Securing ZigBee Communications against Constant Jamming Attack Using Neural Network

Hossein Pirayesh, Pedram Kheirkhah Sangdeh, and Huacheng Zeng, *Senior Member, IEEE,*

***Abstract*—ZigBee is a wireless communication technology that has been widely used to provide low-bandwidth wireless services for IoT applications such as building automation, medical data collection, and industrial equipment control. As ZigBee operates in the ISM radio frequency bands, it may suffer from unintentional interference from coexisting radio devices (e.g., WiFi and Bluetooth) and/or radio jamming attacks from malicious devices. Although many results have been produced to enhance ZigBee security, there is no technique that can secure ZigBee against jamming attack. In this paper, we propose a new ZigBee receiver by leveraging MIMO technology, which is capable of decoding its desired signal in the presence of constant jamming attack. The enabler is a learning-based jamming mitigation method, which can mitigate the unknown interference using an optimized neural network. We have built a prototype of our proposed ZigBee receiver on a wireless testbed. Experimental results show that it is capable of decoding its packets in the face of 20 dB stronger jamming. The proposed ZigBee receiver offers an average of 26.7 dB jamming mitigation capability compared to off-the-shelf ZigBee receivers.**

***Index Terms*—IoT communications, ZigBee networks, jamming and anti-jamming attack, physical-layer security**

I. Introduction

ZigBee is an IEEE 802.15.4-based specification for a suite of high-level communication protocols used to create wireless local area networks for home automation, industrial equipment control, medical data collection, and other low-bandwidth needs. It is typically used for low data rate applications, with a defined data rate of 250 kbps. Its transmission range varies from 10 to 20 meters, depending on output power and environmental characteristics. ZigBee operates in the industrial, scientific and medical (ISM) radio frequency bands. While other frequency bands are possible, most countries and regions in the world use 2.4 GHz for commercial ZigBee devices in indoor environments. With the rapid proliferation of Internet of Things (IoT) devices, ZigBee communications have become an important component of the telecommunication infrastructure in our society.

As ZigBee has been used for many crucial applications in real world, it is of great importance to secure ZigBee communications for reliable wireless connection. However, similar to other wireless technologies, ZigBee faces two challenges in practice. First, ZigBee devices share ISM radio frequency bands with other types of radio devices (e.g., WiFi and Bluetooth), and, therefore, suffer from unintentional interference from those coexisting devices. For example, a ZigBee device may suffer from interference from its co-located WiFi devices, and the interference may disrupt its communication. Second, due to the openness of wireless medium, ZigBee communications are vulnerable to radio jamming attacks. When a malicious device emits high-power jamming signal, all the ZigBee devices in its proximity will be unable to communicate.

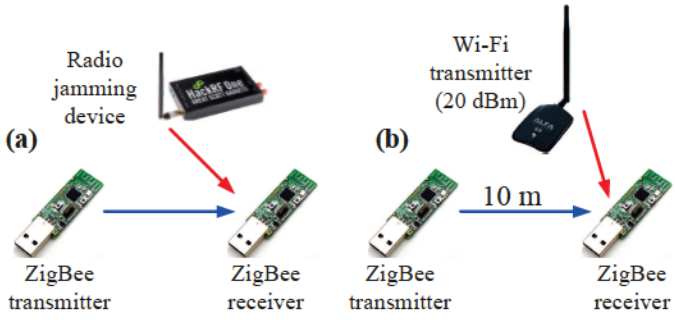


Fig. 1: Illustrating the vulnerability of ZigBee communications. (a) ZigBee is under jamming attack; (b) ZigBee is under cross-network interference.

One may think that ZigBee communications use spectrum spreading at the physical (PHY) layer and, therefore, a ZigBee receiver is resilient to intentional or unintentional interference. This perception is not correct. In ZigBee standard [1], the length of spectrum-spreading code sequence is 32 for every 4 bits. The jamming mitigation capability that it can offer is about $10\log_{10}(32/4) \approx 9$ dB, which is very limited. Fig. 1(a) shows a commercial ZigBee receiver in the face of a jamming device, which constantly sends 5 MHz noise-like interference. Our tests show that the ZigBee receiver frequently fails to decode its packets when its jamming-to-signal ratio (JSR) is greater than -1.6 dB. Fig. 1(b) shows a commercial ZigBee receiver in the proximity of a commercial off-the-shelf WiFi device[1] that is *constantly* sending WiFi data packets. Our tests show that, when their distance is less than 5 meters, the ZigBee receiver suffers from larger than 90% packet error rate.

Although many results have been produced to enhance ZigBee security, there is no solution that can secure ZigBee against jamming attacks. The existing results in this domain are either focused on the enhancing the effectiveness of

The authors are with the Department of Computer Science and Engineering, Michigan State University, East Lansing, MI 48824. Corresponding author: H. Zeng, Email: hzeng@cse.msu.edu.

This work was supported in part by NSF Grants CNS-1717840 and CNS-1846105.

[1]The WiFi device is an Alfa AWUS036NHA wireless USB adapter. We modified its firmware and driver in Linux to disable its carrier sense so that it can constantly send data packets at 20 dBm transmit power.

TABLE I: Related work on jamming and anti-jamming attacks in ZigBee communications.

Jamming attacks	[2], [3]	Survey on conventional (constant, noise, and reactive) and protocol-aware jamming attacks against ZigBee communications.
	[4]	Studied the performance of constant jamming attack in ZigBee communications.
	[5]	Implemented reactive jamming attack against ZigBee communications in real systems.
	[6]	Designed an energy depletion attack against ZigBee communications.
Anti-jamming techniques	[7]	Evaluated the performance of conventional DSSS interference and jamming signals.
	[8]	Presented randomized differential DSSS (RD-DSSS) scheme to secure ZigBee communications.
	[9], [10]	Proposed an anti-jamming scheme (called Dodge-Jam) based on channel hopping and frame segmentation.
	[11]	Proposed a MAC-layer anti-jamming scheme based on frame masking, channel hopping, packet fragmentation, and fragment replication.
	[12]	Designed a digital filter to reject the frequency components of periodically cycling jamming attacks.
	[13], [14]	Enabled ZigBee transmission by harnessing the reaction time of reactive jammer and using the unjammed time slots.
	[15]	Presented a method to detect the presence of jamming attacks by extracting statistics from jamming-free symbols of DSSS synchronizer.

jamming attacks [4], [5], [15] or limited to the interference cancellation for cooperative devices such as WiFi [16]–[18]. Little progress has been made so far in the design of practical solutions to secure ZigBee against jamming attacks. The lack of effective solutions underscores the critical needs and grand challenges in this task.

In this paper, we design a practical scheme to secure ZigBee communications against radio jamming attack (or unknown cross-network interference on ISM bands). The enabler is a new physical-layer design for a ZigBee receiver, making it capable of decoding its data packets in the presence of unknown interference. Our design relies on the assumption that a ZigBee device is equipped with two antennas. It leverages the spatial degrees of freedom (DoF) provided by its antennas to mitigate interference and decode its desired signal. One may argue that many ZigBee devices are powered by battery and, therefore, unsuited for multiple antennas. In fact, with the advancement of semiconductor and antenna technologies in the past decades, two antennas can be easily installed on a battery-powered ZigBee device. Moreover, many ZigBee-based IoT devices (e.g., electronic switches and industrial equipment) have sufficient power supply for their operations. Therefore, it is a mild assumption that a ZigBee device has two antennas in future IoT systems.

To decode ZigBee signal in the presence of unknown interference (jamming signal), we propose a learning-based method for jamming mitigation using a neural network at the physical layer. This neural network works as a linear spatial filter to suppress interference while not requiring any knowledge of the interference. A challenge in this method is the way of training the neural network so that it can decode the packets in real time. To address this challenge, we adopt a small-sized neural network that does not have hidden layers and optimize it by exploiting the inherent relationship of network weights to speed up the training process. ZigBee packet preamble (4 bytes or 32 bits) is then used to train the optimized neural network.

In addition to signal detection, another challenge in the design of jamming-resilient ZigBee receiver is time and frequency synchronization, where time synchronization is to search for the first chip of a packet and frequency synchronization is to compensate the frequency offsets. In the presence of interference, conventional correlation-based synchronization approach does not work. To address this challenge, we propose a projection-based approach for the synchronization component, which first projects received signals in the spatial domain and then employs the conventional approach to compensate the time and frequency offsets.

We have built a prototype of ZigBee receiver on a wireless testbed to validate our design in real-world wireless environments and evaluated its performance in the presence of a malicious device that emits different types of radio jamming signals. We placed the ZigBee transmitter, receiver, and jamming device at 20 different locations in a smart home environment. We examined three cases where a malicious radio attacker interferes with ZigBee receiver using WiFi-like, CDMA-like, or noise-like signal over full ZigBee spectrum. Experimental results show that our prototyped ZigBee receiver offers an addition of 26.7 dB (on average) jamming mitigation capability (JMC) in comparison with an off-the-shelf ZigBee receiver. The results suggest that our designed ZigBee receiver can successfully decode ZigBee packets even if jamming signal is 20 dB stronger than ZigBee signal.

This paper advances the state-of-the-art in the following aspects: i) We have proposed a learning-based jamming mitigation method using an optimized neural network, which is capable of decoding ZigBee signal in the presence of unknown interference. ii) Based on the learning-based jamming mitigation, we have designed a ZigBee receiver to decode its data packets in the face of malicious jamming attack. iii) We have built a prototype of our proposed ZigBee receiver and demonstrated its effectiveness in real-world wireless environments.

II. Related Work

We survey the prior research efforts in relevant to our work in the following three domains.

Jamming and Anti-jamming in ZigBee: While the security problems in Wi-Fi and cellular networks have received a large amount of research efforts and produced a large volume of research results (see, e.g., [19]–[24]), the security problems in ZigBee networks are highly overlooked. This stagnation is reflected by the lack of advances in the design of jamming-resistant ZigBee communications. Table I summarizes the prior work on jamming and anti-jamming attacks in ZigBee communications. Clearly, the existing anti-jamming schemes are limited to spectrum sharing (DSSS) technique. These schemes would not work when jamming signal is stronger than ZigBee signal at ZigBee receiver.

In contrast, our anti-jamming scheme takes advantage of recent advances in MIMO technology and renders much better ability of securing ZigBee communications in the presence of jamming attack.

Interference Cancellation in ZigBee Coexistence: Another research line related to this work is interference cancellation

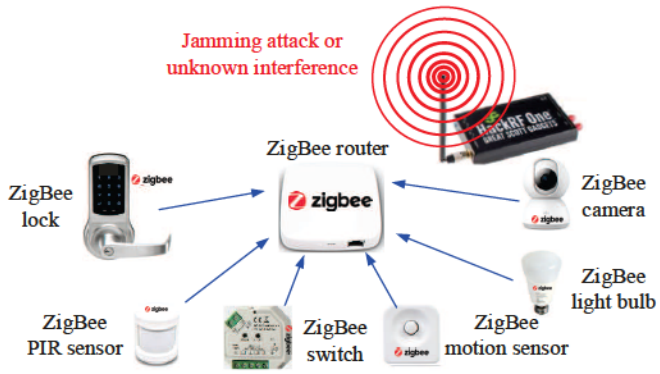


Fig. 2: ZigBee for device and appliance control in the face of jamming attacks or unknown interference.

TABLE II: The mapping from data bits to chip sequence [1].

Binary data ($b_0 b_1 b_2 b_3$)	Symbol value	Chip values ($c_0 c_1 c_2 \ldots c_{32}$)
0000	0	11011001110000110101001000101110
1000	1	11101101100111000011010100100010
0100	2	00101110110110011100001101010010
1100	3	00100011011011011001110000110101
0010	4	01010010000101110110110011000011
1010	5	00110101001000101110110110011100
1110	6	11000011010100100010111011011001
1110	7	10011100001101010010001011101101
0001	8	10001100100101100000011101111011
1001	9	10111000110010010110000001110111
0101	10	01111011000110010010110000000111
1101	11	01110111011100011001001011000000
0011	12	00000111011110111000110010010110
1011	13	01100000011101111011100011001001
0111	14	10010110000001110111101110001100
1111	15	11001001011000000111011110111000

in the coexistence of ZigBee. In [16] and [17], the authors proposed WizBee, a coexistence scheme of ZigBee and WiFi, where the ZigBee device has a single antenna. They assumed that Wi-Fi signal is about 5 to 20 dB stronger than ZigBee signal, and thus employs interference cancellation to mitigate WiFi signal for ZigBee signal detection. This method does not apply to jamming defense because the ZigBee receiver does not have knowledge about the jamming signal. In [18], the authors studied the vulnerability of ZigBee devices to interference from 802.11 devices and proposed a solution for minimizing interference from 802.11 in ZigBee medical sensors. However, the proposed solutions are limited at the MAC layer and unsuited for jamming defense.

Learning-based Interference Management: Recently, machine learning (ML) becomes popular for wireless networking design, and there are many research results on learning-based interference management [25]–[28]. For example, in [25], the authors studied blind interference alignment (BIA) in wireless networks and proposed two reinforcement learning algorithms for selecting the best antenna configuration for BIA. These works, however, are limited to analytical study. So far, we find no prior work that employs neural network for real-time interference mitigation.

III. Problem Description

A. Jamming Attack Model

We consider the ZigBee network, as shown in Fig. 2, where a ZigBee router serves one or multiple ZigBee devices. At one moment, the ZigBee router communicates with a single ZigBee user device. In this network, there is a malicious device that continuously emits jamming signal to disrupt the ZigBee communications, and we have the following assumptions on the jamming attack: i) The ZigBee devices have no knowledge about jamming signal, including its bandwidth, waveform, and frame format. ii) The bandwidth of jamming signal could be larger than, equal to, or less than the bandwidth of ZigBee signal. iii) The waveform of jamming signal may vary over time.

In real world, some ZigBee devices are not constrained by their physical size and their power consumption while playing a critical role in their applications. For example, many ZigBee-based electronic switches are connected to a main power supply and have a large size. These switches are widely used to control factory equipment and machines. In addition, ZigBee routers, which serve as the Internet gateway for ZigBee users as shown in Fig. 2, are not constrained by their physical size or power consumption. On such ZigBee devices, we can install multiple (two) antennas for radio signal transmission and reception.

Our objective is to secure the radio communications for the ZigBee devices, that have two or more antennas, against radio jamming attacks. Specifically, for the ZigBee devices that are equipped with two or more antennas, we design an efficient scheme to decode data packets in the presence of unknown interference, while not requiring any knowledge of interference.

B. Background of ZigBee Communications

Before presenting our design, we first offer a review of ZigBee PHY and MAC layers, which is essential for understanding of our new ZigBee receiver.

PHY-Layer Specs: ZigBee is based on IEEE 802.15.4 standard, which specifies operation in the unlicensed 2.4 to 2.4835 GHz (worldwide), 902 to 928 MHz (North America and Australia), and 868 to 868.6 MHz (Europe) ISM bands. Sixteen channels are allocated in the 2.4 GHz band. These channels are spaced 5 MHz apart, though using only 2 MHz of bandwidth. The radios use direct-sequence spread spectrum (DSSS) coding, and the spectrum-spreading code sequence comprises pre-defined 32 chips, as specified in Table II. For ZigBee devices working in the 2.4 GHz band, offset quadrature phase-shift keying (O-QPSK) is used. In O-QPSK, two chips are modulated onto the in-phase and q-phase carriers, and the over-the-air data rate is 250 kbps per channel. For indoor applications at 2.4 GHz, transmission distance ranges from 10 to 20 meters, depending on the construction materials, the number of walls to be penetrated, and the output power permitted in that geographical location.

MAC Protocols: The current IEEE 802.15.4 standards [29] support two types of networks: Beacon-enabled and non-beacon-enabled networks. In non-beacon-enabled networks, CSMA/CA is used for medium access control. In this type of

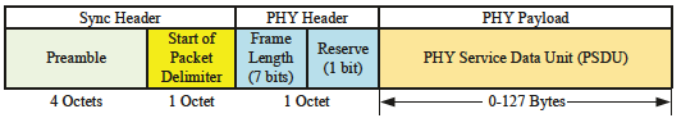


Fig. 3: The frame structure of ZigBee communications.

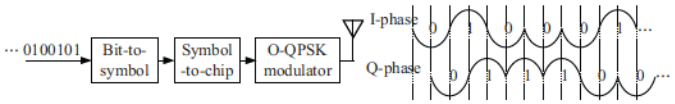


Fig. 4: The PHY-layer diagram of a conventional ZigBee transmitter and an example of O-QPSK waveform.

network, at least one ZigBee device keeps its radio receiver active, listening to possible packets from other ZigBee devices; while other ZigBee devices would remain asleep until they are commanded to transmit. The typical example of such a network is a wireless light switch controller: The ZigBee chipset inside a lamp may continuously receive signals, since it is connected to the main supply, while a battery-powered wireless remote controller would remain asleep until the switch is triggered. The remote controller then wakes up to send a command packet to the lamp, and returns to sleep after receiving an acknowledgment.

In beacon-enabled networks, the special network nodes called ZigBee routers transmit periodic beacons to announce their presence to the other nodes. Beacon intervals depend on data rate; they may range from 15.4 milliseconds to 251.6 seconds at 250 kbps. Nodes may sleep between beacons, thus lowering their duty cycle and prolonging their battery lifetime.

ZigBee Frame Structure: Fig. 3 shows the frame structure of a ZigBee data packet at the physical layer, which comprises three parts: Sync header, PHY header, and PHY payload. Particularly, a ZigBee frame has a preamble in its sync header, which consists of 4 pre-defined Octets (32 bits). The preamble is used by the ZigBee receivers to obtain chip and symbol synchronization for an incoming message. In the standards, the preamble is composed of 32 binary zeros. As we shall see, this preamble plays a key role in our design of jamming-resilient ZigBee receiver, which uses the preamble to train an optimized neural network for jamming mitigation.

ZigBee Transmitter Diagram: Fig. 4 shows the PHY-layer diagram of a conventional ZigBee transmitter and an example of generated O-QPSK signal. As shown in the figure, the bit-to-symbol module first groups every 4 bits as a symbol, with its value in the range from 0 to 15. Then, each of the resulting symbols is mapped to a sequence of predefined 32 chips, as specified in Table II. Finally, the sequence chips are O-QPSK modulated using half-sine pulse shaping filter, and the resulting I/Q signals are sent for radio frequency transmission.

ZigBee Receiver Diagram: Fig. 5 shows the diagram of a conventional ZigBee receiver. The RF front-end module first converts a radio signal to the corresponding baseband signal, followed by a module for energy detection. Then, the analog signal is converted to digital samples using 12× oversampling rate. A matched filter is used to suppress noise and 3× down-sample the digital signal. After that, frequency synchronization

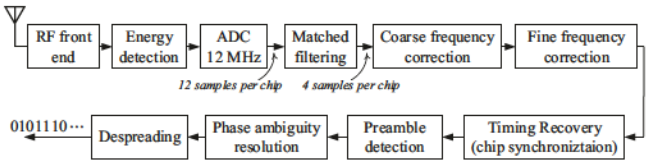


Fig. 5: The PHY-layer diagram of a conventional ZigBee receiver.

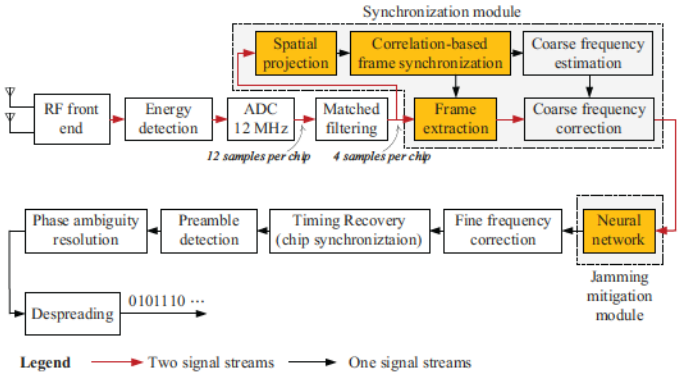


Fig. 6: The diagram of our proposed ZigBee receiver for decoding ZigBee packets in the face of jamming signal.

and timing recovery are performed to decode the chips, which are further used for symbol detection (preamble detection and phase ambiguity elimination). Finally, the decoded chips are despread to estimate the original chips. Similar to other wireless receivers, conventional ZigBee receivers are vulnerable to both jamming attacks and unknown interference.

IV. A New ZigBee Receiver Design

To enable ZigBee communication in the presence of jamming attack, we need a ZigBee receiver that is immune to unknown interference. In what follows, we first describe the basic idea of our design and then present its key components.

A. Basic Idea

The basic idea of our design is to install two antennas on a ZigBee device by leveraging the recent advances in semiconductor and antenna technologies. This is possible for many ZigBee devices that are not constrained by their physical size or power consumption (e.g., ZigBee hubs and ZigBee electronic switches). For a ZigBee device with two or more antennas, we design a new baseband signal processing pipeline to mitigate the jamming signal and recover ZigBee signal.

Fig. 6 shows the diagram of our proposed signal processing scheme for a ZigBee receiver. Compared to the conventional ZigBee receiver in Fig. 5, it has two new modules: Synchronization module and jamming mitigation module. Other modules remain the same as those in conventional ZigBee receiver. In what follows, we focus on these two new modules.

B. Synchronization Module

In the conventional ZigBee receiver, the sync module has two purposes: i) Estimate the carrier frequency offset and

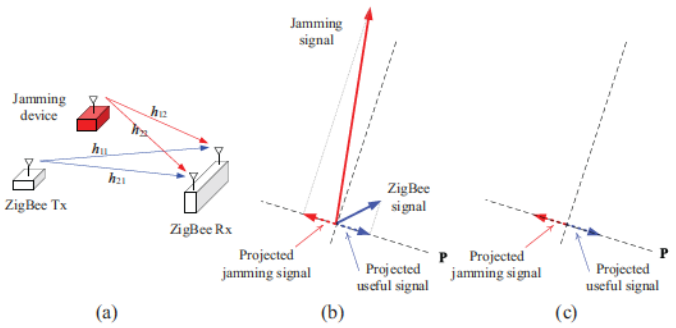


Fig. 7: Illustrating the basic idea of our synchronization method. (a) An example of toy-sized network consisting of a ZigBee transmitter, a ZigBee receiver, and high-power jammer. (b) Signal projection in the time domain at the ZigBee receiver, where projection filter $\mathbf{p}$ is a 2×1 complex vector. (c) Amplitudes of jamming and ZigBee signals after projection.

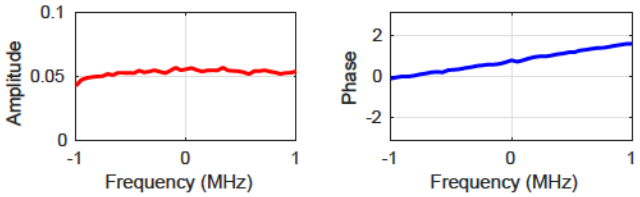
compensate the coarse frequency offset for the received signal; and ii) identify the beginning of a signal frame. To achieve these two purposes, the conventional method performs FFT operation to estimate the frequency offset and use correlation to estimate the time offset. This method, however, does not work for a ZigBee receiver in the face of unknown interference, necessitating a new sync method to estimate the frequency and time offset for the received signal.

To address this challenge, we propose a projection-based method for the alleviation of jamming signal in the spatial domain. Here, projection refers to a filtering operation on the two data streams using a linear spatial vector. Fig. 7 illustrates the basic idea of our method. Consider the network in Fig. 7(a), where a two-antenna ZigBee receiver suffers from jamming attacks. If the jamming signal is much stronger than the ZigBee signal, the frequency and timing offset cannot be accurately estimated at the ZigBee receiver and, as a result, the ZigBee signal cannot be decoded. To alleviate the jamming signal, we project the received signal to a spatial direction using a spatial filter $\mathbf{p}$, as shown in Fig. 7(b). If we can find a good projection direction (e.g., the one perpendicular to the jamming signal direction), then the jamming signal would be significantly weakened on the projection direction, as illustrated in Fig. 7(c).

Now, the question is how to find a good direction for signal projection. We resort to matrix decomposition, and it turns out that a singular vector of the received signals is an effective direction for jamming alleviation. Mathematically, denote $\mathbf{y}(n) \in \mathbb{C}^{2\times 1}$ as the input of the "signal projection" module in Fig. 6, and $y(n) \in \mathbb{C}$ as the output of this module. Then, we construct the projection filter by $\mathbf{p} = singularvector(\sum_{n=1}^{N_{\text{sync}}} \mathbf{y}(n)\mathbf{y}(n)^{\text{H}})$, where N_{sync} is the number of received signal samples for projection. It can be set empirically (e.g., 30). After constructing $\mathbf{p}$, we project the two signal streams by letting $y(n) = \mathbf{p}^{\text{H}}\mathbf{y}(n)$. For this synchronization module, we have the following lemma.

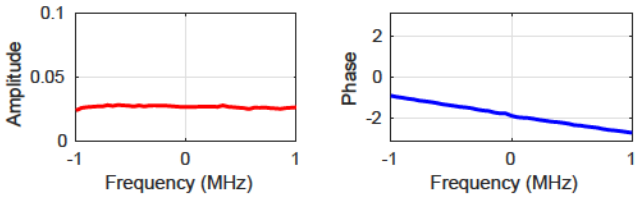
Lemma 1: If the wireless channels are frequency-flat[2] *and there is no noise, then the signal-to-jamming ratio (SJR) after signal projection is greater than or equal to 0 dB, regardless of the jamming signal power before the projection.*

[2]Frequency-flat wireless channel is a channel where all frequency components of a signal experience the same response.



(a) Channel amplitude. (b) Channel phase.

Fig. 8: An instance of measured line-of-sight wireless channel in ZigBee communication.



(a) Channel amplitude. (b) Channel phase.

Fig. 9: An instance of measured non-line-of-sight wireless channel in ZigBee communication.

The proof of this lemma is given in Appendix. Fig. 8 shows the measured wireless channel over 10 m line-of-sight (LoS) distance, and Fig. 9 shows the measured wireless channel over 10 m non-line-of-sight (NLoS) distance. We can see that the channels are relatively frequency-flat. Moreover, since ZigBee is for short-range communication, the noise is small in many scenarios. Therefore, we expect this projection-based method has a performance close to its theoretical limit in (1). It is noteworthy that the conventional sync method is resilient to the interference that has similar power as the signal (i.e., SJR is about 0 dB).

C. Jamming Mitigation Module

Following the signal processing pipeline in Fig. 6, after the compensation of coarse time and frequency offsets, the two signal streams are fed into a neural network, which is used to mitigate jamming signal for the recovery of the ZigBee signal. After the mitigation of jamming signal, the rest of the signal processing modules remain the same as those in the conventional ZigBee receiver as shown in Fig. 5. Then, the key question is how to design the neural network such that it can mitigate the jamming signal to the maximum extent while preserving the ZigBee signal. We address this question in the next section.

V. Learning-Based Jamming Mitigation

In this section, we present a learning-based method to mitigate the jamming signals. We first formulate the jamming mitigation problem as a mathematical problem and then propose a learning-based method for jamming mitigation.

A. Problem Formulation

While ZigBee channels are spaced 5 MHz, ZigBee signal bandwidth is about 2 MHz. Moreover, ZigBee is typically

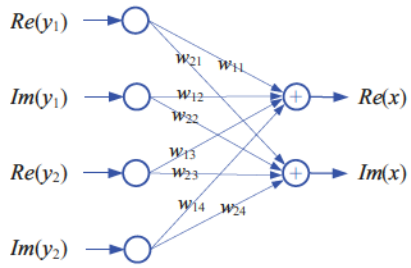


Fig. 10: A neural network for jamming mitigation.

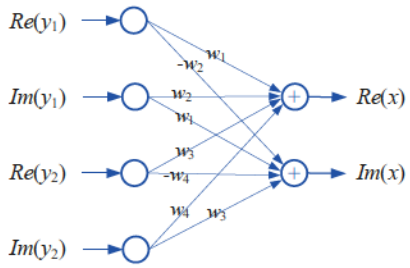


Fig. 11: A simplified neural network for jamming mitigation.

used for short-range communications. Therefore, we assume that the radio signals in ZigBee communications experience frequency-flat wireless channels. As shown in Fig. 8 and Fig. 9, wireless channels are pretty flat over frequency in both real-world LoS and NLoS scenarios.

Based on this assumption, we formulate the jamming mitigation problem as a mathematical problem. Denote $\mathbf{y}(n) \in \mathbb{C}^{2\times N}$ as the two input signal streams of the neural network module in Fig. 6, where N is the number of samples in a ZigBee frame as shown in Fig. 3. Denote $x(n) \in \mathbb{C}^{1\times N}$ as the transmitted ZigBee signal. Denote $z(n) \in \mathbb{C}^{1\times N}$ as the transmitted jamming signal. Then, the received signal $\mathbf{y}(n)$ can be expressed as:

$$\mathbf{y}(n) = \mathbf{h}_1 x(n) + \mathbf{h}_2 z(n) + w(n), \tag{1}$$

where $\mathbf{h}_1 = [h_{11} \quad h_{21}]^\mathsf{T}$ is the channel coefficients between ZigBee transmitter and ZigBee receiver, $\mathbf{h}_2 = [h_{12} \quad h_{22}]^\mathsf{T}$ is the channel coefficients between jamming device and ZigBee receiver, as shown in Fig. 7. $w(n)$ is the noise at the ZigBee receiver.

To mitigate jamming signal, we need to find a filter $\mathbf{g} = [g_1 \quad g_2] \in \mathbb{C}^{1\times 2}$ that can mitigate the jamming signal through properly combining the two signal streams. We intend to design filter satisfying the following requirements: $\mathbf{gh}_1 = 1$ and $\mathbf{gh}_2 = 0$. If we could obtain channel coefficients $\mathbf{h}_1$ and $\mathbf{h}_2$, then it is a trivial task to compute $\mathbf{g}$. After obtaining $\mathbf{g}$, we can mitigate the jamming signal by letting $\hat{x}(n) = \mathbf{gy}(n)$, where $\hat{x}(n)$ is the signal after jamming mitigation, (i.e., the output of the neural network module).

However, in real systems, due to the lack of knowledge about jamming signal, there is no solution that can estimate the channel coefficients in the presence of jamming signal, making it challenging to mitigate jamming signal.

B. Optimized Neural Network for Jamming Mitigation

Challenge and Setting: To mitigate jamming signal, we resort to a neural network to replace the spatial filter $\mathbf{g}$. A challenge in this method is that the neural network should work in real time to decode the ZigBee packets. In other words, the neural network should be capable of mitigating the jamming signal for each individual ZigBee packet. To address this challenge, we adopt a small-size neural network that does not have hidden layers as shown in Fig. 10. This neural network works with real numbers, where the input is the real and imaginary parts of two signal streams (i.e., $\mathbf{y}(n) = [y_1(n) \quad y_2(n)]$) and the output is the real and imaginary parts of one signal stream (i.e., $x(n)$). As neural network works with real numbers by nature, we decompose a complex number into two real numbers, with $Re(\cdot)$ and $Im(\cdot)$ being its real and imaginary parts.

Data for Training: This simple neural network is trained by each individual packet. To train this network, we use the preamble in the ZigBee frame. As shown in Fig. 3, a ZigBee frame has a preamble field, which comprises 4 pre-defined Octets (32 bits). For these 32 bits, every four are modulated to a spectrum-spreading code sequence of 32 chips. Therefore, the preamble of a ZigBee frame has 256 chips, which we use to train the neural network.

Neural Network Optimization: To realize real-time packet detection, we propose a scheme to speed up the training process. Our method takes advantage of the inherent relation of the network weights. Suppose that the noise is negligible. Then, we have

$$\begin{aligned}
\mathbf{gy} &= g_1 y_1 + g_2 y_2 \\
&= [Re(g_1) + iIm(g_1)][Re(y_1) + iIm(y_1)] \\
&\quad + [Re(g_2) + iIm(g_2)][Re(y_2) + iIm(y_2)] \\
&= \big[Re(g_1)Re(y_1) - Im(g_1)Im(y_1) \\
&\quad + Re(g_2)Re(y_2) - Im(g_2)Im(y_2)\big] \\
&\quad + i\big[Re(g_1)Im(y_1) + Im(g_1)Re(y_1) \\
&\quad + Re(g_2)Im(y_2) + Im(g_2)Re(y_2)\big].
\end{aligned} \tag{2}$$

Define four real numbers as follows: $w_1 = Re(g_1)$, $w_2 = -Im(g_1)$, $w_3 = Re(g_2)$, and $w_4 = -Im(g_2)$. Then, (2) can be written to

$$\begin{aligned}
\mathbf{gy} = &\underbrace{\big[w_1 Re(y_1) + w_2 Im(y_1) + w_3 Re(y_2) + w_4 Im(y_2)\big]}_{Re(x)} \\
&+ i\underbrace{\big[w_1 Im(y_1) - w_2 Re(y_1) + w_3 Im(y_2) - w_4 Re(y_2)\big]}_{Im(x)}.
\end{aligned} \tag{3}$$

Based on (3), the weights in the neural network in Fig. 10 can be re-written as those in Fig. 11. It is evident that the new neural network has only four weights, less than the number of weights in Fig. 10.

Training Method: When a ZigBee device receives a packet as shown in Fig. 3, it uses the packet preamble to train the neural network. Specifically, to train weights $\{w_1, w_2, w_3, w_4\}$ as shown in Fig. 11, we transform the network into that shown in Fig. 12. For this neural network, we have a total

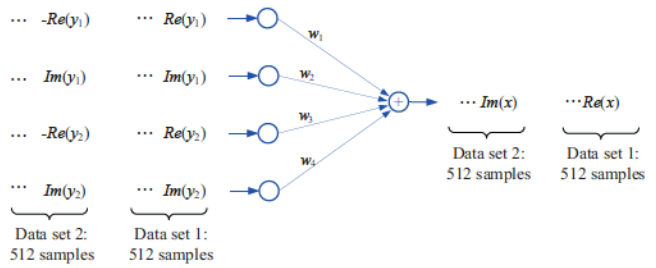


Fig. 12: An optimized neural network used for weight training.

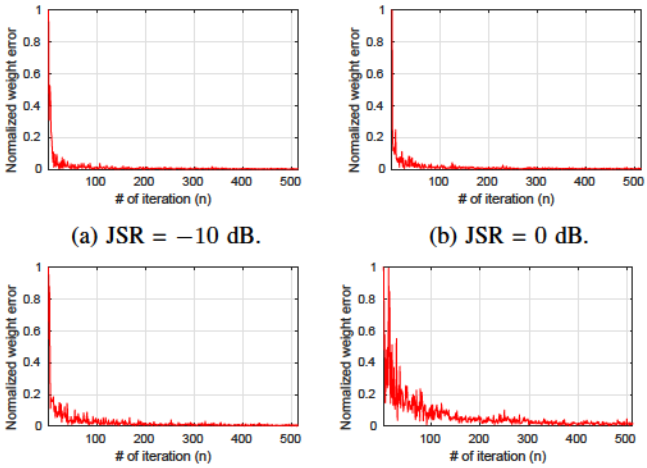
Algorithm 1 Neural network training process.

1: **Input:** Transmitted preamble $x(n)$ of a ZigBee packet, and received preamble $\mathbf{y}(n)$ of the ZigBee packet, $1 \leq n \leq 512$
2: **Output:** The weights of neural network $[w_1 \;\; w_2 \;\; w_3 \;\; w_4]$
3: Obtain $[Re(x(n)) \;\; Im(x(n))]$, $1 \leq n \leq 512$
4: Obtain $[Re(y_1(n)) \;\; Im(y_1(n)) \;\; Re(y_2(n)) \;\; Im(y_2(n))]$, $1 \leq n \leq 512$
5: **for** $1 \leq n \leq 512$ **do**
6: *// the nth iteration*
7: Train the neural network using the following data: $[Re(y_1(n)) \;\; Im(y_1(n)) \;\; Re(y_2(n)) \;\; Im(y_2(n))]$ for input and $Re(x(n))$ for output
8: Train the neural network using the following data: $[Im(y_1(n)) \;\; -Re(y_1(n)) \;\; Im(y_2(n)) \;\; -Re(y_2(n))]$ for input and $Im(x(n))$ for output
9: **end for**
10: Return $[w_1 \;\; w_2 \;\; w_3 \;\; w_4]$

of $128 \times 4 \times 2 = 1024$ samples to update its four weights, where 128 is the number of complex symbols in the preamble, 4 is oversampling rate, and 2 is the number of components in a complex number (real and imaginary). As shown in the figure, the first 512 samples correspond to the real part of the 256 chips in the frame preamble, and the second 512 samples correspond to the imaginary part of the 256 chips in the frame preamble.

Alg. 1 shows our training method for the neural network. In this algorithm, we use backpropagation to train the weights for the neural network and the squared error as neural network cost function. In the training process, we use an adaptive step size for the update of weights. Specifically, for the 512 samples in dataset 1 in Fig. 12, we update the weights as follows: $\{w_1, w_2, w_3, w_4\} \leftarrow \{w_1, w_2, w_3, w_4\} + \lambda(n)$ $[Re(y_1(n)) \;\; Im(y_1(n)) \;\; Re(y_2(n)) \;\; Im(y_2(n))][Re(x(n)) - Re(\tilde{x}(n))]$, where $\lambda(n)$ is the step size for the nth iteration and $Re(\tilde{x}(n))$ is the forward computation output of the nth iteration. For the 512 samples in dataset 2 in Fig. 12, we update the weights as follows: $\{w_1, w_2, w_3, w_4\} \leftarrow \{w_1, w_2, w_3, w_4\} + \lambda(n)[Im(y_1(n)) \;\; -Re(y_1(n)) \;\; Im(y_2(n)) \;\; -Re(y_2(n))][Im(x(n)) - Im(\tilde{x}(n))]$, where $Im(\tilde{x}(n))$ is the forward computation output of the nth iteration. In the nth iteration, we set $\lambda(n) = \frac{w_1^2+w_2^2+w_3^2+w_4^2}{10+n}$, $1 \leq n \leq 512$.

One may wonder why the preamble of each packet is



(a) JSR = −10 dB. (b) JSR = 0 dB.

(c) JSR = 10 dB. (d) JSR = 20 dB.

Fig. 13: Normalized weight errors over the number of training iterations in different JSR scenarios.

enough for the training of neural network. The reasons are actually twofold. First, the neural network is of small size. It does not have hidden layer, and it has only 4 weights to train. Given its small size, it can be envisaged that the training process converges fast over training samples. Second, as we detailed before, the preamble of each ZigBee packet has 512 independent data samples that we can use to train the neural network. This number is not small, and it is sufficient to train those 4 weights.

It is noteworthy that, different from conventional neural networks, which use a portion of data for training and the remainder for test, our neural network uses all the data (packet preamble) for training and does not have test phase. This is because our neural network is of very small size and required to be run in real time. In essence, it is a heuristic algorithm.

As shown in Alg. 1, the training involves 512 iterations, each of which has 8 multiplications and 10 additions in the forward calculation, as well as 21 multiplications and 12 additions in the backward calculation. Collectively, the training algorithm requires 14,848 multiplications and 11,264 additions. We note that, given the advances in semiconductor and battery technologies in the past decades, the training algorithm can be easily carried out by a battery-powered ZigBee device. Hence, the power consumption of our proposed ZigBee receiver should not be an issue in practice. We also note that the new design of our proposed ZigBee receiver lies at the physical layer, which will produce no impact on the topology of a ZigBee network.

Jamming Mitigation: With the weights $\{w_1, w_2, w_3, w_4\}$ from the neural network, we use them to construct the spatial filter $\mathbf{g} = [w_1 - iw_2 \;\; w_3 - iw_4]$. Then, the jamming mitigation is conducted by $\hat{x}(n) = \mathbf{g}\mathbf{y}(n)$, where $\hat{x}(n)$ is the output of the neural network module in Fig. 6. As shown in Fig. 6, output signal stream $\hat{x}(n)$ is sent to the fine frequency correction module, timing recovery module, preamble detection module, phase ambiguity module, and despreading module. These modules are identical to those in conventional ZigBee receivers, as shown in Fig. 5.

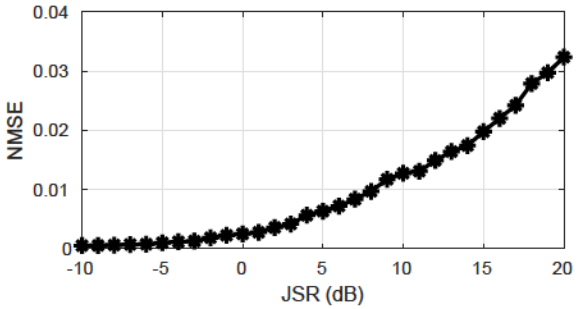
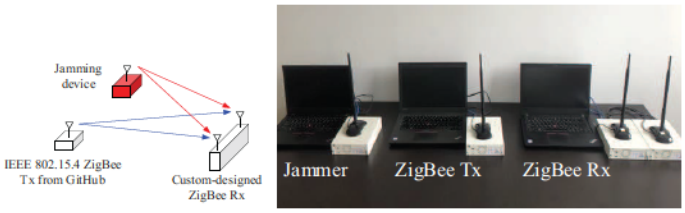


Fig. 14: Normalized mean square error (NMSE) of decoded signal in the presence of jamming attack when using the proposed neural network for signal detection.



(a) Network setting. (b) Network devices.

Fig. 15: Network setting and devices used in our experiments.

C. Performance Analysis

In what follows, we study the performance of this learning-based jamming mitigation in the scenarios without noise. For its performance in realistic noisy scenarios, we resort to experimental evaluation, as presented in Section VI.

Convergence: We first study the convergence of the neural network by observing the fluctuation of its weights. Specifically, we define the normalized weight error as follows:

$$error = \sqrt{\frac{\sum_{i=1}^{4}[w_i(n) - w_i(n-1)]^2}{\sum_{i=1}^{4} w_i(n)^2}}, \tag{4}$$

where n is the number of training iterations in Alg. 1. Based on this definition, we implement this neural network and observe its weights over training iterations in a case study. Fig. 13 shows the normalized weight error over the number of training iterations in different JSR scenarios. It is evident that the weights converge quickly. With 512 samples for training, the fluctuation of weight errors is limited 0.1% when JSR is -10 dB, 0.1% when JSR is 0 dB, 0.9% when JSR is 10 dB, and 1.7% when JSR is 20 dB.

Learning-based Signal Detection: We now study the performance of the neural network in signal detection using extensive simulation. Denote x as the original symbol at ZigBee Tx. Denote $\hat{x}$ as the estimated symbol in the presence of jamming signal at ZigBee Rx. We define normalized mean square error (NMSE) as $\text{NMSE} = (\mathbb{E}|x - \hat{x}|^2)/(\mathbb{E}|x|^2)$. Our simulation results show that the NMSE is less than 4% when JSR is 20 dB. This means that the proposed learning-based method can decode ZigBee packet in zero-noise scenarios even if jamming signal is 20 dB stronger than ZigBee signal.

VI. Experimental Evaluation

A. Implementation and Experimental Settings

We built a prototype of the ZigBee communication network, as shown in Fig. 15, to evaluate the proposed ZigBee receiver.

ZigBee Transmitter: We built the ZigBee transmitter using an USRP N210 device [30] and a laptop with GNURadio software package [31]. We have used the IEEE 802.15.4 ZigBee open-source code from GitHub [32] to implement the ZigBee transmitter. The open-source ZigBee code employs the PHY protocols as that of commercial off-the-shelf ZigBee transmitters. The frame structure in Fig. 3 is used for data transmission, where the length of PHY Service Data Unit (PSDU) is 32 bytes. We have run the ZigBee transmitter using O-QPSK modulation with over-the-air bit rate of 250 kbps. The carrier frequency is 2.48 GHz, and the sampling rate is 12 MHz. The transmit power of this ZigBee transmitter was set 13 dBm.

ZigBee Receiver: We have implemented two types of ZigBee receiver. i) Conventional single-antenna ZigBee device: For this ZigBee receiver, we implemented it by installing the IEEE 802.15.4 ZigBee open-source code from GitHub [32] on an USRP N210 device. ii) Our prototype of two-antenna ZigBee receiver: We built this ZigBee receiver using two USRP N210 devices, which were connected through a MIMO cable, as shown in Fig. 15(b). These two USRP N210 devices were connected to a laptop, on which we implemented our design shown in Fig. 6.

Radio Jamming Device: We have built a radio jamming device using a USRP device and GNURadio software package. The jamming device was able to employ three types of waveforms as follows:

- **WiFi-like Jamming:** We use the legacy WiFi frame consisting of 4 OFDM symbols as preamble and 16 OFDM symbols as random payload. The total number of subcarriers are 64, and 52 subcarriers are used to carry payload. The effective bandwidth is about 4.1 MHz, and the symbol duration is 16 μs (12.8 μs OFDM symbol prepended by a 3.2 μs cyclic prefix).
- **CDMA-like Jamming:** A random bit stream is constantly modulated onto the carrier frequency using QPSK modulation and rectangular I/Q pulse shaping filters. The effective bandwidth is 5 MHz.
- **Noise-like Jamming:** A zero-mean complex Gaussian signal is modulated onto the carrier frequency. The symbol duration is 0.2 μs, and the effective bandwidth is 5 MHz.

The transmit power of the jamming device was set to 20 dBm, and its bandwidth was set to 5 MHz. We note that, since the bandwidth of jamming signal is larger than that of ZigBee signal, this bandwidth is sufficient for jamming attack. In real systems, any out-of-band jamming signal will be filtered out by ZigBee device's RF filter and produce no impact on ZigBee device.

Experimental Settings: Fig. 16 shows the testbed settings of our experiments. The ZigBee receiver was placed on an

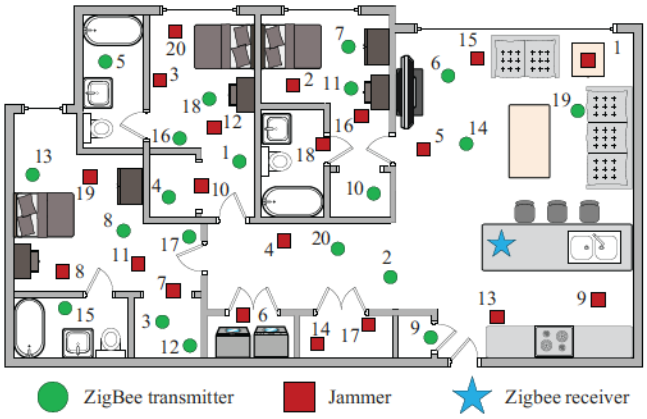


Fig. 16: Floor plan of our experimentation.

office desk, as marked a blue star in the figure. For ease of experimentation, the ZigBee receiver was stationary without movement throughout our experiments. This setting could be justified by real-world ZigBee applications, where most of ZigBee Hubs are placed at a fixed spot to provide services. The ZigBee transmitter was placed at one of the 20 locations marked green circles in the figure, and the radio jamming device was placed at one of the 20 locations marked red boxes. These 20 green/red boxes were randomly selected on the floor to cover the whole home area. The settings of each individual devices in our experiments were specified previously.

B. Performance Metrics

We evaluate the performance of the ZigBee receiver using the following four metrics:

Jamming-to-Signal Ratio (JSR): Focusing on the radio signal received by the ZigBee receiver before jamming mitigation, we define JSR as

$$\text{JSR} = 10\log_{10}\left(\frac{\sum_{n=1}^{N_m}|\mathbf{y}_j(n)|^2}{\sum_{n=1}^{N_m}|\mathbf{y}_s(n)|^2}\right), \tag{5}$$

where $\mathbf{y}_j(n)$ is the received jamming signal at the ZigBee receiver when ZigBee transmitter has been turned off, $\mathbf{y}_s(n)$ is the received ZigBee signal at the ZigBee receiver when jamming device has been turned off, and N_m is the number of measured signal samples (e.g., $N_m = 2000$).

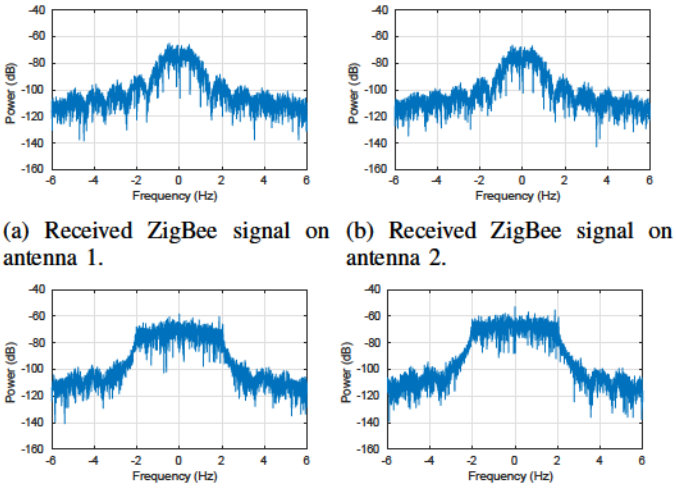
Error Vector Magnitude (EVM): Focusing on the signal at the ZigBee receiver after jamming mitigation, we define EVM as

$$\text{EVM} = 10\log_{10}\left(\frac{\sum_{n=1}^{N_c}\left|x(n)-\hat{x}(n)\right|^2}{\sum_{n=1}^{N_c}\left|x(n)\right|^2}\right), \tag{6}$$

where $x(n)$ is the original chips at the ZigBee transmitter, $\hat{x}(n)$ is the estimated chips at the ZigBee receiver, and N_c is the number of chips.

Packet Reception Rate (PRR): PRR is defined as the ratio of successfully decoded packets per total transmitted packets.

Jamming Mitigation Capability (JMC): Based on the measured JSR and EVM, we define JMC as the gap between JSR and EVM, i.e., JMC = JSR − EVM.



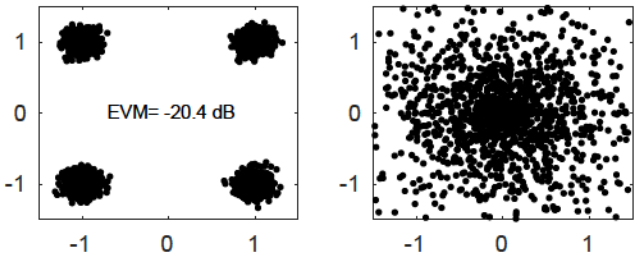
(a) Received ZigBee signal on antenna 1.

(b) Received ZigBee signal on antenna 2.

(c) Received ZigBee and jamming signals on antenna 1.

(d) Received ZigBee and jamming signals on antenna 2.

Fig. 17: The power spectrum of received signals on the ZigBee receiver's two antennas with and without jamming signal.



(a) Signal decoded by the proposed ZigBee receiver.

(b) Signal decoded by the conventional ZigBee receiver.

Fig. 18: Our proposed ZigBee receiver versus the conventional ZigBee receiver.

C. A Case Study

To evaluate the performance of the designed ZigBee receiver, we consider the case where the ZigBee transmitter is placed at location 1 (small green circle) and the jamming device is placed at location 1 (small red square) in Fig. 16. The jamming device emits WiFi-like jamming signal to disrupt ZigBee communications. We first study the performance of proposed ZigBee receiver at the designated location. Fig. 17(a) and (b) show the received power spectrum for ZigBee signal in the absence of jamming signal, and Fig. 17(c) and (d) show the received power spectrum for ZigBee and jamming signals at the ZigBee receiver. It is easy to see that the jamming signal is stronger than the ZigBee signal. According to (5), the measured JSR is 9.6 dB in this case.

We then process the received ZigBee and jamming signals using our proposed scheme in Fig. 6. Fig. 18(a) shows the constellation of the ZigBee signal (without despreading) decoded by our proposed ZigBee receiver. We can see that it can successfully decode the ZigBee packet in the presence of jamming attack. EVM of the decoded ZigBee signal is −20.4 dB. This means that the jamming mitigation capability of our design is 30.0 dB.

TABLE III: Empirical PRR of our proposed and conventional ZigBee receivers.

Location index	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Conventional receiver	0	0.6173	0.6174	0	0	0.6173	0	0	0	0.1756	0.6922	0.1755	0	0.9506	0	0	0	0	0.6168	0.9009
Proposed receiver	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

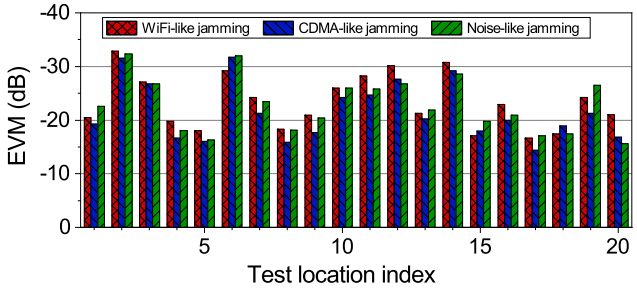


Fig. 19: Measured EVM of our proposed ZigBee receiver.

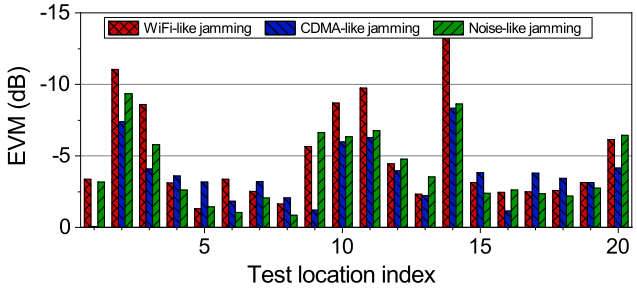


Fig. 20: Measured EVM of conventional ZigBee receiver.

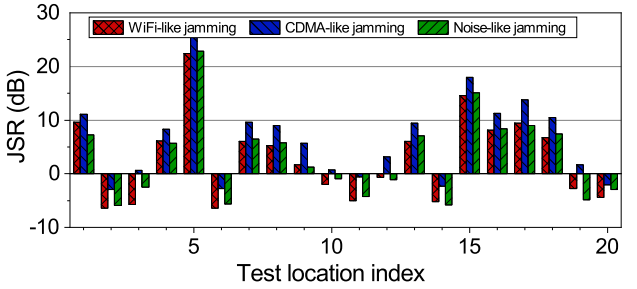


Fig. 21: Measured JSR at our proposed ZigBee receiver.

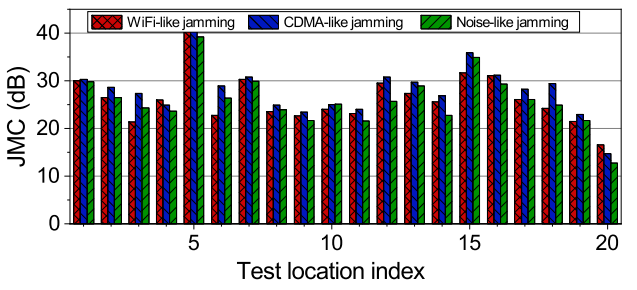


Fig. 22: The JMC of the proposed ZigBee receiver in comparison with an off-the-shelf ZigBee receiver.

In contrast, Fig. 18(a) shows the constellation of the ZigBee signal decoded by conventional ZigBee receiver. It is evident that a conventional ZigBee receiver fails to decode its desired data packet in the presence of jamming attack.

D. Extensive Results

We measure the performance of the proposed ZigBee receiver and the conventional ZigBee receiver at other 19 locations in the same building as shown in Fig. 16. We consider three jamming waveforms: WiFi-like, CDMA-like, and noise-like signals. We report our measured experimental results as follows.

EVM: Fig. 19 shows the measured EVM of our proposed ZigBee receiver when it is placed at the designated locations to decode the ZigBee signals in the face of jamming signals. We can see that for all the locations, the achieved EVM of our proposed ZigBee receiver ranges from -32.9 dB to -14.4 dB, with an average of -22.6 dB. As a comparison, we place a conventional ZigBee receiver at the same locations to decode the ZigBee signals in the presence of jamming signals. Fig. 20 shows our measured results. It is evident that our proposed ZigBee receiver significantly outperforms conventional ZigBee receiver, with an average EVM gain of 18.6 dB.

PRR: Based on the measured EVM, we calculate the average PRR at each location. Table III shows our results. We can see that the proposed ZigBee receiver achieves 100% PRR for all 20 locations, while the conventional receiver achieves 26.8% PRR on average.

JSR: To scrutinize the performance of our proposed ZigBee receiver, we measure its JSR according to (5). Fig. 21 shows our measured results. We can see that the measured JSR covers a highly dynamic range from -6 dB to 25.9 dB. Particularly, at location 5, the JSR is 25.9 dB, and its EVM is -16.0 dB. It means that the receiver achieves 41.9 dB JMC.

JMC: Based on the measured JSR and EVM, we calculate the JMC achieved by our proposed ZigBee receiver. Fig. 22 shows our results. The achieved JMC ranges from 21.0 dB to 41.9 dB, and the average of JMC at all the 20 locations is 26.7 dB.

VII. Conclusion

In this paper, we proposed a jamming-resistant ZigBee receiver by leveraging recent advances in multi-antenna technology. The new ZigBee receiver is capable of decoding ZigBee packets in the presence of jamming signals. The key components of our design are a signal-projection-based sync module and a neural-network-based jamming mitigation module. To speed up its training process, we optimized the neural network by taking advantage of the inherent relations of its weights and used the preamble (256 chips) in each individual ZigBee packet for its training. We have built a prototype of our proposed ZigBee receiver and evaluated its performance in

real-world wireless environments. Experimental results show that our design can salvage ZigBee communications in the presence of jamming signals 20 dB stronger than ZigBee signals and that our design can offer 26.7 dB jamming mitigation capability on average.

APPENDIX

Based on our assumption of zero-noise, (1) can be written as $\mathbf{y} = \mathbf{h}_1 x(n) + \mathbf{h}_2 z(n)$. We assume that $\mathbb{E}[|x(n)|^2] = 1$ and $\mathbb{E}[|z(n)|^2] = 1$. The ZigBee and jamming signal power is expressed by their channels ($\mathbf{h}_1$ and $\mathbf{h}_2$). Let $\mathbf{p} = \mathbf{u}_1^{\mathsf{H}}$, where $\mathbf{u}_1$ is a column of $\mathbf{u}$ and $[\mathbf{u}\ \ \mathbf{d}\ \ \mathbf{v}] = svd\big(\sum_{n=1}^{N_{\text{sync}}} \mathbf{y}(n)\mathbf{y}(n)^{\mathsf{H}}\big)$. Without loss generality, we assume $|v_{11}| \geq |v_{21}|$ for $\mathbf{v} = \begin{bmatrix} v_{11} & v_{12} \\ v_{21} & v_{22} \end{bmatrix}$. At the ZigBee receiver, we use $\mathbf{p}$ as the projection filter for signal projection. The projected signal can be written as:

$$\begin{aligned}
\mathbf{py} &= \mathbf{u}_1^{\mathsf{H}}\mathbf{udv}^{\mathsf{H}}[x(n)\ \ z(n)]^{\mathsf{T}} \\
&= \mathbf{u}_1^{\mathsf{H}}[\mathbf{u}_1\ \ \mathbf{u}_2]\begin{bmatrix} d_1 & 0 \\ 0 & d_2 \end{bmatrix}\begin{bmatrix} v_{11} & v_{12} \\ v_{21} & v_{22} \end{bmatrix}^{\mathsf{H}}[x(n)\ \ z(n)]^{\mathsf{T}} \\
&= [1\ \ 0]\begin{bmatrix} d_1 & 0 \\ 0 & d_2 \end{bmatrix}\begin{bmatrix} v_{11} & v_{12} \\ v_{21} & v_{22} \end{bmatrix}^{\mathsf{H}}[x(n)\ \ z(n)]^{\mathsf{T}} \\
&= [d_1\ \ 0]\begin{bmatrix} v_{11} & v_{12} \\ v_{21} & v_{22} \end{bmatrix}^{\mathsf{H}}[x(n)\ \ z(n)]^{\mathsf{T}} \\
&= d_1[v_{11}^*\ \ v_{21}^*][x(n)\ \ z(n)]^{\mathsf{T}} \\
&= d_1[v_{11}^* x(n) + v_{21}^* z(n)]. \qquad (7)
\end{aligned}$$

Based on (7), the SJR of the sigal after projection can be written as $\frac{|v_{11}^* x(n)|^2}{|v_{21}^* z(n)|^2}$. Given that $|v_{11}| \geq |v_{21}|$ and $\mathbb{E}[x(n)]$ and $\mathbb{E}[z(n)]$, we have the SJR of $\mathbf{py}$ is greater than or equal to 1. This completes the proof.

REFERENCES

[1] IEEE 802 Working Group, "IEEE standard for local and metropolitan area networks–part 15.4: Low-rate wireless personal area networks (LR-WPANs)," *IEEE Std*, vol. 802, pp. 4–2011, 2011.

[2] Y. M. Amin and A. T. Abdel-Hamid, "A comprehensive taxonomy and analysis of IEEE 802.15.4 attacks," *Journal of Electrical and Computer Engineering*, vol. 2016, 2016.

[3] A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos, and G. Pantziou, "A survey on jamming attacks and countermeasures in WSNs," *IEEE Communications Surveys & Tutorials*, vol. 11, no. 4, pp. 42–56, 2009.

[4] J. Rewienski, M. Groth, L. Kulas, and K. Nyka, "Investigation of continuous wave jamming in an IEEE 802.15.4 network," in *Proceedings of International Microwave and Radar Conference (MIKON)*, pp. 242–246, 2018.

[5] M. Wilhelm, I. Martinovic, J. B. Schmitt, and V. Lenders, "Short paper: Reactive jamming in wireless networks: how realistic is the threat?," in *Proceedings of the fourth ACM conference on Wireless network security*, pp. 47–52, 2011.

[6] X. Cao, D. M. Shila, Y. Cheng, Z. Yang, Y. Zhou, and J. Chen, "Ghost-in-ZigBee: Energy depletion attack on ZigBee-based wireless networks," *IEEE Internet of Things Journal*, vol. 3, no. 5, pp. 816–829, 2016.

[7] S. Fang, S. Berber, A. Swain, and S. U. Rehman, "A study on DSSS transceivers using OQPSK modulation by IEEE 802.15.4 in AWGN and flat Rayleigh fading channels," in *TENCON IEEE Region 10 Conference*, pp. 1347–1351, 2010.

[8] Y. Liu, P. Ning, H. Dai, and A. Liu, "Randomized differential DSSS: Jamming-resistant wireless broadcast communication," in *Proceedings of IEEE INFOCOM*, pp. 1–9, 2010.

[9] J. Heo, J.-J. Kim, S. Bahk, and J. Paek, "Dodge-jam: Anti-jamming technique for low-power and lossy wireless networks," in *Proceedings of IEEE International Conference on Sensing, Communication, and Networking (SECON)*, pp. 1–9, 2017.

[10] J. Heo, J.-J. Kim, J. Paek, and S. Bahk, "Mitigating stealthy jamming attacks in low-power and lossy wireless networks," *Journal of Communications and Networks*, vol. 20, no. 2, pp. 219–230, 2018.

[11] A. D. Wood, J. A. Stankovic, and G. Zhou, "DEEJAM: Defeating energy-efficient jamming in IEEE 802.15.4-based wireless networks," in *IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks*, pp. 60–69, 2007.

[12] B. DeBruhl and P. Tague, "Digital filter design for jamming mitigation in 802.15.4 communication," in *Proceedings of IEEE International Conference on Computer Communications and Networks (ICCCN)*, pp. 1–6, 2011.

[13] Y. Liu and P. Ning, "Bittrickle: Defending against broadband and high-power reactive jamming attacks," in *Proceedings of IEEE INFOCOM*, pp. 909–917, 2012.

[14] S. Fang, Y. Liu, and P. Ning, "Wireless communications under broadband reactive jamming attacks," *IEEE Transactions on Dependable and Secure Computing*, vol. 13, no. 3, pp. 394–408, 2015.

[15] M. Spuhler, D. Giustiniano, V. Lenders, M. Wilhelm, and J. B. Schmitt, "Detection of reactive jamming in DSSS-based wireless communications," *IEEE Transactions on Wireless Communications*, vol. 13, no. 3, pp. 1593–1603, 2014.

[16] P. Yang, Y. Yan, X.-Y. Li, Y. Zhang, Y. Tao, and L. You, "Taming cross-technology interference for Wi-Fi and ZigBee coexistence networks," *IEEE Transactions on Mobile Computing*, vol. 15, no. 4, pp. 1009–1021, 2015.

[17] Y. Yan, P. Yang, X.-Y. Li, Y. Zhang, J. Lu, L. You, J. Wang, J. Han, and Y. Xiong, "Wizbee: Wise ZigBee coexistence via interference cancellation with single antenna," *IEEE Transactions on Mobile Computing*, vol. 14, no. 12, pp. 2590–2603, 2014.

[18] 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.

[19] K. Pelechrinis, I. Broustis, S. V. Krishnamurthy, and C. Gkantsidis, "A measurement-driven anti-jamming system for 802.11 networks," *IEEE/ACM Transactions on Networking*, vol. 19, no. 4, pp. 1208–1222, 2011.

[20] H. Zeng, C. Cao, H. Li, and Q. Yan, "Enabling jamming-resistant communications in wireless MIMO networks," in *Proceedings of IEEE Conference on Communications and Network Security (CNS)*, pp. 1–9, 2017.

[21] Q. Yan, H. Zeng, T. Jiang, M. Li, W. Lou, and Y. T. Hou, "Jamming resilient communication using MIMO interference cancellation," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 7, pp. 1486–1499, 2016.

[22] F. M. Aziz, J. S. Shamma, and G. L. Stüber, "Resilience of LTE networks against smart jamming attacks," in *Proceedings of IEEE Global Communications Conference*, pp. 734–739, 2014.

[23] M. Lichtman, R. P. Jover, M. Labib, R. Rao, V. Marojevic, and J. H. Reed, "LTE/LTE-A jamming, spoofing, and sniffing: threat assessment and mitigation," *IEEE Communications Magazine*, vol. 54, no. 4, pp. 54–61, 2016.

[24] T. T. Do, E. Björnson, E. G. Larsson, and S. M. Razavizadeh, "Jamming-resistant receivers for the massive MIMO uplink," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 1, pp. 210–223, 2017.

[25] S. Begashaw, D. H. Nguyen, and K. R. Dandekar, "Enhancing blind interference alignment with reinforcement learning," in *Proceedings of IEEE Global Communications Conference (GLOBECOM)*, pp. 1–7, 2016.

[26] A. Toma, T. Nawaz, Y. Gao, L. Marcenaro, and C. S. Regazzoni, "Interference mitigation in wideband radios using spectrum correlation and neural network," *IET Communications*, vol. 13, no. 10, pp. 1336–1347, 2019.

[27] Y. He, Z. Zhang, F. R. Yu, N. Zhao, H. Yin, V. C. Leung, and Y. Zhang, "Deep-reinforcement-learning-based optimization for cache-enabled opportunistic interference alignment wireless networks," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 11, pp. 10433–10445, 2017.

[28] L. Li, Y. Xu, Z. Zhang, J. Yin, W. Chen, and Z. Han, "A prediction-based charging policy and interference mitigation approach in the wireless powered Internet of Things," *IEEE Journal on Selected Areas in Communications*, vol. 37, no. 2, pp. 439–451, 2018.

[29] S. Farahani, *ZigBee wireless networks and transceivers*. Amsterdam, The Netherlands: Newnes, 2011.

[30] Ettus Research, "USRP N210," *www.ettus.com/product/details/UN210-KIT [Online; Accessed 5-February-2020]*.
[31] E. Blossom, "GNURadio: tools for exploring the radio frequency spectrum," *Linux journal*, vol. 2004, no. 122, p. 4, 2004.
[32] T. Schmid, "GNU Radio 802.15. 4 en-and decoding," UCLA NESL, Los Angeles, CA, Tech. Rep., 2006.