Countering Cross-technology Jamming Attack

Zicheng Chi*, Yan Li*, Xin Liu*, Wei Wang*, Yao Yao*, Ting Zhu*, and Yanchao Zhang§
{zicheng1,liy1,xinliu1,ax29092,yaoyaoumbc,zt}@umbc.edu,yczhang@asu.edu
*University of Maryland, Baltimore County
§Arizona State University

ABSTRACT

Internet-of-things (IoT) devices are sharing the radio frequency band (e.g., 2.4 GHz ISM band). The exponentially increasing number of IoT devices introduces potential security issues at the gateway in IoT networks. In this paper, we introduce a set of new attacks through concealed jamming – an adversary pretends to be (or compromises) a legitimate WiFi device, then sends out WiFi packets to prevent ZigBee devices' communication or collide with ZigBee's packets. By doing this, concealed jamming has the potential to severely delay the reception of ZigBee packets that may contain important information (e.g., critical health data from wearables, fire alarms, and intrusion alarms). To defend against these attacks, we designed a novel ZigBee data extraction technique that can recover ZigBee data from the ZigBee packets that were collided with WiFi packets. We extensively evaluated our design in different real-world settings. The results show that ZigBee devices (protected by our proposed methods) achieve similar performance as those that are not under the concealed jamming attack. Moreover, compared with unprotected devices, their throughput is more than 15 times higher than the unprotected one that is under concealed jamming attacks.

CCS CONCEPTS

• **Security and privacy → Mobile and wireless security**.

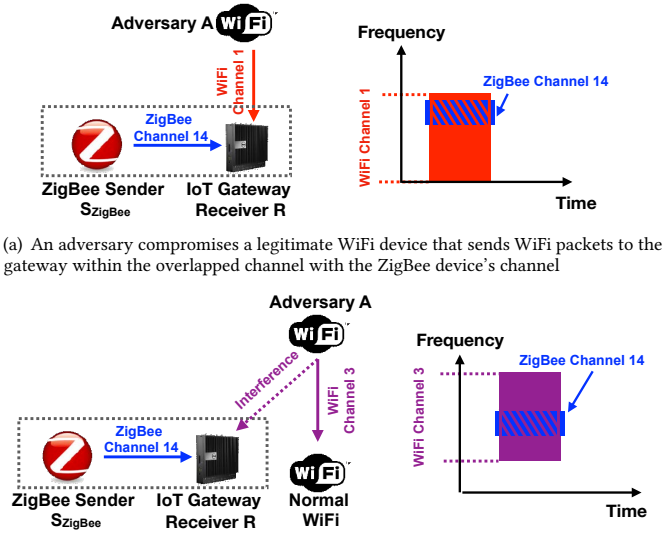
KEYWORDS

wireless networks, security, denial of service attack

ACM Reference Format:
Zicheng Chi*, Yan Li*, Xin Liu*, Wei Wang*, Yao Yao*, Ting Zhu*, and Yanchao Zhang§. 2020. Countering Cross-technology Jamming Attack. In *13th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '20), July 8–10, 2020, Linz (Virtual Event), Austria.* ACM, New York, NY, USA, 12 pages. https://doi.org/10.1145/3395351.3399367

1 INTRODUCTION

Internet-of-thing (IoT) devices have been increasingly used to support smart home, smart health, and smart cities applications. It is expected that the number of IoT devices will be increased exponentially and reach 20 billion by 2020 [3]. Most of these IoT devices are sharing the unlicensed spectrum (e.g., ISM band). The exponentially increasing number of IoT devices introduces potential security issues in IoT networks.



(a) An adversary compromises a legitimate WiFi device that sends WiFi packets to the gateway within the overlapped channel with the ZigBee device's channel

(b) An adversary smartly jams ZigBee device's communication to the gateway by pretending to be a legitimate WiFi device that sends WiFi packets to another WiFi receiver.

Figure 1: Concealed jamming in different network topology

In this paper, we introduce a set of new attacks through concealed jamming, which is illustrated in Figure 1, an adversary pretends to be (or compromises) a legitimate WiFi device, then sends out WiFi packets to the gateway, which i) prevent ZigBee devices' communication to the gateway; or ii) collide with ZigBee's packets. By doing this, concealed jamming has the potential to severely delay the gateway from receiving ZigBee packets that may contain important information (e.g., critical health data from wearables [5, 13, 29, 45], fire alarms from smoke and carbon monoxide detectors, and intrusion alarms from door/window or motion sensors). Given the significantly increasing number of ZigBee devices used in our daily lives (for example, Amazon echo plus and Samsung SmartThings hub contain ZigBee radios to receive the sensing data and control appliances in smart homes), concealed jamming is becoming more and more serious and can cause the malfunction of appliances.

Compared with a designated jammer, using or compromising a commercial off-the-shelf (COTS) WiFi device for jamming is much easier because i) a concealed jamming device can be easily built by hacking a COTS WiFi chip; ii) the COTS WiFi chip is very cheap (e.g., a USB WiFi adapter dongle is less than $10); iii) devices

WiSec '20, July 8–10, 2020, Linz (Virtual Event), Austria

ACM ISBN 978-1-4503-8006-5/20/07…$15.00
https://doi.org/10.1145/3395351.3399367

equipped with WiFi chips are widely available. For example, by hacking and modifying the parameters Short Interframe Space (SIFS), Arbitration Inter-frame Spacing (AIFS), and Random Backoff on a WiFi device (e.g., equipped with a popular WiFi chip such as Atheros AR7010 or AR9271), the WiFi chip is able to transmit WiFi packets to jam a specific frequency band. Furthermore, the WiFi's communication range is up to 80 meters which is sufficient to jam neighboring ZigBee devices.

On the other hand, the concealed jamming signal transmitted by a COTS WiFi device is extremely difficult to detect because i) the jamming signal sent by a COTS WiFi device is actually legitimate WiFi packets; and ii) ZigBee devices are neither able to demodulate WiFi packets nor monitor the channel condition during a long time period because ZigBee devices are working under low duty-cycle (i.e., only wake up for very short time duration) to save energy.

In order to defend the concealed jamming, we have to address the following main challenges:

C1. How does the IoT gateway extract ZigBee packets from the signals collided with WiFi packets? Because of the adoption of CSMA/CA mechanism, a ZigBee device normally senses the channel before transmission. If the channel is busy, it will back off. The adversary can utilize this feature to prevent ZigBee devices' channel access by sending out the legitimate WiFi packets (shown in Figure 3(a)). To defend against concealed jamming, at the ZigBee sender side, we proposed to bypass the CSMA/CA and transmit ZigBee packets along with existing WiFi packets. Thus, at the IoT gateway side, the main challenge is how to extract out the ZigBee signals. To overcome this challenge, we propose a three-fold ZigBee signal recovering scheme which utilizes i) the diversity of ZigBee chip rate and WiFi symbol rate; and ii) the robustness of original DSSS scheme (detailed in Section 4.2).

C2. How to resolve partially collided ZigBee packets? It is possible that a ZigBee packet is partially collided (either at the head, tail, or central) with a WiFi packet. It is challenging to correctly extract the ZigBee packet in this situation. To address this challenge, we develop a correlation module which can process the real-time signal and selectively connect the received signal with: i) a normal ZigBee signal physical layer to demodulate if the incoming signals are normal ZigBee signals; or ii) the concealed jamming extraction module to extract ZigBee signals if the incoming signals are collided with WiFi packets (detailed in Section 4.3).

C3. How to extract packets from multiple ZigBee devices on different channels? As defined by the physical layers of WiFi and ZigBee standards, on the 2.4 GHz ISM band, one WiFi channel is overlapped with up to four ZigBee channels. This means one WiFi device can jam up to four ZigBee transmissions simultaneously. To overcome this challenge, we utilize the unique features in ZigBee protocol (i.e., 3 MHz gap between two ZigBee channels and four parallel correlation modules) to extract the ZigBee signals on different channels (detailed in Section 4.5).

The main contributions of this paper are as follows:

• In this paper, we discovered a new set of attacks–concealed jamming in IoT networks. With the exponentially increasing number of IoT devices deployed, we expect that concealed jamming will become very common because it is very difficult for ZigBee devices to differentiate between the interference and the concealed jamming.

• We proposed methods to defend against these attacks. Our proposed methods are compatible with the WiFi and ZigBee standards. Our methods are generic and have the potential to be applied to defend from attacks among other devices that share the overlapped frequency bands.

• We extensively evaluated our proposed methods under real-world settings with various parameters. Our evaluation results show that ZigBee devices (protected by our proposed methods) achieve similar performance as those that are not under the concealed jamming attack. Moreover, compared with unprotected devices, the packet reception delay can be significantly reduced by a factor of 16 while protected by using our proposed methods.

2 MOTIVATION

In this section, we introduce why concealed jamming is easy to be launched, difficult to detect, impacts and cause serious failure on a wide range of ZigBee devices.

2.1 It is easy to compromise COTS WiFi devices for jamming.

A designated jammer is hard to implement because:

•**Legitimacy:** A designated jammer is illegal because i) it can be used by criminals to block security system during a crime; ii) it can also affect more than just nearby devices; and iii) jamming is seen as property theft.

•**Feasibility:** There are two basic types of designated jammers: i) continuous jammer which continuously emits signal at a target frequency; and ii) selective jammer which analyses the front part (e.g., header) of a packet and selectively corrupts the target packets' later part (e.g., CRCs). However, these two types of jammer are either easy to notice or need special equipment with a high cost.

Compared with a designated jammer, using or compromising a commercial off-the-shelf (COTS) WiFi device for jamming is much easier. For example, by hacking and modifying the parameters Short Interframe Space (SIFS), Arbitration Inter-frame Spacing (AIFS), and Random Backoff on a WiFi chip, the WiFi chip is able to transmit WiFi packets to jam a specific frequency band. Since the WiFi's communication range is up to 80 meters, it is sufficient to jam neighboring ZigBee devices. The COTS WiFi devices are very cheap (e.g., a USB dongle is less than $10) and widely available.

2.2 It is easy to use a WiFi device for jamming ZigBee and difficult to be detected.

It is very easy to use COTS WiFi devices for jamming ZigBee communication because of the following reasons:

•**Channel overlapping:** The most popular WiFi and ZigBee protocols work on the same 2.4 GHz ISM (industrial, scientific and medical) band. Thus, WiFi signal can potentially generate interference to ZigBee communications.

•**Fair channel access:** The distributed channel accessing algorithms (e.g., CSMA/CA) assume different devices have equal rights to access the channel. However, a selfish device (or an attacker) can intentionally access a channel much more than others.

•**Bandwidth**: A typical 2.4GHz WiFi signal spans 20 MHz or 40 MHz so the WiFi signal is much wider than a 2 MHz ZigBee signal.

Brand	Model	Type	ZigBee Profile	Power source	Required Gateway	Jamming Impact
Bosch	ISW-ZPR1-WP13	Pro-Grade Motion Detector	Home Automation	AA Battery	SmartThings Hub	Severe
Centralite	3310-G	Temp & Humidity Sensor	Home Automation	CR-2 Battery	SmartThings Hub	Moderate
Centralite	3323-C	Door Sensor	Home Automation	CR-2450 Battery	SmartThings Hub	Severe
Centralite	3315-C	Water Leak Sensor	Home Automation	CR-2 Battery	SmartThings Hub	Severe
Centralite	3155-wC	Smart Switch	Home Automation	Wall-Powered	SmartThings Hub	Mild
GE	45856GE	Smart Switch	Home Automation	Wall-Powered	Amazon Echo Plus	Mild
GWi	G4-MG-SE-GM-V2	Gas Meter	Smart Energy	Lithium Battery	Smart Energy Hub	Mild
IKEA	50383505	Motion SENSOR	Light Link	CR-2032 Battery	Hue Bridge	Severe
LEVITON	DL6HD-1BZ	DECORA Smart Dimmer	Smart Energy	Wall-Powered	SmartThings Hub	Mild
LEVITON	ZSS10-N0Z	DECORA Smart Switch	Smart Energy	Wall-Powered	SmartThings Hub	Mild
Philips	464602	Motion SENSOR	Light Link	AAA Battery	Hue Bridge	Severe
Samsung	F-IRM-US-2	Motion Sensor	Home Automation	CR-2477 Battery	SmartThings Hub	Severe
Samsung	F-ARR-US-2	Arrival Sensor	Home Automation	CR-2032 Battery	SmartThings Hub	Moderate
Samsung	F-MLT-US-2	Door/Window Sensor	Home Automation	CR-2450 Battery	SmartThings Hub	Severe
Samsung	F-WTR-US-2	Water Leak Sensor	Home Automation	CR-2 Battery	SmartThings Hub	Severe
Samsung	HSR761H	Smoke & CO Sensor	Home Automation	Wall-Powered	SmartThings Hub	Severe
SYLYANIA	E21266	Motion Sensor	Light Link	CR-2 Battery	Wink Hub	Severe
SYLYANIA	SYL-74388	Contact Temperature Sensor	Light Link	CR-2450 Battery	Wink Hub	Moderate
Visonic	MCT-340	Door Window Sensor	Home Automation	CR-2035 Battery	SmartThings Hub	Severe
Visonic	MP-841	PIR Detector	Home Automation	CR-123A Battery	SmartThings Hub	Severe
Visonic	GB-540	Acoustic Glass-break Detector	Home Automation	CR-123A Battery	SmartThings Hub	Severe

Table 1: A list of most popular ZigBee devices for smart home application

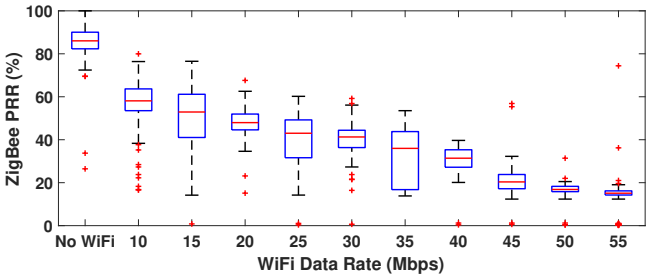


Figure 2: ZigBee device is concealed jammed by COTS WiFi

Therefore, it is very hard for ZigBee communication to survive from WiFi communication.

Furthermore, the concealed jamming is difficult to be detected because i) the jamming signal sent out by a COTS WiFi device are legitimate WiFi packets; and ii) ZigBee devices are neither able to demodulate WiFi packets nor monitor the channel condition during a long time period because ZigBee devices are working under low duty-cycle (i.e., only wake up for very short time duration) to save energy.

2.3 A wide range of ZigBee devices can be affected.

We investigated the commercially available ZigBee devices on the market. In Table 1, we listed the most popular devices used for smart home applications. There is a huge number of home security related sensors (e.g., motion sensors, door/window sensors and glass-break sensors). If the messages from these sensors are blocked, the security system will fail. Another group is safety related sensors, such as smoke, CO, and water leak sensors. If the communications from these sensors get jammed, there will be safety issues or life-threatening issues. Since most of these sensors are battery powered, they are only equipped with ZigBee radio to prolong battery life. Thus, they need to communicate with a multi-radio gateway to transfer the data to other devices.

2.4 Concealed jamming can cause ZigBee communication failures.

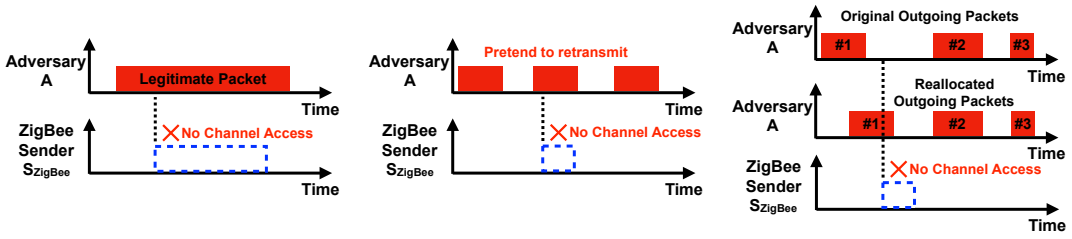
We have conducted a series of proof-of-concept experiments to demonstrate the impact of concealed jamming (i.e., a COTS WiFi device jams a ZigBee device). In the experiment, a WiFi device uploads a large amount of data (with different data rates) to a multi-radio gateway that has both WiFi and ZigBee radios. At the same time, a ZigBee device transmits sensing data to the gateway every second. The result (in Figure 2) shows that, when there is no WiFi transmission, ZigBee communication achieves an average packet reception ratio (PRR) of around 90%. However, when WiFi packets are present, the average ZigBee PRR is as low as 20%. It is worth noting that we did not hack and change any parameters of the WiFi card's firmware in this simple experiment.

3 ASSUMPTIONS AND THREAT MODEL

To defend against concealed jamming, we generalize the assumptions and the threat model in this section.

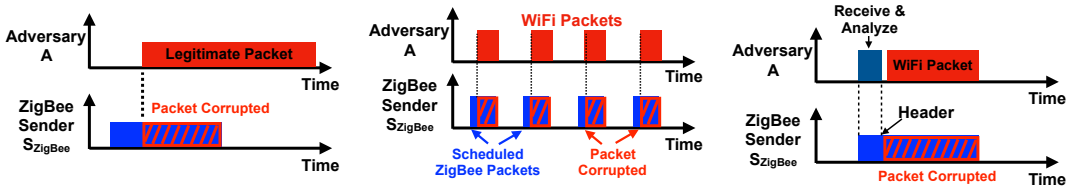
3.1 Assumptions

We assume ZigBee devices (communicating to the gateway) have limited transmission power, computation resources, and energy supply. For the adversary, we assume it is a COTS WiFi radio that is defined by IEEE 802.11a/g/n or later standards. We further relax the assumption that the adversary can have unlimited computing



(a) Channel Access Prevention (b) Adversary pretends to retransmit (c) Adversary reallocates outgoing packets

Figure 3: Attack Action Type I: Channel Access Prevention



(a) Packet Corruption (b) Adversary obtains ZigBee schedule and transmits exactly at wake up time (c) Adversary analyzes ZigBee packet's header and transmits towards the rest part of the packet

Figure 4: Attack Action Type II: Packet Corruption

resource, power supply, and bandwidth (in 2.4 GHz). The adversary is able to eavesdrop on any frequency band and transmit WiFi compatible signals (defined by IEEE 802.11 a/g/n or later standards), but it cannot disable the communication channel by blocking the propagation of signals (e.g., by placing a Faraday cage around the gateway) or does not have physical access to the ZigBee devices (i.e., the adversary cannot physically remove ZigBee devices).

3.2 Threat Model

Different from the traditional radio jamming (introduced in the introduction section), we identified a new threat model in which the adversary pretends to be a legitimate WiFi device and prevents the communications between the ZigBee sender S_{ZigBee} and the IoT gateway receiver R. With the increasing number of ZigBee devices deployed in the world, this type of threat is becoming increasingly serious. For example, Amazon echo plus and Samsung SmartThings hub contain ZigBee radios that serve as a ZigBee hub to collect the data and control appliances inside the smart home. If the adversary prevents the ZigBee communication between the appliances and the Amazon echo plus (or Samsung SmartThings hub), the main entrance door may not be locked as expected.

Specifically, the adversary A can launch the following two types of attack actions:

Type I: Channel Access Prevention. The adversary A transmits legitimate WiFi packets ahead of the ZigBee's transmission (Figure 3(a)). Thus, ZigBee sender S_{ZigBee} cannot obtain the channel access whenever it attempts to transmit. To launch this type of attack, there are two main methods:

• The adversary A can pretend to retransmit legitimate WiFi packets in order to occupy the channel for a long time so that the transmission of ZigBee S_{ZigBee} is blocked (Figure 3(b)).

• The adversary A can reallocate the outgoing packets to prevent the ZigBee's communication. As shown in Figure 3(c), by delaying the transmission of #1 packet, the adversary A can prevent the channel access of the ZigBee sender.

Type II: Packet Corruption. After detecting the transmission of ZigBee sender S_{ZigBee}, the adversary A transmits a legitimate WiFi packet (shown in Figure 4(a)). Therefore, part of the packet transmitted by ZigBee sender S_{ZigBee} will be corrupted at the gateway receiver side. To launch this type of attack, there are two main methods:

• Since most of the ZigBee devices send out the packet periodically, the adversary A can learn the schedule of the targeted ZigBee sender S_{ZigBee} to maximize the attack possibility but minimize the number of transmissions of jamming signal to prevent itself from being detected (shown in Figure 4(b)).

• For ZigBee devices that do not send out packets periodically, the adversary A can continuously sniff the channel. After detecting the ZigBee packet's headers, the adversary immediately transmits a jamming signal that corrupts the ZigBee's packet (shown in Figure 4(c)).

If the ZigBee devices switch to a new channel, the adversary can also switch to the channel that overlapped with the ZigBee devices' new channel and launch the above two types of attacks. Therefore, frequency hopping cannot avoid the concealed jamming attacks.

4 DESIGN

In this section, we introduce how to detect the potential concealed jamming at the ZigBee device side. Then, we describe how to extract ZigBee packets from collided WiFi packets at the IoT gateway side. Finally, we discuss how to deal with partially collided packets,

an adversary using a different WiFi channel, and multiple ZigBee senders.

4.1 Concealed Jamming Detection

As described in Section 3.2, in a concealed jamming attack, the adversary pretends to be a WiFi device. The adversary either continuously transmits packets or reallocates the outgoing packets to occupy the channel. By doing this, the adversary prevents ZigBee devices from accessing the targeted wireless channel by utilizing the knowledge that the ZigBee protocol adopts CSMA/CA to avoid collision,.

In the CSMA/CA method, a ZigBee device senses the channel before the packet transmission. When the ZigBee device attempts to transmit a packet on Channel x, if the channel is not busy, it directly transmits the packet. Otherwise, the ZigBee device backs off, waits for the next wake up time slot and senses again. The device repeats this procedure until the packet is sent. By using CSMA/CA, devices minimize the interference in a distributed way.

However, an adversary can utilize CSMA/CA to prevent ZigBee devices from accessing the channel. Specifically, the adversary can launch a concealed jamming attack, which yields an unacceptably long delay that results in communication failure. At the same time, the IoT gateway does not notice it because the adversary is pretending to be a normal WiFi sender or the adversary compromises a normal WiFi sender so that the packets used for jamming are legal WiFi packets. More seriously, since one WiFi channel spans 20 MHz, it can block up to four ZigBee channels (each of them spans 2 MHz with a 3 MHz guard band).

To deal with this concealed jamming attack, we propose the concealed jamming detection and prevention procedure. Compared with the original CSMA/CA procedure, the concealed jamming detection and prevention procedure contains the following four steps:

STEP 1. Channel Sensing: When the ZigBee device attempts to transmit a packet on channel x, it initiates and records the number of attempts. After conducting channel sensing on channel x, if the channel is not busy, it transmits the packet.

STEP 2. Sweeping Potential WiFi Channel: If channel x is busy, the ZigBee device sweeps from channel i to j. Where $i < x < j$ and channels i to j cover all of the potential overlapped WiFi channels.

The purpose of this step is to check if the signal in the air is WiFi signal. We utilize the pre-knowledge that WiFi channels are located in a specific frequency range. By sensing each ZigBee Channel, the device can determine if the signal is from a WiFi device. Without loss of generality, we assume ZigBee is communicating with the gateway on channel 13 ($x = 13$). In **STEP 1**, channel busy state is detected. Therefore, in **STEP 2**, the ZigBee device sweeps from channel i ($i = 11$ in this case) to j ($j = 15$ in this case) because the potential overlapped WiFi channels are WiFi channels 1, 2, and 3. After sweeping, the ZigBee device finds that four of its channels 11, 12, 13, and 14 are all busy. Thus, it suspects that a potential WiFi pretended jammer is working on WiFi channel 1.

STEP 3. Checking Number of Attempts: After sweeping, the device checks the number of attempts. If the number of attempts is less than a threshold m, the device backs off, waits for the next wake up time slot and increments the number of attempts by one, then repeats **STEP 1**.

The parameter m depends on the requirements of delay and priority for different applications. For example, if the ZigBee device is detecting a fire or carbon monoxide leakage, the delay is critical. Thus, the value of m can be as low as 1. By doing this, the ZigBee device immediately transmits packets even when a normal WiFi packet' is detected. If the ZigBee device is measuring the environmental temperature, which is not very time sensitive, m can be a relatively larger value.

STEP 4. Transmitting with Busy Channel: When the number of attempts exceeds the threshold m, the ZigBee device suspects that it is under the concealed jamming attack. Then, it will transmit the packet immediately even when the channel is busy (i.e., occupied by a WiFi device).

4.2 ZigBee Signal Extraction

In the previous section, we introduced how to detect the potential concealed jamming at the ZigBee device side. We note that ZigBee devices have a very cheap and coarse-grained radio. It is possible for a ZigBee device to incorrectly identify whether it is under the concealed jamming attack or it is under severe interference from the legitimate WiFi devices. Therefore, we need the gateway to extract the ZigBee packets that may collide with WiFi packets. In this subsection, we first review the basis of WiFi and ZigBee communications. Then, we introduce our collided signal disentangling technique to extract ZigBee data from the ZigBee packets that are collided with WiFi signals.

In the OFDM based WiFi modulation process, the WiFi binary data goes into a serial to parallel convertor which allocates the binary bits on different OFDM subcarriers. On each subcarrier, the modulator maps the binary bits into different phases or amplitude states of sine waves, which depends on the modulation scheme (QPSK, QAM, etc.). on subcarrier k, the signal can be expressed as follows:

$$v_k(t) = X_k e^{j2\pi kt/T}, 0 \le t < T_w \tag{1}$$

where X_k is the data symbol, T_w is the WiFi symbol duration (which is the reciprocal of WiFi symbol rate f_w). By using an inverse fast Fourier transform (IFFT), WiFi combines N subcarriers efficiently into an OFDM signal, which is expressed as follows:

$$v_w(t) = \sum_{k=0}^{N-1} X_k e^{j2\pi(kf_w)t} \tag{2}$$

To ensure subcarriers are orthogonal, the symbol rate f_w (which is also known as subcarrier spacing) has to satisfy the following expression:

$$\frac{1}{T}\int_0^T (e^{j2\pi k_1 f_w t})^* (e^{j2\pi k_2 f_w t}) = \frac{1}{T}\int_0^T e^{j2\pi(k_2-k_1)f_w t}\,dt \tag{3}$$

where $(\cdot)^*$ denotes the complex conjugate operator. The result of Expression 3 is 0 while $k_1 \neq k_2$, which means the signals $e^{j2\pi k_1 f_w t}$ and $e^{j2\pi k_2 f_w t}$ are orthogonal. By up-converting to carrier frequency

f_c, the transmitted signal $s_w(t)$ can be represented as:

$$s_w(t) = \mathbb{R}\{v_w(t)e^{j2\pi f_c t}\} = \sum_{k=0}^{N-1} |X_k| \cos(2\pi[f_c + kf_w]t + \arg[X_k]) \quad (4)$$

where $|X_k|$ and $\arg[X_k]$ are the amplitude and phase modulated values, respectively. After these, the radio front-end emits the signal to the media. To demodulate the WiFi signals, the WiFi receiver basically takes the five steps: i) the radio front-end picks up the OFDM signal; ii) the down-converter converts the signal to baseband by multiply the carrier wave; iii) a fast Fourier transform (FFT) module separates the signal onto different subcarriers; iv) the demodulator maps the sine wave (with different phase and amplitude states) to bits; and v) the demodulated bits on each subcarrier are combined by a parallel to serial convertor.

Since the ZigBee protocol devotes on low power wireless transmission, to compensate for channel interference, it uses Direct Sequence Spread Spectrum (DSSS) to spread the signal into a wider band by mapping the ZigBee binary data with a higher rate (2 MHz) pseudorandom noise (PN) code. The ZigBee radio modulates the mapped chips by Offset quadrature phase-shift keying (OQPSK) modulation which reduces the dramatic phase shifts by offsetting the timing of the odd and even bits by one bit-period, the in-phase and quadrature components will never change at the same time. Thus, the phase shifts no more than 90 degrees at a time. This yields much lower amplitude fluctuations when compared with normal QPSK. The baseband signal is up-converted by multiplying the carrier wave and transmitted. A transmitted ZigBee signal (using OQPSK modulation) $s_z(t)$ can be expressed as follow:

$$s_z(t) = A\cos[2\pi f_c t + \theta_n], 0 \le t < T_z, n = 1, 2, 3, 4 \quad (5)$$

Where T_z is the ZigBee symbol duration (which is the reciprocal of ZigBee symbol rate f_z), θ_n is given by:

$$\theta_n = (2n-1)\frac{\pi}{4} \quad (6)$$

Therefore, the four possible signal phases are $\pi/4$,$3\pi/4$,$5\pi/4$ and $7\pi/4$. The ZigBee receiver takes three inverse steps: i) The radio front-end receives the signal and down-converts the signal to baseband; ii) The baseband signal is demodulates by OQPSK demodulator; and iii) demodulated chips are mapped to ZigBee binary data.

As described before, the popular WiFi protocols (succeeding IEEE 802.11g [1]) use OFDM based modulation to achieve efficient use of spectrum. By using OFDM, the whole 20 MHz bandwidth is divided into up to 64 subcarriers. Instead of a wide-band signal (20 MHz), each subcarrier uses a narrow-band signal (312.5 KHz) to carry data. The use of a narrow-band signal compared to a single wide-band signal makes the system very resistant to channel fading and greatly reduces the complexity of the receiver equalizer that is required. Moreover, the 312.5 KHz narrow-band signal yields a slower symbol rate:

WiFi Symbol Rate: the narrow-band subcarriers of the OFDM signal carry data at the symbol rate[1] of 250,000 symbols per second.

[1]The symbol rate is the number of symbol changes across the transmission medium per time unit

On the other hand, since the ZigBee's modulation scheme adopts DSSS (which spreads the data into the 2MHz bandwidth), the chip rate is much higher:

ZigBee Chip Rate: the ZigBee's OQPSK-DSSS modulation scheme carries data at the chip rate[2] of 2,000,000 chips per second.

WiFi symbol rate and ZigBee chip rate reveal signal varying speed in WiFi and ZigBee signals, respectively. By utilizing this property, it is possible to disentangle the two signals if they are collided with each other.

After the WiFi and ZigBee collided signal is received, we first extract and demodulate the ZigBee signal, then apply an error correcting mechanism to the distorted signals. The scheme to recover ZigBee signal is divided into three folds. *First*, for a WiFi and ZigBee collided channel, the ZigBee channel overlaps only a portion (7 out of 64 subcarriers) of the wider frequency-band WiFi signal. By utilizing the diverse chip rate (2,000,000 chip/s) of ZigBee and symbol rate (250,000 symbol/s) of WiFi, we can implement a band-stop filter bank that isolates corresponding slower rate WiFi subcarriers, thus reducing tonal interference. *Second*, though the filter cannot completely remove the impact of WiFi signal, the distorted ZigBee signals can be compensated by the robust DSSS scheme. The DSSS scheme, which spreads the energy into a wider frequency band, originally is used to resist noise and interference. Here, we utilized as a jamming resistant property. *Third*, by appending Forward Error Correcting (FEC) to the ZigBee data packet, we can also increase the probability of correct receptions. Therefore, WiFi overlapped ZigBee packets have a higher likelihood of packet reception.

4.3 Handling Partially Collided Packets

In Section 4.2, we proposed to extract ZigBee packets from overlapped concealed jamming signals. However, to smoothly recover the ZigBee signal, we need to consider four different conditions: 1) entirely collided; 2) collided at the tail; 3) collided at the head; and 4) collided in the middle.

The technique introduced in Section 4.2 can only work under the first condition (i.e., entirely collided). To make the system robust to work in all the conditions, we encounter a main challenge. i.e., how to seamlessly convert between the normal ZigBee demodulation and the concealed jamming extraction.

To overcome this challenge, we designed a correlation module. After receiving the wireless signal from the radio front-end, the correlation module decides whether the received signal $R[n]$ is a normal ZigBee signal $S_{ZigBee}[n]$ or a jammed signal $S_{Jam}[n]$. If the signal is a normal ZigBee signal, it directly feeds to the traditional ZigBee physical (PHY) layer to demodulate the signal. Otherwise, the jammed signal goes into the concealed jamming extraction (introduced in Section 4.2). The extracted ZigBee signal will go to the ZigBee PHY.

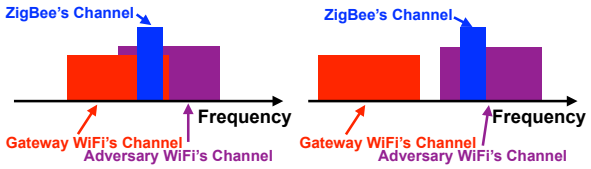
The functionality of correlation module is revealed in Algorithm 1. The inputs are received signal $R[n]$, desired WiFi signal of one symbol duration $G_{WiFi}[n]$, and desired ZigBee signal of one symbol duration $G_{ZigBee}[n]$. The outputs are normal ZigBee signal $S_{ZigBee}[n]$ and $S_{Jam}[n]$ which are fed into traditional ZigBee PHY or concealed jamming extraction, respectively. We first calculate the cross-correlation C_{WiFi} between the received signal $R[n]$ and

[2]The chip rate is the number of chips per second used in the spreading signal.

Algorithm 1 Correlation Module

Input: $R[n]$, $G_{WiFi}[n]$ $n \in [0, T_{WiFi\_symbol}]$, and $G_{ZigBee}[n]$ $n \in [0, T_{ZigBee\_symbol}]$.
Output: $S_{ZigBee}[n]$ and $S_{Jam}[n]$.

1: $C_{WiFi} = \max_{k \in [0, T_{WiFi\_symbol}]} \sum_{n=0}^{\infty} G_{WiFi}[n-k]y[n]$;
2: $C_{ZigBee} = \max_{k \in [0, T_{ZigBee\_symbol}]} \sum_{n=0}^{\infty} G_{ZigBee}[n-k]y[n]$;
3: **if** $C_{WiFi} > C_{ZigBee}$ **then**
4: $S_{Jam}[n] = R[n]$;
5: **else**
6: $S_{ZigBee}[n] = R[n]$;
7: **end if**



(a) Case One (b) Case Two

Figure 5: The relationship of ZigBee's channel, gateway WiFi's Channel, and adversary WiFi's channel in the frequency domain

desired WiFi signal $G_{WiFi}[n]$ within one WiFi symbol duration (Line 1). Similarly, we calculate C_{ZigBee} (Line 2). Then, we decide whether outputs $S_{ZigBee}[n]$ or $S_{Jam}[n]$ based on the value of C_{WiFi} and C_{ZigBee} (Lines 3-7).

4.4 Handling an Adversary using a Different WiFi Channel

In Section 4.2, we introduced how to extract ZigBee signals from overlapped WiFi signals if the IoT gateway receives the combined ZigBee and WiFi signals. However, as we mentioned in the introduction section, it is possible that the adversary smartly jams ZigBee device's communication on the WiFi channel which is different from the one IoT gateway works on. Therefore, IoT gateway will not pick up the WiFi packet and be able to extract ZigBee signal.

An example is shown in Figure 5, in which the blue, red, and purple area are the frequency ranges for ZigBee, gateway WiFi, and the adversary, respectively. There are two possible cases: i) the gateway WiFi and ZigBee work on overlapped channels (shown in Figure 5(a)); ii) the gateway WiFi and ZigBee work on non-overlapped channels (shown in Figure 5(b)). In any cases, the IoT gateway is not able to pick up adversary's jamming packet because the working frequency are different. Therefore, it can not obtain ZigBee packet by simply applying the technique introduced in Section 4.2.

To defend the concealed jamming under this situation, we propose to overhear the overlapped ZigBee packet on any working channel. Note that, originally, the ZigBee receiver discards WiFi signal. To overhear the ZigBee packet, the gateway pick up all the signals on ZigBee channel. If the signal satisfies ZigBee protocol, it will be demodulated by normal ZigBee physical layer. Otherwise,

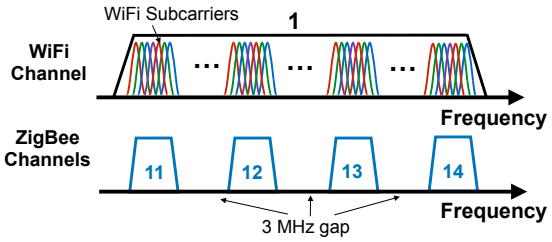


Figure 6: There is a 3 MHz gap between two ZigBee channels

the gateway utilizes the technique we introduced in Section 4.2 to extract ZigBee signal.

Let us take Figure 5 as example again. In either case, the gateway will listen on the blue area frequency channel (the channel ZigBee works on). Instead of discarding the WiFi signal (if the concealed jamming presents), the gateway extracts ZigBee packets from it.

4.5 Handling Multiple ZigBee Senders

As introduced in Section 3, one WiFi channel is overlapped with up to four ZigBee channels, which means one pretended WiFi jammer can invalidate four different ZigBee transmissions on corresponding channels. In the previous section, we proposed how to defend one ZigBee transmission from a concealed jamming attack. In this section, we introduce another benefit of our system that the IoT gateway can extract up to four ZigBee packets on different channels simultaneously.

To support multiple ZigBee senders, we need to answer the following two questions: i) Is it possible to extract ZigBee signals on different channels independently? ii) How to solve the problem if the packets on different channels arrive at different times?

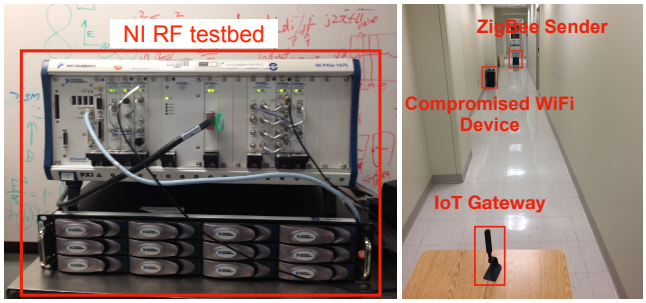
For the first question, we review the ZigBee channel distribution on frequency domain. Figure 6 shows one WiFi channel (i.e., WiFi Channel 1) is overlapping with four ZigBee channels (i.e., ZigBee Channel 11, 12, 13, and 14). Moreover, one ZigBee channel is overlapped with approximately seven WiFi subcarriers. Note that due to the orthogonal property of OFDM modulation, the adjacent subcarriers are overlapped with each other. However, we noticed that between two ZigBee channels, there is a 3MHz gap. Therefore, each subcarrier only overlaps with up to one ZigBee channel. This property guarantees that at the IoT gateway side, each ZigBee channel is independent from others so that we are able to extract ZigBee signal from different overlapped WiFi subcarriers.

To solve the second question, we can utilize four parallel correlation modules (discussed in Section 4.3). For each of them, we apply a band-path filter which corresponds to the frequency band of the ZigBee channel. By doing this, the signals on the four channels can be extracted independently.

5 EVALUATION

5.1 Real-world Implementation

We implemented the identified concealed jamming attack and our defense approach in real-word. Specifically, for the ZigBee devices we implemented on a ZigBee testbed. **TelosB node:** To test the performance of an unprotected and protected system, we used the



(a) Testbed (b) LoS

Figure 7: Experimental Setup

TelosB node [4] as a ZigBee sender because the TelosB node can log low level data such as the transmitted number of data bits and packets. For the concealed jamming device, we implemented the following two platforms: **COTS WiFi device:** For basic evaluation, we used a Dell XPS 9550 laptop as a WiFi sender. The network tool *iPerf* is used to generate concealed jamming packets. **USRP:** For extensive evaluation, we used a B210 USRP to test the system. By using an USRP as the concealed jamming device, it i) can receive and analyze the ZigBee packets; and ii) is more flexible to control the WiFi traffic rate, modulation schemes, and packet length. The IoT gateway receiver is fully implemented on a Soft Defined Radio (SDR) (the NI RF testbed is shown in Figure 7(a)). We strictly followed the IEEE 802.15.4 and IEEE 802.11 standards for ZigBee and WiFi devices, respectively.

5.2 Experimental Setup

The experiments are conducted on the third floors of an on-campus engineering building (shown in Figure 7(b)).

To extensively evaluate and compare with our defensive scheme, we implemented the following three schemes:

No Attack: Normal ZigBee to ZigBee communication without concealed jamming or interference from WiFi. This scheme is used to reflect the typical performance in a ZigBee network.

Victim: The ZigBee to IoT gateway communication is under concealed jamming attack. This schemes is used to illustrate the performance under concealed jamming attack.

Protege: The victim is protected by our defensive scheme. This schemes is used to illustrate the performance under concealed jamming attack and protected by our defensive scheme.

The following metrics are used to evaluate the performance of protege and compare protege with victim and no attack.

Delay: It specifies how long it takes for a packet of data to successfully transmit from the ZigBee sender to the gateway.

BER: The bit error rate (BER) is the number of bit errors per unit time.

PRR: Packet reception ratio (PRR) is the ratio of received packet over sent packet from the ZigBee sender to the gateway.

Throughput: The successfully received bits.

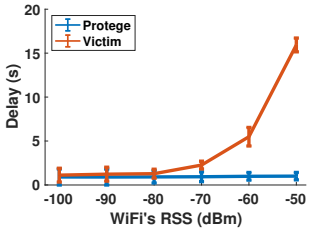


Figure 8: Delay v.s. WiFi's RSS: Compared with victim @ -50 dBm, the delay of protege is reduced by a factor of 16.

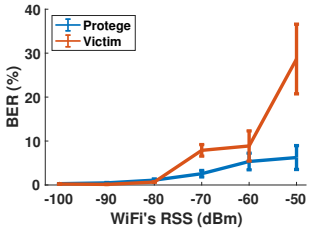


Figure 9: BER v.s. WiFi's RSS: The BER of protege is 2.5 times less than victim @ -50 dBm.

5.3 Delay v.s. WiFi's RSS

We show the results of delay versus WiFi's RSS in Figure 8. In general, the delay of the victim is increasing quickly along with the WiFi's RSS increasing from -100 to -50 dBm. The increasing trend is relatively slow between -100 and -80 dBm but becomes faster at -80 dBm. The reason is that with lower WiFi's RSS, ZigBee may not be backed off by WiFi signal because the relatively weak WiFi interference can be compensated by the DSSS ZigBee's DSSS scheme. However, with higher WiFi's RSS, the ZigBee packets are either corrupted or blocked by strong WiFi signals, which results retransmissions and yields long delay. The general trend for protege is stable across different WiFi's RSS. Compared with victim at -50 dBm, the delay of protege is reduced by a factor of 16. The reason is that our design ensures not only the transmitting of ZigBee packets (as discussed in Section 4.1) but the successful reception (as discussed in Section 4.2) as well.

5.4 BER v.s. WiFi's RSS

Figure 9 shows the BER result. We can observe that when the WiFi's RSS is low (from -100 to -80 dBm), protege and victim show similar BER (as low as 0.13% BER). This is because at the IoT gateway receiver side, with low signal strength, WiFi makes little impact to ZigBee signals. To some extent, the DSSS scheme can compensate the impact from WiFi signal. However, when the signal strength further increases, the BER of victim dramatically increases and finally reaches 27% at -50 dBm. Meanwhile, the BER of protege keeps relatively stable with the value of 6% (which is 2.5 times less than the victim) at -50 dBm. The reason is that victim suffers collisions and is not able to recover the collided ZigBee packets. But for the protege, it can extract ZigBee packets from collided WiFi packets (as described in Section 4), which yields lower BER.

5.5 Impact of WiFi's Traffic Rate

In this section, we evaluate the impact of WiFi's traffic rate (the higher percentage means WiFi transmits more data). We use *iPerf* to control the traffic rate. We compare the victim and protege in Figure 10. When the WiFi's traffic rate is 0.1%, protege and victim have similar delay. When the WiFi's traffic rate increases to 1% and 10%, we can observe the increasing trend on victim but protege keeps stable. By further increasing the WiFi's traffic rate to 100%, the delay of protege is still very low but victim reaches 30 seconds. The reason is that protege can resolve the packets collision and

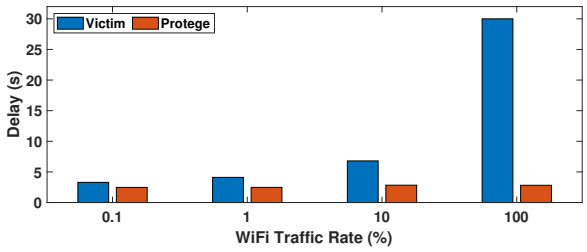
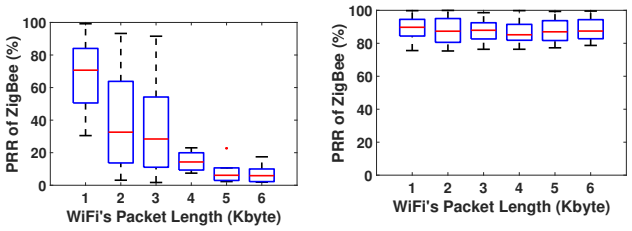
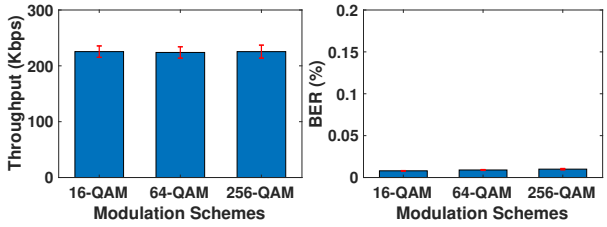


Figure 10: Impact of WiFi's Traffic Rate



(a) Victim (b) Protege

Figure 11: Impact of WiFi's Packet Length



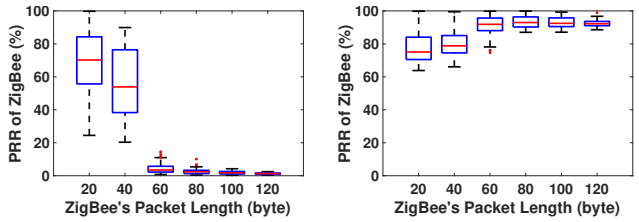
(a) Throughput (b) BER

Figure 12: Impact of WiFi Modulation Schemes

extract ZigBee data without the need of retransmissions while victim requires multiple retransmissions.

5.6 Impact of WiFi's Packet Length

WiFi's packet length provides a negative impact on packet reception ratio (PRR) of ZigBee communication because with longer WiFi packets, more ZigBee packets will be corrupted, and the ZigBee sender gets less chance to successfully transmit a ZigBee packet. Figure 11 shows the evaluation results of ZigBee PRR versus WiFi's packet length. For the victim (the results are shown in Figure 11(a)), the PRR decreases from 67% to 7% along with the WiFi's packet length increases from 1000 bytes to 6000 bytes because the victim approach cannot resolve the collided packets. For protege (the results are shown in Figure 11(b)), the average PRR is around 87%. The reason why the PRR is stable over different WiFi' packet lengths is that we can extract out ZigBee packets from WiFi packets. Therefore, the longer WiFi's packet does not have more an impact on the reception of ZigBee packets.



(a) Victim (b) Protege

Figure 13: Impact of ZigBee's Packet Length: the PRR increases significantly from less than 1% in the Victim to more than 90% in the Protege when the packet length is ≥ 80 bytes.

5.7 Impact of WiFi Modulation Schemes

WiFi protocols include various modulation schemes to adapt to different channel conditions and data rate requirements. To illustrate protege can extract and demodulate ZigBee packets from legitimate WiFi jamming signal with different modulation schemes, we conducted the experiments under three different WiFi modulation schemes: simple (16-QAM), moderate (64-QAM), and sophisticated (256-QAM). In Figure 12(a), for the concealed jamming from all of the three modulation schemes, the ZigBee communication can maintain an average of 224.96 Kbps. Figure 12(b) depicts the BER of the ZigBee communication (under concealed WiFi jamming). The results show that the BER keeps as low as 0.008%. The highest BER (0.01%) occurs when WiFi uses 256-QAM as the modulation scheme. This is because the sophisticated WiFi modulation scheme introduces more interference to ZigBee communication.

5.8 Impact of ZigBee's Packet Length

We investigate the impact of ZigBee's packet length in this section. We observe that for the victim, the packet reception ratio (PRR) decreases while the ZigBee's packet length increases (Figure 13(a)). The reason is that a longer ZigBee packet has a higher probability to collide with WiFi. The median value is 69% when the ZigBee's packet length is 20 bytes. When the packet length increases to 120 bytes, the PRR drops to less than 1%. On the contrary, the PRR of protege is still very high (shown in Figure 13(a)) as if there is no concealed jamming attack. Overall, we can achieve the PPR above 78% regardless of the packet length. In other words, our proposed methods only require the protected ZigBee device to transmit the same packet for less than 2 times (i.e., expected number of transmission is 1/0.78 = 1.28).

5.9 Performance of Multiple ZigBee Senders

We evaluate how the system performs for different numbers of ZigBee devices under concealed jamming. To illustrate the effectiveness for our system, we compare the aggregated throughput of the protege with the victim and "no attack". Figure 14 shows that for different numbers of ZigBee senders, the throughput of victim is very low (because of the interference of WiFi). However, the aggregated throughput of protege is very similar to the "no attack". The difference of average throughput between protege and the "no attack" is only 1.5%.

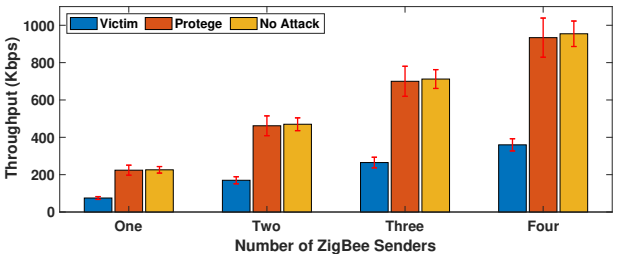


Figure 14: Performance of Multiple ZigBee Senders

6 RELATED WORK

In this Section, we review the prior work that related to our research. Several security/privacy issues were raised in IoT/CPS systems. In metering infrastructure network, a DoS attack was identified [50]. Privacy leakages were found in microgrids [19, 52], security problems in Ad-hoc networks [30, 49, 53, 54], reliability issues in key management [25, 35], gait information leakage via Wi-Fi [22], and UVA navigation with preserving privacy [31]. The most related works can be classified into two categories: **Jamming-related techniques** and **Interference-related techniques**.

6.1 Jamming-related techniques

Radio jamming refers to the deliberated jamming, blocking or interference with authorized wireless communications [2]. There are many types of jammers, including proactive jammers [16, 42] and reactive jammers [12, 18, 44], etc. To detect these jammers, researchers have developed lots of techniques and models [38, 47, 51]. In [40], the author mainly focuses on the reactive jamming detection. It detects the potential jamming by checking the received signal strength during the reception of each individual packets at the receiver side. Signal-to-noise ratio (SNR) and packet dropped per terminal (PDPT) are also applied to detect jamming. In [28], the author presents a centralized jamming detection system based on SNR and PDPT. The true detection rate is as high as 99.8%. There are also many techniques that can be applied to protect legitimate communications from these jammers [27, 46]. The author of [34] considered the impact of multipath effect in jamming attack. Ally Friendly Jamming utilizes controlled signals and shared secret keys to disable the enemy wireless communication and allow authorized wireless communication at the same time [36, 37]. In [33], to enable robust wireless communication under jamming attacks, the author introduces an uncoordinated DSSS (UDSSS) solution, which does not require shared secret keys and therefore has the ability to be applied to the broadcast scenarios. To decrease the delay introduced by UDSSS and improve the network performance, [32] proposes an ID-based cryptography in order to establish a reliable wireless connection without shared secret keys. Antenna techniques are also introduced to defend against jamming. As proposed in [48], the author utilize MIMO techniques at the receiver side to mitigate reactive jamming attack. In [43], the author proposed to automated placing the antenna arrays. Different from above methods, we mainly focus on using COTS WiFi to jam ZigBee. Moreover, we provide a systematic method to defend.

6.2 Interference-related techniques

Our work is also related to the non-intentional interference detection, mitigation and cancellation, which has been widely analyzed and modeled [6–10, 17, 20, 21, 26, 41, 52]. In [11], the author detects the ZigBee interference on commodity WiFi cards by monitoring the reception errors, including synchronization errors, invalid header formats, etc. To mitigate the WiFi interference on the ZigBee network, the common solution is to switch the channel that do not overlap with the active WiFi [24]. However, there are only limited number of channels that do not overlap with 802.11 channels, which is insufficient to accommodate multiple ZigBee networks [23]. In [39], the author utilizes RSSI as an indicator to mitigate the interference. However, it cannot deal with fast-changing interference. To cancel the interference, Zigzag exploits asynchrony across successive collisions to bootstrap the decoding process [14]. Successive interference cancellation for ZigBee nodes is also applied to reduce packet loss rate during collisions [15]. Difference from their approaches, our proposed technique is used to combat intentionally interference generated by WiFi at the ZigBe and gateway side.

7 CONCLUSION

With the exponentially increasing number of IoT devices and the shared radio frequency band among these IoT devices, a new set of attacks can be launched by the adversary. In this paper, we discovered the concealed jamming – an adversary pretends to be (or compromises) a legitimate WiFi device, then sends out WiFi packets to severely delay ZigBee devices' communication or collide with ZigBee's packets. By doing this, concealed jamming has the potential to severely delay the reception of ZigBee packets that may contain important information (e.g., health condition, fire alarms, bridge vibration, earth quake, and etc.). This type of attack will become more and more frequent and serious, when the number of IoT devices increases. To defend against these attacks, we developed the concealed jamming detection method at the ZigBee device side and designed a novel ZigBee data extraction technique at the gateway that can recover ZigBee data from the ZigBee packets that were collided with WiFi packets. We extensively evaluated our design under different real-world settings. Our evaluation results show that ZigBee devices (protected by our proposed methods) achieve similar performance as those that are not under the concealed jamming attack. Moreover, compared with unprotected devices, the packet reception delay can be significantly reduced by a factor of 16 while protected by using our proposed methods. Our proposed defense methods are generic and have the potential to be applied to defend attacks among other devices that share the overlapped frequency bands. Further more, given more and more IoT devices will be in use in the future, the defense technique can be also used for resolve collided WiFi and ZigBee packets which jam each other unintentionally.

ACKNOWLEDGMENTS

This work is supported in part by NSF grants CNS-1824491, CNS-1824355, CNS-1652669, CNS-1933069, CNS-1619251 and CNS-1514381. We also thank anonymous reviewers for their valuable comments.

REFERENCES

[1] [n.d.]. https://en.wikipedia.org/wiki/IEEE802.11a-1999.
[2] [n.d.]. https://en.wikipedia.org/wiki/Radio_jamming.
[3] [n.d.]. https://www.gartner.com/newsroom/id/3598917.
[4] [n.d.]. http://www.memsic.com/userfiles/files/Datasheets/WSN/telosb_datasheet.pdf.
[5] [n.d.]. http://www.zigbee.org/zigbee-for-developers/applicationstandards/zigbee-health-care/.
[6] Z. Chi, Z. Huang, Y. Yao, T. Xie, H. Sun, and T. Zhu. 2017. EMF: Embedding multiple flows of information in existing traffic for concurrent communication among heterogeneous IoT devices. In *IEEE INFOCOM 2017 - IEEE Conference on Computer Communications*. 1–9.
[7] Z. Chi, Y. Li, Z. Huang, H. Sun, and T. Zhu. 2019. Simultaneous Bi-directional Communications and Data Forwarding using a Single ZigBee Data Stream. In *IEEE INFOCOM 2019 - IEEE Conference on Computer Communications*. 577–585. https://doi.org/10.1109/INFOCOM.2019.8737555
[8] Zicheng Chi, Yan Li, Xin Liu, Yao Yao, Yanchao Zhang, and Ting Zhu. 2019. Parallel Inclusive Communication for Connecting Heterogeneous IoT Devices at the Edge. In *Proceedings of the 17th Conference on Embedded Networked Sensor Systems (SenSys '19)*. ACM, New York, NY, USA, 205–218. https://doi.org/10.1145/3356250.3360046
[9] Zicheng Chi, Yan Li, Hongyu Sun, Yao Yao, Zheng Lu, and Ting Zhu. 2016. B2W2: N-Way Concurrent Communication for IoT Devices. In *Proceedings of the 14th ACM Conference on Embedded Network Sensor Systems CD-ROM (SenSys '16)*. ACM, New York, NY, USA, 245–258.
[10] Z. Chi, Y. Li, Y. Yao, and T. Zhu. 2017. PMC: Parallel multi-protocol communication to heterogeneous IoT radios within a single WiFi channel. In *2017 IEEE 25th International Conference on Network Protocols (ICNP)*. 1–10.
[11] Daniele Croce, Domenico Garlisi, Fabrizio Giuliano, and Ilenia Tinnirello. [n.d.]. Learning from errors: Detecting ZigBee interference in WiFi networks. In *IEEE Ad Hoc, 2014.*
[12] S. Fang, Y. Liu, and P. Ning. 2016. Wireless Communications under Broadband Reactive Jamming Attacks. *IEEE Transactions on Dependable and Secure Computing* 13, 3 (May 2016), 394–408. https://doi.org/10.1109/TDSC.2015.2399304
[13] P. Frehill, D. Chambers, and C. Rotariu. 2007. Using Zigbee to Integrate Medical Devices. In *2007 29th Annual International Conference of the IEEE Engineering in Medicine and Biology Society*. 6717–6720. https://doi.org/10.1109/IEMBS.2007.4353902
[14] Shyamnath Gollakota and Dina Katabi. [n.d.]. Zigzag Decoding: Combating Hidden Terminals in Wireless Networks. In *ACM SIGCOMM, 2008.*
[15] Daniel Halperin, Thomas Anderson, and David Wetherall. [n.d.]. Taking the Sting out of Carrier Sense: Interference Cancellation for Wireless LANs. In *ACM MobiCom, 2008.*
[16] M. K. Hanawal, D. N. Nguyen, and M. Krunz. 2016. Jamming attack on in-band full-duplex communications: Detection and countermeasures. In *IEEE INFOCOM 2016 - The 35th Annual IEEE International Conference on Computer Communications*. 1–9. https://doi.org/10.1109/INFOCOM.2016.7524449
[17] Jan-Hinrich Hauer, Vlado Handziski, and Adam Wolisz. [n.d.]. Experimental Study of the Impact of WLAN Interference on IEEE 802.15.4 Body Area Networks. In *EWSN, 2009.*
[18] J. Heo, J. Kim, S. Bahk, and J. Paek. 2017. Dodge-Jam: Anti-Jamming Technique for Low-Power and Lossy Wireless Networks. In *2017 14th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)*. 1–9. https://doi.org/10.1109/SAHCN.2017.7964926
[19] Zhichuan Huang, Ting Zhu, Yu Gu, and Yanhua Li. 2016. Shepherd: Sharing Energy for Privacy Preserving in Hybrid AC-DC Microgrids. In *Proceedings of the Seventh International Conference on Future Energy Systems (e-Energy '16)*. ACM, New York, NY, USA, Article 19, 10 pages. https://doi.org/10.1145/2934328.2934347
[20] Haoran Jiang, Bin Liu, and Chang Wen Chen. [n.d.]. Performance analysis for ZigBee under WiFi interference in smart home. In *IEEE ICC, 2017.*
[21] Yan Li, Zicheng Chi, Xin Liu, and Ting Zhu. 2018. Chiron: Concurrent High Throughput Communication for IoT Devices. In *Proceedings of the 16th Annual International Conference on Mobile Systems, Applications, and Services (MobiSys '18)*. ACM, New York, NY, USA, 204–216.
[22] Yan Li and Ting Zhu. 2016. Gait-Based Wi-Fi Signatures for Privacy-Preserving. In *Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security (ASIA CCS '16)*. ACM, New York, NY, USA, 571–582. https://doi.org/10.1145/2897845.2897909
[23] Chieh-Jan Mike Liang, Jie Liu, Liqian Luo, Andreas Terzis, and Feng Zhao. [n.d.]. RACNet: A High-fidelity Data Center Sensing Network. In *ACM SenSys, 2009.*
[24] Chieh-Jan Mike Liang, Nissanka Bodhi Priyantha, Jie Liu, and Andreas Terzis. 2010. Surviving Wi-fi Interference in Low Power ZigBee Networks. In *Proceedings of the 8th ACM Conference on Embedded Networked Sensor Systems (SenSys '10)*. ACM, New York, NY, USA, 309–322. https://doi.org/10.1145/1869983.1870014
[25] Y. Liu, Z. Xia, P. Yi, Y. Yao, T. Xie, W. Wang, and T. Zhu. 2018. GENPass: A General Deep Learning Model for Password Guessing with PCFG Rules and Adversarial Generation. In *2018 IEEE International Conference on Communications (ICC)*. 1–6. https://doi.org/10.1109/ICC.2018.8422243
[26] Hongyao Luo, Zhichuan Huang, and Ting Zhu. 2015. A Survey on Spectrum Utilization in Wireless Sensor Networks. *Journal of Sensors* 2015 (03 2015), 1–13. https://doi.org/10.1155/2015/624610
[27] Ivan Martinovic, Paul Pichota, and Jens B. Schmitt. 2009. Jamming for Good: A Fresh Approach to Authentic Communication in WSNs. In *Proceedings of the Second ACM Conference on Wireless Network Security (WiSec '09)*. ACM, New York, NY, USA, 161–168. https://doi.org/10.1145/1514274.1514298
[28] Sudip Misra, Ranjit Singh, and SV Mohan. [n.d.]. Information warfare-worthy jamming attack detection mechanism for wireless sensor networks using a fuzzy inference system. In *Sensors, 2010.*
[29] V. Mukala, V. Lakafosis, A. Traille, and M. M. Tentzeris. 2010. A novel Zigbee-based low-cost, low-power wireless EKG system. In *2010 IEEE MTT-S International Microwave Symposium*. 624–627. https://doi.org/10.1109/MWSYM.2010.5517684
[30] P. Yi, T. Zhu, J. Ma, and Y. Wu. 2013. An Intrusion Prevention Mechanism in Mobile Ad Hoc Networks. *Ad Hoc & Sensor Wireless Networks* (2013), 269–292.
[31] Y. Pan, S. Li, J. L. Chang, Y. Yan, S. Xu, Y. An, and T. Zhu. 2019. An Unmanned Aerial Vehicle Navigation Mechanism with Preserving Privacy. In *ICC 2019 - 2019 IEEE International Conference on Communications (ICC)*. 1–6. https://doi.org/10.1109/ICC.2019.8761533
[32] Kim Pecina, Esfandiar Mohammadi, and Christina Pöpper. [n.d.]. Zero-Communication Seed Establishment for Anti-Jamming Techniques. In *NDSS Symposium, 2014.*
[33] Christina Pöpper, Mario Strasser, and Srdjan Čapkun. [n.d.]. Jamming-resistant Broadcast Communication Without Shared Keys. In *USENIX Security, 2009.*
[34] Christina Pöpper, Nils Ole Tippenhauer, Boris Danev, and Srdjan Capkun. 2011. Investigation of Signal and Message Manipulations on the Wireless Channel. In *Proceedings of the 16th European Conference on Research in Computer Security (ESORICS'11)*. Springer-Verlag, Berlin, Heidelberg, 40–59. http://dl.acm.org/citation.cfm?id=2041225.2041229
[35] S. Xiao, W. Gong, D. Towsley, Q. Zhang, and T. Zhu. 2014. Reliability Analysis for Cryptographic Key Management. In *IEEE ICC*.
[36] Swaminathan Sankararaman, Karim Abu-Affash, Alon Efrat, Sylvester David Eriksson-Bique, Valentin Polishchuk, Srinivasan Ramasubramanian, and Michael Segal. 2012. Optimization Schemes for Protective Jamming. In *Proceedings of the Thirteenth ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc '12)*. ACM, New York, NY, USA, 65–74. https://doi.org/10.1145/2248371.2248383
[37] Wenbo Shen, Peng Ning, Xiaofan He, and Huaiyu Dai. [n.d.]. Ally Friendly Jamming: How to Jam Your Enemy and Maintain Your Own Wireless Connectivity at the Same Time. In *IEEE Symposium on Security and Privacy, 2013.*
[38] David Slater, Patrick Tague, Radha Poovendran, and Mingyan Li. [n.d.]. A game-theoretic framework for jamming attacks and mitigation in commercial aircraft wireless networks. In *AIAA, 2009.*
[39] Kannan Srinivasan, Maria A. Kazandjieva, Saatvik Agarwal, and Philip Levis. [n.d.]. The B-factor: Measuring Wireless Link Burstiness. In *ACM SenSys, 2008.*
[40] Mario Strasser, Boris Danev, and Srdjan Čapkun. 2010. Detection of Reactive Jamming in Sensor Networks. *ACM Trans. Sen. Netw.* 7, 2, Article 16 (Sept. 2010), 29 pages. https://doi.org/10.1145/1824766.1824772
[41] Kun Tan, He Liu, Ji Fang, Wei Wang, Jiansong Zhang, Mi Chen, and Geoffrey M. Voelker. [n.d.]. SAM: Enabling Practical Spatial Multiple Access in Wireless LAN. In *MobiCom, 2009.*
[42] Lei Tang, Yanjun Sun, Omer Gurewitz, and David B. Johnson. 2011. EM-MAC: A Dynamic Multichannel Energy-efficient MAC Protocol for Wireless Sensor Networks. In *Proceedings of the Twelfth ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc '11)*. ACM, New York, NY, USA, Article 23, 11 pages. https://doi.org/10.1145/2107502.2107533
[43] Triet D. Vo-Huu, Erik-Oliver Blass, and Guevara Noubir. 2013. Counter-jamming Using Mixed Mechanical and Software Interference Cancellation. In *Proceedings of the Sixth ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '13)*. ACM, New York, NY, USA, 31–42. https://doi.org/10.1145/2462096.2462103
[44] Matthias Wilhelm, Ivan Martinovic, Jens B. Schmitt, and Vincent Lenders. 2011. Short Paper: Reactive Jamming in Wireless Networks: How Realistic is the Threat?. In *Proceedings of the Fourth ACM Conference on Wireless Network Security*. Association for Computing Machinery.
[45] Xin Wu and Shu Li. 2015. ZigBee transmission system for wearable ECG device based on compressed sensing. In *11th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM 2015)*. 1–4. https://doi.org/10.1049/cp.2015.0673
[46] Fengyuan Xu, Zhengrui Qin, Chiu C Tan, Baosheng Wang, and Qun Li. [n.d.]. IMDGuard: Securing implantable medical devices with the external wearable guardian. In *IEEE INFOCOM, 2011.*
[47] Wenyuan Xu, Wade Trappe, Yanyong Zhang, and Timothy Wood. 2005. The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks. In *Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc '05)*. ACM, New York, NY, USA, 46–57. https://doi.

org/10.1145/1062689.1062697

[48] Qiben Yan, Huacheng Zeng, Tingting Jiang, Ming Li, Wenjing Lou, and Y. Thomas Hou. [n.d.]. MIMO-based jamming resilient communication in wireless networks. In *IEEE INFOCOM, 2014*.

[49] Ping yi, Ting Zhu, Ning Liu, Yue Wu, and Jianhua Li. 2012. Cross-layer Detection for Black Hole Attack in Wireless Network. *Journal of Computational Information Systems* 8 (05 2012).

[50] P. Yi, T. Zhu, Q. Zhang, Y. Wu, and J. Li. 2014. A denial of service attack in advanced metering infrastructure network. In *2014 IEEE International Conference on Communications (ICC)*. 1029–1034. https://doi.org/10.1109/ICC.2014.6883456

[51] Q. Zhu, H. Li, Z. Han, and T. Basar. 2010. A Stochastic Game Model for Jamming in Multi-Channel Cognitive Radio Systems. In *2010 IEEE International Conference on Communications*. 1–6. https://doi.org/10.1109/ICC.2010.5502451

[52] T. Zhu, Sheng Xiao, Yi Ping, D. Towsley, and Weibo Gong. 2011. A secure energy routing mechanism for sharing renewable energy in smart microgrid. In *2011 IEEE International Conference on Smart Grid Communications (SmartGridComm)*. 143–148. https://doi.org/10.1109/SmartGridComm.2011.6102307

[53] T. Zhu and M. Yu. 2006. A Dynamic Secure QoS Routing Protocol for Wireless Ad Hoc Networks. In *IEEE Sarnoff*.

[54] T. Zhu and M. Yu. 2006. A Secure Quality of Service Routing Protocol for Wireless Ad Hoc Networks. In *IEEE GLOBECOM*.