8-2021

Spectrum Sharing and Interference in Smart Homes

Biswajit Kumar Dash
The University of Texas Rio Grande Valley

SPECTRUM SHARING AND INTERFERENCE IN SMART HOMES

A Thesis

by

BISWAJIT KUMAR DASH

Submitted to the Graduate College of
The University of Texas Rio Grande Valley
In partial fulfilment of the requirements for the degree of

MASTER OF SCIENCE IN ENGINEERING

August 2021

Major Subject: Electrical Engineering

SPECTRUM SHARING AND INTERFERENCE IN SMART HOMES

A Thesis
by
BISWAJIT KUMAR DASH

COMMITTEE MEMBERS

Dr. Jun Peng
Chair of Committee

Dr. Wenjie Dong
Committee Member

Dr. Mark Yul Chu
Committee Member

August 2021

ABSTRACT

Dash, Biswajit Kumar, Spectrum Sharing and Interference in Smart Homes. Master of Science in Engineering (MSE), August, 2021, 100 pp., 13 tables, 29 figures, 81 references.

Internet of Things networks using Zigbee are very popular in smart homes. However, Zigbee networks are vulnerable to the interference of Wi-Fi networks because they share the same 2.4 GHz Industrial, Scientific, and Medical radio frequency band. Studies have shown that weaker Zigbee signals might be significantly interfered by stronger Wi-Fi signals. This type of interference may cause severe problems when these types of networks coexist in an indoor environment such as in a smart home. In this thesis, the performance of a Zigbee network with and without the presence of a Wi-Fi network has been evaluated in an apartment-based indoor environment mimicking a smart home. The experimental results are obtained and analyzed in terms of received signal strength indicator, packet delay, packet drop rate, and loopback throughput by changing operating channels, distances between Zigbee and Wi-Fi devices, transmission intervals of Zigbee packets, Zigbee transmit power, and Zigbee packet lengths.

DEDICATION

The completion of my master's studies would not have been possible without the love and support of my family. I would like to dedicate my thesis to my parents, Bashanti Rani Dash and Paritosh Dash and my beautiful wife, Prianka Datta, they wholeheartedly inspired, motivated, and supported me by all means to accomplish this degree. Thank you for your love and patience.

ACKNOWLEDGMENTS

I will always be grateful to Dr. Jun Peng, chair of my thesis committee, for all his mentoring and advice given throughout my graduate studies. From preparing to begin research, buying research tools to completing this thesis, he encouraged and guided me to complete this process through his infinite patience and guidance. Besides, I would like to express my gratitude to my honorable thesis committee members, Dr. Mark Yul Chu and Dr. Wenjie Dong for their valuable suggestions and feedback on my thesis.

I would also like to thank my colleagues in the UTRGV library, who helped me locate supporting documents for my research. Also, I would like to acknowledge my other colleagues and classmates who inspired and motivated me to complete this work.

TABLE OF CONTENTS

Page

LIST OF TABLES

Page

LIST OF FIGURES

Page

CHAPTER I

INTRODUCTION

The development of Sensor Networks (SN) has made a tremendous breakthrough in the field of networking and communications. A sensor network comprises a group of small-powered devices and a wireless or wired network infrastructure. Many sensor nodes connected in a sensor network can detect and record conditions/ information (such as heat, pressure, motion, etc.) in any environment, including industrial facilities, farms, and hospitals (Matin and Islam, 2012). A sensor network interconnects to the internet or computer networks to exchange data for use and analysis. Sensors or nodes of the network cooperatively sense any environment as well as control it. Sensor nodes are very vital part of any sensor network to facilitate interaction between persons and computers as well as with the surrounding environment.

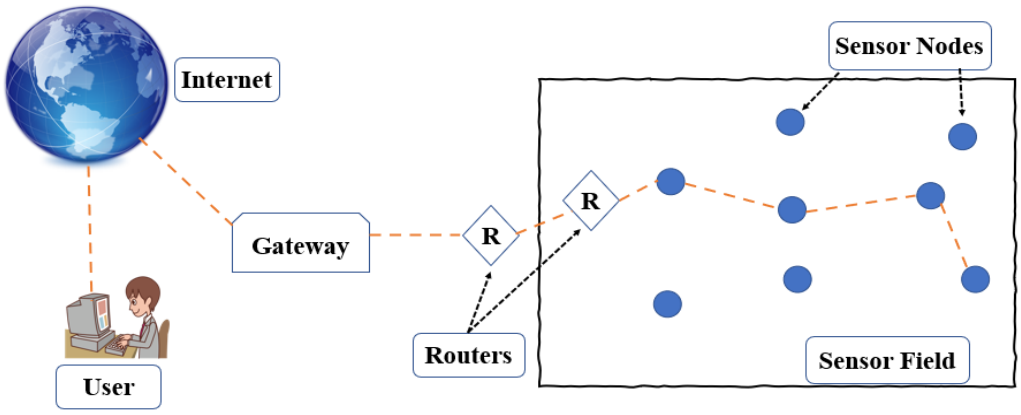

Figure 1.1: A typical Wireless Sensor Network (WSN)

Sensor networks can be categorized into two types: wired or wireless. Due to some disadvantages of wired sensor networks, such as a lot of wiring, maintenance, and deployment difficulties in remote areas, Wireless sensor networks (WSNs) are very popular and commonly used in today's advanced networking and communication sectors. Figure 1.1 shows a typical WSN consisting of nodes, routers, and a gateway. There are two kinds of nodes in any sensor network: sensor nodes (SNs) and actuator nodes (ANs) (Aqeel ur et al., 2014). WSNs utilize different technologies to connect sensors. These technologies include Bluetooth, Wi-Fi, Zigbee, cellular, or Near Field Communication (NFC), etc. One of the great advantages of WSNs is that they are easier to deploy and maintain, also, they offer better flexibility of nodes or devices.

The application areas of WSN are in various domains (Verdone et al., 2010, Akyildiz et al., 2002, Bharathidasan et al., 2001, Sohraby et al., 2007, Yick et al., 2008, Buratti et al., 2009, Boukerche, 2008). With the rapid growth of sensors and wireless technologies, WSNs have emerged as a key factor for the development of the Internet of Things, shortly IoT networks. Simply, IoT is made up of devices, ranging from simple sensors to smartphones and wearables, connected and talk to each other. IoT networks have various applications ranging from the field of home automation to industry applications. The development of smart homes is one of such fields in home automation that is gaining popularity day by day.

Communication protocols play a vital role in IoT networks. The most used and popular communication protocols for IoT networks are Wi-Fi, Zigbee, and Bluetooth which have facilitated the advancement of smart home concepts. For instance, Wi-Fi is an excellent option for data communication and is ideal where the power source or supply is not a problem, like in household devices. Bluetooth is also a good option for exchanging data and can usually be found

in many battery-powered devices, such as computer mice, watches, and sound speakers. Zigbee requires even less transmission power than Bluetooth and is good for a shorter communication range (Challoo et al., 2012). Zigbee, Wi-Fi, and Bluetooth are very common and popular in household environments. In this thesis, the potential problems of spectrum sharing between such IoT technologies (e.g., Wi-Fi and Zigbee) are discussed in a smart home scenario. We will only focus on the coexistence of Zigbee and Wi-Fi networks in this thesis.

Before going any further, let's introduce some of the terminologies and technologies that are not widely known outside the networking and communications fields. This will provide us a brief background in order to grasp the motivation and objective of this thesis.

1.1 Internet of Things (IoT)

The concept of connecting physical objects is gaining popularity day by day resulting in diverse applications of the Internet of Things (IoT). Internet of Things (IoT) is the idea of basically connecting any device with a switch (particularly on and off switch) to the Internet (Morgan, 2014, International Telecommunication Union, 2015, Gillis, 2020). These devices are everything that we basically use in our daily life, include cell phones, washing machines, headphones, coffee makers, lamps, wearable devices, and almost anything else we can imagine (Morgan, 2014). IoT systems are increasingly gaining popularity due to their numerous applications, like home automation (i.e., smart home), medical and healthcare sector (Laplante et al., 2018), transportation sector (Mahmud et al., 2018), infrastructure, and manufacturing sector (Severi et al., 2014), etc. (Al-Fuqaha et al., 2015).

An IoT system or IoT network consists of web-enabled smart devices that use embedded systems, such as processors, sensors, and communication hardware, to collect, send and act on data they acquire from their environments. IoT devices share the collected sensor data to an IoT gateway or network edge devices where data is either directed to the network cloud to be analyzed or the date is analyzed locally. Usually, IoT devices can communicate with each other without any or minimal human intervention (Khan et al., 2016a, Khan et al., 2017). The communications among the network gateway and IoT devices or edge devices happens by the means of IoT communication protocols, such as Wi-Fi, Zigbee, Bluetooth, etc. (Pratt, 2021). Figure 1.2 shows a typical IoT system or network with some of its key elements.

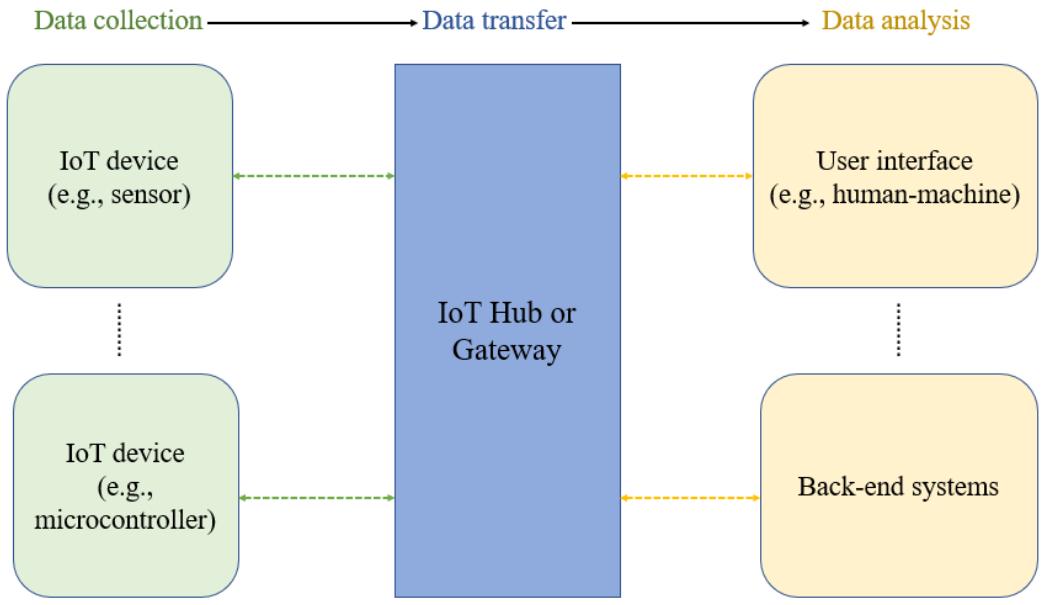

Figure 1.2: A typical IoT system

1.2 IoT Communication Protocols: Zigbee and Wi-Fi

The most vital part of an IoT system is to talk with the connected physical objects to collaborate and share information wirelessly with each other. Because of the significant growth

of IoT network applications in indoor environments, customized IoT-enabled devices are growing at an unprecedented rate to reach consumers diverse demands. One study has shown that the number of IoT devices exceeds the earth's population in 2010 and the number is still growing (Evans, 2011). The total number of devices connected to the internet is projected to cross 25.4 billion in 2030 (Holst, 2021). Therefore, heterogenous device compatible IoT protocols are developing to collaborate among these heterogeneous devices.

Table 1.1: Comparison between Zigbee and Wi-Fi

Indices	**Zigbee**	**Wi-Fi**
Standard	IEEE 802.15.4	IEEE 802.11b/g/n
Frequency bands	(2.4 G,784 M, 868 M & 915 M) Hz (Wang et al., 2014)	802.11b/g/n - 2.4 GHz (2.412G - 2484G) Hz (Electronics Notes)
Number of channels	16	14
Data rate	20 kbit/s (868 MHz) - 250 kbit/s (2.4 GHz)	802.11g – 6 to 54 Mbit/s 802.11b– 1 to 11 Mbit/s 802.11n – 72 to 600 Mbit/s
Power consumption	10 - 100 mW	10 times more than Zigbee
Range	10 - 100 m (Line-of-sight)	1000
Scalability	6000	32
Transmission power	1 mW	50-70 mW <100 mW
Network topology	Star, Tree, Mesh	Star
Main applications	Home automation, Automatic control, Remote control	Local area networking, Wireless access terminal

Popular wireless communication technologies, such as Zigbee (IEEE 802.15.4), Wi-Fi (IEEE 802.11), etc. serves these purposes. Zigbee and Wi-Fi both are the most popular communication protocols for IoT networks in indoor environment applications such as environment monitoring, home automation, device controls, etc. Generally, Wi-Fi is appropriate for the place where power supply is available, like in households and other indoor environments. On the other hand, Zigbee requires less power and suitable for low-range data communications. Like Wi-Fi, Zigbee is not suitable for internet connections or multimedia communications, but it is a good fit for transmitting data from sensors in a field environment.

Wi-Fi is extensively used in indoor environments for internet access, video streaming, etc. Zigbee is well suited for applications where low power consumption, low latency, large scaling capability, low data rate, and flexible topology (De Nardis and Di Benedetto, 2007) are the main criteria. Due to their respective striking attributes, Zigbee and Wi-Fi networks usually coexist in indoor environments like apartment homes or smart homes. Table 1.1 summarizes some of the common attributes of Wi-Fi and Zigbee technologies. The next sections describe how exactly Zigbee, and Wi-Fi protocol works.

1.2.1 Zigbee Protocol

Zigbee is a wireless technology developed as an open global standard to address the unique needs of low-cost, low-power wireless IoT networks. The Zigbee standard operates on the IEEE 802.15.4 physical radio specification and operates in unlicensed bands including 2.4 GHz, 900 MHz, and 868 MHz. Zigbee is commonly used for IoT networks as a communication protocol because of its features like low power consumption, large scaling capability, and flexible topology, etc. Unlike the Wi-Fi networks which are usually used to connect the network

endpoints with the high-speed internet, Zigbee offers much lower data rates and uses a mesh networking protocol to connect network edges to a central hub and creates self-organizing and self-healing networking architecture (Wan et al., 2008).

1.2.1.1 Zigbee specifications. Zigbee protocol is based on the Institute of Electrical and Electronics Engineers (IEEE) Standards Association's 802.15 specifications. In 2003, the 802.15.4 specification got approval for a high-level communication protocol to create personal area networks with small, low-power radios, such as for home automation, other low-power industrial and medical uses, etc. The protocol is very robust in a way that it can be used to facilitate multivendor interoperable offerings. For example, the Zigbee protocol allows devices to communicate in a variety of network topologies (such as star, tree, and mesh) and can have battery life lasting several years. Besides, Zigbee can be used in various hostile RF, Wi-Fi, Bluetooth based environments, which are common in home automation and various industrial and medical applications.

Zigbee protocol is mainly built for wireless sensor networks and control purposes on the IEEE 802.15.4 wireless standard for wireless personal area networks (WPAN) (IEEE SA, 2020). The Zigbee specifications are controlled and maintained by Connectivity Standards Alliance (formerly known as Zigbee Alliance). The Zigbee specifications enhanced the IEEE 802.15.4 wireless standard by adding the network and security layers in addition to the application framework.

There are several Zigbee specifications: Zigbee, Zigbee PRO, Zigbee RF4CE, Zigbee IP, Zigbee 3.0, etc. ZigBee is designed to support smaller networks with hundreds of devices in a single network. Zigbee PRO was developed to provide the fundamental of IoT with the features

to support a low-cost and highly reliable network for device-to-device communications. Founded in 2007, Zigbee PRO also presents Green Power, a new feature for Zigbee that supports energy harvesting technique or self-powered devices that don't require AC power supply or DC powered batteries (Rosencrance, 2017). In short, Zigbee PRO maximizes all the capabilities of Zigbee as well as provides more options for larger networks comprised of thousands of devices. Zigbee PRO operates in the 2.4 GHz ISM band and adds a sub-GHz band (Zigbee Alliance, 2019).

Zigbee RF4CE jointly, developed by Radio Frequency for Consumer Electronics Consortium and Zigbee Alliance (present name Connectivity Standards Alliance), is designed for simple, two-way device-to-device-control applications but doesn’t need the full-featured mesh networking capabilities of Zigbee (Zigbee Alliance, 2008a). RF4CE is designed to offer an immediate, low-cost, low latency, low power, and easy-to-implement networking solution for control-related applications. These applications include but are not limited to entertainment devices, garage door openers, keyless entry systems, and more. RF4CE also provides remote control solutions without line-of-sight restrictions.

Zigbee IP specification aims to provide seamless internet connections to control low-cost and low-power devices a bulk of heterogeneous devices into a single controlled network. This is the first open standard specification for an IPv6-based aimed to provide a full wireless mesh networking solution. Zigbee Smart Energy IP stack is supported by Zigbee IP.

The Zigbee 3.0 has been designed by Connectivity Standards Alliance in 2014. Zigbee 3.0 is developed to provide data communications in noisy RF environments which are very common in home-automation, commercial and industrial applications. Zigbee 3.0 added some new features that were not present in the previous versions (Texas Instruments, 2019). Zigbee

3.0 is based on the Zigbee PRO 2017 (R22). Although Zigbee 3.0 is based on the existing Zigbee standard, the market-specific application profile of the Zigbee is uniformed to allow all devices to be wirelessly connected in the same network, regardless of their market designation and function.

1.2.1.2 System structure of Zigbee technology. Zigbee protocol defines three kinds of nodes: Zigbee Coordinator (ZC), Zigbee Router (ZR), and Zigbee End-Device (ZE). All the types of devices can send and receive data, but they play different roles in the network (Safaric and Malaric, 2006).

- Zigbee Coordinator (ZC): This is the most vital device in the Zigbee network as ZC builds the root of the network tree and acts as a bridge of the Zigbee network. Every Zigbee network must have one coordinator which acts as a hub of receiving and storing important information during the process of data communication among nodes. The coordinator node functions as a Trust Center & repository for the security keys in the Zigbee network. Coordinator nodes are always-on devices, so they require to be powered on all the time during the operation. This requires the coordinator nodes to have a stronger battery capacity than that of the router or end device.
- Zigbee Router (ZR): Zigbee Router is an intermediate node between the coordinator and Zigbee end devices. Besides running an application function, the router acts as a relay to pass data from one to another device.
- Zigbee End-Device (ZE): Zigbee End-Devices are the edge of any Zigbee network. End devices have limited functionalities and can only talk to their parent

devices (either coordinator or router) but cannot relay data from and to other nodes. This causes the end device to stay asleep for a significant amount of time thereby increasing their battery life. Comparing with coordinator and router, the end devices need the least amount of energy.

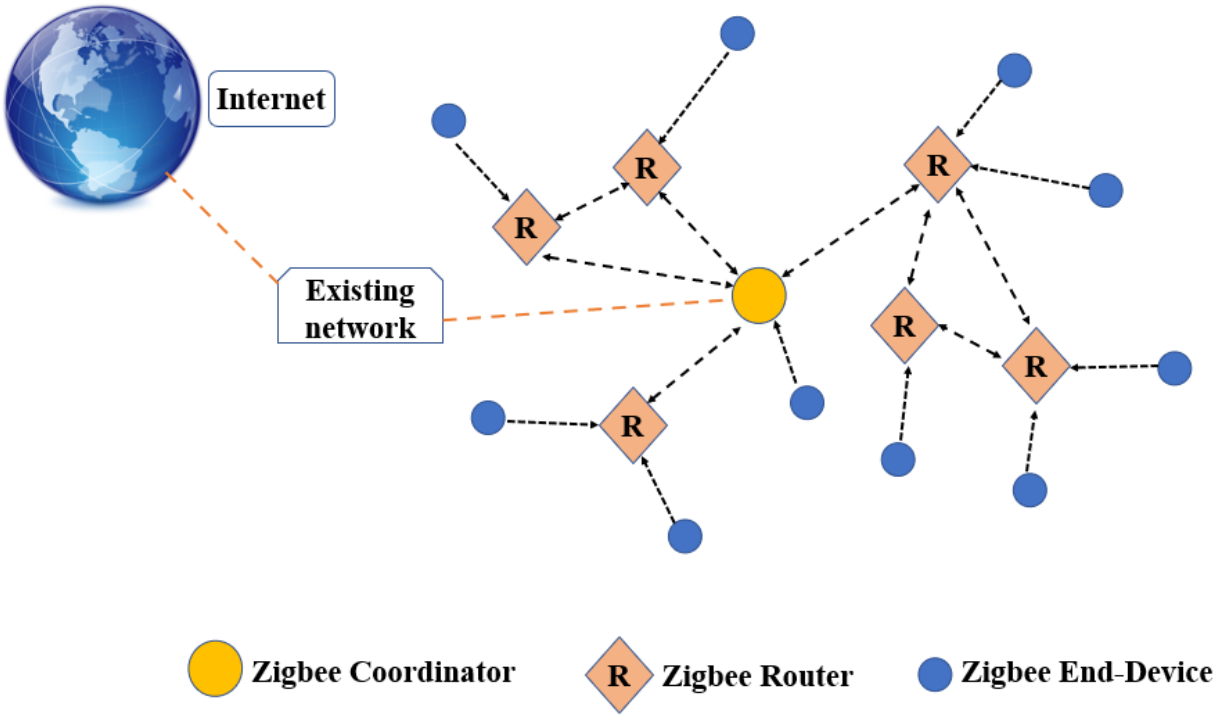

Figure 1.3: A Zigbee mesh network consists of three types of devices

The pattern in which these three components are connected can be star, tree, and mesh networks. Forming mesh networks is one of the popular attributes of the Zigbee. Zigbee uses mesh networking architecture for date communication. A mesh networking structure is a non-synchronized Local Area Network (LAN), Wireless LAN (WLAN), or Virtual LAN (VLAN) wherein one device can talk to multiple devices and the data packets travel on no fixed routes, offers better flexibility and faster communication across devices. A mesh network can be built in

one of the two decentralized connection arrangements: full mesh topology or partial mesh topology.

In a full mesh networking topology, every network node is connected directly to other nodes creating a reliable network. In a partial mesh network architecture, some network nodes are connected to other network nodes, but some nodes are only connected to that nodes which exchange the most data. Mesh networking also means “self-healing networks”, because there are multiple routers in the network. A typical mesh network with three kinds of Zigbee devices (Zigbee coordinator, Zigbee router, and Zigbee end-device) is shown in Figure 1.3.

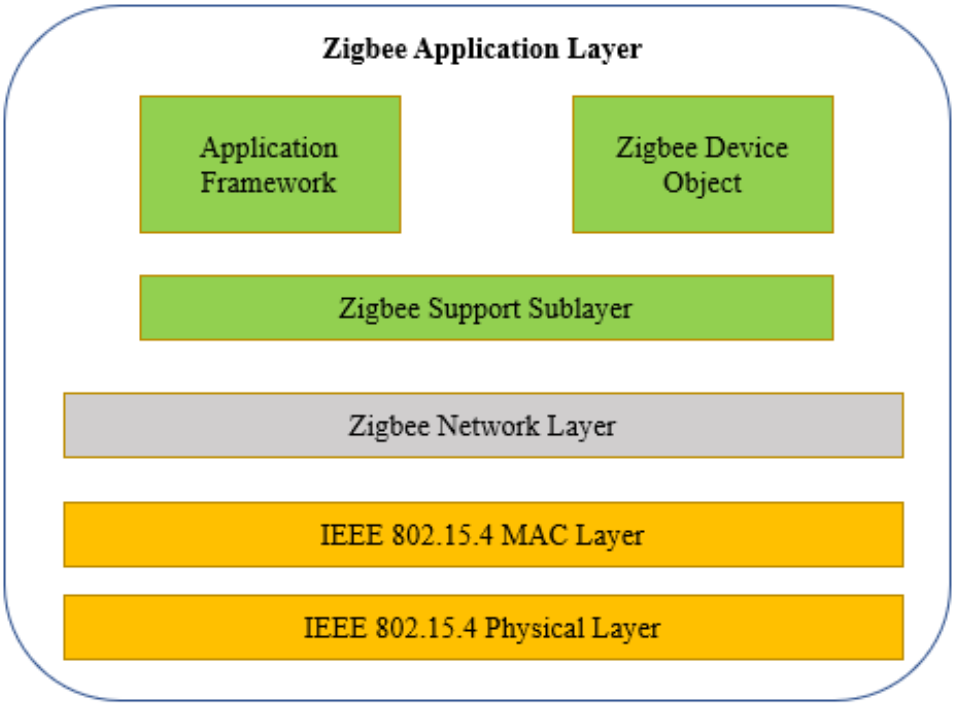

Figure 1.4: Zigbee protocol stack

1.2.1.3 Zigbee protocol architecture. Zigbee protocol structure consists of different layers as per IEEE 802.15.4 standards. Each layer has its own features and function. ZigBee is

developed on the top of the physical and MAC layers of IEEE 802.15.4 where the upper layers of the architecture are defined by the Zigbee specifications which define the way of communication of a node (Carlos-Mancilla et al., 2016). Figure 1.4 shows the basic protocol architecture of Zigbee.

- Physical layer: The physical layer provides data transmission capabilities of the Zigbee network. This layer performs modulation as well demodulation of the transmitted and received signals. This layer also determines the channel, channel frequency, link quality/strength of a received signal of a link - Link Quality Indication (LQI), etc. There are three operating states defined for the Zigbee devices: transmitting, receiving, and sleeping. This allows the Zigbee devices to save energy when the devices sleep.
- MAC layer: This layer is responsible for reliable data communication between different networks using Carrier Sense Multiple Access Collision Avoidance (CSMA) scheme.
- Network layer: The network layer performs all network-related operations. These operations include maintaining a connection between router and end devices, connection and disconnection to the network, routing of the data packets, and configuration of different devices. The routing operation is performed using Ad hoc On-Demand Distance Vector Routing (AODV) protocol. The details of the AODV routing vector can be found in (Royer and Toh, 1999).
- Application support sublayer: The layer is responsible for the interface of the Zigbee device with various object application devices in order to communicate

through the network layer. This layer is specified by the IEEE 802.15.4 specification. The application support sublayer takes the responsibility to interface between the Zigbee system and end users. This layer is responsible for providing service to Zigbee profiles based on their services, application, and needs.

- Application framework: Zigbee application framework provides two types of information administrations. These include developer characterized information, application objects related information. Zigbee device object (ZDO) provides an interface between application items and the APS layer in ZigBee gadgets. Zigbee application framework is in charge of starting, distinguishing, and engaging different gadgets to the system. Application profiles are used to manage the configuration of applications; these application profiles include but not limited to Home Automation, Zigbee Smart Energy 2.0, etc.

1.2.1.4 How Zigbee protocol works. Zigbee transmission technology works in two modes: Beacon mode and Non-Beacon mode. In Beacon enabled mode, the Zigbee coordinator and router devices work on always-on mode and constantly monitor any changes in data flows, therefore, more power is dissipated. In this mode, the network routers and coordinators do not sleep as at any time any network nodes can receive signals or data to respond and communicate.

On the other hand, the coordinators and routers don't need to stay awake all the time in Non-Beacon mode. If there is no data transmission, the coordinators and routers enter in sleeping mode. This is an on-off cyclic process that happens in a periodic order. This mode allows devices to run for a long time but in a lower duty cycle.

1.2.1.4.1 Forming and joining the Zigbee network. Zigbee networks are defined as Personal Area Networks or PANs. According to the Zigbee protocol, the coordinator is the only node that can initiate a network. For this reason, each Zigbee network has only one coordinator. The network starts by configuring a node as coordinator with a unique PAN identifier (PAN ID) and operating channel for that network that is usable and not interfering with other wireless networks. This is because WLAN also operates at the same 2.4 GHz radio bands. It's worth mentioning here that the dynamic assignment of PAN ID is the alternate way of preconfiguring the coordinator PAN ID. The dynamic assignment works by checking other PAN IDs of networks already in the operating nearby of the new network so that PAN ID does not conflict with other networks. Once all the necessary parameters are established and the network is initialized the coordinator can allow other devices such as routers and end devices to join the network. The coordinator sends a broadcast beacon request to all nearby routers and end devices. By this process, the coordinator can receive the PAN ID of nearby routers and end devices. This process is called beacon scan or PAN scan. Once the scan process complete, the routers or end devices send an association request to the coordinator for joining the network.

Joining a network is a process of discovering the network by nearby located networking nodes. So, before joining the network a router or end device must be located near the coordinator or another router device. There are two ways to join a network:

- MAC association and
- Network rejoin

MAC association is implemented by the MAC layer and the Network rejoin is performed by the network layer. Let’s talk about forming a simple network using MAC association.

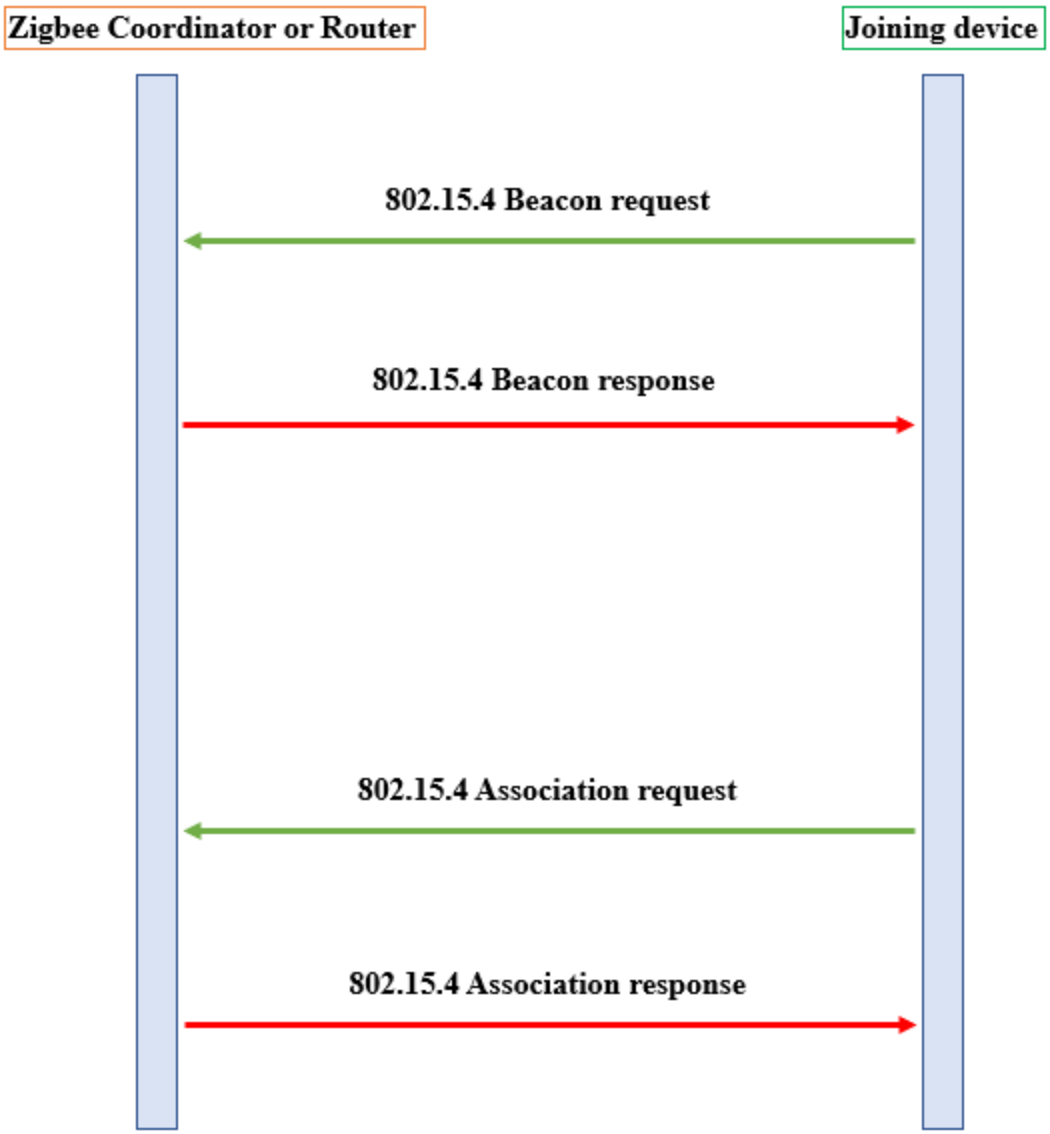

Figure 1.5: A simple process of forming and joining a Zigbee network

Figure 1.5 describes a simple process of forming and joining a Zigbee network. If there is any coordinator with a valid PAN ID, the next step for the routers or end devices will be to find out if the coordinator allows them to join the network or not. So, they start the process of PAN scan or beacon request. Therefore, the joining process starts from using a beacon request by the

Zigbee router or Zigbee end-device. Nodes send beacon requests to get a response from the coordinator. Zigbee coordinator responds to this beacon request. After getting to know that the router or end device can join the coordinator, they will send an association request and will join the network upon receiving the association response. Whether the coordinator or router will allow any new devices to join the network depends on two issues:

- Number of already existing end device and
- Permit joining attribute

1.2.1.4.2 Zigbee routing. Routing is the process of selecting the route or path through which the data will flow between the source and destination. The Zigbee coordinator and routers are fully responsible for discovering and maintaining the route in a network. Zigbee end devices cannot perform route discovery, Zigbee coordinator acts on behalf of Zigbee end devices.

The Zigbee routing algorithm is based on "Distance Vector" (DV). Zigbee Alliance (present name "Connectivity Standards Alliance") suggested a well-defined routing protocol as a default protocol for Zigbee or IEEE 802.15.4 networks: Ad hoc On-Demand Distance Vector (AODV) (Perkins and Royer, 1999). As per the AODV protocol, a node that has data to be transmitted sends a Route Request packet (RREQ) using broadcast to all other nodes. The nodes receive the RREQ request and rebroadcast to other nodes until the RREQ packet reaches the destination node. During this process of rebroadcast of RREQ packet, the intermediate nodes note down the source address of the RREQ packet and its corresponding link cost (Zigbee Alliance, 2008b, Secci and Buratti, 2013). Reporting link cost allows the protocol to compare among the path costs and to choose the best path between the source and destination nodes. Once

the RREQ is received by the destination node, the destination node replies to the request by sending a Route Reply (RREP) packet in unicast mode back to the source in the reverse path.

In the case of link failures or the expiration or entries in the routing table, the nodes repeat the RREQ/RREP transmission process to refresh the route and to update the entries in the routing table. The RREQ/RREP transmission process is used only for the unicast data transmission, while the broadcast packets are just forwarded by all routers to the other nodes of the network.

1.2.2 Wi-Fi Protocol

Wi-Fi stands for Wireless Fidelity is based on the IEEE 802.11 family of wireless standards. Wi-Fi is primarily used for Wireless Local Area Network (WLAN) of devices and internet access. Wi-Fi is the most used local area network in the world, connecting home and small office networks to laptop and desktop computers, smartphones, smart TVs, and other electronic devices to the internet (Wiki, 2021b). Wireless Access Point (simply Access Point, AP) is one the of great benefits of Wi-Fi which is used in home and public places like airports, restaurants, hotels, and institutions to provide public internet access to mobile users.

Wi-Fi is a trademark of Wi-Fi Alliance, a non-profit organization that maintains and takes responsibility for testing the gadgets that claim to fulfill the criteria of Wi-Fi-based networking. Wi-Fi as a wireless protocol uses the 2.4 GHz ISM frequency band which is free and requires no license. The later versions of Wi-Fi also work at 5 GHz frequency along with 2.4 GHz.

1.2.2.1 Wi-Fi standards. Wi-Fi uses 802.11 networking standards which come in several flavors. Wi-Fi defines 802.11x standards where x is the version of Wi-Fi. Popular Wi-Fi versions are a, b, g, and n. Table 1.2 shows the IEEE 802.11 Wi-Fi protocol summary with different popular standards (PHILLIPS, 2021).

Table 1.2: Wi-Fi standards and their features

Protocol name	Frequency	Maximum data rate	Comments
Legacy 802.11	2.4 GHz	2 Mbps	The original version of the IEEE 802.11.
802.11a	5 GHz	54 Mbps	The is one of the oldest standards; not compatible with b/g network.
802.11b	2.4 GHz	11 Mbps	Compatible with g network to support more devices
802.11g	2.4 GHz	54 Mbps	This is the most popular version of Wi-Fi network types.
802.11n	2.4 and 5 GHz	100 Mbps	The fastest type of network. The speed can be up to 600 Mbps with perfect condition.
802.11ac	5 GHz	1.3 GHz	The newest standard. 802.11ac is backward compatible with 802.11n.

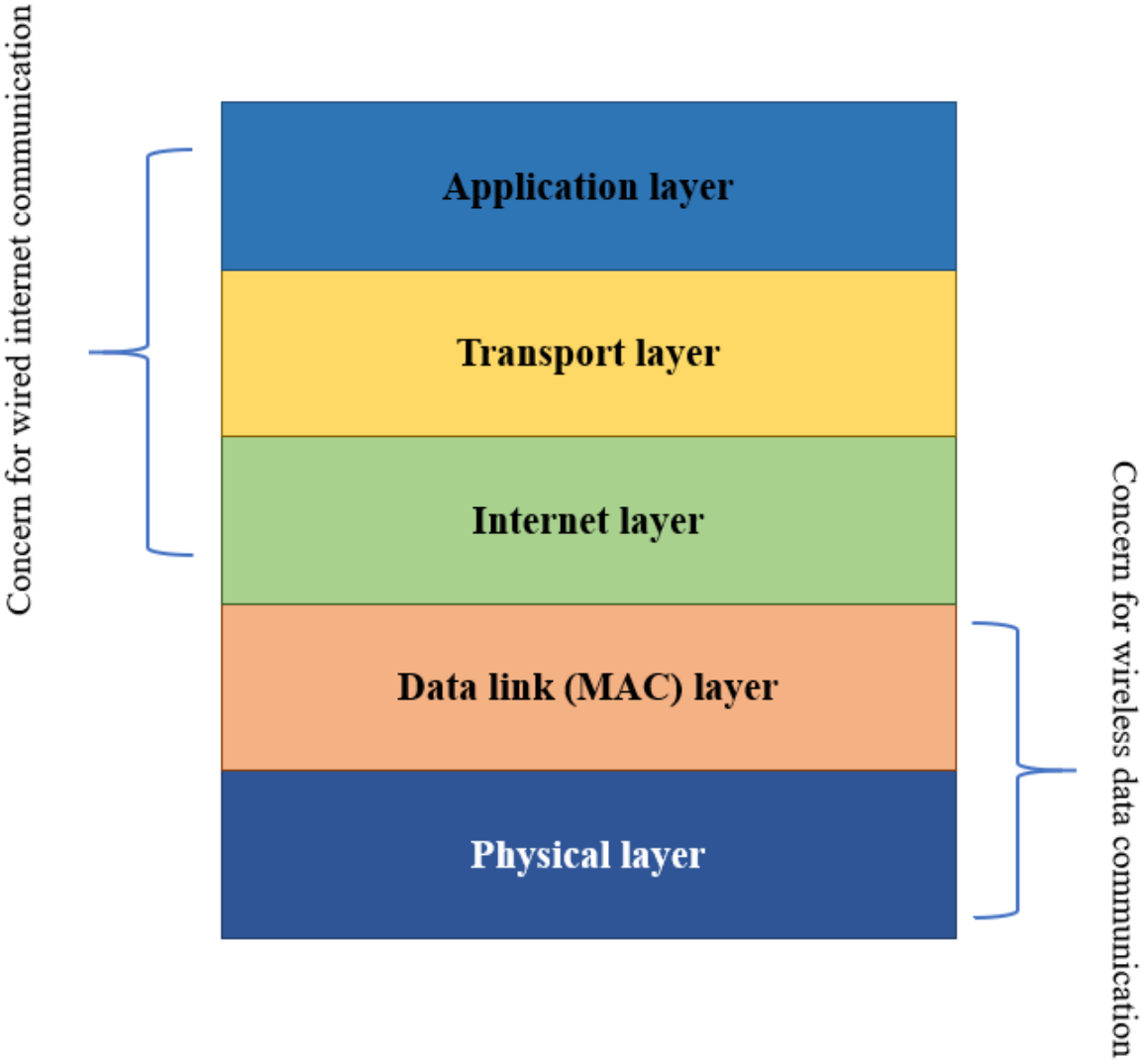

Figure 1.6: Wi-Fi protocol stack

1.2.2.2 Wi-Fi protocol stack. The protocol stack in Wi-Fi defines the data communication in Wi-Fi networks. Wi-Fi protocol stack consists of five layers (van Bloem and Schiphorst, 2011):

- Application layer
- Transport layer

- Internet layer
- Data link (MAC) layer
- Physical layer

whereas the top three layers (application layer, transport layer, and internet layer) concern with the wired internet communication, and the bottom two layers (data link layer and physical layer) of the protocol stack involve wireless communication. Wireless LAN (Wi-Fi) utilizes the physical layer and MAC layer (data link layer) from the well-known OSI (Open Systems Interconnection) model. Figure 1.6 shows the Wi-Fi protocol stack in a layered structure.

- Physical layer: The physical layer of the Wi-Fi protocol stack takes care of the radio interface and wireless data communication. Wi-Fi standards (IEEE 802.11 protocol standards) are designed in such a way that other interfering networks such as microwave ovens, telephones, etc. can work together in the 2.4 GHz ISM radio band. Besides, the data transmission speed and the network's communication quality should be maintained. Upon fulfilling these criteria there are three data exchange schemes adapted by the 802.11 physical layer: Infrared, Frequency Hopping Spread Spectrum (FHSS) technique, and Direct Sequence Spread Spectrum (DSSS) technique. The physical layer of the IEEE 802.11 protocol family can be classified into two sub-layers:
  (i) Physical Layer Convergence Procedure (PLCP) which is responsible to prepare the data packets to be transmitted across the radio channel and analyze the received data packets.

(ii) Physical Medium Dependent (PMD) Protocol performs the modulation of transmitted data packets before they are transmitted and demodulates the wirelessly received data packets.

- Data link (MAC) layer: On the top of the physical layer the Medium Access Control (MAC) layer is placed. MAC layer synchronizes the transmissions of data; the MAC layer maintains the communications between 802.11 wireless stations by coordinating and controlling access to the shared radio channels. Data communication over the wireless medium is also maintained by this layer. To ensure the reliability in data transmission and to manage the channel access between 802.11 stations, the MAC layer utilizes Carrier Sense Multiple Sense with Collision Avoidance (CSMA-CA) technique.
- Internet layer: The Internet layer is responsible for the logical transmission of data packets over the internet. In the layered stack, the internet layer transmits the data packets to its immediate lower layer (data link layer). The internet layer maintains the optimal routing of data packets from the source to the destination.
- Transport layer: This layer maintains the integrity of data transmission; enabling the host to send and receive error-corrected data over the network. The main responsibility of this layer is to provide host-to-host communication services for the running applications.
- Application layer: The application layer is the highest layer of the Wi-Fi protocol stack. The main responsibility of this layer is to provide services directly to the application processes.

1.2.2.3 Communication in Wi-Fi. Wi-Fi works like other wireless devices- it uses radio frequency to send signals between networking devices. Data communication in Wi-Fi can be categorized into three phases:

- Phase 1: The communication starts from the data preparation for transmission, encoding the data, and changed it into frames. The frequency for data transmission is also chosen in this phase based on the wireless data transmission technique.
- Phase 2: Where data is transmission through the wireless medium as a medium of radio signal transmission. The wireless medium can be air medium.
- Phase 3: Where data is received from the air, decoded, retrieved the information, and then used.

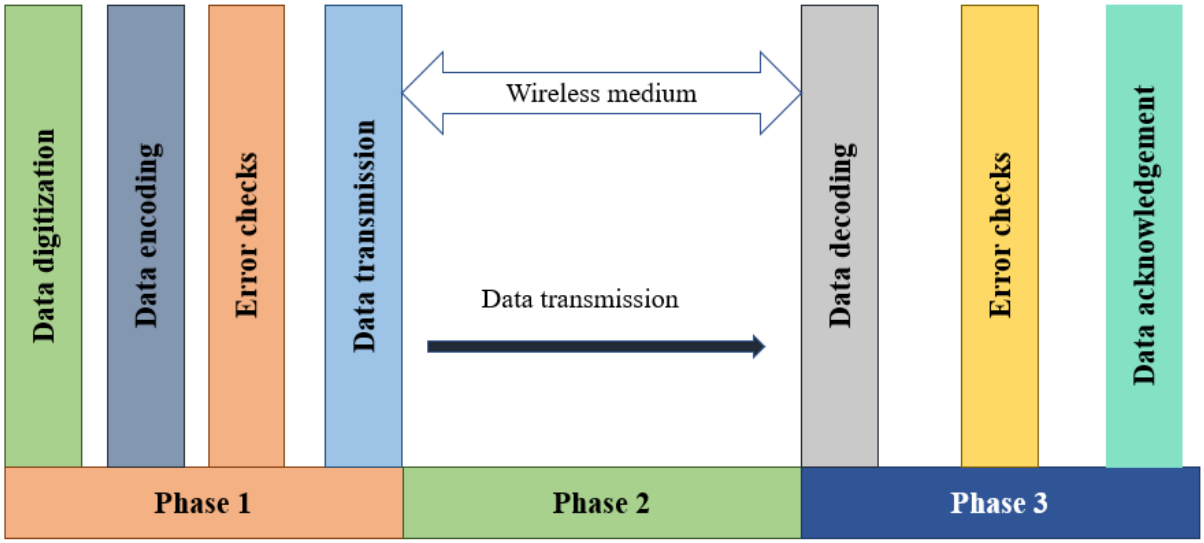

Figure 1.7: Data exchange in Wi-Fi

All of the phases use digital communications spread spectrum techniques for multiplexing the signal and use necessary security measurements for the integrity of the information. Three phases of data exchanges are visualized in Figure 1.7.

1.3 Smart Home

Home automation is one of the popular concepts of modern-day technologies. Home automation as its name implies is building automation for a home, called a smart home. Simply, a smart home refers to an as usual home or house where not just computers and smartphones, but everything: clocks, speakers, lights, doorbells, cameras, windows, window blinds, water heaters, appliances, and cooking utensils are connected to and controlled by the internet. And the data communication among these devices happens by the means of the IoT network which is a key component of home automation and smart homes.

1.4 Spectrum Sharing and Interference

As the demand for wireless devices, networks, and services is growing increasingly, the open radio frequency spectrum—that is the space in which wireless signals can be sent— has been an incredibly valuable asset. Simply, the optimization of the airwaves or wireless communication channels can be called spectrum sharing. Spectrum sharing enables multiple categories of users to safely share the same frequency bands (EITC, 2012). Spectrum sharing is very crucial because the growing demand for wireless networks is crowding the radio frequency/ airwaves.

All spectrum is fundamentally shared. For example, thousands of radios and hundreds of millions of mobile users share the same licensed spectrum which is coordinated by a single

operator. Similarly, an unlicensed spectrum is shared across Wi-Fi access points and end-user devices. Smartphones, the Internet of Things, military and public safety radios, wearable devices, smart vehicles, and countless other devices all depend on the same wireless bands of the electromagnetic spectrum to share data, voice, and images. In the case of IoT networks, the unlicensed 2.4 GHz industrial, scientific and medical (ISM) radio bands are shared among different IoT communication protocol technologies such as Wi-Fi and Zigbee. Figure 1.8 shows the frequency distributions between Wi-Fi and Zigbee in the 2.4 GHz ISM frequency band.

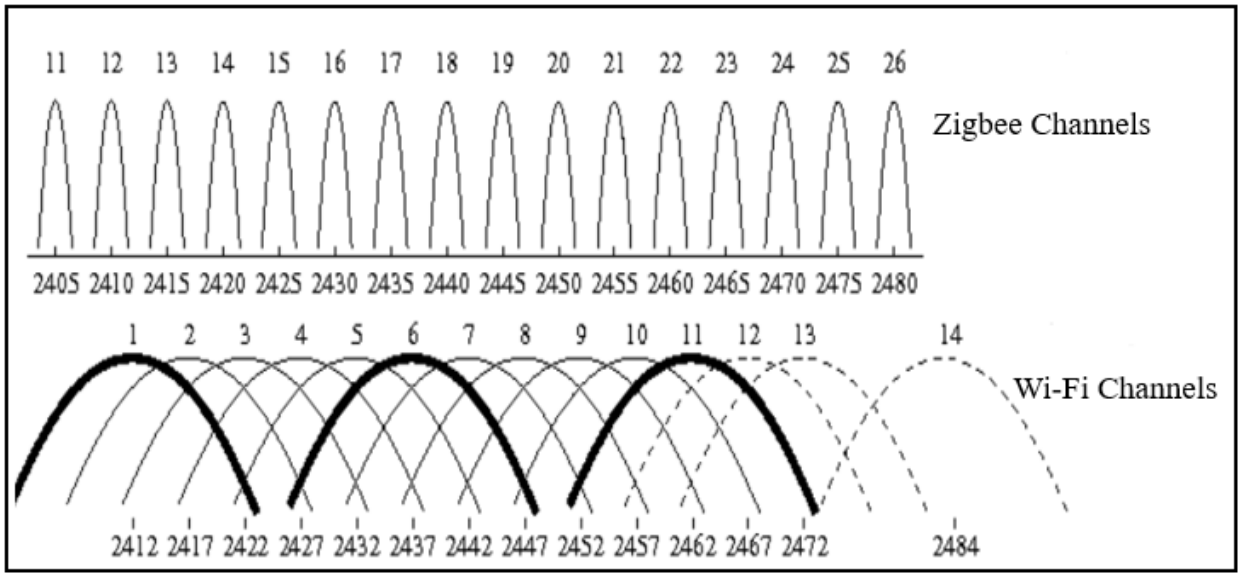

Figure 1.8: Frequency distributions between Wi-Fi and Zigbee in the 2.4 GHz

In the 2.4 GHz radio band, Wi-Fi has 14 channels (channel# 14 is reserved and not in use), spaced 5 MHz apart from each other except for a 12MHz space before channel 14 (IEEE Computer Society LAN/MAN Standards Committee, 2007). On the other hand, Zigbee has 16, 5 MHz channels in the 2.4GHz band. Several channels overlap with Wi-Fi channels. Wi-Fi Channel# 1 overlaps with Channels 11, 12, 13, and 14 for example. As the number of Zigbee and

Wi-Fi-enabled devices is increasing day by day, the coexistence of such heterogeneous communication devices may cause interference to each other.

Interference is simply to interfere with each other. In radio frequency, interference is caused by two or more radios, each on different wireless networks, using the same frequency. For instance, a Wi-Fi-enabled device operating at channel 11 can interfere with a Zigbee-enabled device operating at channel 22. This type of interference may cause severe performance issue for communication networks.

1.5 Statement of the Problem and Objective

1.5.1 Problem Statement

The concept of Smart homes is gaining popularity day by day because of the utilization of many diverse technologies. The Internet of Things (IoT) is one of such striking technology-based concepts, which interconnects everything in a house that we basically use in our daily life, including cell phones, television sets, washing machines, headphones, lamps, wearable devices, and almost anything else we can think of (Morgan, 2014). The vital part of an IoT system is to communicate and collaborate wirelessly among different types of devices connected to it. Popular wireless communication technology, ZigBee (IEEE 802.15.4) serves these purposes because of its numerous advantages, for example, low power consumption, low data rate, large scaling capability, low latency, and flexible topology (De Nardis and Di Benedetto, 2007). Another popular technology, Wi-Fi (IEEE 802.11) is also extensively used in indoor environments for internet access, video streaming, etc. Due to their striking attributes, Zigbee and Wi-Fi networks usually coexist in indoor environments like smart homes.

The growing number of IoT devices and their finite number of operating channels in the 2.4 GHz radio band (e.g., 14 and 16 channels for Wi-Fi and Zigbee enabled devices, respectively) is making the network architecture of the IoT system more complex and congested. This results in an ultimate challenge to find free channels in 2.4 GHz for their operation, especially in indoor environments. This is because Wi-Fi and Zigbee have multiple channels overlapping in the 2.4 GHz ISM radio band as shown in Figure 1.9. The situation becomes worst where multiple IoT networks such as Wi-Fi, Blue-tooth, Zigbee coexist, resulting in interference with each other. For example, the operation of a Zigbee-enabled device can be interrupted badly due to the interference of a Wi-Fi network and vice versa. But due to the low transmission power of Zigbee (Thonet et al., 2008), it tends to suffer more from interference by other wireless technologies, like Wi-Fi, operating in the same frequency band. Therefore, the coexistence of Wi-Fi and Zigbee in proximity creates a great challenge in home automation.

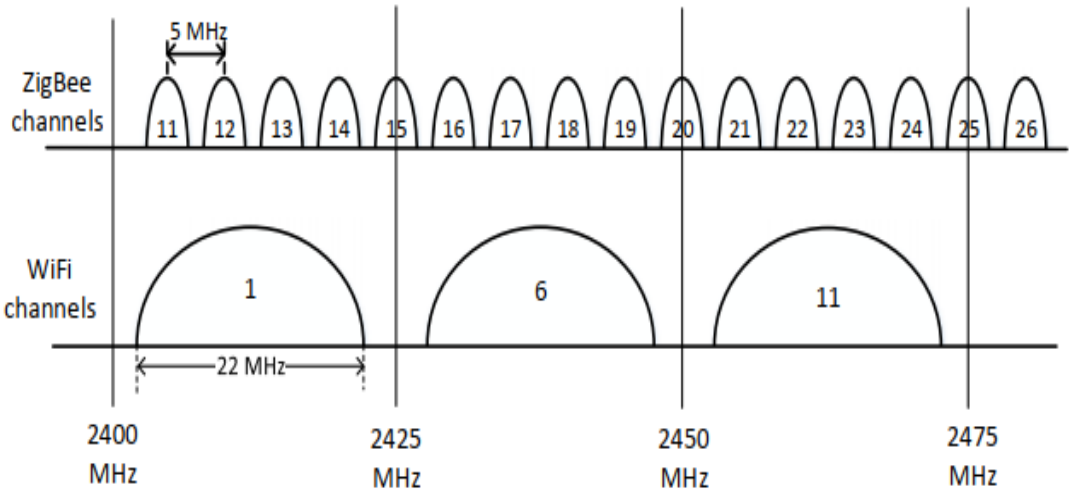

Figure 1.9: Zigbee and Wi-Fi channels in the 2.4 GHz ISM band

To facilitate the coexistence of Zigbee and Wi-Fi networks in smart home applications, several research have been conducted so far on different case studies. For example, WiseBee (Jacob and Ravi, 2015) is one of the powerful suggested mechanisms to ease the coexistence of Zigbee and Wi-Fi networks in proximity but this mechanism fails to provide a comprehensive solution. WiseBee is a simulation-based solution and is suggested for a single-hop network. But in these days, we cannot rely on only a single hop network as the number of IoT devices in indoor environments (e.g., smart homes) is increasing day by day. Also, this solution is simulation-based whereas in this thesis we aimed to work on a real-life testbed deployed in an actual apartment home environment. Another well-known suggested technique on this issue is BuzzBuzz (Liang et al., 2010). Again, this technique fails to provide a viable solution as this mechanism is suggested based on software-implemented results, not from an actual radio chip. Another drawback is that the BuzzBuzz is proposed for midsize networks whereas today's IoT network can be made of hundreds of devices. Another prominent work on this field and close to this thesis theme has been performed by Shi et al. (2013). In this work, the authors the received power and packet loss rate of a Zigbee network in an actual household environment. This research work provides a good reference study for deploying the IoT networks in actual smart home scenarios. But the major downside of this study is that the authors have only considered the Zigbee network to conduct the experiments. So, this study also doesn't provide a comprehensive study to ensure the coexistence of Zigbee and Wi-Fi networks.

All of the above-mentioned studies have failed to some extent to provide a comprehensive Zigbee performance study and a viable solution on the coexistence of Zigbee and Wi-Fi. Motivating by these drawbacks, in this thesis, we have provided a comprehensive

performance study of the Zigbee network deployed in an actual apartment home environment mimicking a smart home. To recreate an actual network scenario in an apartment home, we have also added a well-known and commonly found wireless network in an apartment home, Wi-Fi to our testbed. This inclusion provides the heterogeneity of the wireless networks in the case of smart homes where multiple heterogenous networks like Zigbee, Wi-Fi, etc. can be found. This performance study of the Zigbee network will help us to understand the actual behavior of IoT networks in the case of indoor applications which will further pave the way to find a viable and comprehensive solution for the coexistence of Zigbee and Wi-Fi networks in smart home applications.

1.5.2 Objective

Taking into account the challenges for Zigbee networks in smart home environment as described in section 1.5.1, this thesis attempts to present a comprehensive experimental study of the performance of a Zigbee network in terms of the Received signal strength indicator (RSSI), packet delay, Packet Drop Rate (PDR), and loopback throughput. To get to the real feeling of a smart home environment, we conducted all of our experiments in an apartment home by changing the operating channels of Zigbee and Wi-Fi, the distances between Wi-Fi and Zigbee devices, the transmission interval of Zigbee packets, Zigbee RF payload size, and transmit power of Zigbee transmitter. Our experimental data from loopback throughput shows that bidirectional traffic significantly affect the network performance

It’s worth mentioning here that our first attempt to understand the performance of a Zigbee network was the short version of the present work (Dash and Peng, in press). In the current thesis work, we have presented more comprehensive experimental data and empirical

analysis overcoming some data limitations of the previous work. In this work, first, we carried out some baseline studies on the Zigbee network without the presence of a Wi-Fi network, and then, we analyzed the performance of the Zigbee network in the presence of a Wi-Fi network to realize the behavior of the Zigbee under different interference scenarios.

1.6 Contributions of this Thesis

Some highlights of the contributions of this thesis are listed as follows:

- Presented a step-by-step study of Zigbee's performance with and without the presence of Wi-Fi traffic
- Reviewed some recent related works on the coexistence of Wi-Fi and Zigbee.
- Offered a detailed analysis of experimental results found from a real-life testbed scenario using an apartment-based indoor environment mimicking a smart home.

1.7 Research Hypothesis

The experiments were conducted in an apartment-based indoor environment. The apartments in a building stay very close to each other and every apartment has its own wireless connectivity such as a Wi-Fi network. We detected some unwanted Wi-Fi networks in our experiment testbed region. Therefore, the experimental testbed was never free from the impact of those neighbor's networks (e.g., Wi-Fi networks). To have minimal impact from such unwanted networks and other sources on the testbed networks, we conducted the experiments at midnight when the neighbors' Wi-Fi network usages were low. We used some Wi-Fi network scanner application software like MetaGeek's inSSIDer (Home-Network-Help.com, 2008) and Xirrus

Wifi Inspector (Chen, 2016) to scan those unwanted Wi-Fi networks to ensure their minimal usage time frames. We ignored such unwanted Wi-Fi networks during the experiments. So, the experimental results would have been more accurate and reliable if we could completely avoid the impact from such unwanted traffic sources on testbed networks using special devices like Wi-Fi signal jammers.

Modern home microwave ovens operate at the 2.4 GHz frequency (Matink, 2020). In theory, a properly shielded microwave shouldn't leak any radiation, but the reality is that they can leak quite a bit, resulting in electromagnetic, or radiofrequency (RF) interference to the networks that also operate at the same 2.4 GHz spectrum. Other interference sources can include ultrasonic pest control devices, toaster ovens, etc. This interference at 2.4 GHz can be impactful and harmful for other wireless networks (e.g., Wi-Fi networks and Zigbee-enabled devices) located in the same indoor environments such as apartment homes. To avoid this interference, all such smart devices were kept off during the experiments. Still, there was a chance of getting impact from neighbor apartment’s devices. Controlling such unwanted impacts can improve the accuracy of the experimental results.

1.8 Thesis Outline

In this thesis, the performance of a Zigbee network is analyzed with and without a Wi-Fi network in an apartment-based indoor environment mimicking a smart home. The test data were taken under different interference circumstances with various networking and communication parameters. To study the behavior of the Zigbee network, the data were collected in terms of received signal strength indicator, packet delay, packet drop rate, and loopback throughput. The rest of this thesis book is outlined as below:

Chapter II. Literature Review: The relevant state-of-the-art on the coexistence of Wi-Fi and Zigbee networks are discussed in this chapter.

Chapter III. Motivation for the Thesis: This chapter offers the motivation behind the thesis topic and the experimental setup.

Chapter IV. Experimental Setup and Methodology: This chapter illustrates the experimental testbed and methodology used to obtain the results. The instrumentation and design of both Wi-Fi and Zigbee networks are also described here.

Chapter V. Experiments and Results Analyses: Experimental settings for the experiments and experimental results are reported in this section. In-depth analyses and comparisons among empirical data are also discussed in this chapter.

Chapter VI. Summary and Conclusion: An overall summary of the thesis problem and experiments are discussed. Finally, the chapter is closed with a conclusion.

1.9 Chapter Summary

In this chapter, we discussed the technical background of the thesis topic. We learned about IoT networks and their protocols. Zigbee and Wi-Fi are the most used protocol for IoT networks in indoor environments, but they have compatibility issues when they coexist in proximity. We reviewed the working principles of Zigbee and Wi-Fi protocols as well as their protocol stack. Zigbee and Wi-Fi share the unlicensed 2.4 GHz radio band. We discussed how this spectrum sharing can create interference issues with each other. In this chapter, we talked about our research problems, motivations, thesis objectives, and contributions.

CHAPTER II

LITERATURE REVIEW

Wi-Fi and Zigbee have some overlapping channels in the 2.4 GHz radio band as presented in Figures 1.8 and 1.9. Therefore, the stronger Wi-Fi networks interrupt weaker Zigbee communications adversely when they coexist in proximity (Thonet et al., 2008). Due to the popularity of Zigbee and Wi-Fi technologies in short-distance and low power communications, especially in indoor applications, the study of the coexistence of these two networks has earned a great point of interest among researchers. Different studies and experiments have been conducted to understand the impact of the coexistence of Zigbee and Wi-Fi networks on communication performance. Generally, it is considered that the impact of Zigbee on Wi-Fi networks is negligible, but some papers have pointed out that in some cases Zigbee significantly impacts Wi-Fi communication (Yoon et al., 2006, Pollin et al., 2008). As the study of Zigbee interference on Wi-Fi networks is not our major focus for this thesis, we are leaving this issue here and focusing on only Zigbee communication performance.

To draw the related recent state-of-the-art of our area of interest, I have divided this chapter into two sections: 2.1. interference study of Wi-Fi on Zigbee and 2.2. potential ways to ensure the coexistence of Wi-Fi and Zigbee.

2.1 Interference Study of Wi-Fi on Zigbee

The performance of Zigbee networks in terms of Packet Loss Ratio (PLR) and Packet Error Rate (PER) has been evaluated by Yang and Yu (2009) with the presence of 802.11b/g interference traffic. Incel et al. (2006) have analyzed the interference level of IEEE 802.15.4 standardized wireless sensor networks by varying channel spacings with respect to the distance of a receiver to a jammer and a transmitter. The impact of Wi-Fi interference on Zigbee networks with respect to PLR and Average Round Trip Time (RTT) by using overlapped and non-overlapped channels have been analyzed by Abrignani et al. (2014).

The effect of interference in the case of adjacent and alternate channels has been investigated by Khan et al. with respect to packet drop ratio (Khan et al., 2016b). A comprehensive survey to evaluate the impact of continuously changing communication environments on various networking parameters (for example, RSSI and latency) has been conducted by Sherazi et al. (2016) in the presence of multiple physical obstacles that may downgrade the overall performance of the network severely. Eventually, a suitable Zigbee frame size of the ZigBee packet has been suggested for different situations. 802.11 interference on Zigbee has been studied by Hou et al. in the case of ZigBee medical sensors (Hou et al., 2009).

While all the pieces of work discussed above are related to the coexistence of Wi-Fi and Zigbee networks, some studies have also been conducted solely on Zigbee networks to understand their performance as wireless sensor networks in indoor environments. For example, Hyncica et al. (2006) has found based on the results obtaining from a series of experiments under an indoor environment of a supreme condition like communication through drywalls that the effective range of a Zigbee network is approximately 12 meters. Piyare and Lee (2013) have

evaluated XBee module-based Zigbee wireless sensor networks for both single-hop and multi-hop network scenarios and claimed the modules are perfect for applications that require lower data rates. Results obtained from a testbed in an actual household environment have shown the network performance in the line-of-sight case is better than non-line-of-sight (Shi et al., 2013).

2.2 Potential Ways to Ensure the Coexistence of Wi-Fi and Zigbee

Besides analyzing the interference, some potential ways and scopes have been suggested by some authors to facilitate the coexistence of Zigbee and Wi-Fi networks in the same place. Traditional methods to mitigate interference between ZigBee and WLAN are to change the MAC frame structure or MAC parameters which arise communication complexity between these two technologies. This issue can be addressed by inserting a transmission time interval between two consecutive packets of Wi-Fi traffic (Nomura and Sato, 2014). Another way called WiseBee has been proposed to help the coexistence of ZigBee and Wi-Fi in IoT systems (Jacob and Ravi, 2015). A heterogeneous network integrating multiple wireless technologies has been proposed by Wang and Yang (2017) to facilitate Wi-Fi networks to access Zigbee. A Cognitive Radio (CR) Algorithm for mitigation of interference of IEEE 802.11 b/g/n network to IEEE 802.15.4 network has been presented by Mishra (2019) based on the analytical and empirical model of packet error rate (PER).

The Extended Network Allocation mechanism has been demonstrated by Leugner and Hellbrück (2019) which reduces a maximum of 50 percent IEEE 802.15.4 frame losses in the case of strong interference. A comparative study between Advanced Clear Channel Assessment and Clear Channel Assessment mechanism has been conducted by Leugner and Hellbrück (2018). A multiple radio channels-based adaptive scheme has been designed and evaluated by

Won et al. (2005) address the coexistence of 802.15.4 and 802.11b in the case of large-scale sensor network applications. BuzzBuzz, a MAC solution has been proposed by Liang et al. (2010) to enable the coexistence of Wi-Fi and Zigbee networks. This solution is particularly effective to mitigate Zigbee packet loss due to bit error.

Though some suggestions mentioned in the above two paragraphs have been presented depending on that particular networking scenario but the behavior of interference between Zigbee and other IoT networks like Wi-Fi is still an interesting topic among researchers because of the growing applications of Zigbee.

2.3 Chapter Summary

In this chapter, we reviewed some research works related to our thesis topic. Zigbee became a hot cake due to its diverse applications in short-range and low data rate communications. Therefore, Zigbee has become a great point of interest among consumers. Besides, the coexistence of Zigbee with other heterogeneous networks, such as Wi-Fi networks has become a challenging research topic among researchers. We have covered some of the interesting and challenging works in this chapter. Besides discussing the challenges, we have also covered some of the solutions in order to facilitate the coexistence of Zigbee and Wi-Fi. These solutions have been proposed and implemented case by case.

CHAPTER III

MOTIVATION FOR THE THESIS

3.1 Motivation Behind the Thesis Topic

Internet of Things (IoT) is a hot topic nowadays. Since the born of the IoT concept (Mattern and Floerkemeier, 2010), the application areas of IoT networks are increasing in different aspects, ranking from household applications to industrial areas (Brown, 2016). Though IoT networks can be used in many fields including embedded systems, wireless sensor networks, in this thesis we are only focusing on the application areas of IoT networks in home automation, more specifically in smart homes. In the consumer IoT market, the concept of IoT technology is mostly equivalent to the products related to the concept of the smart home. These products include household appliances such as thermostats, lighting, wearable devices, cameras, and other home appliances (Business Insider, 2020).

With time, different smart devices have included to the IoT networks of smart homes in order to ease the daily life of consumers. Most of the devices are Zigbee-enabled devices and the number is increasing day by day (Henderson, 2021, Zigbee Alliance, 2021, Carlsen, 2021). According to the recent announcement of Zigbee Alliance (current name Connectivity Standards Alliance), they are expected to ship about 3.8 billion IEEE 802.15.4 units by 2023 (Stables, 2021).

Due to the diversity and increasing number of Zigbee-enabled devices in the smart home applications, the coexistence of Zigbee and Wi-Fi networks in smart home has been a serious challenge along with the security and privacy of the devices (WiKi, 2021a, Khan et al., 2018). Motivating with this challenge, in this thesis, we have focused on the coexistence of Zigbee and Wi-Fi networks. More specifically, the performance of Zigbee-enabled devices with the presence of Wi-Fi networks has been our major focus.

In this thesis, we have presented an empirical analysis of a Zigbee network with and without the presence of a Wi-Fi network that acts as an interference network. The reason behind choosing a Wi-Fi network is that Wi-Fi networks are very common in apartment homes. As we have chosen the term smart home in this thesis, we wanted to focus on two common networks which play a vital role in turning a traditional apartment home into a smart home.

3.2 Motivation Behind the Experimental Setup

In this thesis, we have analyzed the Zigbee network's performance in a practical environment. We wanted to get data from a real-life indoor environment using real-time experiments so that we can sense the behavior of a network from a real-life testbed. Another vision of this thesis was to understand the behavior of a Zigbee network in the presence of a heterogeneous network. Both Bluetooth and Wi-Fi are common networks in indoor environments, but Wi-Fi is more popular. So, we decided to have a Wi-Fi network as the interference source in the testbed. Therefore, our experimental testbed consisted of two common networks that exist in a smart home environment: Zigbee and Wi-Fi networks. We considered the simplest topology of the network where both the Zigbee and Wi-Fi network consisted of only two devices: transmitter and receiver. To get a practical feeling of a smart home scenario, we

decided to deploy the network in an indoor environment. Therefore, the UTRGV lab environment was the perfect match for our testbed scenario, where we can get a strong Wi-Fi network. Because of the sudden lockdown due to the COVID-19 pandemic, UTRGV facilities were temporarily inaccessible at that time. So, we had to change our plan and later, decided to deploy the network in an apartment home environment to continue the research.

Later, we figured out that the UTRGV lab environment could give us a perfect environment for testbed setup, but we would have to encounter some problems. Firstly, since the UTRGV Wi-Fi connection is a centralized network, we could not be able to turn them off/on according to our purpose. So, we never could get an environment for our baseline study, where we need a Wi-Fi-free environment. Secondly, we could not be able to configure and change the operating channel of the Wi-Fi network. The varying operating channel is one of the important parameters for our Zigbee performance study. Instead of UTRGV lab, we got a perfect environment for our testbed deployment in an apartment home.

In this thesis, we have tried to get data from the most possible practical environment equivalent to a smart home. From the testbed of an apartment-based indoor environment, we got a feeling of a smart home. Another advantage of deploying the network in an apartment home was that we didn't have to wait to go back to the school to continue the research. Most importantly, we were able to configure the Wi-Fi network as required for our research. Despite having the advantages, we encountered some difficulties in an apartment home that includes detection of neighbor's home Wi-Fi network in the testbed region, a possible case of interference from home microwave. To get rid of these unwanted interference sources, we took some

prevention measurements such as taking data at mid night, turning off the microwave during the experiments, etc.

3.3 Chapter Summary

In this chapter, we have discussed our motivation behind the thesis topic and experimental setup. The concept of an IoT system is full of opportunities and challenges. Due to the unprecedented growth of IoT devices, the challenges have become more open than ever. Spectrum scarcity is one of the great challenges for IoT devices as most of the devices operate at the same 2.4 GHz ISM frequency band. Presence of the heterogeneous networks like Zigbee, Wi-Fi, etc. at proximity in smart home applications turns into a great challenge for the normal operation of the networks. Motivated by this challenge, we have presented a comprehensive analysis of the Zigbee network in a real-life apartment home environment. Due to the sudden impact of COVID-19, we have been encouraged to deploy our testbed in an actual apartment home which gives us a practical sense of a smart home environment.

CHAPTER IV

EXPERIMENTAL SETUP AND METHODOLOGY

4.1 Overview of the Testbed

The experimental testbed used in this study is based on an indoor environment, more specifically a home apartment to mimic a smart home. The main focus of this thesis is to understand the performance of a Zigbee network with and without the presence of a Wi-Fi network. As I mentioned in section 1.7 of Chapter I, this research ignores other Wi-Fi networks detected from neighbor's apartments in the experimental testbed region. To minimize the impact from these unwanted networks, data were taken at midnight when the usages of such detected unwanted networks were minimal.

The experimental testbed comprises two IoT networks: a Zigbee network and a Wi-Fi network. The Zigbee network consists of two Zigbee modules: one XBee Zigbee coordinator module acting as Zigbee receiver (RX) and one Xbee Zigbee end device acting as a Zigbee transmitter (TX). Digi International's XBee Configuration & Test Utility (XCTU) (Digi International, 2019), a free multi-platform application designed software, was used to configure Zigbee modules as well as to exchange Zigbee traffic between the modules. On the other hand, the Wi-Fi network comprises two Wi-Fi-enabled mobile devices generating Wi-Fi traffic: one transmitter device and another receiver device.

Figures 4.1 and 4.2 show the experiment testbed topologies without and with the presence of a Wi-Fi network, respectively. In these figures, the terms, d_z denotes the distance between the Zigbee transmitter (TX) and Zigbee receiver (RX), d_{zw} represents the distance between the Zigbee receiver (RX) and Wi-Fi transmitter (TX), and d_w indicates the distance between the Wi-Fi transmitter and Wi-Fi receiver. The topology in Figure 4.1 was considered when the experiments required a Wi-Fi-free environment and Figure 4.2 was used when the experiments were conducted under the interference of a Wi-Fi network.

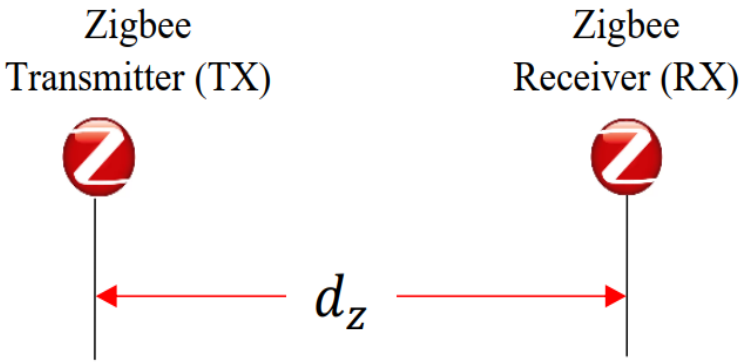

Figure 4.1: Testbed topology with only Zigbee network

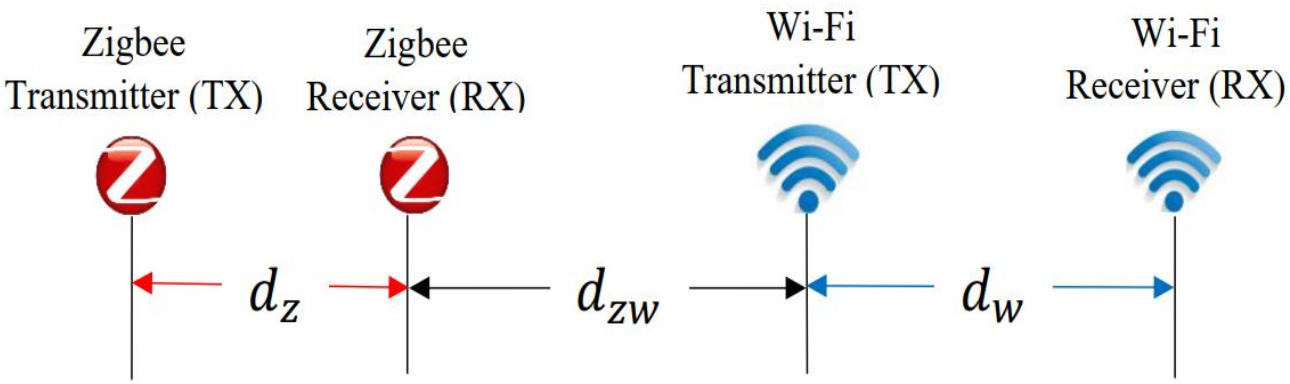

Figure 4.2: Testbed topology with both Zigbee and Wi-Fi networks

4.2 Instrumentation

4.2.1 Zigbee Network

As showing in Figures 4.1 and 4.2, the Zigbee network consisted of two Zigbee-enabled devices: Zigbee transmitter device acting as a Zigbee end device and Zigbee receiver device acting as a Zigbee coordinator device. Digi International's XBee Zigbee Mesh Kits (Part Number XKB2-Z7T-WZM) were used to deploy the Zigbee network (Digi International, 2017). In this section, I will describe the functionality of the Zigbee modules used in this experimental setup including their hardware components and their functions.

4.2.1.1 Components of XBee Zigbee modules. The Digi International's XBee Zigbee Mesh Kits come with three (03) Digi XBee Grove Development Boards, three (03) Digi XBee Zigbee Modules, three (03) Micro-USB Cables, and two (02) XBee Stickers. In this experimental setup, the simplest form of Zigbee network was used consisting of a Zigbee transmitter and a Zigbee receiver. Therefore, only two Zigbee modules were used to represent the transmitter and receiver.

A complete XBee Zigbee communication device consists of two main hardware components that come separately: an XBee grove development board and an XBee Zigbee RF radio module as shown in Figure 4.3. Some of the hardware modules use Through-hole technology (THT) and some of them use Surface-mount technology (SMT). In our experiments, both Zigbee XBee modules (acting as Zigbee transmitter and receiver) were made of Through-hole technology.

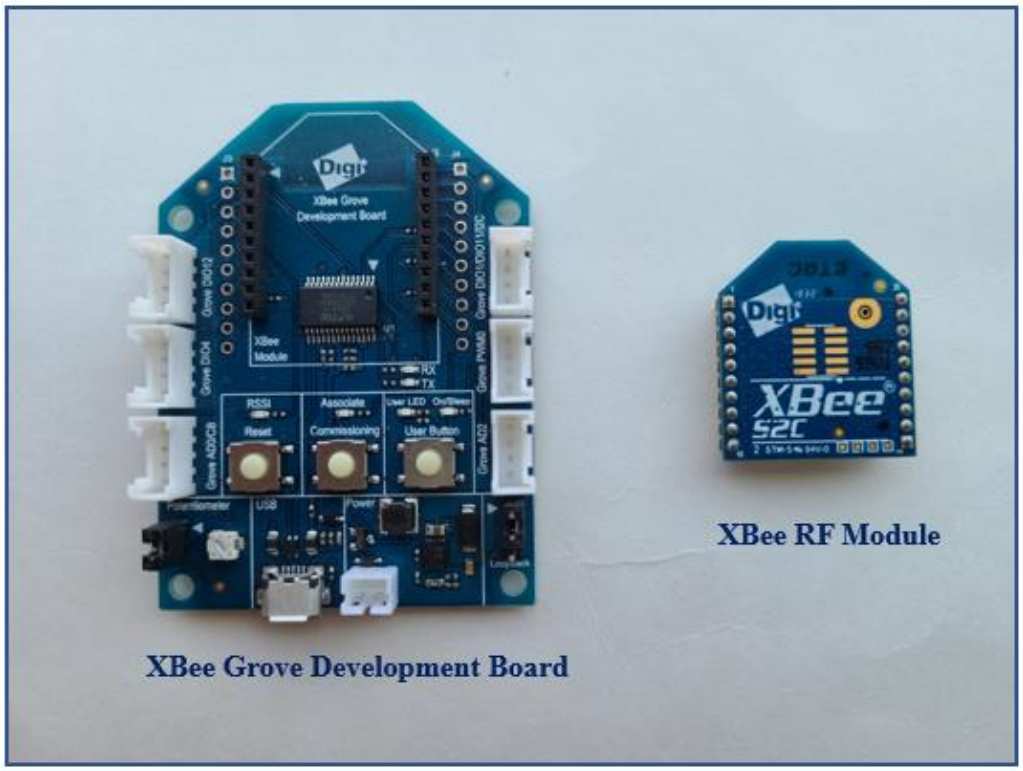

Figure 4.3: Hardware components of XBee Zigbee modules

4.2.1.1.1 Zigbee XBee radio frequency module. Between two major components of the XBee Zigbee modules, XBee Radio Frequency (RF) modules are small RF devices that transmit and receive data over the air using radio signals. XBee RF modules are highly configurable and can support multiple protocols. These devices also provide wireless capability that is very essential for sensor networks deployment especially where connections using cable or wire is impractical.

The XBee RF modules or simply XBee modules are not standalone devices, which means, other hardware devices like microcontrollers, traditional computers or laptops, Raspberry Pi, and Arduino modules are needed to setup to transmit data wirelessly using XBee modules. Thanks to Digi International, with the Mesh Kits, Digi also provides an XBee grove development

board to use with the XBee modules for connecting them to microcontrollers, laptops, Raspberry Pi, etc.

4.2.1.1.2 XBee Grove Development Board. The XBee Grove Development Board is one of the main hardware components of the Zigbee Mesh Kits (Digi International, 2016) (p. 203). This is a very simple hardware module that is used to connect the XBee modules to a PC or microcontroller. The board contains several Grove connectors where we can easily plug in a Grove Module. This grove board also facilitates the communication between the XBee RF module and configuration (XCTU) software through microcontrollers, laptops, or Raspberry Pi. Figure 4.4 shows an XBee Grove Development Board with various major components.

- Power supply: A 5V power supply can be used to power the XBee Grove Development Board. The power source can be connected either through Micro USB directly from the computer or a traditional external battery connected to a 2-pin, 2 mm pitch, PH-type connector from JST.
- XBee connector: The XBee Grove Development Board provides two 10 pin, THT 2 mm pitch sockets to attach the XBee module. It provides good compatibility with the XBee and other programmable XBee modules. The upper section of the board shows the XBee connector section. Table 4.1 describes the major pins (both sides) of the XBee connector with necessary comments.
- USB: The XBee Grove Development Board has a USB connector (bottom side of the board) and an FT232RL USB to RS-232 converter to communicate with the serial port of the XBee. The MicroUSB port is used to serve two purposes:

connecting the board to the laptop to communicate with XCTU software and powering up the board using a USB cable.

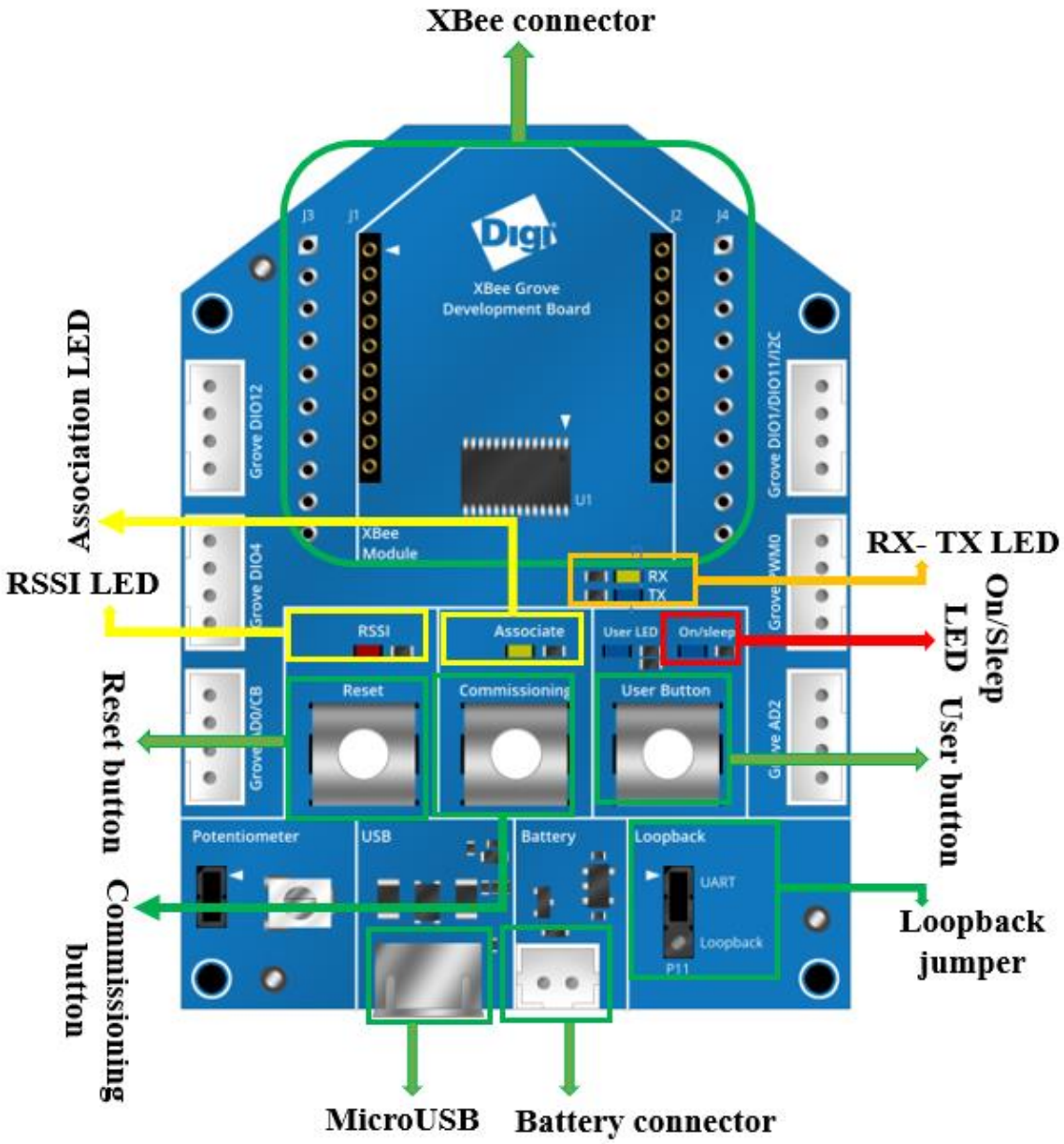

Figure 4.4: XBee Grove Development Board with major components

Table 4.1: Major XBee connectors with comments (Digi International, 2016) (P. 209)

Left			Right		
Pin	**Signal**	**Comments**	**Pin**	**Signal**	**Comments**
1	3.3V	XBee supply	1	DIO4	To GROVE_DIO4 and user LED/button
2	XBEE_TX	To serial to USB device	2	XBEE_CTS_N	To serial to USB device
3	XBEE_RX	To serial to USB device	3	DIO9	To On/Sleep LED
4	DIO12	To GROVE_DIO12	4	VREF	
5	RESET_N	To reset button	5	ASSOC_LED	To association LED
6	RSSI/PWM0	To RSSI LED and GROVE_PWM	6	XBEE_RTS_N	To serial to USB device
7	DIO11/I2C_SDA	To GROVE_I2C	7	AD3	To potentiometer
8	XBEE_PIN8	Connected to breadboard header	8	AD2	To GROVE_AD2
9	XBEE_DTR_N	To serial to USB device	9	DIO1/ISC_SCL	To GROVE_I2C
10	GND		10	AD0/CB	To commissioning button and GROVE_AD0

- RX-TX LED: The RX (yellow) and TX (green) LEDs show the status of RX and TX lines, respectively. The RX-TX LEDs is blinked during the reception and transmission of Zigbee packets. The blinking RX-TX LEDs indicates a good sign of Zigbee communication during the experiment.
- Reset button: The button indicating the Reset button is used to reset the XBee module. Sometimes, the modules stuck after a long period of communication. The Reset button becomes handy in such cases.
- Commissioning button: The XBee Grove Development Board comes with a push button attached to the commissioning pin of the XBee module. The commissioning pin or the commissioning push button is used to help deploy devices in a network. For example, if a new Zigbee device is deployed in a preexisting network, sometimes the commissioning button is used to connect the new Zigbee device to that network using its Personal Area Network Identifier (PAN ID). This button also helpful when the Zigbee devices are disconnected due to heavy interference cases; pushing the commissioning button reconnects the Zigbee devices with each other.
- Association LED: The XBee Grove Development Board offers an LED connected to the association pin of the XBee module.
- RSSI LED: The XBee Grove Development Board presents an LED connected to the RSSI/PWM0 pin of the XBee module. The RSSI/PWM signal is also connected to the PWM Grove connector. For every received packet, this pin provides the RSSI value. The brightness of the LED is associated with the RSSI

value. For example, if the PWM0 pin (P0) is configured as RSSI, the brightness of this LED displays the signal strength of the last packet received. For a larger RSSI value, the LED shows brighter light and for a smaller value of RSSI, the LED provides dimmer light.

- User button and User LED: The XBee Development board comes with a user button and corresponding LED light called user LED. Although the user LED button and user button both share the same input-output pin of the XBee module, we cannot use both the button and LED at a time.
- On/sleep LED: The on/sleep pin (DIO9) of the XBee Grove Development Board is attached with an on/sleep LED light. This LED provides the on/off status of the XBee board. If the XBee module is awake, the LED turns on otherwise it turns off when the module sleeps.
- Loopback jumper: The XBee Grove Development Board offers a three-pin jumper to connect the Universal Asynchronous Receiver/Transmitter (UART) to the USB (normal mode) or to make a loopback connection between the RX and TX signals of the UART. In loopback mode, we can connect the RX line to the TX line, which transmits back any received data. This configuration was used during the experiments to the signal strength and throughout or data transfer ratio between two the Zigbee transmitter and receiver.

4.2.1.2 Assembling the XBee hardware components. The previous subsections provide details about the hardware components of XBee Zigbee modules. To start data communication, it is very important to assemble those hardware modules to make a complete Zigbee module. This

subsection will describe the steps to assemble those hardware components to make a complete Zigbee module. The following steps were covered to make a complete Zigbee module:

(i) One XBee Zigbee Mesh Kit was plugged into the Zigbee connector of the XBee Grove Development Board.

(ii) Once the XBee module was plugged into the board, the board was connected to a computer using the micro-USB cable.

(iii) We have to make sure the loopback jumper is in the UART position during the assembly.

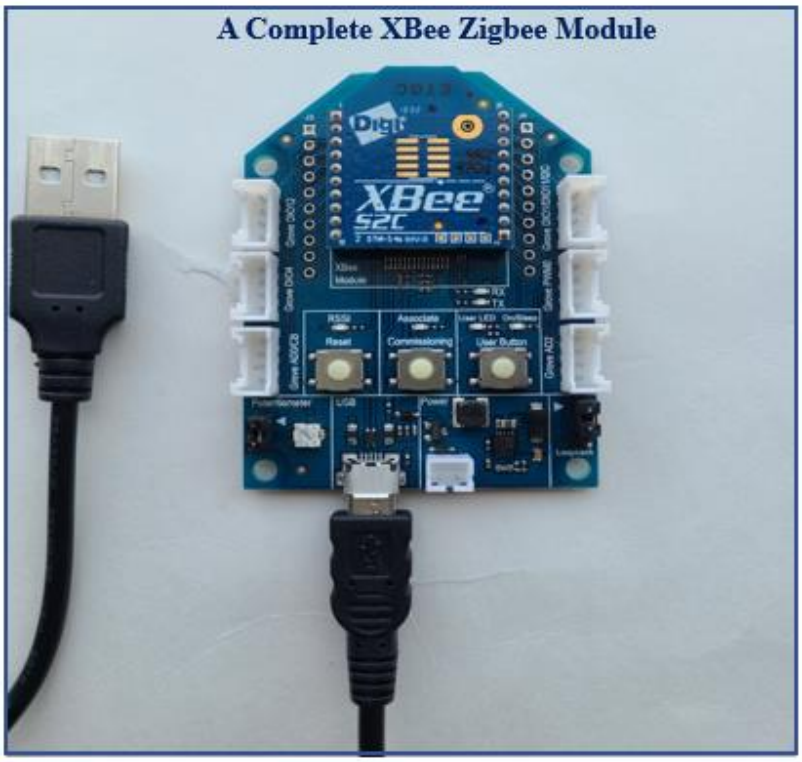

Figure 4.5: A complete XBee Zigbee module

A complete XBee Zigbee module will look like as shown in Figure 4.5. Once all hardware components were assembled, the XBee Zigbee modules were configured using XBee Configuration and Test Utility (XCTU) software.

4.2.1.3 Configuring the XBee Zigbee modules. To transmit or receive Zigbee data packets, the XBee Zigbee modules need to be configured as Zigbee transmitter and receiver, respectively. Digi International's XBee Configuration & Test Utility (XCTU), a free multi-platform application designed software, was used to serve this purpose. In order to configure the XBee Zigbee modules, communication between the XCTU software and an XBee module was performed through the XBee module's USB interface connected to a personal computer (e.g., laptop) using a USB cable as shown in Figure 4.6. The XCTU was installed on that computer before configuring the modules.

Figure 4.6: Interfacing a Zigbee XBee module to the XCTU through a laptop using USB cable

XCTU software has three working modes: Configuration, Consoles, and Network (Digi International, 2019) (p. 27). The selected working mode determines which specific operations we

can perform with a radio module or modules. To configure the radio modules, XCTU uses its Configuration mode. Figure 4.7 shows a sample display page of the “configuration working mode” of XCTU.

Initially, a complete XBee Zigbee module comes with a preloaded configuration. Before setting up communication between or among Zigbee devices, we need to configure the modules for any particular operation. In the device configuration stage, we had to configure some parameters like ID, JV, CE, NI, SP, SM, SO, AP, etc. It's worth mentioning here that XBee modules operate in two operating modes: transparent mode and Application Programming Interface (API) mode (Digi International, 2016) (p. 34). In transparent mode, the radio device passes information exactly as it receives. In API mode, the radio module sends data in orderly and an organized manner.

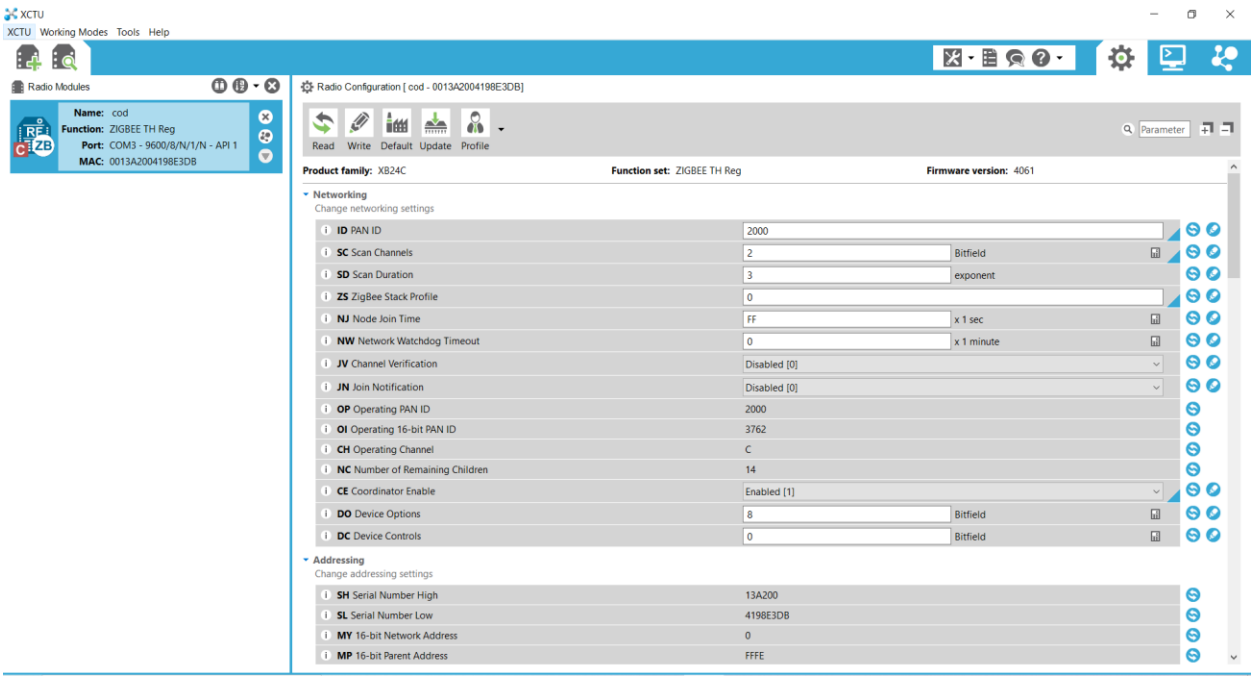

Figure 4.7: A sample page of “configuration working mode” of XCTU

In this thesis, we have used XBee Zigbee modules in API mode for communication. So, we had to set up some extra parameters for that purpose. The following steps show the configuration process.

(i) The XBee modules were added to the XCTU software which was running previously on a laptop (Digi International, 2016) (p. 24).

(ii) After adding the radio modules (XBee modules) to the XCTU, it was time to configure some parameters, such as ID, JV, CE, DH, DL, NI, SP, SM, and SO of the modules according to the experimental testbed requirements. Table 4.2 provides a brief of the parameters used to configure the testbed XBee Zigbee modules.

(iii) Configuring parameters does not ensure the modules are running with those parameter settings. To complete the configuration step, the settings must be written by clicking the "**write radio settings**" button of the XCTU.

Once all the parameters are successfully configured, we can use the modules for data communication, i.e., exchanging Zigbee packets between the Zigbee transmitter and Zigbee receiver. As I mentioned before, all the Zigbee communications in this research were made through the Zigbee API mode. In the following sections, I will discuss how Zigbee devices communicate with each other, particularly using API mode.

Table 4.2: Major XBee configuration parameters with notes (Digi International, 2016) (P. 25)

Parameter	Name	Note
ID	PAN ID	ID or PAN ID refers to the network ID a radio attach to. This ID must be the same for all radio modules working in the same Zigbee network.
JV	Channel Verification	This parameter verifies if a coordinator exists on the same channel to join the network. For the coordinator device, JV is disabled and enabled for other devices in the network.
CE	Coordinator Enable	CE sets a device as a coordinator. So, CE is enabled in the coordinator device.
NI	Node Identifier	NI sets a human-friendly name of each device, e.g., Coordinator and End Device for coordinator and end device, respectively.
SP	Cyclic Sleep Period	Specifies the duration of time the radio module spent sleeping.
SM	Cyclic Sleep Mode	Enables cyclic sleep mode in the end device only.
SO	Cyclic Sleep Mode	This option keeps any module awake during the entire period. This is generally used for the coordinator device which is needed to be active for the entire time.

4.2.1.4 Communication between XBee Zigbee modules. This section describes how XBee Zigbee devices work or communicate. Besides, I will provide a brief description of two communications methods of XBee modules: wireless communication and serial communication (Digi International, 2016) (p. 31).

XBee devices exchange data with each other over the air, transmitting and receiving wireless messages. The devices only transfer information wirelessly, they don't control or manage the sent or received data. To control or manage data, the XBee devices can collaborate with intelligent devices via their serial interface. XBee devices transmit data that comes from the serial input through the air, and they send the received data to the serial output wirelessly. Intelligent devices like microcontrollers, PCs can control and manage those data before transmission and after the reception. Therefore, the communication between two XBee devices can be classified into two parts: wireless communication and serial communication. The below figure shows the overall process of XBee communication.

4.2.1.4.1 Type of communications. In this section, I will discuss two types of communications that take place between two XBee modules: wireless communication and serial communication. Figure 4.8 shows both types of communications.

1. Wireless Communication: Wireless Communication happens between two XBee modules. Both modules need to be in the same network using a single PAN ID. Also, the operating frequency of both modules must be the same. Upon meeting these requirements, all the modules can communicate with each other wirelessly.
2. Serial Communication: Unlike wireless communication, serial communication is wired communication. This takes place between the XBee device and the

intelligent device connected with the module through its serial interface. In this thesis, we have used a laptop as an intelligent device.

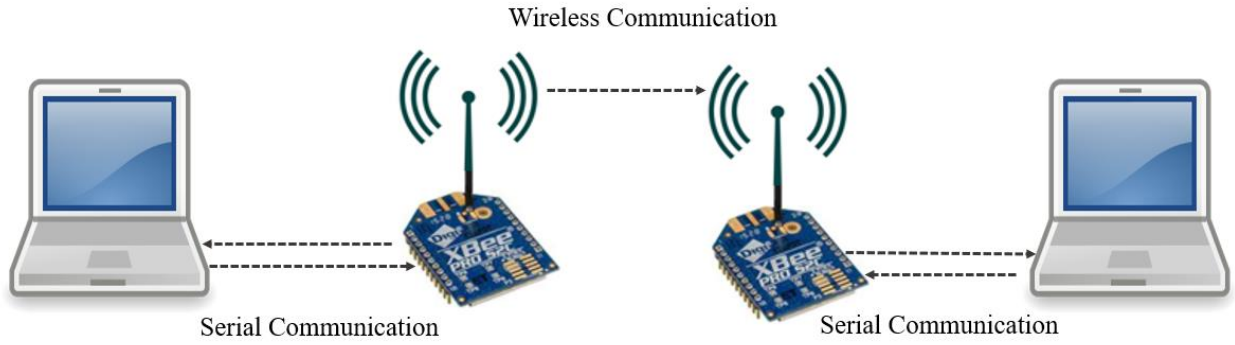

Figure 4.8: Communication scenario between XBee devices

The XBee modules can either be operated as a stand-alone device or with an intelligent device to control and manage the sent and received data. For example, I have used laptops as intelligent devices with the XBee modules via their serial interface to control and manage the data. Other devices such as Arduino or Raspberry Pi, sockets, and Breadboards can also be used as intelligent devices. When the intelligent device is connected with the XBee module, it can send data via the serial interface to the XBee module to be transmitted to other devices wirelessly. On the receiver side, the receiver XBee module receives the data and sends those data to the intelligent device connected through the serial interface.

4.2.1.4.2 XBee operating modes in serial communication. XBee devices interact with their host devices such as PC or microcontrollers through their serial connection in different ways. The “Operating Mode” determines the way the host device communicates with the XBee modules. Digi XBee modules are compatible with two different operating modes:

- Application Transparent (“transparent mode”)
- Application Programming Interface ("API mode")

1. Application Transparent (“transparent mode”): In this operating mode, the XBee radio module passes information exactly as it receives. All the data received by the radio module is sent wirelessly to the remote module. When the receiver module receives the data, the data is forwarded through the serial port as it was received. This is why this operating mode is called “transparent mode”.
2. Application Programming Interface (“API mode”): Unlike the transparent mode, the API mode enables the user to manage and control the data. In API mode, a protocol defines the way the data is exchanged. Data is communicated in packets, called API frames. This mode is mostly helpful for developing a large network like a sensor network to collect data from multiple locations, controlling the devices, etc. In API mode, the sent and received data are not identical: received data contains some control data and extra information.

In this thesis, API mode is used as the XBee operating mode (Digi International, 2016) (p. 42). This because the transparent mode has some limitations. Besides resolving those limitations, API mode offers a structured interface where data are exchanged through the serial interface in organized packets and in a determined order. This packet structure and ordered delivery of packets are controlled by defining the protocol. This mode also allows the user to configure the local and remote XBee modules in the network. One of the important advantages of API mode is the reception of success/failure status of each transmitted packet.

4.2.1.4.3 XBee frame structure. The structured Zigbee packets in API mode are called API frames (Digi International, 2016) (p. 45). API frames are sent and received through the serial interface of the XBee module and contain wireless data as well as some control data and extra information. Generally, an API frame is structured in the following:

Start delimiter	**Length**		**Frame data**						**Checksum**
			Frame type	**Data**					
1	2	3	4	5	6	7	……	n	n+1
0x7E	MSB	LSB	API frame type	API-specific structure					Single byte

Any data received through the serial interface before the start delimiter is silently discarded by the XBee. If the frame is not received correctly, or if the checksum fails, the data is also discarded. In such a case, the module indicates the nature of the failure by replying with another frame.

- Start delimiter: The first byte of a frame consisting of a special sequence of bits that indicate the beginning of a data frame is called the start delimiter. Start delimiter maintains a unique value (0x7E) all the time which enables easy detection of a new incoming Zigbee frame.
- Length: This field tells us the total number of bytes included in the frame data. This is a two-byte value.
- Frame data: This field contains the information received or to be transmitted. There is two-division of Frame data: API frame type which tells what type of API

frame the XBee is using (I will discuss this later) and Data that contains the actual data itself.

- Checksum: The last byte of an API frame is the checksum. Checksum maintains the data integrity of the communication. For example, if any Zigbee frame is sent through the serial interface of Zigbee with an incorrect checksum, the frame is never proceeded by the module and eventually the data will be discarded. Frame checksum is computed by taking the hash sum of all the API frame bytes that came before it, excluding the first three bytes (start delimiter and length).

There are different types of supported API frames depending on the type of XBee modules. Some of the transmit data frames are:

- AT Command
- AT Command Queue Parameter Value
- Transmit Request
- Remote AT Command Request
- Register Joining Device

There are various receive data frames received through the serial output, with data received wirelessly from remote XBees. Some of the received data frames include:

- AT Command Response
- Modem Status
- Transmit Status
- Receive Packet

- Router Record Indicator
- Extended Modem Status
- Join Notification Status
- Remote AT Command Response

In this thesis, Transmit Request and Transmit Status type API frames are used for the transmitted and received data, respectively. Transmit Request transmits wireless data to the specified destination. The value of the Frame Type field for Transmit Request API fame is 0x10. A typical structure of the Transmit Request API frame is given in Table 4.3.

The Transmit Status frame indicates the success or failure of wireless data transmission. This is a subsequent frame of Transmit Request frame with the ID 0x8B. Another frame called "Receive Packet" is also found in this type of data transmission. This frame sends wirelessly received data out of the serial interface. Receive Packet contains the data received over the air and the source address. Therefore, data communication in any Zigbee network is the exchange of some frames (Transmit Request, Receive Packet, and Transmit Status). The next topic will cover the procedure of exchanging XBee frames.

4.2.1.4.4 Transmission and reception of wireless data in XBee (Transmit Request/Receive Packet). We now understand what API mode is and how API frames are structured. We also know the data communication in XBee modules is the exchange of API frames. This section will provide more details on how the XBee frame are exchanged (Digi International, 2016) (p. 58).

Table 4.3: Fields of Transmit Request API frame (Digi International, 2016) (P. 49)

Frame Fields		Offset	Example	Description
Start delimiter		0	0x7E	Indicates the start of the new frame
Length		MSB1		Number of bits between the length and the checksum
		LSB2		
Frame Data	Frame type	3	0x10	0x10-spcifies this is a Transmit Request frame
	Frame ID	4	0x01	Indicates the sender will receive a Transmit Status frame with the result of the transmission.
	64-bit Destination address	MSB5		Set to the 64-bit address of the destination XBee
		6		
		….		
		LSB12		
	16-bit Destination address	MSB13		16-bit address of the destination XBee, if known.
		LSB14		
	Broadcast Radius	15	0x00	0x00 sets the maximum number of hops a broadcast transmission can occur.
	Options	16		
	RF Data	MSB14		This is the actual data of up to 255 bytes that is sent to the destination.
		15		
		…		
		LSB18		
Checksum		22		Maintains the integrity of the data. Hash sum of frame data bytes

A Transmit Request frame contains data with its destination address and some transmission options. The data received wirelessly by an XBee module is included in a Receive Packet frame with the source address and some options for the reception. There are two other frames: Explicit Addressing Command Frame and Explicit RX Indicator. They specify the application layer addressing fields (endpoints, cluster ID, profile ID). The following Figure 4.9 shows the API frame exchanges at the serial interface when transmitting wireless data to another XBee module.

1. The intelligent device connected with the XBee module sends the Transmit Request (0x10) or an Explicit Addressing Command Frame (0x11) to XBee TX through the serial input in order to transmit data to the XBee RX.
2. XBee TX transmits the data wirelessly to the destination module (XBee RX).
3. The remote XBee module receives the data and sends a Receive Packet or an Explicit RX Indicator frame through the serial output depending on the configuration of the module. These frames contain the received wireless data and the source/transmitter address.

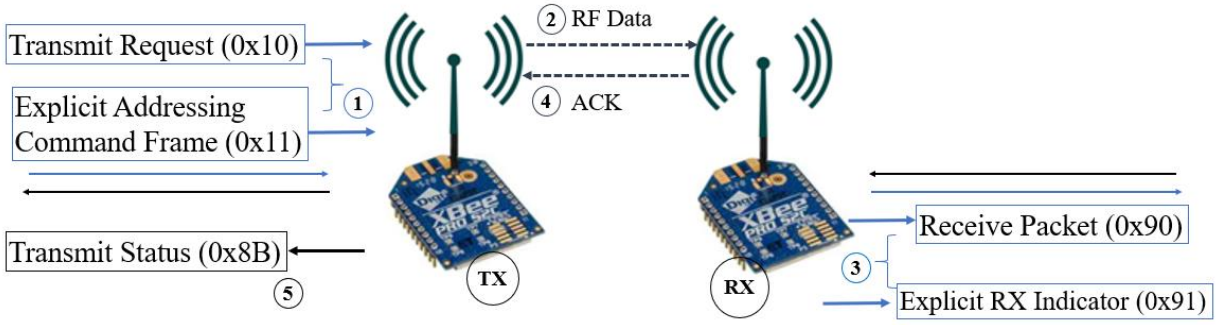

Figure 4.9: API frames exchange between two XBee modules

4. After the reception of Receive Packet or Explicit RX Indicator frame, the XBee RX sends an ACK frame to the XBee TX with the status of the transmission.
5. The sender XBee TX sends out a Transmit Status frame through the serial interface with the status of the transmission (success/failure). The Transmit Status frame is sent at the end of each transmission. If the packet cannot be delivered to the destination, the transmit status frame indicates the cause of failure.

4.2.2 Wi-Fi Network

The Wi-Fi network was deployed using a home Wi-Fi router (which acted as a Wi-Fi AP) along with two smartphones: one smartphone acted as a Wi-Fi transmitter (TX) and another acted as a Wi-Fi receiver (RX). A Netgear- R6020 AC750 Wireless Dual-Band Router was used to keep internet connectivity between the Wi-Fi transmitter and receiver.

To generate and exchange Wi-Fi traffic between the Wi-Fi TX and RX devices, popular network performance measurement and tuning software, Iperf3 was used (Iperf, 2021). The Iperf3 software was installed in client mode and server mode in the Wi-Fi transmitter smartphone and receiver smartphone, respectively. There are two traffic modes in Iperf3 software: TCP and UDP traffic. For our experiments, the Iperf3 TCP data traffic mode was used to generate and transmit the TCP traffic from the Wi-Fi transmitter to the Wi-Fi receiver.

4.2.2.1 Wi-Fi traffic generation using Iperf3. First, Iperf3 was installed in server mode in the Wi-Fi receiver smartphone. Usually, the device in server mode listens on port 5201 by default. Then, Iperf3 was installed in client mode in the Wi-Fi transmitter smartphone. Iperf3 specifies the host on which the server is running (either using its IP address, domain, or hostname). As soon as all the procedures were completed, the smartphones were started

exchanging the traffic. There is an option in Iperf3 to specify the runtime of the smartphones as client and server mode. After that prespecified runtime, the client device terminates and produces results indicating the average throughput of the period, as shown in the following Figure 4.10.

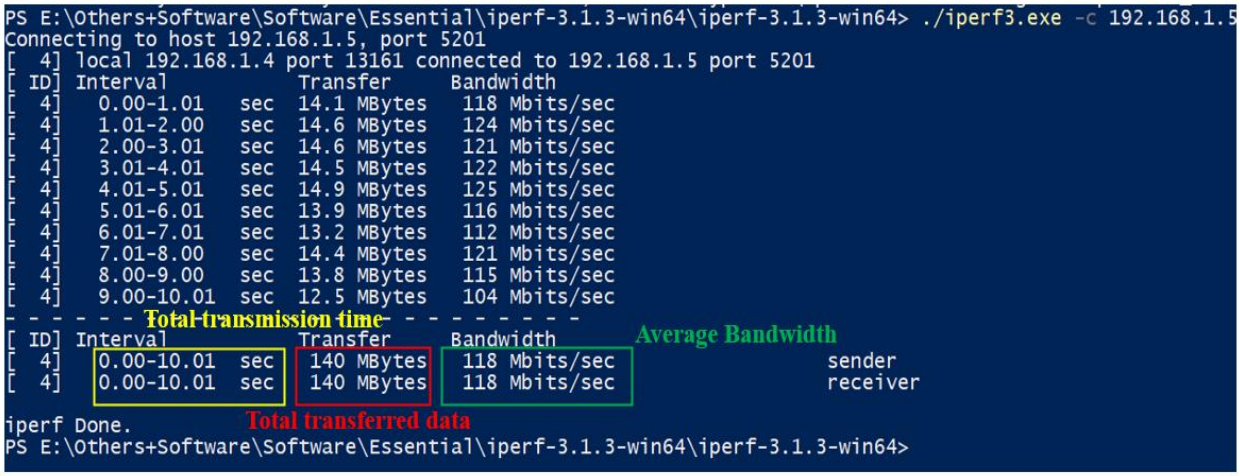

Figure 4.10: An example of transmission window of Iperf3

In this thesis paper, the bandwidth refers to the maximum amount of data that was transferred by the channel in every second for an ideal case and the data rate represents the amount of data that was actually transferred in every second using that channel. During the experiments, we didn't assign any specific bandwidth for the TCP session, so Iperf3 assigned an ideal bandwidth for each TCP traffic transfer session and made the average to generate the average value.

4.3 Methodology

The goal of my thesis is to understand and analyze the performance of a Zigbee network with and without the presence of a Wi-Fi network. For this purpose, we first conducted a baseline study of the Zigbee network without the presence of Wi-Fi traffic. This gave an optimal

Zigbee packet transmission interval which was used later in other experiments. Then, we conducted some experiments to measure the Zigbee network's performance in terms of Received Signal Strength Indicator (RSSI), packet delay, Packet Drop Rate (PDR), and loopback throughput with no Wi-Fi traffic condition. Later, a Wi-Fi network was introduced in the experimental testbed to understand the impact of Wi-Fi traffic interference on the Zigbee network. The packet drop rate was measured with unidirectional traffic whereas the loopback throughput was measured with the loopback function of the XBee modules with bidirectional traffic. Details of these two methods will be discussed in packet drop rate and loopback throughput measurements chapter. During the experiments, 200 Zigbee packets were exchanged between the Zigbee transmitter and receiver. Experimental data were collected in terms of RSSI, packet delay, PDR, and loopback throughput. For the Wi-Fi interference condition, three interference cases were considered:

(i) Overlapping channel (Zigbee channel 12 & Wi-Fi channel 1)

(ii) Adjacent channel (Zigbee channel 14 & Wi-Fi channel 1), and

(iii) Non-overlapping channel (Zigbee channel 12 & Wi-Fi channel 11)

Wi-Fi traffic was generated and exchanged using Iperf3 software. In this thesis, our focus was to measure the performance from the Zigbee receiver side, so the Wi-Fi transmitter was placed on the side of the Zigbee receiver module. During the experiments, the distances between Zigbee transmitter and receiver and between Zigbee receiver and Wi-Fi transmitter were varied while maintaining a fixed distance between Wi-Fi transmitter and receiver. Figure 4.11 shows the overall process of our experiments and data collections.

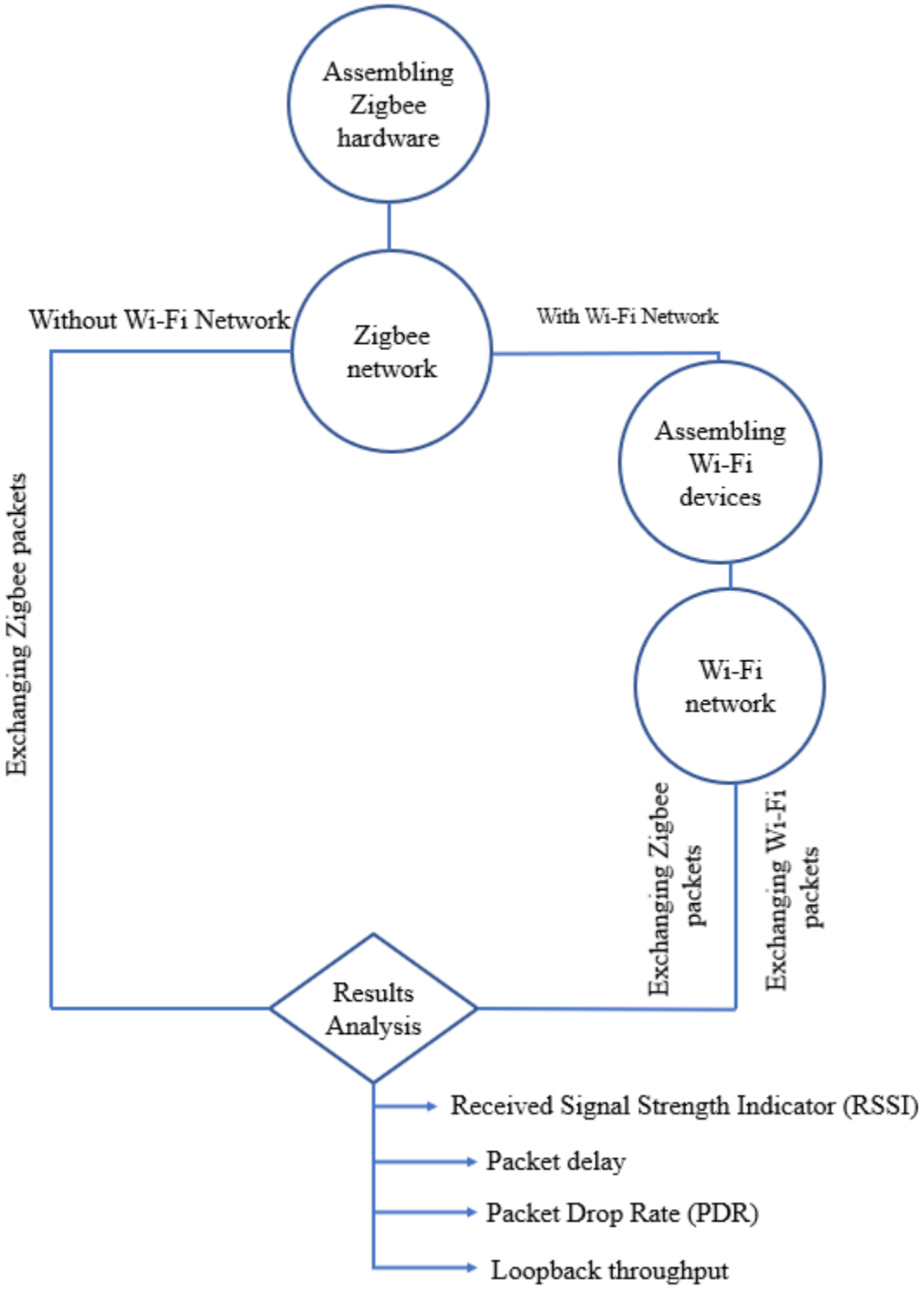

Figure 4.11: Overall process of the experiment

4.4 Chapter Summary

This chapter covers the experimental testbed and data collection methodology of this thesis work. Here, we have discussed the components of the testbed and their functions. The preparation procedures of the testbed components: Zigbee and Wi-Fi are also depicted in this chapter. XBee Zigbee modules consist of a radio module and XBee grove development board. Each hardware component must be assembled and configured before deploying in the testbed. We have covered how data communications happen in the XBee module. The process of generating Wi-Fi interference traffic using Iperf software is also covered in this chapter.

CHAPTER V

EXPERIMENTS AND RESULTS ANALYSES

In these experiments, an experimental testbed configured with a Zigbee network and a Wi-Fi network according to the topology shown in Figure 4.1 and 4.2 was deployed in a real-life apartment home environment. Then, the performance data of the Zigbee network were measured and analyzed under various testbed settings and performance metrics. The experiments reported in the following sections were carried out in a home apartment to evaluate the performance of a Zigbee network.

I divide the data measurements and analyses into two sections: 5.1 Zigbee Baseline Study and 5.2. Zigbee Performance Study. The experiments presented in Section 5.1 (Zigbee Baseline Study) were carried out before performing the main experiments (Zigbee Performance Study) in order to obtain an optimal transmission time interval between Zigbee packets. This obtained transmission interval was used in the experiments for Section 5.2 (Zigbee Performance Study) which is the main body of the experiments of this thesis to understand the performance of a Zigbee network with and without the presence of Wi-Fi traffic.

5.1 Zigbee Baseline Study

The purpose of this study was to obtain an optimum Zigbee transmission time interval when no Wi-Fi traffic was present. Here, the optimum Zigbee transmission time interval means the time interval at which the Packet Drop Rate (PDR) and loopback throughput were minimal. Therefore, PDR and network throughout data are used to analyze and obtain the time interval. This study provides the baseline to measure the performance of the Zigbee network. The experimental setup shown in Figure 4.1 was considered for these experiments.

5.1.1 Baseline Study with Packet Drop Rate (PDR) Measurement

The XBee module configured as a Zigbee end device and the transmitter sends Zigbee packets, aka Zigbee frames to the Zigbee coordinator device acting as a receiver which calculates the number of successfully received packets over the transmission period. The PDR measurement was conducted using unidirectional traffic mode. In this mode, the data was sent from the transmitter module to the receiver module. Before sending the next data packet, the transmitter module waits for the transmission status of the previous packet. The transmission status says the status of the previous packet (success/failure).

During the experiment, the distance between Zigbee TX and Zigbee RX (d_z) was varied between 0m to 5m. The experiment was conducted with five transmission intervals (100ms, 200ms, 400ms, and 500ms) and repeated three times with the same parameter setting to get a reliable result. At each transmission period, 200 Zigbee packets were transmitted from Zigbee TX to the Zigbee RX and the number of successfully received packets was counted using XCTU at the receiver side to generate the PDR using the following formula.

$$\text{Packet Drop Rate, PDR (\%)} = \frac{P_{Tx} - P_{Rx}}{P_{Tx}} * 100 \quad (5.1)$$

Where, P_{Tx} = Number of Zigbee packets sent by Zigbee TX

P_{Rx} = Number of successfully received packets by Zigbee RX

Table 5.1: Experimental parameters for the experiment 5.1.1

Parameters	**Zigbee**	**Wi-Fi**
Operating Channel	12	No Wi-Fi Traffic
Transmit Power, P_t	8 dBm	
Packet Size	64 Bytes	
Distance between Zigbee devices, d_z	0m – 5m	
Traffic mode	Unidirectional	-

The parameters used in this experiment are listed in Table 5.1. Figure 5.1 shows the result obtained from this experiment with Packet Drop Rate vs d_Z graph. The graph shows that the packet drop rate for the 500ms time interval overall lags the packet drop rate for other transmission time intervals, such as 100ms, 200ms, and 400ms. At most of the data collection points, the PDR data for 100ms and 200ms are very close to each other and they are higher than that of 400ms and 500ms. Similarly, the data of 400ms and 500ms transmission intervals closely match each other. Comparing the data of 400ms with 500ms, the PDR data of 500ms is either smaller than that of 400ms or equal to 400ms PDR data.

The smaller the packet drop rate value, the better the network performance, which means the PDR data of 500ms specifies the network's optimal performance when there are no interventions from the Wi-Fi interference traffic. But there were always some packets drop issues

at every point, even if the distances between the Zigbee TX and RX were short. This was probably because of the collision of packets in the same channel due to less time interval between two consecutive transmissions as well as other issues like the detection of neighbor's Wi-Fi access points in the experimental zone, Zigbee antenna alignments, etc.

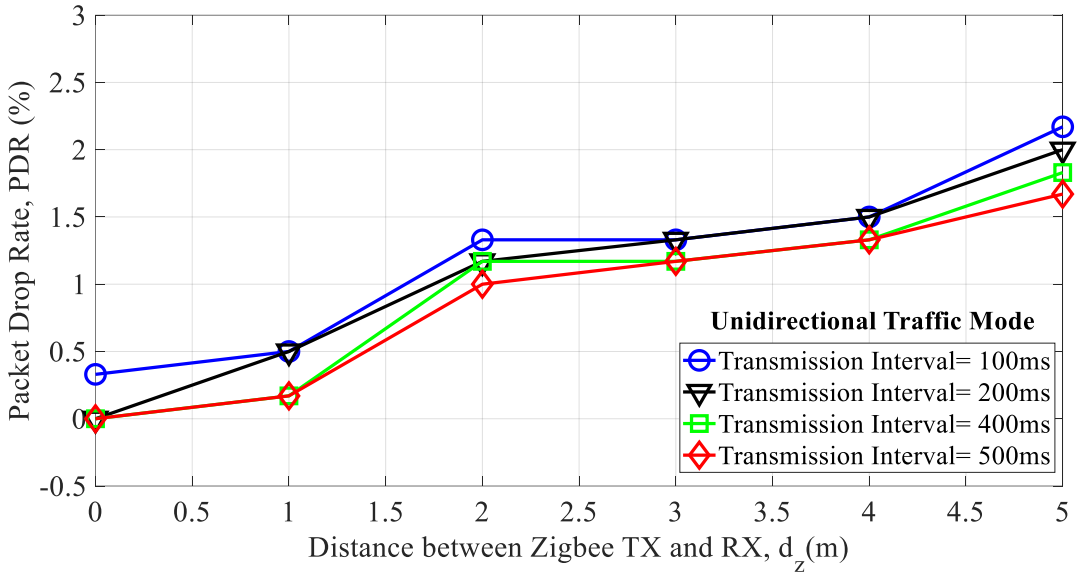

Figure 5.1: PDR with respect to various values of d_z and transmission intervals

5.1.2 Baseline Study with Loopback Throughput Measurement

Throughput is a vital performance metric of a communication network that allows measuring the data transfer ratio between two radio modules located in the same network. In other words, throughput is the expression of how much data is sent from the transmitter or received in the receiver during a specific time interval. To measure the loopback throughput, the XCTU software's built-in "Throughput tool" (Digi International 2016) (p. 189) was used. An XBee module was set as a local radio module (Zigbee transmitter module in this case) and another module was set as a remote radio module (Zigbee receiver module in this case) of the

same network to perform a loopback throughput measurement. The local module performs the throughput on the remote module that receives the data. The data was taken with the bidirectional traffic mode using the loopback function of the XBee module. A hardware loopback is created that connects the DOUT (TX) pin to DIN (RX) pin on the XBee module. This mode echo back the entire packet (from the remote module) sent by the host PC (that is connected to the local radio module) (Digi International 2016) (p. 193).

A Zigbee packet of 64 Bytes was sent at every transmission interval of 100ms, 200ms, 400ms, and 500ms from the local XBee module to the remote module. The transmission interval determines the throughput session to wait to receive the data/transmit status packet back from the remote module. The experiment was carried out with various distances between Zigbee TX and Zigbee RX (d_z) (0m to 5m). Each time 200 Zigbee packets were transmitted from the local device (Zigbee TX) to the remote device (Zigbee RX) and the experimental trial was repeated three times at each data collection point. The parameters used in this experiment are shown in Table 5.2.

Table 5.2: Experimental parameters for the experiment 5.1.2

Parameters	**Zigbee**	**Wi-Fi**
Operating Channel	12	No Wi-Fi Traffic
Transmit Power, P_t	8 dBm	
Packet Size	64 Bytes	
Distance between Zigbee devices, d_z	0m – 5m	
Traffic mode	Bidirectional	-

The loopback throughput data collected from the XCTU at the local module (as we are using loopback throughput mode) follows the general throughput formula (throughput of a communication network can be measured from the packet size and total transmission time).

$$\text{Loopback throughput} = \frac{8 * Number\ of\ bytes\ that\ are\ successfully\ echoed\ in\ the\ loop}{Total\ transmission\ time\ (sec)}\ \text{(bit/sec)} \qquad (5.2)$$

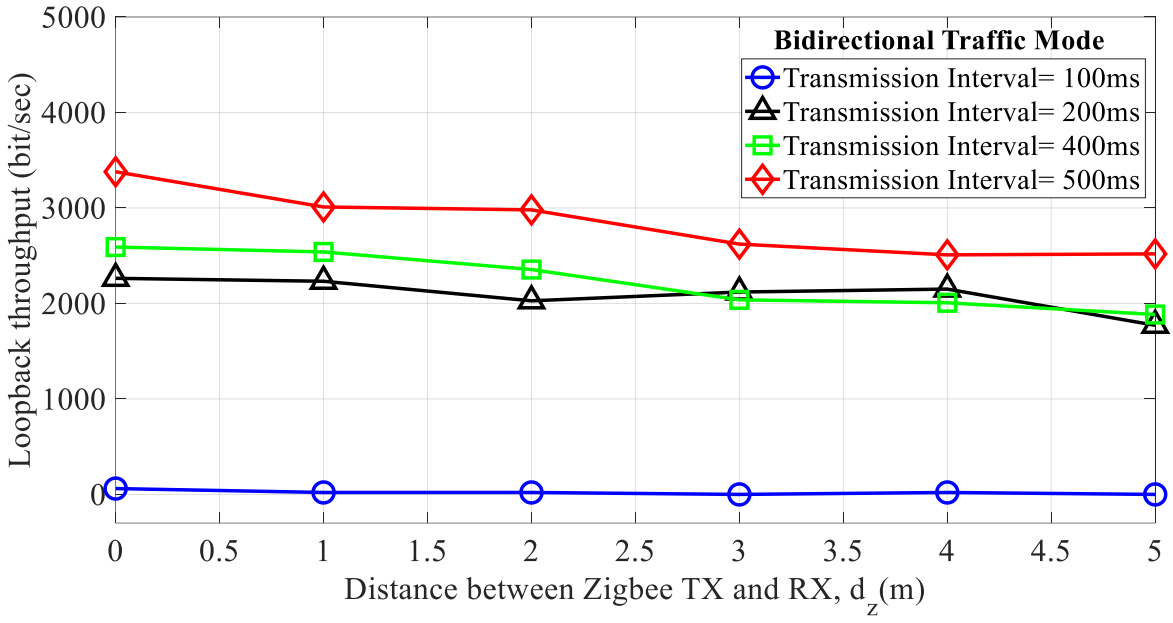

Figure 5.2: Throughput with respect to various values of d_z and transmission intervals

Figure 5.2 shows the result obtained from this experiment with a loopback throughput vs d_Z graph. The figure shows that the loopback throughput for the 500ms time interval every time lags the throughout data for other transmission time intervals like100ms, 200ms, and 400ms. At every data point, the throughput data for 200ms and 400ms are very close to each other but the data for the 100ms transmission interval is the worst so far. For a lower transmission interval like 100ms, the wait time for the acknowledgment of a transmitted packet is very short that another packet is being transmitted from the transmitter before receiving the acknowledgment of the

previously transmitted packet. Therefore, the previous packet is considered as a lost packet which results in a degraded throughput result. Therefore, the transmission interval must be large enough to receive the acknowledgment packet but not too high which may create communication delay. It is also worth mentioning here that the throughput of a network degrades with the distances between the transmitter and receiver. This is because the increasing distance between the transmitter and receiver devices introduces a delay in the network that is inversely promotional to the network throughout (equation 2) and even results in packet drop in the worst-case scenario. As Figure 5.2 shows, among the 100ms, 200ms, 400ms, and 500ms transmission intervals, 500ms gives the network's optimal throughput without any interventions from the Wi-Fi interference traffic.

Analysis from the perspective of both the packet drop rate and network throughout (Figures 4.1 and 4.2) shows that the Zigbee network performs better in terms of PDR and throughout under 500ms transmission interval than others when no Wi-Fi traffic was present. Therefore, the 500ms time interval is the desired transmission interval which was used as the transmission interval of Zigbee packets to conduct further experiments.

5.2 Zigbee Performance Study

The goal of the Zigbee performance study is to examine the performance of the Zigbee network with and without the presence of a Wi-Fi network. The experiments of this study were conducted in terms of Received Signal Strength Indicator (RSSI), Packet delay, Packet Drop Rate (PDR), and loopback throughput by varying parameters like the distance between Zigbee transmitter and receiver and between Zigbee receiver and Wi-Fi transmitter, Zigbee transmit power, Zigbee RF payload size, and operating channel of Zigbee and Wi-Fi networks. In these

experiments, an experimental environment with Wi-Fi and without a Wi-Fi network was considered. Therefore, both Figures 4.1 and 4.2 were considered in this study. This study provides the core measurements to analyze the performance of the Zigbee network.

5.2.1 Received Signal Strength Indicator (RSSI) Measurement

Received Signal Strength Indicator (RSSI) is an important performance indicator for a wireless network measured in -dBm. The goal of this measurement is to examine the performance of a Zigbee network in terms of received signal strength with various values of d_z under different transmit powers (P_t). In order to generate the experimental data, the network topology in Figure 4.1 was considered. Using the XCTU software, the Zigbee TX was configured to send 200 packets of 50 Bytes RF payload length at every 500ms interval. The Zigbee RX module received the packets and sent back the echoes (like the acknowledgment packets) of the successfully received packets to the Zigbee TX side. The RSSI value of both local (Zigbee TX) and remote (Zigbee RX) modules was measured from the Zigbee TX side. This measurement was repeated three times to generate averaged RSSI values. Five different values of transmit power, P_t are studied in this case: (i) 8 dBm, (ii) 5 dBm, (iii) 1 dBm, (iv) -1 dBm, and (v) -5 dBm. Other experimental specifications used in this measurement are listed in Table 5.3.

Figure 5.3 shows the measured RSSI values with respect to d_z for five different values of P_t. As anticipated, during the experiment, the RSSI values decreased with the increment of d_z as shown in the graph. Generally, the RSSI value decreases with the distances due to some external factors influencing radio waves- such as absorption, interference, or diffraction. This is because the Zigbee signal propagates via the air in all directions. At d_z= 0m, the level of RSSI did not

degrade much. Because when the Zigbee TX and RX were placed in close contact (i.e., d_z= 0m), the signal didn't have to travel any distance to reach the receiver end and therefore there was no scope to affect the signal by those external networking phenomena (absorption, interference, or diffraction). Explicitly, improving Zigbee's transmit power leads to better performance.

Table 5.3: Experimental parameters for the experiment 5.2.1

Parameters	**Zigbee**	**Wi-Fi**
Operating Channel	12	No Wi-Fi Traffic
Transmit Power, P_t	(8, 5, 1, -1, -5) dBm	
RF payload size	50 Bytes	
Distance between Zigbee devices, d_z	0m – 6m	
Traffic mode	Unidirectional	-

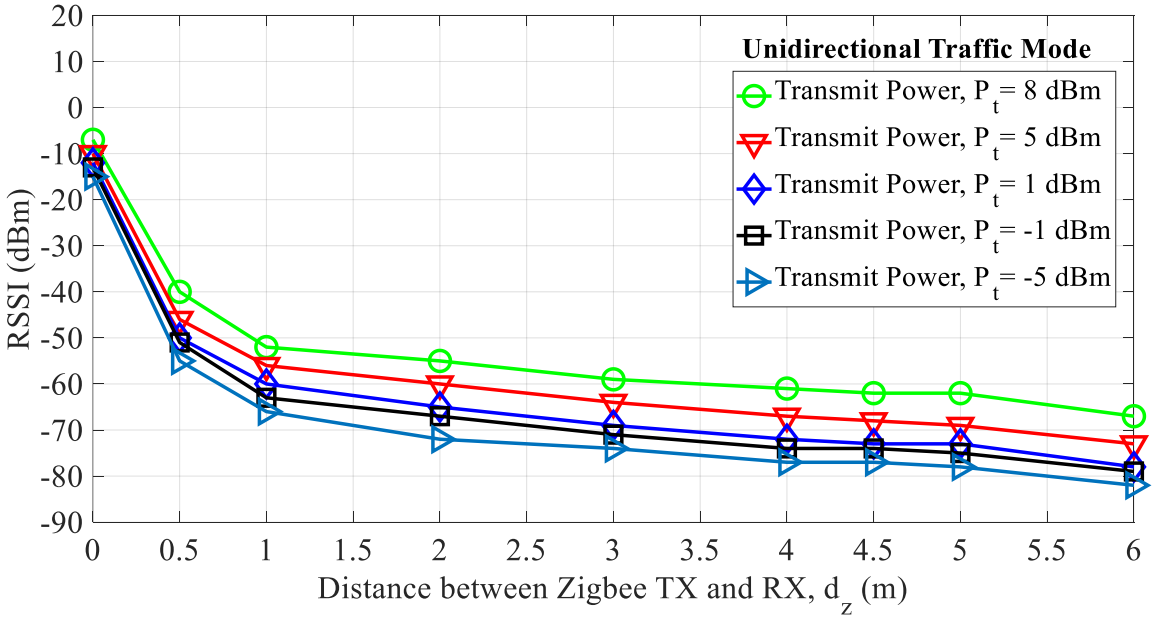

Figure 5.3: RSSI values versus d_z at different levels of Zigbee transmit power

5.2.2 Packet Delay Measurement

Packet delay, the delay between the transmission of a packet and reception of acknowledgment of that packet, is another important performance indicator of the Zigbee network. The goal of this experiment is to understand the packet delay of the Zigbee network when there is no Wi-Fi traffic. In this experiment, the packet delay is defined as the duration between the moment of initiation of packet transmission by the Zigbee transmitter and the time when the acknowledgment of that packet is received by the transmitter including the issuing of Transmit Status API frame by the transmitter. In other words, the delay between the transmission of a Transmit Request API frame and the reception of the Transmit Status API frame of the XBee's Transmit Request/Receive Packet API frame model is considered as packet delay for this experiment. Figure 5.4 shows the theoretical setup of the packet delay measurement. The experimental network was deployed following the setup in Figure 4.1 with no Wi-Fi traffic.

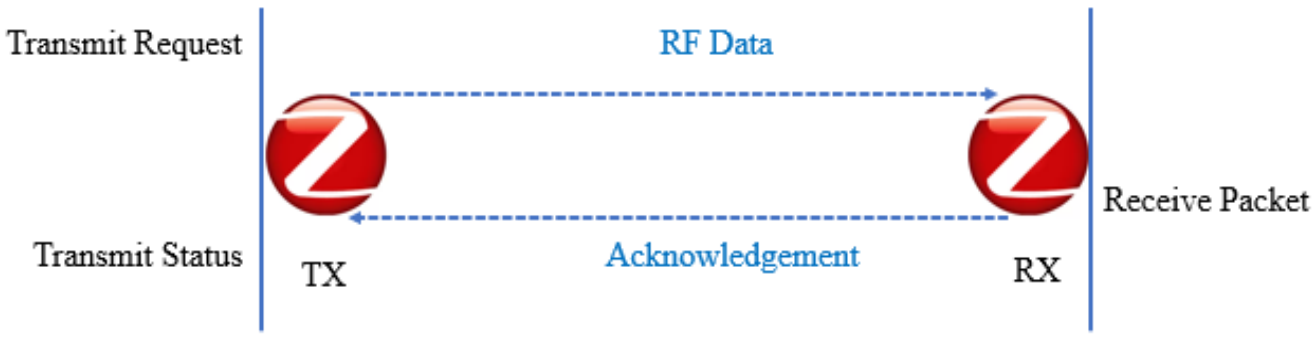

Figure 5.4: Setup for packet delay measurement

Table 5.4: Experimental parameters for the experiment 5.2.2

Parameters	**Zigbee**	**Wi-Fi**
Operating Channel	12	No Wi-Fi Traffic
Transmit Power, P_t	8 dBm	
RF payload size	1 Byte -84 Bytes	
Distance between Zigbee devices	d_z= 2m	
Traffic mode	Unidirectional	-

This experiment was conducted with the following criterion: the absence of Wi-Fi traffic, Zigbee transmission power, P_t= 8 dBm, Zigbee packet transmission interval= 500ms, and varied RF payload length. Table 5.4 lists all the required parameters for this experiment. The packet delay was measured after sending 15 Zigbee packets to generate the average packet delay. The measurement was conducted from the minimum RF payload length (=1 Byte) to the maximum RF payload (=84 Bytes) offered by the deployed XBee modules without packet fragmentation to the payload length of 1 Byte.

Figure 5.5 shows the results of packet delay as a function of RF payload length for d_z = 2m. For the minimum RF payload length of 1 Byte, the average packet delay was calculated 0.0785 sec for the value of d_z = 2m, while for maximum payload (84 Bytes) the delay was 0.1659 sec. As shown in the data graph, the packet delay of the Zigbee network was increased with RF payload lengths. This is because a larger payload size requires more processing time at the Zigbee transmitter side as well as more transmission time during the transmission over the air.

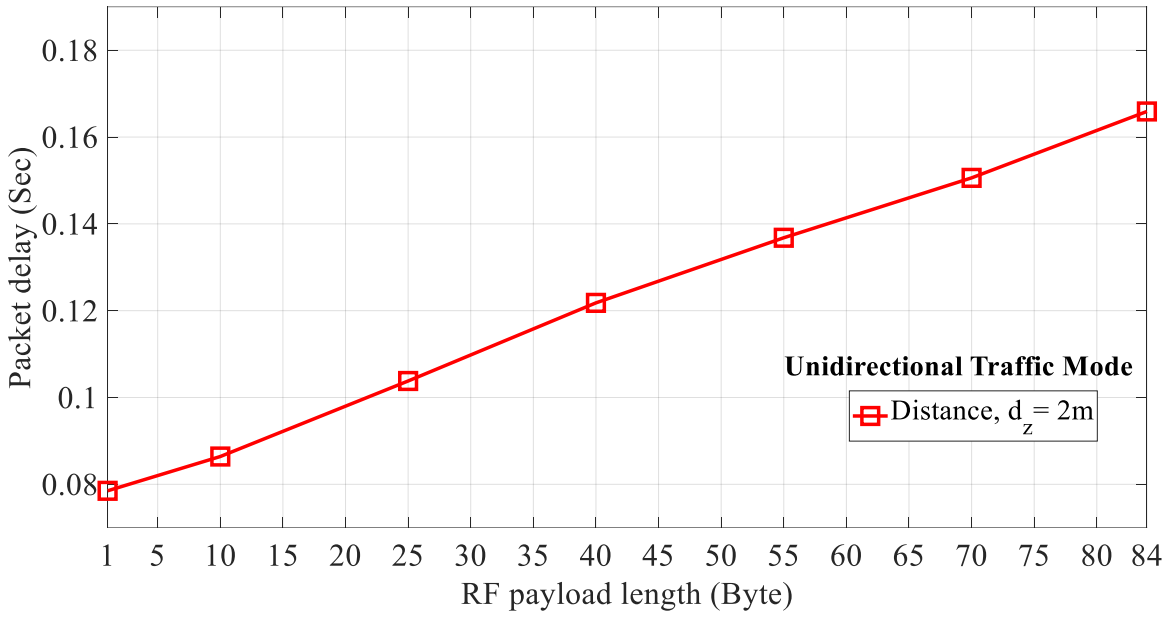

Figure 5.5: Packet delay versus RF payload length

5.2.3 Packet Drop Rate (PDR) Measurement

This experiment was aimed to measure and analyze the adverse effects of Wi-Fi interference traffic on Zigbee communication in terms of Packet Drop Rate (PDR). The PDR measurement study was conducted in two phases: without Wi-Fi traffic and with Wi-Fi traffic.

Table 5.5: Experimental parameters for the experiment 5.2.3.1

Parameters	Zigbee	Wi-Fi
Operating Channel	12	No Wi-Fi Traffic
Transmit Power, P_t	8 dBm	
Packet Size	64 Bytes	
Distance between Zigbee devices, d_z	0m – 6m	
Traffic mode	Unidirectional	-

5.2.3.1 Packet Drop Rate (PDR) measurement without Wi-Fi traffic. The goal of this experiment is to understand the behavior of the Zigbee network when there is no Wi-Fi traffic. For this experiment, the experimental topology in Figure 4.1 was considered. During the experiment, the distance between Zigbee transmitter and receiver (d_z) was varied between 0 m to 6m and the data was taken in terms of PDR. The experiment was carried out with the transmission of 200 Zigbee packets at every 500ms transmission time interval from the Zigbee TX. The number of successfully received packets were counted at the receiver side to generate the PDR using equation 5.1. Experimental parameters used in this experiment are listed in Table 5.5.

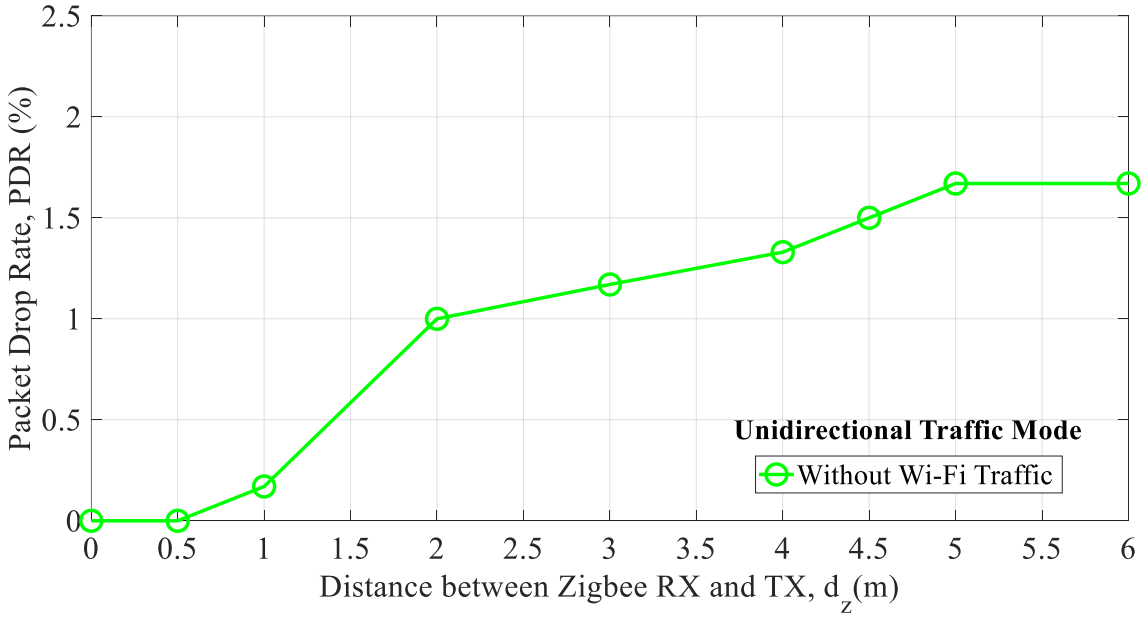

Figure 5.6: PDR vs d_z under no Wi-Fi traffic environment

The PDR data obtained from this experiment is plotted against different values of d_z as shown in Figure 5.6. Under no Wi-Fi traffic circumstance, the maximum PDR value was found

at d_z= 5m and 6m (1.67%). The best figure was obtained at d_z= 0m and 0.5m (0.00%), which means that there was no packet drop issue for a closer distance between the Zigbee transmitter and receiver devices. At d_z= 1m, the PDR was 0.17%; only one packet dropped out of 200 packets. Overall, the PDR was increased with the increase of distances. Therefore, it can be said that the PDR of a wireless network gets worsen with the distances. Considering this data as a reference, now we will compare this data with the one when there is Wi-Fi interference traffic.

5.2.3.2 Packet Drop Rate (PDR) measurement with Wi-Fi traffic. After measuring the PDR of the Zigbee network with no Wi-Fi traffic circumstance, a Wi-Fi network was introduced within the testbed region as shown in Figure 4.2. According to the Zigbee and Wi-Fi channels distribution in Figures 1.4 and 1.5, the experiment was carried out for three interference cases:

(i) Overlapping channel (Zigbee channel 12 & Wi-Fi channel 1)

(ii) Adjacent channel (Zigbee channel 14 & Wi-Fi channel 1), and

(iii) Non-overlapping channel (Zigbee channel 12 & Wi-Fi channel 11)

Table 5.6 provides the experimental parameters used to measure the PDR in this experiment. Here, the bandwidth is the maximum amount of data that can be transferred by the channel in every second for an ideal case and the data rate is the amount of data that was actually transferred in every second using that channel. During the experiment, we didn't assign any specific bandwidth for the TCP session, so Iperf assigned an ideal bandwidth for each TCP traffic transfer session and made the average to generate the average value (Iperf, 2021).

In order to obtain the experimental data, each time 200 Zigbee packets were transmitted from Zigbee TX to Zigbee RX with a 500ms transmission time interval, and the PDR was

calculated at the Zigbee RX side using the equation (5.1). The experiment was repeated three times to get a reliable result.

Table 5.6: Experimental parameters for the experiment 5.2.3.2

Parameters		**Zigbee**	**Wi-Fi**
Operating Channel	Case (i)	12	1
	Case (ii)	14	1
	Case (iii)	12	11
Transmit Power, P_t		8 dBm	-
Packet Size		64 Bytes	-
Average Bandwidth		-	18.8 Mbits/Sec
Average Data Rate		-	17.84 Mbits/Sec
Traffic mode		Unidirectional	-
Distance between Zigbee and Wi-Fi devices		d_z = 1m, d_w = 1m, d_{zw} = 0m – 6m	

The data of PDR (%) are plotted against different values of d_{zw} as shown in Figure 5.7. Initially, the PDR was much higher for the adjacent channel case, but it was alleviated with distances. Unarguably, the major impact was noticed in the case of the overlapping channel, especially for the smaller values of d_{zw}. The reasons behind the worst performance of Zigbee communication under overlapping channel interference can be listed as:

1. During the simultaneous transmission of Zigbee and Wi-Fi data, Zigbee transmitter (TX) was competing with Wi-Fi to get channel access but was failing to get it due to the continuous flow of stronger Wi-Fi traffic.

2. Even if the Zigbee TX got channel access and sent the packets, the packets (also the Acknowledgement (ACK) packet) were lost in the air due to interruption by Wi-Fi signals.

3. During the experiments, I noticed that sometimes Zigbee TX and RX got disconnected or disassociated due to heavy Wi-Fi interference traffic.

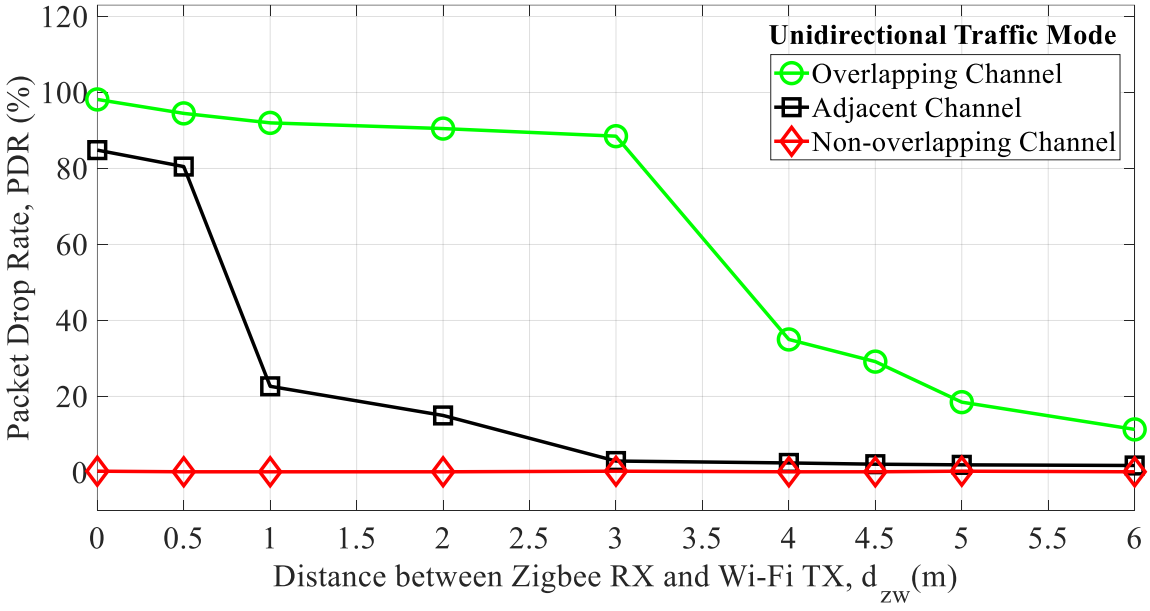

Figure 5.7: PDR versus d_{zw} with three interference cases

In the case of the non-overlapping channel, the PDR data was quite similar for every measurement point (0.17% - 0.33%); only one/two packet(s) was dropped out of 600 packets in total. This was because, in the case of the performance study, we varied the distance between the interference source (i.e., Wi-Fi transmitter) and Zigbee receiver (d_{zw} = 0m - 6m) while keeping the distance between Zigbee transmitter and Zigbee receiver d_z & Wi-Fi transmitter and Wi-Fi receiver d_w same (=1m) all the time.

For both overlapping and adjacent channel cases, with the increase of distance between the interference source (i.e., Wi-Fi transmitter) and Zigbee receiver, d_{zw}, Zigbee receiver gets some space to recover from the impact of interference of Wi-Fi transmitter, so the packet reception rate improves over the distance. But the non-overlapping channel interference traffic has a negligible impact on the Zigbee receiver. So, the increase of the distance between the Wi-Fi transmitter and Zigbee receiver (d_{zw}) doesn't have an impact on the Zigbee packet reception rate. That means, for the non-overlapping channel case, we got quite similar data for every measurement as the distance between Zigbee transmitter and receiver, d_z is fixed (=1m) and the increasing distance (d_{zw}) has nearly no impact on the Zigbee receiver. This is quite similar to the no-Wi-Fi traffic case when the distance between the Zigbee transmitter and receiver is 1m.

5.2.4 Loopback Throughput Measurement

This experiment was aimed to measure and analyze the adverse effects of Wi-Fi interference traffic on Zigbee communication in terms of loopback throughput. The throughput measurement study was conducted in two phases: without Wi-Fi traffic and with Wi-Fi traffic.

5.2.4.1 Loopback throughput measurement without Wi-Fi traffic. The goal of this experiment is to understand the behavior of the Zigbee network when there is no Wi-Fi traffic. For this experiment, the experimental topology in Figure 4.1 was considered. During the experiment, the distance between Zigbee transmitter and Zigbee receiver (d_z) was varied between 0m to 6m and the data was taken in terms of throughput. The experiment was carried out with the transmission of 200 Zigbee packets from Zigbee TX to Zigbee RX to calculate the throughput using XCTU's built-in "throughout tool" (Digi International, 2019) (p. 185) as

described in Section 5.1.2. The experiment trial was repeated three times to generate a reliable result. Experimental parameters used in this experiment are listed in Table 5.7.

Table 5.7: Experimental parameters for the experiment 5.2.4.1

Parameters	**Zigbee**	**Wi-Fi**
Operating Channel	12	No Wi-Fi Traffic
Transmit Power, P_t	8 dBm	
Packet Size	64 Bytes	
Distance between Zigbee devices, d_z	0m – 6m	
Traffic mode	Bidirectional	-

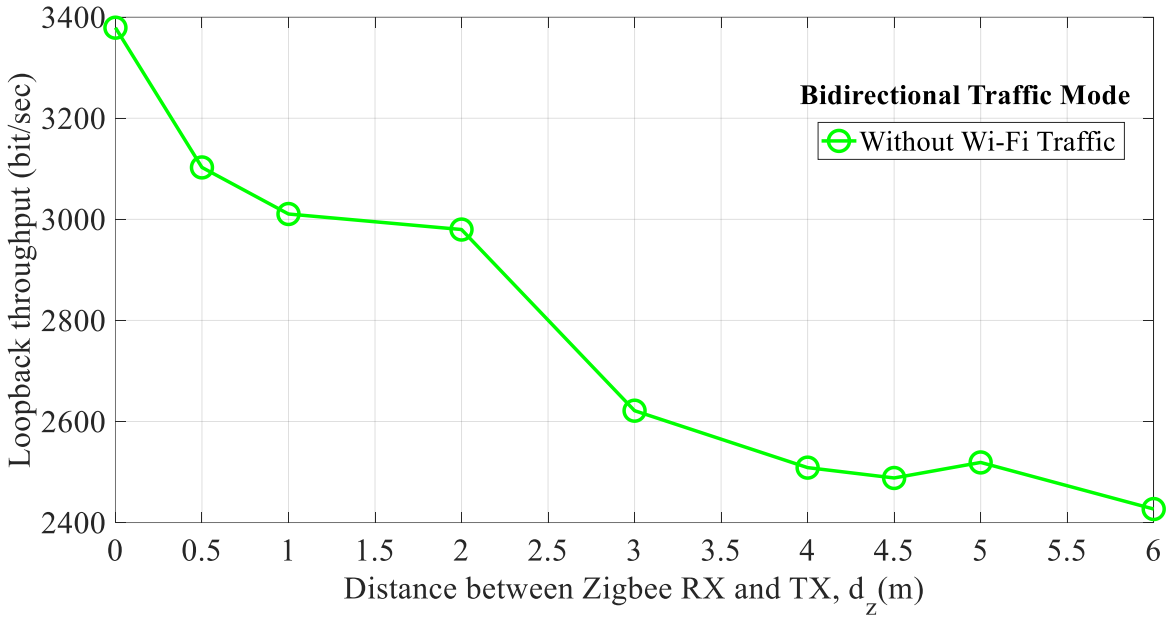

Figure 5.8: Loopback throughput Vs d_z for no Wi-Fi traffic condition

The throughput data obtained from this experiment is plotted against different values of d_z as shown in Figure 5.8. Under no Wi-Fi traffic circumstance, the maximum throughput value

(i.e., 3379.2 bit/sec) was found at d_z= 0m. The worst figure was found at d_z= 6m (2426.88 bps), which means that lower throughput values were obtained for longer distances between the Zigbee transmitter and receiver devices. Unlike the PDR characteristic, loopback throughput was dropped with the distances. Therefore, we can say that network performance drops with the distances between the transmitter and receiver.

5.2.4.2 Loopback throughput measurement with Wi-Fi traffic. After measuring the throughput of the Zigbee network with no Wi-Fi traffic circumstance, a Wi-Fi network was introduced within the testbed region as shown in Figure 4.2. The purpose of this experiment was to measure the throughput or the average data transfer ratio between two XBee Zigbee modules with the presence of Wi-Fi traffic. In this case, three interference cases were considered as we did for the packet drop rate measurement in Section 5.2.3.2:

(i) Overlapping channel (Zigbee channel 12 & Wi-Fi channel 1)

(ii) Adjacent channel (Zigbee channel 14 & Wi-Fi channel 1), and

(iii) Non-overlapping channel (Zigbee channel 12 & Wi-Fi channel 11)

The parameters used in this experiment are shown in Table 5.8. During the experiment, the distance between the Zigbee RX and Wi-Fi TX (d_{zw}) was varied from 0m to 6m while maintaining a fixed distance between Zigbee TX and Zigbee RX (d_z= 1m) and Wi-Fi TX and Wi-Fi RX (d_w= 1m). Each time 200 Zigbee packets were transmitted from Zigbee TX to Zigbee RX at a 500ms transmission interval with the presence of Wi-Fi traffic to calculate the throughput using XCTU's "throughput tool" (Digi International, 2019) (p. 185) which justifies equation 5.2. The experiment trial was repeated three times to generate a reliable result.

Table 5.8: Experimental parameters for the experiment 5.2.4.2

Parameters		**Zigbee**	**Wi-Fi**
Operating Channel	Case (i)	12	1
	Case (ii)	14	1
	Case (iii)	12	11
Transmit Power, P_t		8 dBm	-
Packet Size		64 Bytes	-
Average Bandwidth		-	18.8 Mbits/Sec
Average Data Rate		-	17.84 Mbits/Sec
Traffic mode		Bidirectional	-
Distance between Zigbee and Wi-Fi devices		d_z = 1m, d_w = 1m, d_{zw} = 0m – 6m	

Figure 5.9 shows a graph of throughput data as a function of the distance between Zigbee RX and Wi-Fi TX, d_{zw} for three interference cases. The throughputs of the Zigbee network under non-overlapping and adjacent channel cases were tolerable but the biggest impact was found in the case of the overlapping channel. The loopback throughput obtained for the non-overlapping channel case was quite similar (around 3010.56 bps) for every data measurement point. On the other hand, the impact of adjacent channel interference on Zigbee communication was noticeable for smaller distances but the Zigbee network gradually recovered as the distance between the Zigbee receiver and interference source, i.e., Wi-Fi transmitter was increased. The throughput data for the adjacent channel interference case started from only 419.84 bps at d_{zw}= 0m and reached 2488.32 bps at d_{zw}= 3m. However, the biggest impact was noticed in the case of

overlapping channel interference with only 20.48 bps at d_{zw}= 0m. The throughput increased with the distances but still, the impact was highly considerable with the highest throughput of 1792.0 bps only at d_{zw}= 6m. That was much lower than that of adjacent and non-overlapping channel interference cases.

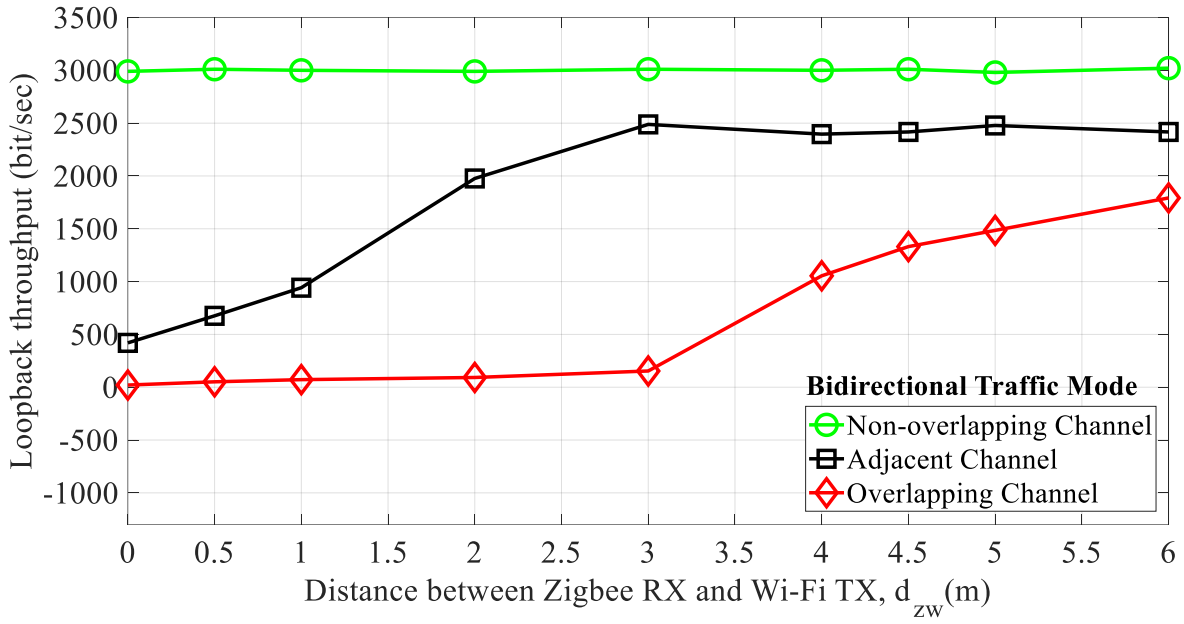

Figure 5.9: Loopback throughput versus d_{zw} at different interference cases

Interestingly, the throughput of the Zigbee network didn't change much with the distances for the non-overlapping channel case whereas the data was improved for adjacent and overlapped channel cases. This is because the non-overlapping channel interference traffic had a negligible impact on Zigbee communication and therefore the throughputs were not impacted by the increasing distances between Zigbee receiver and Wi-Fi transmitter whereas the impacts of the overlapping and adjacent channel cases on Zigbee devices were severe initially. Therefore, we were getting nearly the same throughput for the same distance between Zigbee receiver and

transmitter, d_z =1m in the case of every data point. We can also notice from the throughput measurement (with and without Wi-Fi network) data that bidirectional traffic has a significant impact on network performance than unidirectional traffic.

5.3 Chapter Summary

This chapter can be referred to as the core of the thesis. During the experiments, we have collected large-scale data to discuss the performance of the Zigbee network in the presence of a Wi-Fi network. In this chapter, we have discussed the data collection parameters and data collection process step by step. We have collected the experimental data in terms of received signal strength indicator, packet delay, packet drop rate, and loopback throughput by changing various parameters, such as operating channel, Zigbee packet size, Zigbee transmit power, and the distance between the Zigbee and Wi-Fi devices. This chapter also provides a comprehensive analysis and comparison of the experimental data.

CHAPTER VI

SUMMARY AND CONCLUSION

6.1 Summary of This Thesis Work

The performance of any communication network is very important for reliable data communication. Hence, the performance measurement of a wireless sensor network is very crucial before deploying the sensors in real life for actual operation. Zigbee networks as wireless sensor networks are very popular for indoor applications like smart homes (Tillman, 2021), but the tentative interference from other IoT networks is very challenging, especially when multiple heterogeneous networks are deployed at proximity in indoor environments.

In this thesis, the technical backgrounds of Zigbee, Wi-Fi, the spectrum sharing between Zigbee and Wi-Fi, and the performance of a Zigbee network with and without the presence of Wi-Fi traffic are studied. The experimental tested was deployed in an apartment-based indoor environment mimicking a smart home. In the first phase of this thesis, a baseline study in terms of packet drop rate and loopback throughput was carried out on the Zigbee network only to obtain a modest Zigbee transmission interval. These experiments provide us some reference points to compare and discuss the data with the data obtained with the presence of Wi-Fi traffic.

In the next phase, the performance of a Zigbee network was studied in terms of some significant performance metrics such as Received Signal Strength Indicator (RSSI), packet delay, Packet Drop Rate (PDR), and loopback throughput with and without the presence of a Wi-Fi network. The RSSI and packet delay was solely studied in an environment when there was no Wi-Fi traffic whereas the PDR and loopback throughput were studied for both with and without a Wi-Fi traffic conditions. First, the experiment for PDR measurement was conducted without Wi-Fi network to observe the ideal performance of a Zigbee network in an apartment home environment. Second, a stronger interference source (a Wi-Fi network in this case) was introduced in the testbed region to observe the impact of that interference source on the performance of the Zigbee network. The loopback throughput measurement was also conducted in the same two conditions as we did for the PDR; the only difference is that the PDR was measured with unidirectional traffic and the throughput data was collected with bidirectional traffic using loopback function. The results show the bidirectional traffic significantly affect the network performance compared to the unidirectional traffic.

6.2 Conclusions Drawn from The Results

This thesis broadly shows that the communication performance of a Zigbee network degrades badly in the case of the proximity of an interference network (i.e., a Wi-Fi network in this case) and their channel selection. This is because multiple wireless networks such as Zigbee and Wi-Fi share the 2.4 ISM radio spectrum for their operations.

In conclusion, we can see from the results and plotted figures that the worst performance of the Zigbee network was recorded in the case of overlapping channel interference (Figure 5.7 and Figure 5.9). In the case of adjacent channel interference, an interference source at a shorter

distance can heavily impact the operation of a Zigbee network as presented in Figures 5.7 and 5.9. But the performance improves as the distance between the Zigbee receiver and interference source (Wi-Fi transmitter) increases. Undoubtedly, the performance of the Zigbee network under a no interference environment was the best figure for the network (Figure 5.6 and Figure 5.8). But the impact of non-overlapping channel traffic (Figures 5.6 and 5.8) on the Zigbee network was so optimal that it looked very similar to that of no Wi-Fi traffic case. In this case, the channel selection was such far away from each other that there was nearly no interference from the Wi-Fi traffic to the Zigbee network.

In summary, our data and empirical analyses show that the Wi-Fi interference network has a significant impact on the performance of the Zigbee network, particularly in the case of the overlapping channel. The impact is more noticeable for shorter distances between the Wi-Fi transmitter (i.e., interference source) and Zigbee receiver (the main network). Therefore, we must maintain a safe distance between two heterogeneous networks (Zigbee and Wi-Fi in this case) and wisely select operating channels between Zigbee and Wi-Fi networks when they coexist, particularly in indoor environments. That means, one must ensure the proper channel section between Zigbee and Wi-Fi networks. This thesis provides a solid analysis of empirical results of a real-world Zigbee network deployed in a real-life apartment home-based indoor environment.

6.3 Future Research

In this thesis, an IoT network scenario consisting of Zigbee and Wi-Fi networks were studied in the case of an apartment-based indoor environment. Because of the temporary shutdown due to the COVID-19 pandemic, we deployed the experimental testbed in an

apartment home and started taking data. As mentioned in “section 1.7 Research Hypothesis” we detected some unwanted Wi-Fi networks (other than the testbed one) in the experimental testbed region from the surrounding neighbor apartments. Detection of multiple Wi-Fi networks is very common in an apartment home (Brown, 2020) as the apartments in a community located very close to each other and every apartment has at least a Wi-Fi internet connection.

In this thesis, those unwanted networks were ignored. To get minimal impact from such unwanted Wi-Fi networks, the experiments were conducted at midnight when there was minimal usage of those networks. Therefore, one of our future projects would be to consider these unwanted neighborhood networks and design a new testbed to analyze the communication performance of the desired network. Also, the performance of a Zigbee network with the presence of both Wi-Fi and Bluetooth networks and finding a viable solution to ensure the coexistence of these heterogeneous networks are our future study.

REFERENCES

ABRIGNANI, M. D., BURATTI, C., FROST, L. & VERDONE, R. Testing the impact of Wi-Fi interference on ZigBee networks. 2014 Euro Med Telco Conference (EMTC), 2014. IEEE, 1-6.

AKYILDIZ, I. F., SU, W., SANKARASUBRAMANIAM, Y. & CAYIRCI, E. 2002. Wireless sensor networks: a survey. *Computer networks,* 38**,** 393-422.

AL-FUQAHA, A., GUIZANI, M., MOHAMMADI, M., ALEDHARI, M. & AYYASH, M. 2015. Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. *IEEE Communications Surveys & Tutorials,* 17**,** 2347-2376.

AQEEL UR, R., ABBASI, A. Z., ISLAM, N. & SHAIKH, Z. A. 2014. A review of wireless sensors and networks' applications in agriculture. *Computer Standards & Interfaces,* 36**,** 263-270.

BHARATHIDASAN, A., ANAND, V. & PONDURU, S. 2001. Sensor Networks: An Overview, Department of Computer Science, University of California. *DAVIS, CA,* 95616.

BOUKERCHE, A. 2008. *Algorithms and protocols for wireless and mobile ad hoc networks,* John Wiley & Sons.

BROWN, E. 2016. *21 Open Source Projects for IoT* [Online]. Available: https://www.linux.com/NEWS/21-OPEN-SOURCE-PROJECTS-IOT/ [Accessed July 30, 2021].

BROWN, V. 2020. *Can other Wi-Fi networks interfere with mine?* [Online]. Available: https://www.allconnect.com/blog/wifi-interference [Accessed July 30, 2021].

BURATTI, C., CONTI, A., DARDARI, D. & VERDONE, R. 2009. An overview on wireless sensor networks technology and evolution. *Sensors,* 9**,** 6869-6896.

BUSINESS INSIDER. 2020. *How IoT devices & smart home automation is entering our homes in 2020* [Online]. Available: https://www.businessinsider.com/iot-smart-home-automation [Accessed July 30, 2021].

CARLOS-MANCILLA, M., LÓPEZ-MELLADO, E. & SILLER, M. 2016. Wireless sensor networks formation: approaches and techniques. *Journal of Sensors,* 2016.

CARLSEN, J. 2021. *Outfitting Your Smart Home: Zigbee Devices* [Online]. Available: https://www.safewise.com/zigbee-devices/ [Accessed July 30, 2021].

CHALLOO, R., OLADEINDE, A., YILMAZER, N., OZCELIK, S. & CHALLOO, L. 2012. An Overview and Assessment of Wireless Technologies and Co- existence of ZigBee, Bluetooth and Wi-Fi Devices. *Procedia Computer Science,* 12**,** 386-391.

CHEN, K. 2016. *Easily Scan Nearby Wireless Network with Xirrus Wi-Fi Inspector* [Online]. Available: https://www.nextofwindows.com/easily-scan-nearby-wireless-network-with-xirrus-wi-fi-inspector [Accessed July 28, 2021].

DASH, B. K. & PENG, J. Performance Study of Zigbee Networks in an Apartment-Based Indoor Environment. 6th International Congress on Information and Communication Technology (ICICT 2021), in press London, UK. Springer.

DE NARDIS, L. & DI BENEDETTO, M.-G. Overview of the IEEE 802.15. 4/4a standards for low data rate Wireless Personal Data Networks. 2007 4th Workshop on Positioning, Navigation and Communication, 2007. IEEE, 285-289.

DIGI INTERNATIONAL. 2016. *XBee® Zigbee® Mesh Kit* [Online]. Available: https://www.digi.com/resources/documentation/digidocs/pdfs/90001942-13.pdf [Accessed July 28, 2021].

DIGI INTERNATIONAL. 2017. *Digi XBee Zigbee Mesh Kit* [Online]. Available: https://www.digi.com/products/models/xkb2-z7t-wzm [Accessed July 30, 2021].

DIGI INTERNATIONAL. 2019. *XCTU User Guide - Digi International* [Online]. Available: https://www.digi.com/resources/documentation/digidocs/PDFs/90001458-13.pdf [Accessed July 28, 2021].

EITC. 2012. *Spectrum Sharing, Spectrum Management, and Cognitive Radio* [Online]. Available: http://www.eitc.org/research-opportunities/5g-and-beyond-mobile-wireless-technology/5g-and-beyond-technology-roadmap/radio-spectrum-signal-processing-and-beamforming/spectrum-sharing-spectrum-management-and-cognitive-radio [Accessed July 30, 2021].

ELECTRONICS NOTES. *Wi-Fi Channels, Frequencies, Bands & Bandwidths* [Online]. Available: https://www.radio-electronics.com/info/wireless/wi-fi/80211-channels-number-frequencies-bandwidth.php [Accessed July 29, 2021].

EVANS, D. 2011. The internet of things: How the next evolution of the internet is changing everything. *CISCO white paper,* 1**,** 1-11.

GILLIS, A. S. 2020. *internet of things (IoT)* [Online]. Available: https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT [Accessed July 28, 2021].

HENDERSON, D. 2021. *21 of the Best Zigbee Devices for Your Smart Home!* [Online]. Available: https://www.smarthomeperfected.com/best-zigbee-devices/ [Accessed July 30, 2021].

HOLST, A. 2021. *Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2030* [Online]. Available: https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/ [Accessed July 28, 2021].

HOME-NETWORK-HELP.COM. 2008. *Scanning Tool to Identify Interference – inSSIDer* [Online]. Available: https://www.home-network-help.com/wireless-scanning.html [Accessed July 28, 2021].

HOU, J., CHANG, B., CHO, D.-K. & GERLA, M. Minimizing 802.11 interference on zigbee medical sensors. Proceedings of the Fourth International Conference on Body Area Networks, 2009. 1-8.

HYNCICA, O., KACZ, P., FIEDLER, P., BRADAC, Z., KUCERA, P. & VRBA, R. The Zigbee experience. Proceedings of the 2nd International Symposium on Communications, Control, and Signal Processing, 2006.

IEEE COMPUTER SOCIETY LAN/MAN STANDARDS COMMITTEE 2007. IEEE Standard for Information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. *IEEE Std 802.11^*.

IEEE SA 2020. IEEE Standard for Low-Rate Wireless Networks. *IEEE Std 802.15.4-2020 (Revision of IEEE Std 802.15.4-2015)***,** 1-800.

INCEL, O. D., DULMAN, S., JANSEN, P. & MULLENDER, S. Multi-channel interference measurements for wireless sensor networks. Proceedings. 2006 31st IEEE Conference on Local Computer Networks, 2006. IEEE, 694-701.

INTERNATIONAL TELECOMMUNICATION UNION. 2015. *Internet of Things Global Standards Initiative* [Online]. Available: https://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx [Accessed July 29, 2021].

IPERF. 2021. *iPerf - The TCP, UDP and SCTP network bandwidth measurement tool* [Online]. Available: https://iperf.fr/ [Accessed July 28, 2021].

JACOB, S. & RAVI, P. 2015. Enabling coexistence of ZigBee and WiFi. *Communications on Applied Electronics (CAE)–ISSN***,** 2394-4714.

KHAN, A. A., REHMANI, M. H. & RACHEDI, A. When Cognitive Radio meets the Internet of Things? 2016 International Wireless Communications and Mobile Computing Conference (IWCMC), 5-9 Sept. 2016 2016a. 469-474.

KHAN, A. A., REHMANI, M. H. & RACHEDI, A. 2017. Cognitive-Radio-Based Internet of Things: Applications, Architectures, Spectrum Related Functionalities, and Future Research Directions. *IEEE Wireless Communications,* 24**,** 17-25.

KHAN, A. U. R., HASSAN, Q. F. & MADANI, S. 2018. *Internet of Things: Challenges, Advances, and Applications.*

KHAN, S., KRISHNAN, T. S., KOTHARI, S., EBENEZER, J., MADHUSOODANAN, K. & MURTY, S. S. Interference study in adjacent and alternate channels of ieee 802.15. 4 spectrum. 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), 2016b. IEEE, 391-395.

LAPLANTE, P. A., KASSAB, M., LAPLANTE, N. L. & VOAS, J. M. 2018. Building Caring Healthcare Systems in the Internet of Things. *IEEE systems journal,* 12**,** 10.1109/JSYST.2017.2662602.

LEUGNER, S. & HELLBRÜCK, H. Listen and talk in IEEE 802.15. 4 with dual radio. 2018 Advances in Wireless and Optical Communications (RTUWO), 2018. IEEE, 229-233.

LEUGNER, S. & HELLBRÜCK, H. eNAV-Enhanced Co-Existence of IEEE 802.15. 4 and IEEE 802.11. 2019 IEEE International Symposium on Local and Metropolitan Area Networks (LANMAN), 2019. IEEE, 1-6.

LIANG, C.-J. M., PRIYANTHA, N. B., LIU, J. & TERZIS, A. Surviving wi-fi interference in low power zigbee networks. Proceedings of the 8th ACM conference on embedded networked sensor systems, 2010. 309-322.

MAHMUD, K., TOWN, G. E., MORSALIN, S. & HOSSAIN, M. J. 2018. Integration of electric vehicles and management in the internet of energy. *Renewable and Sustainable Energy Reviews,* 82**,** 4179-4203.

MATIN, M. A. & ISLAM, M. 2012. Overview of wireless sensor network. *Wireless sensor networks-technology and protocols***,** 1-3.

MATINK. 2020. *Microwave And Wi-Fi* [Online]. Available: https://thegadgetsjudge.com/why-running-microwave-kill-wifi-connection [Accessed July 30, 2021].

MATTERN, F. & FLOERKEMEIER, C. 2010. From the Internet of Computers to the Internet of Things. *In:* SACHS, K., PETROV, I. & GUERRERO, P. (eds.) *From Active Data Management to Event-Based Systems and More: Papers in Honor of Alejandro Buchmann on the Occasion of His 60th Birthday.* Berlin, Heidelberg: Springer Berlin Heidelberg.

MISHRA, A. 2019. Co-existence Issue in IoT Deployment using Heterogeneous Wireless Network (HetNet): Interference Mitigation using Cognitive Radio. *International Journal on Advanced Science, Engineering and Information Technology,* 9**,** 109-120.

MORGAN, J. 2014. *A Simple Explanation Of 'The Internet Of Things'* [Online]. Available: https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/?sh=11fc7da81d09 [Accessed July 29, 2021].

NOMURA, K. & SATO, F. A performance study of ZigBee network under Wi-Fi interference. 2014 17th International Conference on Network-Based Information Systems, 2014. IEEE, 201-207.

PERKINS, C. E. & ROYER, E. M. Ad-hoc on-demand distance vector routing. Proceedings WMCSA'99. Second IEEE Workshop on Mobile Computing Systems and Applications, 1999. IEEE, 90-100.

PHILLIPS, G. 2021. *The Most Common Wi-Fi Standards and Types, Explained* [Online]. Available: https://www.makeuseof.com/tag/understanding-common-wifi-standards-technology-explained/ [Accessed July 29, 2021].

PIYARE, R. & LEE, S.-R. 2013. Performance analysis of XBee ZB module based wireless sensor networks. *International Journal of Scientific & Engineering Research,* 4**,** 1615-1621.

POLLIN, S., TAN, I., HODGE, B., CHUN, C. & BAHAI, A. Harmful coexistence between 802.15. 4 and 802.11: A measurement-based study. 2008 3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom 2008), 2008. IEEE, 1-6.

PRATT, M. K. 2021. *Top 12 most commonly used IoT protocols and standards* [Online]. Available: https://internetofthingsagenda.techtarget.com/tip/Top-12-most-commonly-used-IoT-protocols-and-standards [Accessed July 29, 2021].

ROSENCRANCE, L. 2017. *Zigbee* [Online]. Available: https://internetofthingsagenda.techtarget.com/definition/ZigBee [Accessed August 07, 2021].

ROYER, E. M. & TOH, C.-K. 1999. A review of current routing protocols for ad hoc mobile wireless networks. *IEEE personal communications,* 6**,** 46-55.

SAFARIC, S. & MALARIC, K. ZigBee wireless standard. Proceedings ELMAR 2006, 7-10 June 2006 2006. 259-262.

SECCI, L. & BURATTI, C. Reducing traffic congestion in ZigBee networks: Experimental results. 2013 9th International Wireless Communications and Mobile Computing Conference (IWCMC), 2013. IEEE, 627-632.

SEVERI, S., SOTTILE, F., ABREU, G., PASTRONE, C., SPIRITO, M. & BERENS, F. 2014. *M2M technologies: Enablers for a pervasive Internet of Things*.

SHERAZI, H. H. R., IQBAL, R., UL HASSAN, S., CHAUDARY, M. H. & GILANI, S. A. 2016. ZigBee's received signal strength and latency evaluation under varying environments. *Journal of Computer Networks and Communications,* 2016.

SHI, J., WANG, Y., LI, C. & JIANG, Y. Test method of power and packet loss rate in smart home. Proceedings 2013 International Conference on Mechatronic Sciences, Electric Engineering and Computer (MEC), 2013. IEEE, 729-732.

SOHRABY, K., MINOLI, D. & ZNATI, T. 2007. *Wireless sensor networks: technology, protocols, and applications*, John wiley & sons.

STABLES, J. 2021. *Zigbee explained: Hubs, the best Zigbee devices and everything you need to know* [Online]. Available: https://www.the-ambient.com/guides/zigbee-devices-complete-guide-277#:~:text=There%20are%20over%20400%20members,for%203.8%20billion%20IEEE%20802.15. [Accessed July 30, 2021].

TEXAS INSTRUMENTS. 2019. *What's New in Zigbee 3.0* [Online]. Available: https://www.ti.com/lit/an/swra615a/swra615a.pdf?ts=1625779126483&ref_url=https%253A%252F%252Fwww.google.com%252F [Accessed July 28, 2021].

THONET, G., ALLARD-JACQUIN, P. & COLLE, P. 2008. Zigbee-wifi coexistence. *Schneider Electric White Paper and Test Report,* 1**,** 1-38.

TILLMAN, M. 2021. *What is Zigbee and why is it important for your smart home?* [Online]. Available: https://www.pocket-lint.com/smart-home/news/129857-what-is-zigbee-and-why-is-it-important-for-your-smart-home [Accessed July 30, 2021].

VAN BLOEM, J. W. H. & SCHIPHORST, R. 2011. Measuring the service level in the 2.4 GHz ISM band. *CTIT Technical Report Series.* Centre for Telematics and Information Technology (CTIT), Enschede.

VERDONE, R., DARDARI, D., MAZZINI, G. & CONTI, A. 2010. *Wireless sensor and actuator networks: technologies, analysis and design*, Academic Press.

WAN, J., CHEN, W., XU, X. & FANG, M. An Efficient Self-Healing Scheme for Wireless Sensor Networks. 2008 Second International Conference on Future Generation Communication and Networking, 13-15 Dec. 2008 2008. 98-101.

WANG, C., JIANG, T. & ZHANG, Q. 2014. *ZigBee Network Protocols and Applications*, Auerbach Publications.

WANG, X. & YANG, K. A real-life experimental investigation of cross interference between wifi and zigbee in indoor environment. 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2017. IEEE, 598-603.

WIKI. 2021a. *Internet of things* [Online]. Available: https://en.wikipedia.org/wiki/Internet_of_things [Accessed August 08, 2021].

WIKI. 2021b. *Wi-Fi* [Online]. Available: https://en.wikipedia.org/wiki/Wi-Fi [Accessed July 28, 2021].

WON, C., YOUN, J., ALI, H., SHARIF, H. & DEOGUN, J. Adaptive radio channel allocation for supporting coexistence of 802.15. 4 and 802.11 b. IEEE Vehicular Technology Conference, 2005. IEEE; 1999, 2522.

YANG, G. & YU, Y. ZigBee networks performance under WLAN 802.11 b/g interference. 2009 4th International Symposium on Wireless Pervasive Computing, 2009. IEEE, 1-4.

YICK, J., MUKHERJEE, B. & GHOSAL, D. 2008. Wireless sensor network survey. *Computer networks*, 52**,** 2292-2330.

YOON, D. G., SHIN, S. Y., KWON, W. H. & PARK, H. S. Packet error rate analysis of IEEE 802.11 b under IEEE 802.15. 4 interference. 2006 IEEE 63rd Vehicular Technology Conference, 2006. IEEE, 1186-1190.

ZIGBEE ALLIANCE. 2008a. *What is Rf4ce?* [Online]. Available: https://zigbeealliance.org/solution/rf4ce/ [Accessed July 28, 2021].

ZIGBEE ALLIANCE. 2008b. *Zigbee specification* [Online]. Available: https://zigbeealliance.org/solution/zigbee/ [Accessed July 28, 2021].

ZIGBEE ALLIANCE. 2019. *ZigBee Pro* [Online]. Available: https://web.archive.org/web/20191102191652/https:/www.zigbee.org/zigbee-for-developers/zigbee-pro/ [Accessed July 28, 2021].

ZIGBEE ALLIANCE. 2021. *Products CERTIFIED BY THE ALLIANCE* [Online]. Available: https://zigbeealliance.org/product_type/certified_product/ [Accessed July 30, 2021].

BIOGRAPHICAL SKETCH

Biswajit Kumar Dash was born on January 20, 1993, in a small village in Bangladesh. He graduated from Rajshahi University of Engineering & Technology (RUET) in 2015 with a bachelor's degree in Electronics and Telecommunication Engineering. Following graduation, he started a professional carrier as a System Engineer in a telecom operator in 2016 and later, worked with another telecommunication and networking company as an Engineer till 2019. Biswajit started the Electrical Engineering master's program at the University of Texas Rio Grande Valley (UTRGV) in the Fall of 2019. Upon entering the graduate program, he began working with Dr. Jun Peng for his master's level research. Biswajit was awarded the university's most prestigious scholarship, "Presidential Graduate Research Assistantship (PGRA)". He attended several poster competitions at the University of Texas Rio Grande Valley during his academic journey in UTRGV and one of his posters won first place in the 2021 Engineers Week poster competition in the Electrical and Computer Engineering Department graduate student category. One of his papers has recently been presented at the 6th International Congress on Information and Communication Technology (ICICT 2021) that was held in London, the United Kingdom on February 25- 26 2021. Biswajit received his master's degree in Electrical Engineering from the University of Texas Rio Grande Valley in the Summer of 2021 and can be reached through email at biswajit.rueten@gmail.com.