COLLISION AVOIDANCE AND EXTENDING RANGE & CAPACITY IN ZIGBEE

by

Rashmi Mohan Kumar, B.S.

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
May 2020

Committee Members:

Harold Stern, Chair

Rich C. Compeau

William Stapleton

Semih Aslan

FAIR USE AND AUTHOR'S PERMISSION STATEMENT

Fair Use

Duplication Permission

DEDICATION

This thesis is dedicated to my parents, brother and to everybody who has taught me something valuable in this journey of life. I am grateful for their prayers, blessings and time.

ACKNOWLEDGEMENTS

I would like to express my sincere gratitude to my thesis advisor **Dr. Harold Stern**, for his support and continuing encouragement throughout my research and for his guidance and suggestions at each step for shaping and helping me in developing and presenting this research. It is a genuine pleasure to work with him on this research. Dr. Stern has always been kind with his timely advice, scholarly suggestions and scientific approach which are the main constituents for completing this research. He has always inspired and motivated me to become an independent researcher and helped me realize the power of critical thinking and reasoning. I will forever be grateful to him.

I would also like to extend my deepest gratitude to my committee members **Dr. William Stapleton, Dr. Rich C. Compeau** and **Dr. Semih Aslan** for their excellent suggestions and valuable insights in the process of developing and presenting this thesis. Without their passionate participation and input, the validation and evaluation of the results for this research could not have been successfully conducted. I am grateful to them for introducing me to all the possible challenges and methodologies during the proposal presentation to accomplish the goals of this research.

I am grateful to **Dr. Vishu Viswanathan**, my graduate advisor at the Ingram School of Engineering. His valuable suggestions and commitment to achieve high standards has always kept me motivated throughout my journey as a graduate student at Texas State University.

Finally, I am extremely grateful and will always be in debt to my father, B K Mohan for supporting my dreams, my mother Jalaja Mohan for all her valuable lessons in life. I am grateful for their blessings, care, and sacrifices for educating and teaching me to work hard and to be dedicated to every goal in my life. My brother, Rahul Mohan Kumar for motivating me to study masters and standing as my pillar throughout my journey. My friends, for always supporting me and helping me to stay positive in every situation.

I am deeply grateful to every other person who as always taught me something valuable at every stage in my life which has helped me in becoming the person I am today.

TABLE OF CONTENTS

Page

LIST OF TABLES

Table **Page**

LIST OF FIGURES

Figure **Page**

ABSTRACT

ZigBee technology is a low data rate, low power consumption, low cost, wireless networking protocol built on top of the IEEE 802.15.4 short range communications protocol [1]. It is usually targeted towards automation and remote control applications. ZigBee is one of the most widely used communication protocols of the Internet of Things (IoT) for transmission of information in a wireless mesh network between sensors and/or actuators, and for network connectivity which enables devices to connect and exchange data with each other.

ZigBee applications require that the devices operate for long periods of time with small, non-rechargeable batteries which in turn mandates low power consumption which limits transmission distance to 10-100m line of sight. As ZigBee operates in the same radio frequency band as Wi-Fi which is 2.4 GHz, it sometimes experiences interference when a Wi-Fi user is trying to transmit at the same time, resulting in a collision. Similarly a ZigBee network also experiences collisions when two or more ZigBee devices are trying to transmit data at the same time. Even though ZigBee employs a Direct Sequence Spread Spectrum system and uses the ALOHA protocol to overcome these interferences and collisions, some messages are still lost during transmission.

The Spread Spectrum system reduces the effects of noise and increases the probability of a message being successfully received despite collision with a message from a Wi-Fi user, but if a message collides with another ZigBee message then both

messages are still always lost. The reason for this loss is the fact that ZigBee employs only one particular set of Pseudorandom Noise (PN) codes to perform the spreading of data during modulation. When two or more messages transmitting at the same time are involved in a collision using the same PN sequence, the signal-to-interference ratio is too low for successful recovery of either message, resulting in either the loss of data or the need of retransmission of both messages involved in the collision. Retransmission requires additional time and uses additional power which results in energy wastage, slower transmission, and reduction of system throughput.

This thesis will propose and analyze a system where ZigBee transmitters are allowed to randomly choose a PN code from among a large set of possible PN codes. Performance improvement will be shown in terms of increased percentage of successfully transmitted messages, which produces improved accuracy, improved energy efficiency (enabling increased range and/or longer battery life) and increased system throughput.

1. INTRODUCTION

1.1. Problem Statement

Currently ZigBee is one of the most widely used communication protocols of the Internet of Things (IoT), for transmitting information in a wireless mesh network between sensors and/or actuators, and for network connectivity which enables devices to connect and exchange data with each other. It is usually targeted towards automation and remote control applications and with today's ever growing demand for comfort and leisure, it finds its applications in homes, offices, hospitals, etc for implementing smart networks.

The high demand results in millions of devices to transmit data across the networks, which sometimes can result in collision between these messages if they are being transmitted at the same time. ZigBee employs a particular PN code to spread the data for transmission. This PN code helps reduce the effects of noise and interference from other systems using the same frequency band (such as Wi-Fi) but since all ZigBee users currently employ the same PN code, if two or more ZigBee messages are involved in a collision it makes demodulation a difficult task resulting in the transmitted data being lost or destroyed, often requiring re-transmission.

Retransmission requires additional time and uses additional power which results in energy wastage, slower transmission as well as less data transmitted over a given period of time. This thesis will propose and analyze a system where ZigBee transmitters are allowed to randomly choose a PN code from among a large set of possible PN codes. The results will be analyzed and compared with the current system to show the

improvement in terms of increased energy efficiency (which can be translated into increased range and/or longer battery life) and increased system throughput.

1.2. Internet of Things

The Internet of Things (IoT) has not been around for very long but it has recently become ingrained in our everyday life. It surrounds us almost everywhere today - connected cars driving on the street, home automation devices located in the house, smart office sensors embedded at the workplace, and fitness trackers. It has created a large ecosystem of 17 billion connected things that influence societies and economies worldwide. The concept of connected devices dates back to early 1800s [2] where there had been visions of machines communicating with one another. In 1832 the first electromagnetic telegraph was designed, the telegraph enabled direct communication between two machines by sending electrical signals. However, the true history of the Internet of Things started with the invention of the Internet its major component, in the late 1960s and ever since it is rapidly developing every decade.

The Internet is a significant component of the IoT. The Internet- started out as part of the Defense Advanced Research Projects Agency (DARPA) in 1962, and later evolved into ARPANET in 1969. One of the very first examples of Internet of Things (IoT) or the connected device was a Coca-Cola vending machine situated at Carnegie Melon University and operated by local programmers. They integrated micro-switches into the machine and used the Internet to see if the cooling device kept the drinks cold enough and if there were any available Coke cans before making the trip to get one. This invention fostered further studies into this field and also on the development of connected machines all over the world.

In the year 1990, John Romkey connected the first toaster to the Internet with a TCP/IP protocol. A year later, scientists from the University of Cambridge came up with the idea to use the first prototype of a web camera to monitor the amount of coffee available in a coffee pot that was located in a local computer lab. The webcam took pictures of a coffee pot three times a minute and sent the images to the local computers, thus allowing everyone to see if there was coffee in it or not.

The year 1999 was marked as one of the most significant years in the history of IoT, as Kevin Ashton , the Executive Director of Auto-ID Labs at MIT, was the first to describe the Internet of Things and coined the term "the internet of things" while giving a presentation for Procter & Gamble. Being a visionary technologist, Kevin described IoT as a technology connecting several devices with the help of RFID tags for supply chain management. He concluded if all devices were "tagged," computers could manage, track, and inventory them. To some extent today, the tagging of things has been achieved through technologies such as digital watermarking, barcodes, and QR codes whereas inventory control is one of the more obvious advantages of the Internet of Things. Mr. Ashton used the word "internet" in the title of his presentation to draw the audience's attention since the internet was a big deal at that time. Although his idea of the RFID-based device connectivity differs from the present-day IP-based IoT, Ashton's breakthrough played an essential role in the history of Internet of Things and technological development.

By 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. The traditional fields of

automation, wireless sensor networks, GPS, control systems, and various others, all support the IoT [2] [3].

The Internet of Things (IoT) can be defined as a network or a system which inter-relates various computing devices, mechanical and digital machines, objects, animals or people, all that are provided with unique identifiers (UIDs) and with the ability to transfer data over a network without requiring any human-to-human or human-to-computer interaction [4]. This includes almost anything you can think of, ranging from cell phones to building maintenance to the jet engine of an airplane. Medical devices, such as a heart monitor implant or a biochip transponder in a farm animal, can transfer data over a network and are members of the IoT. If it has an off/on switch, then it can, theoretically, be part of the system [2]. The IoT consists of a gigantic network of internet connected "things" and devices.

The definition of Internet of Things has evolved over time due to its ability to converge with multiple technologies, real-time analytics, machine learning, commodity sensors, and embedded systems [4]. In today's ever growing technology environment IoT uses some of the most popular protocols, standards and communication technologies like Wi-Fi, Bluetooth, ZigBee, Z-Wave, Cellular, Advanced Message Queuing Protocol, Data Distribution Service, Message Queue Telemetry Transport, etc. to implement the communication process between the various connected devices of a network to transfer messages and data [5].

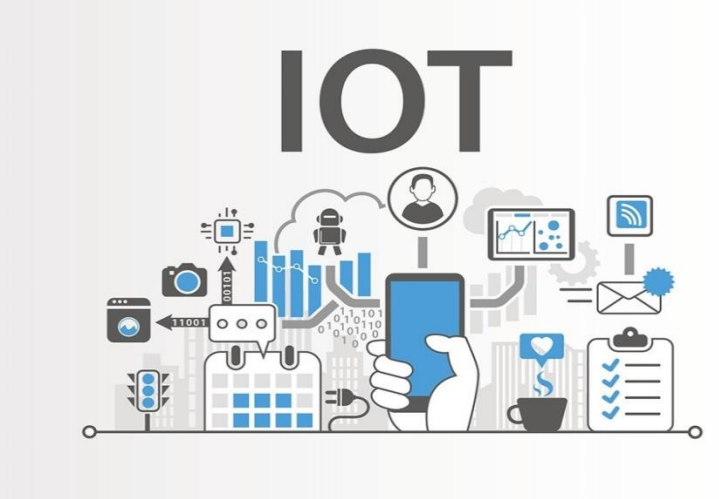


Figure 1.1. Internet of things [6]

1.3 ZigBee in the Internet of Things

ZigBee technology is a low data rate, low power consumption, low cost, wireless networking protocol built on top of the IEEE 802.15.4 short range communications protocol [1]. It is usually targeted towards automation and remote control applications. Due to its low power consumption and low cost, ZigBee is one of the most widely used communication protocols of the Internet of Things for transmitting information in a wireless mesh network between sensors and/or actuators, and for network connectivity which enables devices to connect and exchange data with each other. ZigBee features a mesh topology and frugal power requirements making it the go-to wireless standard for Internet of Things (IoT) when compared to Wi-Fi or Z-Wave.

ZigBee is a very useful communication protocol but its applications require that devices operate for long periods of time with small, non-rechargeable batteries which in turn mandates low power consumption which limits transmission distance to 10-100m

line of sight. ZigBee operates in the same radio frequency band as Wi-Fi which is 2.4 GHz, so it can sometimes experience interference when a Wi-Fi user is trying to transmit at the same time as ZigBee. To combat Wi-Fi interference, ZigBee employs a Direct Sequence Spread Spectrum system with a fixed pseudo-noise (PN code) and processing gain of 8 which allows it to successfully demodulate the signals transmitted even in the presence of interference from a Wi-Fi user using a different PN code. An in-depth description of ZigBee will be provided in Chapter 2 of this thesis.

1.4. Thesis Objective

Since all ZigBee users currently employ the same PN code, ZigBee faces a real problem when multiple ZigBee transmitters attempt to transmit at the same time. In other words, if two ZigBee signals are transmitted at the same time, they collide and neither signal can be successfully demodulated because they are using the same PN code. To avoid most collisions between two ZigBee signals, ZigBee uses an ALOHA protocol. Even though the ALOHA protocol reduces the number of collisions, some collisions still occur and, when they do, the two signals involved in the collision must be retransmitted. The retransmission requires additional time, uses additional power, and creates additional traffic which results in energy wastage, slower transmission, and potentially a smaller number of users that can be satisfactorily handled within an IoT system.

This thesis proposes and analyses a system where ZigBee transmitters are allowed to randomly choose a PN code from among a larger set of possible PN codes. Performance improvement will be shown in terms of increased system throughput and evaluated in the contexts of enabling more traffic in an IoT system and providing greater energy efficiency (which can be translated into increased range and/or longer battery

life). Performance of the proposed system will be determined by a combination of simulation and analytical techniques.

1.5. Organization of Thesis

This thesis is organized as follows:

Chapter 1 began with a problem statement followed by an introduction to Internet of Things (IoT), the main reason for which the ZigBee technology was introduced and developed. It also talks about how ZigBee is implemented in Internet of Things (IoT), followed by the main objective of this thesis along with its chapter organization. Chapter 2 gives an in-depth description of ZigBee. It provides an introduction to the IEEE 802.15.4 standard on top of which the ZigBee protocol is developed. Further it also gives an insight about the different network topologies that can be used to implement the ZigBee network and lastly it provides a brief knowledge about the working of a ZigBee network. Chapter 3 talks about the layered architecture of ZigBee, explaining the various operations and functionalities managed and performed by the different layers of ZigBee. Chapter 4 begins with explaining the different types of modulation systems that can be implemented in a ZigBee network. It explains in detail about the PHY Protocol Data Unit (PPDU), the primary data unit which stores data in the Physical (PHY) layer. It describes the process of modulation and data-spreading along with demodulation and data de-spreading. Furthermore it introduces the concept of a Pseudorandom Noise Sequences (PN) and its usage in the Direct Sequence Spread Spectrum (DSSS) technique. Lastly it also explains the Carrier Sense Multiple Access (CSMA/CA) technique employed by a ZigBee network to avoid or handle collisions as well as the Superframe structure of a data frame. Chapter 5 provides a brief description of the previous research work

performed on ZigBee Network systems using various methods and technologies available today. Chapter 6 begins with an introduction to our proposed solution. It describes the mathematical analysis and simulation methodologies that we have used for evaluating the performance of our solution along with a flowchart describing the process and design steps. Chapter 7 gives a detailed analysis of the performance of our proposed solution. It also provides a comparison of the results between the current ZigBee system and our new proposed ZigBee system. The observations and simulation plots of the research are explained at a later section of this chapter. Chapter 8 finally concludes with the objectives achieved with this research and Chapter 9, proposes the various possible ideas for future research.

2. IN-DEPTH DESCRIPTION OF ZIGBEE

2.1. Wireless Networking

During the initial periods of the current information era, obtaining and sharing information was a wired experience. As the multitudes started gravitating towards home personal computers, they began experiencing "The Internet" through a variety of wired technologies. As the need for information increased, the sophistication and capability of these wired technologies also improved. However, over time, we began to desire high capability and convenience and, with the proliferation of laptop computers along with the advent of mainstream wireless networking technologies, we began to enjoy the Internet on our own terms. The initial wireless networking technologies provided us only with primitive capability, but they showed us all what the potential information experience could be. In the subsequent years we have been rapidly untethering our information devices and increasingly accessing information on our terms [7].

In the mid-20th century the cellular network was a common extension of the wired telephony network that became extensive. Simultaneously as the need for mobility and the cost of laying new wires increased, the motivation for a personal connection independent of location to that network also increased. Coverage of large areas is provided through 1-2km cells that cooperate with their neighboring cells to create a seemingly seamless network. Some examples of cellular standards are GSM, IS-136, IS-95 [8]. Cellular standards are basically aimed at facilitating voice communications throughout a metropolitan area.

The wireless networking standards are broadly classified into three main categories based on their range of operation:

• Wireless personal area networks (WPANs)

• Wireless local area networks (WLANs)

• Wireless metropolitan area networks (WMANs)

The conventional differentiator in technology classification is the geographic range of operation, WPANs typically spans up to tens of meters, WLANs typically can span hundreds of meters up to a few kilometers and WMAN typically spans tens to hundreds of kilometers. The hierarchical relationship between these three categories is shown in Figure 1.1, along with the most significant wireless networking communication standards in terms of mass-market deployments. The ranges listed are approximate and will vary between standards and environments in which the technology is deployed.

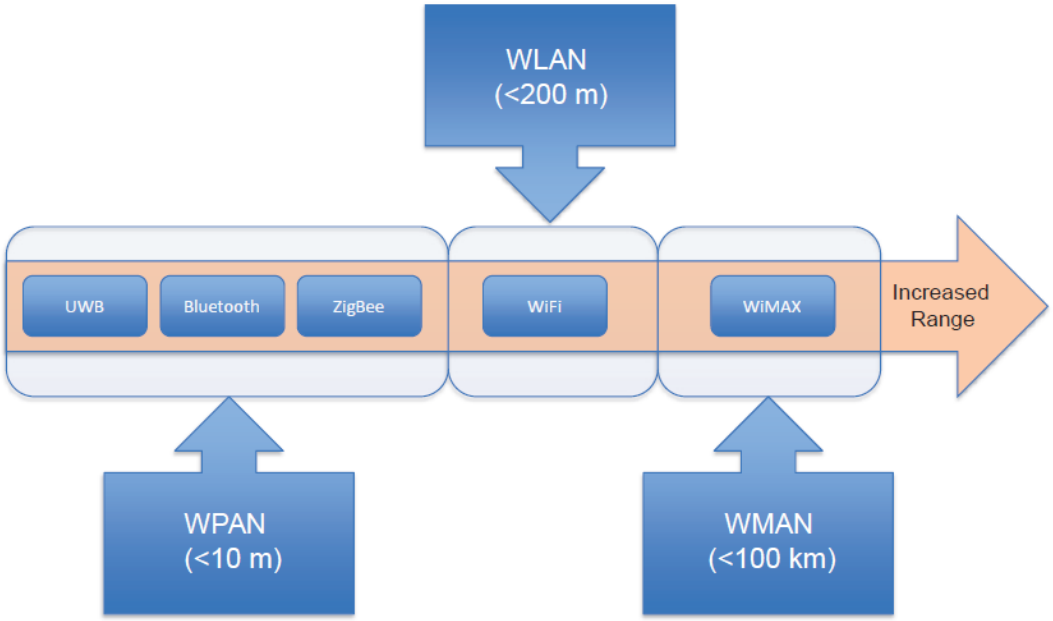


Figure 2.1. Wireless networking standards [7]

During the mid-1980s, due to the higher user densities and the emergent data traffic there was a need for much smaller coverage areas and more extensive frequency reuse. The IEEE 802.11 working group for WLANs was formed to create a wireless local area network standard [8]. As the IEEE 802.11 was concerned with features such as Ethernet's matching speed, long range (100m), complexities in handling seamless roaming, message forwarding, and data throughput around 2-11Mbps, the IEEE 802.15 working group was formed to create WPAN standard. WPANs are focused on the space around a person or object which typically extends up to 10m in all directions. The focus of WPANs is low-cost, low power, short range and very small size.

The IEEE 802.15 working group formed to create the WPAN standard defines three different classes of WPANs that are differentiated by data rate, battery drain and

quality of service (QoS). The high data rate WPAN (IEEE 802.15.3) is suitable for multi-media applications which require very high QoS. Whereas the medium data rate WPANs (IEEE 802.15.1/Bluetooth) can handle a variety of tasks ranging from cell phones to PDA communications and have QoS suitable for voice communications. The low rate WPANs (IEEE 802.15.4/LR-WPAN) are intended to serve a set of industrial, residential and medical applications with very low power consumption and cost requirement not considered by the above WPANs and with relaxed needs for data rate and QoS. The low data rate enables the LR-WPAN to consume very little power [8].

2.2 ZigBee Alliance

The ZigBee Alliance is a non-profit association of business, academia, and government agencies with the aim of developing standards to "deliver greater freedom and flexibility for a smarter, more sustainable world". Established in 2002 [16], it specifically focuses on the development of green, low-power, and open global low-power consumption wireless networking standards for sensor, control, and monitoring applications, while maintaining a high degree of simplicity and ease of use. ZigBee Alliance defines multiple specifications and stacks. The ZigBee PRO uses the IEEE 802.15.4-2003 standard as the basis for the Physical (PHY) and Media Access (MAC) layers, while defining a specification for layers above the MAC layer, whereas the ZigBee RF4CE uses the IEEE 802.15.4-2006 standard. As of 2011, over 55% of IEEE 802.15.4-compliant devices in the market were ZigBee devices and growing. The ZigBee Alliance has worked along with the IEEE 802.15.4 standard to design and define the entire protocol stack for the ZigBee communication standard [7].

2.3. IEEE 802.15.4

The IEEE 802.15.4-2006 standard [13] defines the Physical (PHY) and Media Access Control (MAC) layers for Low-Rate Wireless Personal Area Networks (LR-WPANs) also popularly known as ZigBee. These technologies are suited for operation in data sensors, wireless automation, or other applications that do not require high data rates, such as high-quality video teleconferencing. We can compare this to the IEEE 802.11 family of technologies that operate at much higher data rates and can readily support bandwidth-intensive applications. The IEEE 802.15.4-2006 standard is a revision to the IEEE 802.15.4-2003 standard, which is the primary technology employed in ZigBee products [7]. The main objectives of IEEE 802.15.4 include:

- Easy user installation
- Reliable transfer of data
- Low cost
- Short range
- Low power consumption
- Simple, flexible protocol design and implementation

These objectives are essential to the commercial viability of IEEE 802.15.4-compliant products. WPAN technologies often exist on small devices that exhibit or desire these characteristics for an acceptable user experience. The IEEE 802.15.4 has defined several key technical characteristics including the followings:

- Wireless data rates ranging from 20 to 250 kbps
- Peer-to-peer or star topology operation

- Flexible 16- or 64-bit addressing schemes
- Optional support for allocating guaranteed time slots (GTS)
- Carrier sensing multiple access with collision avoidance (CSMA/CA) media access method
- Reliable protocol features, including full acknowledgments
- Low power consumption
- Energy level detection
- Link quality estimation and indication
- 16 channels defined in the 2.4 GHz band, 30 channels defined in the 915 MHz band, 3 channels defined in the 868 MHz band

The IEEE standard along with the ZigBee Alliance is working to specify the entire protocol stack. The IEEE 802.15.4 standard focuses on the specifications of the lower two layers of the protocol stack i.e. the physical and the data link layers. On the other hand, ZigBee Alliance aims to provide the specifications for the upper layers of the protocol stack i.e. from network to the application layers, for interoperable data networking, security services and control solutions for a range of wireless homes & buildings, interoperability compliance testing, marketing of the standard and advanced engineering for the evolution of the standard. This will assure the consumers to buy the products from different manufacturers with confidence that the products will work together [8].

2.4. Description of Current ZigBee Systems

Based on the IEEE 802.15.4 standard, ZigBee is currently the de facto standard for wireless sensor networks (WSNs) [1]. Its design focuses on the field of low-power, low-cost, and low-bit rate communications, which has been widely used in sensor networks, cyber-physical systems, and smart buildings. The IEEE 802.15.4 committee started working on a low data rate standard and later decided to join forces with ZigBee Alliance and ZigBee is the commercial name for this technology.

The ZigBee technology began to be conceived around 1998, when many installers realized that both Wi-Fi and Bluetooth were going to be unsuitable for many applications. In particular, many engineers saw a need for self-organizing ad-hoc digital radio networks [9]. ZigBee is a wireless mesh network specification (or protocol) that is built on top of the IEEE 802.15.4 short-range communications standard. The name ZigBee is originated from the fact that bees can dance to pass messages to each other, also in a multihop fashion. Amongst all the different cutting edge technologies today, ZigBee is considered one of the most popular wireless mesh networking standards for communication in a wireless personal area network (WPAN), which has been called the "Internet of Things".

ZigBee is usually targeted towards automation and remote control applications. ZigBee is one of the most widely used communication protocols of the Internet of Things (IoT), for transmitting information in a wireless mesh network between sensors and/or actuators, and for network connectivity which enables devices to connect and exchange data with each other. Theoretically, your ZigBee-enabled coffee maker can communicate with your ZigBee-enabled toaster. ZigBee focuses on the field of low-power, low-cost,

and low-bit rate communications, which has been widely used in sensor networks, cyber-physical systems, control systems and smart buildings. It is widely used in a large number of applications today, a few of which are as follows:

- Home and office automation
- Industrial automation
- Medical monitoring
- Low-power sensors
- HVAC control
- Plus many other control and monitoring uses

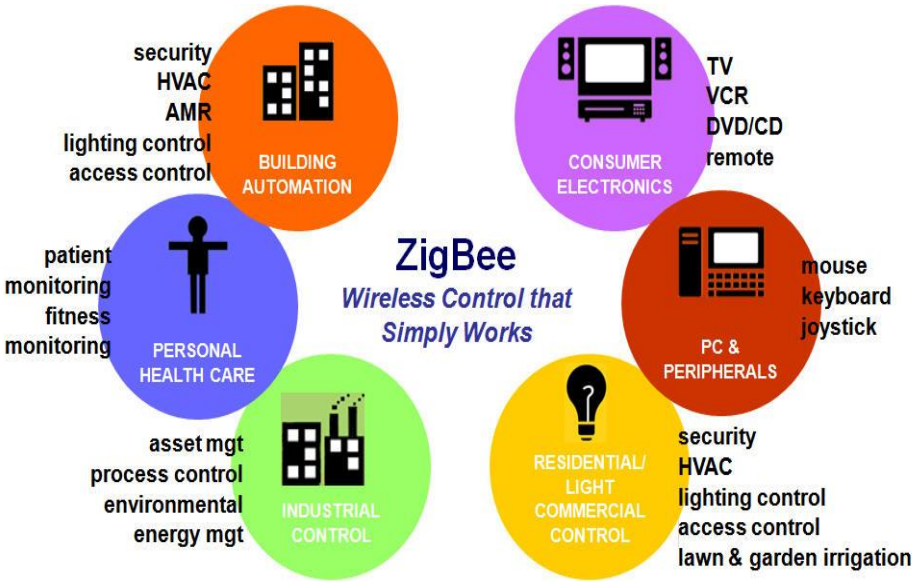


Figure 2.2. ZigBee applications [10]

The ZigBee RF4CE standard enhances the IEEE 802.15.4 standard by providing a simple networking layer and standard application profiles that can be used to create interoperable multi-vendor consumer electronic solutions. ZigBee incorporates the upper layers of the protocol stack, while IEEE 802.15.4 is in charge of MAC and PHY layers. ZigBee is intended for low-throughput, low-power, low-cost applications, so it is much simpler than other wireless personal area network protocols such as Wi-Fi (IEEE 802.11) and Bluetooth (IEEE 802.15.1) [9]. It has the support for mesh topologies, which means that ZigBee devices relay messages for each other through multiple wireless hops.

ZigBee operates in one of the industrial, scientific and medical (ISM) radio bands: 2.4 GHz in most jurisdictions worldwide and some devices also use 784 MHz in China, 868 MHz in Europe and 915 MHz in the USA and Australia, however even those regions and countries still use 2.4 GHz for most commercial ZigBee devices for home use, with data rates varying from 20 kbit/s (868 MHz band) to 250 kbit/s (2.4 GHz band). In our research work we focus on the commercially operated ZigBee, which operates in 16 channels of the 2.4GHz ISM band with a defined data rate of 250kbit/s, which is best suited for intermittent data transmissions from a sensor or input device. Its low power consumption limits transmission distances to 10–100 meters line-of-sight, depending on power output and environmental characteristics. ZigBee devices can transmit data over long distances by passing data through a mesh network of intermediate devices to reach more distant ones. It is typically used in low data rate applications that require long battery life and secure networking.

2.5. ZigBee Network Devices

ZigBee operates in three different network topologies. Along, with the star topology the ZigBee network layer also supports various other complex topologies like the tree and the mesh network topologies. A ZigBee network uses two different types of network devices: a full function device (FFD) and a reduced function device (RFD). All FFDs can communicate with RFDs or other FFDs, but RFDs can only communicate with FFDs. Because of this definition, RFDs are considered as simple devices and some examples of them include passive sensors that do not send large volumes of data or coordinate network functions among multiple devices. In a WPAN, there must be at least one FFD and FFDs can operate in three modes, while the RFDs can only operate in one mode. The FFD modes are as follows:

- **PAN Coordinator:** it is one of the most powerful devices in a ZigBee network. It is responsible for the initial Personal Area Network (PAN) setup and principal coordinator. There will be a single coordinator in each network and it is this node that creates the network while the other nodes simply join in. In a WSN this node usually acts as a sink which gathers all the data that is transmitted. Assigning short addresses is one of the tasks performed by a PAN coordinator.
- **Router/ Coordinator:** these are the intermediate devices in a network and they relay packets and messages for other nodes in the network. They usually join an already existing network and announce or indicate it using beacons. Thus, they can have “children” nodes that join the network by establishing communication with the router.

- **End Devices:** these are the simplest devices in a network. They cannot forward nor can they relay packets or messages in a network. They do not have children nodes that depend on them and when not in operating mode they usually enter into sleep mode in order to save energy.

In a ZigBee network there are two types of data transactions that take place between the devices as follows:

- In the first method the data is transferred between a coordinator and a device, in which a device transmits the data to or receives the data from a coordinator. This method is usually used in a star topology network.
- In the second method the data is transferred between two peer devices. In a peer-to-peer topology, data is exchanged between any two devices in the network; consequently all three transactions are used in this topology.

2.6. ZigBee Network Topologies

2.6.1. Star Topology

In a star topology network communications between the devices is established through a single central coordinator, known as the PAN Coordinator. Simply stated all the devices can communicate only via the PAN coordinator FFD, and all-star topologies operate independently from each other. While the PAN Coordinator is mostly powered by the main power supply, the devices are most likely to be battery powered. This type of topology is advantageous to applications like home automation, personal computer (PC) peripherals, toys and games.

2.6.2. Peer-to-Peer Topology

A peer-to-peer topology network also contains a PAN Coordinator but in contrast to a star topology network any device can communicate with any other device as long as they are in range of one another or in other words FFDs can communicate directly to each other, while the RFDs must exchange communications with the PAN Coordinator only. A peer-to-peer network can be ad hoc, self-organizing and self-healing. This type of topology is advantageous to applications such as industrial control and monitoring, wireless sensor networks, and asset and inventory tracking. A peer-to-peer topology also allows multiple hops to route the messages from any device to any other device in the network. It can provide reliability by multipath routing.

2.6.3. Cluster-Tree or Tree Topology

A Cluster-tree network is a special case of the peer-to-peer network in which most of the devices are FFDs and an RFD can connect to a cluster-tree network as a leaf node at the end of a branch. Any of the FFDs can act as a coordinator and provide synchronization services to other devices and coordinators, but only one of these coordinators can be the PAN coordinator. The PAN coordinator forms the first cluster by establishing itself as the cluster head (CLH) with a cluster identifier (CID) of zero, by choosing an unused PAN identifier, and broadcasting it using beacon frames to the neighboring devices. A candidate device receiving a beacon frame may request to join the network at the CLH. If the PAN coordinator permits the device to join, it will add this new requesting device as a child device in its neighbor list and the newly joined device will add the CLH as its parent in its neighbor list and begin transmitting periodic beacons such that the other candidate devices may then join the network at that device. Once the

network or the application requirements are met, the PAN coordinator can instruct a device to become the CLH of a new cluster adjacent to the first one. The advantage of this clustered structure is the increased coverage area at the cost of increased message latency. Figure 1.2 illustrates the different types of devices and topologies considered.

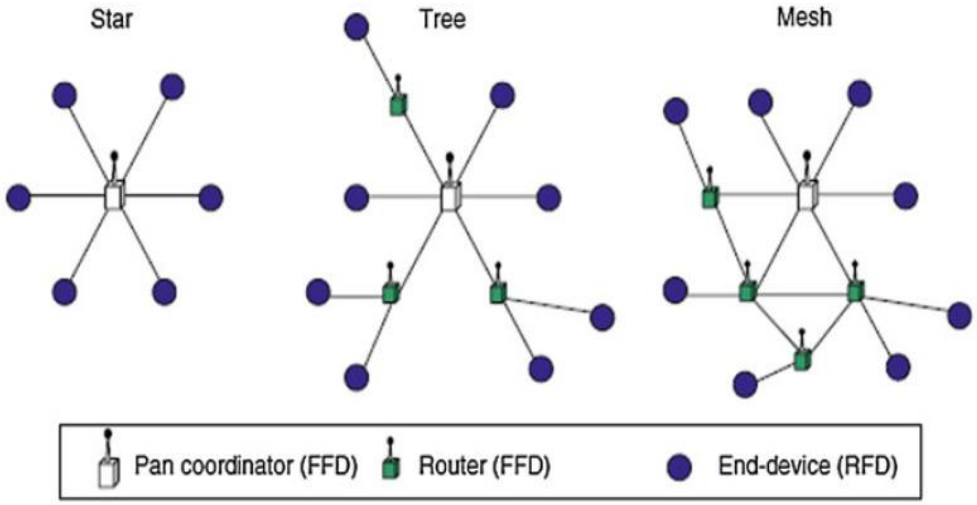


Figure 2.3. ZigBee network topologies [1]

2.7. How ZigBee Works?

In a ZigBee network digital radios are used to allow the devices to communicate with one another. As previously mentioned a ZigBee network consists of different types of devices- a coordinator, route and an end device. Every ZigBee network must contain a network coordinator. The network coordinator is a device that establishes as well as handles the entire network. It is aware of all the nodes that are present within its network and also maintains information about them. It is knowledgeable about the information that is being transmitted and received within its network. In a ZigBee network there are other Full Function Devices (FFD) present as well and these can serve as either network coordinators, network routers or just as devices that interact with the physical world. In a

ZigBee network a Reduced Function Device (RFD) just serves as a device which only interacts with the outside world.

As previously mentioned a ZigBee network supports several network topologies including the star, mesh and cluster tree network topologies. A star network topology is most useful when there are several end devices present in the network and they are located close together, so that they can communicate with a single router node. Then this node can be a part of a larger mesh network that communicates with the network coordinator. In contrast, mesh networking allows for redundancy in the node links, so that if one node goes down then the devices can find an alternative path to communicate with one another [10].

3. ZIGBEE LAYERED ARCHITECTURE

The ZigBee communications standard has a layered architecture as depicted in Figure 3.1. As previously mentioned it is built on top of the IEEE 802.15.4 short range communications standard, due to which the architecture of ZigBee is divided into two main sections depending on which standard or communications entity specifies or handles the functionalities or operations of a layer. The IEEE 802.15.4 standard specifies the functions and operations for the Physical (PHY) and Media Access Control (MAC) layers, whereas the ZigBee standard (or ZigBee Alliance) specifies the functionalities and the operations for the remaining layers in the system architecture - the network layer, the ZigBee device object (ZDO), the application sublayer, and security management.

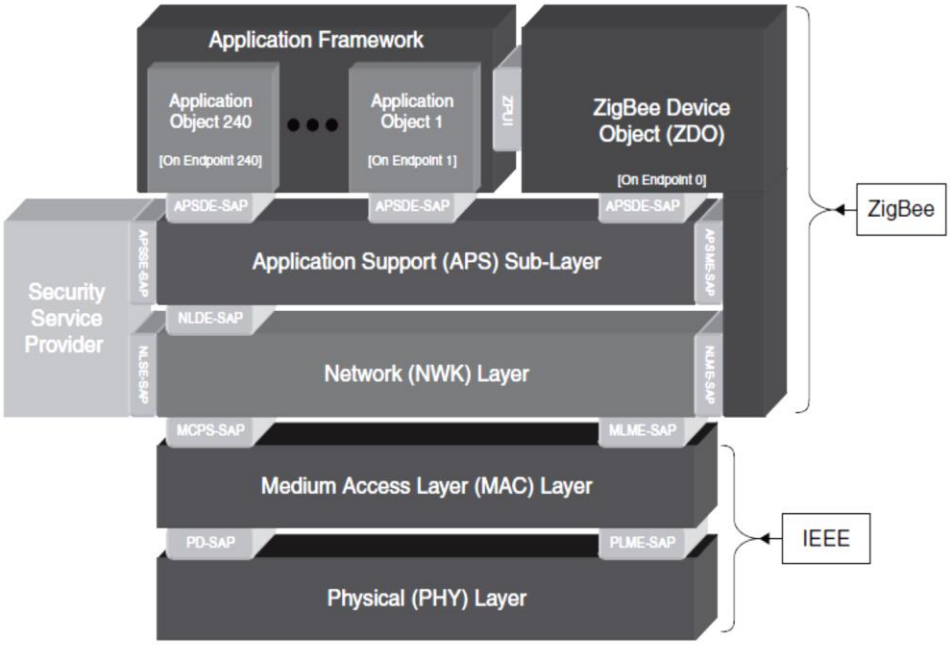


Figure 3.1. ZigBee layered architecture [11]

3.1. The IEEE 802.15.4 Physical Layer

The IEEE 802.15.4 standard builds on the functionalities and the operations for the ZigBee PHY layer. The Physical Layer was designed to accommodate the need for low cost wireless networking yet allowing for a high level of integration. The application of direct sequence spread spectrum allows the analog circuitry to be very simple and makes it very free and easy going towards inexpensive implementations [9]. It acts as an interface between the MAC sublayer and the physical radio channel, through the RF firmware and the RF hardware.

The Physical Layer provides two types of services: the PHY data service and the PHY management service interfacing with the physical layer management entity (PLME). The PHY data service implements the transmission and reception of the PHY protocol data units (PPDU) across the physical radio channel. Figure 3.2 illustrates the two service access points (SAPs) of the PHY layer which are used to interact with the local MAC layer and remote PHY/MAC layers: the PHY data service access point (PD-SAP) and the physical layer management entity SAP (PLME-SAP).

The PD-SAP supports the transport of data, through the MAC protocol data units (MPDUs), while the PLME-SAP enables the management and coordination with the MAC layer. The service-specific convergence sublayer (SSCS) is defined above the MAC layer to handle specific services and functions. For example, the ZigBee Alliance describes specific SSCSs and network layers to support their desired applications [7]. The IEEE 802.2 Logical Link Control (LLC) can also be employed above the SSCS to act as a common interface to any of the higher layer protocols that may be implemented on a device.

The PHY layer also includes the following functionalities: activation/deactivation of the RF transceiver, energy detection within a defined channel, link quality estimation for received packets, clear channel assessment for CSMA/CA, channel frequency selection, as well as data transmission and reception.

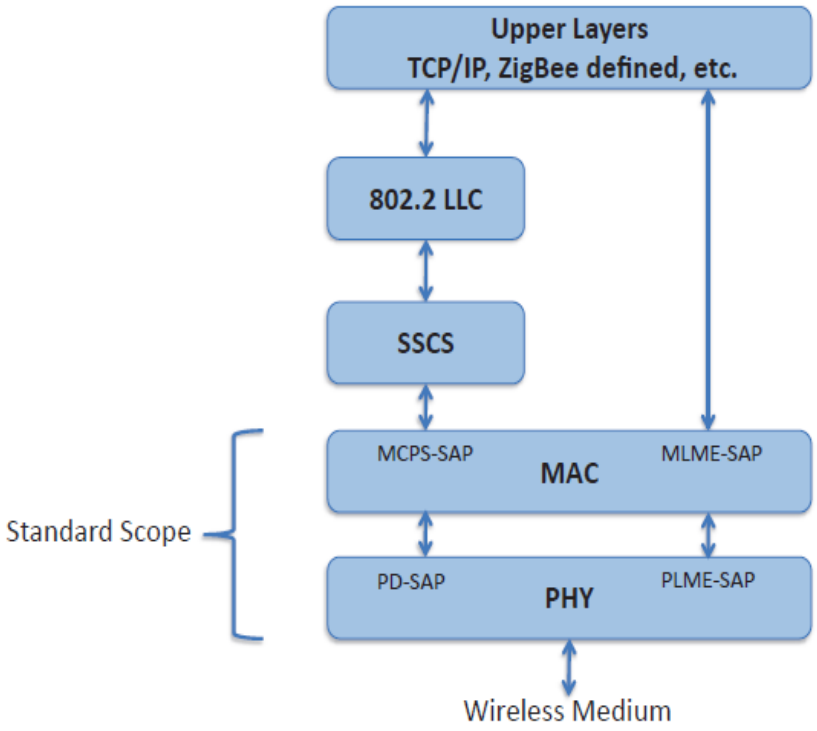


Figure 3.2. PHY layer service access points [7]

The IEEE 802.15.4-2006 standard defines four PHY schemes as follows:

- Direct sequence spread spectrum (DSSS) with binary phase-shift keying (BPSK) modulation in the 868 MHz (20 kbps data rate) and 915 MHz (40 kbps data rate) frequency bands
- DSSS offset quadrature phase-shift keying (O-QPSK) modulation in the 868 MHz (100 kbps) and 915 MHz (250 kbps) frequency bands

- Parallel sequence spread spectrum (PSSS) BPSK and amplitude shift keying (ASK) modulation in the 868 and 915 MHz bands (250 kbps for both bands)
- DSSS O-QPSK modulation in the 2.4 GHz (250 kbps) band- and for our research work we implement our system based on this PHY modulation scheme

The initial IEEE 802.15.4-2003 specification defined a BPSK PHY in 868 and 915 MHz bands operating at 20 and 40 kbps, respectively, and an O-QPSK PHY in the 2450 MHz frequency band. These specifications form the basis for the ZigBee enabled devices designed today. Table 3.1 [7] [12] summarizes the frequency bands and data rates for IEEE 802.15.4-2006. The higher data rate at 2.4GHz is attributed to a higher-order modulation scheme. Low frequencies provide longer range due to lower propagation losses. Also, low data rate can be translated into better sensitivity and larger coverage area whereas higher data rate means higher throughput, lower latency or lower duty cycle [1].

Table 3.1. Frequency bands and data rates [12]

PHY (MHz)	Frequency band (MHz)	Chip rate (kchips/s)	Modulation	Bit rate (kbps)	Symbol rate (ksymbols/s)	Symbols
868/915	868–868.6	300	BPSK	20	20	Binary
	902–928	600	BPSK	40	40	Binary
868/915	868–868.6	400	ASK	250	12.5	20-bit PSSS
(optional)	902–928	1600	ASK	250	50	5-bit PSSS
868/915	868–868.6	400	O-QPSK	100	25	16-ary
(optional)	902–928	1000	O-QPSK	250	62.5	16-ary
2450	2400–2483.5	2000	O-QPSK	250	62.5	16-ary

For more details concerning the IEEE 802.15.4 physical layer, see Appendix A Section1.

3.2. The IEEE 802.15.4 MAC Layer

The functionalities and operations of the Media Access Control (MAC) layer in ZigBee, is specified by the IEEE 802.15.4-2006 standard. The MAC layer is located between the physical and network layers in the architectural design. The MAC layer allows a network to be formed, for channels to be shared, and for data to be transferred in a reasonably reliable way between the physical and the network layers. The MAC layer as specified by the IEEE 802.15.4-2006 standard is divided into two parts: the MAC common part sublayer (MCPS) and the MAC layer management entity (MLME). Some of the functions as handled by the MAC layer are as follows [7]:

- Coordinator generation of network beacons
- Synchronization to network beacons
- Support of PAN association and disassociation
- Security
- CSMA/CA channel access mechanism
- Handling/maintaining guaranteed time slot (GTS) availability to devices
- Maintaining a reliable link between peer devices (at the MAC layer)

The MAC layer depicts a high level architecture as illustrated in Figure 3.3. The MLME segment of the MAC layer contains the MAC PIB, which is a set of attributes that can be accessed or set through the MLME by either one of its two SAPs. There are two primary services provided by the MAC layer as follows:

- Data service, which can be accessed through the CPS and associated SAPs (MCPS, PD)

- Management, which can be accessed through the MLME-SAP

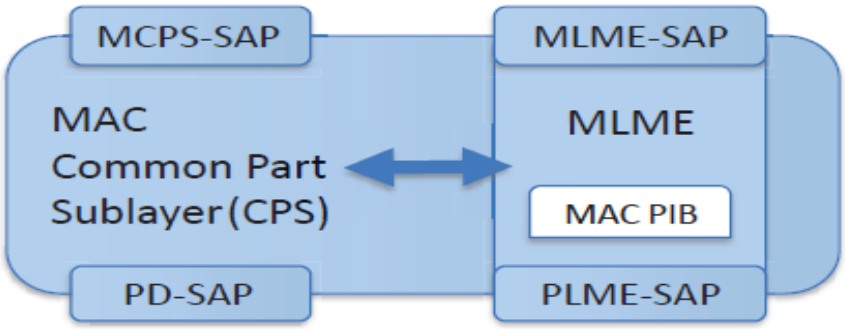


Figure 3.3. MAC layer architecture [7]

The PD-SAP and PLME-SAP act as an interface to the PHY layer, while the MCPS- and MLME-SAP interfaces to a service-specific convergence sublayer (SSCS) such as defined by the ZigBee specification [13]. The data units at the SSCS are passed in the form of SSCS protocol data units (SPDUs) between peer SSCS entities. It should be noted that these SPDUs are encapsulated in the MAC service data units (MSDUs) that are handled by the MAC layer.

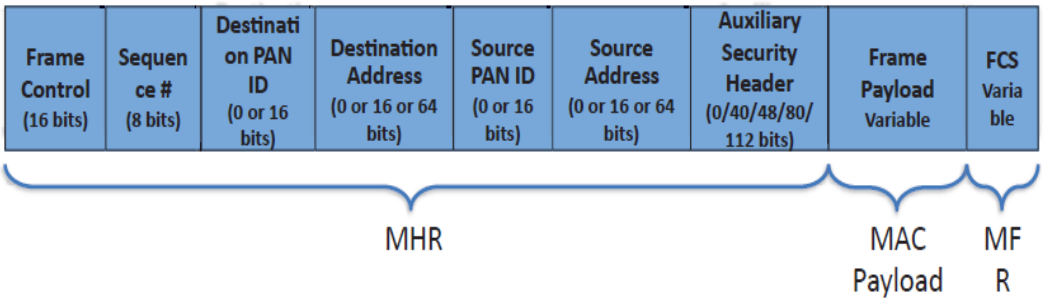


Figure 3.4. MAC frame format [7]

Figure 3.4 illustrates the generalized MAC frame format. The MAC frame header (MHR) consists of the frame control field, sequence number, destination PAN ID, destination

address, source PAN ID, source address, and auxiliary security header. The MAC payload contains the frame payload, which contains information from the higher layers including the user data, and the MAC footer (MFR), which contains the frame check sequence [7].

- Frame control indicates the type of frame, addressing fields, and other control flags. There are four primary types of frames supported by the MAC layer: beacon, data, acknowledgment, and MAC command. Not all the frames will contain all the fields mentioned.
- The sequence number field indicates a sequence ID for each frame. For beacon frames, it specifies a beacon sequence number (BSN), while for data, acknowledgment, or MAC command frames; it specifies a data sequence number (DSN).
- When present, the destination PAN ID field indicates the unique ID of the PAN identifier for the intended receiver.
- When present, the destination address is the unique address ID for the receiver device.
- When present, the source PAN ID field specifies the unique ID of the PAN identifier for the transmitter.
- When present, the source address is the unique address ID for the transmitter device.
- When present, the Auxiliary Security Header field provides information to be processed by security mechanisms, including frame protection (security-level) information and which keying is used from the MAC security PIB.

- The Frame Payload field contains the information specific to the four types of frames. This could include user data, beacon identifier information, or MAC commands.
- The frame check sequence (FCS) field is 16 bits long and uses an ITU-T cyclic redundancy check (CRC) that is calculated over the MHR and MAC payload frame portions. It is used for error detection.

The MAC layer also, handles the MAC Command frames which act as a primary method to provide MAC control in the IEEE 802.15.4 standard. There are nine MAC command frames employed as follows:

- Association Request – employed to request an association to a PAN through a PAN coordinator or a coordinator
- Association Response – the PAN coordinator or a coordinator get to respond via this command to an association request
- Disassociation Notification – this command is employed to indicate a device disassociation from a PAN by either a PAN coordinator, coordinator or by an associated device
- Data Request – usually sent to a device to request data from a PAN coordinator or coordinator
- PAN ID Conflict – employed by a device to indicate to a PAN coordinator when a PAN ID is already used or in a conflict
- Orphan Notification – used by an associated device which has lost synchronization with the coordinator

- Beacon Request – used by a device to locate all the coordinators within a range during the scanning process
- Coordinator Realignment – sent by a PAN coordinator or coordinator following the receipt of an orphan notification or when there are any changes to the PAN configuration attributes
- Guaranteed Time-slot (GTS) Request – employed by an associated device to request allocation of a new GTS or deallocation of an existing GTS from a PAN coordinator

The MAC layer along with these command frames performs a number of functions and handles multiple operations such as MAC data transfer, device association and disassociation, PAN formation message exchange for FFD and much more. Additional relevant information is provided later in this thesis.

While the IEEE 802.15.4-2003 standard defines the PHY and MAC layers for ZigBee, similarly the ZigBee stack layers above the MAC layer are defined by the ZigBee Alliance. The ZigBee stack layers are similarly based on the OSI 7-layer model. It only incorporates the functionalities that are required in the intended markets [10].

3.3. The ZigBee Network Layer

The Network (NWK) layer connects the IEEE 802.15.4 MAC layer to an associated APL layer and ensures proper operation of the MAC layer. It natively supports the star and tree network topologies, as well as the generic mesh network topology. Among other functionalities it is the network layer at which wireless networks are formed, joined, left and discovered. Similar to the PHY and MAC layers the NWK layer

also contains two primary service entities: one for passing data and the other for management. They are known as the network layer data entity (NLDE) and the network layer management entity (NLME). SAPs are defined to connect the entities to the MAC layer. The NLDE provides the following services:

- Generation of network-level PDUs (NPDUs)
- Routing based on network topology

The NLME provides the following services:

- New device configuration
- Network start up
- Joining, leaving, and re-joining a network
- Addressing
- Neighbor device/ node discovery
- Route discovery
- Reception control
- Routing

When a coordinator attempts to establish a ZigBee network, it first does an energy scan to find the most suitable RF channel for its new network. When it finds a channel, the coordinator assigns the logical network identifier, also known as the PAN ID, to all devices that join the network. A node or a new device can join the network either directly or through association. To join directly, a system designer must add the node's extended address into the neighbor table of the device. The direct joining device will initiate an orphan scan, and the node with the matching extended address (in its neighbor table) will

respond to it, allowing the device to join. To join by association, a node must send out a beacon request on a channel, repeating it on other channels as well until it finds a suitable network to join. The network layer also ensures the security of a network, thus ensuring both authenticity and confidentiality of a data transmission [10].

3.4. The ZigBee Application (APL) Layer

The APL layer as defined by the ZigBee Alliance is made up of many sublayers as illustrated in Figure 3.5. The Application Support Sublayer (APS), the Application Framework and the ZigBee Device Object layers (ZDO) together form the Application layer for ZigBee. The manufacturer-defined application objects are also present at this layer in order to provide the application-specific functionality using ZigBee. There are two services supported at this layer: data and management. Similar to the NWK layer, this layer also has two service entities: the application layer service data entity (APSDE) and the application layer service management data entity (ASMDE).

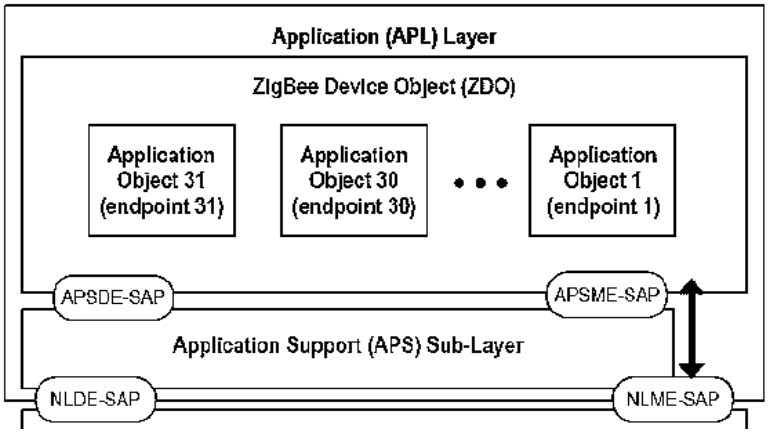


Figure 3.5. Application layer components [10]

For more details concerning the various sublayers of the Application layer, see Appendix A Section 2.

4. MODULATION SYSTEMS AND MULTIPLE ACCESS TECHNIQUES USED IN A ZIGBEE NETWORK

4.1. Types of Modulation Systems Used in a ZigBee Network

The IEEE 802.15.14-2003 PHY layer manages various functions such as activation and de-activation of the RF transceiver, channel assignment and switching, receiver energy detection, link quality indication and clear channel assessment. Along with these many functions that it performs, the PHY layer is also responsible for the transmission and reception of data across the physical radio channel. There are a total of 27 channels defined in ZigBee, with one channel in the 868 MHZ frequency band, ten channels in the 915 MHz and sixteen channels in the 2450 MHZ frequency band. These channels are numbered 0 to 26 using the following method, where k denotes the channel number:

$$F_c = 868.3\ MHz, \quad for\ k = 0 \tag{4.1}$$

$$F_c = 906 + 2(k-1)\ MHz, \quad \text{k} = 1, 2, \ldots\ldots..10 \tag{4.2}$$

$$F_c = 2405 + 5(k-11)\ MHz, \quad \text{k} = 11, 12, \ldots\ldots.26 \tag{4.3}$$

Since ZigBee can operate in different frequency bands, any of these channels within a particular network's band can be used for data transmission but the PAN coordinator in each network determines which channel will be used. The coordinator device will first perform an active scan to locate other networks, and assess the peak energy level on each channel to choose the most suitable one for its network. Then the function of channel assignment is performed by the PHY layer using its channel assignment functionality [14].

In ZigBee before any data or information can be transmitted over the channel, the data first has to be modulated. There are different modulation schemes employed depending on which frequency band is used. The IEEE 802.15.4-2006 defines four different PHY schemes for modulation in ZigBee depending on the frequency band and data rates employed as follows:

- In the 868 MHz and 915 MHz frequency bands, ZigBee employs the Direct Sequence Spread Spectrum (DSSS) with Binary Phase Shift Keying (BPSK) modulation scheme with a data rate of 20 kbps and 40 kbps respectively. More details are provided in Appendix A section 3.
- In the 868 and 915 MHz frequency bands, ZigBee employs the Parallel sequence spread spectrum (PSSS) BPSK and amplitude shift keying (ASK) modulation scheme with a data rate of 250kbps each. More details are provided in Appendix A section 3.
- In the 868 MHz (100 kbps) and 915 MHz (250 kbps) frequency bands, ZigBee employs the DSSS with offset quadrature phase-shift keying (O-QPSK) modulation scheme with a data rate of 100kbps and 250 kbps respectively
- In the 2.4 GHz frequency band, ZigBee employs the DSSS O-QPSK with a data rate of 250kps. This modulation scheme is what we will be using for developing and implementing our new ZigBee system.

4.1.1. 868/915 MHz O-QPSK PHY Modulation Scheme

This modulation scheme operates at a data rate of 100 kbps and employs a16-ary modulation scheme. In this method for each data symbol that is transmitted there are four

information bits utilized to choose one of the sixteen PN sequences. These PN sequences are then concatenated together, and later the resulting combined sequence is modulated using O-QPSK. Figure 4.1 illustrates the block diagram of an 868/915 MHz O-QPSK PHY Modulation Scheme.

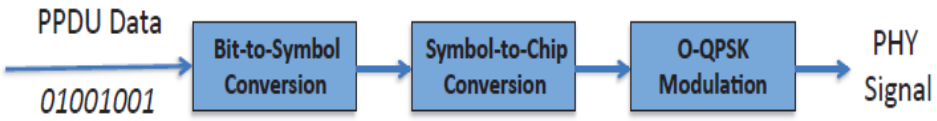


Figure 4.1. 868/915 MHz O-QPSK PHY modulation scheme [7]

The IEEE 802.15.4-2006 standard defines a table illustrating the data mapping between the data symbols and the associated chip values for the 868/915 MHz O-QPSK PHY Modulation Scheme. These PN sequences are modulated on the O-QPSK carrier with a half-sine pulse-shaping method. In this method the chips are numbered (from 1 to 16), and the chips that are even numbered are modulated on the in-phase (I) carrier while the odd numbered chip values are modulated on the quadrature phase (Q) carrier. The chip rate for an 868 MHz frequency band is 400kchips/s and 1Mchips/s for a 915 MHz frequency band. When compared to the I-phase chips the Q-phase chips are delayed by a single chip period.

4.1.2. 2450 MHz O-QPSK PHY Modulation Scheme

ZigBee most frequently operates in the commercially available industrial, scientific and medical (ISM) frequency band at 2450 MHz in most jurisdictions worldwide. This modulation scheme uses a data rate of 250 kbps and employs a 16-ary modulation scheme with O-QPSK, which is similar when compared with the 868/915

MHz O-QPSK PHY modulation scheme, except that the PN chips in this method are 32-bits long instead of 16-bits. For our research work we focus on ZigBee operations only in this frequency band.

4.2. PHY Protocol Data Unit (PPDU)

Before we can understand more about how the modulation scheme operates it is important to know about the primary data unit that holds the data in the PHY layer. These data units are known as the PHY protocol data unit (PPDU). The schematic view of the PPDU is illustrated in Figure 4.2.

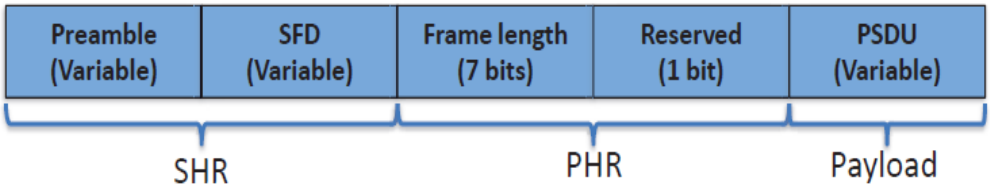


Figure 4.2. Schematic view of PPDU [7]

Each PPDU packet consists of three basic components as follows:

- Synchronization header (SHR), which allows a receiver or a receiving device to synchronize and lock onto the bit stream
- PHY header (PHR), which contains frame length information
- A variable length payload, which contains the frame from the MAC sublayer. It also contains other layer headers and user data

For more information concerning the content of the PPDU, see Appendix A Section 3.

4.3. Modulation and Data Spreading

In a ZigBee network once a message or data is ready for transmission, it first has to be modulated before it can be transmitted across the network. ZigBee employs a direct sequence spread spectrum (DSSS) technique that uses a digital spreading function representing pseudorandom noise (PN) chip sequences, to improve the signal-to-noise ratio (SNR) of the received signals at the receiver [1]. In a PN code the bits are also referred to as chips, thus a PN code is also known as a PN chip sequence. Each data symbol in ZigBee is presented using predefined chip sequences.

At the sender side of the data transmission, before the bit sequences can be modulated and transmitted through the antenna there is an additional process of grouping or breaking down the sequences into symbols and then replacing each symbol with its corresponding PN chip sequence, which will be modulated to the baseband transmission waveform and finally up-converted and transmitted over the air.

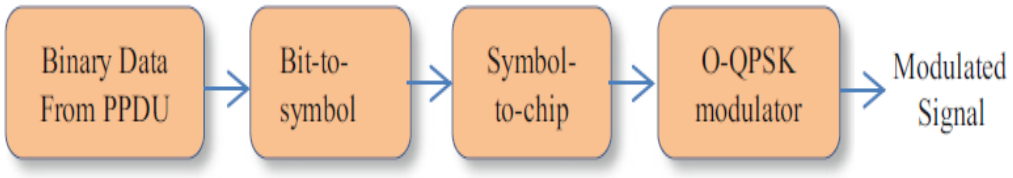


Figure 4.3. Modulation and spreading function [1]

Figure 4.3 illustrates the modulation and spreading function employed in ZigBee. The binary data from PPDU is nothing but the bit sequences as obtained from the PPDU. The data from the PPDU is sent out as bytes and these outgoing bytes are then applied to the bit-to-symbol conversion block as illustrated. These outgoing bytes are then divided into

two 4-bit symbols each; by grouping the 4 least significant bits as one symbol (LSB) and the 4 most significant bits into another symbol (MSB). Each 4 bit symbol is then spread into its corresponding 32-bit long PN sequences. The IEEE 802.15.4 standard predefines the map from 4-bit symbol to 32-bit chip sequences, as illustrated in Table 4.4. The radio then encodes these chip sequences using orthogonal quadrature phase shift keying (O-QPSK) and transmits them at 2 Mchips/s (producing an effective data rate of 250 kbps). The O-QPSK PHY modulation scheme is employed when ZigBee is operating in the 2450 MHz frequency band.

For an example let us consider that we have one byte of binary data from the PPDU as $b_0 b_1 b_2 b_3 b_4 b_5 b_6 b_7$. This byte is then grouped into two 4-bit data symbols each as follows $b_0 b_1 b_2 b_3$ and$b_4 b_5 b_6 b_7$. Each 4-bit data symbol will then be spread into its corresponding 32-bit PN chip sequence, $C_0 C_1 C_2 \ldots \ldots C_{31}$ as predefined by Table 4.1 as specified by the IEEE 802.15.4 standard. Each bit or chip (C_i) in a PN sequence is then modulated using the 2450 MHz O-QPSK PHY modulation scheme. The modulated O-QPSK signal is then applied to the half-sine pulse shaping stage, followed by the digital–analog conversion block to convert the digital baseband waveform into an analog baseband waveform. The radio front-end up-converts the baseband waveform to 2.4 GHz carrier and finally transmits it by the radio frequency (RF) transmitter. The radio encodes these chip sequences using the orthogonal quadrature phase shift keying (O-QPSK) and transmits them at a data rate of 250 kbps [1].

Additionally the even numbered chips $C_0 C_2 C_4 \ldots \ldots$ are modulated as the In-phase (I) component of the carrier while the odd numbered chips $C_1 C_3 C_5 \ldots \ldots$ are modulated as the Quadrature (Q) phase component of the carrier. It should be noted that a chip valued

‘1’ is shaped into a positive half sine wave and a chip valued ‘0’ is shaped into a negative half sine wave as illustrated in Figure 4.4. The ‘O’ in the O-QPSK describes a half chip time offset. Since each chip has a duration of 1µs the offset time between the Q-phase and I-phase is half a chip time or in other words 1µs/2 = 0.5µs. This offset results in a continuous phase change and constant envelope.

Table 4.1. Symbol to chip mapping for 2450 MHz O-QPSK modulation scheme [1]

Data symbol (b_0 b_1 b_2 b_3)	Chip values (c_0 c_1 … c_{30} c_{31})
0000	(PN_1) = 11011001110000110101001000101110
1000	(PN_2) = 11101101100111000011010100100010
0100	(PN_3) = 00101110110110011100001101010010
1100	(PN_4) = 00100010111011011001110000110101
0010	(PN_5) = 01010010000101110110110011100011
1010	(PN_6) = 00110101001000101110110110011100
0110	(PN_7) = 11000011010100100010111011011001
1110	(PN_8) = 10011100001101010010001011101101
0001	(PN_9) = 10001100100101100000011101111011
1001	(PN_{10}) = 10111000110010010110000001110111
0101	(PN_{11}) = 01111011100011001001011000000111
1101	(PN_{12}) = 01110111101110001100100101100000
0011	(PN_{13}) = 00000111011110111000110010010110
1011	(PN_{14}) = 01100000011101111011100011001001
0111	(PN_{15}) = 10010110000001110111101110001100
1111	(PN_{16}) = 11001001011000000111011110111000

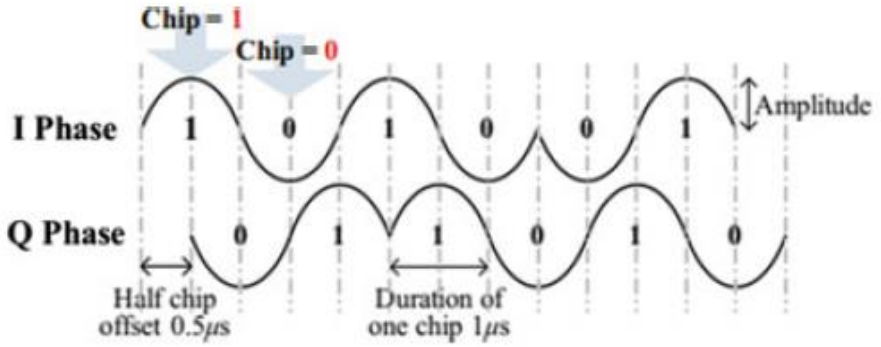


Figure 4.4. Half sine pulse shaping in O-QPSK [1]

4.4. Demodulation and Data De-spreading

During the process of demodulation the radio at the receiver's side converts each incoming half-sine pulse wave signals into PN chips. These PN chips are then grouped into PN sequences. The de-spreading process is performed by mapping these PN sequence to the symbol with the highest correlation. A correlator is responsible for separating out the PN-Codes amongst all of the chips that were received. The correlator captures chip sequences that are the same or similar to PN-Codes pre-defined in the Table 4.1 as specified by the IEEE 802.15.4 standard and later the correlator tries to find a best-match PN-Code for a received chip sequence.

In the case of an 'ideal' situation a best-match PN-Code should be exactly the same as the captured chip sequence but in the case of a real situation, it is a completely different story. While transmitting a sender should never transmit a wrong PN sequence or in other words a sender should not transmit a PN sequence which is not predefined in the PN table specified by the IEEE 802.15.4 standard. However some chips can become

corrupted while transmitting in the presence of an interference and multipath. Interference and noise can corrupt the incoming chip stream, thereby causing the 32-chip sequences to not match with any one of the 16 valid sequences as predefined in the table. In case of corrupted chips, however, the best-match PN-Code need not fully agree with the erroneous chip sequence.

There are many different methods that can be implemented to find a "best-match" PN-Code. One such method is Maximum Likelihood Decoder (MLD) where each received 32-bit chip sequence P is compared with the predefined PN-Codes $PN_1 PN_2 PN_3$ ... ... PN_{16} in Table 4.4 in order select the corresponding symbol such that the Hamming distance of P and the PN-code of the symbol is minimized. Here Hamming distance is the number of different positions of two bit strings. In case of a corrupted packet, the receiver maps the input sequence to the valid sequence with the smallest Hamming distance.

Apart from this the literature [15] mentions that some 802.15.4 radios (like the CC2420) enables users to control the correlation threshold so that they can control the maximum Hamming distance between the received 32-chip PN sequence and the valid SFD sequence that the receiver is willing to tolerate. If this threshold is high, the received signal must closely match with the ideal signal. Otherwise, the receiver will allow a low signal-to-noise (SNR) ratio at the expense of potentially interpreting corrupted packets or channel noise as valid packets. Based on the above understanding we summarize the whole process of spreading and dispreading as illustrated in Figure 4.5.

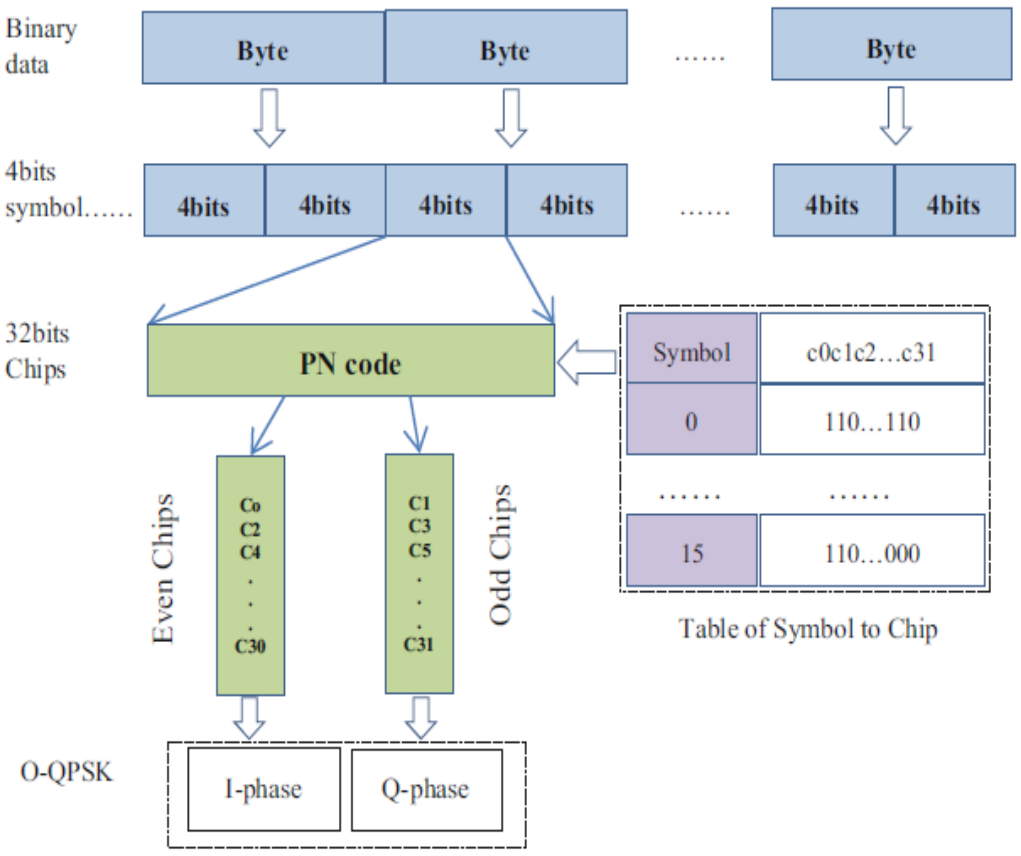


Figure 4.5. Flowchart of spectrum spreading and de-spreading [1]

4.5. Pseudorandom Sequences (PN)

A pseudorandom noise (PN) signal is similar to a noise signal which satisfies one or more of the standard tests for statistical randomness. Although PN signals do not have a definite pattern, these signals consist of a deterministic sequence of pulses that will repeat itself after a certain period of time. The pseudorandom sequence pattern is determined by a key and the repetition period can be very long, sometimes even millions of digits. There are many application areas today that use these periodic signals in their implementation. Some applications that depend on the PN sequences are cellular (mobile) telephones and base stations, GPS navigation systems, wireless Internet (Wi-Fi)

communications, Bluetooth communications protocol, satellite communications transmitters and receivers, deep space probes, satellite TV transmitters and receivers, garage door openers, wireless (residential) telephones, data scramblers, dither generators, timing recovery modules, system synchronization modules, noise generators, concert hall equalizers, and many more applications [16].

A PN sequence is a sequence of symbols (also known as chips), representing binary 1's and 0's. At a first glance a PN sequence appears to be just random noise and it also has many characteristics of a random noise signal. But if a person or an entity understands the "secret" or the "pattern" of these signals then each of these PN sequences are deterministic and can be generated, predicted, or even extracted from a signal easily. The time duration of a chip is usually much shorter than the time duration of a bit, due to which the bandwidth (or the spectrum) of a PN sequence is usually much greater than the bandwidth of the data.

The concept of PN sequences is used greatly in spread spectrum communications, especially in the Direct Sequence Spread Spectrum modulation (DSSS) technique to modulate the data by spreading the data greatly over the spectrum. This has many advantages, for example in the case of the output power of a transmitter, spreading out the bandwidth lowers the energy at any given particular frequency, especially near the apparent noise level, making it difficult to detect spread spectrum signals, if one is not aware of their presence. But instead at the same time if we have a receiver that "knows" the correct PN sequence, then the data from the spread spectrum signal can be easily separated from the noise and recovered. There are various other advantages of employing spread spectrum communications that include offering greater resistance to jamming or

interference signals, better performance in multipath environments, and providing the ability for multiple users (each having their "own" PN sequence) to simultaneously share the same frequency band (a technique called code division multiple access, or CDMA). PN sequences also provide precise ranging and timing measurements allowing for robust synchronization of data even in noisy environments.

4.6. Direct Sequence Spread Spectrum

Along with employing the O-QPSK modulation technique, the ZigBee communication standard also employs the Direct Sequence Spread Spectrum data spreading technique (DSSS) in order to improve the signal-to-noise ratio (SNR) of the received signals. The concept of data spreading and de-spreading was described in earlier sections of this chapter. DSSS also helps to minimize the effects of interference and fading and supports a larger cover range due to its low SNR requirement at the receiver [17].

4.7. Carrier Sense Multiple Access/ Collision Avoidance (CSMA/CA)

Along with handling various functions such as coordination of network beacons, managing access to the physical layer, reliable data transfer, and PAN association and disassociation the IEEE 802.15.4-2003 MAC sublayer also employs Carrier Sense Multiple Access/ Collison Avoidance (CSMA/ CA) and an optional superframe structure to provide channel access for multiple devices within the PAN.

4.7.1. Carrier Sense Multiple Access/ Collision Avoidance (CSMA/ CA) Algorithm

Carrier Sense Multiple Access with Collison Avoidance is a multiple access technique which is employed in various wireless communication standards today to transmit data across networks while at the same time trying to avoid collisions between two or more network links which are transmitting at the same time. An IEEE 802.15.4 network can operate in two modes: the Beacon enabled mode or in the Non-Beacon mode.

In the Beacon-enabled mode to control communications in the network, regular beacons are transmitted by the network coordinator for synchronization and association procedures. The data transfer between a device and a coordinator is synchronized in a superframe, which can have an active and as well as an inactive portion. All communications between the devices take place during the active period, and during the inactive period the nodes are allowed to enter a low-power mode. While operating in this mode the slotted CSMA/ CA technique is employed for contention access. The active period consists of a contention access period (CAP) and a contention-free period (CFP). The CFP is dedicated towards low-latency applications or towards those applications which require specific data bandwidth and it is formed by the guaranteed time slot (GTS). The CFP usually appears at the end of the active superframe starting at a slot boundary, immediately following the CAP [1]. Additional details of the superframe and its structure are given in Section 4.8.

In the Beaconless or Non-Beacon mode there are no regular beacons and the devices communicate with each other using the unslotted CSMA/CA protocol for channel access, in contrast to the beacon mode where slotted CSMA /CA protocol is used. In the

unslotted CSMA/ CA mode every time a device wants to transmit data frames or MAC commands, it has to wait for a random period of time for a channel to become idle – i.e., it performs a clear channel assessment (CCA) before transmitting. If a channel is found to be idle following the random back-off period, the device transmits the data. If the channel is found to be busy even after the random back-off period, then the device has to wait for another random period before trying to access the channel again. Acknowledgment frames are sent to identify successful data transmissions. If the acknowledgement frames are not received then the transmission is assumed to have failed. In such cases, a random back-off period is chosen, and the device waits for the period before performing another CCA to identify an idle channel and begin retransmitting the data. For our thesis we consider the ZigBee system operating in the beacon mode [14].

During the mode of operation where slotted CSMA/CA is employed, the back-off periods of one device is aligned with the start of the beacon transmission. Every time a device wants to transmit data frames during the CAP, it has to locate the boundary of the next back-off period and then wait for a random number of back-off periods. If the channel is found to be idle, then the device begins transmitting on the next available back-off period boundary. In conclusion, the status switching in slotted CSMA/CA should be related with the slots arrangement [1].

While the classical CSMA/CA protocol uses binary exponential back-off, in practice some CSMA/CA protocol implemented in TinyOS uses a fixed length back-off interval [18]. Also, at the same time, IEEE 802.15.4 does not employ RTS/CTS since the normal packet has a short packet length, when compared with IEEE 802.11. This RTS/CTS overhead proves to be useful when traffic load is high, but obviously too

expensive for low-data rate applications as of the case of WPANs for which IEEE 802.15.4 is designed [1]. The CSMA /CA algorithm can be illustrated using a flowchart as represented in Figure 4.6 below.

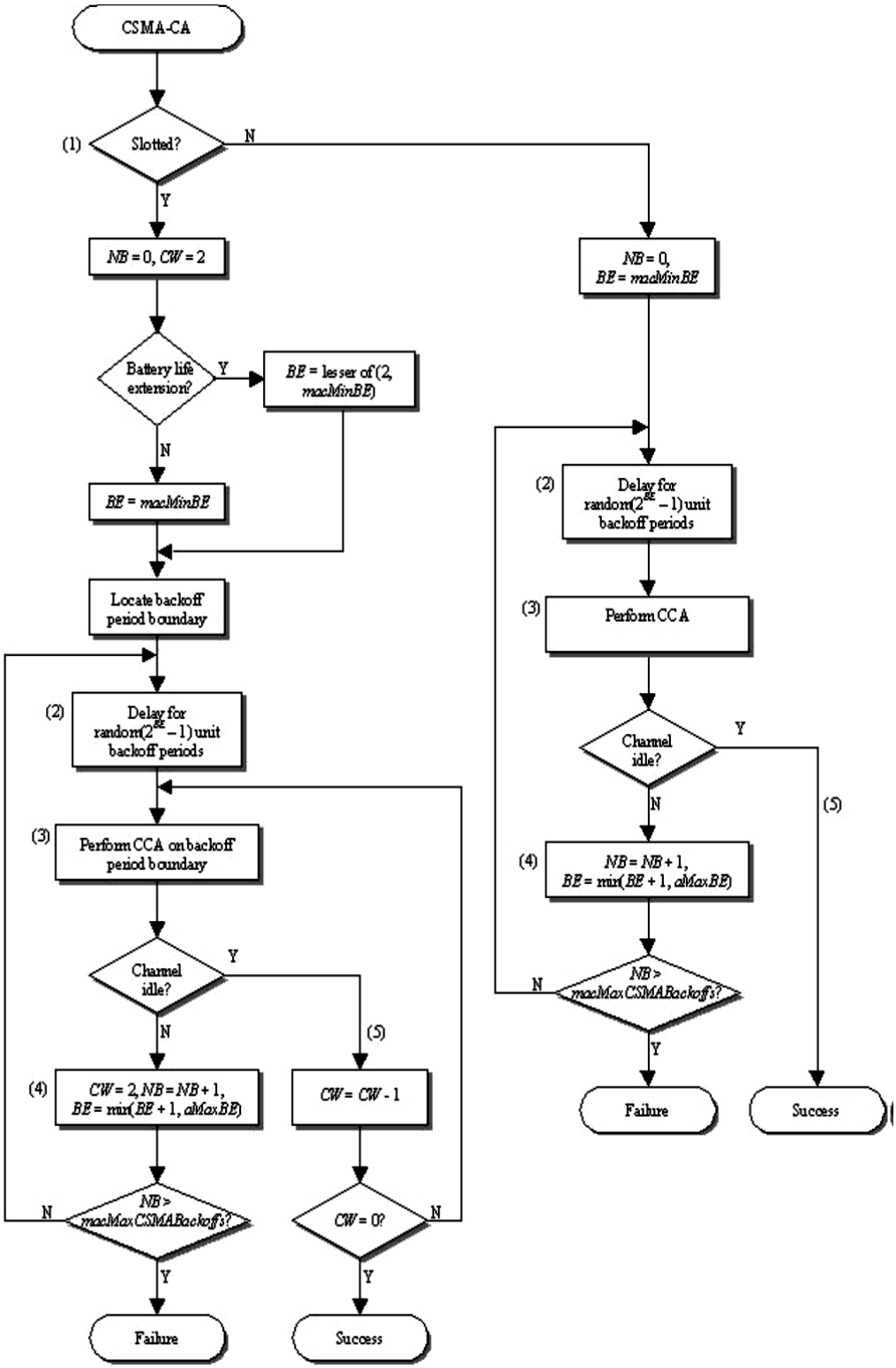


Figure 4.6. CSMA/ CA algorithm [14]

4.8. The Superframe Structure

The frame format of a superframe structure is defined by the coordinator. The superframe is divided into 16 equally sized slots and it is bounded by network beacons. An example of the superframe structure is illustrated in Figure 4.7. During the first slot of each superframe a beacon frame is sent and if a coordinator does not need to use the superframe structure it can turn off the beacon transmissions [8]. An active time period of a superframe structure is signified by a PAN coordinator by periodically transmitting beacons. This also has an advantage of saving power, as the coordinator can enter into a low power (sleep) mode during the inactive time period of the superframe structure. The active time period of a superframe structure is divided into a Contention Access Period (CAP) and Contention Free Period (CFP) [14].

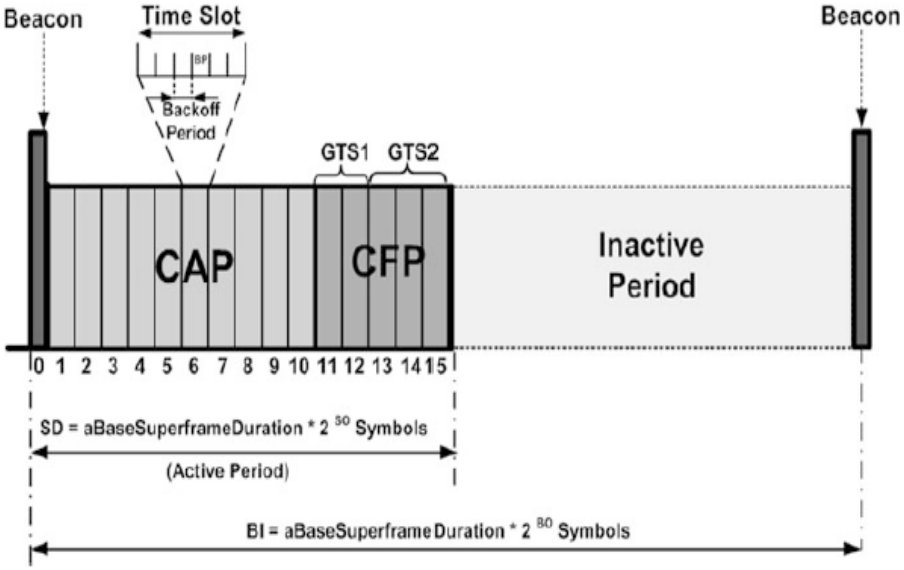


Figure 4.7. An example of the superframe structure [14]

4.8.1. Contention Access Period (CAP)

The CAP immediately follows a beacon and all transmissions in a CAP use the slotted CSMA/ CA algorithm to access the channel. A device transmitting in the CAP ensures that all transmissions and acknowledgements are completed before the end of the CAP. A transmission will be deferred to the next superframe if a device transmitting in a CAP cannot complete its transmissions or acknowledgements before the end of the CAP. MAC frames are also transmitted in the CAP [14].

4.8.2. Contention Free Period (CFP)

For exclusive use of a channel(s), devices should request a guaranteed time slot (GTS) from the PAN coordinator. The length of a GTS determines the length of a CFP. In the CFP, all transmissions are carried out without using the CSMA/ CA algorithm, and the transmissions must be completed before the end of their respective GTS [14].

The different portions of the superframe have different durations which are defined by the values of *macBeaconOrder* and *macSuperFrameOrder*. The *macBeaconOrder* defines the interval at which the coordinator will transmit its beacon frames. The relationship between the beacon interval (BI) and the *macBeaconOrder* (BO) is defined by Equation 4.4, also the superframe will be ignored if BO = 15

$$BI = aBaseSuperFrameDuration 2^{BO}, \quad 0 \leq BO \leq 14 \qquad (4.4)$$

The value of *macSuperFrameOrder* defines the length of the active portion of the superframe. The relationship between the superframe duration (SD) and the *macSuperFrameOrder* (SO) is defined by Equation 4.5 and if the SO = 15, then the superframe should not remain active after the beacon.

$$SD = aBaseSuperFrameDuration 2^{SO} \ , \quad 0 \leq SO \leq 14 \qquad (4.5)$$

The active portion of each superframe is divided into, *aNumSuperFrameSlots* equally spaced slots and each slot of duration, $2^{SO} aBaseSlotDuration$ and is composed of three parts: a beacon, a CAP and CFP. The beacon is transmitted at the start of slot 0 without the use of CSMA. The CAP starts immediately after the beacon and it is at least *aMinCAPLength* symbols, until and unless additional space is required to temporarily accommodate the increase in the beacon frame length to perform GTS maintenance. Similarly the CFP, if present, starts on a slot boundary immediately following the CAP and extends to the end of the active portion of the superframe [8].

5. PREVIOUS RESEARCH WORK

There are several other researchers and authors who have tried to address the interference problem of ZigBee. There is a case study on ZigBee which focuses on ZigBee's interference problem with Wi-Fi and Bluetooth, its technical challenges and range difficulties [19]. In this case study the researchers performed a set of tests like the range and packet error rate (PER) test in order to determine the transmission range between two ZigBee nodes and PER with respect to the distance between the nodes. They estimated a transmission range of 100m for indoor line of sight (LOS) and similarly a transmission range of 120m for outdoor LOS. This is considered good as it exceeds the 100m range mark specified by the ZigBee Alliance. The PER test results gave a much deeper understanding about the effects of distance between two nodes and the performance of the network. An acceptable PER is dependent on the requirements of the applications and critical operating environments.

The authors of the case study also mention conducting an RF interference test, the aim of which was to identify and address the problems faced by ZigBee when operating in environments where other 2.4GHz signals are present. They used different software packages and tested in different situations and environments to understand the effect of interference on ZigBee. The results indicated that in order to eliminate or to reduce interference, one should employ a ZigBee network through careful channel selection as well as ensure it's placed more than 10m away from the Wi-Fi network. The case study also summarizes various mitigation steps for interference.

Other authors and researchers have tried to address the interference problem of ZigBee by using different techniques and methods. One researcher proposed a low

complexity spread spectrum scheme for ZigBee based in smart home networks [20]. This paper tried to address the biggest challenge that consumers and service providers face in connecting to a wide range of consumer electronics in a smart home environment. They developed a MATLAB/Simulink simulator to improve the ZigBee physical layer in order to cope with coexistence issues from other technologies like Wi-Fi, Bluetooth, codeless phones and microwave ovens. They use an Ergodic Chaotic Parameter Modulation (ECPM) scheme and then the conventional Direct Sequence Spread Spectrum (DSSS) scheme used at the physical layer of ZigBee to implement the spread spectrum communication scheme and then evaluated their system using the Simulink ZigBee transmitter. The proposed scheme was found to be more robust against multipath fading effects and the robustness was maintained without the need of any computational complexity at the receiver side. Thus the scheme proposed was found to be highly desirable to integrate with the ZigBee physical layer in order to improve network coexistence in smart home environments.

Strong Wi-Fi signals trigger false alarms to ZigBee devices which are performing idle listening and cause appreciable energy wastage [21]. This is due to the concurrent deployment of wireless networks such as Wi-Fi, Bluetooth and ZigBee in the same 2.4GHz ISM band which has led to strong interference problems. In this paper the authors propose a ZigBee signal detection scheme known as CoSense which accurately helps in identifying ZigBee signals in the presence of crosstalk interference. CoSense is a highly reliable signal correlation technique which is backward compatible with traditional ZigBee networks and it greatly reduces false wake ups which consume energy unnecessarily. They conducted experiments in different environments to analyse the

characteristics of false wake ups. They also implemented the ContikiMAC protocol and ZiSense to compare the performance between them and CoSense. It was found that CoSense was effective in reducing false wake ups as well as consuming less energy when compared to ContikiMAC and ZiSense. CoSense is shown to work well with bad channel conditions and it also leverages both CCA (clear channel assessment) and signal correlation mechanism. It was concluded that CoSense not only reduced false wake ups but it also saves energy by up to 63%, especially in heterogeneous network environments.

A ZigBee network not only experiences interference problems from other technologies but it also experiences interference from other ZigBee signals within the same network when they are trying to transmit at the same time. The research work on the simulation study and performance analysis of a ZigBee system with CCI (Co-channel interference) focuses on interference from both the existing technology as well as on the interference within the same network [22]. In this research the authors analyse and simulate the system in SIMULINK. They use the BER (bit error rate) tool to analyse the degree of influence of CCI on the system, since the larger the CCI, the larger will be the BER of the system. They performed the experiment for getting system BER with different types and power gain of CCI. In order to reduce the effect of CCI they propose the use of an LMS adaptive filter in the receiver. It was noticed that using the LMS adaptive filter in the receiver reduced the effect of interference on the system as well as reducing BER, thereby improving system performance.

As mentioned earlier, ZigBee employs DSSS which uses a set of PN spreading codes which are publicly known and can be used by anyone for transmitting data and information. Since these spreading codes are publicly known there is always a threat of

an intruder trying to attack the system by listening to changes in energy variations on the channel. Reference [23] aims at overcoming this problem by obfuscating IEEE 802.15.4 communication by using secret spreading codes. In this research the authors propose to replace the conventional spreading codes with random codes, in order to do so they consider the receiver sensitivity. To vary the codes they analyse the hamming distance between the codes, coding gain and to maintain minimum receiver sensitivity. They perform the experiments in different situations and analyse the results. The results showed that the approach improved obfuscation but at the cost of marginal performance degradation in terms of packet error rate.

In all, there has been a significant amount of research done in the area of overcoming problems with interference, energy wastage and security of ZigBee. The researchers have developed approaches, some of which only address interference from external networks, which reduce interference, increase privacy, and/or increase energy efficiency at the cost of significantly increasing receiver complexity and slightly increasing packet error rate. In the next section of this paper, we propose a different approach which reduces the effects of interference and increases energy efficiency while only slightly increasing receiver complexity.

6. PROPOSED SOLUTION

Today ZigBee is one of the most popularly used communication protocols in wireless networks to transmit data or messages between devices due to its low cost, low data rate and low power consumption needs. With millions of devices transmitting ZigBee data and information, every second the possibilities of a collision among them is very high and when a collision does occur between two or more transmitting devices which are trying to transmit on the same frequency channel at the same time, both messages are lost or destroyed since they currently use the same PN sequence for spreading the data during modulation before transmission. The messages then need to be re-transmitted. Re-transmission as mentioned earlier requires additional power and time, thereby resulting in significant energy wastage, slower transmission as well as reducing the amount of data that could have been transmitted if the current ZigBee system could have successfully recovered the messages involved in the collision.

To overcome or reduce the effects of such collisions, in this thesis we propose a solution to this problem. We introduce a new ZigBee system where instead of all the ZigBee transmitting devices using the same set of PN sequences as defined by the IEEE 802.15.4 standard, we will allow each transmitting ZigBee device to randomly select a PN sequence from a list of, say, eight or sixteen different possible codes. This way, if a collision between two ZigBee devices occurred, seven out of eight times (or fifteen out of sixteen times), the two users would be using different PN codes and it would be possible to successfully demodulate one or both users' signals. The benefit in this approach is that seven out of eight times we don't need a retransmission of the data thereby saving on that additional power and time that would have been needed if it had to be retransmitted.

Also, at the same time we will be able to transmit more data compared to the current ZigBee system which uses a defined set of PN sequences. The proposed new system can significantly increasing the capacity of the ZigBee network.

Allowing different PN sequences also reduces the excessive churning that mostly occurs in ALOHA-based systems with a large number of ZigBee transmitters. But it does involve a trade-off where the transmitting and receiving devices will need to be a little more complex and require a little more computational sophistication (the larger the number of possible PN codes, the more complexity is needed in the transmitters and receivers). For many applications, this trade-off may be worthwhile because saving power will either allow the ZigBee transmitters to last longer before their battery dies or else will allow the transmitters to last the same amount of time but to transmit with a little more power and thereby increase their range. The trade-off will also increase system throughput, which might be important for systems with a large number of transmitters.

6.1 Mathematical Methodology Adopted in Developing the Proposed ZigBee Network System

We initially began our work by first mathematically developing a small queueing system with a small number of messages to be transmitted at random. We calculated the message arrival time, message length and end time of each message using the Queuing theory and the Poisson arrival process. We developed a MATLAB program to simulate the system, verified our simulation, and added capability in the MATLAB code to increase system size, analyze collisions, and incorporate our proposed ZigBee network system.

6.1.1. A brief description on Queuing Theory and the Poisson Process

Queuing theory is a branch of mathematics which studies and models the act of almost anything and everything waiting in lines or in queues [24]. “The Theory of Probabilities and Telephone Conversations” is the very first paper published on queuing theory in 1909 by Agner Krarup Erlang, who is today considered as the father or creator of this field. His work with the Copenhagen Telephone Company is what prompted his initial foray into this field and made him to ponder over the problem of determining how many telephone circuits were necessary to provide a phone service that would prevent customers from waiting too long for an available circuit or connection. In developing a solution for this problem, he began to realize that the problem of minimizing waiting time was applicable to many fields, and began developing the theory further [24]. Queueing theory has since seen applications in many fields including telecommunication, traffic engineering, computing and particularly in industrial engineering, in the design of factories, shops, offices and hospitals, as well as in project management [25].

The subject of queueing theory can be described as follows: consider a *service center* and a *population* of *customers*, which at sometime enter the service center in order to obtain a service. It is often the case that the service center can only serve a limited number of customers. If a new customer arrives and if the service facility is exhausted, he enters a *waiting line* and waits until the service facility becomes available. So we can identify three main elements of a service center: a population of customers, the service facility and the waiting line. Also within the scope of queueing theory is the case where several service centers are arranged in a *network* and a single customer can walk through this network at a specific path, visiting several service centers [26]. This very same

concept of queuing can be applied to communication networks, where there are a number of messages waiting to be transmitted by a network of sensors which are either currently transmitting previous messages or are ready to transmit the next waiting message in line or in queue, where the number of customers waiting in line to be serviced can be translated into the number of messages waiting to be transmitted, the service facility can be translated into the network of sensors and with the waiting line remaining the same. Queueing theory tries to provide answers to questions like the mean waiting time in the queue, the mean system response time (waiting time in the queue plus service times), mean utilization of the service facility, distribution of the number of customers in the queue, distribution of the number of customers in the system and so forth. These questions are mainly investigated in a stochastic scenario, where the interarrival times of the customers and/or the service times are assumed to be random [26].

The very same concept of queuing theory can also be applied to communication networks and it is what we have implemented in our MATLAB simulation to implement a ZigBee network of sensors to successfully transmit the arriving messages across the network to their respective receivers or destinations. We have considered a network with N different sensors and the sensors generate a total number of λ_{sys} messages. These numbers can be varied depending on how small or big the network of sensors we will be considering along with the number of messages waiting to be transmitted. The arrival of these messages is modelled using the Poisson Process.

The Poisson process is a simple and most widely used stochastic process for modelling the times at which arrivals enter a system. It is in many ways the continuous-time version of the Bernoulli process. For the Poisson process, the arrivals may occur at

arbitrary positive times, and the probability of an arrival at any given instant of time is 0. This means that there is no very clean way of describing a Poisson process in terms of the probability of an arrival at any given instant. It is more convenient to define a Poisson process in terms of the sequence of interarrival times [27]. In any given system the number of messages initiated over a particular interval of time is defined by Equation (6.1).

$$\boldsymbol{P\{n\ messages\ are\ initiated\ in\ the\ system\ during\ time\ interval} = \frac{(\boldsymbol{\lambda_{sys}T})^{\boldsymbol{n}}}{\boldsymbol{n!}}\boldsymbol{e^{-\lambda_{sys}T}} \quad (6.1)$$

where λ_{sys} can be defined as the average number of messages initiated in the system per unit time or it can also be defined as the message arrival rate. Since the arrival of a message is modelled using the Poisson process, the message interarrival time is exponentially distributed as defined in Equation (6.2).

$$\boldsymbol{P\{time\ between\ initation\ of\ nth\ and\ n+1st\ calls \leq t\} = 1 - e^{-\lambda_{sys}t}} \quad (6.2)$$

Let us initially assume that the message 0 arrives at time t=0 (or i=0 as defined in our MATLAB simulation) and from Equation (6.2), we want to describe the time between message 0 and message 1. We then generated a uniformly distributed random number R_1 between 0 and 1. The arrival time of message 1 can be defined according to Equation (6.3).

$$P\{message\ 1\ arrives\ at\ or\ before\ time\ t_1\} = R_1 \quad (6.3)$$

From Equations (6.2) and (6.3) we can solve for t_1 , which is the time at which message 1 arrives as follows.

$$R_1 = 1 - e^{-\lambda_{sys} t_1} \tag{6.4}$$

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

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

$$t_1 = \frac{-\ln(1 - R_1)}{\lambda_{sys}} \tag{6.5}$$

Thus message 1 arrives at time t = 0 + t_1. Similarly for message 2 we generate another uniformly distributed random number R_2 and calculated the time t_2 as defined by Equation (6.6).

$$t_2 = \frac{-\ln(1 - R_2)}{\lambda_{sys}} \tag{6.6}$$

Thus the arrival time of message 2 is calculated as t = 0 + $t_1 + t_2$. In this way the arrival times of the remaining messages in the system can be calculated using the same equations and steps as described above.

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. Therefore with the help of Queuing theory and the Poisson message arrival process we were able understand in a much clearer way how the messages arrive in a system and how we can simulate the arrival process. We can then simulate the ZigBee

superframe and slotted CSMA process and, using the results, evaluate system performance concerning how message that arrive in a system are transmitted and gain insight about how two or three messages which are being transmitted at the same time might experience a collision with each other. In the present ZigBee system this collision results in all colliding messages being lost or destroyed, thereby, resulting in the need for these messages to be re-transmitted requiring additional time and resources. In the proposed ZigBee system which allows sensors to choose different PN sequences, one or more of the colliding messages may be successfully received. The simulation results show us an how efficient the proposed ZigBee system will be when compared to the current ZigBee system in terms of reduced number of collisions and the number of re-transmissions required, as discussed in the next section. All Equations from (6.1) – (6.6) were referenced from [28].

6.1.2. Probability of Successful Message Demodulation for a message involved in a two message collision

To calculate the probability of a successful message demodulation for a message involved in a two message collision, we considered a ZigBee network system implemented using the 2.4 GHz, O-QPSK modulation system.

Let us assume 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 6.7.

$$P_b = Q\left(\sqrt{\frac{2E_b}{N_o}}\right) \tag{6.7}$$

Where 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. Substituting the value of $P_b = 10^{-5}$ in equation (6.7), we can calculate for what value of $\frac{E_b}{N_o}$ produces $P_b = 10^{-5}$ as given below.

$$P_b = Q\left(\sqrt{\frac{2E_b}{N_o}}\right)$$

$$10^{-5} = Q\left(\sqrt{\frac{2E_b}{N_o}}\right)$$

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

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

$$\frac{E_b}{N_o} = 9.11645 \tag{6.8}$$

Suppose the length of a ZigBee 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. For a 200 bit message, the

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

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

$$Probability\ of\ a\ message\ with\ no\ error\ = 0.99800 \qquad (6.9)$$

Thus for a 200-bit message with $\frac{E_b}{N_o} = 9.11645$, the message error rate is as shown below.

$$Probability\ of\ a\ message\ with\ error\ = (1\text{-}0.99800)$$

$$Message\ error\ rate = 0.002 \qquad (6.10)$$

Therefore from equation (6.10), we can say that even when there is no collision there is still a 0.2% probability of a message to being received in error. When there is a two-message collision, for the current system both messages will be destroyed. However, for the new proposed system, as shown in the calculations below when two messages collide, there is a significant probability that one or both messages can still be recovered.

In the new system if a second message or signal is transmitted at the same time, with the same energy, if the second message uses a different PN spreading sequence then only $\frac{1}{G_p}$ of its energy will interfere with the first signal after de-spreading, where G_p is the processing gain of the system. Both the current ZigBee system as well as the new proposed system uses a fixed processing gain of 8. Thus for a two-message collision where the messages use different PN spreading sequences, after de-spreading,

$$\frac{E_b}{N_o} = \frac{9.11645}{1 + \frac{1}{8}(9.11645)} = 4.2609 \qquad (6.11)$$

$$and, \qquad P_b = Q\left(\sqrt{2X4.2609}\right) = Q(2.9192) = 0.0018 \qquad (6.14)$$

Note that the probability of two messages using different PN sequences is $\frac{7}{8}$.

Thus for a message length of 200-bits,

$$P_{current\ system}(message\ destroyed \mid 2\ messages\ collide) = 1 \qquad (6.13)$$

but,

$$P_{new\ system}(message\ destroyed \mid 2\ messages\ collide)$$

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

thus,

$$P_{new\ system}(message\ destroyed \mid 2\ messages\ collide) = 0.389731 \qquad (6.14)$$

$$P_{new\ system}(message\ successful \mid 2\ messages\ collide)$$

$$= (1 - 0.389731) = 0.61026 \qquad (6.15)$$

From the above calculations it can be seen that when compared to the current system, the probability of a message to be destroyed in a two message collision is significantly less using the new system.

6.2. MATLAB Simulation

We used MATLAB as the simulation software for implementing our proposed ZigBee system. The code is shown in Appendix B. After we had mathematically developed a queuing system and had mathematically calculated the value for the probability of a message in a two-message collision being successfully demodulated, as described in the above section, we simulated the proposed system in MATLAB and randomly generated messages in the network thereby creating message traffic in the system. We were able to generate the data and tabulate the values for arrival time, message length and end time of each message which arrived in the system, for the length of time for which it stayed in the system and the time when it left the system respectively. Further we set certain variable values and simulated the code for different values of Lambda (λ_{sys}), different message lengths and different number of CAP slots within the superframe. The remaining design steps implemented in the MATLAB simulation are explained as follows:

1. Initially we set values for lambda, number of messages and number of sensors (or transmitting devices) in the system. These values can be variable depending upon the size and the needs of the network transmitting the messages.
2. Each sensor (or transmitting device) is then allowed to randomly select one of the PN table numbers out of the 8 (or 16) possible PN tables defined in the system, to modulate the data and spread its messages before transmitting them.
3. Further each sensor is randomly associated with a message which needs to be transmitted in the system but making sure that no two transmitting messages are assigned to the same sensor if they are transmitting over the same time interval.

4. The superframe size for the system is initially set to a constant value of 125 ms, and we also initially set the message length of each message to be 200 data bits, corresponding to 6.4 ms per message after applying the PN spreading code.
5. As mentioned in Chapter 4, every superframe has an active and an inactive period with CAP slots for transmitting the messages during the active period of the superframe. When we change message length in the simulation, we also change superframe size to maintain a constant ratio between active and inactive periods.
6. For our research work we have initially configured 13 CAP slots in the system for the active period of the superframe and randomly assigned a CAP slot each for the messages in the system. The number of CAP slots per superframe is adjustable in the simulation.
7. Also, we calculated the frame number of each message using equation (6.16)

$$frame = floor\left(\frac{endtime}{framesize}\right) + 1 \qquad (6.16)$$

   Where floor is a MATLAB function used to round off an integer to its nearest value, end time is the end time of the message which is under consideration and frame size = 125 ms for 200-bit messages.
8. Then we ran simulations to identify message collisions and to calculate the total number of messages being transmitted in the system and how many of them are involved in a message collision, identifying messages which are transmitting within the same superframe using the same CAP slot number. In the current ZigBee system, all messages involved in collisions are destroyed. This value was

recorded, so we know what percentage of messages are destroyed in the current system.

9. Evaluating the messages involved in a collision in step 8, we next determined how many of these messages would be destroyed using the new proposed system. The following steps describe this process in detail.
10. Any time if there are more than two messages trying to transmit within the same superframe with the same CAP slot number then those messages are marked as destroyed and cannot be successfully demodulated in the new system. This value was recorded.

    Similarly if there are two or more messages trying to transmit within the same superframe with the same CAP slot number as well as with the same PN table number then those messages are also marked as destroyed as the receiver system will have a great deal of difficulty in trying to separate the messages and demodulate since all of them would be transmitted using the same PN table sequence.
11. At the same time we also identified collisions where exactly two messages were involved in a collision, transmitting within the same superframe and with the same CAP slot number. The total number of messages involved in a two message collisions, was also recorded.
12. To estimate the total number of messages that get destroyed in a two message collision, we generated a random number for each message between 0 and 1.
13. The value of the random number generated for each message involved in a two-message collision was compared with the value that was determined

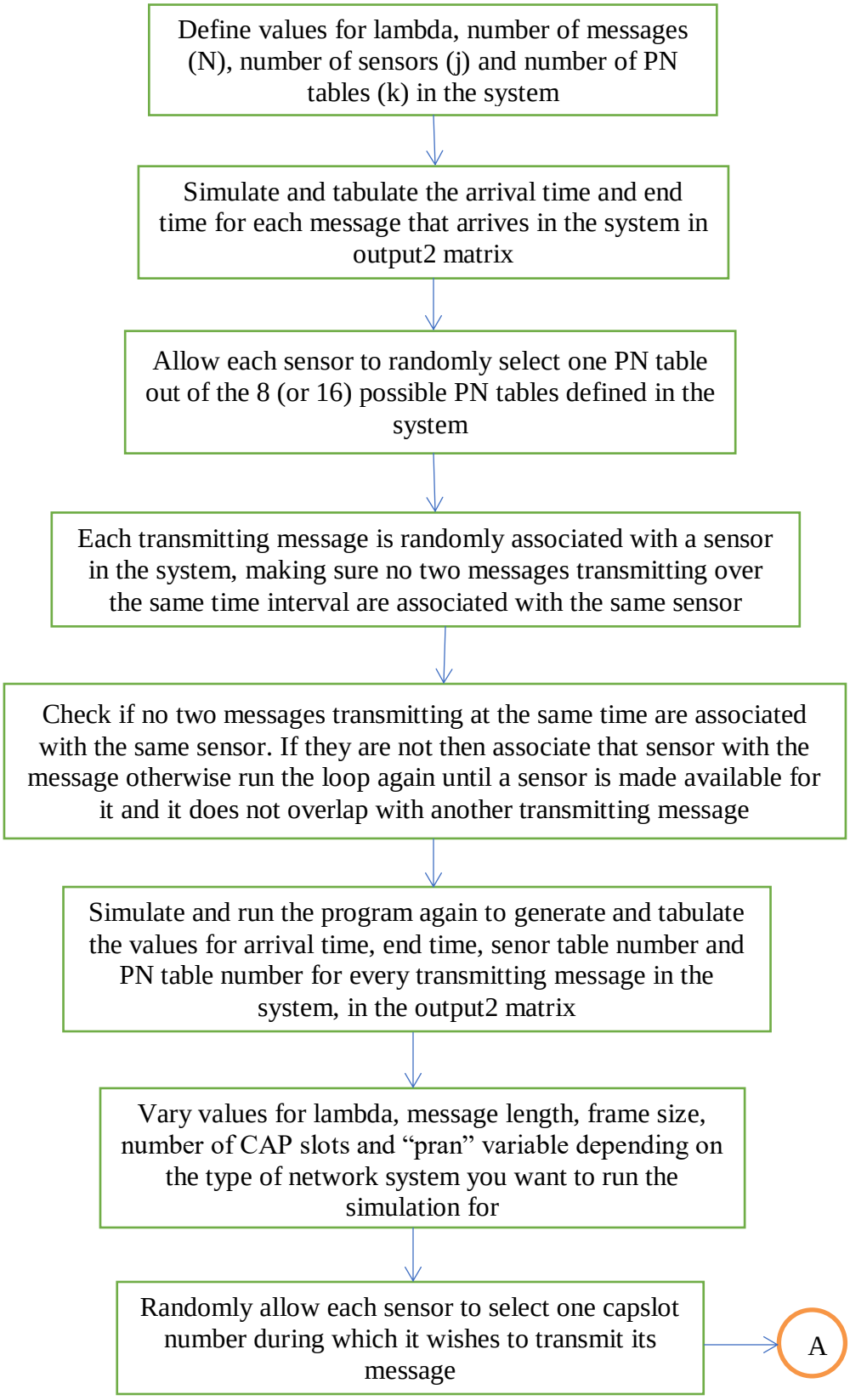
mathematically for the probability of a message in a two message collision to be successfully demodulated (see equation 6.16 and 6.17, with adjustments for message length if not 200 data bits).

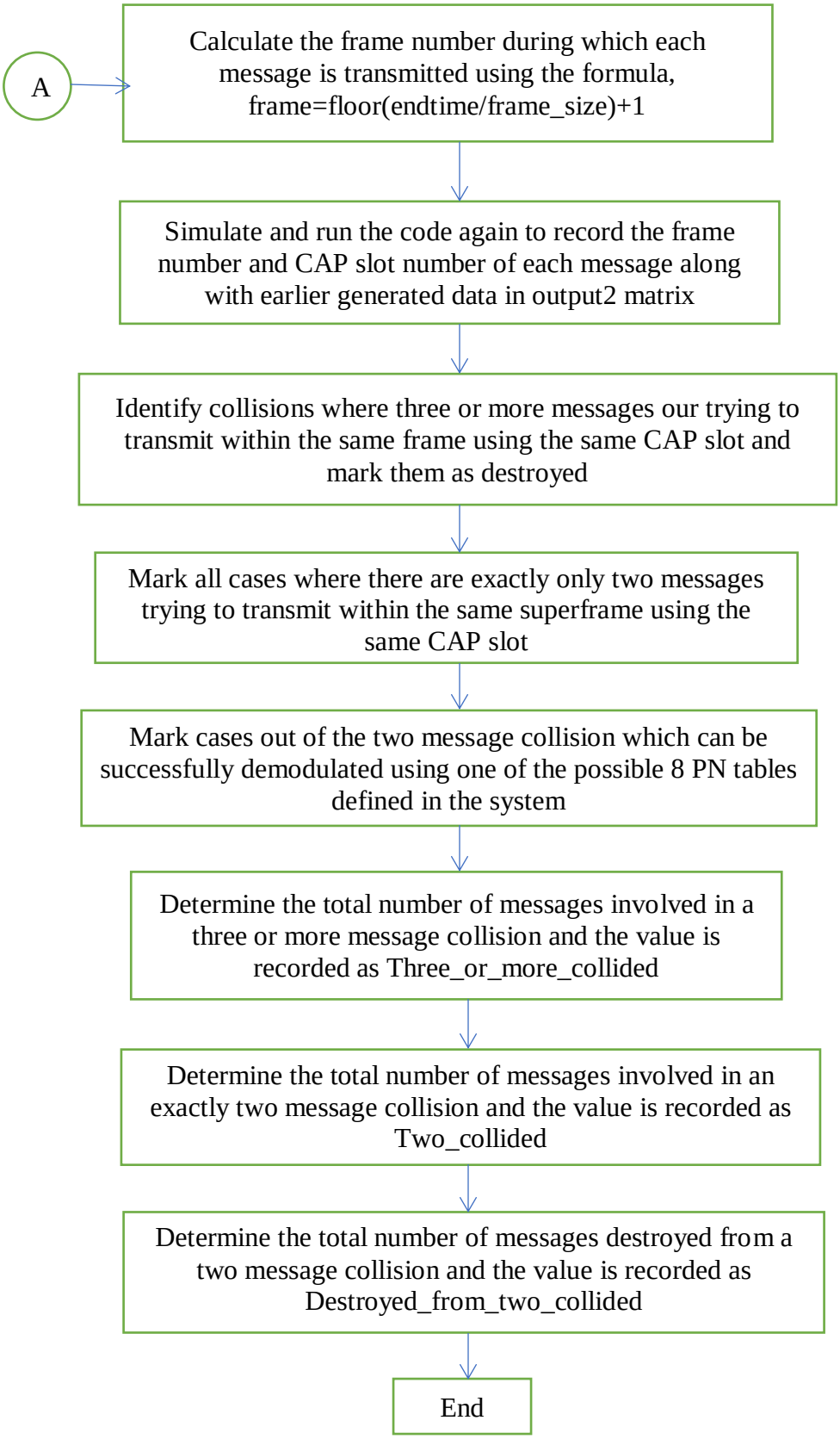
14. If the generated random number for a message is less than or equal to the value determined for the probability of a message in a two message collision to be successfully demodulated, then that message was not destroyed and the receiver system was successful in demodulating that message which was involved in a two message collision.
15. But if the random number generated for a message involved in a two message collision was found to be greater than the estimated value for the probability of a message in a two message collision to be successfully demodulated then the receiver system was not successful in demodulating that message and it was destroyed or lost resulting in that message to be re-transmitted.
16. Therefore out of the total number of messages which were involved in a two message collision we were able to estimate 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.
17. We ran multiple simulations for different values of lambda (λ_{sys}), different message lengths, and different numbers of CAP slots and recorded the value of total number of messages that get involved and destroyed in a three or more message collision, total number of messages involved in a two message collision and the total number of messages that get destroyed from a two-message collision using our proposed new system.

18. Further we also calculated the percentage of messages that could be successfully transmitted using our proposed solution and compared it with the percentage of messages that were successfully transmitted using the current ZigBee system.

From the observations made, it was seen that there was a significant increase in the percentage of messages that could be transmitted using the proposed solution when compared to the percentage of messages that were transmitted using the current ZigBee system for each value of lambda, message length, and number of CAP slots. In case of the messages involved in a two message collision, using the current ZigBee system all of the messages would be either lost or destroyed resulting in all of them needing to be re-transmitted. Retransmission requires additional power and time. It also, reduces the capacity of the messages that could have been transmitted over the same interval of time when compared to a system which would use our solution instead to transmit the messages in a system. Although there are a few messages which still have to be retransmitted using our solution, it is significantly less when compared to the number of messages which have to be retransmitted using the current ZigBee system. Therefore a significant amount of energy and time can be saved by using our system when compared to the current ZigBee system. Finally our system is also more efficient in terms of managing collisions and it also increases the range of a system. The results of our simulations, along with plots and recorded data are given in Chapter 7.

6.3. Flowchart of the Proposed Solution




A
Calculate the frame number during which each message is transmitted using the formula, frame=floor(endtime/frame_size)+1
Simulate and run the code again to record the frame number and CAP slot number of each message along with earlier generated data in output2 matrix
Identify collisions where three or more messages our trying to transmit within the same frame using the same CAP slot and mark them as destroyed
Mark all cases where there are exactly only two messages trying to transmit within the same superframe using the same CAP slot
Mark cases out of the two message collision which can be successfully demodulated using one of the possible 8 PN tables defined in the system
Determine the total number of messages involved in a three or more message collision and the value is recorded as Three_or_more_collided
Determine the total number of messages involved in an exactly two message collision and the value is recorded as Two_collided
Determine the total number of messages destroyed from a two message collision and the value is recorded as Destroyed_from_two_collided
End

7. RESULTS AND ANALYSIS

In the previous chapter we discussed the new system that we propose as a solution to reduce the number of messages which get lost or destroyed when they get involved in a collision using the current ZigBee system. We described the mathematical methodologies and MATLAB simulation design steps that we had developed and implemented in designing our proposed solution. We also, theorized, based on Equation (6.18) that our system would be effective in reducing the number of re-transmissions required for the lost or destroyed messages in the system when they get involved in a collision, thereby saving a significant amount of energy and time when compared to the current ZigBee system. This behavior would also mean that with the new proposed system we could successfully transmit more messages over a given period of time when compared to the current ZigBee system, thus increasing the capacity of the system, and that, if desired, we could trade off the saved energy to instead achieve an increase in the system's range. To test and verify the effectiveness of our new proposed system we ran running multiple simulations of our developed code for different loads, different message sizes, and different CAP slot values. All simulations represent a system using a star topology and the beacon-enabled mode. The simulations do not incorporate the effects of retransmission for messages lost or damaged due to collisions (i.e., the simulations do not include threshing effects). Incorporation of threshing, which will create an even wider difference between the performance of the present system and the proposed system, is suggested for future research. For networks with a large number of sensors sending information with a rapid sampling rate, a system often handles missing information not by requesting retransmission but rather by just waiting until the next sample is

transmitted. In such networks, the proposed ZigBee system provides an increase in accuracy by significantly reducing the number of lost or missing packets. The results obtained and the graphical representations of the data sets are given in the next three sections of this chapter.

7.1. Evaluating the Effects of Varying System Load with Fixed Message Size

In this section we evaluated the effects of varying system load with a fixed message size. For a fixed message length of 200 bits, we generated a data set by varying the system load that is the lambda value (the system's number of generated messages per second). We used lambda values of 25, 50, 75 & 100 messages/sec, and were able to record the number of messages that get involved in a 3-or-more-message collision (these messages will be destroyed in both the present and proposed system), the number of messages that get involved in a 2-message collision (these messages will all be destroyed in the present system), and the number of messages that get destroyed after getting involved in a 2-message collision using the new ZigBee system. With the data values generated we calculated the number of messages that can be successfully transmitted after getting involved in a 2-message collision as well as the overall success rate of messages using the new system compared to the current system. We were able to verify that with the new ZigBee system even though some messages would still get destroyed after getting involved in a 2-message collision most of the messages could still be successfully demodulated, resulting in a significant increase in the percentage of messages that the new system successfully receives compared to the current ZigBee system. Table 7.1 and Figure 7.1 show message success rates for the current and

proposed systems with a fixed message size of 200 bits, varying system load, 13 CAP slots allocated per superframe, and a simulation run of 20,000 messages.

Table 7.1. Data set for a fixed message size = 200-bits

Lambda	3 or more colliding	2 colliding	2 colliding & destroyed	Current System Success	New System Success
25	529	3816	1469	0.78275	0.9001
50	1650	5982	2329	0.6184	0.80105
75	3294	6976	2713	0.4865	0.69965
100	5144	7178	2803	0.3839	0.60265

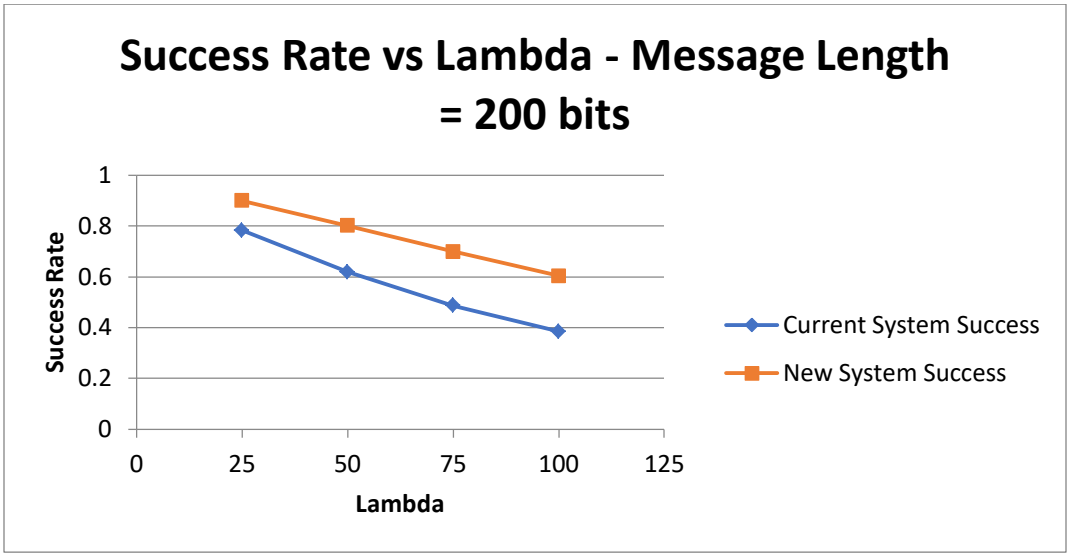


Figure 7.1. Graphical representation of success rate vs lambda – message length = 200-bits

The simulation results in Table 7.1 and Figure 7.1 show a significantly higher success rate for the new system under all evaluated system loads. Higher loads produced more 2-message collisions, and as expected the difference in success rate between the two systems therefore becomes larger as system load increases. In a system where

unsuccessful messages are retransmitted, this difference in success rate affects the battery life of the connected devices in the system as well as on the effectiveness of the system. The improvements of the new system become even greater when the value for the system load (or lambda) is 100 or more. Also as more and more messages get lined up for a re-transmission, there will be more load on the system to operate, and in addition to draining more power from the connected devices, the churning might cause the network to shut down or go through a break down, which is not a very desired user experience. But with the new system most of the messages that get involved in a collision will get successfully transmitted reducing the load on the system even for a re-transmission in turn saving those additional power requirements for the battery life of the network as well as the time that goes in with it. Over any given period of transmitting messages the new system successfully transmits more messages than the current ZigBee system significantly increasing the capacity of the system. Thus it was seen that the new ZigBee system significantly increases the overall effectiveness and performance of the system in terms of battery life, time and transmitted message capacity when compare to the current ZigBee system. To verify the stability and the performance of the system for different message length sizes we ran simulation for a 300-bit and a 400-bit message as well, with which we were able to generate the same type of improvement in system effectiveness as with for a 200-bit message.

A graphical plot of Success Rate versus Lambda (system load) for each fixed message size was created to evaluate and compare the overall system performance with varying load and fixed message sizes for both the current as well as the new ZigBee

system based on the data we generated for each. All the recorded data and the graphical representations for the same are tabulated and generated respectively as shown below.

7.1.1 For a fixed message size of 300 bits, with N=20000 and number of CAP slots=13

Table 7.2. Data set for a fixed message size = 300-bits

Lambda	3 or more colliding	2 colliding	2 colliding & destroyed	Current System Success	New System Success
25	1046	5092	2460	0.6931	0.8247
50	3391	6878	3399	0.48655	0.6605
75	5894	7332	3625	0.3387	0.52405
100	8528	6692	3331	0.239	0.40705

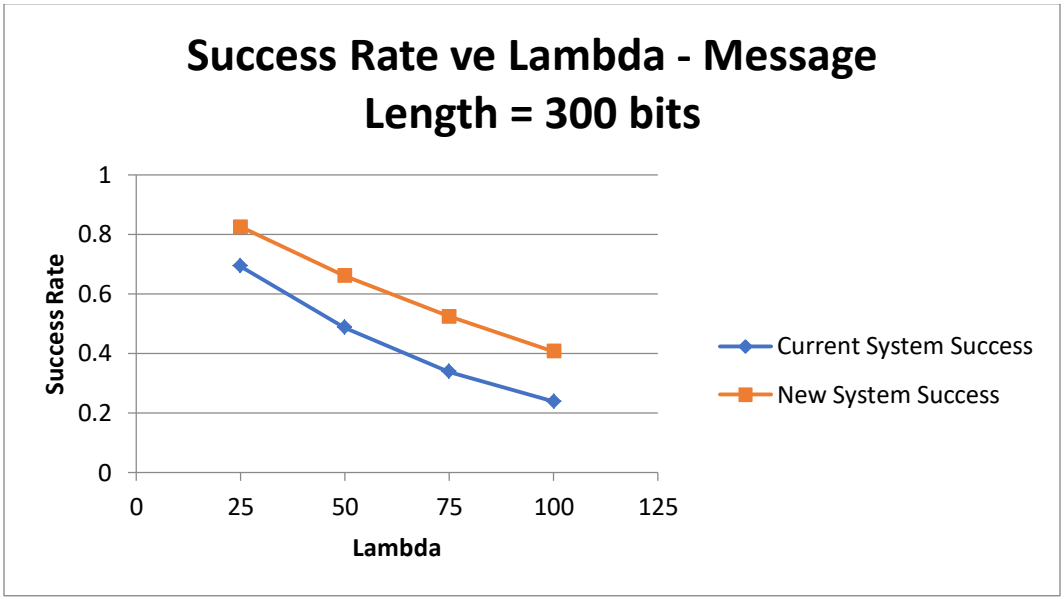


Figure 7.2. Graphical representation of success rate vs lambda – message length = 300-bits

7.1.2 For a fixed message size of 400 bits, with N=20000 and number of CAP slots=13

Table 7.3. Data set for a fixed message size = 400-bits

Lambda	3 or more colliding	2 colliding	2 colliding & destroyed	Current System Success	New System Success
25	1766	5924	3463	0.6155	0.73855
50	5110	7390	4192	0.375	0.5349
75	8580	6628	3776	0.2396	0.3822
100	11479	5448	3129	0.15365	0.2696

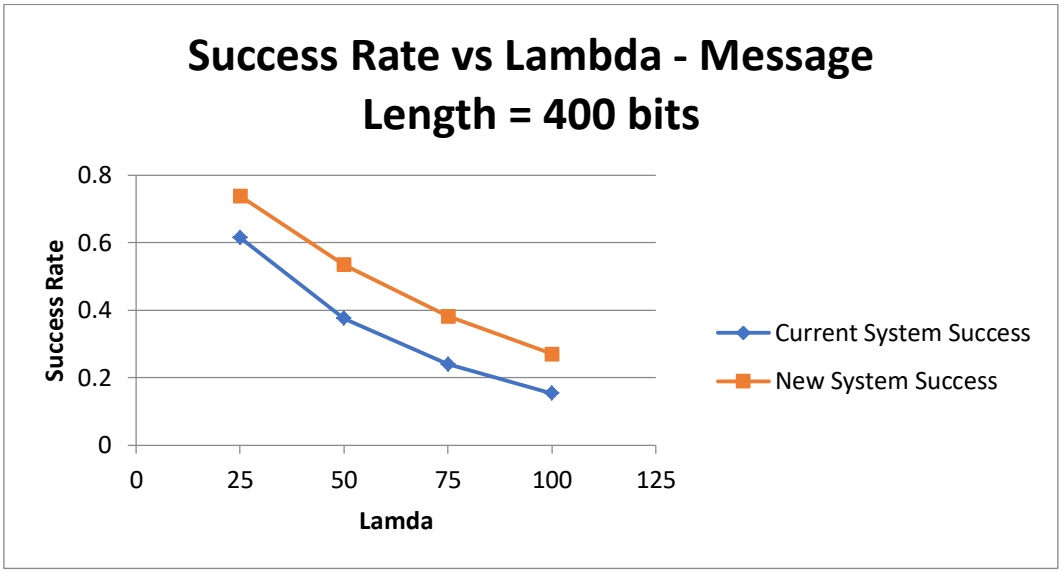


Figure 7.3. Graphical representation of success rate vs lambda – message length = 400-bits

7.2. Evaluating the Effects of Varying Message Size with Fixed Lambda (messages per second)

In this section we evaluated the effects of varying message size with a fixed lambda value. Initially, for a fixed lambda value of 25, we generated a data set by varying the message size from 200, 225, 250, 275, 300, 350 and 400 – bits. Based on the data generated we were able to record the number of messages that get involved in a 3 or more message collision and get destroyed from it, the number of messages that get involved in a 2-message collision as well as the number of messages that get destroyed after getting involved in a 2-message collision using the new ZigBee system. From the values generated we were able to verify that the new ZigBee system produces significant improvements over the current ZigBee system in terms of battery power, time and capacity of messages transmitted over a given period of time. It was seen that the changes in message length do not affect the stability of the network and we were still able to verify the same effectiveness of the system as described in the previous section. Furthermore to verify the system stability and performance with different message sizes when the system load increases we also, ran simulations with varying messages sizes for different lambda values equal to 50, 75 and 100. From the results generated we created graphical plots for success rate versus message lengths which shed more light on all the improvements and advantages that the new system provides when compared to the current ZigBee system as discussed in the previous section. All the data recorded and graphical plots generated respectively for this section are as shown below.

7.2.1 For a fixed lambda value = 25, with N=20000, number of CAP slots=13 and with varying message sizes

Table 7.4. Data set for fixed lambda value = 25

Length	3 or more colliding	2 colliding	2 colliding & destroyed	Current System Success	New System Success
200	529	3816	1469	0.78275	0.9001
225	590	4230	1716	0.759	0.8847
250	800	4350	1928	0.7425	0.8636
275	908	4850	2310	0.7121	0.8391
300	1046	5092	2460	0.6931	0.8247
350	1326	5620	2982	0.6527	0.7846
400	1766	5924	3463	0.6155	0.73855

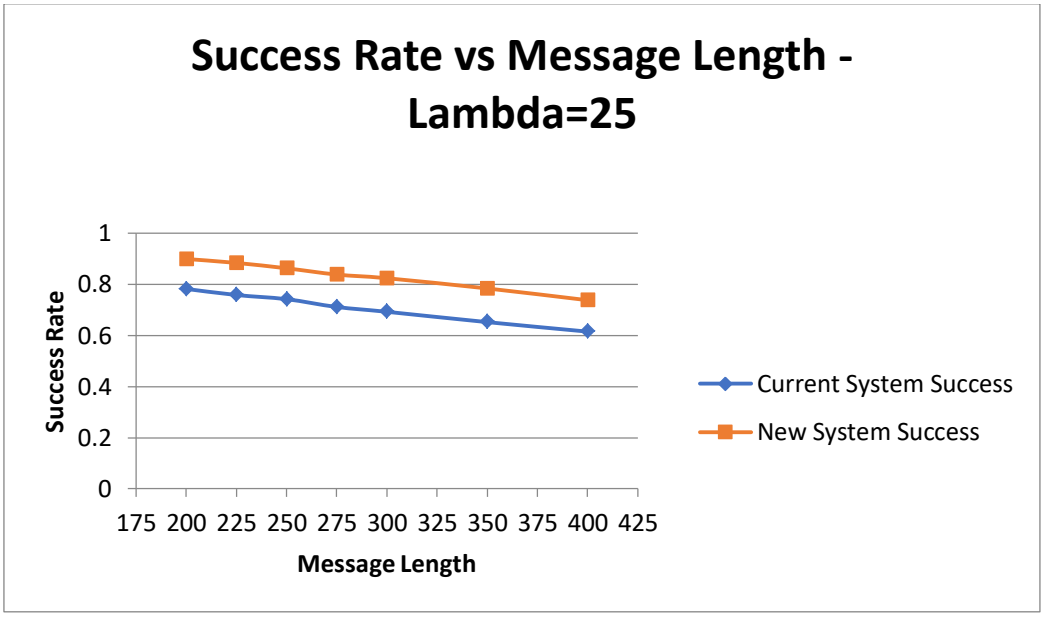


Figure 7.4. Graphical representation of success rate vs message length – lambda=25

7.2.2. For a fixed lambda value = 50, with N=20000, number of CAP slots=13 and with varying message sizes

Table 7.5. Data set for fixed lambda value = 50

Length	3 or more colliding	2 colliding	2 colliding & destroyed	Current System Success	New System Success
200	1650	5982	2329	0.6184	0.80105
225	2056	6368	2559	0.5788	0.76925
250	2426	6612	2953	0.5481	0.73105
275	2706	6838	3147	0.5228	0.70735
300	3391	6878	3399	0.48655	0.6605
350	4141	7236	3878	0.43115	0.59905
400	5110	7390	4192	0.375	0.5349

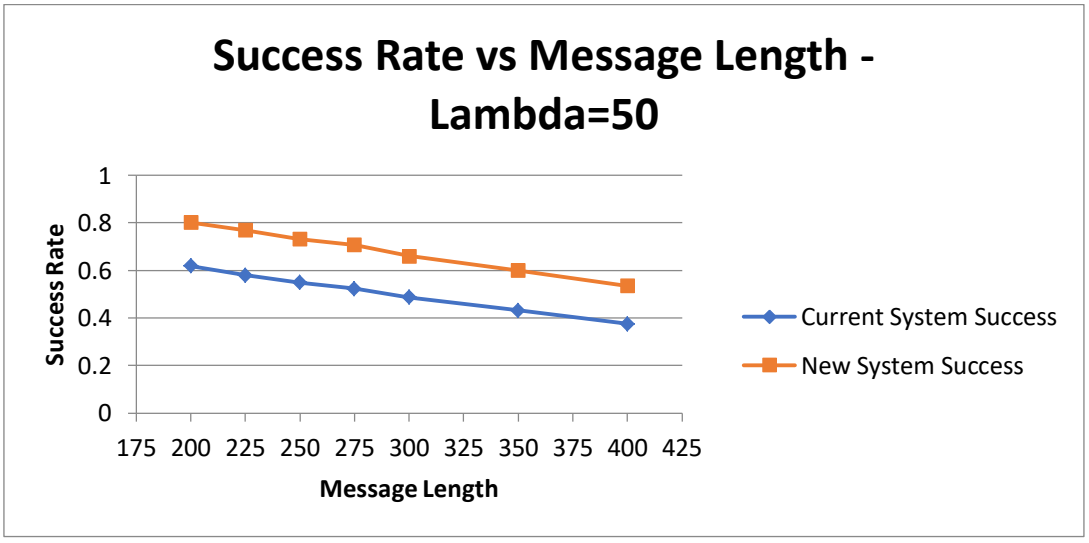


Figure 7.5. Graphical representation of success rate vs message length – lambda=50

7.2.3. For a fixed lambda value = 75, with N=20000, number of CAP slots=13 and with varying message sizes

Table 7.6. Data set for fixed lambda value = 75

Length	3 or more colliding	2 colliding	2 colliding & destroyed	Current System Success	New System Success
200	3294	6976	2713	0.4865	0.69965
225	3897	7274	2988	0.44145	0.65575
250	4441	7362	3274	0.40985	0.61425
275	5140	7490	3443	0.3685	0.57085
300	5894	7332	3625	0.3387	0.52405
350	6958	7204	3765	0.2919	0.46385
400	8580	6628	3776	0.2396	0.3822

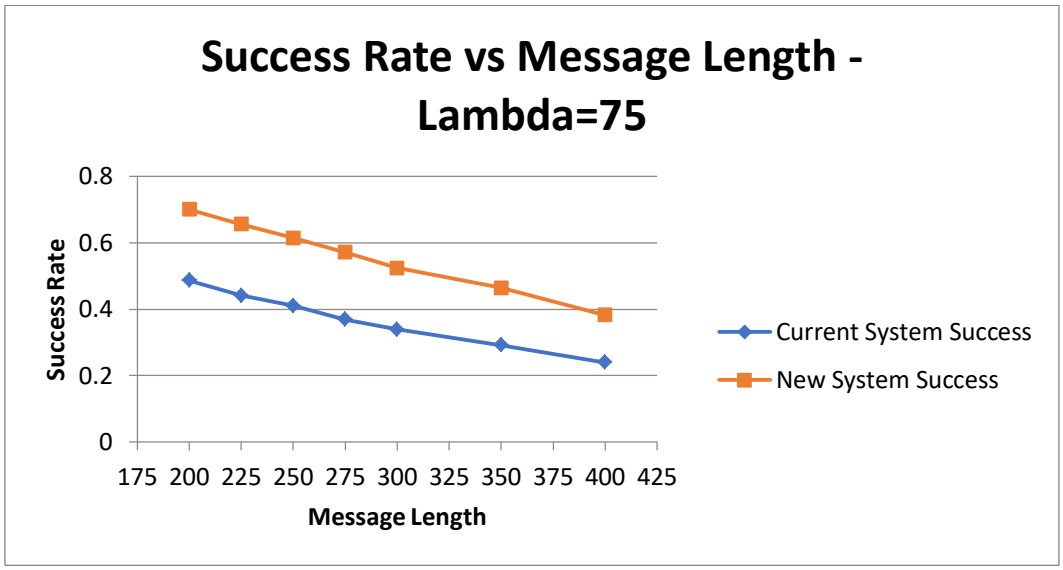


Figure 7.6. Graphical representation of success rate vs message length – lambda=75

7.2.4. For a fixed lambda value = 100, with N=20000, number of CAP slots=13 and with varying message sizes

Table 7.7. Data set for fixed lambda value = 100

Length	3 or more colliding	2 colliding	2 colliding & destroyed	Current System Success	New System Success
200	5144	7178	2803	0.3839	0.60265
225	5899	7336	3066	0.33825	0.55175
250	6696	7364	3304	0.297	0.5
275	7595	7090	3330	0.26575	0.45375
300	8528	6692	3331	0.239	0.40705
350	10030	6202	3214	0.1884	0.3378
400	11479	5448	3129	0.15365	0.2696

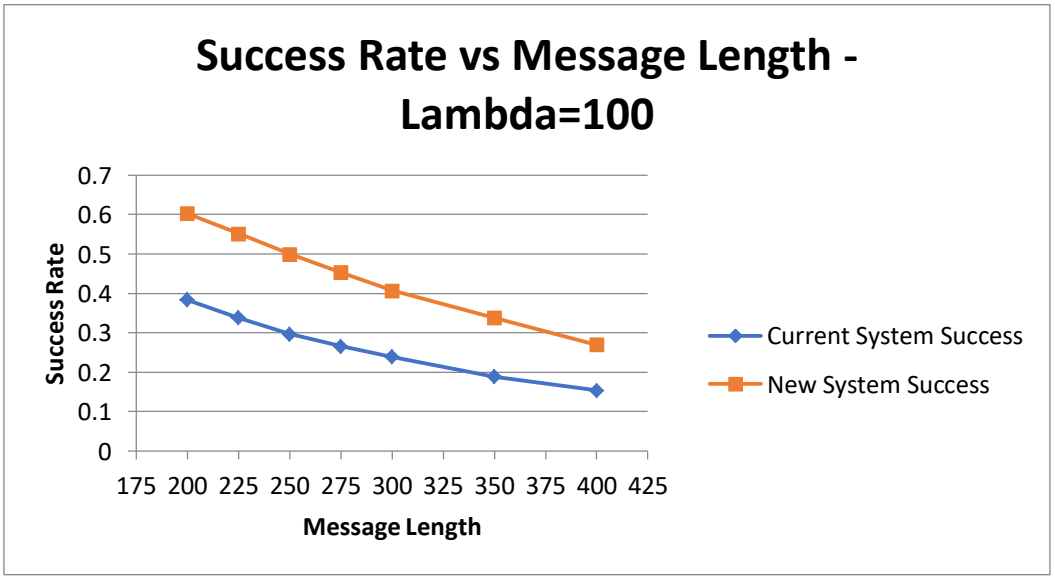


Figure 7.7. Graphical representation of success rate vs message length – lambda=100

7.3. Evaluating the Effects of Varying CAP Size

In this section we evaluated the effects of varying the number of CAP slots (CAP size) for message transmission in a superframe. According to the IEEE 802.15.4 standard, the maximum number of slots in the superframe for the active portion and for operation in the beacon mode is 14, if it is more than that the superframe should not remain active and you will then be operating in the non-beacon mode. In other words devices which do not wish to use the superframe or those devices which want to operate in the non-beacon mode will ignore the superframe by setting a CAP slot value of 15 for the active period and will transmit the data frame to the coordinator, using unslotted CSMA/CA as mentioned earlier for operation in the non-beacon mode. Since our research focuses on the ZigBee network operating in the beacon mode which considers the superframe for message transmission, while running simulations for this section, we varied the number of CAP slots values as 11, 12, 13 and for a maximum of 14 for the active period of the superframe to evaluate the effects of varying CAP sizes. For the simulation runs in this section, we considered a random network with lambda = 50, number of sensor = 25 and generated different data sets for a 200-bit, 300-bit and a 400-bit message length. The frame size and the message length in seconds were also varied accordingly. As mentioned earlier based on the data generated from the simulation runs for this section, we were able to record the number of messages that get involved in a 3 or more message collision and get destroyed from it, the number of messages that get involved in a 2-message collision as well as the number of messages that get destroyed after getting involved in a 2-message collision using the new ZigBee system. With the data generated it was seen that the new ZigBee system was still consistent in generating significant results and

improvements when compared to the current ZigBee system even with different CAP slot numbers and varying message lengths. On comparing the results generated for this section with the results generated in section 7.1, we were able to verify that with reduced number of CAP slots the number of collisions increases for both the current as well as the new system and even though the number of collisions increase as the CAP slot size varies the new system is significantly better than the current system for all the cases. With this we were once again able to verify the stability as well as the effectiveness of the new ZigBee system to produce consistent results even with different varying parameters and from the data generated to compare between the current and new ZigBee system we calculated the success rate for each as well as generated graphical representations for the same. All the data generated and graphical representations created for this section is as shown below.

7.3.1. For a lambda value = 50, with N=20000, message length = 200-bits and with varying CAP sizes

Table 7.8. Data set for lambda = 50, message length = 200-bits and varying CAP sizes

Number of CAP Slots	3 or more colliding	2 colliding	2 colliding & destroyed	Current System Success	New System Success
11	2171	6472	2573	0.56785	0.7628
12	1870	6334	2468	0.5898	0.7831
13	1781	5958	2368	0.61305	0.79255
14	1510	5674	2202	0.6408	0.8144

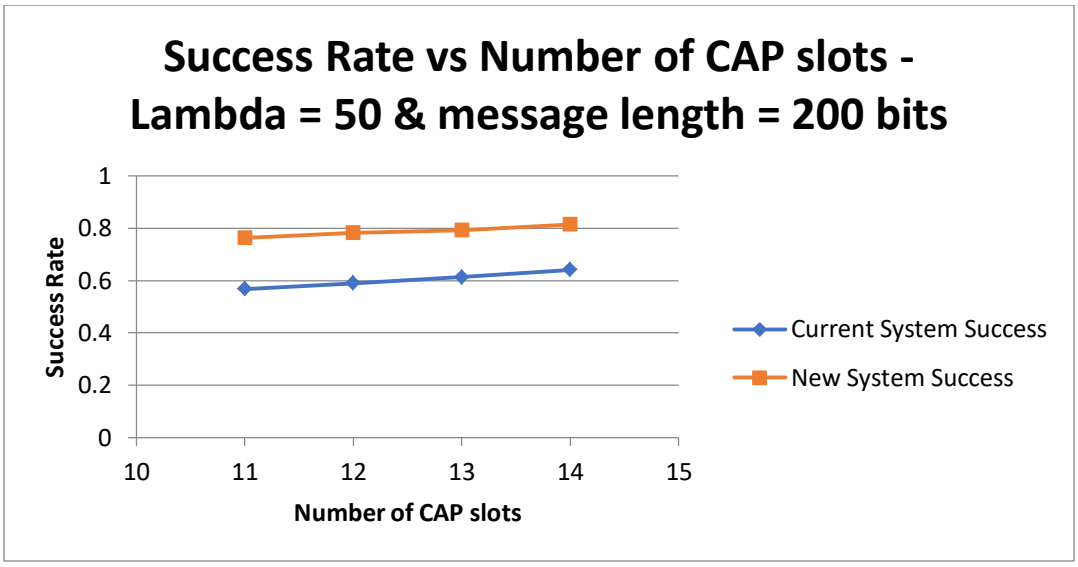


Figure 7.8. Graphical representation of success rate vs CAP slots-message length = 200-bits

7.3.2. For a lambda value = 50, with N=20000, message length = 300-bits and with varying CAP sizes

Table 7.9. Data set for lambda = 50, message length = 300-bits and varying CAP sizes

Number of CAP Slots	3 or more colliding	2 colliding	2 colliding & destroyed	Current System Success	New System Success
11	4321	7172	3483	0.42535	0.6098
12	3644	7232	3526	0.4562	0.6415
13	3325	7074	3399	0.48005	0.6638
14	2937	6778	3328	0.51425	0.68675

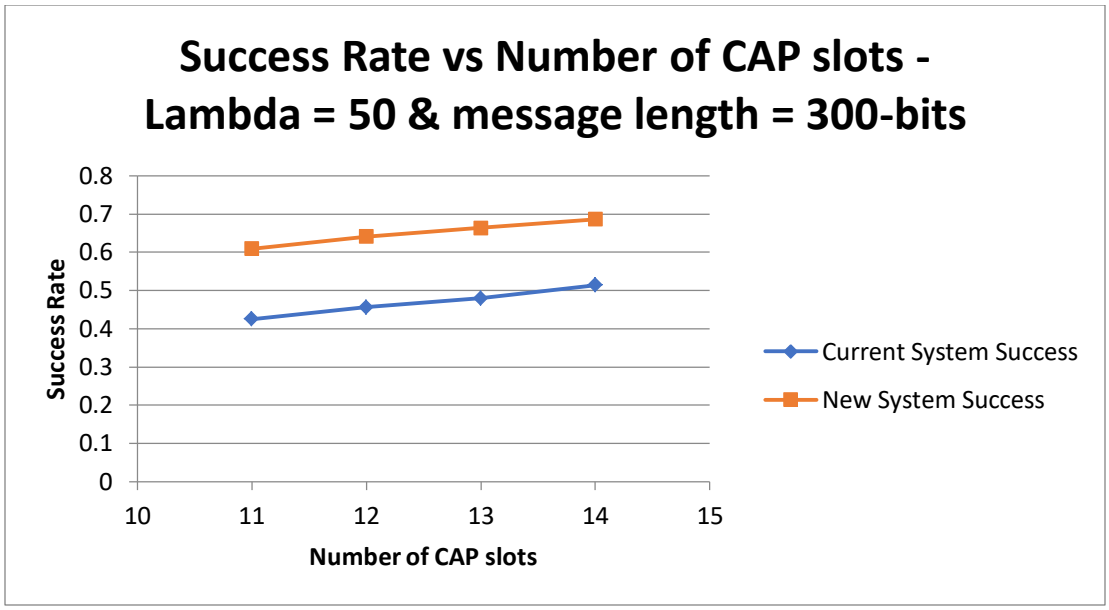


Figure 7.9. Graphical representation of success rate vs CAP slots-message length = 300-bits

7.3.3. For a lambda value = 50, with N=20000, message length = 400-bits and with varying CAP sizes

Table 7.10. Data set for lambda = 50, message length = 400-bits and varying CAP sizes

Number of CAP Slots	3 or more colliding	2 colliding	2 colliding & destroyed	Current System Success	New System Success
11	6241	7356	4249	0.32015	0.4755
12	5584	7380	4216	0.3518	0.51
13	4999	7300	4176	0.38505	0.54125
14	4549	7296	4245	0.40775	0.5603

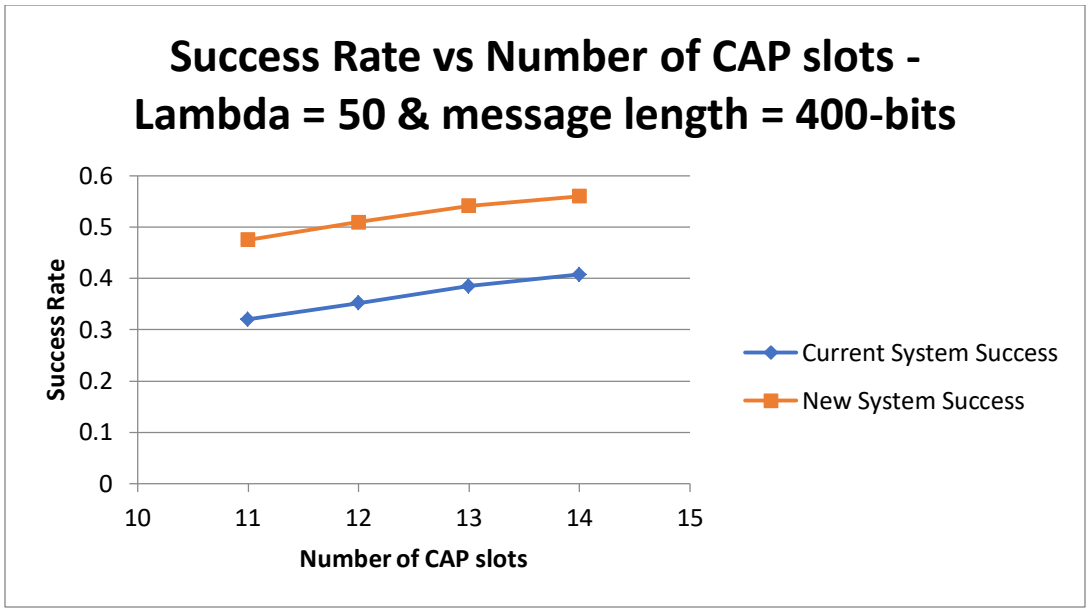


Figure 7.10. Graphical representation of success rate vs CAP slots-message length = 400-bits

8. CONCLUSION

Many of the wireless networks today use IoT as one of the ground technologies for transmitting information between controllers and sensors or actuators, and for transmitting information across wireless cloud networks. Amongst the various IoT wireless communications protocols available today, ZigBee is considered as the only complete IoT solution – from networking to the universal language that allows smart objects to communicate and work together transmitting information and data across wireless networks [29]. ZigBee acts as a digital bridge between users and wireless smart networks, providing users with the comfort and leisure of sitting at their homes and office spaces, to manage their smart devices like smart phones, tablets, light sensors, smart fans and various other devices at their convenience according to their needs and requirements, and at the same time providing them with a sense of security and protection. ZigBee also finds applications in commercial enterprises such as hospitals, offices, and testing labs, usually targeted towards automation, data acquisition, and remote control applications.

ZigBee applications require that the devices operate for long periods of time with small, non-rechargeable batteries which in turn mandates low power consumption which limits transmission distance to 10-100m line of sight. As discussed earlier in this thesis, since ZigBee operates in the same radio frequency band as Wi-Fi (2.4 GHz), it sometimes experience interference when a Wi-Fi user is trying to transmit at the same time as it is resulting in a collision. Similarly a ZigBee network also experiences collisions when two or more ZigBee devices are trying to transmit data at the same time. Even though ZigBee employs a Direct Sequence Spread Spectrum system and uses the ALOHA protocol to

overcome these interferences and collisions, some messages are still lost during transmission.

As a solution to this issue, in our thesis we have developed a system where ZigBee transmitters are allowed to randomly choose a PN code from among a large set of possible PN codes. We've analyzed the new ZigBee system using Queueing theory and the Poisson arrival process as the mathematical basis on which we developed and implemented our code using MATLAB Simulation. We ran multiple simulations of our code with varying message sizes, various traffic loads, and various numbers of CAP slots in each ZigBee superframe. For each data set that we generated, there was a significant increase in the percentage of messages that can be successfully transmitted using our new system when compared to the current ZigBee system. With the new system we are able to successfully demodulate most of the messages which get involved in a two-message collision, where all of these messages would have been destroyed with the current ZigBee system. Thus with the new system we were successful in reducing the number of re-transmissions that would have been required originally for the lost or destroyed messages, along with saving a significant amount of energy as well as the time that goes in with it. We were also able to increase the capacity of a system with the increase in the number of messages that can be accurately transmitted over a given time interval, and the savings in energy can be translated, if desired, into an extension of battery life and/or an extension of range.

The new system has better performance in managing collisions when compared to the current system, and this will be effective in reducing the excessive churning that occurs in congested ALOHA based systems. Also, by using different PN tables instead of

the pre-defined PN table, the new system makes ZigBee transmissions more reliable and secure now as they are no longer publicly known. All though the new system offers various advantages and improvements over the current ZigBee system it does have a few drawbacks. It might increase the computational complexity as well as the memory requirement of the transmitter and receiver systems. Even though there are a few trade-offs to be made with the new system it offers significant improvements and advantages over the current ZigBee system, which plays vital role in wireless networking for the Internet of Things.

9. SUGGESTIONS FOR FUTURE RESEARCH

As established in this thesis the newly developed ZigBee system is shown to be more effective in handling collisions, which increases system capacity & range as well as reducing the number of retransmissions required in the case of a collision when compared to the current ZigBee system. While evaluating the system there are many areas in which future research can yield additional insights. Firstly while developing our system we considered only fixed-length messages, as a future analysis the system can be changed a little to test and evaluate system response for variable length messages. We anticipate improvements relative to the current system similar to those we experienced for fixed-length messages.

Secondly in our developed system we introduced the concept of using 8 (or 16) possible different PN tables instead of just one like the current system. As a further development to this, different PN sequences can be developed for theses tables to further analyze the system. This will make the ZigBee transmissions more secure and reliable compared to the current ZigBee system which has its PN sequences publicly known and defined, giving an intruder an easier access to capture message patterns and intrude into the system. Thirdly an intriguing mind can extend the functionality of the system to the network layer as well, investigating the effects of the proposed improvements on multi-hop networks and on reducing churning.

Fourthly as our developed solution saves the additional energy which would have instead been required in the case of a re-transmission for the current ZigBee system, as a future development one can work on estimating how much energy our developed solution can effectively save or how much the system's range can be extended by using that

energy. Furthermore in this thesis we have tested our developed solution for system loads up to 100 messages/second, as a further development one can test our solution for higher load values. We anticipate that the system might break down at higher loads but at the same time we also expect it to give useful insights about how the system breaks. Also, as there are a few trade-offs that do come with our developed solution, one can quantify the impact of our solution on increasing the sensor's memory requirement as well as the computational complexity of the sensor system.

APPENDIX SECTION

APPENDIX A

SECTION 1

A.1.1 Channel Assignment and Switching

As mentioned earlier in the thesis report, the IEEE 802.15.4 PHY layer supports or can operate in three different frequency bands: a 2450 MHz frequency band, a 915 MHz frequency band and an 868 MHz frequency band. The three bands have 16 channels, 10 channels and 1 channel respectively, and all bands use the Direct Sequence Spread Spectrum (DSSS) multiple access technique. Amongst the three frequency bands only the 2.4 GHz frequency band overlaps with that of the Wi-Fi frequency band. Therefore only the protocol for operating on the 2.4 GHz ISM band is defined. The 2.4 GHz frequency band in the IEEE 802.15.4 standard is further subdivided into different frequency spectra ranging from 2400 MHZ to 2483.5 MHZ. Each of these 16 channels is 2 MHz wide with an inter-channel gap band of 3MHz as shown in Figure 10.1.

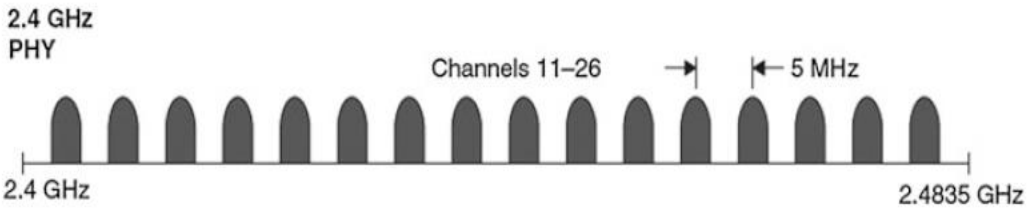


Figure 10.1. Frequency spectra [1]

The center frequency for these channels is calculated using Equation 10.1 as given below, where F_c is the centre frequency and k is the channel number. Table 10.1 represents the frequency ranges and the centre frequencies for every channel.

$$F_c = 2405 + 5(k - 11) \quad in\ MHz \quad , \quad for\ k = 11, 12 \ldots \ldots \ldots 26 \qquad (10.1)$$

Table 10.1. PHY channel frequencies [1]

Channel ID	Lower frequency	Center frequency	Upper frequency
11	2404	2405	2406
12	2409	2410	2411
13	2414	2415	2416
14	2419	2420	2421
15	2424	2425	2426
16	2429	2430	2431
17	2434	2435	2436
18	2439	2440	2441
19	2444	2445	2446
20	2449	2450	2451
21	2454	2455	2456
22	2459	2460	2461
23	2464	2465	2466
24	2469	2470	2471
25	2474	2475	2476
26	2479	2480	2481

These channels are non-overlapping in the frequency band and a channel is not orthogonal to all the other channels. The concurrent transmissions on adjacent channels can cause interference due to energy spill over and imperfect filtering [1]. Thus the 16 channels are divided into two sets of orthogonal 3 channels, with each set comprising of eight channels- (11, 13….25) and (12, 14….26). Channels are scanned in order from the lowest channel number to the highest if the scanning is for channel selection. The scanning process will provide the energy level feedback and the nodes will select the quietest one for their new working channel.

The channel switching operation, occurs through the channel register writing, and occurs only when the radio is in IDLE state and will induce a cost of time. In other

words, the channel switching operation will not come into effect immediately if the request is sent out when the radio is not in IDLE state. The procedures for channel switching roughly include radio status change, channel number register writing, and PLL (phase-locked loop) calibrating.

A.1.2. Receiver Energy Detection (ED)

The receiver energy detection (ED) measurement is calculated for use by a network layer as a part of the channel selection algorithm. It is a measure of the received signal power within the bandwidth of an IEEE 802.15.4 channel. During this process there is no attempt made to identify or decode signals on the channel. The ED time should be equal to 8 symbol periods. The ED result indicates the power level of the received signal including interference and noise. The ZigBee network node can use this information to infer the interference condition so that a better channel can be selected. Also, the ED result will be reported as an 8-bit integer ranging from 0x00 to 0xff. The minimum ED value (0) will indicate received power less than 10dB above the specified receiver sensitivity. The range of received power spanned by the ED values shall be at least 40dB. Within this range, the mapping from the received power in decibels to ED values shall be linear with an accuracy of +/− 6dB [1] [8].

A.1.3. Link Quality Indication (LQI)

When a data packet is received, the PHY sends the PSDU length, the PSDU itself and its link quality (LQ) in the PD-DATA.indication primitive. LQI estimates the strength and/or the quality of the packet received. The process of estimation can be implemented using the receiver ED, a signal-to-noise estimation or a combination of both

these methods. The use of an LQI result is up to the network or the application layers. An LQI result is recorded as an integer ranging from 0x00 to 0xff. The minimum and maximum LQI values are associated with the lowest and highest quality IEEE 802.15.4 signals which are detectable by the receiver and LQ values should be uniformly distributed within these limits [8].

A.1.4. Clear Channel Assessment (CCA)

CCA is a key component in wireless networks employing channel sensing as part of their medium access mechanism. CCA is implemented at the PHY layer as viewed from the protocol stack, but it is often used by the MAC layer. When the MAC layer receives a packet to transmit, it instructs the PHY to perform the CCA using one of the methods as described below. The standard specifies that the CCA duration shall be 8 symbol periods or128 μs. The CCA is performed according to at least one of the following three methods [1]:

- Energy above threshold. CCA shall report a busy medium upon detecting any energy above the ED threshold.
- Carrier Sense only. CCA shall report a busy medium only upon the detection of a signal with the modulation and spreading characteristics of IEEE 802.15.4. This signal may be above or below the ED threshold.
- Carrier sense with energy above threshold. CCA shall report a busy medium only upon the detection of a signal with the modulation and spreading characteristics of IEEE 802.15.4 with energy above the ED threshold.

SECTION 2

A.2.1. Application Support Sublayer (APS)

The APS layer provides the following functionalities [10]:

- Binding tables
- Message or data forwarding between bound devices
- Group address definition and management
- Address mapping from 64-bit extended addresses to 16-bit NWK addresses
- Fragmentation and reassembling of packets
- Reliable data transport

The concept of binding can be defined as the act of interfacing devices at the need or the service level. A coordinator manages the binding tables and all the routers in the network. A binding table maps a source address and source endpoint to either one or more destination addresses and endpoints and the cluster ID for a bound set of devices will be the same.

A.2.2. Application Framework

An application object(s) is defined by the manufacturer of the ZigBee-enabled device. Also, as defined by ZigBee an application object is present at the top of the application layer and is determined by the device manufacturer. It implements the application or the operation of a device, for example it can be a light bulb, a light switch, an LED, an I/O line, etc. and the application profile is run by the application objects. The

application framework layer creates or provides an execution environment for these application objects to send and receive data amongst each other.

Every application object is addressed through its corresponding endpoint numbers ranging from 1 to 240. Endpoint 0 is the address of the ZigBee Device Object (ZDO). Endpoint 255 is the broadcast address, implementing messages are sent to all of the endpoints on a particular node while the endpoints 241 through 254 are reserved for future use. ZigBee defines function primitives, not an application programming interface (API).

A.2.3. ZigBee Device Object (ZDO)

The responsibility of managing the overall working of a device is handled by the ZDO layer along with the following functionalities [10]:

- Initializing the APS sublayer and the NWK layer
- Defining the operating mode of the device (i.e., coordinator, router, or end device)
- Device discovery and determination of which application services the device provides
- Initiating and/or responding to binding requests
- Security management

Any ZigBee device can initiate a device discovery inquiry process. In response the inquiry end devices send their own IEEE or NWK address (depending on the request). A coordinator or router will send its own IEEE or NWK address along with the NWK addresses of the devices associated with it (a device is associated with a coordinator or router if it is a child node of the coordinator or router.). A device discovery

allows for an ad-hoc network or also allows for a self-healing network, while service discovery is a process of finding out which or what application services are available on each node. This information is then used in binding tables in order to associate a device offering a service with a device that needs that particular service.

SECTION 3

A.3.1. 868/ 915 MHz BPSK PHY Modulation Scheme

Operating in this frequency band includes a three stage process to implement the chip modulation sequence and differential bit encoding. In the first stage, the differential encoder performs an exclusive-OR operation of the current input bit with the input bit that is immediately prior to it. The bit to a DSSS chip conversion will be executed at a much faster rate than the user data rate by using the bit-to-chip conversion. In this case, the chip rate is 300 kchips/s for the 868 MHz band and 600 kchips/s for the 915 MHz band while the symbol rate is 20 and 40 ksymbols/s for the 868 and 915 MHz frequency bands, respectively. A raised cosine filter is applied at the BPSK modulator to shape the signal and Figure 10.2 illustrates a block diagram of a 868/ 915 MHz BPSK PHY Modulation Scheme.

Figure 10.2. 868/ 915 MHz BPSK PHY modulation scheme [7]

A.3.2. 868/915 MHz ASK PHY Modulation Scheme

Operation in this frequency band employs a multicode modulation method known as Parallel Sequence Spread Spectrum (PSSS). In this method for every data symbol that is transmitted during the transmission period there are about 20 or 5 information bits transmitted for 868 MHz or 915 MHz frequency bands respectively. Each of which are then modulated into 20 or 5 orthogonal pseudorandom (PN) sequences. These PN sequences are then linearly added to constitute a 32-chip PN sequence. The 32-chip symbol is equal to a multilevel 64-chip half-symbol for a 868 MHz frequency band, while a full 32-chip symbol for 915 MHz frequency band, Figure 10.3 illustrates the block diagram of a 868/915 MHz ASK PHY Modulation Scheme.

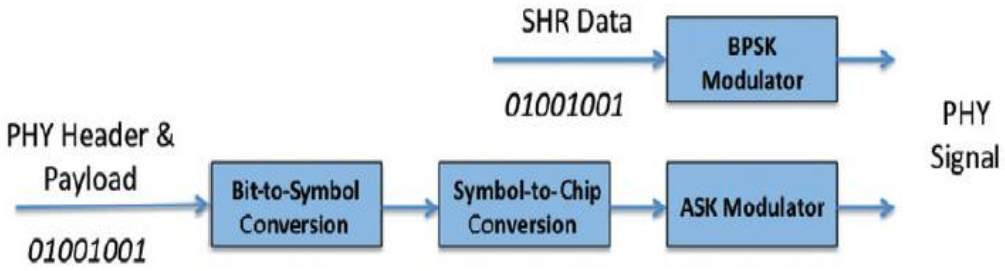


Figure 10.3. 868/915 MHz ASK PHY modulation scheme [7]

As illustrated in Figure 10.3, the PHY header and pay load bits are initially sent to a bit-to-symbol converter, followed by a symbol-to-chip converter and finally applied to the ASK modulator. In this modulation scheme the bit-to-symbol mapping is a little more complex when compared to the other modulation schemes employed. The mapping is illustrated in Figure 10.4.

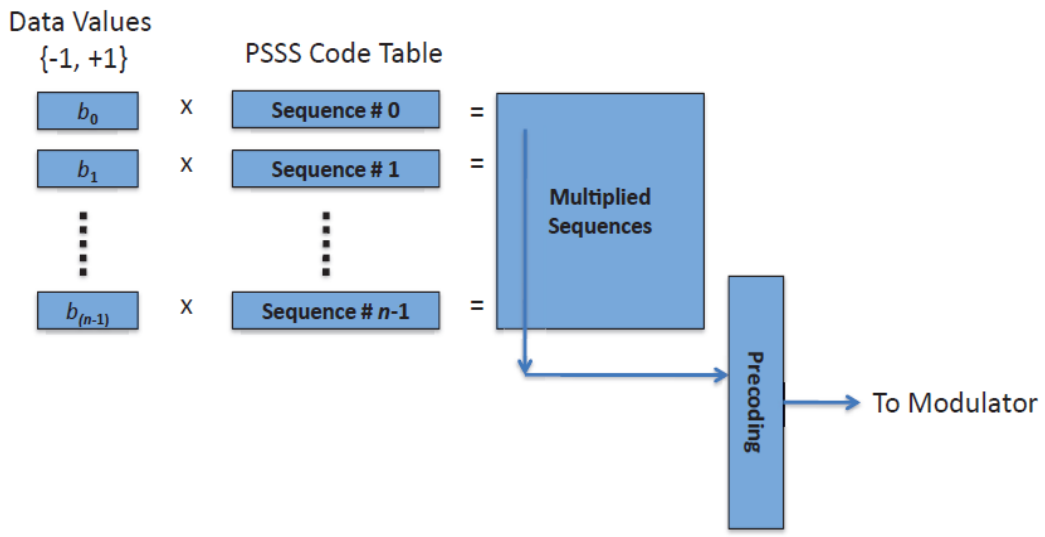


Figure 10.4. Symbol-to-chip mapping in 868/915 MHz ASK PHY modulation scheme [7]

As represented in Figure 10.4 each bit (0/1) is converted into a data value, with -1 corresponding to bit 0 and +1 corresponding to bit 1. The corresponding data values are multiplied by set sequences and then linearly added; following which a precoding operation is applied. The resulting chip sequences are modulated using ASK, with a square root-raised cosine pulse-shaping method. The ASK symbol rate is 12.5 ksymbols/s for 868 MHz and 50 ksymbols/s for 915 MHz.

A.3.3. Contents of the PPDU

The PPDU begins with a Preamble field and it is used for chip and symbol synchronization at the receiver part of the transceiver. It is composed of 32 binary zeros (all bytes set to 0x00) and has a variable length of 3.75–5 octets depending on the frequency band and modulation employed. The Start of frame delimiter (SFD) field follows the preamble and it indicates the end of the synchronization (SHR) field and the start of packet data and it is set to 0x7A [1]. The 802.15.4 radio on the receiver side

synchronizes with the incoming zero-symbols and searches for the SFD sequence to receive incoming packets. This is an 8 bit field segregated between the preamble and the actual physical layer data. This field also has a variable length between 0.625 and 2.5 octets. The payload is the PHY service data unit (PSDU), which is a 1-byte length field describing the number of bytes in the packet's payload along with the 2-byte CRC and it also contains information about user data or data packets. The PSDU field carries a PHY packet but the payload is usually transferred from the MAC sublayer and it has a variable length.

Consider Figure 10.5 illustrating the 802.15.4 PHY protocol data units format. Figure 4.6 shows that the ZigBee PPDU Frame consists of the SHR (Preamble 4 bytes, SFD 1 byte) + PHR (Frame length 1 bit, Reserved 1 bit) + PHY Payload (PSDU variable length). Therefore, the maximum packet size in a IEEE 802.15.4 ZigBee is 133 bytes, including all the headers. Also, Table 10.2 [12] summarizes the preamble and the SFD field lengths in octets and symbols as defined in the standard.

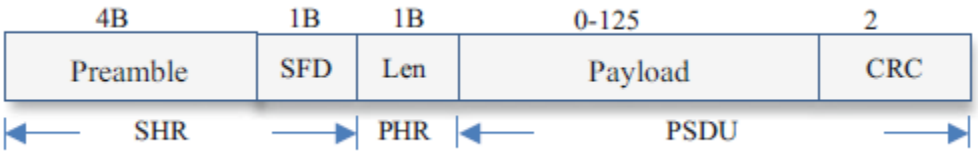


Figure 10.5. PHY protocol data unit format [7]

Table 10.2. Preamble and SFD field lengths [7]

PHY	Preamble length		SFD length	
868–868.6 MHz BPSK	4 octets	32 symbols	1 octet	8 symbols
902–928 MHz BPSK	4 octets	32 symbols	1 octet	8 symbols
868–868.6 MHz ASK	5 octets	2 symbols	2.5 octets	1 symbol
902–928 MHz ASK	3.75 octets	6 symbols	0.625 octets	1 symbol
868–868.6 MHz O-QPSK	4 octets	8 symbols	1 octet	2 symbols
902–928 MHz O-QPSK	4 octets	8 symbols	1 octet	2 symbols
2400–2483.5 MHz O-QPSK	4 octets	8 symbols	1 octet	2 symbols

In the PHY layer, there are a set of primitives used to specify each SAP of the PHY layer. These primitives are nothing but the particular functions that are supported by the SAP. For example, there are primitives defined for the PD-SAP in order to request a transfer of the MPDUs from the MAC layer to the PHY layer, to either confirm the end of a transfer of an MPDU from a local node (local PHY entity) to a remote node (peer PHY entity), or to confirm if a primitive request is sent from the MAC to the PHY via the SAP. These primitives provide the basic functions required to transfer the user data between the MAC layer and the PHY layer in a controlled way. The set of primitives described in the IEEE 802.15.4 standard are very small when compared with other technologies (such as IEEE 802.16), which there by keeps the protocol complexity and implementation costs low. Table 10.3 [12] summarizes the PD-SAP primitives and their functions, while Table 10.4 summarizes the PLME-SAP primitives and their functions.

Table 10.3. PD-SAP primitives and functions [7]

Primitive	Types/description
PD-DATA	*Used for passing MPDUs (data packets) between the local MAC layer entity and a remote PHY entity.* ***Request***: MAC layer requests transmission of MPDU ***Confirm:*** Local PHY entity confirms end of transmission of MPDU to a peer PHY entity ***Indication***: Indicates transfer of MPDU from the PHY to the local MAC sublayer

Table 10.4. PLME-SAP primitives and functions [7]

Primitive	Types/description
PLME-CCA	*Used to perform a clear channel assessment, which is a necessary function of CSMA/CA before transmission of a MPDU.*
	Request: Requests that the PLME conduct a CCA
	Confirm: Reports the results of the CCA
PLME-ED	*Utilized to perform an energy detection measurement. This measurement can be used to determine the level of energy in the channel at the moment of measurement, and is useful for determining whether or not to move to a different channel. For instance, if the energy detection measurement comes in above a certain threshold, the device may decide to choose another channel whose energy detection measurement is lower.*
	Request: Requests the PLME conduct an energy detection measurement
	Confirm: Reports the results of the energy detection measurement
PLME-GET	*Used to gather information from the PHY PAN Information Base (PIB) (Table 3.16). The PIB contains various metrics that can be used to determine the state of the network, similar to the management information base (MIB) concept used in routers and other network devices. This primitive is used by passing a particular PIB attribute as an input.*
	Request: Requests information about a particular PHY PIB attribute
	Confirm: Reports the results of the information request for a particular PHY PIB attribute
PLME-SET-TRX-STATE	*Handles transmitter and receiver states. Can turn on the transmitter function alone, receiver function alone, or disable both.*
	Request: Generated by the MLME and sent to the PLME when the transceiver operation state needs to be changed
	Confirm: Confirms the results of the request function
PLME-SET	*Used to set particular PHY PIB attributes. Inputs include the PHY PIB attribute and value to be set.*
	Request: Generated by MLME, sent to PLME to write a particular PHY PIB attribute value
	Confirm: Confirms that the request to write an attribute was successful or not

APPENDIX B : The developed Simulation Code

```
%considering a system initiating messages at random
%assuming the system as initiated 50 messages at random starting from
%message 0 to message 50
Lambda = 50; %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=.250; %size of superframe in seconds
capslots=14; %number of CAP slots in a superframe
%H = 5; %assuming average length of a call in seconds (1.5-
dr.stern)initially 5sec
j=[1:25];%number of sensors in the system
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','P
N_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 uniformaly 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
% for n=1:N
% S(n)=rand;%generate a uniformly distributed random number between
(0,1)
% length(n)= -H*log(1-S(n));%calculating length of each message
% end
for n=1:N
    length(n)=0.0128; %time is seconds
end
 messagelength=length;%calculated message length of each message

for n=1:N
    endtime(n)=arrival(n)+length(n);%calculating the end time of each
message
    frame=floor(endtime/frame_size)+1;%determine superframe number for
each message
end
```

```
y(1)=randi(a);%selecting a random sensor between 1 to j
msg_sensor(1)=y(1);%associating the random sensor number to message 1
sensor_end(y(1))=endtime(1);
for n=2:N %looping to generate sensor numbers for the remaining
messages
    y(n)=randi(a);%generate random sensor number
    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
            %  pass through the loop below increments the sensor number
by
            %  1 and checks to see if the new sensor number is
currently
            %  transmitting a message.  If not, the message is
associated to
            %  the new sensor number and the loop terminates.  If so,
the
            %  loop is repeated.  After the sensor number is increased
to
            %  j, if another loop is necessary the new sensor number
will
            %  be 1, the 2, then 3, etc.
            %  The sensor number will continue to be incremented once
per loop
            %  until the number 5 is reached.  If all the sensors are
            %  transmitting other messages, a "system at capacity"
message
            %  will then be printed.
            for ix=2:a
                y(n)=mod(y(n),a)+1 ;
                if arrivaltimes(n) > sensor_end(y(n));
                    msg_sensor(n)=y(n);
                    sensor_end(y(n))=endtime(n);
                    break
                else
                    if ix==a fprintf('system at capacity for sensor
number')
                        n
                    end
                end
            end
            %msg_sensor(n)=randi(a);%if not start all over
        end
```

```
    end
end
sensor=y;
%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
%output=[arrivaltimes;messagelength];

output2=[arrivaltimes;messagelength;endtime;sensor;tablenum;frame;cap_m
sgs]';

output=[frame;cap_msgs;tablenum]'; %creating a matrix containing the
superframe numbers, CAP slot numbers and PN table numbers of each
message

%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
% sssc= find(any(matchIdx .* (sum(matchIdx,1)==2),2)); %get the row
numbers of messages with same superframe and CAP slot numbers
for msgcount=1:N
    if output1(msgcount,4)==1
        pran=rand;
        if pran>=0.426
            output1(msgcount,5)=1;
        else
        end
    else
    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,9)=output1(n,4);%Mark all cases where there are 2 and only 2
messages in the same superframe and CAP slot
output2(n,10)=output1(n,5);%Mark those cases where the use of eight PN
tables allows one or both messages to be successfully received
output2(n,8)=output1(n,3);%Mark those cases where there are 3 or more
messages in the same superframe and CAP slot
Three_or_more_collided=Three_or_more_collided+output2(n,8); % Determine
total number of messages destroyed by collision of 3 or more
Two_collided=Two_collided+output2(n,9); % Determine total number of
messages involved in collisions of exactly 2 messages
Destroyed_from_two_collided=Destroyed_from_two_collided+output2(n,10);
%Determine number of messages destroyed in 2-message collisions
end
Three_or_more_collided
Two_collided
Destroyed_from_two_collided
```

REFERENCES

[1] G. Shi and K. Li, "Chapter 2," in *Signal Interference in WiFi and ZigBee Networks*, Springer International Publishing, 2017.

[2] [Online]. Available: https://www.dataversity.net/brief-history-internet-things/.

[3] [Online]. Available: https://www.itransition.com/blog/the-history-and-future-of-the-internet-of-things.

[4] "Wikipedia-Internet of Things," [Online]. Available: https://en.wikipedia.org/wiki/Internet_of_things.

[5] [Online]. Available: https://www.sam-solutions.com/blog/internet-of-things-iot-protocols-and-connectivity-options-an-overview/.

[6] Google Photos.

[7] 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.

[8] S. C. Ergen, "ZigBee/IEEE 802.15.4 Summary," 10 September 2004. [Online].

[9] A. K. Akshay Kanwar, "ZigBee: The New Bluetooth Technology," *International Journal Of Engineering And Computer Science ISSN:2319-7242*, vol. 1, no. 2 Nov 2012, pp. 67-74, 2012.

[10] A. Tomar, "Introduction to ZigBee Technology," 2011.

[11] "Chapter 4-ZigBee Applications".

[12] "Part 15.4: Wireless Medium Access Control and Physical Layer Specifications forLow-Rate Wireless Personal Area Networks," *IEEE 802.15.4-2006*, Sptember 8 2006.

[13] "ZigBee Specifi cation," *ZigBee Document 053474r17, Sponsored by ZigBee Alliance*, 17 January 2008.

[14] C.-H. Yang, "TSKS03 Wireless Systems Report-The ZigBee Specification," May 2016.

[15] N. P. J. L. A. T. C.M. Liang, "Surviving Wi-Fi interference in low power," in *ACM SenSys*, 2010.

[16] C. H. W. M. G. M. Thad B. Welch, Real-Time Digital Signal Processing from MATLAB® to C with the TMS320C6x DSPs, CRC Press Taylor & Francis Group, 2012.

[17] [Online]. Available: https://www.rfwireless-world.com/Terminology/Advantages-and-disadvantages-of-DSSS.html.

[18] D. C. A. Woo, "A transmission control scheme for media access in sensor networks," in *MobiCom*, 2001.

[19] a. E. F. Halit Eren, "Technical Challenges for Wireless Instrument Networks- A Case Study with ZigBee," February6-8 2007.

[20] C. S. a. H. Leung, "A Low Complex Spread Spectrum Scheme forZigBee based Smart Home Networks," in *13th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, 2016.

[21] D. B. W. P. a. C.-K. K. Sangsoon Lim, "CoSense: Interference Resilient ZigBee Detection in Heterogeneous Wireless Networks," *IEEE ICC 2016 Ad-hoc and Sensor Networking Symposium*, 2016.

[22] X. L. J. S. L. D. Jianxin Zhang, "Simulation Study and Performance Analysis on Zigbee System with CCI," in *25th IEEE Wireless and Optical Communication Conference (WOCC)*, 2016.

[23] V. L. F. L. a. B. P. Bjorn Muntwyler, "Obfuscating IEEE 802.15.4 Communication Using Secret Spreading Codes," in *9th IEEE Annual Conference on Wireless On-Demand Network Systems and Services (WONS)*, 2012.

[24] R. Berry, "Queuing Theory, white paper," [Online]. Available: https://mafiadoc.com/queuing-theory-1-introduction-queuing-theory-is-a-branch-of-_59bfc4f01723dd93e746c00d.html.

[25] "Queuing Theory - Wikipedia," [Online]. Available: https://en.wikipedia.org/wiki/Queueing_theory.

[26] A. Willig, "A Short Introduction to Queuing Theory," Berlin, 1999, pp. 3-4.

[27] "Poisson Process".

[28] H. P. Stern, *Simulating Voice Traffic in a Cellular System.*

[29] [Online]. Available: https://zigbeealliance.org/solution/zigbee/.