acting as a messenger for communications between other devices that are too far apart to convey information on their own.
- Like the coordinator, a router also buffers wireless data packets for sleeping end device children. It allows other routers and end devices to join the network.
- Routers should be powered on all the time.
- Multiple router devices can coexist in a network.

An example of a router is a smart water meter which can read the usage from a wireless sensor, then transmit data to a field engineer's handheld device.

2.2.3 End Device

An end device is basically a reduced version of a router. An end device receives and responds to its parent node (coordinator or router), but it can't talk to other devices on the

network. Because of this, the node can rest and preserve battery life.

This end device's functions are given below:

- End device can join existing networks and send and receive information. But it cannot act as messenger between any other devices.
- It can't allow other devices to join the network.
- An end device can power itself down intermittently and thus it saves energy by temporarily entering a non-responsive sleep mode. It uses less expensive hardware.
- It always needs a router or the coordinator to be its parent device. Because the parent helps end devices join the network, and stores messages for them when they are asleep.

An example of an end device would be a light switch on an automated home management system.

So, mainly a ZigBee network consists of these three types of devices. ZigBee networks may have any number of end devices. In fact, a network can be composed of one coordinator, multiple end devices, and zero routers. [13] [14]

2.3 ZigBee Operating Modes

There are two types of mode in which ZigBee operates, which are,

- Beacon Mode and
- Non-Beacon Mode.

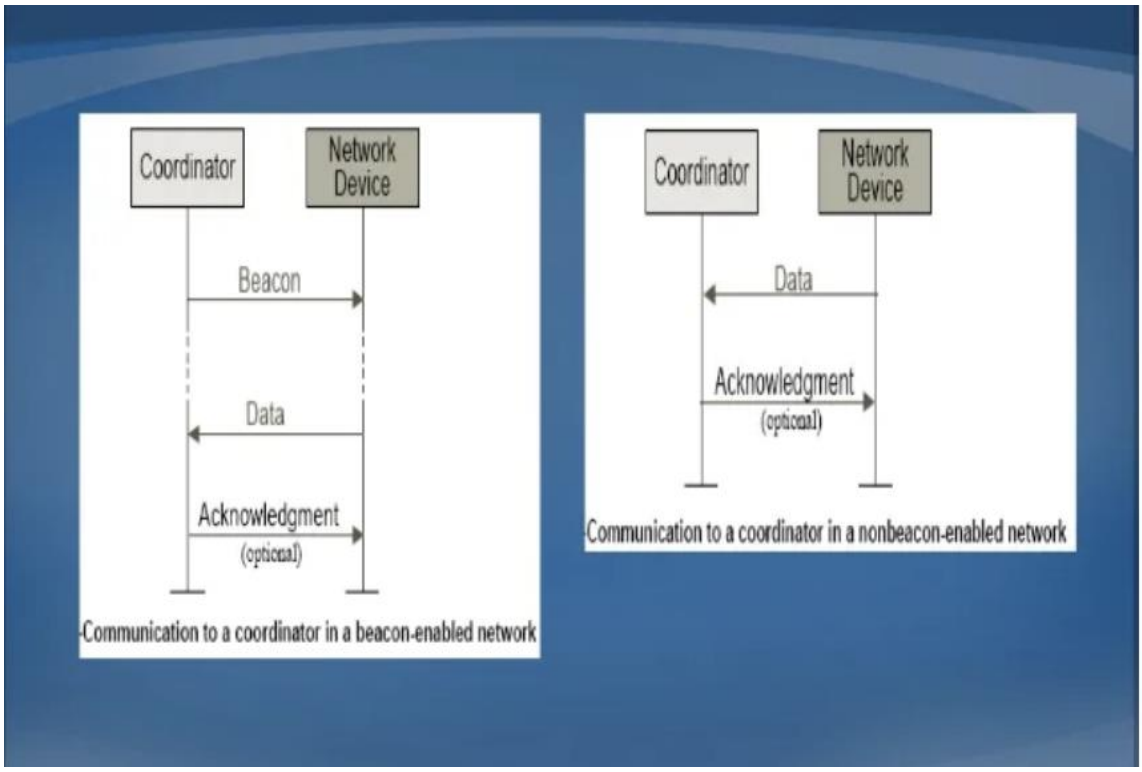


Figure 2.2. ZigBee Modes of Operation [10]

These modes are described in the following,

2.3.1 Beacon Mode

In the beacon mode, a device watches out for the coordinator's beacon which gets transmitted periodically, then locks on and looks for messages addressed to it. After complete message transmission, the coordinator dictates a schedule for the next beacon so that the device 'goes to sleep'. Also, the coordinator itself switches to sleep mode.

By using the beacon mode, in a ZigBee network all the devices can know when to communicate with each other. In this mode, the timing circuits must be quite accurate or

wake up sooner to be sure not to miss the beacon. This means an increase in power consumption by the coordinator's receiver and causes nonoptimal increase in costs. [10]

2.3.2 Non-Beacon Mode

The non-beacon mode is included in a system where devices are 'asleep' nearly always, as an example in smoke detectors and burglar alarms. So, at random intervals, the devices wake up and confirm their continued presence in the network.

On activity detection, all the sensors spring to attention, as it were, and transmit to the ever-waiting coordinator's receiver since it remains powered. But there is the remotest of chances that a sensor finds the channel busy, in which case the receiver, unfortunately, will miss a call. [10]

2.4 Network Topologies of ZigBee

Network topology is the design of the elements such as links or nodes of a communication network. ZigBee can have multiple network structures and those are described below.

2.4.1 Star Topology

Star network is a single hop network which is composed of a coordinator and multiple end devices. All devices are connected to the single coordinator node. End devices are

physically and electrically separated from each other and can't communicate directly with each other but only communicate with the coordinator. End devices pass information only through the coordinator. Star topology is the simplest and most limited one in the ZigBee network. It is defined by the underlying 802.15.4 specification which Zigbee builds on. The disadvantage of star topology is that it's wires or cable get damages easily and expensive. The evaluation of the system proposed in Reference [3] assumed a star topology.

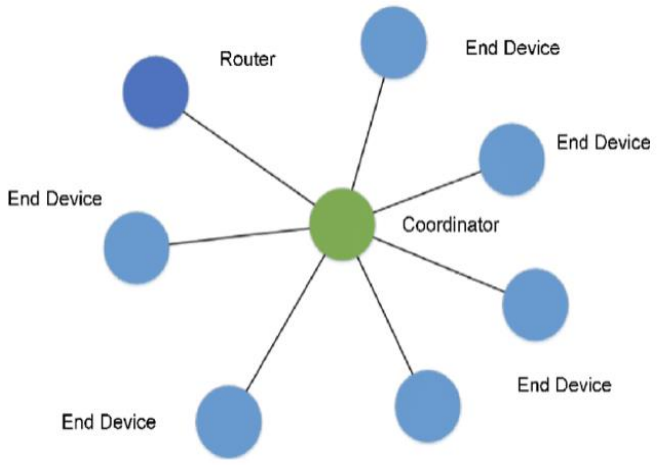


Figure 2.3. Star Topology Model [10]

2.4.2 Tree Topology

The tree network has similarities to a star network, but the difference is that nodes on different branches can communicate with each other. The tree topology consists of a coordinator, few routers and end devices. The routers operate as an extension for the network coverage. The parent nodes are coordinators or routers. The end nodes connecting

to the parent (coordinators or routers) are known as children. Only the end devices can communicate with the parent. Some end devices communicate directly with the coordinator, but other end devices require two hops for their message to arrive at the coordinator i.e., one hop to the router, the second hop from the router to the coordinator. This is the topology we will be evaluating in our thesis. The drawback of the tree topology is if one parent is disabled, the children of the disabled parent cannot communicate with other devices in the network even if they are close to each other.

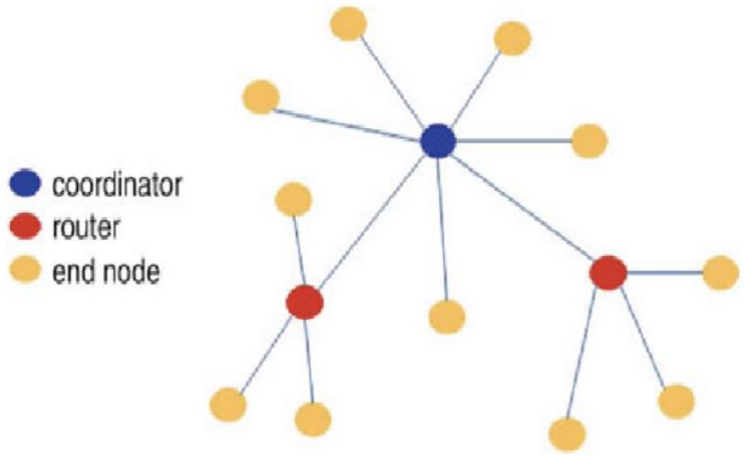


Figure 2.4. Tree Topology Model [10]

2.4.3 Mesh Topology

The mesh topology consists of a coordinator, a few routers and end devices and network range can be expanded by adding more devices into the network. In mesh network, nodes can communicate with any other nodes within their range. So, if during the transmission

one of the paths fails, the node will find the alternate path to reach to the destination.

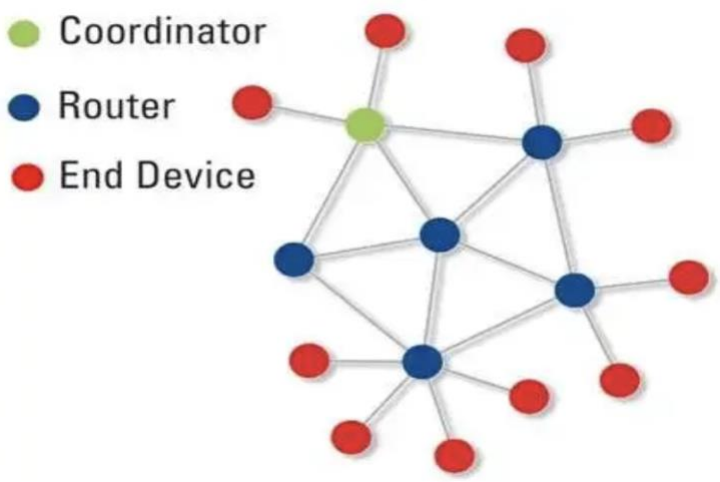


Figure 2.5. Mesh Topology Model [10]

With routing, the messages hop from one node to another node to reach its destination. Mesh networks are multi-hop networks. Thus, in this network dead zones can be eliminated. By using this topology, it is easier for a user to add or remove the device because those can communicate with any destination device in the network. So, mesh networks are more robust than star and tree networks but are more complex. [10] [15]

2.5 Present ZigBee Working System

With the rapid development of ZigBee, a promising new system has recently been proposed by Ms. Rashmi Mohan Kumar in her thesis on “Collision Avoidance and Extending Capacity and Range in ZigBee” [3]. She proposed a solution to overcome the effects of collisions in ZigBee systems. She introduced a system where all ZigBee transmitting

devices randomly select PN sequences for spreading the data from a multiple codes list (eight or sixteen codes) instead of all devices using the same PN sequence, as currently defined by IEEE802.15.4. Thus, collisions can be avoided. Even if collisions occur, still it would be possible to successfully transmit messages (seven out of eight times or fifteen out of sixteen times). The capacity of the ZigBee system is increased as more data can be transmitted. Also, retransmission of data will not be needed, and so additional power can be saved [3]. So, saved energy can be traded off to increase a system's range.

Reference [3] developed a code and ran multiple simulations in MATLAB to test the proposed system. The author represented the system using star topology, meaning a single hop network. Also, the effects of the system were verified using only a fixed message size. So, for further research, we have incorporated variable message length and two-hop topology (tree network) in this system, enabling a larger set of applications in IoT networks.

3. ZIGBEE ARCHITECTURE

The relationship between Zigbee and IEEE 802.15.4 is often confusing, but the two are not the same. IEEE created the 802.15.4 specification and maintains the specification. It defines the physical (PHY) layer and media access control (MAC) of the wireless network. Mechanisms like discovering, forming, and joining networks, changing channels, detecting noise and interference in channels are defined by IEEE 802.15.4. But it doesn't specify how to implement multi-hop communications. So, for single hop, only IEEE 802.15.4 MAC/PHY are needed. [16] The protocol stack of ZigBee is shown in Figure 3.1,

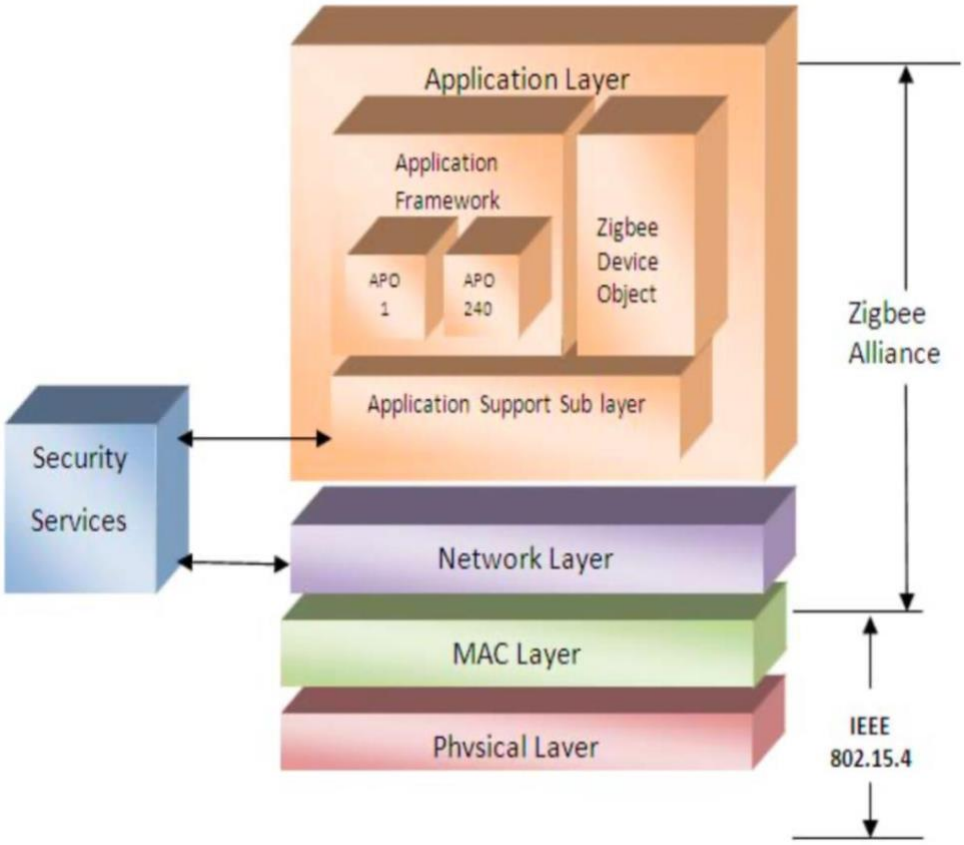


Figure 3.1. ZigBee Architecture [16]

Zigbee is the primary protocol that builds on the 802.15.4 standard. It adds network layer, which is capable of multi hop networking, security layer, capable of complex security situations and application layer for interoperable application profiles. It's ZigBee that provides tree and mesh networking and multi hop capabilities and it enhances the data packet reliability and specifies application-to-application interoperability. ZigBee does not use all the 802.15.4 MAC/PHY specification, but only a subset. ZigBee differs from 802.15.4 specification in the time out beacon responses. The default 802.15.4 specification time out responses to beacon requests don't allow enough time for all the nodes to respond in the network. It is not built with large networks, but ZigBee is built for larger networks. [16]

Protocol architecture is primarily based on Open System Interconnection (OSI) model. ZigBee builds on IEEE standard 802.15.4 which defines the physical & media access control (MAC) layers and ZigBee alliance defines the network layer and application layer. The layers are described in the following sections of this thesis.

3.1 Physical Layer

In the system, the physical layer is the closest layer to the hardware, and it directly controls and communicates with the radio transceiver. It handles tasks such as channel selection, clear channel assessment and hardware initialization which involves ZigBee hardware. The standard mainly offers PHY options based on the frequency band, and they are using direct sequence spread spectrum (DSSS). DSSS is a form of spread spectrum transmission which

uses spreading codes to spread the signal out over a wider bandwidth then would normally be required. In physical layer the data rate is 250kbps at 2.4GHz, 40kbps at 915MHz and 20kbps at 868MHz. [12]

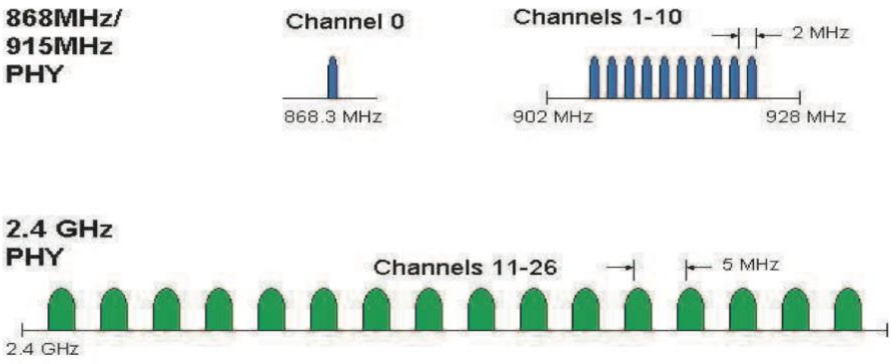


Figure 3.2. Physical layer operating frequency bands [12]

Table 3.1. Frequency bands and data rates in physical layer [12]

PHY (MHz)	**Frequency Band (MHz)**	**Spreading Parameters**		**Data Parameters**		
		Chip Rate (kchip/s)	**Modulation**	**Bit Rate (kb/s)**	**Symbol Rate (ksymbol/s)**	**Symbols**
868/915	868-868.6	300	BPSK	20	20	Binary
	902-928	600	BPSK	40	40	Binary
2450	2400-2483.5	2000	O-QPSK	250	62.5	16-ary Orthogonal

The higher data rate at 2.4GHz is assigned to a higher-order modulation scheme. This means higher throughput, lower duty cycle or lower latency. Lower frequency provides longer range due to lower propagation losses. Thus, larger coverage area and better sensitivity can be translated from low rate. This information is summarized in Table 3.1.

3.1.1 Receiver Energy Detection (ED)

In the physical layer, the receiver energy detection (ED) measurement is used by the network layer for the selection algorithm. It is an estimation of the received signal power within the bandwidth of an IEEE 802.15.4 channel. The ED result will be defined as an 8-bit integer ranging from 0x00 to 0xff. The minimum value (0) indicates received power less than 10dB above the specified receiver sensitivity. The range of received power will be at least 40dB spanned by the ED values. Within this range, the mapping from the received power in decibels to ED values is linear with an accuracy of +−6dB. [12]

3.1.2 Link Quality Indication (LQI)

The LQI measurement is a characterization of the strength and quality of a received packet. By receiving a packet, the PHY sends the PSDU length, PSDU itself and link quality (LQ). The PLCP Service Data Unit (PSDU) is a view of the MPDU from the other side. The Physical layer refers to the 802.11 frame as the PSDU. By using receiver ED or a signal to noise estimation, or a combination of these methods, measurement of the LQI is accomplished.

The LQI result is reported as an integer ranging from 0x00 to 0xff. The highest and lowest quality of IEEE 802.15.4 signals observed by the receiver are associated with the minimum and maximum LQI values consecutively and these values are distributed between these two limits. LQI result is used up to the network or application layers. [12]

3.1.3 Clear Channel Assessment (CCA)

The clear channel assessment (CCA) is performed according to at least one of the three methods described below:

i) CCA will report a busy medium upon any energy above the ED threshold.
ii) By detecting any signal with modulation and spreading characteristics of IEEE 802.15.4, CCA will report a busy medium. This signal might be above or below the Receiver Energy Detection (ED).
iii) With the detection of a signal with the modulation and spreading characteristics of IEEE 802.15.4 with energy above the ED threshold, CCA will report a busy medium. [12]

3.1.4 PPDU Format

Physical layer has two sublayers, i) Physical layer convergence procedure (PLCP) and ii) Physical medium dependent (PMD). At first the PLCP takes the frame from the MAC sublayer and creates the PLCP Protocol Data Unit (PPDU) and thus the frame is prepared for transmission. Then PMD sublayer modulates and transmits the data as bits. When the

MAC Protocol Data Unit (MPDU) is passed on to the physical layer it is then referred to as a PLCP Service Data Unit (PSDU).

Each PPDU packet consists of basic components, which are,

i) SHR: A receiving device is synchronized and locked into the stream because of SHR.

ii) PHR: This contains frame length information.

iii) A variable payload: This carries the MAC sublayer frame. [12]

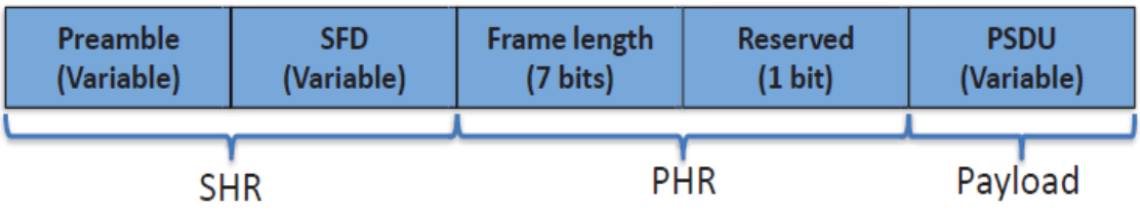


Figure 3.3. PPDU format [17]

3.1.5 Pseudorandom Sequences (PN)

A PN sequence is a sequence of symbols, also known as chips, which represents binary 1's and 0's. A pseudorandom noise (PN) signal is like a noise signal which satisfies one or more of the standard tests for statistical randomness. It is "pseudorandom" because it has a deterministic sequence of pulses that will repeat itself after a certain time period. The time duration of a chip is normally much shorter than the time duration of a bit and because of that the bandwidth or spectrum of a PN sequence is normally much greater than the bandwidth of the data. [3]

One of the great advantages of using a PN sequence to spread data is that the effects of noise are significantly reduced in the received signal. As transmitter output power spreading out the bandwidth lowers the energy at a given frequency, if no one knows presence of the spread spectrum signal, among high noise level, the data cannot be detected. But if the receiver knows the correct PN sequence, the data can be separated from most of the noise in the spread spectrum signal. [3]

The Direct Sequence Spread Spectrum modulation (DSSS) technique uses the concept of PN sequences to modulate the data by spreading the data over the spectrum. The PN sequences are used in many applications such as cellular (mobile) telephones and base stations, GPS navigation systems, wireless Internet (Wi-Fi) communications, Bluetooth communications protocol, satellite communications transmitters and receivers, wireless (residential) telephones, noise generators and many other applications. So, ZigBee uses a PN sequence to spread the data but it uses the same PN sequence for all transmitters. This practice reduces the effects of noise and interference from other non-ZigBee systems on the received signal, but the received signal is still vulnerable to collisions if multiple ZigBee end nodes and/or routers transmit their data at the same time. [3]

3.2 MAC Layer

The MAC layer provides data service and management service by being the interface between the physical layer and network layer [18]. It has two services, i) MAC data services and ii) MAC management service interfacing to the MAC sub–Layer Management

Entity (MLME) Service Access Point (MLME-SAP). The MAC data service enables the transmission and reception of MAC Protocol Data Units (MPDUs) across the PHY data. This layer generates beacons and synchronizes devices to the beacon signal in beacon enabled services. Also, association and dissociation functions are done here. Mac layer defines the following four frame structures [18], which are (i) Beacon frame, (ii) Data frame, (iii)Acknowledge frame and (iv) MAC command frame.

3.2.1 Superframe Structure

The format of the superframe is confined by network beacons and divided into 16 equal sized slots. The functions of the beacon are to describe the structure of superframes, synchronize the attached devices and identify the PAN. The beacon frame is sent in the first slot of each superframe. The superframe is defined by the coordinator, if a coordinator does not want to use the superframe structure, it will turn off the beacon transmissions.

There are two portions in a superframe, i) Active portion and ii) Inactive portion. In an inactive portion, the coordinator will not interact with its PAN and will enter a low-power mode. The active portion has two types of periods, i) Contention access period (CAP) and ii) Contention free period (CFP). If any device wants to communicate during CAP, it will have to compete with other transmitting devices by using a slotted CSMA-CA mechanism, which is described in section 3.2.2. But CFP also has guaranteed time slots (GTSs) and they appear at the end of the active superframe, starting at a slot boundary immediately following the CAP. For the GTSs, the PAN coordinator allocates up to seven GTSs, as they

can occupy more than one slot period. [12]

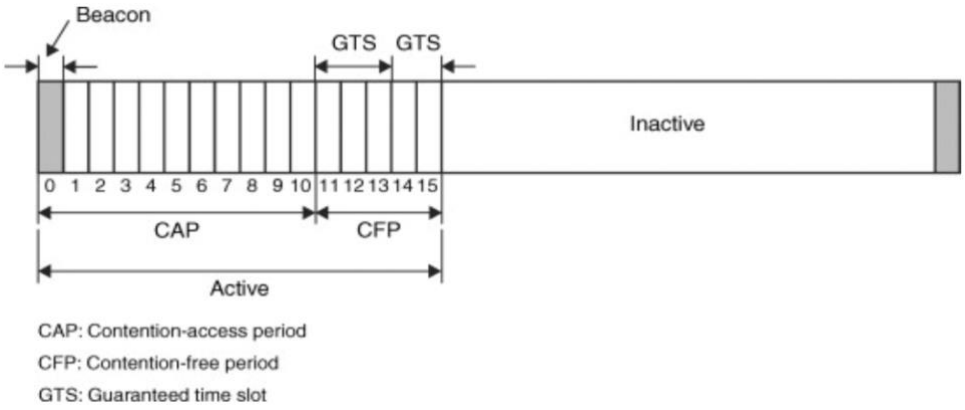


Figure 3.4. Superframe structure [19]

3.2.2 Carrier Sense Multiple Access with Collision Avoidance (CSMA-CA) Algorithm

In the MAC layer, there is CSMA/CA network protocol for carrier transmission. Unlike Carrier Sense Multiple Access/Collision Detection (CSMA/CD) which deals with collisions after their occurrence, CSMA/CA attempts to prevent collisions prior to their occurrence. The algorithm of the CSMA/CA is as follows:

(i) At first when a frame is ready, the transmitting station checks whether the channel is idle or busy.

(ii) If the channel is busy, the transmitting station wait for the channel becomes idle. So, if the channel is idle, the station waits for an Inter-frame gap (IFG) amount of time and then sends the frame.

(iii) After the frame is sent, it sets a timer.

(iv) After frame being sent, the receiver has to send an acknowledgement and the station waits for that. So, if the station receives the acknowledgement before expiration of the timer, it is a successful transmission.

(v) But if the time is expired before an acknowledgement is received, then it waits for a back-off time-period and restarts the algorithm. [20]

A general CSMA/CA algorithm is shown below,

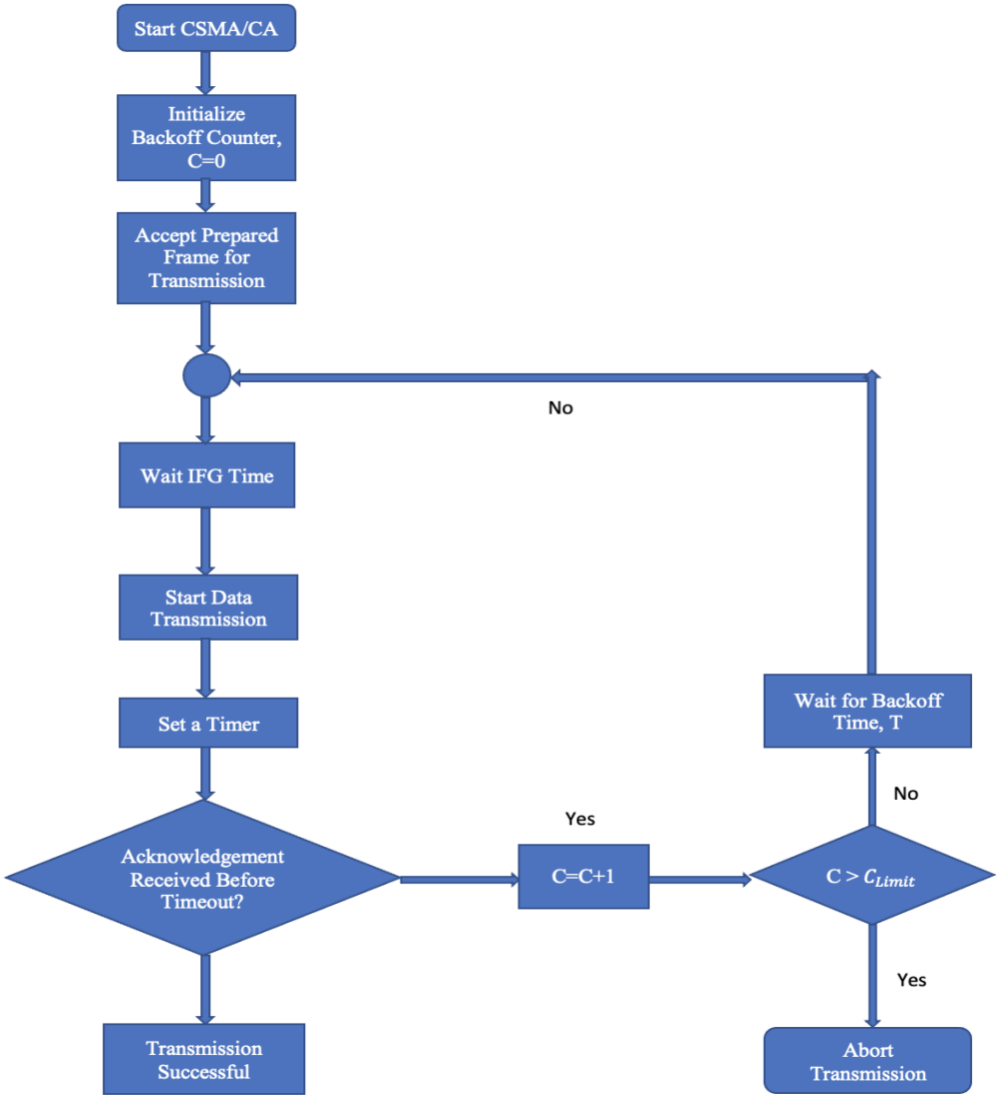


Figure 3.5. The CSMA-CA Algorithm [20]

3.2.3 MAC Frame Formats

The general MAC frame consists of the following basic components:

(i) A MAC header, which comprises frame control, duration, sequence number, address information and optionally, traffic category information.

(ii) A MAC payload of variable length contains information specific to the frame type. Acknowledgement frames do not contain a payload.

(iii) A fixed length header check sequence (HCS) contains the cyclic redundancy code (CRC) parity bits for the frame header. That also includes the PHY header and the MAC header.

(iv) A variable length frame body contains information specific to the frame type and subtype.

(v) A frame check sequence (FCS) contains an IEEE 32-bit cyclic redundancy code (CRC). [21]

octets: 2	2	1	1	2	2	2	2	0-2030	4
Frame Control	PNID	Destination Address (DA)	Source Address (SA)	Stream ID	Sequence Number	Duration	HCS	Frame Body	FCS
MAC Header									

Figure 3.6. MAC frame format [21]

3.3 Network Layer

Network layer interfaces between application layer and MAC Layer. In the network layer, routing and formation of the network is done. Routing is the process of selection of the optimal path to relay the messages to the destination node. Routing is done by special network devices called routers. A router is always configured with some default route. But if there are multiple paths existing to reach the same destination, the router can make decisions based on hop count, bandwidth, prefix-length, delay, and various other metrics. [22]. Because of these decisions, the network involves joining and leaving of nodes, maintaining routing tables (coordinator/router), actual routing and address allocation. This layer provides network-wide security so that the authenticity and confidentiality of a transmission can be maintained and allows low power devices to maximize their battery life. [18] As described earlier in Section 2.4, there are three network topologies considered in IEEE802.15.4.

A coordinator does an energy scan to find the best RF channel for its new network before establishing a ZigBee network. After the channel has been chosen, the coordinator assigns the logical network identifier, known as the PAN ID, and this ID will be applied to all devices that join the network. The PAN ID is a 16-bit number that is used as a network identifier. A device can join any network, or it can limit itself to a network with a particular PAN ID. ZigBee PRO defines an extended PAN ID which is a 64-bit number.

A node can join the network either in two ways, directly or through association, as

described below,

- For the node to join the network directly, a node's extended address must be added into the neighbor's table of a device. The direct joining device will issue a scan, and thus the node with the matching extended address (in its neighbor's table) will respond and in this way, they will be able to join.

- For the node to join by association, a node sends out a beacon request on a channel and repeats the same beacon request on other channels until it finds an acceptable network to join. The network layer provides security for the network, ensuring both authenticity and confidentiality of a transmission. [23]

3.4 Application Layer

The application layer is the highest layer in the ZigBee protocol stack. There are three sub layers which are described below:

3.4.1 The Application Objects (APO)

The application objects (APO) are a piece of software that controls and manages protocol layers and the hardware. Each application object is allocated with unique end point number and other APO's can use that number as an extension to the network device address to interact with it. A ZigBee application must conform to an existing application profile and

that must be accepted by the ZigBee Alliance. Message formats and protocols are defined by an application profile for interactions between application objects. The application profile framework allows different vendors to independently build and sell ZigBee devices, so that they can interoperate with each other in each application profile. There can be up to 240 application objects in a single ZigBee device.

3.4.2 ZigBee Device Object

ZigBee Device Object discovers nodes and binds nodes to resources and applications and binds devices with the channel. The ZigBee device object addresses three main operations, 1. service discovery, 2. security, and 3. binding. The discovery is mainly to find nodes and determine the MAC address of the coordinator/router by using unicast messages. Also, it facilitates the procedure for locating some services through their profile identifiers. Thus, profile plays a very important role. Also, ZigBee device object provides security services by authenticating the required keys for data encryption. The network manager is implemented in the coordinator. It selects an existing PAN to interconnect, and it supports the creation of new PANs. The binding manager role is to bind nodes to recourses and applications, and also to bind devices to channels.

3.4.3 Application Support Sub Layer

The Application Support (APS) sub layer is an interface between the network and the application layers which is through a general set of services provided by APS data and

management entities. This sub layer securely transmits & receives the frames and establishes and manages the cryptographic keys by processing outgoing and incoming frames. APS sub layer is issued primitives by the upper layers to use its services. It provides entity authentication and gives updates about the device. Additional services include Establish Key, Transport Key, Update Device, Remove Device, Request Key, Switch Key, Entity Authentication, and Permissions Configuration Table. [18]

4. LITERATURE REVIEW

There are many researchers who have focused on the transmission reliability, efficiency, and collision avoidance for a ZigBee system. One of the major reliability issues for communication in WSNs is access control, where collisions of multiple packets can cause the packets to be unreadable. Mantri et al. have proposed a Schedule based Collision Avoidance (SCA) algorithm for reliability using a fusion of CSMA/CD (Carrier-Sense Multiple Access with Collision Detection) and TDMA (Time Division Multiple Access) techniques. Mainly for avoiding collisions in multiple hopping, this fusion of CSMA and TDMA proposed activity-based sleep/wake up scheduling. As a result, it improves packet delivery ratio by 69.13% in multi hop tree networks along with a 30% reduction in energy consumption. In this way network lifetime is improved in sensor networks. [24] Also, they used the multi-path data propagation for collision avoidance.

Other researchers and authors have tried to address the issue of packet collisions within the context of WSN. They examined how a high number of collisions can lead to congestion in WSN. In their paper, Yaakob et al. use a Contention Window (CW) as an integration technique for avoiding major packet collisions. Along with this technique they have incorporated optimization of packet size in the WSN system for ensuring successful transmission. By experimenting, they have observed that large packets are more susceptible to error and corruption unlike small packet size which can be more favorable in high BER scenarios. Also, these results show significant performance improvement over the existing IEEE 802.15.4 protocol. The incorporation of packet size into distributed collision control

demonstrates effective deployment in real time and delay sensitive applications in WSN. [25]

The key features of smart home applications are easy installation, low cost, and low power consumption. These characteristics nicely match with ZigBee features which will fulfill the networking requirements in smart homes. Seneviratne and Lueng have proposed a Chaotic Parameter Modulation scheme along with Direct Sequence Spread Spectrum (DSSS) at the physical layer for implementing the spread spectrum communication [26]. In their paper, they have implemented a MATLAB/Simulink simulator to improve the physical layer to coincide with Wi-Fi, Bluetooth etc. and evaluated the whole system with a Simulink ZigBee transmitter. The scheme was robust and highly desirable in the physical layer of ZigBee in smart home environments.

ZigBee networks can experience interference problems because of co-channel interference (CCI) with other wireless communication systems (for example, Bluetooth and Wi-Fi). Zhang et al. aim at overcoming this problem by using a Least Mean Square (LMS) adaptive filter in the receiver. Their paper mainly analyzed BER results & simulated CCI and proposed putting an adaptive channel equalizer at the receiver. Thus, it will reduce the CCI affecting the BER. They have analyzed and simulated their whole system in Simulink, using a bit error rate (BER) tool for analyzing the degree of impact of CCI. In their results, they have seen that it has reduced the impact of CCI along with reducing BER which improves the performance of the system. [27]

It is known that in general the transmission in wireless networks is more unreliable than the wired network environment. In addition to reliability, studies in wireless sensor networks often focus on broadcast efficiency. So, reliable data transmission is very important, and it is required in many applications. Sung et al. proposes the ZigBee Acknowledgement-based Reliable Broadcast (ZARB) data broadcast algorithm in wireless sensor networks. In this paper, authors proposed to achieve efficient data broadcast for which they described a hierarchical acknowledgement mechanism, reduction of rebroadcast packets and ACK packets, degree-based ACK/rebroadcast jitter, and parent-oriented retransmission as the key schemes. By using these schemes, the simulation results show that high reliable broadcast transmission can be attained, that broadcast efficiency is better maintained, and also, there was efficient reduction in the acknowledgement traffic as well as communication overhead. [28]

With the improvement of people's standard of life, networks for smart home systems are becoming more popular and there are complicated problems like cost and complex wiring. For these kinds of problems, Li et al. have designed a smart home system based on ZigBee and Wi-Fi. [29] In this system, the home's internal network is controlled through ZigBee by the terminal node and the remote control accesses the home's internal network through WIFI. For transmission information of the underlying sensor network, ZigBee is used and to ensure the stability of the system, a star connection structure is built in the system. The user can easily monitor and control the room by input control commands or query commands on the terminal device. The system mainly detects the data transmission quality and tests the reliability of the transmitted data. In this way, a smart home system is created

with low energy consumption that is easily deployable that is wirelessly connected and has lower cost.

However, there are still some challenges for designing ZigBee based home network systems like improving the integrated efficiency. To address these challenges, some researchers and authors proposed a stack structure node for home service integration. Because of the node, a user can quickly develop a coverage monitoring application integration of ZigBee technology. In this structure, data of the sensing nodes with adaptive Weighted Fusion Algorithm (AWF) processing is passed to a gateway and from gateway to packet processing and then reported to a monitoring center. In this way, it optimizes the data processing efficiency. A testbed for the proposed ZigBee system was created, and its experimental results show that the testbed is convenient enough to perform wireless network coverage and monitoring tasks, and each node can visually display its working state. Also, for evaluating the performing status of each node, linear interpolation theory is used. Thus, a highly efficient ZigBee network system is created for home service. [30]

For building and home automations ZigBee has gained increasing acceptance. Bunyai and Krammer analyze ZigBee's network size constraints in reference [31]. They have done OMNeT++ simulation which checks ZigBee's performance. To estimate the capabilities and limits of the ZigBee network system, a regular and easy to analyze network structure is used. By simulation, feasibility of the designed network is estimated. Further, by creating the presented regular structure performance of more complex structures can be estimated. Also, adapting and extending estimation can be done for more accurate results.

Cloud Computing is on-demand network access to resources like networks, applications, and servers. Researchers have done work accessing Cloud Manufacturing (CM) based on ZigBee and they have used an improved AODVir routing algorithm. [32] In the algorithm, cluster tree routing is used with hops of Route Request (RREQ) packets added to the algorithm. Then the performance optimization of the ZigBee system is done. Thus, the proposed algorithm improves the performance of ZigBee networks by using the application in resource accessing of CM. Lastly the original AODVjr algorithm and the improved AODVjr algorithm are simulated under the same environment parameters and their experimental results showed that the improved AODVjr algorithm provides better performance.

In many networks, two-way communication is very important too. So, reference [33] aims at constructing a Metering Infrastructure (AMI) LAN. In this structure researchers have chosen ZigBee as their communication protocol because of its features of reliability, safety, easy installation, and low cost. But in LAN, there can be situations like losing network connection and requiring additional time for network construction which reduce the reliability. So, in this paper, the authors suggested Fast Join Process (FJP) and enhanced FJP for shortening the time of re-construction since the proposed FJP doesn't waste any time by scanning unnecessary channels. Comparing between IEEE 802.15.4 and FJP or enhanced FJP, a lot of time can be saved by using FJP or enhanced FJP because i can respond to node association failures easily. So, this proposed method is more suitable for AMI. Furthermore, they discovered that the construction time and successful rate are still good when a large number of meters are connected to the network.

So, many researchers have developed different methods for enabling ZigBee systems to be more reliable, cost efficient and to overcome restrictions like collisions, energy wastage and security issues. For our research, we will focus on using multiple spreading codes to increase the system's efficiency and to reduce vulnerability to collisions. Such a system, which has been proposed in reference [3] is less complex than many of the systems mentioned above and can be more easily incorporated into the IEEE 802.15.4 standard with minimal changes. Unlike reference [3], we will evaluate the system using multiple hopping topology and we will show how to adapt the evaluation for variable length messages.

5. PROPOSED SOLUTION

With development of IoT networks, many promising new systems have been proposed. For our thesis, we plan to focus on improvements to greater range and longevity in ZigBee systems. As proposed in reference [3], we will incorporate multiple spreading codes. Our innovation is that, unlike reference [3], we will adapt the system to allow variable length messages and to incorporate multiple hop network topology (a two-hop tree). These adaptations, especially multiple hop topology, will enable flexibility and additional applications and also it will increase range and longevity.

5.1 Mathematical Methodology Adopted in Simulating Variable Message Length

Queuing theory and Poisson arrival process was used in the Reference [3] system to randomly transmit fixed-length messages in the system and calculate arrival time and end time of each message. We will employ queueing theory and the exponential distribution to produce variable length messages.

Queuing theory is a branch of mathematics that studies and models the act of waiting in lines. It is basically mathematics that studies how lines form, how they function, and why they malfunction. The origin of queuing theory can be traced to the early 20^{th} century in a study of the Copenhagen telephone exchange by Agner Krarup Erlang, a Danish engineer, statistician, and mathematician. He attempted to determine how many circuits were needed to provide an acceptable level of telephone service and for people not to be “on hold” (or

in a telephone queue) for too long. Also, he was very curious to find out how to process a given volume of calls and for that how many telephone operators were needed. [34]

His mathematical analysis culminated in his 1920 paper “Telephone Waiting Times”, which served as the foundation of applied queuing theory. [35] His work led to the Erlang theory, and the international unit of telephone traffic is called the Erlang in his honor. There is a very wide range of real-life applications of queuing theory, like providing faster customer service, increasing traffic flow, improving order shipments from a warehouse, or designing more efficient data networks, call centers, factories, hospitals, and offices.

A simple example of queuing theory can be given like in a movie theater. There are sometimes long waiting lines of people to purchase movie tickets and to eliminate the situation, the theatre owner would likely need to set up fifty to a hundred ticket booths. However, for the theater it will be very expensive to pay a hundred ticket sellers. Therefore, businesses use information gained from queuing theory in order to set up their operational functions, so that they can strike a balance between the cost of servicing customers and the inconvenience to customers caused by having to wait in line. [36]

A Poisson process is a simple and widely used stochastic process for modeling the times at which arrivals enter a system. This process is used in Reference [3] and in our system to model the generation of new messages. Basically, a Poisson process is the continuous-time version of the Bernoulli process. For this process, arrivals may occur at arbitrary positive times, and the probability of an arrival at any particular instant is 0. So, there is not a very

clean way of describing a Poisson process in terms of the probability of an arrival at any given instant but it is convenient for a Poisson process to be defined in terms of the sequence of interarrival times. [37]

In any given system the number of messages initiated over a particular interval of time is defined by Equation (5.1),

$$P\{n\ messages\ are\ initiated\ in\ the\ system\ during\ time\ interval\ T\} = \frac{(\lambda_{sys}T)^n}{n!} e^{-\lambda_{sys}T} \quad (5.1)$$

Where λ_{sys} is defined as the average number of messages arriving per second. Since the arrival of a message is modelled using the Poisson process, the message interarrival time is exponentially distributed as defined in Equation (5.2),

$$P\{time\ between\ initation\ of\ nth\ and\ n+1st\ calls \leq t\} = 1 - e^{-\lambda_{sys}T} \quad (5.2)$$

The message length is exponentially distributed as given by the following MATLAB Function exprnd. The exprnd function exponentially randomly generates numbers with a certain mean value m in the system.

$$Length\ of\ message = exprnd\ (m) \quad (5.3)$$

We typically used a value of 0.0064 seconds for the mean in exponential distribution,

corresponding to a message size of 200 data bits Also, we varied this mean value for verification of the message length generator in the system (see Appendix A).

Initially we assume that the message 0 arrives at time t=0 and it is defined as i=0 in our MATLAB Simulation. To simulate the time between the arrivals of message 0 and message 1, we start by generating a uniformly distributed random number R_1 between 0 and 1. The time between the arrival of message 0 and of message 1, t_1, is then determined by applying Equation (5.4) and the algebraic manipulation in Equation (5.5) to produce Equation (5.6),

$$P\{message\ 1\ arrives\ at\ or\ before\ time\ t_1\} = R_1 \tag{5.4}$$

$$R_1 = 1 - e^{-\lambda_{sys} t_1} \tag{5.5}$$

$$1 - R_1 = e^{-\lambda_{sys} t_1}$$

$$\ln (1 - R_1) = -\lambda_{sys}\ t_1$$

$$t_1 = \frac{-\ln (1-R_1)}{\lambda_{sys}} \tag{5.6}$$

Thus message 1 arrives at time t = 0 + t_1.

Similarly for message 2, another uniformly distributed random number R_2 is generated and the interarrival time between message 1 and message 2, t_2, is defined by Equation (5.7),

$$t_2 = \frac{-\ln(1-R_2)}{\lambda_{sys}} \tag{5.7}$$

So, from equation (5.7), the arrival time of message 2 is calculated as t = 0 + $t_1 + t_2$. Using these equations, the arrival time of each message in the system can be realistically simulated.

Once a message arrives in the system, it can be transmitted across the network in a slot within the next Zigbee superframe, provided it does not collide with another message. In a queuing system that models a ZigBee network of sensors, after messages have been successfully transmitted to their coordinators, these messages are out of the system.

The time at which a message leaves the system after it has been successfully transmitted is known as the end time of a message. The end time of a message is very simple to estimate as it is the sum of the arrival time and length of a message, as shown in Equation (5.8),

$$end\ time = arriavl\ time + message\ length \tag{5.8}$$

Equation (5.8) can be repeated to estimate the end time of all the messages in the system. So, by using Queuing theory and the Poisson message arrival process, we were able calculate the arrival time, end time and message length of each message in the simulation of the ZigBee system. All Equations in this section except (5.3) and adaptation of (5.6) and (5.7) for multi-hop systems were referenced from [3].

5.2 Probability of Successful Message Demodulation for a Message Involved in a Two-Message Collision

In the proposed system, each sensor uses one of eight different PN sequences, so even if two messages are transmitted at the same time, there is a nonzero probability that they can be successfully demodulated. Reference [3] determines the probability calculation of a successful message demodulation for a message involved in a two-message collision, by considering a ZigBee network system implemented using the 2.4 GHz, O-QPSK (Offset Quadrature Phase Shift Keying) modulation system.

The simulation models an O-QPSK modulation system with a probability of bit error rate, $P_b = 10^{-5}$. For an O-QPSK system, the probability of bit error rate is as given by Equation (5.9),

$$P_b = Q\sqrt{\frac{2E_b}{N_0}} \qquad (5.9)$$

Here, Q is the tail distribution function of the standard normal distribution and $\frac{E_b}{N_o}$ is the energy per bit to noise power spectral density ratio.

Using the value of $Pb = 10{-}5$ in the equation,

$$10^{-5} = Q\sqrt{\frac{2E_b}{N_0}}$$

$$Q\sqrt{\frac{2E_b}{N_0}} = 4.27$$

$$E_b = \left(\frac{4.27^2}{2}\right)N_o$$

$$\frac{E_b}{N_o} = 9.11645. \qquad (5.10)$$

Consider that the length of a message is 200 bits, including overhead. This is a relatively short message, but it's a reasonable length for sensors that transmit a given parameter such as pressure or temperature in real time.

Probability of a message with no error = $(1 - P_b)^{200}$

$$= (1 - 10^{-5})^{200}$$

Probability of a message with no error = 0.99800 (5.11)

Then, for a 200-bit message with $\frac{E_b}{N_o} = 9.11645$, the error rate of the message is,

Probability of a message with error = (1- 0.99800)

= 0.002 (5.12)

Therefore, from Equation (5.12), it can be said that even when there is no collision there is still a 0.2% probability of a message being received in error.

In the current system if two messages collide, both messages will be destroyed in the two-message collision. But, for the new proposed system with different PN codes, there is a

significant probability that one or both messages can still be recovered. Let G_p represent the system's processing gain (the number of different PN codes available). If a second message is transmitted at the same time along with the first message, with the same energy, and if the second message uses a different PN sequence, then after de-spreading only $\frac{1}{G_p}$ of second message's energy will interfere with the first message. Both the current ZigBee system and new proposed system use a fixed processing gain of 8. Thus, for a two-message collision where the messages use different PN spreading sequences, after de-spreading,

$$\frac{E_b}{N_0} = \frac{9.11645}{1+\frac{1}{8}(9.11645)} = 4.2609 \tag{5.13}$$

and

$$P_b = Q\left(\sqrt{2X4.2609}\right) = Q(2.9192) = 0.0018 \tag{5.14}$$

Note that the probability of two messages using different PN sequences is $\frac{7}{8}$. Thus, for a message length of 200-bits,

$$P_{current\ system} = (message\ destroyed|two\ messages\ collided) = 1 \tag{5.15}$$

$$P_{new\ system} = (message\ destroyed|two\ messages\ collided)$$

$$= \frac{1}{8}(1) + \frac{7}{8}[1 - (1 - 0.0018)^{200}]$$

$$P_{new\ system} = (message\ destroyed|two\ messages\ collided) = \quad 0.389731 \tag{5.16}$$

$$P_{success,new\ system} = (message\ successful|two\ messages\ collided)$$

$$= (1 - 0.389731) = 0.61026 \quad (5.17)$$

From the above equations and calculations, it can be said that the probability of a message being destroyed in a two-message collision is significantly less if the sensors are allowed to choose one of 8 PN codes rather than having all sensors use the same PN code. All the equations from (5.9) to (5.17) were referenced from [3]. Due to the relatively small processing gains used in the proposed system, collisions involving three or more messages were assumed to destroy all messages.

5.3 Multiple Hopping Network Topology Incorporated in ZigBee System

At present there are various systems like reference [3] that have used single hopping, but there are vast applications of wireless sensor networks for which system requirements could change significantly and multiple hopping topology will work better. In single hopping, nodes only contact with the coordinator but can't communicate with each other. So, range must be restricted or it requires a lot of power to transmit messages.

With multiple hopping, the system will be able to set up a hierarchy with a coordinator (or base station), a limited number of routers, and a large number of sensors. Some of the sensors will communicate directly with the coordinator, others will communicate with a router. So, by using multiple hopping, the system will save a lot of power. Saving power means longer battery life for ZigBee. Also, collisions can be avoided. There will be fewer

collisions in the system because different nodes are using different paths to transmit messages. The capacity of the ZigBee system will be increased.

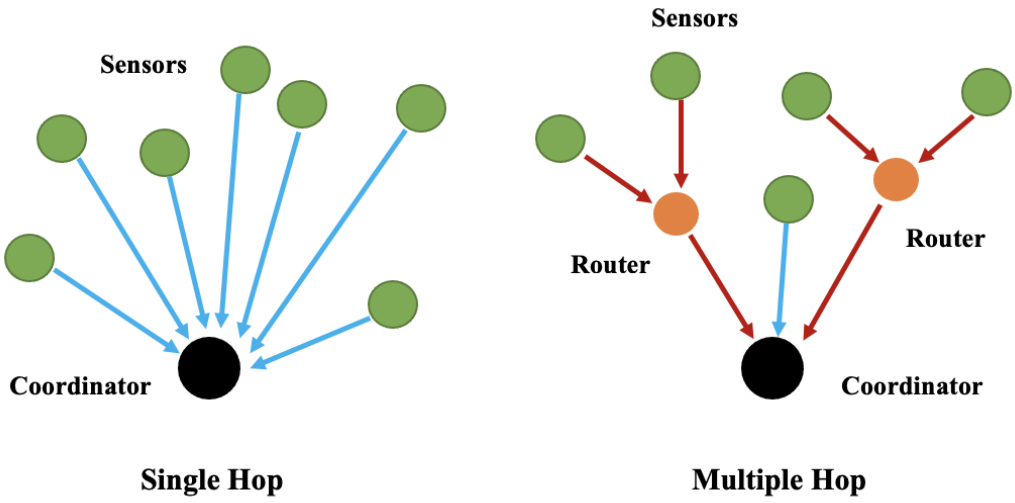


Figure 5.1. Single Hop vs Multiple Hops in Communication Networks [38]

One of the most important issues in wireless sensor networks is an energy efficient communication protocol and for this there is no significant precedent in wireless network history. The ratio between the energy needed for transmitting and for processing a bit of information is usually assumed to be large. So, designing the communication protocols should be according to the criterion of energy efficiency.

In the present ZigBee single hop system, the range can be extended by increasing transmitted power. But we don't want to increase the transmitted power in our applications. So, we are proposing a tree topology instead of a star topology and using multi-hop to extend the range of our sensor network. In Figure 5.1, the difference between single hop and multiple hop can be seen. In multiple hop there are routers and sensors. The routers

communicate both with sensors that are close to it but far away from the coordinator, and with the coordinator. The messages hop from the far-off sensors to the router and from the router to the coordinator. So, there are two hops in the system instead of a single hop. By using the router, we can extend the range of the ZigBee system without increasing the power. In this way, by using multiple hops, the ZigBee system has extended range and saves power.

For our application, we will model a static network with sensors distributed roughly uniformly through a region. The system will allow two hops, which can increase the system's range by 40.7% relative to a single hop system without increasing the transmitted power (and thereby shortening the life) of the sensors. Since the system is static, it will employ a tree network topology with the coordinator centered in the region and with four routers that are each assigned a series of far-off sensors. Figure 5-2 shows this topology. For this thesis, we assume that communication is unidirectional (although ZigBee allows bidirectional) with the sensors updating their information often enough that in the case of a message being destroyed by collision, the coordinator waits for the next update from the sensor rather than requesting retransmission.

There are a large variety of applications of Zigbee in the real world like environmental and medical monitoring, health care, positioning and tracking, logistic and localization, and so on. For many of these applications most dominant requirement is energy efficiency as nodes basically have limited power supply or are battery powered. [38] So, our multiple hop ZigBee system would be more efficient than a single hop system for these kinds of

applications. Because, in our system we have extended the range of the system without increasing the power and thus power is saved & also the capacity of the system is increased.

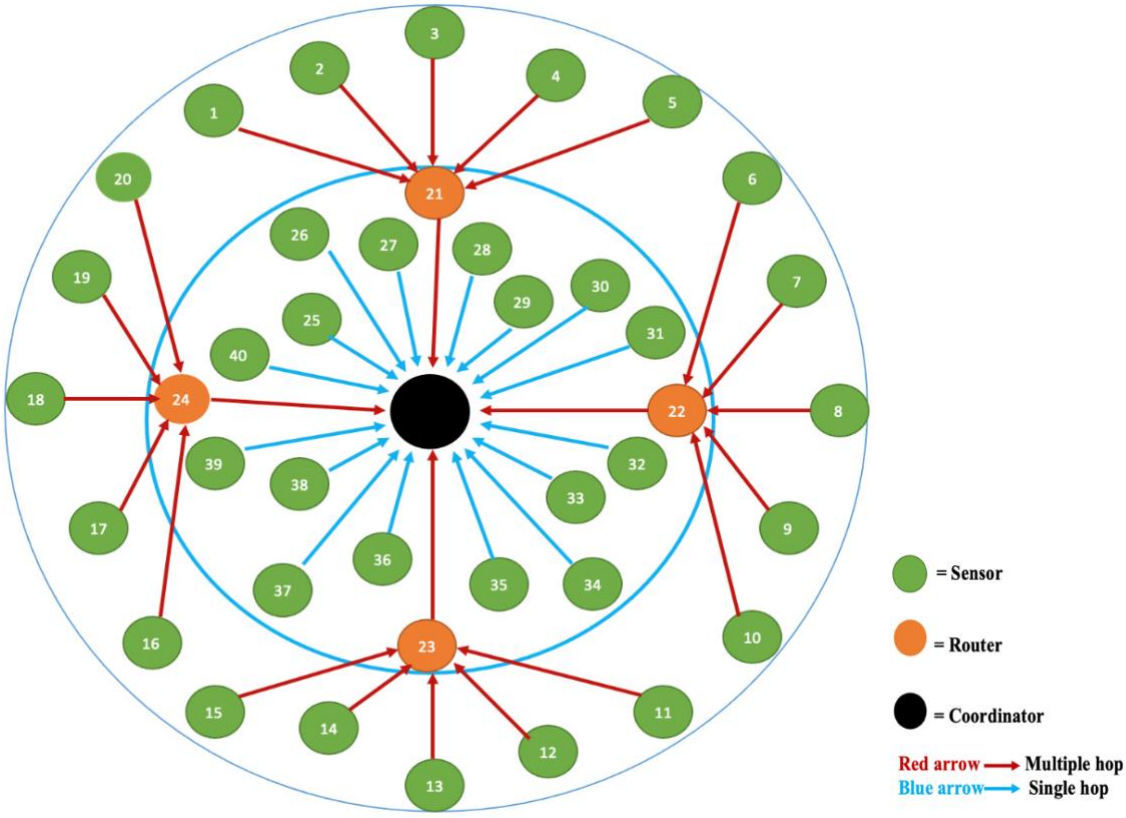


Figure 5.2. Our New Proposed Multiple Hop ZigBee Network

In our simulation, there are total a total of 40 sensors in the new proposed system (although, as we shall show later, the total system traffic is a far more important parameter for system performance than the number of sensors). At first each transmitting message is randomly associated with a sensor in the system, making sure no two messages transmitting over the same time interval are associated with the same sensor. We accomplish this by checking if no two messages transmitting at the same time are associated with the same sensor. If they are not, then associate that sensor with the message otherwise associate those messages

with a sensor that is available, and it does not overlap with another transmitting message. There are four routers in the system, which are collocated with sensors numbered 21, 22, 23 and 24 and are within the range of the coordinator. We can see from figure 5.2, each router is connected to five sensors which are in the outer circle and these sensors 1-20 are out of range from the coordinator. In our system, router 21 is wirelessly connected to sensors 1-5, router 22 connected to sensors 6-10, router 23 connected to sensors 11-15 and router 24 connected to sensors 15-20. Before messages hop from sensor 1-20 to routers 21-24, the sensor checks if its assigned router is busy or not. If router is not busy, then messages are transmitted to the router from the assigned sensors or else if router is busy, then messages wait for 100 msec and then again check before transmission. Then messages transmit from the routers to the coordinator. Thus, through two hops messages are transmitted in the system. The remaining sensors 25-40 transmit messages directly to the coordinator in single hop as those sensors are in the range of the coordinator.

In our new multiple hop system, through two hops we have increased the range of the system compared to the system in Reference [3]. A single-hop ZigBee system, such as described in Reference [3] can be enlarged, but for that in the system every sensor has to transmit with very high level so that messages could reach the coordinator. Because of this, system will need more power & thus the sensors longevity will be reduced. So, we have created a multiple hop system where sensors 21-40 which are closer to the coordinator can transmit messages at lower power level to the coordinator. Also, sensors 1-20, which are not in the range of the coordinator, use routers 21-24 to transmit to the coordinator. In this way, we have expanded our range and longevity without having to spend more power.

So, we hope to find advantages from our proposed method in terms of reliability and security, throughput, range, and the operating life of the ZigBee system. This method will also reduce the collisions of simultaneous ZigBee signals; thus, it will make ZigBee more efficient. Evaluation with variable message length and multiple hop network topologies will be significant for an environment for greater applications and it will bring more customers. So, with the design of a high-performance ZigBee wireless communication network, it will have broad application space in real life.

5.4 MATLAB Simulation

We developed simulations for our new proposed ZigBee multiple hop system in MATLAB. The steps in the MATLAB simulation for implementing our new ZigBee system are described in the following:

1) At first, we set values for Lambda (Total message arrival rate per second), N (Number of messages initiated over time-period), Frame size, CAP slots and Number of sensors.

2) Then, we have a set of 8 possible PN tables in the system and each sensor in our system randomly selects one of the PN table numbers which then modulates and spreads the message before transmission. Here, each sensor is randomly associated with each message and any multiple messages which transmit over same time interval are associated with different sensors.

3) For the superframe size, we initially considered the length of each message as 200 bits, which corresponds to 6.4 msec per message after applying PN spreading code. So, superframe size is set to 0.125sec at first. In the chapter 3, it was mentioned that a superframe has two periods which are (i) active period and (ii) inactive period with CAP slots and only in active period message transmission is done. We changed the superframe size according to message length so that we can maintain a constant ratio between active and inactive period.

4) For our system, we have initially considered 16 CAP slots per superframe and each message is randomly associated with CAP slots. The CAP slots number is adjustable in the simulation.

5) We use a fixed message length in the simulation, but to demonstrate how to adapt the simulation to variable message length we have exponentially randomly generated a variable message length with a specified mean in the line 38 of our MATLAB code.

6) We have plotted a histogram for our length generator to verify its correct operation and added 40 bins to get a smoother histogram plot. The histograms are shown in Appendix A.

7) Then we ran simulations to calculate the total number of messages that are involved in a message collision, meaning the simulation identifies messages which are transmitting within the same superframe using the same CAP slot number. In the current system

these messages that are involved in collisions are considered destroyed. These values are calculated to know the destroyed message rate in the current system.

8) We generated a random number for each message between 0 and 1 for estimation of total number of messages destroyed in two message collisions. This random number value generated for each message involved in a two-message collision was compared with the value that was determined for the probability of a message in a two-message collision to be successfully demodulated in section 5.2 earlier.

9) If the generated random number for a message is less than or equal to the value determined for the probability of a message in a two-message collision to be successfully demodulated, then that message was not destroyed. It means that the receiver system was successful in demodulating that message involved in that collision and the message was successfully transmitted.

10) But if the random number generated for a message involved in a two-message collision was greater than the estimated value for the probability of a message in a two-message collision to be successfully demodulated, then that message was destroyed. It means that the receiver system was unsuccessful in demodulating that message.

11) In this way, we can estimate the total number of messages which were involved in a two-message collision. Also, we can calculate the total number of messages which get destroyed as well as the total number of messages which can be successfully

transmitted using the proposed solution.

12) We have considered 40 sensors in our proposed ZigBee system which we can see from figure 5.2. There are four routers out of these forty sensors. These four routers are connected as the following,

- Sensor numbers 1,2,3,4,5 (outer circle) = 21 sensor number (inner circle)
- Sensor numbers 6,7,8,9,10 (outer circle) = 22 sensor number (inner circle)
- Sensor numbers 11,12,13,14,15 (outer circle) = 23 sensor number (inner circle)
- Sensor numbers 16,17,18,19,20 (outer circle) = 24 sensor number (inner circle)

So, sensor numbers 21, 22, 23 & 24 are the routers. Messages hop from 1-20 sensors to 21-24 routers and then hop from the routers 21-24 to the coordinator. There are two hops for transmission of these messages. Also, the sensor numbers 25-40 transmit the messages to the coordinator directly by one hop.

13) We have added a 100 msec delay before each of the four routers and this delay will be activated only if incoming messages see that the routers are still transmitting other messages; meaning routers are busy.

14) If the routers are free, this 100 msec delay will not be activated and the messages will be transmitted normally.

15) If after 100 msec delay, the router is still busy, then the system will show at capacity

for that message and it will be considered destroyed.

16) In the proposed ZigBee network both transmission and reception cannot happen at the same time. So, it will always operate in half duplex mode. As shown in Appendix B, the codes for 100 msec delay are in lines 113, 142, 169 and 196 of the code. This thesis will suggest evaluation of a full duplex system as a possible area of future work.

17) We have calculated initial arrival time and initial end time along with final arrival time and final end time for each message in the system.

18) For single hop we calculated that, initial arrival time = final arrival time and initial end time = final end time.

19) We found out which messages transmit through single hop and which messages transmit through multiple hops by comparing initial end time and final end time for each message. If initial end time is the same as final end time, then the message was transmitted through a single hop and if the initial end time is different than final end time, then the message was transmitted through multiple hops. Also, we calculated total number of messages associated with single hop and double hop.

20) We found out initial sensor number and final sensor number for each message.

- Initial sensor numbers 1,2,3,4,5 = 21 final sensor (router) number
- Initial sensor numbers 6,7,8,9,10 = 22 final sensor (router) number

- Initial sensor numbers 11,12,13,14,15 = 23 final sensor (router) number
- Initial sensor numbers 16,17,18,19,20 = 24 final sensor (router) number

21) We also calculated which and how many messages are at system capacity. For the messages at capacity, there are no collisions occurring for that message as they will not be transmitted by the sensors. So, we considered three or more collided, two collided and destroyed from two collided to be zero for that message.

22) We calculated total successfully transmitted messages by equation below, total successfully transmitted messages = total number of messages - (number of messages at capacity + three or more collided + messages destroyed by two collided + total number of messages destroyed in single hop).

23) The output parameters for the whole system can be seen from output2_op on line 294.

24) We calculated the frame number of each message using the equation below,

frame = floor (final_endtime / frame_size) +1

25) We analyzed our system for verification of the message length generator by using histogram which produces an exponential probability density function with the appropriate mean.

26) Also, we have incorporated the destroyed message length in single hop from Reference

[3] into our system and evaluated our system.

27) We ran multiple simulations for different values of message lengths, lambda values and CAP slots and compared success rates of current multiple hopping ZigBee system to our new ZigBee multiple hopping system.

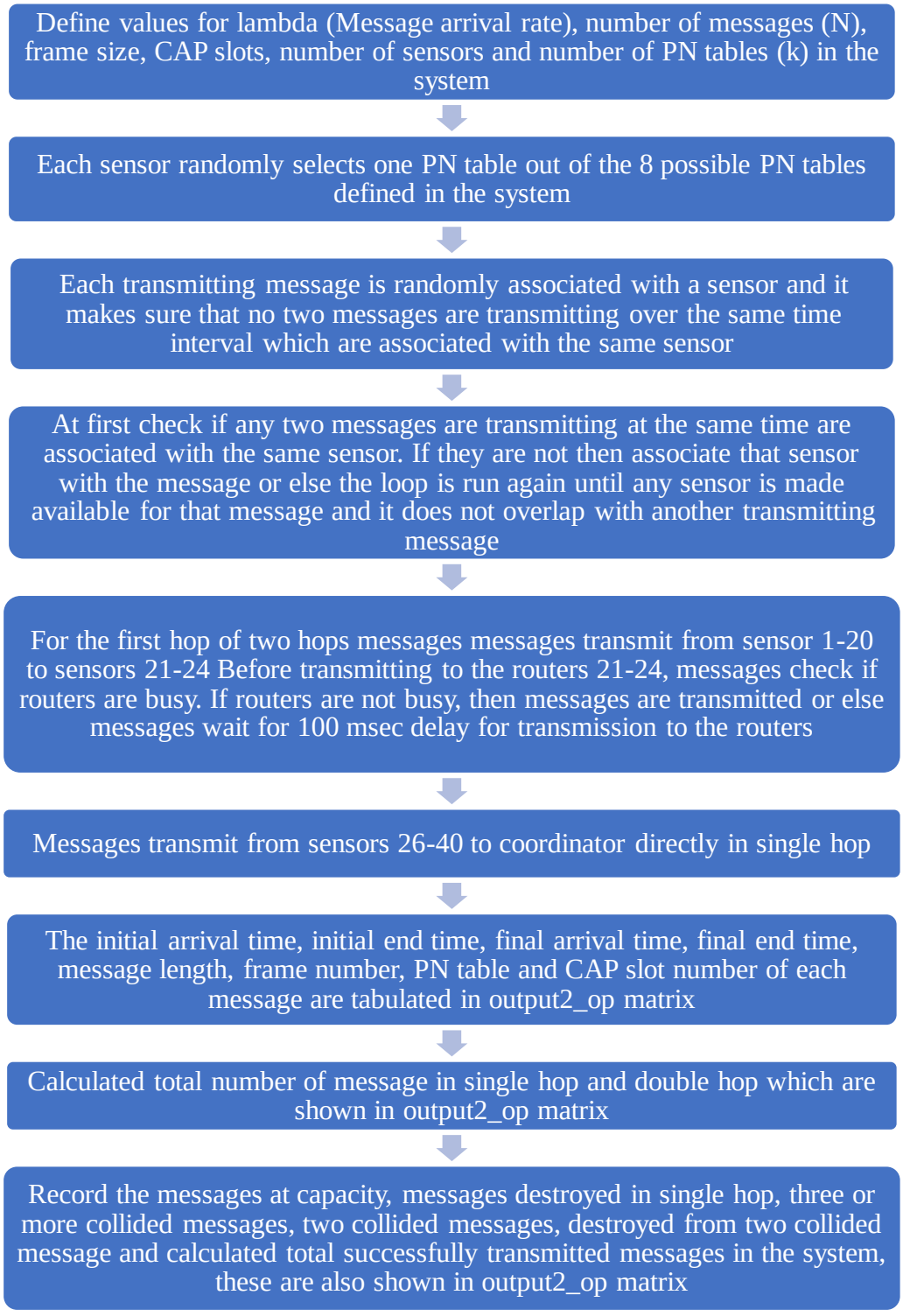
These are the steps of the MATLAB simulation of our new proposed system. From the results, it was seen that there was a significant increase in successful messages transmission rate in our proposed ZigBee system compared with the current ZigBee system. That's because large number of messages were saved which were involved in two message collisions in our new proposed system because of using 8 different PN sequences. But for the current system which uses the same PN sequence for each message, all the messages were destroyed which were involved in two message collision.

So, our system is more efficient in terms of managing collisions and also increases the range and longevity. We have evaluated our new proposed system and compared it to the current system by varying lambda, message length and number of CAP slots in chapter 6, Results Analysis.

5.5 Flowchart of the Proposed Solution

We have developed MATLAB simulation for our proposed new multiple hop ZigBee network and also, we described the steps for our proposed system in the earlier 5.4 section,

MATLAB simulation. In this section we have done a flowchart describing the steps. A flowchart of our new proposed ZigBee system is shown below,



6. RESULTS ANALYSIS

In earlier chapters, we discussed how our new ZigBee system with multiple hops supports extended range and larger networks than the ZigBee system proposed in Reference [3]. Our new system has a larger network without using higher power and because of saving significant power, our proposed system has greater longevity than the system proposed in Reference [3]. Also, compared to the current ZigBee system our new system will experience significantly fewer message collisions. Since, in case the of two-message collisions, our new system uses 8 different PN sequences compared to the current system which uses only one PN sequence, so a large number of messages are saved from two message collisions and successfully transmitted in our new system whereas in current system all the messages that were involved in two message collision are destroyed. This means our new system's capacity is higher as it successfully transmits more messages over a given period of time than the current system. So, our new system has lot of advantages over the current system. We have developed simulations for our new system in MATLAB and we discussed the simulation steps in the previous chapter.

We have used 40 sensors for our MATLAB simulation as described in the proposed system in sections 5.3 and 5.4. But we have analyzed the whole system with 20 sensors and with 40 sensors, and we saw that by comparing these two with the same amount of total message traffic (lambda), the success rates are almost same. So, the number of sensors, by itself, doesn't make a difference in the system as long as there are a sufficient number of sensors for the probabilistic model to be accurate. We designed the whole new proposed ZigBee

network with 40 sensors where all the sensors are uniformly distributed throughout the range of the system. So, for the simulation and result analysis we have used our designed new ZigBee network with 40 sensors.

In this chapter, we have run simulations for message generator verification of our new system and discussed how we used the simulation in Reference [3] to determine the percentage of multi-hop messages that were destroyed in their first hop. Also, we ran multiple simulations for our multi-hop system with different message lengths, different lambda values (system message arrival rate) and different number of CAP slots. Then we analyzed and compared the success rates of both our new ZigBee system and the current Zigbee system. All the results and analysis are described in this chapter.

6.1 Determining Percentage of Multi-Hop Messages That Were Destroyed in Their First Hop

We have considered that with multi-hop messages, there will be cases where the first hop of a multi-hop message i.e., messages from sensors 1-20 to routers 21, 22, 23 & 24 will collide at the router with a message from another sensor. For example, considering figure 6.1 and the red circle around router 21, there are sensors 1, 2, 3, 4 & 5 that are transmitting to router 21 and sensors 25, 26, 27, 28, 29, 30 and 31 are within the range of the router but are transmitting to the coordinator (Center black circle). Suppose sensor 1 and sensor 25 transmit at the same time. The message from sensor 25 successfully arrives at the coordinator because the message from sensor 1 is too far away from the coordinator to

interfere, but both the message from sensor 25 and the message from sensor 1 collide at the router 21. So, there's a possibility that the router can't read the message from sensor 1.

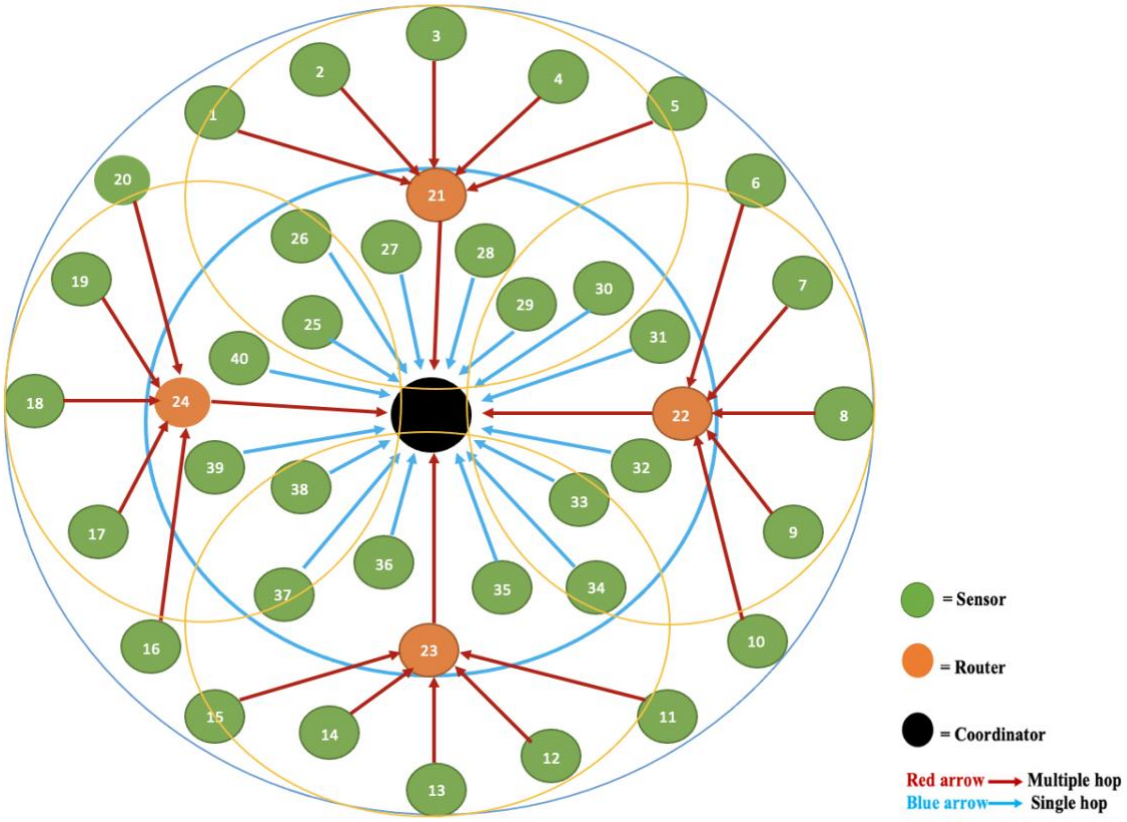


Figure 6.1. Our Proposed ZigBee System

Now, suppose the original no-hop simulation from Reference [3] is run from the viewpoint of router 21, using 12 sensors, meaning sensors 1, 2, 3, 4, 5, 21, 25, 26, 27, 28, 29 & 30. We have found out around 10%, 14% and 18% of the total messages are destroyed for 200 bits, 300 bits and 400 bits consecutively which includes all three message collisions and two message collisions that can't be resolved by the PN codes. We represented these as destroyed messages in the first hop in our new proposed ZigBee system.

6.2 Analyzing Our New Multiple Hop System vs Current Multiple Hop System by Varying Message Length

In this section, we compared success rate of our new multiple hop system (with 8 PN codes) and the current multiple hop system (which has one PN code for all sensors) by varying message length with fixed lambda (system message arrival rate per second). At first, for a fixed lambda value of 25 and different message lengths from 200, 250, 300, 350 and 400 bits, we ran simulations and generated a data set of success rate for both of our new system and current system. Further we also ran simulations and created data sets by varying messages sizes for different lambda values equal to 50, 75 and 100. Lambda=100 represents a very high level of network traffic, approximately 0.64 Erlangs on a single channel for message lengths of 200 bits, and 1.28 Erlangs for 400-bit messages. All simulations were run with N (total number of messages) = 20,000.

For calculating the success rate of the current multiple hop system, we used the following equation, success rate of current system = total number of messages – (number of messages at capacity + three or more collided messages + two collided messages + total number of messages destroyed in single hop). All the messages which were involved in three or more message collisions and two message collisions are destroyed in the current multiple hop system.

Then for calculating the success rate of our new multiple hop system, we used the following equation, success rate of current system = total number of messages – (number of messages

at capacity + three or more collided messages + messages destroyed from two collided messages + total number of messages destroyed in single hop). Same as the current system, all the messages which were involved in three or more message collisions are also destroyed in our new multiple hop system. But not all the messages which were involved in two message collisions are destroyed in our new proposed system because of using different PN sequences. The current system uses the same PN sequence for each message, but our new system uses 8 different PN sequences and that's why a large number of messages got saved from two message collisions. So, for calculation of success rate of our new system, we only subtract the messages that were destroyed in two message collision from total number of messages.

From all the generated data in the tables below, we can verify that our new multiple hop ZigBee system has a higher success rate than the current multiple hop ZigBee system. From the tables, we can see that with increasing message lengths for fixed lambda values, success rate decreases for both systems but our system's success rate is always significantly higher than the current system. Our proposed multiple hop system performance shows much more stability than the current multiple hop system.

Also, our new system has higher range and capacity than the Reference [3] system. So, there are more advantages in our system. From the data set, we have also created graphical plots for each table. The result shows stability and performance improvements of our system over the current system. The data set tables and their graphical plots are shown in the following.

6.2.1 Results for Different Message Lengths with N = 20000, Lambda (Message Arrival Rate Per Second) = 25 and Number of CAP Slots = 16

Table 6.1. Data table for variable lengths with fixed lambda value=25

Message Length	Success Rate of Current Multiple Hop System	Success Rate of Our New Multiple Hop System
200	0.7993	0.9181
250	0.7679	0.8908
300	0.7427	0.8783
350	0.7080	0.8598
400	0.6802	0.8399

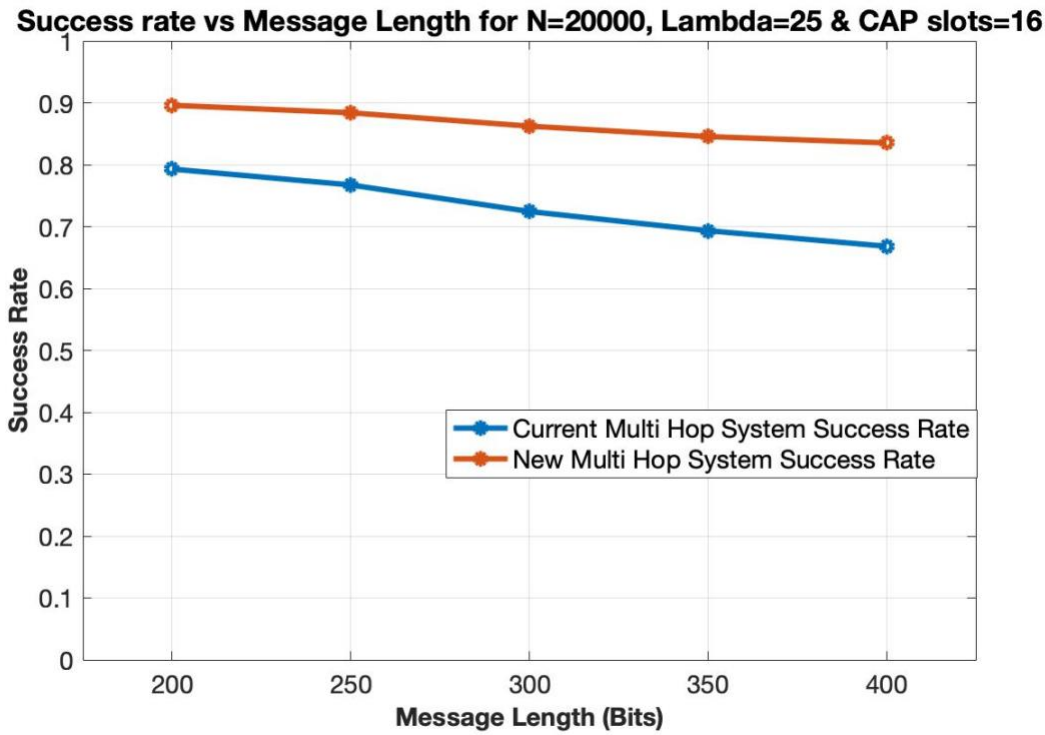


Figure 6.2. Success rate vs message length (Bits) graph for lambda=25

From this graph it can be seen that, for both systems as the message length increases from 200 bits to 400 bits in a fixed lambda 25, their success rates are decreasing. Also, by comparing the results, it can be seen that the difference in success rates between our new multiple hop system and current multiple hop system becomes larger. For 200 bits, difference in their performance is around 11% and for message length 400 bits, their performance difference is almost 16% which is even larger. So, the difference in success rates becomes larger as the message lengths get longer between our new system and current system.

6.2.2 Results for Different Message Lengths with N = 20000, Lambda (Message Arrival Rate Per Second) = 50 and Number of CAP Slots = 16

Table 6.2. Data table for variable lengths with fixed lambda value=50

Message Length	**Success Rate of Current Multiple Hop System**	**Success Rate of Our New Multiple Hop System**
200	0.6543	0.8210
250	0.6031	0.7802
300	0.5623	0.7474
350	0.5219	0.7171
400	0.4967	0.6883

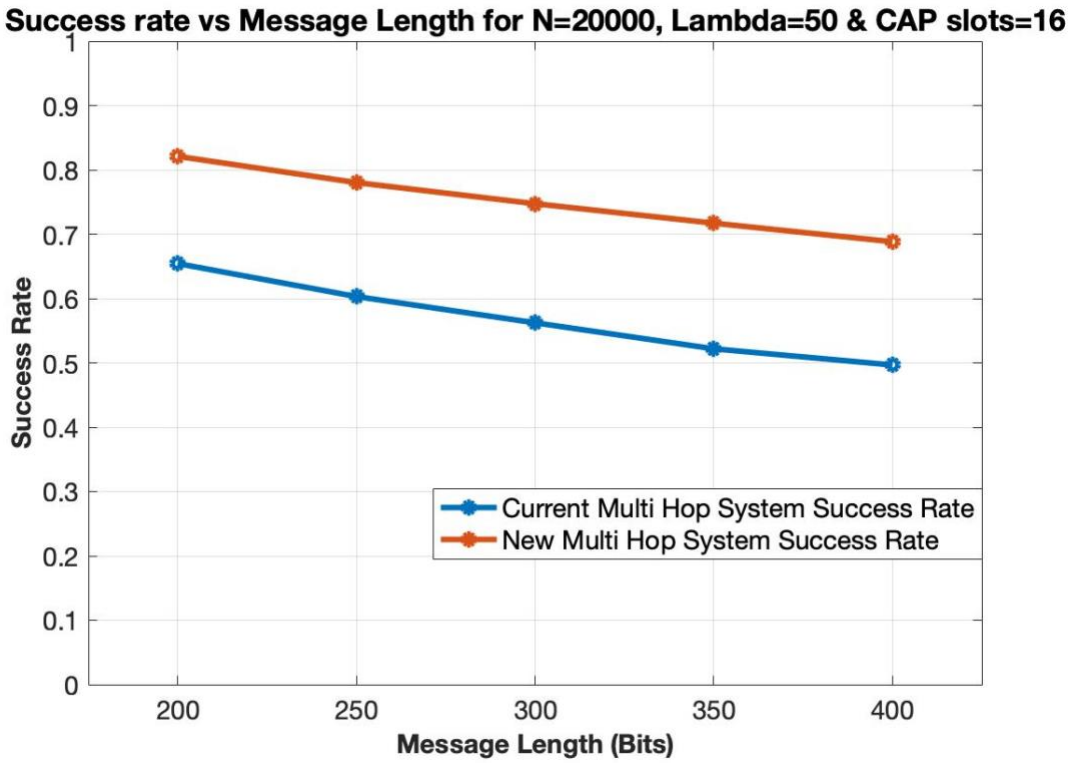


Figure 6.3. Success rate vs message length (Bits) graph for lambda=50

Here, for fixed lambda value 50 both systems performance decreases relative to the performance shown in the earlier section 6.2.1 with fixed lambda 25. For 200 bits, current system has success rate of 65.43% and our new proposed system success rate of 82.10% which is higher. Also, our proposed system's performance is higher than the current system for message length of 250, 300 and 350. Then lastly, for message length 400 bits, current system success rate is around 49.67 and our new proposed system success rate is around 68.83% which is also significantly higher. So, difference in success rates gets larger. These results mean our system is showing higher performance that the current system. Also, from the graph, we can see that our proposed system shows more stability than the current system.

6.2.3 Results for Different Message Lengths with N = 20000, Lambda (Message Arrival Rate Per Second) = 75 and Number of CAP Slots = 16

Table 6.3. Data table for variable lengths with fixed lambda value=75

Message Length	Success Rate of Current Multiple Hop System	Success Rate of Our New Multiple Hop System
200	0.5501	0.7379
250	0.5021	0.6918
300	0.4649	0.6486
350	0.4165	0.5947
400	0.3923	0.5654

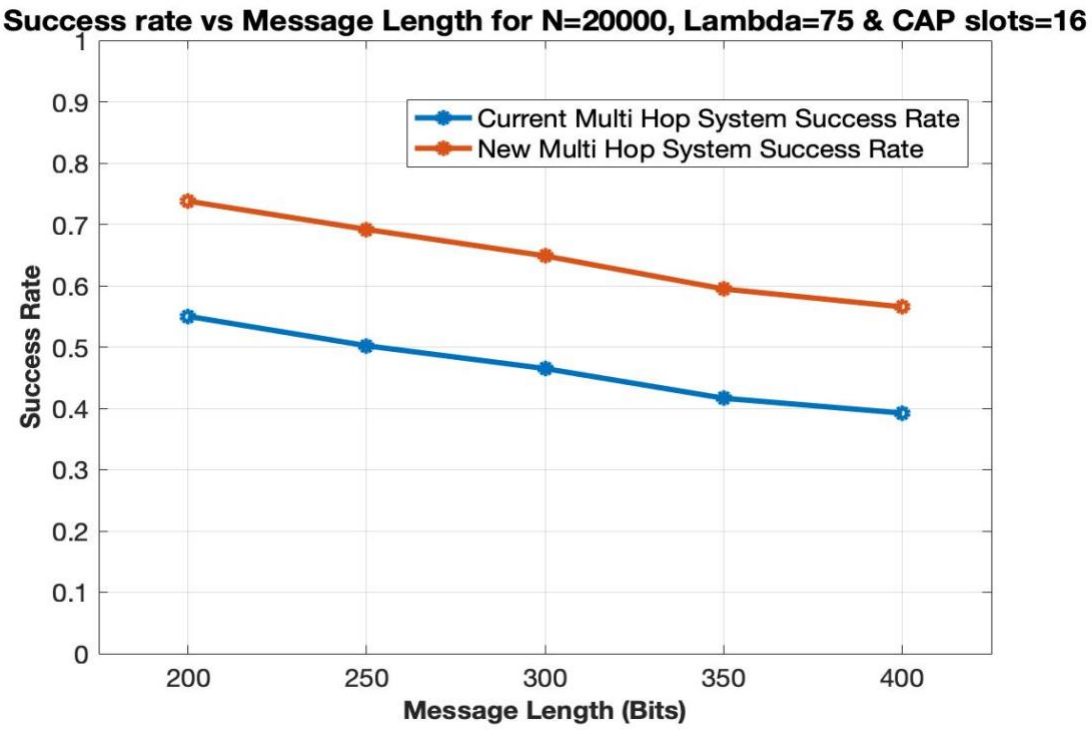


Figure 6.4. Success rate vs message length (Bits) graph for lambda=75

For fixed lambda value 75 by varying length, both system's performance got even worse than the earlier sections with lambda value 25 and 50. Message length increasing from 200 bits to 400 bits, the success rate of our new system is around 56.54% and the current system success rate is 39.23%, which is very poor. It means the current system was almost not able to function. But our system was still stable with 56.54% success rate.

6.2.4 Results for Different Message Lengths with N = 20000, Lambda (Message Arrival Rate Per Second) = 100 and Number of CAP Slots = 16

Table 6.4. Data table for variable lengths with fixed lambda value=100

Message Length	**Success Rate of Current Multiple Hop System**	**Success Rate of Our New Multiple Hop System**
200	0.4659	0.6538
250	0.4146	0.6018
300	0.3752	0.5541
350	0.3264	0.4992
400	0.3053	0.4689

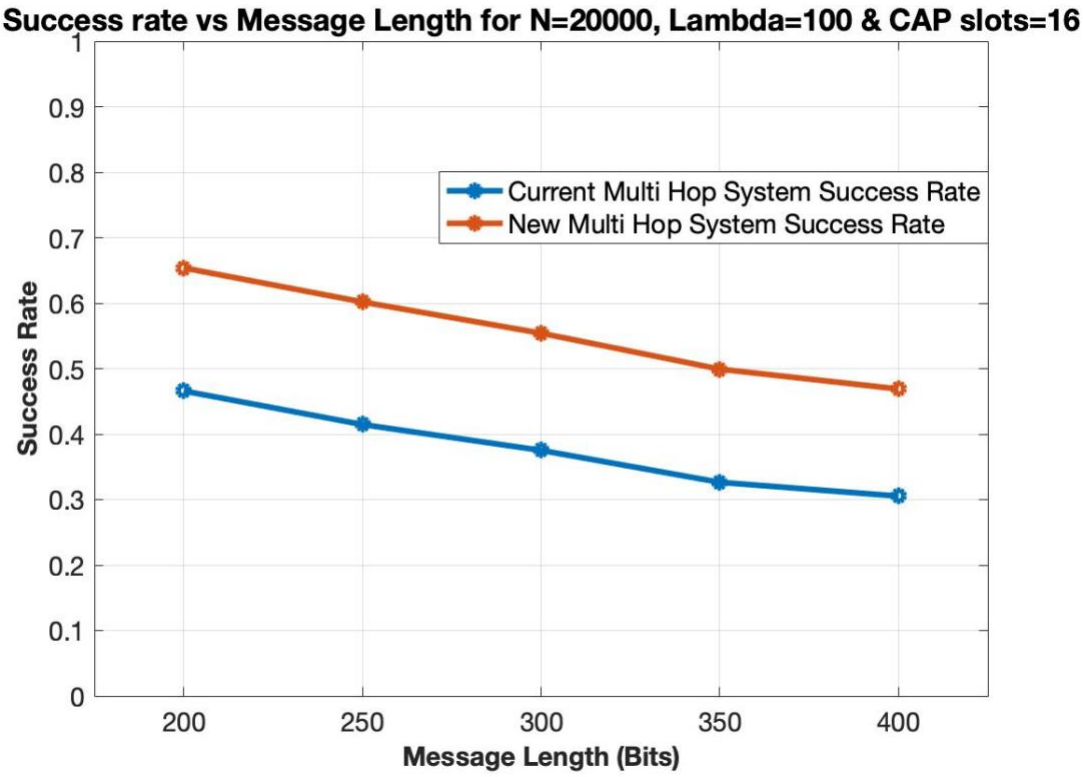


Figure 6.5. Success rate vs message length (Bits) graph for lambda=100

From this data table and graph, it can be seen that both systems are performing even worse than before. Increasing message lengths from 200 bits to 400 bits with fixed lambda values, the success rate of the current system and our new proposed system is around 30.53% and 46.89% consecutively. So, the performance of the current system shows very poor results. But by varying the message length with fixed lambda 100, our system is still showing stability with 46.89% success rate in this worst-case scenario. Again, note that Lambda=100 represents a very high level of network traffic, approximately 0.64 Erlangs on a single channel for message lengths of 200 bits, and 1.28 Erlangs for 400-bit messages. So, by varying the message length with fixed lambda values of 25, 50, 50 and 100, it can be seen that our new proposed multiple hop ZigBee system works much better than the

current ZigBee multiple hop system. The current system was almost shut down at the end of the results and its performance was not stable. But our system was much more stable and had a higher performance rate.

6.3 Analyzing Our New Multiple Hop System vs Current Multiple Hop System by Varying Lambda (Message Arrival Rate)

For this section, we varied lambda which is the message arrival rate with fixed message length for the comparison of success rate of our new multiple hop system and current multiple hop system. we calculated the success rates for both new and current systems like the previous sections. For simulations, we used different lambda values of 25, 50, 75 & 100 with fixed message length for 200 bits, 300 bits & 400 bits which are shown below,

6.3.1 Results for Different Lambda Values with N = 20000, Message Length = 200 Bits and Number of CAP Slots = 16

Table 6.5. Data table for variable lambda values with fixed message length=200 bits

Lambda	**Success Rate of Current Multiple Hop System**	**Success Rate of Our New Multiple Hop System**
25	0.8048	0.9029
50	0.6594	0.8179
75	0.5549	0.7416
100	0.4656	0.6647

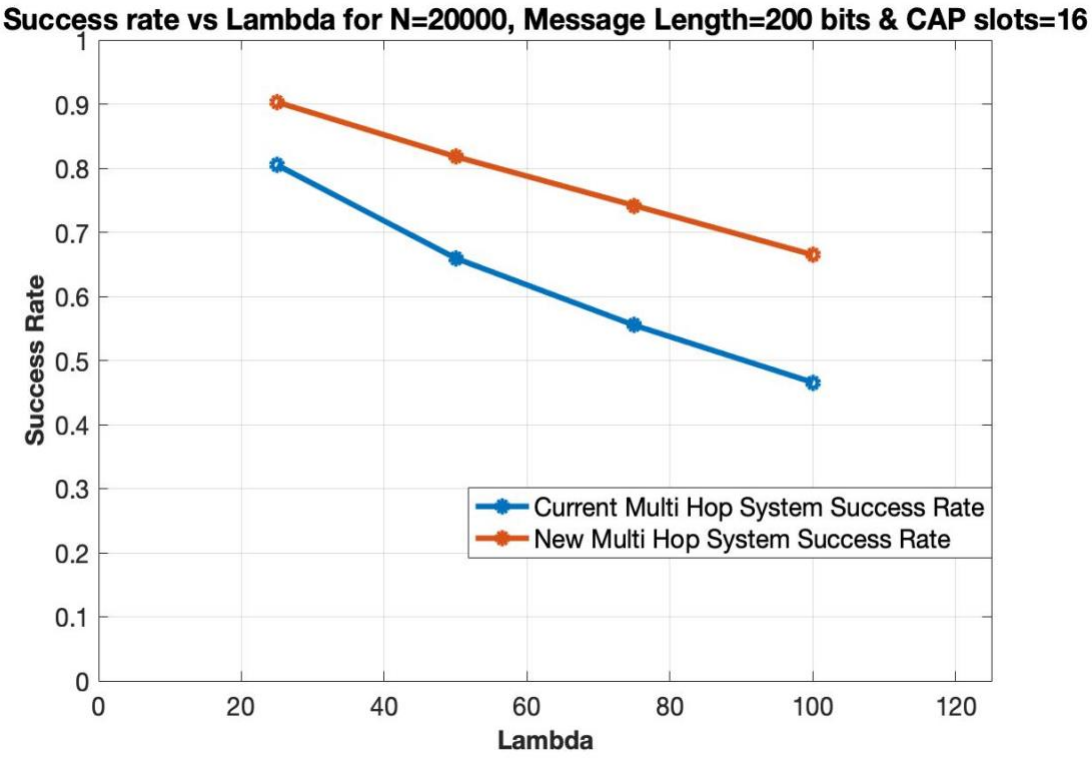


Figure 6.6. Success rate vs lambda graph for message length=200 bits

Here, by varying lambda values 25, 50, 75 & 100 with fixed message length 200 bits, there is decrease in success rates for both our new system and the current system. Also, their performance difference gets larger with increasing lambda values.

At first, for lambda value of 25, difference between our system and the current system is around 10%. Also, for lambda values of 50 & 75, both of the systems performance difference is around 15% & 18% consecutively. Lastly, with lambda value 100, their performance difference is 20%. So, the performance difference gets larger with increasing lambda value and our new system is showing much better performance even in this scenario.

6.3.2 Results for Different Lambda Values with N = 20000, Message Length = 300 Bits and Number of CAP Slots = 16

Table 6.6. Data table for variable lambda values with fixed message length=300 bits

Lambda	Success Rate of Current Multiple Hop System	Success Rate of Our New Multiple Hop System
25	0.7436	0.8780
50	0.5601	0.7555
75	0.4534	0.6454
100	0.3819	0.5482

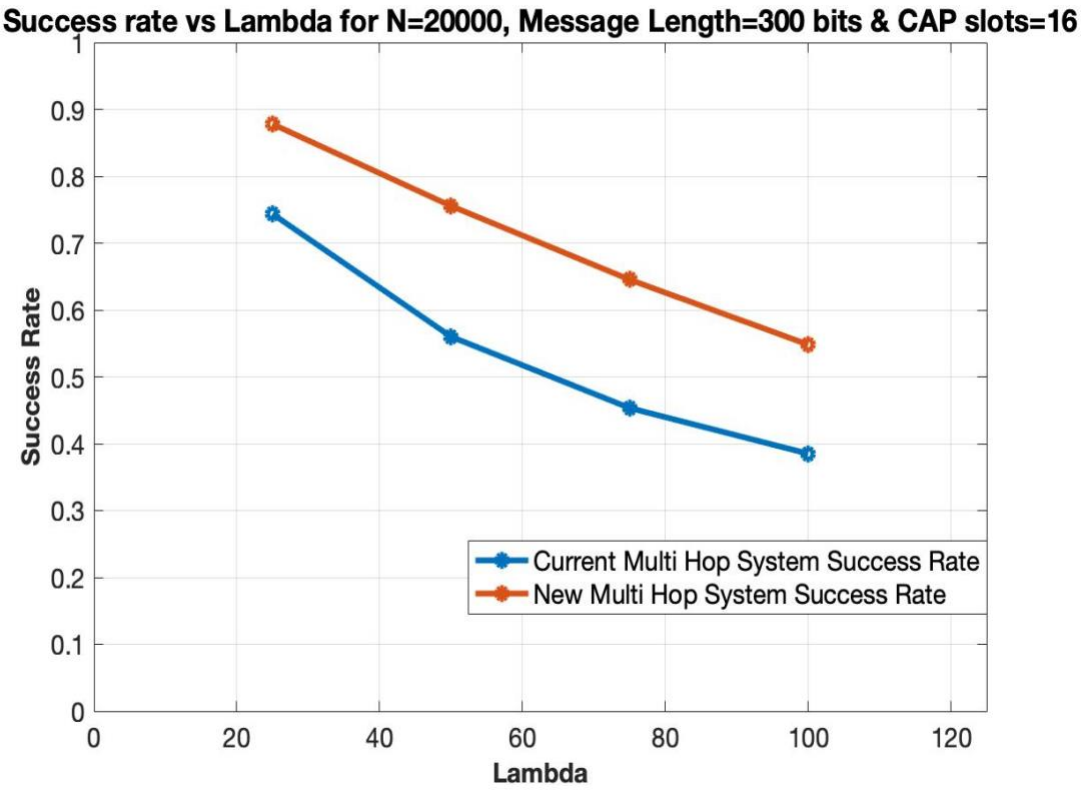


Figure 6.7. Success rate vs lambda graph for message length=300 bits

Like the earlier section, these results show even more performance difference between our new multiple hop ZigBee system and the current multiple hop ZigBee system. With lambda values from 25 to 100 with fixed message length 300 bits, difference between the success rate of our proposed system and the current system gets from 14% to 16% consecutively. Also, for 50 and 75 lambda values the current system performance shows significant decrease than the new proposed system. the So, our system is more stable than the current system even in this scenario.

6.3.3 Results for Different Lambda Values with N = 20000, Message Length = 400 Bits and Number of CAP Slots = 16

Table 6.7. Data table for variable lambda values with fixed message length=400 bits

Lambda	**Success Rate of Current Multiple Hop System**	**Success Rate of Our New Multiple Hop System**
25	0.6861	0.8393
50	0.4961	0.6852
75	0.3838	0.5681
100	0.3282	0.4628

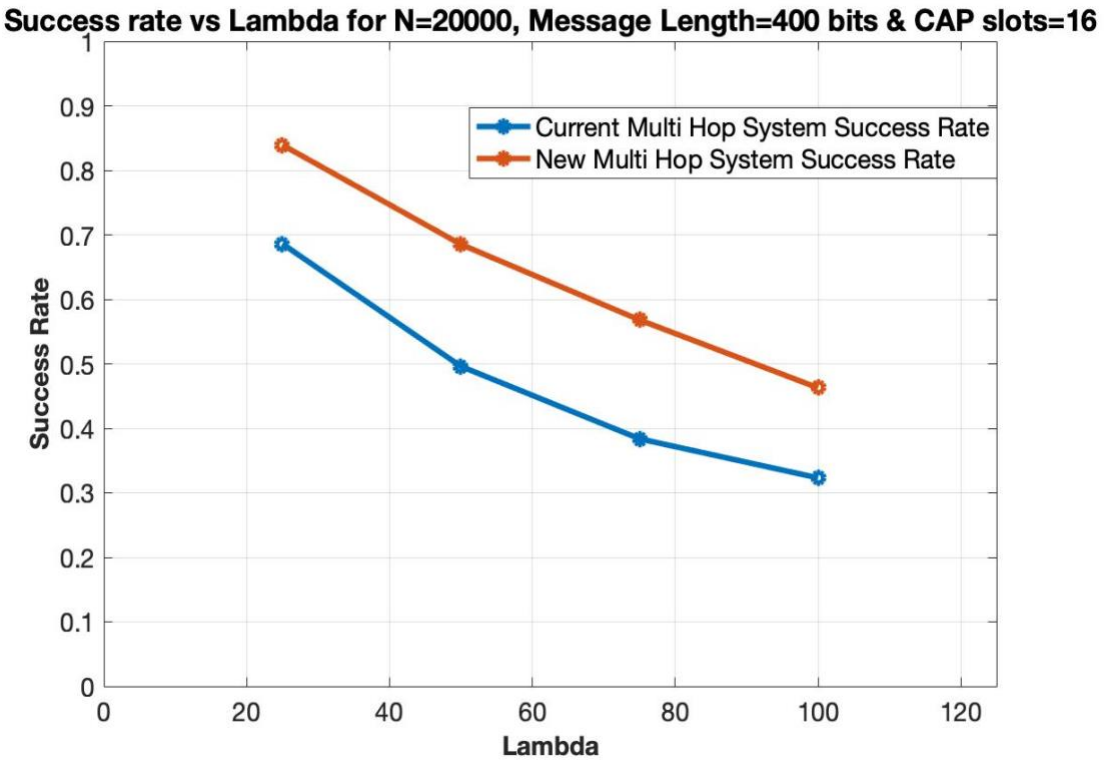


Figure 6.8. Success rate vs lambda graph for message length=400 bits

Here, with fixed message length 400 bits and by varying lambda values, the success rates got even worse than before. There is a much performance difference from 17% to 26% between our system and the current system. Even more so, with increasing lambda values, the current system success rate goes down to 32.82%. This means the current system almost goes down as the performance is so poor. But our new proposed system success rate was 46.28% which means that our system is still much more stable than the current system even in this worst-case scenario.

From these values from the tables, we can see that with increasing values of lambda from 25 to 100, the success rates decrease for both the current multiple hop ZigBee system and

our new multiple hop Zigbee system. But our new system has notably higher success rates than the current system. Also, differences between the two systems get larger by increasing lambda values with fixed message length in this section. Even for earlier section 6.2, with varying message length with fixed lambda value 25, the systems' performance difference is higher. So, for both sections 6.2 and 6.3, our new proposed system shows higher success rate and stability than the current system.

6.4 Analyzing Our New Multiple Hop System vs Current Multiple Hop System by Varying Number of CAP Slots

In this section, we evaluated the effects of varying the number of CAP slots (CAP size) for fixed message length. We varied the number of CAP slots values as 10, 12, 14 and 16 for fixed message lengths of 200 bits, 300 bits and 400 bits.

Like the earlier sections, we have calculated the success rates for both our new proposed system & the current system and compared them. So, we again ran simulations in MATLAB and from the data set, we have created the data tables & graphs. The results show consistent results and improvements for our proposed multiple hop ZigBee system over the current multiple hop system. Also, our new proposed multiple hop system performance shows much more stability and higher success rate than the current multiple hop system.

All the results and analysis are shown in the following subsections.

6.4.1 Results for Different Number of CAP Slots with N=20000, Message Length = 200 Bits and Lambda (Message Arrival Rate) = 100

Table 6.8. Data table for variable CAP size with fixed message length=200 bits

Number of CAP Slots	Success Rate of Current Multiple Hop System	Success Rate of Our New Multiple Hop System
10	0.3525	0.5016
12	0.3922	0.5682
14	0.4283	0.6249
16	0.4635	0.6636

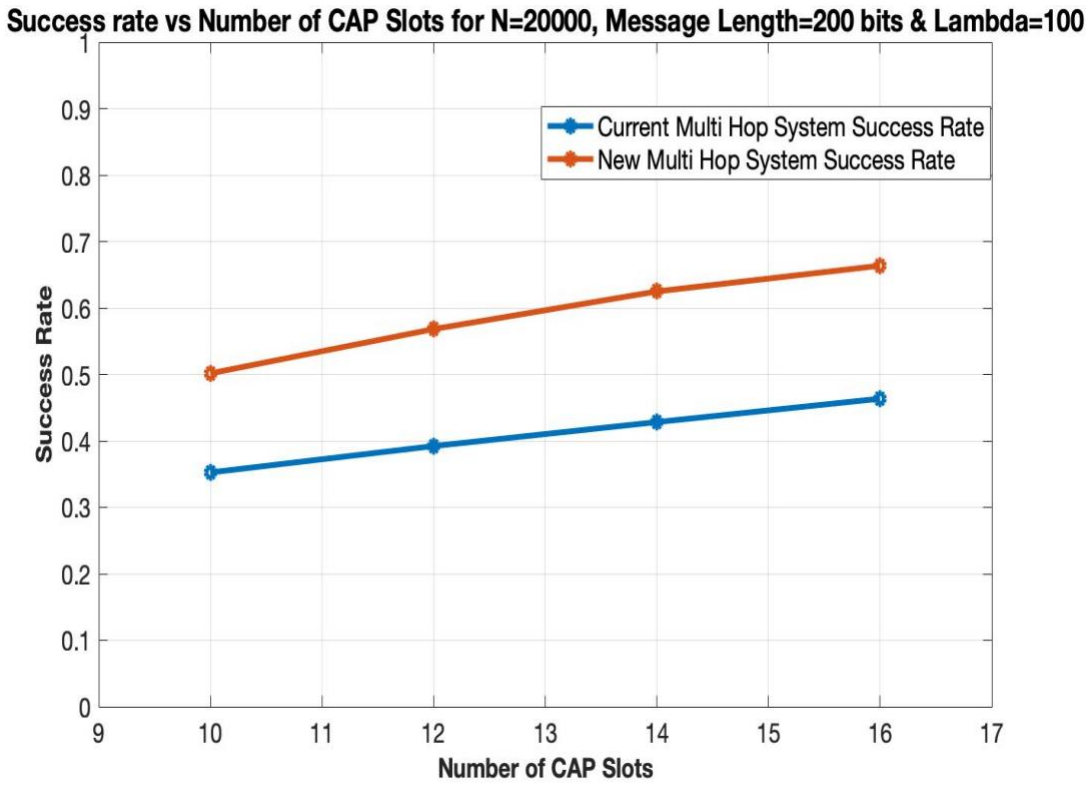


Figure 6.9. Success rate vs number of CAP slots for message length=200 bits

From this graph it can be seen that, for both systems as the number of CAP slots increases from 10 to 16 with fixed message length 200 bits, their success rates are increasing. Also, by comparing the results, it can be seen that initially for 10 CAP slots, the current system success rate is almost 35.25% which is really poor and for this our proposed system's success rate was 50.16%, which shows stability. Then after increasing number CAP slots to 12, 14 and 16, lastly in the data we can see that for 16 CAP slots, the success rate of our proposed system and the current system are 66.36% and 46.35% consecutively. This shows around 20% performance improvement for our new proposed multiple hop system over the current multiple hop system.

6.4.2 Results for Different Number of CAP Slots with N = 20000, Message Length = 300 Bits and Lambda (Message Arrival Rate) = 100

Table 6.9. Data table for variable CAP size with fixed message length=300 bits

Number of CAP Slots	**Success Rate of Current Multiple Hop System**	**Success Rate of Our New Multiple Hop System**
10	0.3066	0.3888
12	0.3270	0.4447
14	0.3552	0.5065
16	0.3805	0.5459

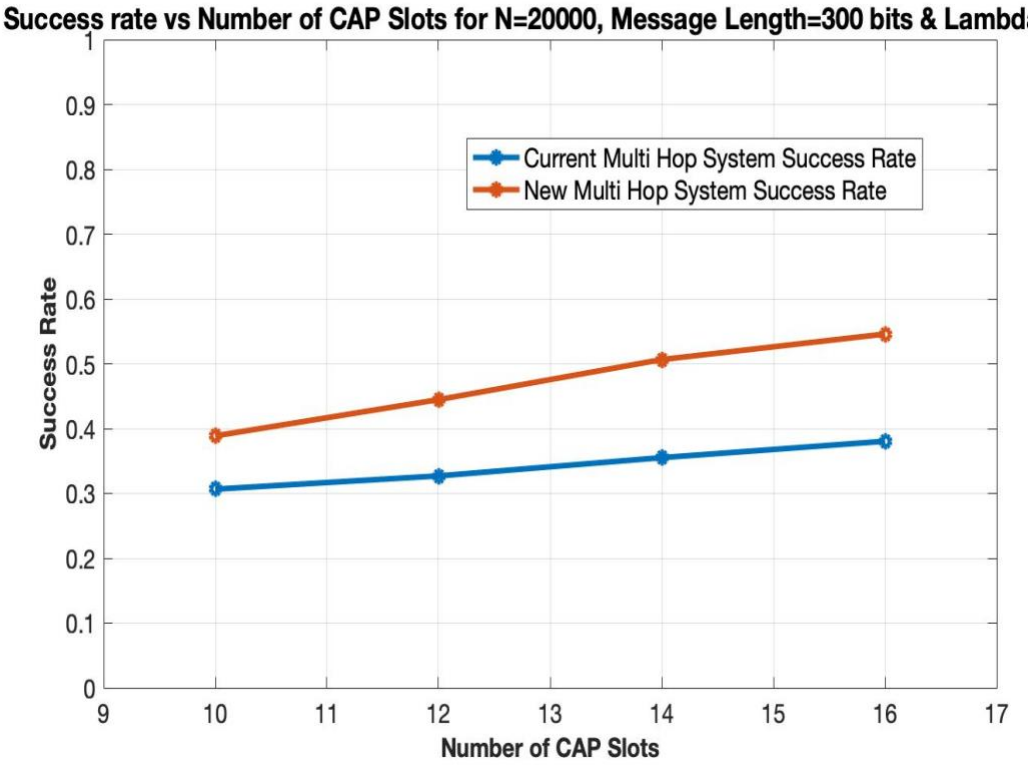


Figure 6.10. Success rate vs number of CAP slots for message length=300 bits

For fixed message length of 300 bits by varying number of CAP slots, both systems performance got even worse than the earlier sections. Initially for 10 CAP slots, the success rate of our new system is around 38.88% and the current system success rate is 30.66%, which is very poor. Their performance difference is around 8%. But for 16 CAP slots, both our new proposed system and the current system performance difference is around 16%.

So, in this section our new proposed system shows significant improvement over the current system. Also, for all the results our proposed system shows much more stability than the current system.

6.4.3 Results for Different Number of CAP Slots with N = 20000, Message Length = 400 Bits and Lambda (Message Arrival Rate) = 100

Table 6.10. Data table for variable CAP size with fixed message length=400 bits

Number of CAP Slots	Success Rate of Current Multiple Hop System	Success Rate of Our New Multiple Hop System
10	0.2976	0.3207
12	0.3031	0.3686
14	0.3143	0.4204
16	0.3404	0.4582

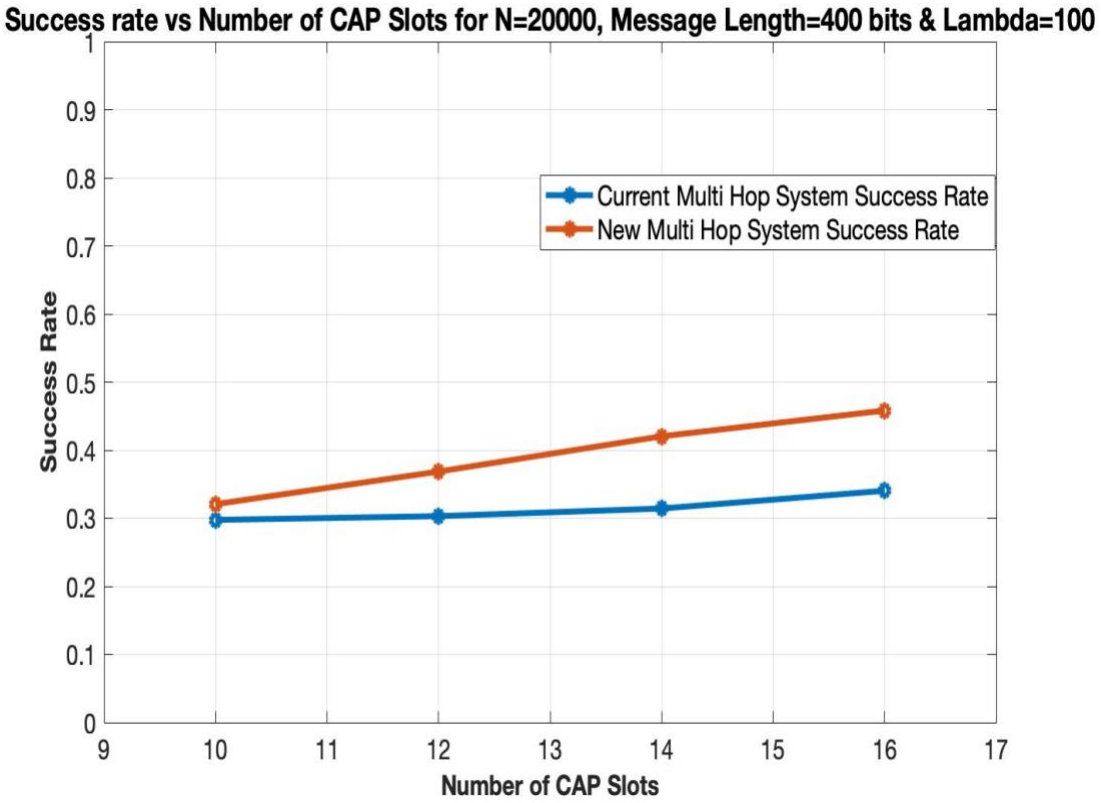


Figure 6.11. Success rate vs number of CAP slots for message length=400 bits

From this data table and graph, it can be seen that both systems are performing even worse than before after setting fixed message length to 400 bits. Initially for 10 CAP slots, the success rate of the current system is around 29.76% and the new system success rate is 32.07%. So, for the current system success rate, it means that the system is virtually really poor. But for 16 CAP slots, difference between the current system and our new proposed system is around 11%. Our system shows stability and much higher success rate than the current system even in this very-worst-case scenario. So, our new proposed system shows significant improvement over the current system.

Here, by varying the number of CAP slots 10, 12, 14 and 16 with fixed message lengths of 200 bits, 300 bits and 400 bits, it can be seen that our new proposed multiple hop ZigBee system works much better than the current ZigBee multiple hop system. The current system was almost shut down at the end of the results and its performance was not stable. But our system was much more stable and had a higher performance rate.

So, we know that our system has more range without having to spend more power. Because of saving power, our system will have longevity. In all 6.2, 6.3 and 6.4 sections, by varying message lengths, lambda values and number of CAP slots, the results again show significant improvements and stability for our new ZigBee system over the current ZigBee system for all cases.

7. CONCLUSIONS

Zigbee is a wireless technology developed as an open global standard to address the unique needs of low-cost, low-power, and reliable wireless IoT networks. In recent years it has been used in many intelligent applications, many control and monitoring systems like home and office automation, medical monitoring, industrial automation, low power sensors, HVAC systems and wireless remote control. But, as discussed in our thesis, in current ZigBee systems, many messages experience collisions when two or more ZigBee devices are trying to transmit at the same time. Also, there is lot of power usage when trying to increase the range of the system and thus battery life decreases. In reference [3] Ms. Mohan Kumar proposed a system where all ZigBee transmitting devices randomly select PN sequences for spreading the data from a list of 8 PN codes instead of all devices using the same PN sequence, as is done by current ZigBee systems. In this way even if collisions occur, still it would be possible to successfully transmit messages. Thus, the capacity of the ZigBee system is increased. However, the system in Reference [3] has only been evaluated with constant message lengths and single hop topology. Systems with such restrictions represent only a small subset of IoT networks.

So, in our thesis we have proposed a multiple hop ZigBee system using the system in Reference [3] and adding multiple hops in that system. We have extended the range in our new multiple hop system through two hops compared to the Reference [3] system. We have used routers in our larger network so that sensors which are not close to the coordinator can transmit their messages through a router, which involves two hops. In this way, we

have expanded our range compared to the Reference [3] system and reduced collisions compared to current ZigBee systems. Also, for the larger network we don't have to spend more power, which increases battery life of the whole system. Thus, we have extended range and longevity and increased message success rates of the ZigBee system. We have developed a code in MATLAB for our new proposed system. We have also shown how the simulation code would need to be modified to incorporate variable length messages.

We have run multiple simulations in MATLAB varying lambda, message lengths and number of CAP slots. We have compared success rates between our proposed system and current system and we have plotted graphs for each data table. Those results show that our new multiple hop ZigBee system's success rate is always significantly higher than the current multiple hop system. In our result analysis, we can see that, by increasing message lengths with fixed lambda value 50, for 200 bits the current system has success rate of 65.43% and our new proposed system success rate of 82.10% which is higher. Then also, for message length 400 bits, current system success rate is around 49.67% and our new proposed system success rate is around 68.83% which is also significantly higher. So, difference in success rates gets larger. These results mean our system is showing higher performance that the current system. Even more so, by varying lambda values with fixed message length 200 bits, there is decrease in success rates for both our new system and the current system. Also, their performance difference gets larger with increasing lambda values. With lambda value 25, difference between our system and the current system is around 10% and with lambda value 100, their performance difference is 20%. So, our new system is showing much better performance. Then, for fixed message length of 300 bits by

varying number of CAP slots, both systems performance got even worse. Initially for 10 CAP slots, the success rate of our new system is around 38.88% and the current system success rate is 30.66%, which is very poor. Their performance difference is around 8%. But for 16 CAP slots, both our new proposed system and the current system performance difference is around 16%. So, our new proposed system shows significant improvement and stability over the current system. The results from chapter 6, Result Analysis, again show significant improvements and stability for our new ZigBee system over the current ZigBee system for all cases.

So, our new system has more advantages in terms of higher range, longer battery life and higher success rate comparing to the current system. Our multiple hop ZigBee network has significant improvements which plays a vital role in wireless networking for the Internet of Things. It will also have broader applications in real life than the earlier single hop, multi PN code network.

8. FUTURE RESEARCH SUGGESTIONS

In this thesis, we have developed a multiple hop ZigBee network which is more efficient than the current ZigBee system. Our system has higher range and longer battery life. We have evaluated the system by varying parameters like lambda (message arrival rate), message length and number of CAP slots. But there are many areas where future research can yield additional advantages to ZigBee networks.

We have established a multiple hop system which involves two hops to transmit the message to the coordinator. By incorporating two hops, we have increased the range of the system compared to the Reference [3] single hop system without using additional power. So, this can also increase longevity and range compared to the current ZigBee system. So, for further research more hops can be added in the system and in this way a system using multiple PN codes can further increase range. Along with this future research, an imbalance in the number of sensors in each hop can be analyzed to see how an imbalance in the number of one-hop nodes and two-hop nodes and/or an imbalance in the number of nodes connected to each of the routers affects the system. Also, quantification of power reduction can be done for future research.

In our system, we have used 8 different PN codes to spread the messages and because of this, fewer messages were destroyed which were involved in collisions compared to the current system where all the messages involved in collisions were destroyed because the current system uses only one PN code. This feature is even more important with multiple

hop systems than with single hop systems. So, in the future, different PN sequences with possibly greater processing gains can be developed for the system. In this way, data transmissions will be more reliable and secure. This will open up many new applications.

Also, in a ZigBee multiple hop system, variable length messages can be incorporated in the simulation code using the information we have provided in Appendix A. The results can be evaluated in the future by determining optimum frame size and optimum number of CAP slots for various mean lengths with multiple hops.

We have established the system using tree topology and got good results in terms of range and longevity. In future research mesh topology can be incorporated in the system and analysis can be done on its effects on network reliability. Because mesh topology is much more robust than tree topology, we believe that there will be much more improvement in the results analysis, especially when failure of routers is considered.

Also, in future research, in the multiple hop ZigBee system another software package which was discussed in chapter 4, like reference [31] OMNeT++ simulation, can be used for checking ZigBee system's performance with all the networking traffic included i.e., control messages that set up the network, monitor the health of the sensors and routers and strength of the system's various signals, and changes in the network based on received information.

APPENDIX SECTION

APPENDIX A: Analyzing Our Multiple Hop ZigBee System for Verification of the Message Length Generator

In this section we have shown how to modify the simulation to model varying message size. At first, we have temporarily adjusted N, number of messages initiated over the time-period to 20000 and added 40 bins to allow us to get a smoother histogram plot.

As described in the thesis, the goal was to vary the message length using an exponential distribution. In the code line 38 (see Appendix B), the argument inside exprnd is the mean; we adjusted this value to verify that the simulation is working well. We adjusted the argument inside exprnd and we produced a histogram for each argument value. The data set table is in the following.

Table 9.1. Data table for variable length message

Argument Value in line 38	Mean of length
0.0064	0.0064
0.0054	0.0054
0.0044	0.0044
0.0034	0.0034
0.0024	0.0024

For the data set in the table, the histogram produces an exponential probability density function with the appropriate mean for each argument value. The histogram plots for the data set are given below,

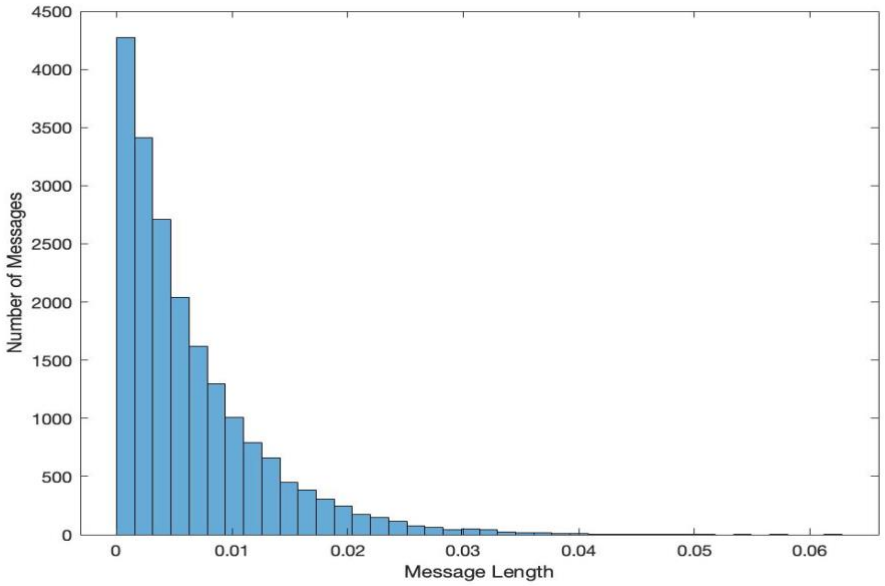


Figure 9.1. Histogram plot for argument value 0.0064

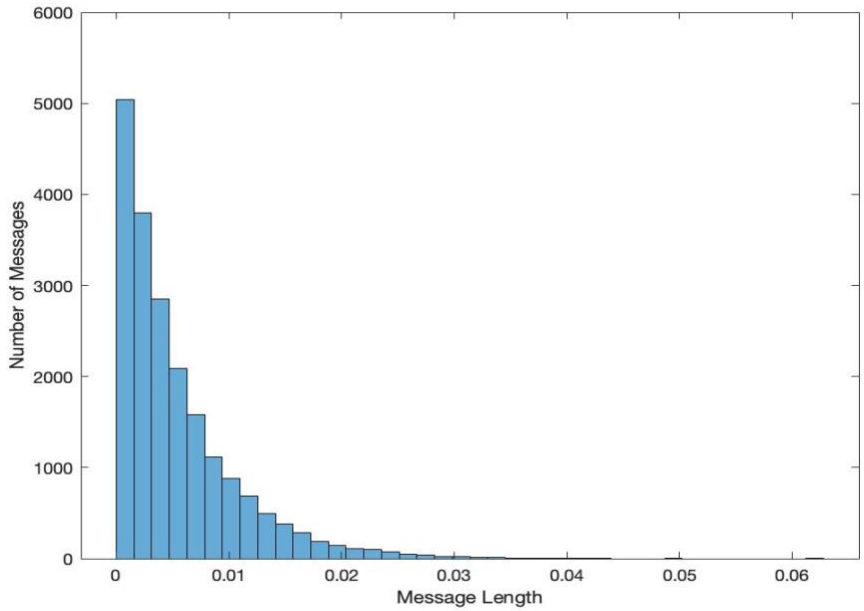


Figure 9.2. Histogram plot for argument value 0.0054

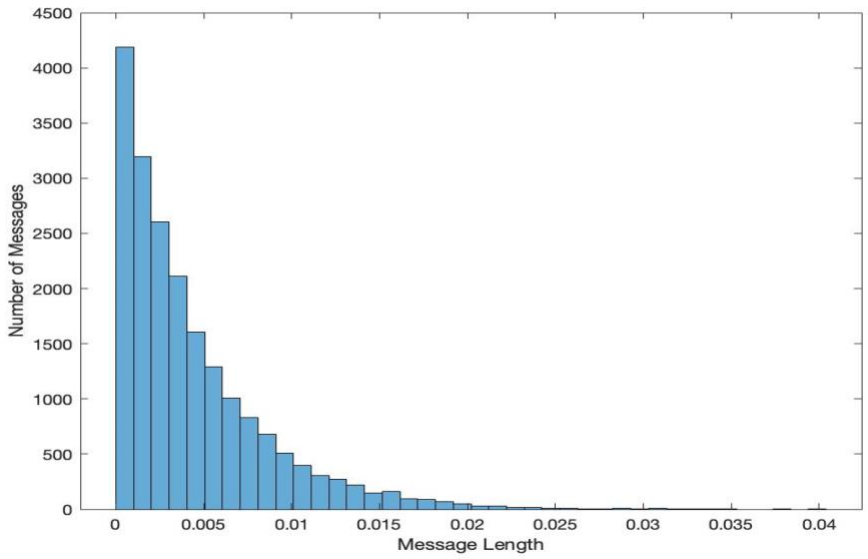


Figure 9.3. Histogram plot for argument value 0.0044

The histogram plots for 0.0064, 0.0054 and 0.0044 argument values we got mean of message lengths 0.0064, 0.0054 and 0.0044 consecutively which are the same as their argument values. So, we got appropriate mean for the histograms.

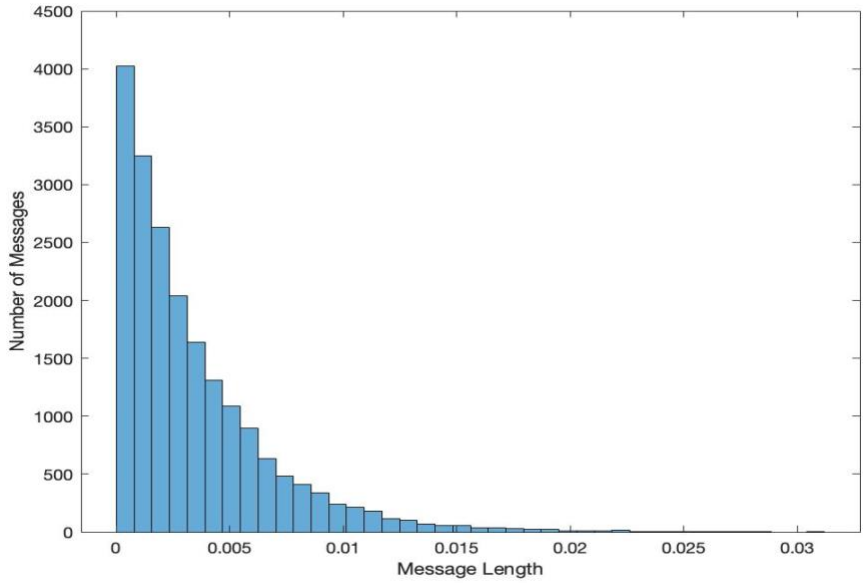


Figure 9.4. Histogram plot for argument value 0.0034

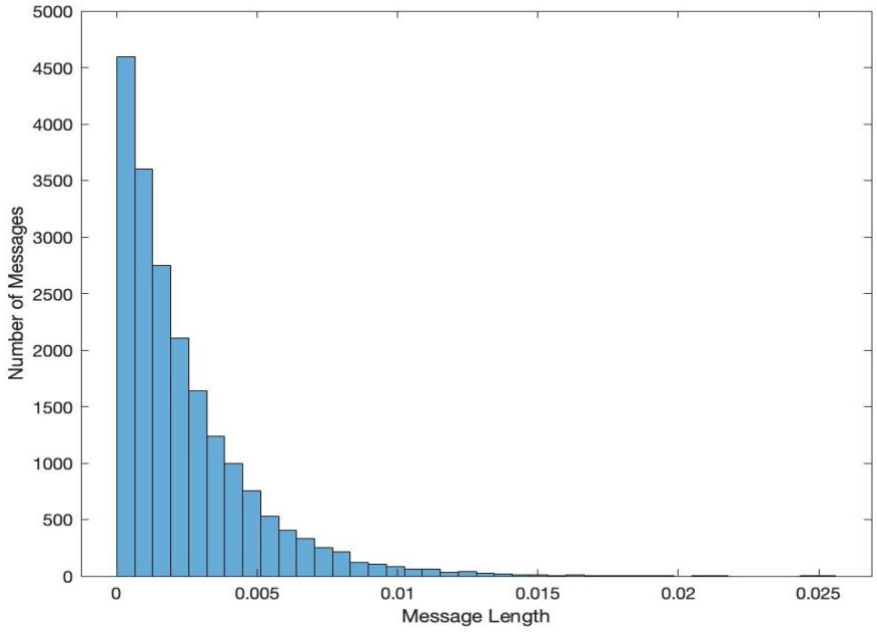


Figure 9.5. Histogram plot for argument value 0.0024

Lastly for argument values 0.0034 and 0.0024, we got message lengths mean of 0.0034 and 0.0024 consecutively which are also same as their argument values.

So, from five different argument values, we got different mean of message lengths which are same as their consecutive argument values. We can now verify that each histogram produces an exponential probability density function with the appropriate mean. Also, thus we can verify that the message length generator is working correctly as the new pdf has the correct mean.

So, in the simulation, for truly model variable message length, we have done the first step, which is to create a message length following an exponential distribution. The second step will be to break any message that is longer than one CAP slot into multiple packets. The

third step will be to place all of the multiple packets into appropriate CAP slots (the same slot number will be used in consecutive frames to transmit multiple packets from the same message). The fourth step occur after transmission, where there will be need to inspect all the packets associated with a long message and count the message as successfully received only if all the packets from the message are successfully received.

APPENDIX B: Developed MATLAB Simulation Code

In the following, the MATLAB simulation code is given. The blue colored bars indicate the lines that are newly added and the green colored bars indicate the lines that are modified from the previous version of the code [3] to develop the proposed new ZigBee multiple hop system for the thesis.

```
%considering a system initiating messages at random
%assuming the system as initiated 50 messages at random starting from
%message 0 to message 50
 Lambda = 100; %message arrival rate/avg number of messages initiated for whole system (messages per second)
i = 0; %assuming  message 0 arrives 0 seconds
N = 20000; %number of messages initiated over the time period
frame_size=.125; %size of superframe in seconds
capslots=16; %number of CAP slots in a superframe
%H = 5; %assuming average length of a call in seconds, initially 5sec
j1=[1:20]; %number of sensors in the system 1
j2=[21:24]; %number of sensors in the system 2
j3=[25:40]; %number of sensors in the system 3
j=[j1, j2, j3];
k=[1:8];  %number of different pn tables
a=numel(j);
b=numel(k);
for n=1:a
   pnt_sensor(n)= randi(b); %randomly assigning each sensor with a pn table
end
assignment=[j;pnt_sensor]';

assignment_op=array2table(assignment,'variablenames',{'SensorNumber','PN_TableNumber'});

   sensor_end=zeros(1,a); %This array records the endtime of the last message transmitted by each sensor

for n=1:N
R(n)=rand; %generate a exponentially distributed random number between (0,1)
old(n) = ((-log(1-R(n)))/Lambda); %calculating arrival times of each message
end
arrival(1)=i+old(1);
```

```
for n=2:N
    arrival(n)=(i+sum(old(1:(n))));
end
arrivaltimes=arrival; %calculated arrivaltimes of each message
 initial_arrivaltimes=arrivaltimes; %This is the initial arrival times of the messages before the multi hopping


for n=1:N
length(n)=exprnd(0.0064);
end
    nbins=40;
    histogram(length,nbins)
 messagelength=length; %calculated message length of each message
 xlabel('Message Length')
ylabel('Number of Messages');
for n=1:N
    endtime(n)=arrival(n)+length(n); %calculating the end time of each message
   initial_endtime(n)= endtime(n); % this is the initial end time of the messages before multiple hopping
end

q=0.10; % Percent of destroyed messages in Single Hop
for n=1:N %looping to generate sensor numbers for the remaining messages
    y(n)=randi(a); %generate random sensor number
    z(n)=y(n); %initially assigned sensor number
      D(n)=rand; %Generate random number from 0 to 1 for calculating how many messages are destroyed in Single Hop
    messages_at_capacity(n)=0;
    destroyed_in_single_hop(n)=0;
     if y(n)~= y(1:n-1) %check if it is not the same number as any of the previously generated sensor numbers
       msg_sensor(n)=y(n); %if it is not the same then associate that sensor number to current message
       sensor_end(y(n))=endtime(n);
    else %if it is the same ...
       % The "if" statement below is executed if that sensor has finished
       % transmitting its previous message
       if arrivaltimes(n) > sensor_end(y(n));
          msg_sensor(n)=y(n);
          sensor_end(y(n))=endtime(n);
       % The "else" statement below is executed if that sensor has not
       % finished transmitting its previous message and so a different
       % sensor has to be associated to the message.
       else
          %  Suppose the original sensor number was 6.  Each
```

```
71          %  pass through the loop below increments the sensor number by
72          %  1 and checks to see if the new sensor number is currently
73          %  transmitting a message.  If not, the message is associated to
74          %  the new sensor number and the loop terminates.  If so, the
75          %  loop is repeated.  After the sensor number is increased to
76          %  j, if another loop is necessary the new sensor number will
77          %  be 1, the 2, then 3, etc.
78          %  The sensor number will continue to be incremented once per loop
79          %  until the number 5 is reached.  If all the sensors are
80          %  transmitting other messages, a "system at capacity" message
81          %  will then be printed.
82          for ix=1:a
83             y(n)=mod(y(n),a)+1 ;
84             if arrivaltimes(n) > sensor_end(y(n));
85                msg_sensor(n)=y(n);
86                sensor_end(y(n))=endtime(n);
87                break
88             else
89                if ix==a fprintf('system at capacity for message number')
90                   n
91                   messages_at_capacity(n)=1;
92                end
93             end
94          end
95       end
96    end
97
98    if (y(n)==1) || (y(n)== 2) || (y(n)==3)||(y(n)==4)||(y(n)==5)
99       y(n)=j(21);
100       arrivaltimes_1(n)=endtime(n);
101       endtime_1(n)=arrivaltimes_1(n)+length(n);
102       arrivaltimes(n)=arrivaltimes_1(n);
103       endtime(n)=endtime_1(n);
104       if D(n)<q
105          fprintf('Message number destroyed in Single Hop')
106          n
107          destroyed_in_single_hop(n)=1;
108       else
109          if arrivaltimes(n) > sensor_end(y(n))
110          msg_sensor(n)=y(n);
111          sensor_end(y(n))=endtime(n);
112          else
113          arrivaltimes_x(n)=arrivaltimes(n)+0.1; %%%Delay of 100 ms
114          arrivaltimes(n)=arrivaltimes_x(n);
115          endtime_x(n)=arrivaltimes(n)+length(n);
116          endtime(n)=endtime_x(n);
```

```
117             if arrivaltimes(n)<sensor_end(y(n))
118             fprintf('system at capacity for message number')
119             n
120             messages_at_capacity(n)=1;
121             end
122
123           end
124         end
125
126     end
127   if (y(n)==6) || (y(n)== 7) || (y(n)==8)||(y(n)==9)||(y(n)==10)
128         y(n)=j(22);
129         arrivaltimes_2(n)=endtime(n);
130         endtime_2(n)=arrivaltimes_2(n)+length(n);
131         arrivaltimes(n)=arrivaltimes_2(n);
132         endtime(n)=endtime_2(n);
133         if D(n)<q
134           fprintf('Message number destroyed in Single Hop')
135           n
136           destroyed_in_single_hop(n)=1;
137         else
138           if arrivaltimes(n) > sensor_end(y(n));
139           msg_sensor(n)=y(n);
140           sensor_end(y(n))=endtime(n);
141           else
142           arrivaltimes_x(n)=arrivaltimes(n)+0.1; %%%Delay of 100 ms
143           arrivaltimes(n)=arrivaltimes_x(n);
144           endtime_x(n)=arrivaltimes(n)+length(n);
145           endtime(n)=endtime_x(n);
146             if arrivaltimes(n)<sensor_end(y(n))
147             fprintf('system at capacity for message number')
148             n
149             messages_at_capacity(n)=1;
150             end
151           end
152         end
153   end
154   if (y(n)==11) || (y(n)== 12)||(y(n)==13)||(y(n)==14)||(y(n)==15)
155         y(n)=j(23);
156         arrivaltimes_3(n)=endtime(n);
157         endtime_3(n)=arrivaltimes_3(n)+length(n);
158         arrivaltimes(n)=arrivaltimes_3(n);
159         endtime(n)=endtime_3(n);
160         if D(n)<q
161           fprintf('Message number destroyed in Single Hop')
162           n
```

```
163             destroyed_in_single_hop(n)=1;
164         else
165                 if arrivaltimes(n) > sensor_end(y(n));
166             msg_sensor(n)=y(n);
167             sensor_end(y(n))=endtime(n);
168             else
169             arrivaltimes_x(n)=arrivaltimes(n)+0.1; %%%Delay of 100 ms
170             arrivaltimes(n)=arrivaltimes_x(n);
171             endtime_x(n)=arrivaltimes(n)+length(n);
172             endtime(n)=endtime_x(n);
173               if arrivaltimes(n)<sensor_end(y(n))
174               fprintf('system at capacity for message number')
175               n
176               messages_at_capacity(n)=1;
177               end
178             end
179         end
180   end
181   if (y(n)==16) || (y(n)== 17)||(y(n)==18)||(y(n)==19)||(y(n)==20)
182         y(n)=j(24);
183         arrivaltimes_4(n)=endtime(n);
184         endtime_4(n)=arrivaltimes_4(n)+length(n);
185         arrivaltimes(n)=arrivaltimes_4(n);
186         endtime(n)=endtime_4(n);
187         if D(n)<q
188             fprintf('Message number destroyed in Single Hop')
189             n
190             destroyed_in_single_hop(n)=1;
191         else
192             if arrivaltimes(n) > sensor_end(y(n));
193             msg_sensor(n)=y(n);
194             sensor_end(y(n))=endtime(n);
195             else
196             arrivaltimes_x(n)=arrivaltimes(n)+0.1; %%%Delay of 100 ms
197             arrivaltimes(n)=arrivaltimes_x(n);
198             endtime_x(n)=arrivaltimes(n)+length(n);
199             endtime(n)=endtime_x(n);
200               if arrivaltimes(n)<sensor_end(y(n))
201               fprintf('system at capacity for message number')
202               n
203               messages_at_capacity(n)=1;
204               end
205             end
206         end
207   end
208   final_arrivaltimes(n)=arrivaltimes(n);
```

```
final_endtime(n)=endtime(n);
if initial_endtime(n)==final_endtime(n)
   single_hop(n)=1;
   multi_hop(n)=0;
elseif messages_at_capacity(n)==1 || D(n)<q
      single_hop(n)=0;
      multi_hop(n)=0;
else
   single_hop(n)=0;
   multi_hop(n)=1;
end
end

frame=floor(final_endtime/frame_size)+1; %determine superframe number for each message
sensor=y;
initial_sensor=z;%initially assigned senors
final_sensor=y;%finally assigned sensors after multiple hopping
 %assigning PN table numbers with their corresponding sesnor numbers for all the messages in the system
w=sensor;
for n=1:N
 t(n)=find(w(n)==assignment(:,1));%finds the row number in the assignment matrix of the sensor number in 'w' matrix
p(n)=assignment(t(n),2);%gets the PN table number of that sensor
end
tablenum=p;

%defining CAP slots for the messages during the active period of the superframe and randomly
%assigning them to the messages in the system
for n=1:N
 cap_msgs(n)=randi(capslots);
end

  output2=[initial_arrivaltimes; messagelength; initial_endtime; final_arrivaltimes; messagelength; final_endtime;initial_sensor; final_sensor; tablenum;frame;cap_msgs; messages_at_capacity; destroyed_in_single_hop; single_hop; multi_hop]';
 output=[frame;cap_msgs;tablenum]'; %creating a matrix containing the superframe numbers, CAP slot numbers and PN table numbers of each message

Total_Number_of_Messages_Destroyed_in_Single_Hop=0;
Total_Number_of_Messages_at_capacity=0;
Number_of_messages_with_Single_Hop=0;
Number_of_messages_with_Double_Hop=0;
%checking for messages with same superframe numbers and CAP slot
```

```
%numbers. If there are more then 2 msessages with the same CAP slot numbers
%trying to transmit within the same superframe,
%then those messages will be destroyed and indicated by a "1" in the 3rd column of output1 matrix
output1=[frame;cap_msgs]';
unqRows = unique(output1,'rows','stable'); %unique row numbers
        matchIdx = cell2mat(arrayfun(@(i)ismember(output1,unqRows(i,:),'rows'), 1:size(unqRows,1), 'UniformOutput', false));
output1(:,3) = any(matchIdx .* (sum(matchIdx,1)>2),2); %mark rows with 3 or more msgs in same superframe and CAP slot
 output1(:,4) = any(matchIdx .* (sum(matchIdx,1)==2),2); %mark rows with 2 msgs in same superframe and CAP slot

for msgcount=1:N
    if output1(msgcount,4)==1
        pran=rand;
        if pran>=0.610
            output1(msgcount,5)=1;
        else
        end
    else
    end
end
 %%%when the system is at capacity for a certain message ignore the 3, 2 and destroyed from two
%%%collided to be 0
for n=1:N
if messages_at_capacity(n)==1 || D(n)<q
output1(n,3)=0;
output1(n,4)=0;
output1(n,5)=0;
end
end

%moving contents of matricies output and output1 into output2 matrix
Three_or_more_collided=0;
Two_collided=0;
Destroyed_from_two_collided=0;
for n=1:N
output2(n,17)=output1(n,4);  %Mark all cases where there are 2 and only 2 messages in the same superframe and CAP slot
 output2(n,18)=output1(n,5); %Mark those cases where the use of eight PN tables allows one or both messages to be successfully received
output2(n,16)=output1(n,3);  %Mark those cases where there are 3 or more messages in the same superframe and CAP slot
```

```
285     Three_or_more_collided=Three_or_more_collided+output2(n,16); % Determine total number of messages destroyed by collision of 3 or more
286   Two_collided=Two_collided+output2(n,17); % Determine total number of messages involved in collisions of exactly 2 messages
287           Destroyed_from_two_collided=Destroyed_from_two_collided+output2(n,18); %Determine number of messages destroyed in 2-message collisions
288
Total_Number_of_Messages_at_capacity=Total_Number_of_Messages_at_capacity+output2(n,12);%Determine total number if messages at capacity
289
Total_Number_of_Messages_Destroyed_in_Single_Hop=Total_Number_of_Messages_Destroyed_in_Single_Hop+output2(n,13); %Determine total number of messages destroyed in Single Hop
290
Number_of_messages_with_Single_Hop=Number_of_messages_with_Single_Hop+output2(n,14);%Determine number of messages transmitted with Single Hop
291
Number_of_messages_with_Double_Hop=Number_of_messages_with_Double_Hop+output2(n,15);%Determine number of messages transmitted with Double Hop
292   end
293
294
output2_op=array2table(output2,'variablenames',{'Initial_Arrival_Time','Message_lenght','Initial_endtime','Final_Arrival_Time','Message Length', 'Final_endtime','Inital_sensor_Number','Final_Sensor_Number','PN_Table','Frame','Capslot','Messages at Capacity', 'Message Destroyed in Single Hop', 'Single_Hop', 'Multi_Hop', '3 or More Collided', '2 collided', 'Destroyed from 2 collided'});
295   Three_or_more_collided
296   Two_collided
297   Destroyed_from_two_collided
298   Total_Number_of_Messages_at_capacity
299   Total_Number_of_Messages_Destroyed_in_Single_Hop
300   Number_of_messages_with_Single_Hop
301   Number_of_messages_with_Double_Hop
302
303   Total_Successfully_Transmitted_Messages=N-(Total_Number_of_Messages_at_capacity+Three_or_more_collided+Destroyed_from_two_collided+Total_Number_of_Messages_Destroyed_in_Single_Hop)
```

REFERENCES

[1] “ZigBee Technology Architecture and Its Applications”, Available at: https://www.elprocus.com/what-is-zigbee-technology-architecture-and-its-applications/.

[2] “The ZigBee vs Wi-Fi Battle for M2M Communication”, Available at: https://www.link-labs.com/blog/zigbee-vs-wifi-802-11ah.

[3] Rashmi Mohan Kumar, “Collision Avoidance and Extending Capacity and Range in ZigBee”, A thesis submitted to the Graduate Council of Texas State University in partial fulfillment of the requirements for the degree of Master of Science with a Major in Engineering, April 2020.

[4] “A Brief History of the Internet of Things”, Available at: https://www.dataversity.net/brief-history-internet-things/ .

[5] Google photos.

[6] Yi-Chiao Wu, Liang-Bi Chen, Wan-Jung Chang, Che-Ching Yang and Chao-Tang Yu, “Implementation of a Zigbee-based Wireless Router for Home Automation Systems”, IEEE International Conference on Consumer Electronics - Taiwan (ICCE-TW), 2017.

[7] “Bluetooth vs WIFI vs ZigBee”, Available at: https://www.electronicproducts.com/bluetooth- vs-wi-fi-vs-zigbee/.

[8] “ZigBee Wireless Mesh Networking”, Available at: https://www.digi.com/solutions/by- technology/zigbee-wireless-standard.

[9] “What is ZigBee technology? Architecture, topologies and applications”, Available at: https://www.electronicshub.org/zigbee-technology-architecture-applications/.

[10] “Zigbee and its Significance in IoT Applications”, Available at: https://iot4beginners.com/zigbee-and-its-significance-in-iot-applications/.

[11] Xiyuan Wei, “The Design and Completion of Remote Data Monitoring Based on ZigBee Wireless Sensor Network”, *International Journal of Online and biomedical Engineering*, Vol 12, No 10, 2016.

[12] “ZigBee/IEEE 802.15.4 Summary”, Available at: http://users.eecs.northwestern.edu/~peters/references/ZigtbeeIEEE802.pdf.

[13] “ZigBee Networks”, Available at: https://www.digi.com/resources/documentation/Digidocs/90002002/Concepts/c_device_types.htm?TocPath=Zigbee%20networks%7CZigbee%20networking%20concepts%7C_____1.

[14] “What is a ZigBee Network?”, Available at: https://www.assured-systems.com/us/news/article/what-is-a-zigbee-network/.

[15] Wei Wang, Guangyu He, Junli Wan, “Research on Zigbee wireless communication technology”, *International Conference on Electrical and Control Engineering (ICECE),* 2011.

[16] Drew Gislason, “ZigBee Wireless Networking”, Chapter 7, 2008.

[17] J. A. J. S. E. W. T. K. Jack L. Burbank, "Wireless Personal Area Networks," in Wireless networking: understanding internetworking challenges, New Jersey, John Wiley & Sons, Inc., Hoboken, 2013, pp. 71-92.

[18] Muthu Ramya.C, Shanmugaraj.M, Prabakaran.R, “Study on ZigBee Technology”, *International Conference on Electronic Computer Technology*, 2011.

[19] Vijay K. Garg,“Wireless Communications & Networking”, Chapter 20 - Wireless Personal Area Networks: Low Rate and High Rate, 2007.

[20] “CSMA with Collision Avoidance (CSMA/CA)”, Available at: https://www.tutorialspoint.com/csma-with-collision-avoidance-csma-ca.

[21] “MAC frame formats”, Available at: https://grouper.ieee.org/groups/802/15/pub/2001/Jul01/01292r1P802-15_TG3-Proposed-Changes-to-Frame-Formats.pdf.

[22] “Network Layer Routing”, Available at: https://www.tutorialspoint.com/data_communication_computer_network/network_layer_routing.htm.

[23] A. Tomar, "Introduction to ZigBee Technology”, *Global Technology Centre Volume 1,* July 2011.

[24] Dnyaneshwar Mantri, Neeli Rashmi Prasad, Ramjee Prasad, “Scheduled Collision Avoidance in Wireless Sensor Network using Zigbee”, *International Conference on Advances in Computing, Communications, and Informatics (ICACCI),* 2014.

[25] Naimah Yaakob, Ibrahim Khalil, Mohammed Atiquzzaman, Ibrahim Habib, Jiankun Hu, “Distributed collision control with the integration of packet size for congestion control in wireless sensor networks”, Wireless Communications and Mobile Computing, Wirel. Commun. Mob. Comput., 16:59–78, Published online 18 July 2014 in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/wcm.2488, 2016.

[26] Chatura Seneviratne, Henry Leung, “A Low Complex Spread Spectrum Scheme for ZigBee based Smart Home Networks”, *13th IEEE Annual Consumer Communications & Networking Conference (CCNC),* 2016.

[27] Jianxin Zhang, Xuemei Lei, Jing Shi, Lehei De, “Simulation Study and Performance Analysis on Zigbee System with CCI”, 25th Wireless and Optical Communication Conference (WOCC), 2016.

[28] Tien-Wen Sung, Ting-Ting Wu, Chu-Sing Yang, Yueh-Min Huang, “Reliable Data Broadcast for ZigBee Wirelss Sensor Networks”, *INTERNATIONAL JOURNAL ON SMART SENSING AND INTELLIGENT SYSTEMS, VOL. 3, NO. 3,* September 2010.

[29] Chentao Li, Kaifeng Dong, Fang Jin, Junlei Song, Wenqin Mo, “Design of Smart Home Monitoring and Control System Based on Zigbee and WIFI”, *Proceedings of the 38th Chinese Control Conference, Guangzhou, China*, July 27-30, 2019.

[30] Fei Ding, Aiguo Song, “Development and Coverage Evaluation of ZigBee-Based Wireless Network Applications”, *Hindawi Publishing Corporation Journal of Sensors, Volume 2016, Article ID 2943974, 9 pages, http://dx.doi.org/10.1155/2016/2943974,* 2016.

[31] Dominik Bunyai, Lukas Krammer, Wolfgang Kastner, “Limiting Constraints for ZigBee Networks”, *IECON 2012 - 38th Annual Conference on IEEE Industrial Electronics Society,* 24 December 2012.

[32] Chunquan Li, Ming Zhang, Hanzhao He, Cailin Li, Yuhe Chang, Yuling Shang, “Research of Improved ZigBee-based AODVjr Routing Algorithm in Cloud Manufacturing”, *International Journal of Online and Biomedical Engineering (iJOE) – eISSN: 2626-8493*, March 2015.

[33] Chih-Heng Ke, Sun-Yuan Hsieh, Ti-Cheng Lin, and Tai-Hsuan Ho, “Efficiency Network Construction of Advanced Metering Infrastructure Using Zigbee”, *IEEE Transactions on Mobile Computing, Vol. 18, No. 4,* April 2019.

[34] “Queuing theory: Definition, history & real-life applications”, Available at: https://queue-it.com/blog/queuing-theory/.

[35] Erlang, Agner K. (1920), “Telefon-Ventetider. Et Stykke Sandsynlighedsregning” [Telephone Waiting Times. A Bit of Probability Calculation], *Matematisk Tidsskrift B,* 31: 25-42.

[36] “Queuing theory”, Available at:
https://corporatefinanceinstitute.com/resources/knowledge/other/queuing-theory/.

[37] “Chapter 2 – Poisson Process”, Available at:
https://www.rle.mit.edu/rgallager/documents/6.262lateweb2.pdf.

[38] Ahmed Ahmed Abouelfadl, Farid Shawki, Mohsen El-bendary, “Enhancing Transmission over Wireless Image Sensor Networks Based on ZigBee Network”, Article *in* Life Science Journal, January 2014.