Hindawi
Journal of Computer Networks and Communications
Volume 2022, Article ID 2144702, 14 pages
https://doi.org/10.1155/2022/2144702

*Research Article*

# Zigbee Wireless Sensor Networks: Performance Study in an Apartment-Based Indoor Environment

**Biswajit Kumar Dash and Jun Peng**

*Department of Electrical and Computer Engineering, The University of Texas Rio Grande Valley, Edinburg, TX 78539, USA*

Correspondence should be addressed to Jun Peng; jun.peng@utrgv.edu

Received 6 March 2022; Revised 6 July 2022; Accepted 15 July 2022; Published 5 August 2022

Academic Editor: Bilal Khalid



Zigbee is a very popular technology for Internet of things (IoT) networks mainly because of its low power consumption and low-cost features. It shares the unlicensed 2.4 GHz Industrial, Scientific, and Medical (ISM) radio band with other wireless networks such as Wi-Fi. Usually, Zigbee and Wi-Fi networks coexist in indoor environments for their respective applications. Hence, the coexistence introduces interference for both types of networks lowering the performance of the networks, but Zigbee suffers more significant performance losses because of its lower transmission power than Wi-Fi. Since the number of IoT devices is increasing at an unprecedented rate due to numerous emerging applications and thus making the indoor environments very populous, the peaceful coexistence between Zigbee and Wi-Fi networks in proximity becomes an important research study. For this purpose, this paper presents a comprehensive performance study of a Zigbee network in the presence of a Wi-Fi interference network in a real-life apartment-based indoor environment where Wi-Fi access points of dense neighbors exist. The experiments were done in a XBee module-based Zigbee network for measuring the received signal strength indicator (RSSI), packet drop rate (PDR), and loopback throughput with and without nearby Wi-Fi traffic introduced on purpose. Various networking parameters such as the operating channels, the distances between Zigbee devices and Wi-Fi devices, the transmit timeout of Zigbee packets, and the transmission power of the Zigbee transmitter have been used in the experiments to study the network performance. Our results show that in the deployment of IoT networks in a smart home, radio interference from neighboring homes would not be an important factor, but serious considerations may need to be taken inside the same home. The experimental observations of this paper can serve as a good reference study for Zigbee network deployments in real indoor environments, particularly when interference sources are present in proximity.

## 1. Introduction

The concept of networking all the physical objects around us is gaining popularity day by day, and thus, it introduces diverse applications of the Internet of things (IoT). There are several fields where the IoT can play a vital role to improve the standards of our lives. These fields include home automation, transportation, environment monitoring, and healthcare [1]. Since the number of IoT devices is growing at an unprecedented rate, this is also opening new scopes for emerging applications resulting in a large amount of data that further couple with artificial intelligence and offer new opportunities and green innovations for business sectors [2, 3]. One study has shown that the number of physical objects connected to the Internet has exceeded the Earth's population in 2010 and the number is still growing [4]. Another study has predicted that the number of IoT devices is projected to cross 29 billion in 2030 [5]. Therefore, innovative and adaptive IoT technologies are developing for collaborating among different physical devices. Zigbee is one of such IoT technologies defined by the IEEE 802.15.4 standard. Zigbee is effectively used in many sectors such as industrial sectors [6, 7], home automation [8, 9], and medical and healthcare sectors [10, 11] as a popular IoT technology because of its numerous advantages, for example, low latency, low power consumption, large scaling capability, low cost, and flexible topology [12]; however, Zigbee has gained the ultimate popularity in indoor applications where new IoT-enabled devices are adding at an unprecedented rate and so the application types to meet customers' diverse demands.

The application of the IoT technology in home automation is to interconnect almost everything in a home, such as cell phones, television sets, washing machines, headphones, lamps, wearable devices, and thermostats so that they work together to make the home comfortable and accommodating to the residents. The prime goal of an IoT system is to enable autonomous communications among physical objects for collaboration and information sharing among them. This is a challenging task since there are diverse and heterogeneous types of IoT devices in indoor environments or in smart home environments. This is becoming more challenging because of emerging application types such as machine-to-machine communication (M2M). Moreover, there are a significant number of devices operating in another commonly used wireless technology, namely Wi-Fi (IEEE 802.11) in indoor environments. Wi-Fi in indoor environments is mainly used for the Internet access, video streaming, etc. Both Zigbee and Wi-Fi protocols operate in the same 2.4 GHz ISM spectrum band and thus create potential interference opportunities to each other. Since the smart home environments (also refer to indoor environments) are getting populous due to the growing number of IoT devices that operate with different IoT technologies such as Zigbee and Wi-Fi, the possibility of interference among such devices is increasing day by day. Moreover, Zigbee and Wi-Fi operate at some finite number of channels in the 2.4 GHz spectrum. Table 1 provides a comparative analysis of the features of Zigbee and Wi-Fi technologies.

The increasing number of heterogeneous IoT-enabled devices and their finite number of operating channels in the 2.4 GHz radio band (e.g., 14 and 16 channels for Wi-Fi-enabled and Zigbee-enabled devices, respectively) [13] are making the architecture of the IoT system more complex and congested than before. This results in an ultimate challenge to find free channels in the 2.4 GHz band for their operations, especially in indoor environments where Zigbee and Wi-Fi networks usually coexist. This situation becomes the worst where multiple IoT networks such as Wi-Fi and Zigbee coexist in proximity, resulting in interference with each other. For example, the operation of a Zigbee-enabled device can be interrupted badly due to interference from a Wi-Fi-enabled device and vice versa. However, due to the low transmission power attribute (typically 1 mW) of Zigbee devices, they tend to suffer more from interference than Wi-Fi-enabled devices while operating in the same frequency band (2.4 GHz in this case). Therefore, the coexistence between Wi-Fi and Zigbee networks in proximity poses severe challenges in the case of indoor applications of IoT networks in environments such as smart homes.

Considering the aforementioned challenges for Zigbee network implementations in smart homes, this article presents a comprehensive experimental study of a Zigbee network to analyze the performance of the network in terms of the received signal strength indicator (RSSI), packet drop rate (PDR), and loopback throughput. Moreover, to mimic a smart home environment, all experiments were carried out in a real-life home apartment by changing the operating channels of both Zigbee and Wi-Fi networks, the distance between Zigbee and Wi-Fi devices and between Zigbee devices themselves, the Zigbee transmit power, the Zigbee packet size, and the transmit timeout of Zigbee packets. Unlike the existing works such as Refs. [14–19] (discussed broadly in the related work section) where the system evaluations are performed either in simulated environments or in impractical environments, as well as in scenarios that lack considering some actual real network attributes, such as interference from other networks and continuous transmission from an interference source, that are very common in real world, our paper provides experimental results obtained from a real hardware-based experimental testbed located in an indoor environment. The main contributions of the paper relate to the performance analysis of a Zigbee network in the presence of a Wi-Fi interference network. To get real-world data, we implemented a real hardware-based Zigbee network using Digi International Zigbee XBee hardware modules [20]. Moreover, the testbed was built in a real-world apartment home where Wi-Fi access points of dense neighbors exist. The actual home Wi-Fi network acted as the testbed Wi-Fi network for the interference source of the Zigbee network. Our study and the subsequent empirical analysis reveal that the neighbor apartments' Wi-Fi access points do not act as a severe interference source; however, necessary considerations, such as the distance between devices and operating channels, need to be taken when multiple IoT networks are deployed in the same smart home. The experimental study of this paper can help determine the network configurations mentioned above during the deployment of actual Zigbee-based devices in practical indoor environments, particularly in smart home scenarios where multiple IoT networks coexist.

Regarding our previous works on this research topic, our earlier preliminary results were published in a conference proceeding [21]. Having published the initial results of this work, we provide here a significantly evolved version of that work offering more comprehensive experimental results and empirical analyses overcoming some data limitations of our earlier work. The rest of the article is organized as follows: Section 2 provides a summary of the literature review on the coexistence between Wi-Fi and Zigbee networks; Section 3 presents the components of the experimental testbed; Section 4 presents the experiments and results of this study; and finally, Section 5 concludes the paper with a summary of this study.

## 2. Literature Review

Wi-Fi and Zigbee have some overlapping operating channels in the 2.4 GHz ISM radio band as illustrated in Figure 1. Therefore, a Wi-Fi network may interrupt a Zigbee communication when they coexist in proximity [22]. For this reason, the increasing popularity of the Zigbee technology in short-range communications, especially in indoor applications, is drawing attention of researchers to study the performance of Zigbee communication and its compatibility

Table 1: Comparisons between Zigbee and Wi-Fi.

| Indices | Zigbee | Wi-Fi |
|---|---|---|
| Standard | IEEE 802.15.4 | IEEE 802.11 b/g/*n* |
| Frequency band | (2.4 G, 784 M, 868 M, and 915 M) Hz | 802.11 b/g/*n*–2.4 GHz (2.412 G–2.484 G) Hz |
| Number of channels | 16 | 11–14 |
| Data rate | 20 kbit/s (868 MHz)–250 kbit/s (2.4 GHz) | 802.11 g–6 to 54 Mbit/s<br>802.11 b–1 to 11 Mbit/s<br>802.11 n–72 to 600 Mbit/s |
| Power consumption | 10–100 mW | 10 times more than Zigbee |
| Range | 100 m (line-of-sight) | 1000 m (line-of-sight) |
| Scalability | Thousands of devices | Hundreds of devices |
| Typical transmission power | 1 mW | 50–70 mW (≤100 mW) |
| Network topology | Star, tree, and mesh | Mainly star |
| Main applications | Automation and control | Local area networking |

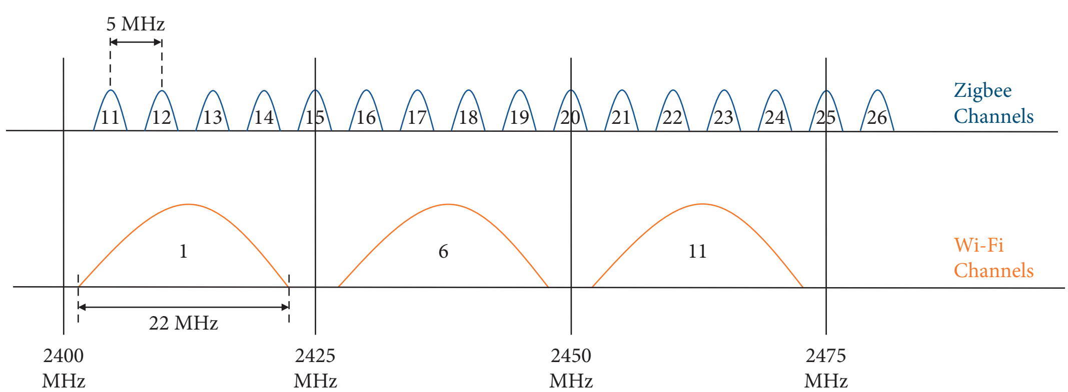


Figure 1: Zigbee and Wi-Fi channel distribution.

issues with other common indoor wireless networks such as Wi-Fi networks when they locate at proximity. Various studies and experiments have been conducted to understand the impact of the coexistence between Zigbee and Wi-Fi networks on communication performance. Generally, it is considered that the impact of interference from Zigbee networks on Wi-Fi communications is negligible, but in Refs. [23, 24], the authors have pointed out that in some cases, Zigbee can significantly impact Wi-Fi communications. However, as aforementioned, Zigbee as a low power-based technology suffers more from the Wi-Fi interference. Therefore, in this research article, we have mainly focused on the performance of Zigbee communication in the presence of a Wi-Fi network in a smart home environment.

To clearly and concisely build a discussion on the state of the art of our research topic, we present some related works in two subsections: 2.1. is on interference study of Wi-Fi over Zigbee, and Subsection 2.2. is on potential ways to ensure the coexistence between Wi-Fi and Zigbee.

*2.1. Interference Study of Wi-Fi over Zigbee.* Jamming to IEEE 802.15.4 standardized wireless sensor networks (WSNs) has been studied in Ref. [25] in which the channel spacing is changed with respect to the distance of a receiver to a jammer and a transmitter. This paper empirically shows that the impact of adjacent channel interference is not trivial. Although the results of the paper are very interesting, they do not directly applicable to industrial networks based on IEEE 802.15.4 specifications. The authors in Ref. [26] have evaluated the performance of Zigbee networks in terms of packet loss ratio (PLR) and packet error rate (PER) with the presence of 802.11 b/g interference traffic. The analytical results presented in this paper provide some insightful findings on the distance between wireless local area network (WLAN) and Zigbee nodes and the cochannel interference. The impact of interference on Zigbee networks with respect to PLR and average round-trip time (RTT) is studied in Ref. [27] using overlapped and nonoverlapped channels, but no method to improve the PLR is proposed. A comprehensive study on evaluating the impact of continuously changing communication environments on various networking performances (e.g., RSSI and latency) has been conducted in Ref. [28] in the presence of multiple obstacles that may lead to severe degradation of the overall performance of the network. Eventually, a suitable frame size of the Zigbee packet is suggested for different situations. The interference of 802.11 over Zigbee has been studied in Ref. [29] using Zigbee medical sensors. The effect of adjacent and alternate channel interference has been investigated in Ref. [14] using packet drop ratio. However, the interference sources used in this paper are not continuous, while in our paper, transmission from the interference source (i.e., Wi-Fi) is continuous, which is very common for wireless communications in practice.

While all the works discussed above are related to the coexistence between Wi-Fi and Zigbee networks, some studies have also been conducted that consist of only Zigbee networks to understand their performance as wireless sensor networks in indoor environments. For example, in Ref. [15], the authors perform the rage and timing test of a customized radio module in an indoor setting. The paper claims that the effective range of a Zigbee network is approximately 12 meters based on the results obtained from a series of experiments in an indoor environment where radios go through drywalls. However, this conclusion is based on a specific test case and cannot be implied in real-world wireless communications as a universal truth. In Ref. [16], Piyare and Lee evaluate XBee module-based Zigbee wireless sensor networks of both single-hop and multi-hop networks and claim that the Zigbee modules are suitable for applications that require lower data rates. Another work on evaluating the performance of Zigbee-based WSNs for temperature and humidity monitoring under different environments reaches the same conclusion [17]. Results obtained from a testbed in an actual household environment show that the network performance in the line-of-sight case is better than in the non-line-of-sight case [18], as expected.

While the works in Refs.[15–18] provide some interesting results and analyses, they fail to consider some real network scenarios such as interference from other communication types that are very common in practice. Besides, in our paper, we have created a real-world network scenario consisting of an interferer network, i.e., a Wi-Fi network. Moreover, we have conducted our experiments in a real-life apartment environment where the communication scenario is very complex due to the presence of heterogeneous wireless networks such as Wi-Fi and Bluetooth in dense neighbors.

*2.2. Potential Ways to Ensure the Coexistence between Wi-Fi and Zigbee.* Besides analyzing the interference, some researchers have proposed some potential ways to facilitate the coexistence between Zigbee and Wi-Fi networks for indoor environments. The traditional method to mitigate the interference between Zigbee and WLAN is to change the MAC frame structure or MAC parameters, which increases the protocol complexity of both technologies. Instead, leaving a time interval between two consecutive packets of Wi-Fi traffic has been proposed in Ref. [30]. However, this study does not offer any appropriate time interval that can be used as a universal case. Another method called WiseBee is proposed in Ref. [19] to help the coexistence between Zigbee and Wi-Fi in IoT systems. The experiment of this paper is conducted in a simulation environment (i.e., Simulink), not in a real environment where the communication scenario is very challenging. One of the popular strategies to cope with the interferers is to detect the interference and retreat from the interferers by dynamically adjusting power and switching operating channels [31]. However, in paper [32], the authors have shown that channel switching and Wi-Fi radio power adjustment cannot be an effective way to diminish the interference in some scenarios where two heterogeneous radio modules (Zigbee and Wi-Fi in this case) are placed near to each other. Further, a heterogeneous network integrating multiple wireless technologies has been proposed to facilitate Wi-Fi networks accessing Zigbee communications. A cognitive radio (CR) algorithm for mitigating the interference of IEEE 802.11 b/g/n network to IEEE 802.15.4 network is presented in Ref. [33], which is based on the analytical and empirical packet error rate (PER).

A comparative study of Advanced Clear Channel Assessment and Clear Channel Assessment mechanisms is presented in Ref. [34]. However, those strategies are not quite sufficient to reduce collisions due to protocol deficiencies of IEEE 802.15.4. Hence, in Ref. [35], the authors have demonstrated a reduction of up to 50 percent of IEEE 802.15.4 frame losses under strong interference using a mechanism called the extended network allocation mechanism. Moreover, an adaptive scheme has been designed and evaluated in Ref. [36] to address the coexistence between 802.15.4 and 802.11 b in the case of large-scale sensor network applications. The proposed scheme is based on using multiple radio channels; however, it is difficult to implement it in practice since Zigbee uses only a single channel in each personal area network. BuzzBuzz, a MAC solution, has been proposed in Ref. [37] using an additional header and payload to enable the coexistence between Wi-Fi and Zigbee networks. This solution is particularly effective to mitigate Zigbee packet losses due to bit errors, but it needs additional spectrum resources such as 30% additional bytes.

While some of the works discussed in the above two subsections provide some interesting results, they still lack considering numerous wireless communication features that are present in practice. Most of the works have used either simulation, whereas the result could not be as effective as in real-world experiments or used environments that are not practical. Some of the schemes use extra overhead and payload for Zigbee, which may need additional spectrum resources and thus cause complexity. In addition, some of the previous studies have not considered continuous transmission from interference source(s) in the case of the coexistence between Zigbee and interferer networks. On the contrary, in this research article, we present a set of experimental results using a XBee module-based Zigbee testbed in the presence of a continuously transmitting Wi-Fi network. Moreover, all our experiments were performed in an actual apartment home mimicking a smart home environment where Wi-Fi access points of dense neighbors exist besides the Wi-Fi access point that we purposefully introduced in the proximity in some experiments. We also propose some guidelines for the positioning of Zigbee devices and selecting operating channels with respect to the interference network (a Wi-Fi network in our case) in a smart home environment, particularly when the Zigbee and interference networks are present in proximity.

## 3. Overview of the Experimental Testbed

All of the experiments in this study were done in an indoor, apartment environment. The testbed comprised two IoT networks: a Zigbee network and a Wi-Fi network. We used

Digi XBee Zigbee Mesh Kit [20] from Digi International for the Zigbee network. The Digi International's XBee Configuration and Test Utility (XCTU) [38], a free multiplatform application, was used to configure Zigbee modules and to generate Zigbee traffic between the transmitter and receiver modules. Communication between the XCTU software and XBee modules was performed through the XBee USB interface connected to a personal computer (i.e., a laptop) using a USB cable as shown in Figure 2. The reasons behind using Digi's XBee Zigbee modules are that they are quite popular among research communities for Zigbee experimentations in different environments [39–41] including indoor environments [30, 42–45] and that they are low-cost devices. Moreover, the manufacturer states that their modules can interact with other standard Zigbee modules or devices [46]. Hence, it is reasonable to use XBee modules as Zigbee products in our experiments.

In our experiments, the coordinator device and the end device act as a Zigbee receiver (RX) and a Zigbee transmitter (TX), respectively. For the rest of the paper, we refer to XBee Zigbee modules as either XBee modules or Zigbee modules and transmitter and receiver as transmitter/TX and receiver/RX, respectively. In addition to the Zigbee network, a Wi-Fi network was deployed using a home Wi-Fi router, which acted as a Wi-Fi access point, along with two smartphones running the Iperf version 3 software [47] to generate and receive Wi-Fi traffic. It is worth mentioning here that we used the TCP data traffic mode of the Iperf to generate the TCP traffic from one Wi-Fi-enabled smartphone to the other. Figure 3 shows the experimental setup for our testbed, where $d_z$ denotes the distance between the Zigbee TX and the Zigbee RX, $d_{zw}$ represents the distance between the Zigbee RX and the Wi-Fi TX, and $d_w$ indicates the distance between the Wi-Fi TX and the Wi-Fi RX. Some of our experiments were done with the topology in Figure 3(a) where no Wi-Fi transmitter was introduced in the proximity; some others were done with the topology in Figure 3(b) where a Wi-Fi transmitter was placed in the proximity of the Zigbee receiver.

## 4. Experiments and Results

In our experiments, an experimental testbed comprising a Zigbee network and a Wi-Fi network, as shown in Figure 3, was deployed in an apartment home. The performance data of the Zigbee network were collected and analyzed under various testbed settings and performance metrics.

We divide the data measurements and analyses into two sections: Section 4.1, Zigbee Baseline Study; and Section 4.2., Zigbee Performance Study. The experiments presented in Section 4.1 were carried out before the experiments in Section 4.2 so that some parameters such as the transmit timeout of Zigbee packets can be studied first. The parameters such as the transmit timeout of Zigbee packets determined in Section 4.1 were used for the experiments in Section 4.2. The experiments together are used to study Zigbee performance with and without the presence of nearby Wi-Fi traffic.

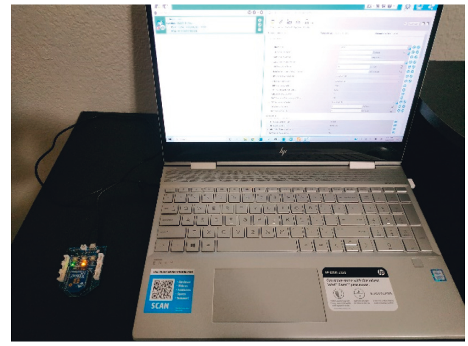

Figure 2: Interfacing XBee module to the XCTU via USB cable.

*4.1. Zigbee Baseline Study.* One purpose of this baseline study was to determine a transmit timeout for the Zigbee frames when no Wi-Fi traffic was present. We tried to determine a Zigbee packet transmit timeout that offers a high loopback throughput and a Zigbee packet transmission interval that offers a low packet drop rate (PDR). This study also provides some baseline data for the other experiments. The experimental setup shown in Figure 3(a) was used in these experiments.

*4.1.1. Baseline Study with Packet Drop Rate (PDR) Measurement.* One XBee module was configured as a Zigbee end device (also as Zigbee TX), which transmitted Zigbee frames to the Zigbee coordinator device that acted as the receiver and counted the number of successfully received packets over the transmission period. The PDR measurement was conducted using unidirectional traffic; data frames were transmitted only from the end device to the coordinator.

In the experiments, the distance between the Zigbee TX and the Zigbee RX, i.e., $d_z$, was varied in a range from approximately 0 meters to 5 meters. Each experiment was repeated three times with the same parameter settings for an average. The experiments were carried out for four different Zigbee packet transmission intervals such as 100 ms, 200 ms, 400 ms, and 500 ms. In each transmission period, 200 Zigbee frames were transmitted from the Zigbee TX to the Zigbee RX and the number of successfully received packets was counted by the XCTU at the receiver side. The PDR was calculated using the following formula:

$$\text{Packet Drop Rate PDR}\,(\%)\,\frac{P_{Tx} - P_{Rx}}{P_{Tx}} * 100, \tag{1}$$

where $P_{Tx}$ is the number of Zigbee frames transmitted by the Zigbee TX, and $P_{Rx}$ is the number of successfully received packets by the Zigbee RX. The configurations used in the experiments in this section are listed in Table 2.

Figure 4 shows the results of packet drop rate (PDR) vs $d_Z$ that were obtained from the experiments. We can see from Figure 4 that the PDR for a packet transmission interval of 500 ms is, on average, smaller than that for other packet transmission intervals, which are 100 ms, 200 ms, and 400 ms, although the PDRs are very close to each other under the same transmission distance. Note that there were always

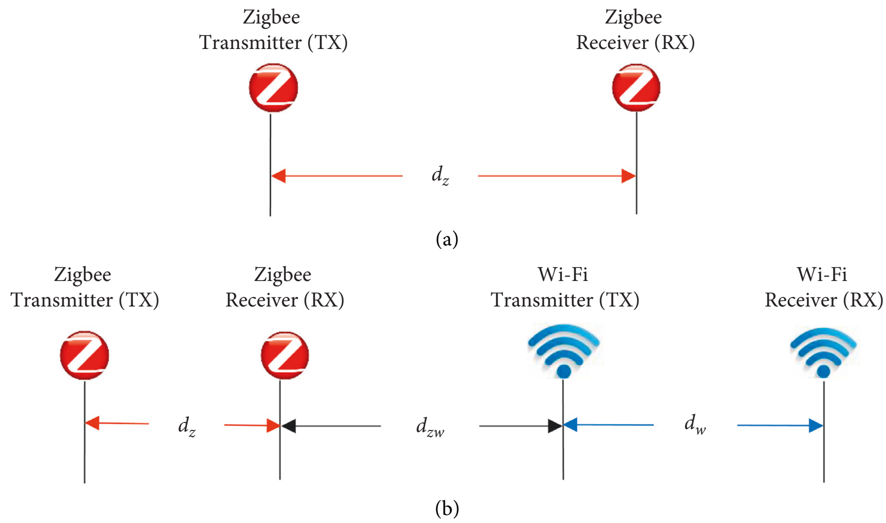


Figure 3: Testbed topologies: (a) Zigbee without a nearby Wi-Fi network. (b) Zigbee with a nearby Wi-Fi network.

Table 2: Parameters for the experiments in Section 4.1.1.

| Parameters | Zigbee | Wi-Fi |
|---|---|---|
| Operating channel | 12 | No Wi-Fi traffic |
| Transmit power, $P_t$ | 8 dBm | |
| Payload size | 64 bytes | |
| Distance between the Zigbee transmitter and receiver | $d_z = 0\,\text{m}–5\,\text{m}$ (approximately) | |
| Traffic mode | Unidirectional | |

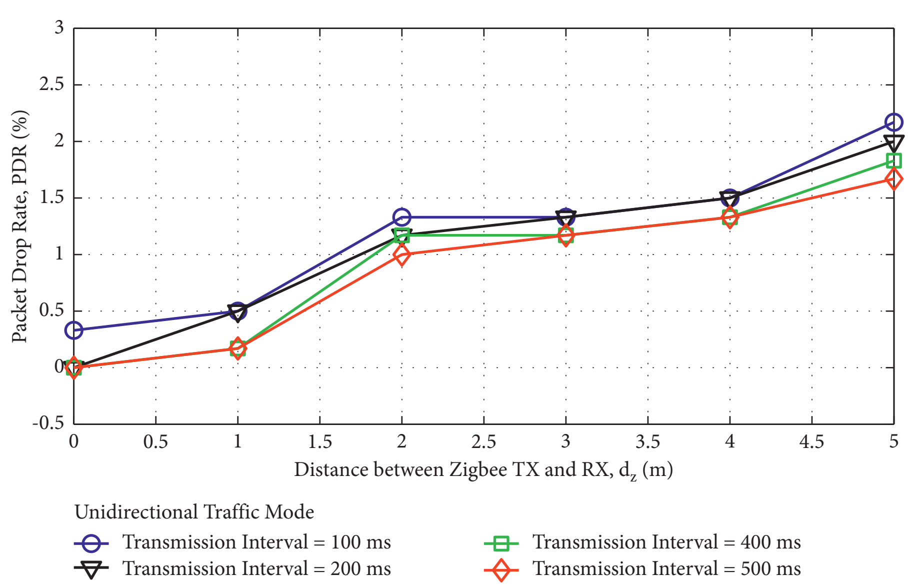


Figure 4: PDR versus $d_z$ for a range of transmission intervals.

some unrecovered losses at every distance. This was probably because of environmental noises such as the Wi-Fi traffic from the access points of dense neighbors in the building.

The authors in Ref. [30] did some experiments to assess the Zigbee packet arrival rate in the presence of Wi-Fi interference and with various Zigbee data transmission intervals, but they used an environment and network parameters different from ours.

*4.1.2. Baseline Study with Loopback Throughput Measurement.* Throughput is a vital performance metric of a communication network that measures the data transfer rate between two radio modules located in the same network. We used the hardware loopback setup in the XCTU to test bidirectional data on the link. The XCTU software package's built-in "throughput tool" [38] was used in our experiments. For this experiment, a XBee module was configured as a local radio module that acted as a Zigbee transmitter and another XBee module was configured as a remote radio module that acted as a Zigbee receiver in the same network to perform a loopback throughput measurement. A hardware loopback was created by connecting the DOUT pin to the DIN pin on the receiver XBee module so that the receiver module could echo back a successfully received frame transmitted by the host PC, which was connected to the transmitter module [38].

In the experiments, Zigbee frames with a payload of 64 bytes were transmitted with four different Zigbee packet transmit timeouts (100 ms, 200 ms, 400 ms, and 500 ms) from the local XBee module to the remote XBee module. The experiments were also carried out at various distances between the Zigbee TX and the Zigbee RX, $d_z$ (approximately 0 m to 5 m). In each experiment, 200 Zigbee packets were transmitted from the local device to the remote device and each experiment was repeated three times for an averaged performance. The main configurations used in the experiments are shown in Table 3. The loopback throughput data were collected from the XCTU controlling the local XBee module. The throughput was defined based on the following formula:

$$\text{Through put} = \frac{8 * \text{Number of bytes successfully echoed}}{\text{Transmission period}} \left(\frac{\text{bit}}{\text{sec}}\right). \tag{2}$$

The results obtained from the experiments are shown in Figure 5 as a loopback throughput vs $d_Z$ graph. The figure shows that the loopback throughput with the packet transmit timeout of 500 ms is higher than that with other packet transmit timeouts, which are 100 ms, 200 ms, and 400 ms. A longer packet transmit timeout thus helped to improve the loopback throughput in the experiments. Interestingly, a packet transmit timeout of 100 ms resulted in nearly zero loopback throughput, which showed that the packet transmit timeout of 100 ms was too small compared with the round-trip time in the loopback setup.

As aforementioned, in this baseline study, we mainly focused on testing XBee modules under different Zigbee packet transmit timeouts and transmission intervals, particularly to determine a transmit timeout and a transmission interval for Zigbee frames under an ideal condition, i.e., when no Wi-Fi traffic was present. There is a similar set of experiments presented in Ref. [16] aiming to assess the throughput of a XBee module as a function of the baud rate and the packet length. However, the parameters and other communication settings are quite different from ours. For instance, we measure the loopback throughput of the Zigbee network with bidirectional traffic flow, which is different than the regular throughput measurement as presented in Ref. [16]. Moreover, we evaluate the performance of a XBee Zigbee module under various distances between Zigbee TX and RX with a fixed Zigbee payload size.

*4.2. Zigbee Performance Study.* The experiments in this section were conducted to measure the network performance in terms of the received signal strength indicator (RSSI), packet drop rate (PDR), and loopback throughput. The Zigbee transmit timeout (500 ms) and transmission interval (500 ms) determined in the previous section were used to carry out the experiments in this section. The experiments also used other communication parameters, such as the distance between the Zigbee transmitter and its receiver, the distance between the Zigbee receiver and the Wi-Fi transmitter, the Zigbee transmission power, and the operating channels of the Zigbee and the Wi-Fi networks. The topologies used in these experiments are shown in Figure 3.

*4.2.1. Received Signal Strength Indicator (RSSI) Measurement.* The received signal strength indicator (RSSI) is an important performance indicator for a receiver in a communication network. Our experiments measured the performance of the Zigbee link in terms of its RSSI values at the receiver. In the experiments, we used various distances between the Zigbee TX and the Zigbee RX, $d_z$, and various Zigbee transmission powers, $P_t$. The experiments were performed according to the topology in Figure 3(a).

In the experiments, the Zigbee transmitter was configured to transmit 200 frames each with a payload size of 50 bytes. When the Zigbee receiver module received a packet, it sent back an acknowledgment to the Zigbee transmitter. The RSSI values at both the local module (the Zigbee TX) and the remote module (the Zigbee RX) were measured. Each experiment was repeated three times for the averaged RSSI values. Five different values of the transmission power were used in the experiments, which were 8 dBm, 5 dBm, 1 dBm, −1 dBm, and −5 dBm. Other experimental configurations used in the measurements are shown in Table 4.

Figure 6 shows the RSSI data versus the transmission distance, in a range of approximately 0 meters to 6 meters. The data in the figure show the RSSI values for five different values of the transmission power, $P_t$. As anticipated, the RSSI values decrease with the increase in the transmission distance. The figure also shows that the RSSI drops fast in the first couple of meters and then slows down in decreasing for longer transmission distances.

*4.2.2. Packet Drop Rate (PDR) Measurement.* The experiments presented in this section were done to study the adverse effects of nearby Wi-Fi transmissions on a Zigbee network in terms of packet drop rate (PDR). The experiments were first done without the nearby Wi-Fi transmissions for reference and then with the Wi-Fi transmissions for comparison.

*(1) Packet Drop Rate (PDR) Measurement without the Wi-Fi Transmissions.* There were no nearby Wi-Fi transmissions for the experiments shown in this section. The experiments were conducted using the topology in Figure 3(a). In the experiments, the distance between the Zigbee transmitter and its receiver, $d_z$, was varied between approximately 0 meters and 6 meters, and the data were collected to measure PDR using the same procedure as described in Section 4.1.1.

Table 3: Parameters for the experiments in Section 4.1.2.

| Parameters | Zigbee | Wi-Fi |
|---|---|---|
| Operating channel | 12 | No Wi-Fi traffic |
| Transmit power, $P_t$ | 8 dBm | |
| Payload size | 64 bytes | |
| Distance between the Zigbee transmitter and receiver | $d_z = 0$ m–5 m (approximately) | |
| Traffic mode | Bidirectional, loopback | |

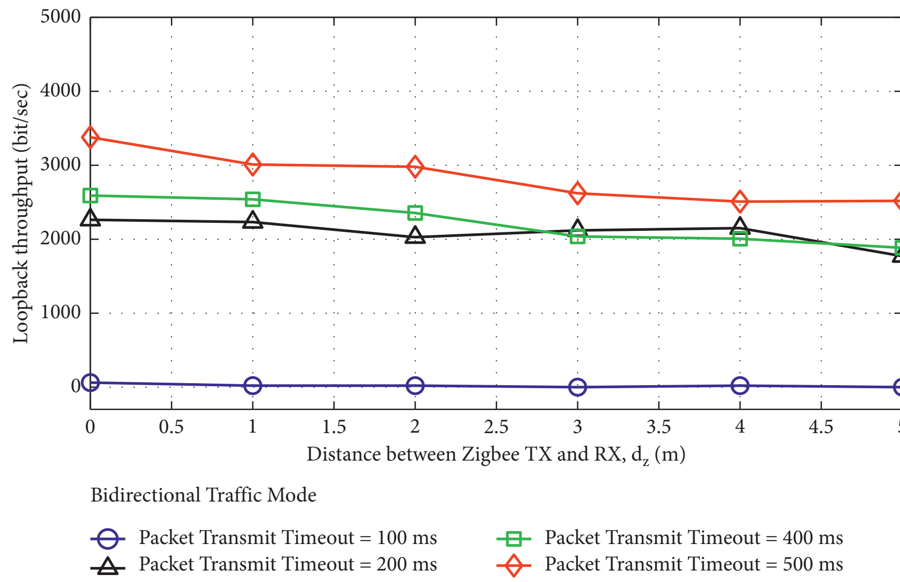


Figure 5: Throughput versus $d_z$ for a range of packet transmit timeouts.

Table 4: Parameters for the experiments in Section 4.2.1.

| Parameters | Zigbee | Wi-Fi |
|---|---|---|
| Operating channel | 12 | No Wi-Fi traffic |
| Transmit power, $P_t$ | (8, 5, 1, −1, −5) dBm | |
| Payload size | 50 bytes | |
| Distance between the Zigbee transmitter and receiver | $d_z = 0$ m–6 m (approximately) | |
| Traffic mode | Unidirectional | |

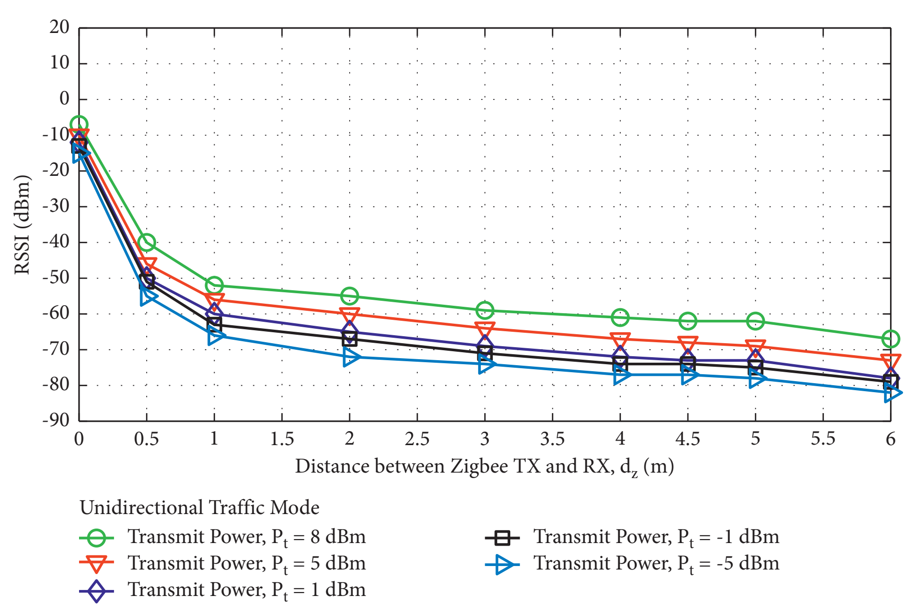


Figure 6: RSSI versus $d_z$ for a range of transmit power.

In each experiment, 200 Zigbee frames were transmitted, and each experiment was repeated three times for averaging. Parameters used in the experiments are shown in Table 5.

The PDR data obtained in the experiments are shown against the transmission distance, $d_z$, in Figure 7. When there were no nearby Wi-Fi transmissions, the highest PDR was about 1.67% as shown in the figure. The results imply that the PDRs were low when there were no nearby Wi-Fi transmissions. The PDR, in general, increases with the distance, as expected.

*(2) Packet Drop Rate (PDR) Measurement with Nearby Wi-Fi Transmissions.* In the experiments presented in this section, a Wi-Fi transmitter was introduced in proximity to the Zigbee receiver as shown in Figure 3(b). The Wi-Fi transmitter acted as an interference source that was continuously transmitting Wi-Fi traffic during the experiments. Based on the Zigbee and Wi-Fi channel distributions shown in Figure 1, the experiments were carried out to study three interference cases:

(1) Overlapping channels (Zigbee channel 12 and Wi-Fi channel 1);
(2) Adjacent channels (Zigbee channel 14 and Wi-Fi channel 1); and
(3) Nonoverlapping channels (Zigbee channel 12 and Wi-Fi channel 11).

Table 6 presents the experimental parameters used in the experiments shown in this section. In the experiments, the Iperf tool was used to measure the Wi-Fi average link speed in the channel. In each experiment, 200 Zigbee frames were transmitted from the Zigbee transmitter to its receiver. Each experiment was repeated three times to obtain an average.

The collected data of PDR are shown against the distance between the Zigbee receiver and the Wi-Fi transmitter, $d_{zw}$, in Figure 8. In the case of nonoverlapping channels, the PDR of the Zigbee network was near zero (0.17%) at $d_{zw}$ of approximately 0 meters and 0.5 meters. The packet drop rate only slightly increased with the increase in the distance, which was caused by the attenuation of Zigbee signals over distance. The data show that the Wi-Fi network operating in a channel nonoverlapping with that of the Zigbee network had a negligible impact on the Zigbee network.

The situation changed when the two networks operated at overlapping channels and adjacent channels. In the case of adjacent channels, the PDR of the Zigbee network was severely or significantly high when the Wi-Fi transmitter was within 3 meters of the Zigbee receiver. The PDR became very low after the Wi-Fi transmitter was moved out of the range of 3 meters. The situation became worse when the two networks used overlapping channels. As shown in Figure 8, the PDR of the Zigbee network was severely high when the Wi-Fi transmitter was within 5 meters of the Zigbee receiver; at 3 meters, the PDR was close to or more than 90%. The PDR was still significant when the Wi-Fi transmitter was at 6 meters to the Zigbee receiver. During the experiments, the Zigbee transmitter and the Zigbee receiver sometimes became even disassociated due to heavy Wi-Fi interference traffic.

*4.2.3. Loopback Throughput Measurement.* This section presents a set of experiments studying the adverse effects of nearby Wi-Fi transmissions on a Zigbee network in terms of loopback throughput. The experiments were first done without the nearby Wi-Fi transmissions for reference and then were done with the Wi-Fi transmissions in proximity.

*(1) Loopback Throughput Measurement without Nearby Wi-Fi Transmissions.* The experiments presented in this section were conducted to understand the behavior of the Zigbee network when there were no nearby Wi-Fi transmissions. In the experiments, the topology in Figure 3(a) was used, and the distance between the Zigbee transmitter and the Zigbee receiver, $d_z$, was varied in the range of approximately 0 meters to 6 meters. Each experiment was done with the transmission of 200 Zigbee loopback packets from the Zigbee TX to the Zigbee RX with the XCTU's built-in "throughout tool" [38]. Each experiment was repeated three times for an average throughput data. The parameters used in the experiments are listed in Table 7.

The throughput data obtained in the experiments are shown against the transmission distance, $d_z$, in Figure 9. When there was no nearby Wi-Fi traffic, the highest throughput of 3379.2 bps was found at the transmission distance of about 0 meters. The lowest throughput occurred at the transmission distance of about 6 meters, which was 2426.88 bps. Explicitly, the loopback throughput, in general, decreases with the distance.

*(2) Loopback Throughput Measurement with Nearby Wi-Fi Transmissions.* Experiments introduced in this section were performed according to the topology in Figure 3(b), where a Wi-Fi transmitter was placed in proximity of the Zigbee receiver. In the experiments, the loopback throughput between the Zigbee transmitter and its receiver was obtained. There were three interference cases in the experiments:

(1) Overlapping channels (Zigbee channel 12 and Wi-Fi channel 1);
(2) Adjacent channels (Zigbee channel 14 and Wi-Fi channel 1); and
(3) Nonoverlapping channels (Zigbee channel 12 and Wi-Fi channel 11).

The parameters used in the experiments are shown in Table 8. In each experiment, 200 loopback Zigbee frames were transmitted from the Zigbee TX to the Zigbee RX. Each experiment was repeated three times for average throughput data. Figure 10 shows the throughput as a function of the distance between the Zigbee RX and the Wi-Fi TX, $d_{zw}$, for the above-mentioned three interference cases. In the case of nonoverlapping channels, the loopback throughput of the Zigbee network was not significantly affected by the nearby Wi-Fi transmissions. However, the other two cases were different.

In the case of adjacent channels, the loopback throughput increased gradually as the distance between the Wi-Fi transmitter and the Zigbee receiver increased from approximately 0 meters to 3 meters. For the distances over 3

Table 5: Parameters for the experiments in Section 4.2.2 (1).

| Parameters | Zigbee | Wi-Fi |
|---|---|---|
| Operating channel | 12 | No Wi-Fi traffic |
| Transmit power, $P_t$ | 8 dBm | |
| Payload size | 64 bytes | |
| Distance between the Zigbee transmitter and receiver | $d_z = 0$ m–6 m (approximately) | |
| Traffic mode | Unidirectional | |

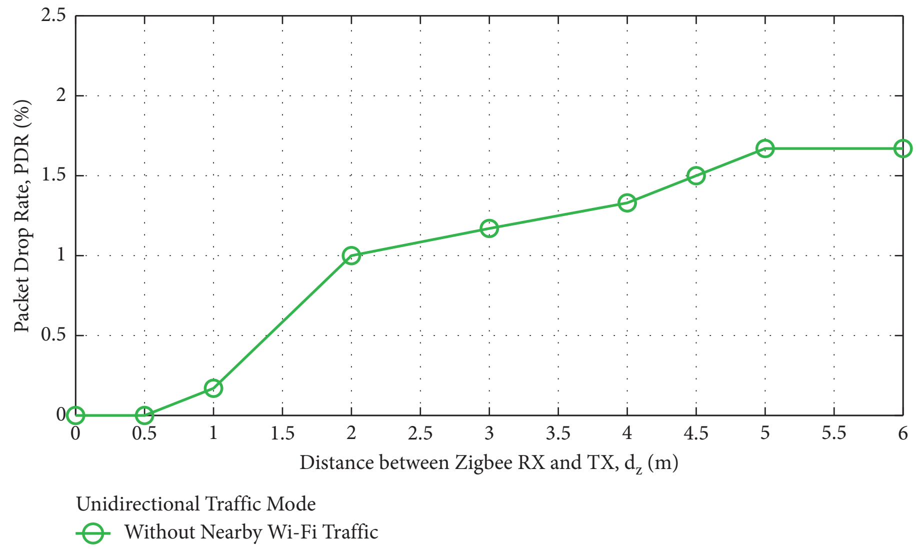


Figure 7: PDR vs $d_z$ without nearby Wi-Fi transmissions.

Table 6: Parameters for the experiments in Section 4.2.2 (2).

| Parameters | | Zigbee | Wi-Fi |
|---|---|---|---|
| Operating channel | Interference case 1 | 12 | 1 |
| | Interference case 2 | 14 | 1 |
| | Interference case 3 | 12 | 11 |
| Transmit power, $P_t$ | | 8 dBm | - |
| Payload size | | 64 bytes | - |
| Average link speed | | — | 18.8 mbps |
| Traffic mode | | Unidirectional | — |
| Distances between Zigbee and Wi-Fi devices | | $d_z = 1$ m, $d_w = 1$ m, $d_{zw} = 0$ m–6 m (approximately) | |

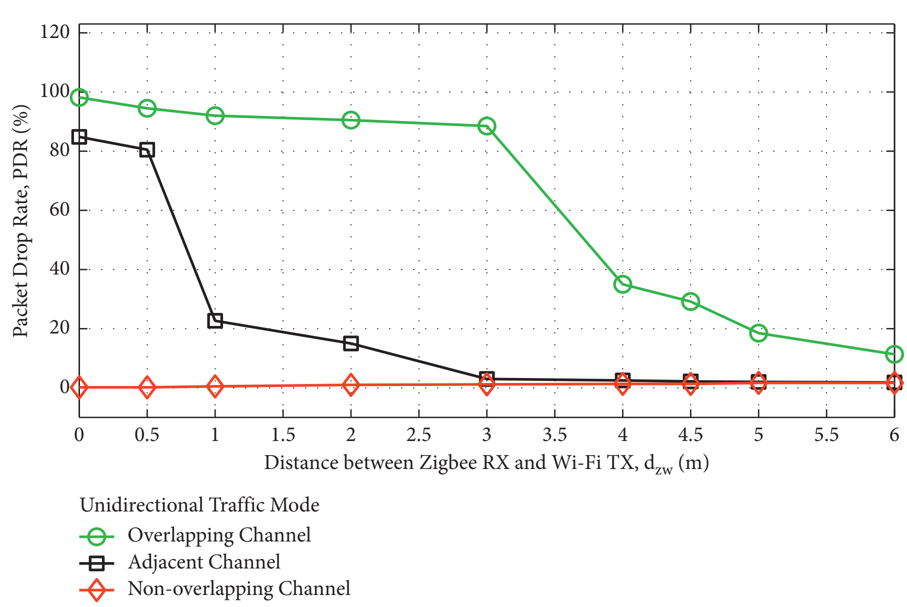


Figure 8: PDR versus $d_{zw}$ for three interference cases.

Table 7: Parameters for the experiments in Section 4.2.3 (1)

| Parameters | Zigbee | Wi-Fi |
|---|---|---|
| Operating channel | 12 | |
| Transmit power, $P_t$ | 8 dBm | |
| Payload size | 64 bytes | No Wi-Fi traffic |
| Distance between the Zigbee transmitter and receiver | $d_z = 0$ m–6 m (approximately) | |
| Traffic mode | Bidirectional | |

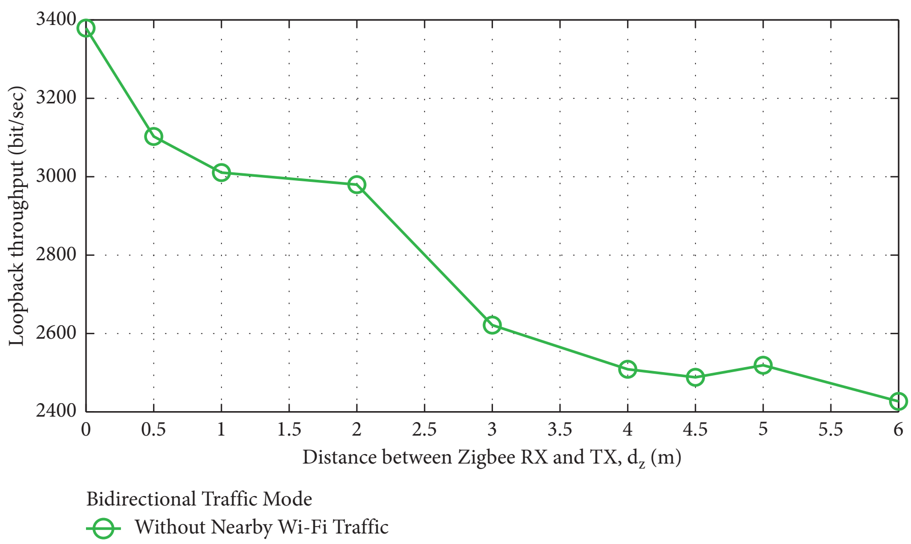


Figure 9: Loopback throughput versus $d_z$ without nearby Wi-Fi transmissions.

Table 8: Parameters for the experiments in Section 4.2.3 (2)

| Parameters | | Zigbee | Wi-Fi |
|---|---|---|---|
| Operating channel | Interference case 1 | 12 | 1 |
| | Interference case 2 | 14 | 1 |
| | Interference case 3 | 12 | 11 |
| Transmit power, $P_t$ | | 8 dBm | — |
| Payload size | | 64 bytes | — |
| Average link speed | | — | 18.8 mbps |
| Traffic mode | | Bidirectional | — |
| Distances between Zigbee and Wi-Fi devices | | $d_z = 1$ m, $d_w = 1$ m, $d_{zw} = 0$ m–6 m (approximately) | |

meters, the throughput became relatively stable in the test range of up to 6 meters as shown in Figure 10. In the case of overlapping channels, the loopback throughout was close to zero when the Wi-Fi transmitter was within 3 meters of the Zigbee receiver. The throughput gradually increased after the distance of 3 meters. In the tested range, the throughput in the overlapping channel case was always below that in the adjacent channel case for the same distance between the Wi-Fi transmitter and the Zigbee receiver.

As discussed earlier, our Zigbee performance study was aimed to rigorously assess the performance of the Zigbee network, first without any interference network and then under Wi-Fi interference. Numerous studies were performed to evaluate the Zigbee network performance under Wi-Fi interference as we have discussed in the "Literature Review" section. However, the testbed environments, network settings, performance metrics, and the goal of those studies are different from ours. For example, the authors in Ref. [30] evaluate the impact of Wi-Fi interference on a Zigbee network with respect to the Zigbee arrival rate for various distances between Zigbee nodes. Unlike the work in Ref. [30] where only one interference case was considered, we rigorously measured the PDR of the Zigbee network under three different interference conditions and provided detailed comparisons. The RSSI values of a Zigbee network were measured under no interference in Refs. [28, 48] for various distances between Zigbee nodes. We, however, extensively analyzed the impact of distances on Zigbee's RSSI for five different Zigbee transmit powers. Besides, unlike the works in Refs. [16, 48] where the throughput of Zigbee was measured under an ideal environment, no interference environment, and a simulated environment, respectively,

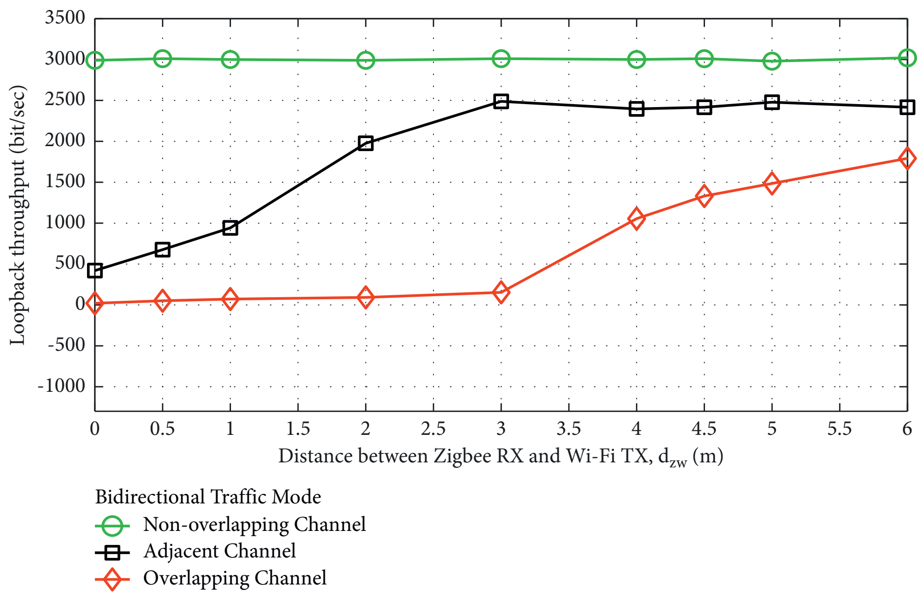


Figure 10: Loopback throughput versus $d_{zw}$ for three interference cases.

our paper presents a detailed, empirical analysis and comparisons among various interference cases, i.e., no interference, overlapping channel interference, adjacent channel interference, and nonoverlapping channel interference in a testbed located in a real apartment home environment.

## 5. Conclusion

In this paper, we present the results of an experimental study on the performance of a Zigbee network in an environment where Wi-Fi access points of dense neighbors exist besides a nearby one introduced on purpose. Our experiments were conducted in an apartment building where each of the closely spaced neighbors was supposed to own a Wi-Fi access point. Besides considering a robust environment, we performed all our experiments in a real hardware-based testbed.

We first conducted some baseline experiments without introducing a nearby Wi-Fi transmitter on purpose. In the experiments, we measured the packet drop rate of unidirectional traffic and the throughput of bidirectional traffic in the Zigbee network. We varied the distance between the Zigbee transmitter and its receiver during the experiments. We also varied the transmission power of the Zigbee transmitter in some experiments. The goals of these experiments were to determine a suitable Zigbee transmit timeout and an appropriate Zigbee transmission interval under an ideal environment, i.e., without any nearby Wi-Fi interference.

After that, we did some experiments with a Wi-Fi transmitter introduced in the proximity of the Zigbee receiver. We focused on three interference cases in our experiments. The first case was that the Zigbee network and the Wi-Fi network used channels that did not overlap with each other and were relatively far away from each other in the spectrum. The second case was that the channels were basically adjacent but not severely overlapped. In the third case, the channels were fully overlapping.

By comparing the experimental data obtained from the experiments in which a Wi-Fi transmitter was not introduced on purpose in the proximity of the Zigbee receiver with the results obtained from the experiments with such an introduced Wi-Fi transmitter, we found that neighbors' Wi-Fi access points did not severely interfere with the operation of a Zigbee network in an apartment home. So, the deployment of IoT networks in a smart home would not need to seriously consider the neighbors' radio interference. However, the data from the experiments in which a Wi-Fi transmitter was introduced in the proximity of the Zigbee receiver show that considerations need to be taken when multiple IoT networks are deployed in the same smart home. The factors include the distances between the devices of various types of networks and the channel selections among the networks for optimal performances, particularly when an owner chooses manual network configurations. Our analyses based on real-world data can also serve as a good reference study for the deployment of Zigbee-enabled devices in smart-home environments where interfering sources such as Wi-Fi networks are present.

Finally, our study is based on a relatively small testbed of Zigbee and Wi-Fi networks. Each experiment in our testbed used two Zigbee nodes and two Wi-Fi nodes to observe the interference between those two types of networks. Although our testbed was in a very small physical area so that intense interference scenarios were effectively created in our experiments, experiments in a larger testbed involving more nodes and more links might produce some other interesting results or insights. We plan to explore such scenarios in our future studies of the topic.

## Data Availability

This research does not use any preexisting dataset. However, the experimental data are available from the authors upon reasonable request.

## Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this article.


## Acknowledgments

This research received no external funding. However, the authors were employed by the University of Texas Rio Grande Valley during the research. The authors acknowledge the support received from the Electrical and Computer Engineering Department of the University of Texas Rio Grande Valley.


## References


[1] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: a survey on enabling technologies, protocols, and applications," *IEEE communications surveys & tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015.

[2] S. Chaveesuk, B. Khalid, and W. Chaiyasoonthorn, "Emergence of new business environment with big data and artificial intelligence," in *Proceedings of the 9th International Conference on Information Communication and Management*, pp. 181–185, NY York, Augest 2019.

[3] C. Muangmee, Z. Dacko-Pikiewicz, N. Meekaewkunchorn, N. Kassakorn, and B. Khalid, "Green entrepreneurial orientation and green innovation in small and medium-sized enterprises (SMEs)," *Social Sciences*, vol. 10, no. 4, p. 136, 2021.

[4] D. Evans, "The internet of things: how the next evolution of the internet is changing everything," *CISCO white paper*, vol. 1, pp. 1–11, 2011.

[5] L. S. Vailshery, "Number of IoT connected devices worldwide 2019-2030," *Stat*, 2022.

[6] Li. Zheng, "ZigBee wireless sensor network in industrial applications," in *Proceedings of the 2006 SICE-ICASE International Joint Conference*, pp. 1067–1070, IEEE, Busan, Korea (South), October 2006.

[7] S. P. Rajan and T. Abirami, "Smart sensing technology," *Smart Systems for Industrial Applications*, vol. 11, pp. 333–366, 2022.

[8] C. Gomez and J. Paradells, "Wireless home automation networks: a survey of architectures and technologies," *IEEE Communications Magazine*, vol. 48, no. 6, pp. 92–101, 2010.

[9] K. Yuneela and A. Sharma, "A review paper on technologies used in home automation system," in *Proceedings of the 2022 6th International Conference on Computing Methodologies and Communication (ICCMC)*, pp. 366–371, IEEE, Erode, India, March 2022.

[10] Z. Zhang and X. Hu, "ZigBee based wireless sensor networks and their use in medical and health care domain," in *Proceedings of the 2013 Seventh International Conference on Sensing Technology (ICST)*, pp. 756–761, IEEE, Wellington, New Zealand, December 2013.

[11] M. Islam, S. Nooruddin, F. Karray, and G. Muhammad, "Internet of things device capabilities, architectures, protocols, and smart applications in healthcare domain: a review," 2022, https://arxiv.org/ftp/arxiv/papers/2204/2204.05921.pdf.

[12] L. De Nardis and M. G. Di Benedetto, "Overview of the IEEE 802.15. 4/4a standards for low data rate wireless personal data networks," in *Proceedings of the 2007 4th Workshop on Positioning, Navigation and Communication*, pp. 285–289, IEEE, Hannover, Germany, March 2007.

[13] Wikipedia, "2.4 GHz radio use," 2022, https://en.wikipedia.org/wiki/2.4_GHz_radio_use.

[14] S. Khan, T. S. S. Krishnan, S. Kothari, J. Ebenezer, K. Madhusoodanan, and S. A. V. Satya Murty, "Interference study in adjacent and alternate channels of IEEE 802.15. 4 spectrum," in *2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, pp. 391–395, IEEE, 2016.

[15] O. Hyncica, P. Kacz, P. Fiedler, Z. Bradac, P. Kucera, and R. Vrba, "The Zigbee experience," in *Proceedings of the 2nd International Symposium on Communications, Control, and Signal Processing*, 2006.

[16] R. Piyare and S.-R. Lee, "Performance analysis of XBee ZB module based wireless sensor networks," *International Journal of Scientific Engineering and Research*, vol. 4, no. 4, pp. 1615–1621, 2013.

[17] H. Fitriawan, M. Susanto, A. S. Arifin, D. Mausa, and A. Trisanto, "ZigBee based wireless sensor networks and performance analysis in various environments," in *2017 15th International Conference on Quality in Research (QiR): International Symposium on Electrical and Computer Engineering*, pp. 272–275, IEEE, 2017.

[18] J. Shi, Y. Wang, C. Li, and Y. K. Jiang, "Test method of power and packet loss rate in smart home," in *Proceedings 2013 International Conference on Mechatronic Sciences, Electric Engineering and Computer (MEC)*, pp. 729–732, IEEE, 2013.

[19] S. Jacob and P. Ravi, "Enabling coexistence of ZigBee and WiFi," *Communications on Applied Electronics*, pp. 2394–4714, CAE)–ISSN, 2015.

[20] Digi International, "Digi XBee zigbee Mesh Kit," 2022, https://www.digi.com/resources/documentation/digidocs/PDFs/90001458-13.pdf.

[21] B. K. Dash and J. Peng, "Performance study of zigbee networks in an apartment-based indoor environment," in *Proceedings of the Sixth International Congress on Information and Communication Technology*, pp. 473–482, Springer, Singapore, July 2022.

[22] G. Thonet, P. Allard-Jacquin, and P. Colle, "Zigbee-wifi coexistence," *Schneider Electric White Paper and Test Report*, vol. 38, no. 1, pp. 1–38, 2008.

[23] D. G. Yoon, S. Y. Shin, W. H. Kwon, and H. S. Park, "Packet error rate analysis of IEEE 802.11 b under IEEE 802.15. 4 interference," in *2006 IEEE 63rd Vehicular Technology Conference*vol. 3, pp. 1186–1190, IEEE, 2006.

[24] S. Pollin, I. Tan, B. Hodge, C. Chun, and B. Ahmad, "Harmful coexistence between 802.15. 4 and 802.11: a measurement-based study," in *2008 3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom 2008)*, pp. 1–6, IEEE, 2008.

[25] Incel, O. Durmaz, S. Dulman, P. Jansen, and S. Mullender, "Multi-channel interference measurements for wireless sensor networks," in *Proceedings. 2006 31st IEEE Conference on Local Computer Networks*, pp. 694–701, IEEE, 2006.

[26] G. Yang and Y. Yu, "ZigBee networks performance under WLAN 802.11 b/g interference," in *2009 4th International Symposium on Wireless Pervasive Computing*, pp. 1–4, IEEE, 2009.

[27] M. D. Abrignani, C. Buratti, L. Frost, and R. Verdone, "Testing the impact of Wi-Fi interference on Zigbee networks," in *2014 Euro Med Telco Conference (EMTC)*, pp. 1–6, IEEE, 2014.

[28] H. H. R. Sherazi, R. Iqbal, S. Ul Hassan, M. H. Chaudary, S. A. Gilani, and S. Asfandyar Gilani, "ZigBee's received signal strength and latency evaluation under varying environments,"

*Journal of Computer Networks and Communications*, pp. 1–8, 2016.

[29] J. Hou, B. Chang, D.-K. Cho, and M. Gerla, "Minimizing 802.11 interference on zigbee medical sensors," in *Proceedings of the Fourth International Conference on Body Area Networks*, pp. 1–8, 2009.

[30] K. Nomura and F. Sato, "A performance study of ZigBee network under Wi-Fi interference," in *2014 17th International Conference on Network-Based Information Systems*, pp. 201–207, IEEE, 2014.

[31] W. Xu, K. Ma, W. Trappe, and Y. Zhang, "Jamming sensor networks: attack and defense strategies," *IEEE network*, vol. 20, no. 3, pp. 41–47, 2006.

[32] X. Wang and K. Yang, "A real-life experimental investigation of cross interference between wifi and zigbee in indoor environment," in *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)*, pp. 598–603, IEEE, 2017.

[33] A. Mishra, "Co-Existence issue in IoT deployment using heterogeneous wireless network (HetNet): interference mitigation using cognitive radio," *International Journal of Advanced Science, Engineering and Information Technology*, vol. 9, no. 1, pp. 109–120, 2019.

[34] S. Leugner and H. Hellbrück, "Listen and talk in IEEE 802.15. 4 with dual radio," in *2018 Advances in Wireless and Optical Communications (RTUWO)*, pp. 229–233, IEEE, 2018.

[35] S. Leugner and H. Hellbrück, "eNAV-Enhanced Co-Existence of IEEE 802.15. 4 and IEEE 802.11," in *2019 IEEE International Symposium on Local and Metropolitan Area Networks (LANMAN)*, pp. 1–6, IEEE, 2019.

[36] C. Won, J. Youn, H. Ali, H. Sharif, and J. Deogun, "Adaptive radio channel allocation for supporting coexistence of 802.15. 4 and 802.11 b," in *IEEE Vehicular Technology Conference*, vol. 62, no. 4, p. 2522, IEEE, 1999.

[37] C.-J. M. Liang, N. Bodhi Priyantha, J. Liu, and A. Terzis, "Surviving wi-fi interference in low power zigbee networks," in *Proceedings of the 8th ACM Conference on Embedded Networked Sensor Systems*, pp. 309–322, 2010.

[38] Digi International, "XCTU-configuration and test utility software: user guide," 2022, https://www.digi.com/resources/documentation/digidocs/PDFs/90001458-13.pdf.

[39] M. Mahi, J. Nayeen, S. Chaki, S. Ahmed, I. Tamanna, and M. Biswas, "LCADP: a low-cost accident detection prototype for a vehicular ad hoc network," in *Proceedings of the Third International Conference on Trends in Computational and Cognitive Engineering*, pp. 391–403, Springer, Singapore, 2022.

[40] K. Rasheed, L. Shahzad, S. Syed, H. A. Khan, W. Ahmed, and T. Sadiq, "Parking guidance system using wireless sensor networks," in *2021 International Conference on Decision Aid Sciences and Application (DASA)*, pp. 573–577, IEEE, 2021.

[41] Wardoyo, A. Susilo, I. Purwita Sary, and I. Taufik Maulana, "An experimental of xbee communication performance for forest fires monitoring," in *2021 3rd International Symposium on Material and Electrical Engineering Conference (ISMEE)*, pp. 325–330, IEEE, 2021.

[42] P. Lopez-Iturri, F. Casino, E. Aguirre, L. Azpilicueta, F. Falcone, and A. Solanas, "Performance analysis of zigbee wireless networks for aal through hybrid ray launching and collaborative filtering," *Journal of Sensors*, vol. 2016, pp. 1–16, 2016.

[43] Abdulwahab, M. Mohammed, M. Waled, A. Allah Osman, and A. Al-Tahir, "Wireless sensor networks for real-time monitoring and controlling of poultry farm," *Journal of Telecommunication, Electronic and Computer Engineering*, vol. 14, no. 1, pp. 21–26, 2022.

[44] K. F. Haque, A. Abdelgawad, and K. Yelamarthi, "Comprehensive performance analysis of zigbee communication: an experimental approach with XBee S2C module," *Sensors*, vol. 22, no. 9, p. 3245, 2022.

[45] T. Tuncer and E. Erdem, "Location detection of the mobile sensor with fingerprinting-based cascade artificial neural network model using received signal strength indicator in 3D indoor environment," *International Journal of Communication Systems*, vol. 34, pp. e5000–18, 2021.

[46] Digi International, "Can Digi's XBee ZB modules communicate with other manufacturer's zigbee modules?," 2022, https://www.digi.com/support/knowledge-base/can-digi-s-xbee-zb-modules-communicate-with-other.

[47] iPerf, "iPerf - the ultimate speed test tool for TCP, UDP and SCTP," 2022, https://iperf.fr/.

[48] M. Petrova, J. Riihijarvi, P. Mahonen, and S. Labella, "Performance study of IEEE 802.15. 4 using measurements and simulations," in *IEEE Wireless Communications and Networking Conference*, vol. 1, pp. 487–492, IEEE, 2006.