Signal Emulation Attack and Defense for Smart Home IoT

Xiaonan Zhang*, Sihan Yu†, Hansong Zhou*, Pei Huang†, Linke Guo†, and Ming Li,‡

Abstract—Internet of Things (IoT) is transforming every corner of our daily life and plays important roles in the smart home. Depending on different requirements on wireless transmission, dedicated wireless protocols have been adopted on various types of IoT devices. Recent advances in Cross-Technology Communication (CTC) enable direct communication across those wireless protocols, which will greatly improve the spectrum utilization efficiency. However, it incurs serious security concerns on heterogeneous IoT devices. In this paper, we identify a new physical-layer attack, cross-technology signal emulation attack, where a WiFi device eavesdrops a ZigBee packet on the fly, and further manipulates the ZigBee device by emulating a ZigBee signal. To defend against this attack, we propose two defense strategies with the help of an anchor. Particularly, the passive defense strategy focuses on misleading the ZigBee signal eavesdropping, while the proactive approach develops a real-time detection mechanism on distinguishing between a common ZigBee signal and an emulated signal. We implement the complete attacking process and defense strategies with TI CC26x2R LaunchPad, USRP-N210 platform, and smart LED light bulbs, as well as a self-designed prototype, where a general light bulb can be turned on/off by a Nexus 5 smartphone directly. Extensive experiments have demonstrated the existence of the attack, and the feasibility, effectiveness, and accuracy of the proposed defense strategies.

Index Terms—Internet of Things, Signal Emulation Attack, Cross-Technology Communication

1 Introduction

The proliferation of the Internet of Things (IoT) enables ubiquitous connections among various wireless devices, such as wearable health monitors, security locks, fitness trackers, etc., for bettering our daily life [1, 2]. According to a recent market report [3], it is expected the number of IoT devices will reach to a total of 41.6billion by 2025. Among different wireless technologies being used, ZigBee is one of the dominant protocols used for smart home applications. Many household appliances have equipped with ZigBee chips for receiving commands from a multi-protocol gateway (ZigBee communication) and further being managed by users' mobile devices (WiFi communication). However, the wireless transmission between the gateway and ZigBee devices can be easily overheard by eavesdroppers, in the sense that the smart home IoT devices have the potential of being hacked in the wireless environment. Considering the dramatic growth of IoT used in home areas and the critical functionalities that IoT has involved, the loss could be immense. For example, attackers can turn on the cooling on smart thermostats during winter, unlock the smart garage door, and even turn off security camera for break-in, by transmitting the eavesdropped ZigBee signal directly without using the authorized gateway. Even worse, as our experimental results demonstrate, existing upper-layer cryptographic approaches do not work, and thus the attacker can completely bypass the upper-level security detection at ZigBee receivers.

Besides ZigBee, WiFi and Bluetooth protocols also play important roles in smart home applications. They all occupy the Industrial, Scientific, and Medical (ISM) 2.4 GHz band, generating a heterogeneous environment [4–7]. To tackle the interoperability issue, Cross-Technology Communication (CTC) serves as a feasible solution by enabling direct communication among devices across different wireless technologies [8–10]. It can greatly avoid repeated data transmission among different protocols, enhance the spectrum efficiency in the already-crowded ISM band, and reduce the cost of gateway deployment. However, this new paradigm poses significant security challenges. One of them is:an attacker with a different protocol can take advantages of CTC to launch long-range attacks to IoT devices without being identified. Even worse, the low-computational capabilities of IoT devices hinders the deployment of computational-intensive cryptographic approaches at higher layers for detection. Taking WiFi to ZigBee CTC as an example, with a much higher transmission power and mobility, WiFi devices can generate a stronger signal with a greater transmission range than ZigBee devices. As a result, WiFi devices can successfully attack ZigBee devices from a further distance without being found, making the attack more practical and powerful. Given the increasing deployment of IoT devices, it is critical to detect this type of attack and design effective countermeasures.

In this paper, we identify a new attack named as **Signal Emulation Attack** in the practical smart home scenario, where a WiFi attacker first eavesdrops on the control message by listening to the communication between ZigBee devices and their gateway. Then, it embeds the control message into its WiFi signal to manipulate the functionality of ZigBee devices. The emulated signal can pass the demodulation process at the ZigBee receiver, and thus it is infeasible to be detected. To protect the ZigBee devices, this work proposes two defense strategies with the help of an auxiliary anchor. We list our contribution as follows,

- We identify a new physical-layer attack, the signal

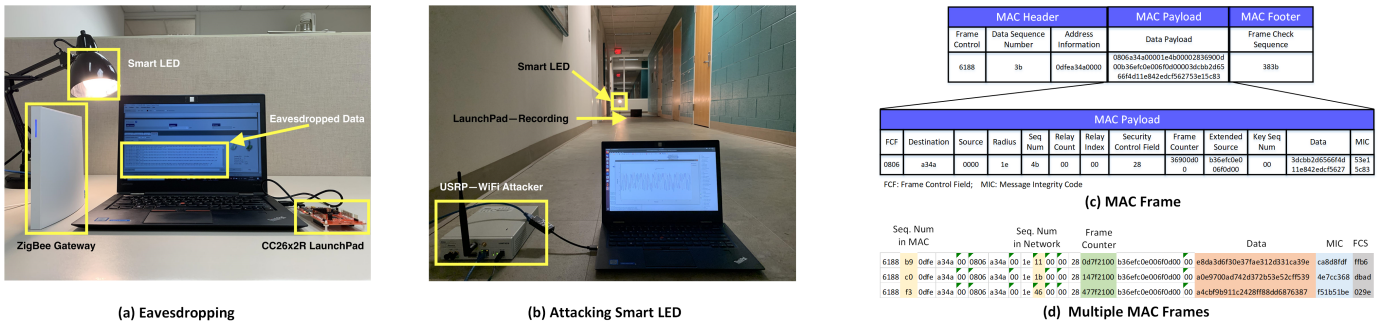
The previous version of this paper was published at the 39th International Conference on Distributed Computing Systems (IEEE ICDCS).

X. Zhang and H. Zhou are with the Department of Computer Science, Florida State University, Tallahassee, FL, 32306. E-mail: xzhang@cs.fsu.edu, hz21e@my.fsu.edu.

†*S. Yu, P. Huang, and L. Guo are with the Department of Electrical and Computer Engineering, Clemson University, Clemson, SC, 29634. E-mail: sihany@g.clemson.edu, peih@g.clemson.edu, linkeg@clemson.edu*

‡ *M. Li is with the Department of Computer Science and Engineering, the University of Texas at Arlington, Arlington, TX 76019. Email: ming.li@uta.edu*

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2022.3169705, IEEE Transactions on Dependable and Secure Computing



(a) Eavesdropping (b) Attacking Smart LED (c) MAC Frame (d) Multiple MAC Frames

Fig. 1: Experiment on the Vulnerability of ZigBee devices

emulation attack, in the heterogeneous environment.

- The proposed passive defense strategy prevents the WiFi attacker from emulating a perfect ZigBee signal by leveraging an anchor, i.e., a smartphone or a software-defined radio (SDR) transmitter, who can send the noise on the same spectrum as the ZigBee signal.
- We also propose a proactive defense strategy to protect ZigBee receiver with the help of the anchor, i.e., a software-defined radio (SDR) WiFi receiver, which can get the QAM symbols from the received signal and determine whether the signal is coming from a valid ZigBee source in a real-time manner.
- We perform extensive experiments to validate threats of the signal emulation attack and further demonstrate the effectiveness of two defense strategies.
- We design a real-world prototype and a smartphone testbed to enable the smartphone to perform the signal emulation attack, while defense strategies are thoroughly evaluated in practical scenarios.

The rest of this paper is organized as follows. Sec.2 illustrates the motivation of signal emulation attack, together with the introduction of a threat model. Sec. 3 gives some background information about the ZigBee receiver and the WiFi transmitter, based on which we demonstrate the details of the signal emulation attack in Sec. 4. As the countermeasures, passive and proactive strategies are proposed in Sec. 5 and Sec. 6, respectively. We give our experimental confirmation of the signal emulation attack as well as evaluation of two defense strategies in Sec. 7. Sec. 8 discusses related work, followed by the conclusion in Sec. 9.

2 Motivation

From the attackers' perspective, when performing attacks to ZigBee devices, one of the major difficulties is the short attacking range (approx. 10m). Due to the limited transmission power, attackers are identified within the line-of-sight (LoS) range. In what follows, we conduct an experiment to demonstrate the limitation of attacking ZigBee devices using the ZigBee protocol, and further discuss the feasibility and severeness of the WiFi-enabled emulation attack.

2.1 Experimental Results and Observations

2.1.1 Experiment Settings

As shown in Fig.1a, we use a Commercial off-the-shelf (COTS) Sylvania ZigBee LED [11] light bulb as the IoT device. We let a gateway send "`TURNING ON`" and "`TURNING OFF`" commands to the LED. The CC26x2R LaunchPad [12] (ZigBee attacker) is deployed to eavesdrop on the communication between the gateway and LED. The command messages are stored and re-sent using both the launchPad and USRP (WiFi attacker) as shown in Fig. 1b, where the USRP sends an emulated signal based on the eavesdropped ZigBee signal. Given the experimental results, we analyze the advantages of using WiFi for launching the attack.

2.1.2 Payload Analysis

We use WireShark [13] to analyze the packets sent by the gateway in Fig.1c. The CC26X2R LaunchPad is deployed to send the eavesdropped ZigBee packet for attacking the LED. Although the commands change over time, the ciphertext form of "`TURNING ON`" shown in the "Data" field can still be re-used on the LaunchPad for turning on the LED as shown in Fig.1d. In our case, the receiver LED does not verify the sequence numbers and frame counters, making it already vulnerable to the replay attack. However, even if the protocol enforces the verification to defend, this type of attack is still possible because of the potential key leakage issue during the initialization process [14–16] especially when there is a new device added into the network [17]. Many cracking tools [18] can be used to steal the keys and finally decrypt the received commands. Therefore, even if ZigBee devices are using symmetric upper-layer encryption schemes, such as AES-CCM, this type of attacker still can change the sequence number and/or frame counters in the decrypted message and then re-encrypt as a new message, achieving the successful replay attack to ZigBee devices.

2.1.3 Attacking Performance Analysis

From the perspective ZigBee devices, given the above vulnerability, they may suffer even more serious attacks in the heterogeneous environment consisting of malicious WiFi attackers because of their advantages as follows.

- **Attacking range**: Adopting IEEE802.15.4 protocols, the transmission power of ZigBee attackers is relatively low at 5dBm, while a common smartphone WiFi transmission power is 6-7 times more than that, making the attacking range greatly improved.
- **Attacker detection**: The low transmission power of ZigBee attackers prevents them from performing the attack at Non Line-of-Sight (NLoS) locations. Thus, they are at a higher risk of being detected. However, the WiFi attacker can stay at NLoS locations to attack ZigBee devices without being found.

- **Device ubiquity**: Compared to WiFi devices that pervasively exist in people's daily life, devices with ZigBee protocol are always fixed at certain places, which reduces the feasibility for attacks.

From the attacker's viewpoint, to verify the feasibility and benefits brought by WiFi protocol, we extend the above experiment by using a USRP to attack LED using both ZigBee signal and WiFi emulated signal (detail will be presented later). We also deploy a LaunchPad next to LED to record received packets.

As shown in Table.1, both the symbol-error-rate (SER) and packet-error-rate (PER) will increase in the LoS scenario for both ZigBee and WiFi attackers, resulting in a significant drop in attack success rate. When both attackers are closer to the LED, their SER and PER remain similar. However, the WiFi attacker has higher attacking success rate as the distance increases to 15m and 20m. In addition, due to the NLoS propagation feature of the WiFi signal, the WiFi attacker can also launch the attack when hiding outside of the house. According to the above discussion, WiFi attackers are more powerful than ZigBee attackers in terms of 1) longer attacking range; 2) NLoS capability; 3) ubiquity of devices. Given these advantages, the resulting consequences would be immense if no prevention mechanism is deployed.

TABLE 1: Symbol/Packet Level Performance (LoS)

Distance	5m	10m	15m	20m
SER (WiFi)	0.55%	0.4%	0.52%	1.23%
PER (WiFi)	0.75%	1.8%	4.1%	4.8%
SER (ZigBee)	0.51%	0.44%	1.34%	2.31%
PER (ZigBee)	1.1%	1.7%	6%	15.2 %

2.2 Threat Model

Motivated by the above observation, we focus on a physical-layer signal emulation attack on ZigBee devices. Instead of launching the attack using ZigBee devices, we consider a WiFi attacker for longer attacking range and higher success rate, for which it can hide somewhere (50m away) without being found. Specifically, the entire signal emulation attack consists of the following steps.

Step 1: Signal Eavesdropping. The WiFi attacker moves close to ZigBee devices to eavesdrop on the communication between ZigBee devices and their authorized gateway.

Step 2: Signal Emulation. The WiFi attacker "translates" the eavesdropped ZigBee signals into its "own language", the emulated signal.

Step 3: Device Attacking. By ensuring the channel is not occupied by ZigBee devices, the WiFi attacker sends the emulated signal via its RF component for attacking purpose.

With this being said, the WiFi attacker follows the IEEE 802.11g standard for physical (PHY) and media access control layer (MAC) when launching the attack. We assume it is able to eavesdrop on the overlapped frequency band between WiFi and ZigBee within a close proximity. The WiFi attacker has the ability of storing the historical knowledge of ZigBee signals, such as eavesdropping time, location, and amplitude. Given previously discussed advantages, the WiFi attacker can be any device with a WiFi radio, which sends signals with a higher power (approx. 8dB higher than ZigBee) at any place within the transmission range. Due to protocol differences, the WiFi capabilities are limited in the following aspects: 1) WiFi attackers are unable to generate a WiFi signal that is completely the same with the eavesdropped ZigBee signal; and 2) WiFi attackers are unable to simply replay and amplify the eavesdropped ZigBee signal.

As for ZigBee devices, they follow the IEEE 802.15.4 standard. Mostly, they are fixed at specific locations, such as kitchen, bedroom, and garage, where they communicate with gateways as usual. In particular, they are unable to detect the existence of WiFi attackers. Most importantly, we assume they cannot distinguish the sources of received signals and can only execute the command as long as the signal passes its security check (in the case where cryptographic keys have been compromised).

3 Preliminaries

Before stepping into the detailed design of signal emulation attack, we first analyze its feasibility by reconsidering the ZigBee transmitter/receiver and WiFi transmitter.

3.1 ZigBee Transmitter and Receiver

ZigBee devices work in the unlicensed 2.4 to 2.4835 GHz ISM bands where 16 channels are allocated. Each channel occupies 2 MHz bandwidth with 5 MHz spaced apart. They apply Direct Sequence Spread Spectrum (DSSS) to improve interference/noise resilience. At the transmitter, each original ZigBee symbol (4 bits) is mapped to a 32-chip sequence by being multiplied by a pseudo-random noise spreading code. Offset Quadrature Phase Shift Keying (OQPSK) is deployed as the modulation scheme, which maps every 2 DSSS chips to one of the 4 complex symbols. At the receiver, after OQPSK decoding, the ZigBee receiver calculates the Hamming distance between received 32-chip sequence and all the 16 predefined 32-chip sequences, where each predefined one corresponds to a ZigBee symbol. The predefined chip sequence having the minimum Hamming distance is chosen as the candidate. Meanwhile, the ZigBee receiver sets a threshold. If the minimum Hamming distance is smaller than the threshold, the received chip sequence is decoded to the ZigBee symbol that the candidate represents. Otherwise, the received chip sequence is discarded.

3.2 WiFi Transmitter

WiFi devices have a higher transmission power and longer transmission range compared to ZigBee devices. They also work in the 2.4GHz ISM band with 20 MHz bandwidth for each channel, which results in the potential spectrum overlapping between the WiFi and ZigBee signals. One example is that the ZigBee signal occupied on channel 17 ($2434-2436$MHz) is completely overlapped with that of the WiFi signal centered on the 2442 MHz ($2432-2452$MHz). WiFi transmitters deploy complete different PHY techniques compared to ZigBee transmitter. In our paper, we mainly consider the following three differences.

3.2.1 Modulation scheme.

WiFi transmitter deploys 64-Quadrature Amplitude Modulation (QAM) followed by the Orthogonal Frequency Division Multiplexing (OFDM). Specifically, after preprocessing (scrambling, encoding, and interleaving), every 6 data bits are mapped to one of the 64 complex symbols on QAM constellation. Every 48 complex symbols together with 4 pilot symbols and 12 null symbols, representing the signal

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2022.3169705, IEEE Transactions on Dependable and Secure Computing

on 64 subcarriers (each occupies 312.5 kHz bandwidth) respectively, form an OFDM symbol [19] in frequency domain. The 64-point Inverse Fast Fourier Transform (IFFT) is then employed, changing the OFDM symbol from the frequency domain to the time domain.

3.2.2 Cyclic Prefix (CP)

After IFFT, a guard interval (CP), which is the repetition of the last 16 complex data, is added to the beginning, forming a complete WiFi symbol with 80 complex data. The CP together with OFDM helps WiFi signals combat multi-path effect by inhibiting inter-symbol interference (ISI) between adjacent OFDM symbols. ZigBee transmitter does not have CP process.

3.2.3 Repetitive Short Training Sequences (STSs)

WiFi receiver calculates the carrier frequency offset (CFO) from the center frequency via auto correlation among 10 repetitive STSs. Each STS contains 16 raw WiFi symbol. Those repetitive STSs do not exist in the ZigBee signals.

In practice, the WiFi device can overhear the ZigBee signal due to spectrum overlapping. However, it cannot generate a signal that is completely the same as the ZigBee signal. Fortunately, the DSSS demodulation allows a few errors in received signals at the ZigBee receiver, which gives attackers opportunities to control ZigBee devices. Based on the above discussion, we list the main challenges in launching signal emulation attack, 1) how to generate a WiFi signal that is similar enough to the actual ZigBee signal? and 2) how to guarantee that the emulated signal can pass the DSSS demodulation and be decoded correctly?

4 Signal Emulation Attack

To answer the above questions, we detail our design in the signal emulation attack in this section.

4.1 Attack Overview

The signal emulation attack is shown in Fig.2. The WiFi attacker eavesdrops on the signal from the communication between ZigBee devices. Then, it generates a signal that is similar to the eavesdropped one. As a result, the emulated signal passes the DSSS demodulation process and the ZigBee device executes the command from the WiFi attacker.

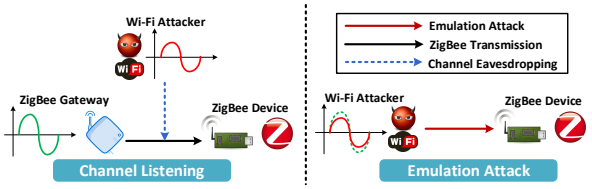


Fig. 2: Cross-Technology Signal Emulation Attack

4.2 ZigBee Signal Eavesdropping

4.2.1 Overview

To launch the attack, the WiFi attacker needs to know the ZigBee transmitter's signal. Locating close to ZigBee devices, the attacker passively senses the channel and records the received ZigBee signal. However, with a 20 MHz sensing bandwidth, the WiFi attacker also senses the signals from other sources, especially the environmental WiFi signals. Thus, the difficulty lies in how to recognize and further capture the ZigBee signal from the received ones.

4.2.2 Short-Distance Eavesdropping

We first conduct an experiment to explain why the WiFi attacker has to eavesdrop on the ZigBee signal from a short distance to ZigBee devices. Two USRPs operating at the Channel 11 (centered at 2405MHz) play roles of the ZigBee transmitter and receiver, respectively. Their distance is set to 0.5m, 1m and 1.5m and 2m, respectively. The ZigBee transmitter randomly sends two signals each time. The real component amplitude of the received signals is shown in Fig.3, where the amplitude of the ZigBee signal decreases with the increase of the distance. When the transmitter is 2m away from the receiver, the ZigBee signal is overwhelmed by the noise. However, the ZigBee signal can still be decoded by the ZigBee receiver due to the error tolerance of DSSS. For the WiFi attacker, unfortunately, with completely different PHY layer techniques, it cannot extract the ZigBee signal from the noise. Therefore, the WiFi attacker has to locate in the close proximity to ZigBee devices to eavesdrop on the ZigBee signal.

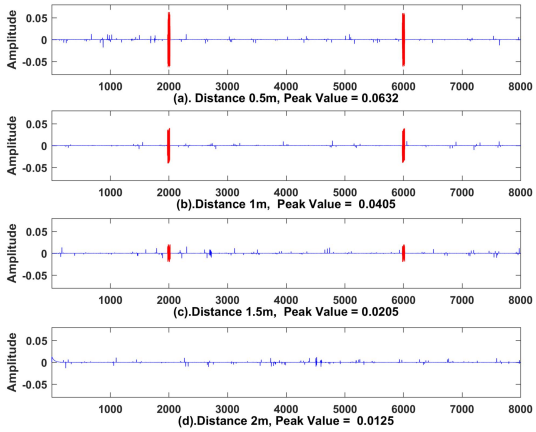


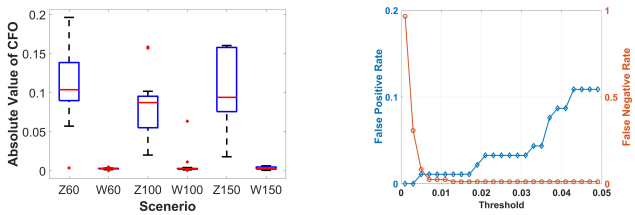
Fig. 3: Received signal at ZigBee receiver

4.2.3 ZigBee Signal Distinguish and Extraction

WiFi attacker distinguishes the ZigBee signal from the view of WiFi frame structure. After detecting a sufficiently high amplitude, WiFi attacker temporarily stores the received signal and calculates the CFO as,

$$f_o = \frac{1}{16} \arg \sum_{n=0}^{N_{STS}-1-16} t[n]t^*[n+16], \qquad (1)$$

where $t[n]$ denotes the n-th STS sample and $N_{STS} = 160$ represents total STS samples. t^* is the complex conjugate of the t. If f_o is above a given threshold, the received signal is supposed to be the ZigBee signal. WiFi attacker stores it for the further emulation. Otherwise, WiFi attacker assumes it as a WiFi signal and begins to decode it.



(a) CFO (b) Accuracy

Fig. 4: Eavesdropping Performance at WiFi attacker

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2022.3169705, IEEE Transactions on Dependable and Secure Computing

An experiment is conducted to verify the above method. Two USRPs send WiFi and ZigBee signals alternately while another USRP plays the role of the WiFi receiver. The distance between the transmitters and receiver is 0.6m, 1.5m and 2m. Each transmitter sends signals 100 times on each location. We illustrate the CFO performance in Fig.4a. The CFO of WiFi signal centralizes at 0 whereas the CFO of ZigBee signal is far larger (e.g., Z60 denotes ZigBee signal at 60cm and W100 denotes WiFi signal at 100cm). Fig.4b shows the eavesdropping accuracy. The false positive rate represents that the received WiFi signal is mistakenly considered to be from the ZigBee transmitter whereas the false negative rate denotes that the received ZigBee signal is regarded as from another WiFi device. As we can see, when the WiFi attacker sets its decision threshold for CFO to around 0.001, it can effectively eavesdrop on ZigBee signal while the WiFi signal receiving is not affected.

Note that WiFi attacker can effectively extract the ZigBee signal without buffer overflow and extra cost as explained in the following. (1), Because WiFi attacker locates near to ZigBee devices, most RF samples with high amplitudes should come from either WiFi or ZigBee devices instead of other devices equipped with different wireless protocols. (2), Since users' operations to smart home ZigBee devices usually have the daily routines, WiFi attacker eavesdrops the ZigBee signal during a fixed period. Hence, WiFi attacker does not have to store the received signal all the time. (3), CFO calculation is the necessary step in signal decoding, there is no extra computational cost at the WiFi attacker.

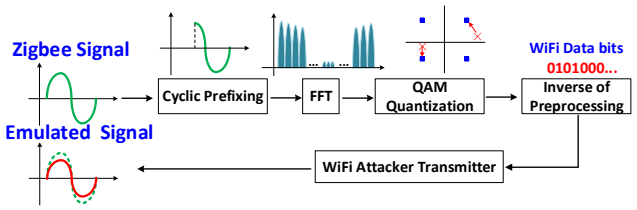


Fig. 5: ZigBee Waveform Emulation

4.3 ZigBee Signal Emulation

The objective of the ZigBee signal emulation is to generate a WiFi signal that is similar to the eavesdropped ZigBee signal. As shown in Fig.5, the attacker processes the eavesdropped signal in a reverse direction to obtain the corresponding WiFi data bits, which are sent to ZigBee devices when launching the attack. We ponder the problem step by step by comparing the difference between the ZigBee and WiFi transmitters.

4.3.1 Cyclic Prefix Manipulation

Each WiFi symbol consists of 80 complex data, including 16 cyclic prefix data followed by the 64 effective data. However, the ZigBee signal does not have such a characteristic. Hence, given 80 eavesdropped data, the attacker inevitably discards the first 16 data and chooses the rest 64 data as the emulation objective. We assume every 64 data to be emulated constructs a sample. Meanwhile, we denote $z(n,s)$, where $n = 1, 2, \cdots, N$ and $s = 1, 2, \cdots, S$, as the n-th data in the s-th sample. We further assume there are S samples in the eavesdropped ZigBee signal and $N = 64$.

4.3.2 Frequency Subcarrier Selection

To get the corresponding WiFi data bits for each raw sample, a 64-point FFT is applied,

$$Z(k,s) = \sum_{n=1}^{N} z(n,s) e^{-j\frac{2\pi}{N}nk}, k = 1, 2, \cdots, K, \quad (2)$$

where the FFT point $Z(k,s)$ denotes the component on the subcarrier k in the s-th raw sample in the frequency domain and $K = 64$. Since each WiFi symbol occupies 20MHz bandwidth with 64 subcarriers whereas 2MHz bandwidth is occupied by the ZigBee signal, only 7 subcarriers ($\frac{2}{20} \times 64$) of the WiFi signal are overlapped with the ZigBee signal. The WiFi attacker emulates the eavesdropped signal by manipulating the components on 7 subcarriers. The question becomes how to locate those subcarriers.

Since the signal on non-overlapped subcarriers is mostly the noise, the signals on overlapped subcarriers is much more powerful. Thus, a folding process is deployed to locate them by considering the energy of the FFT points $E(k,s)$,

$$E(k,s) = Z(k,s)Z^*(k,s), \quad (3)$$

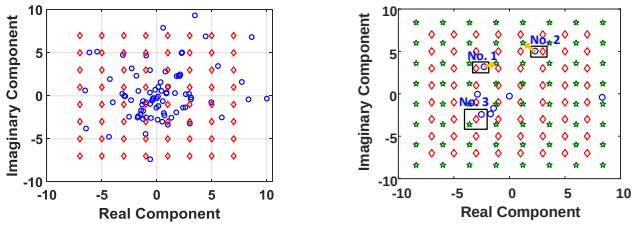
where $Z^*(k,s)$ indicates the conjugate of $Z(k,s)$. The energy $E(k,s)$ forms a two-dimension matrix, where the elements in the kth row indicate the energy of each raw sample on the subcarrier k whereas those in the sth column signify the energy on each subcarrier in the raw sample s. Thus, a histogram $ES(k)$ of $E(k,s)$ is built according to the following equation,

$$ES(k) = \sum_{s=1}^{S} E(k,s), k = 1, 2, \cdots, K, \quad (4)$$

where $ES(k)$ is the total energy of all the samples on the subcarrier k. We sort $ES(k)$ using the merge-sort algorithm [20] to identify the location of 8 most powerful subcarriers. The reason to choose 8 subcarriers instead of 7 is to ensure that the spectrum occupied by the emulated signal completely overlaps that occupied by the ZigBee signal. Here, subcarrier $29 - 36$ are chosen.

4.3.3 64-QAM Quantization Optimization

WiFi and ZigBee signals have different constellation structures. An example is shown in Fig. 6a, where blue circles and red diamonds represent FFT points of the eavesdropped signal and the 64-QAM constellation, respectively. To get WiFi data bits, the WiFi attacker quantizes FFT points to 64-QAM points. Such quantization results in irreversible distortion. WiFi attacker attempts to minimize the quantization distortion.



(a) Constellation Comparison (b) Quantization Errors

Fig. 6: 64-QAM Quantization Optimization

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2022.3169705, IEEE Transactions on Dependable and Secure Computing

Based on the Parseval's theorem view [20], minimizing the signal distortion in the time-domain under energy metric is equivalent to minimizing the total deviation of frequency components after quantization. Hence, our principle is to choose the closest 64-QAM constellation point to each of the FFT points in term of Euclidean distance. Without considering constellation scale, the real and imaginary components of the 64-QAM points, Q_{Re} and Q_{Im}, are chosen from the set {-7, -5, -3, -1, +1, +3, +5, +7}, respectively. To minimize quantization errors, a scalar α is introduced. We have the following optimization problem,

$$\begin{aligned} \min_{\alpha} \quad & \sum_{k=SS}^{SE} \left(Z_{Re}(k,s) - \alpha Q_{Re}(m)\right)^2 + \\ & \left(Z_{Im}(k,s) - \alpha Q_{Im}(m)\right)^2 \\ & \alpha > 0, \end{aligned} \tag{5}$$

where $Z_{Re}(k,s)$ and $Z_{Im}(k,s)$ represent real and imaginary components of the FFT point $Z(k,s)$ respectively. SS and SE denote the start and end locations of the chosen FFT points, respectively. Let $j = \sqrt{-1}$. We have $Z(k,s) = Z_{Re}(k,s) + jZ_{Im}(k,s)$. In particular, $\alpha(Q_{Re}(m) + jQ_{Im}(m))$ indicates the 64-QAM point that is the nearest to the FFT point $Z(k,s)$. The optimization problem (5) aims to find the optimal scalar α such that the total quantization error between the chosen FFT points and their nearest QAM points is minimized. However, we cannot solve the problem directly since different $Q_{Re}(m)$ and $Q_{Im}(m)$ are chosen for the same FFT point $Z(k,s)$ given different scalar αs. For example, we choose 3 FFT points from Fig.6a and mark them as No. 1, 2, and 3 as shown in Fig. 6b. The scalar for the red-diamond 64-QAM constellation is $\alpha = 1$ while that of the green-pentagram 64-QAM constellation is $\alpha = 1.2$. In Fig.6b, the basic QAM point $Q_{Re}(m)$ and $Q_{Im}(m)$ for No.3 FFT point does not change, which is $-3 - 3j$. However, for No.1 FFT point, it is changed from $-3 + 3j$ to $-1 + 3j$ while from $3 + 5j$ to $1 + 5j$ for No.2 FFT point.

Algorithm 1: Quantization Error Minimization

Input: initial start and end of the scalar range α_S and α_E
basic 64 QAM constellation points $Q_{Re}(m)$ and $Q_{Im}(m)$, $m = 1, 2, \cdots, 64$
chosen FFT points from ZigBee signal samples $Z(k,s), k = SS, SS+1, \cdots, SE, s = 1, 2, \cdots, S$ its increasing gap $\delta = 1$
error threshold $\eta = 10^{-5}$
Output: α^*

1 $\hat{e} = 0, \overline{e} = 10^5$;
2 **while** $|\hat{e} - \overline{e}| > \eta$ **do**
3 $M = \alpha_E - \alpha_S/\delta$;
4 $\hat{e} = \overline{e}$;
5 **for** $i = 0; i < M$ **do**
6 $\alpha_i = \alpha_S + i * \delta$; $e_i = 0$;
7 **for** $i = 1; i \leq 8 * S$ **do**
8 **for** $m = 1; m \leq 64$ **do**
9 $D(i,m) = (Z_{Re}(k,s) - \alpha_i Q_{Re}(m))^2 + (Z_{Im}(k,s) - \alpha_i Q_{Im}(m))^2$
10 **end**
11 $E(i) = \min_{0 \leq m \leq 64} D(i,m)$;
12 $k = \arg_{0 \leq i \leq 64} E(i)$;
13 $e_i = e_i + E(k)$
14 **end**
15 **end**
16 $\overline{e} = \min_{0 \leq i \leq M} e_i$; $k = \arg_{0 \leq i \leq M} \overline{e}$;
17 $\alpha_S = \alpha_k - \delta/2$; $\alpha_E = \alpha_k + \delta/2$; $\delta = \delta/10$;
18 **end**
19 $\alpha^* = \alpha_k$;
20 return α^*;

The above result indicates that an optimal scaler definitely exists that results in the least quantization error. We propose a quick algorithm to find the optimal scalar. As shown in Algorithm 1, we define a unit quantization (Line $7 - 14$) as the process that quantizes the FFT points to the 64-QAM points given a scalar and calculates the corresponding quantization error. Our key idea is that: instead of processing each unit quantization given a fixed scalar range $[\alpha_S, \alpha_E]$ with a fixed gap δ, we attempt to minimize the number of unit quantization process with a variable range and gap. As shown in Step 17, we shrink the optimal scalar range and decrease the gap simultaneously. Since the quantization error is a convex function of the scalar, the global optimal scalar is unique [21]. After each unit quantization, a current optimal scalar is found given a scalar range and gap. The global optimal scalar must be around the current one. Hence, after a few iterations, we can get a global optimal scalar.

Next, we demonstrate how the proposed algorithm speeds up the quantization process. Denote the number of the iterations as I_{num}. To ease description, we apply the symbol $'$ on the upper right to represent the initial values while the symbol $*$ to denote the values with the global optimal scalar. Without our algorithm, the unit quantization is processed $\frac{\alpha'_S - \alpha'_E}{\delta^*}$ times to minimize the quantization error by choosing the optimal scalar. Our algorithm reduces the times to $\frac{\alpha'_S - \alpha'_E}{\delta'} + 10I_{num}$, where $\delta^* = \delta' 10^{-I_{num}}$ as shown in Step 17. In the case with more iterations, our algorithm decreases the number of unit quantization processes by about $10^{I_{num}}$ times.

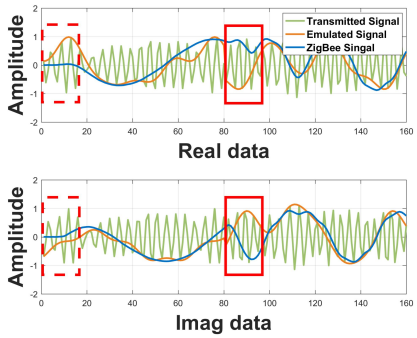


Fig. 7: Eavesdropped Signal Vs. Emulated Signal

After 64-QAM quantization, WiFi data bits are obtained from the inverse process of the interleaver, convolution encoding, and scrambler as in [8]. Those bits are stored in the cache. The WiFi attacker launches the attack by sending them to ZigBee devices.

Fig.7 compares the ZigBee and emulated signals in a general case where ZigBee devices and WiFi attackers are centered in different frequencies, e.g., ZigBee on 2405MHz and WiFi on 2410MHz. The blue lines are the waveform of the ZigBee signal and the orange line represents the emulated signal. Those two waveforms are very similar except those in the red rectangle due to cyclic prefix rules. To achieve the goal of attacking the ZigBee receiver at its operation frequency, the WiFi attacker allocates the subcarriers $13 - 20$ to the emulated signal, which are 16 subcarriers' ahead from the central subcarrier locations $29 - 36$. Hence, the waveform of the transmitted signal is shown as the green lines in Fig.7.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2022.3169705, IEEE Transactions on Dependable and Secure Computing

5 Passive Defense Strategy

5.1 Motivation

The intuition behind our passive defense strategy is that *"Quantitative Changes lead to Qualitative Changes"*. By making trouble to the eavesdropping process, we mislead the WiFi attacker to generate the imperfect emulated signal, which cannot pass the detection at the ZigBee receiver. The proposed approach makes use of an auxiliary WiFi transmitter, for which we refer as an anchor. As shown in Fig. 8, locating near the ZigBee transmitter, the anchor transmits the AWGN noise n_z with the mean 0 and the variance σ^2 when the ZigBee device transmits the signal. The signal received at both the ZigBee receiver and the WiFi attacker becomes,

$$z'(n,s) = z(n,s) + n_z(n,s). \tag{6}$$

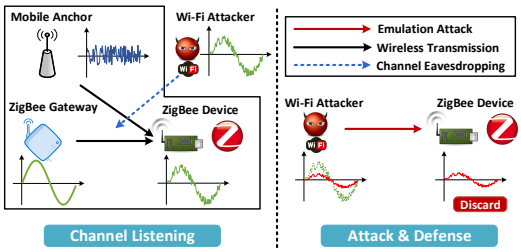


Fig. 8: Passive Defense Model

5.2 Noise Effect to the WiFi Attacker

In the DSSS demodulation, ZigBee devices set a threshold to the number of error chips between the received chip sequence and the predefined ones. In other words, ZigBee devices tolerate a few error chips for each received chip sequence. Therefore, even if the ZigBee receiver receives a signal with a slightly smaller signal-to-noise ratio (SNR), it still can find one predefined chip sequence, which is decoded to the corresponding ZigBee symbol. However, different from the regular decoding process, the noise concealed in the eavesdropped signal would propagate to the signal emulation process at the WiFi attacker, resulting in larger quantization distortion.

As in (6), the signal eavesdropped by the WiFi attacker is a noised ZigBee signal $z'(n,s)$. After the FFT operation, the output is,

$$Z'(k,s) = Z(k,s) + N_Z(k,s), \tag{7}$$

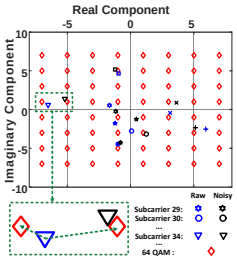
where $N_Z(k,s)$ is the FFT points of the AWGN in the frequency domain. The WiFi attacker quantizes the FFT point $Z'(k,s)$ to a QAM point based on Algorithm 1. Denote the QAM point associated with the FFT point $Z'(k,s)$ as $Q'(k,s)$. After quantization, the square error $e'(k,s)$ between the QAM point and the FFT point of raw signal is,

$$e'(k,s) = \left(Z_{Re}(k,s) - \alpha Q'_{Re}(m)\right)^2 + \left(Z_{Im}(k,s) - \alpha Q'_{Im}(m)\right)^2$$

However, if the anchor does not emit AWGN noise, the square error $e(k,s)$ for the FFT point $Z(k,s)$ is,

$$e(k,s) = \left(Z_{Re}(k,s) - \alpha Q_{Re}(m)\right)^2 + \left(Z_{Im}(k,s) - \alpha Q_{Im}(m)\right)^2 \tag{8}$$

The noise sent by the anchor tempts the WiFi attacker to quantize the FFT point $Z'(k,s)$ to a different QAM point $Q'(k,s)$. The new QAM point is farther to the FFT point $Z(k,s)$ of the ZigBee signal without the added noise, resulting in larger distortion in the emulated signal. To make it more clear, we pick up the noisy FFT points with the variance σ_F^2 in the first sample, $s = 1$, and draw them in Fig. 9 where the optimal scalar is $\alpha = 1$. σ_F^2 is the variance in the frequency domain. For the AWGN, variances in the time domain σ^2 and frequency domain σ_F^2 form a linear relationship. The blue marks in Fig. 9 denote the FFT points without the anchor whereas the black marks represent the FFT points with the added AWGN. We take the FFT point $k = 34$ as an example, which is amplified at lower left. When there is no added noise, the FFT point is quantized to the QAM point $-7 + j$ whereas the quantized QAM point becomes $-5 + j$ affected by the noise, which deviates the FFT point. Such a false quantization results in higher quantization error. The table in Fig. 9 further demonstrates our idea: the quantization error becomes larger when the anchor transmits the AWGN together with the ZigBee transmitter.



Subcarrier	$Q(k,s)$	$e(k,s)$	$Q'(k,s)$	$e'(k,s)$
29	$-1+j$	0.6466	$-1-j$	2.8371
30	$-1-3j$	1.2294	$1-3j$	0.8794
31	$-1-5j$	0.2995	$-1-5j$	0.2995
32	$3-j$	0.3377	$3+j$	2.0649
33	$5-3j$	1.0989	$5-3j$	1.0989
34	$-7+j$	0.3899	$-5+j$	2.4421
35	$-1-j$	0.6528	$1-j$	5.5319
36	$-1+5j$	0.1200	$-1+5j$	0.1199

Fig. 9: Constellation Performance under AWGN Effect

Based on the Parseval's theorem [22], the energy in the time-domain is equalized to that in frequency-domain. Hence, the larger quantization error in the frequency domain results in the larger signal distortion. When the ZigBee device receives such a distorted signal, the chip error exceeds the threshold in DSSS. It discards the received signal. Therefore, the passive defense strategy prevents the WiFi attacker from controlling the ZigBee devices.

In practice, we assume that both the WiFi attacker and the ZigBee transmitter change their transmission power slowly. Even though the WiFi device adapts its transmission power to the wireless environment, the noise with the power comparable to the ZigBee signal does not trigger the transmission power change at the WiFi device. The ZigBee transmitter and the anchor work together to defend against the signal emulation attack. The ZigBee transmitter will not update its transmission power with the changes of noise power from the anchor. Every time ZigBee receiver successfully decodes the signal, it will send an acknowledgment frame to the ZigBee transmitter [23]. If the ZigBee transmitter gets the acknowledgment frame with the incorrect sequence number, it knows that the ZigBee receiver is attacked and allows the anchor to increase its noise power. If the ZigBee transmitter cannot receive the acknowledgment frame after sending the ZigBee signal, it suggests that the noise overwhelms the ZigBee signal reception and thus asks the anchor to decrease its noise power. The above process continues until the feasible noise power is found. To close the defense loop, when the ZigBee transmitter receives the acknowledgment frame with the incorrect sequence number from the ZigBee receiver, it knows that the ZigBee receiver is attacked and thus asks the anchor to send the AWGN noise with the found noise power.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2022.3169705, IEEE Transactions on Dependable and Secure Computing

6 Proactive Defense Strategy

The major shortage in the passive defense strategy is that the added noise level cannot be too high. Otherwise, the ZigBee receiver cannot decode the valid information from the ZigBee transmitter neither. Besides, with the strong computation capability, the WiFi attacker can launch the signal emulation attack via the exhaustive search on its constellation and periodically check the current state of the ZigBee receiver. Hence, new defense strategies are needed.

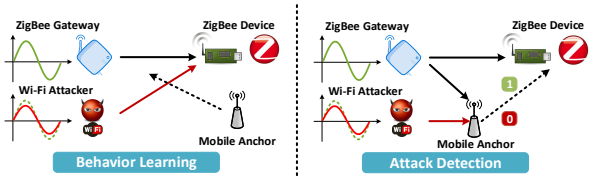


Fig. 10: Proactive Defense Strategy

6.1 Motivation

As shown in Fig.10, the goal of this proactive defense strategy is to distinguish whether the received signal is from the WiFi attacker or the ZigBee transmitter in a real-time manner. To achieve it, the anchor will first proactively learn the behavior of both the WiFi attacker and the ZigBee transmitter from previously received signals. When the new signal is detected, the anchor classifies the signal source based on the historic learning knowledge.

Note that our proactive approach is different from radio frequency fingerprinting techniques [24–27], which leverage the uniqueness in the transmitted signal to localize or identify the specific source based on the analog properties, particularly the presence of analog components in the radio transmission chain. However, our proactive scheme does not differentiate devices. Instead, we use features to find differences between protocols. Besides, our used metric will only be evaluated within each signal (e.g., cosine difference) compared to RF fingerprinting-based approaches applying metrics for comparison of two same-protocol signals.

6.2 Feature Extraction

To identify the differences between the ZigBee signal and emulated signal, the anchor extracts unique features from received signals on both the time and frequency domain.

6.2.1 Time Domain Feature

The cyclic prefix is obtained by prepending a copy of the last 16 complex data from the end to its beginning for the emulated ZigBee sample. With this being said, a circular signal structure appears, i.e., the first 16 data and last 16 data should be the same in each emulated sample. However, the ZigBee signal does not have such property. Therefore, the anchor can check whether the signal has such a circular structure. In particular, the anchor sends the received signal into the folding process after signal alignment. Because there are 80 complex data in each emulated sample, the anchor chooses 80 as the length of each column instead of 64. Denote the folding matrix as $\mathbf{F}$. Its element $F(n,s)$ is the n-th complex data in the s-th signal sample. To be consistent with the previous discussion, there are in total of S signal samples. Theoretically, if the signal comes from the WiFi attacker, the n-th row vector is the same with the $(n+64)$-th row vector in the folding matrix, $i = 1, 2, \cdots, 16$. The cosine distance, which finds the angle between two vectors, is applied to measure the similarity between two row vectors. The value of the cosine distance is close to 1 if the two vectors are similar. To consider the similarity between the first 16 row vectors and the last 16 corresponding ones, we calculated the averaged cosine distance D_F as follows,

$$D_F = \frac{1}{16}\sum_{n=1}^{16}\frac{\sum_{s=1}^{S}F(n,s)F^*(n+64,s)}{\sqrt{\sum_{s=1}^{S}F^2(n,s)}\sqrt{\sum_{s=1}^{S}F^2(n+64,s)}} \quad (9)$$

In addition, we simulate the cosine distance of both the eavesdropped signal and the emulated signal as illustrated in Fig. 11a, from which we see that the first 16 row vectors of the emulated signal and their related vectors in the end are almost the same. Different from this, the corresponding vectors of the ZigBee signal are negatively correlated.

6.2.2 Frequency Domain Features

The largest difference between the eavesdropped and the emulated signal is the constellation difference as shown in Fig.6a. Since the emulated signal is a WiFi signal, its constellation has a squared structure. However, the constellation of the eavesdropped signal does not have such a performance. Therefore, the constellation structure of the received signal is considered for detection.

The 64-QAM constellation has constant normalized fourth-order stimulants C_{40}, C_{41} and C_{42} [28]. Given received signal data $z(n,s)$, the anchor estimates them as follows,

$$\widetilde{C}_{40} = \frac{1}{N*S}\sum_{s=1}^{S}\sum_{i=n}^{N}z^4(n,s) - 3\widetilde{C}_{20}^2$$

$$\widetilde{C}_{41} = \frac{1}{N*S}\sum_{s=1}^{S}\sum_{i=n}^{N}z^3(n,s)z^*(n,s) - 3\widetilde{C}_{20}\widetilde{C}_{21}$$

$$\widetilde{C}_{42} = \frac{1}{N*S}\sum_{s=1}^{S}\sum_{i=n}^{N}|z^4(n,s)| - |\widetilde{C}_{20}|^2 - 2\widetilde{C}_{21}^2 \quad (10)$$

In addition, the second-order moments $\widetilde{C}_{20}$ and $\widetilde{C}_{21}$ are estimated,

$$\widetilde{C}_{20} = \frac{1}{N*S}\sum_{s=1}^{S}\sum_{i=n}^{N}z^2(n,s), \quad \widetilde{C}_{21} = \frac{1}{N*S}\sum_{s=1}^{S}\sum_{i=n}^{N}|z(n,s)|^2.$$

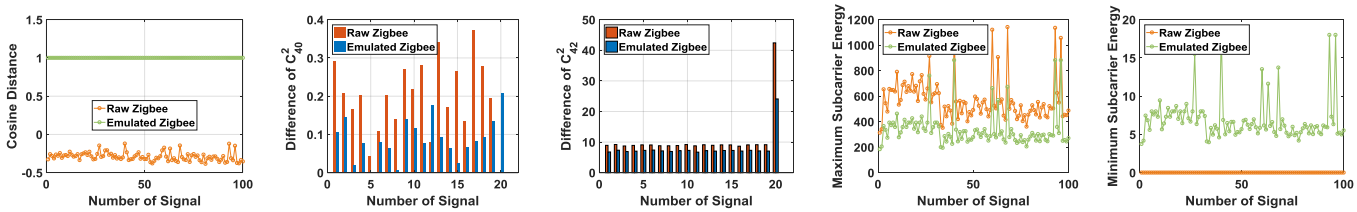
Finally, the normalized second-order moments and fourth-order stimulants are given as,

$$\widehat{C}_{2q} = \widetilde{C}_{2q}/\widetilde{C}_{21}^2, q = 0, 1, \quad \widehat{C}_{4q} = \widetilde{C}_{4q}/\widetilde{C}_{21}^2, q = 0, 1, 2 \quad (11)$$

Their theoretical values are $C_{21} = 1$, $C_{20} = 0$, $C_{40} = C_{42} = -0.6190$ for the 64-QAM constellation.

By comparing the difference between the estimated second-order/fourth-order stimulants and their theoretical values, the anchor can roughly estimate the signal source. If the difference is small, the signal is from the attacker. Otherwise, it is from a ZigBee device. We deploy $(\widetilde{C}_{20} - C_{20})^2$, $(|\widehat{C}_{40}| - |C_{40}|)^2$ and $(\widetilde{C}_{42} - C_{42})^2$ to represent the above features. The reason for the absolute value of C_{40} is to avoid the effect brought by the signal phase rotation in transmission [28]. Their performance is shown in Fig. 11b,

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2022.3169705, IEEE Transactions on Dependable and Secure Computing



(a) Cosine Distance (b) C_{40} Difference (c) C_{42} Difference (d) Maximum Energy (e) Minimum Energy

Fig. 11: Time-domain and Frequency-domain Features

and Fig. 11c, respectively, where the difference between the second-order/fourth-order stimulants and their theoretical values in the emulated signal is smaller than that in the eavesdropped signal.

Besides the features related to stimulants, we consider the energy of the points in the constellations. By investigating Fig. 6a again, we see that the quantization process amplifies the FFT points with the smallest energy and shrinks the FFT points with the largest energy, resulting in their energy changes. We show the comparison of the maximum and minimum energy between the eavesdropped signal and the emulated signal in Fig.11d and Fig.11e, respectively, all of which validate our idea. Therefore, the maximum and minimum energy of the points after FFT operation from the received signal are chosen as the features.

6.3 Data Collection

In the training process, the anchor collects the data from both the WiFi attacker and the ZigBee transmitter based on the following process. As long as it is receiving the signal, the anchor first checks whether the state of the ZigBee receiver changes. If it is not changed, the anchor regards the signal as the emulated signal; otherwise, the anchor inquiries the ZigBee transmitter on whether it has transmitted signal. If it did not send any signal, the anchor likewise regards the signal as the emulated signal. If the ZigBee transmitter sends the signal, the anchor marks it as the signal source.

6.4 Signal Classification

The anchor deploys the binary logistic regression model [29, 30] to distinguish whether the currently received signal is either from the WiFi attacker ('1') or the ZigBee transmitter ('0') by calculating the corresponding probability $P(Y = 1|x)$ and $P(Y = 0|x)$ after extracting the features,

$$P(Y = 1|x) = \frac{exp(\hat{w} \cdot x + \hat{b})}{1 + exp(\hat{w} \cdot x + \hat{b})}$$

and

$$P(Y = 0|x) = \frac{1}{1 + exp(\hat{w} \cdot x + \hat{b})}$$

where x is a feature vector consisting of all the features described above. It denotes the feature extracted from the current received signal. If $P(Y = 1|x)$ is larger than $P(Y = 0|x)$, the anchor decides the signal is from the WiFi attacker; otherwise, the signal is from the ZigBee transmitter.

In particular, $\hat{w} \in \mathbf{R}^n$ and $\hat{b}$ are the estimated parameters learned from the training data set $T = \{(x_1, y_1), (x_2, y_2), \cdots, (x_T, y_T)\}$. They are obtained by maximizing logarithm likelihood $L(w, b)$,

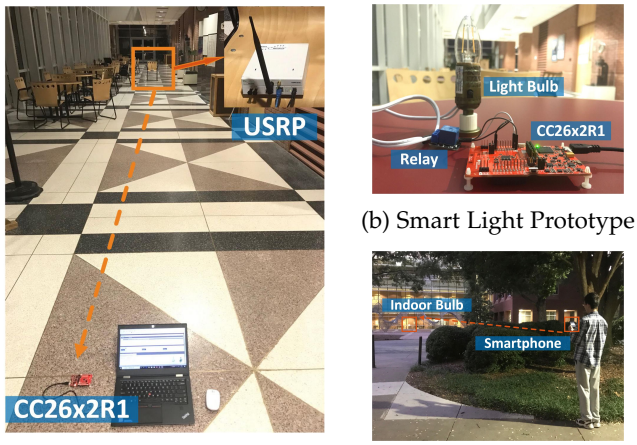
$$L(w, b) = \sum_{i=1}^{T} [y_i(w \cdot x_i) - \log(1 + exp(w \cdot x_i))]. \quad (12)$$

If the anchor verifies that the received signal comes from the WiFi attacker, it will notify the ZigBee receiver by sending a CTC signal [31–33].

7 Performance Evaluation

7.1 Experiment Settings

We implement the emulation attack and its defense strategies on the USRP testbed, the prototype, and the smartphone testbed respectively to thoroughly evaluate their performance.



(a) USRP Testbed (b) Smart Light Prototype (c) Prototype

Fig. 12: Experiment Settings and Prototype

In the USRP testbed, the USRP-N210 is deployed as a WiFi attacker, attempting to control the ZigBee device CC26x2R Wireless MCU LaunchPad as shown in Fig. 12a. Both of them are centered at 2405MHz. The distance between them is set to 5m, 10m, 15m, and 20m, respectively. USRP testbed gives freedom to choose parameters (e.g., transmission power, central frequency, payload length, etc.) for each step in the entire design, which can better simulate different environments.

As assumed in the motivation, we claim the signal emulation attack is severe due to the ubiquity of WiFi devices, where arbitrary devices with WiFi RF can launch the attack. Hence, we also implement experiments on a prototype, where the Nexus 5 smartphone (centered on 2412MHz) attempts to control a smart light prototype (centered on 2412MHz) in both LoS and NLoS as shown in Fig.12c.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2022.3169705, IEEE Transactions on Dependable and Secure Computing

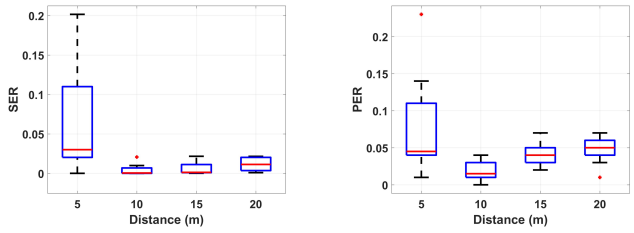
Nexus 5 whose WiFi chip is BCM4339 supports the widely used Nexmon framework which realizes modifications on the WiFi part [34] from a lower level. In Nexmon, we only change the WiFi packet length in order to fit the length of the ZigBee's "TURNING ON" command. To be specific, the length of a WiFi packet normally is around 1500 bytes. If the data is greater than that, it will be divided into several packets. Hence, we use Nexmon to ensure that a larger packet can be transmitted instead of being divided into several packets. In the smart light prototype in Fig.12b, the CC26x2R turns on the common light bulb by triggering a high level to the I/O output D100 as soon as detecting the "`TURNING ON`" command. Because the bulb needs a 110V voltage whereas the maximum supply voltage is 5V on CC26x2R, an extra relay is introduced playing the role of the switch.

To further demonstrate the severeness of the emulation attack from the commercial WiFi card, we conduct the experiments where the above smartphone playing the role of the attacker attempts to manipulate the ZigBee device from the distance of 5m, 10m, 15m, and 20m respectively. The settings of the smartphone are the same as those on the prototype. Note that due to limited RAM, the smartphone cannot continuously eavesdrop the raw ZigBee signal samples. We ask for the help of USRP N210 during the signal eavesdropping process.

7.2 Signal Emulation Attack Performance

7.2.1 USRP Testbed

The attacker USRP sends 100 fixed-length emulated signals to ZigBee device CC26x2R 10 times given each distance. Symbol error rate (SER) denotes the number of symbols that are mistakenly decoded plus the number of symbols that are not received, which are divided by the number of total symbols. Packet error rate (PER) represents the number of emulated signal packet being received with error over the number of total packets. The packet error happens if at least one symbol in it is detected with error. As can be seen in Fig.13, both the SER and PER are small even if the distance between them is long, e.g., 15m and 20m, which demonstrates that WiFi attacker can control the ZigBee device from a longer distance.



(a) SER (b) PER

Fig. 13: Signal Emulation Attack on USRP Testbed

7.2.2 Prototype

The smartphone continuously sends "10000" as the "`TURNING ON`" commands from different locations. A USRP is deployed next to the bulb to help analyze the received signal. The result is illustrated in Table. 2. As the distance increases, both the SER and PER decrease. However, even the distance between the smartphone and the light bulb is beyond 20m, the PER is still very small. In other words, the smartphone successfully controls the ZigBee device from a longer distance, which demonstrates the effectiveness of our signal emulation attack.

TABLE 2: Prototype Signal Emulation Attack Performance

Distance	5m	10m	15m	20m	25m
SER	0.94%	3.26%	10.88%	15.93%	14.25%
PER	0.026%	0.082%	0.25%	0.36%	0.32%

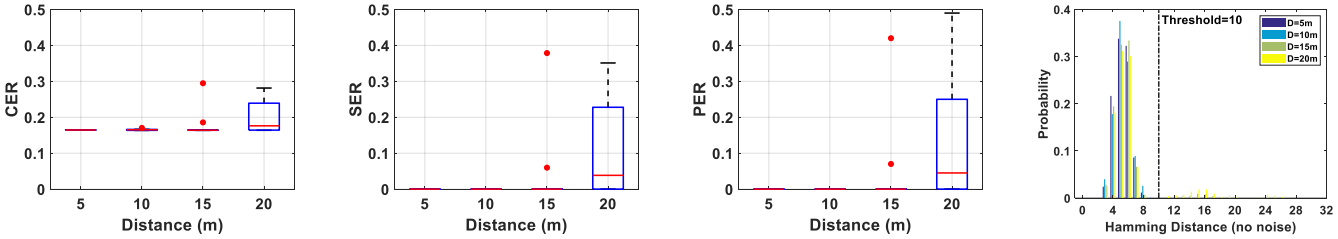
7.2.3 Smartphone Testbed

The smartphone sends 100 fixed-length emulated signal to ZigBee device 10 times given each distance. The transmission power is 40dBm on the smartphone. Chip error rate (CER), SER, PER, and Hamming distance are calculated from the received emulated signal. We depict their performance in Fig.14. When the WiFi attacker is close to the ZigBee device, e.g., 5m and 10m, the CER is around 0.18 in all 10 trials. In that case, the SER and PER approach to 0. Such observations demonstrate that the smartphone can completely attack the ZigBee device from the distance up to 10m. We continue to increase the distance to 20m. In that case, the attacking performance becomes slightly worse. Fortunately, the median SER and PER are under 0.05 although the maximum PER approaches to 0.5, demonstrating that the emulation attack launched by the smartphone is successful most of the time. Digging deep into the reason why the emulation attack is successful, we further analyze the distribution of Hamming distance where the threshold is set to the normal value 10. The number of different chips between the predefined chip sequence and the received chip sequence in each ZigBee symbol is mainly within the threshold expect for the cases under the distance 15m and $20m$, which means that the ZigBee receiver cannot map those received chip sequences to the predefined ones and thus drop them. That is reason why the SER and PER performance becomes worse. Overall, we can conclude from the experiment on smartphone testbed that the smartphone attacker can control the ZigBee device by launching our proposed attack from the distance up to 20m.

7.3 Passive Defense Strategy

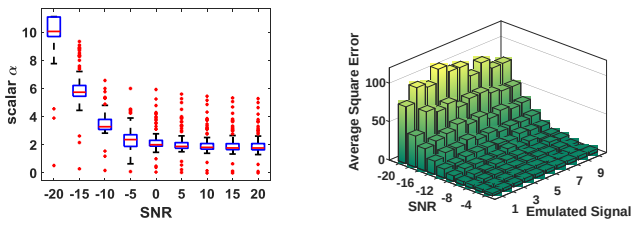
To evaluate the passive defense strategy, we deploy another USRP to perform as the anchor in both the USRP testbed and prototype, which transmits the AWGN with the ZigBee signal simultaneously during the eavesdropping phase. The ZigBee signal-to-noise ratio (SNR) is set from -20dB to 30dB. During the attacking process, we mainly consider the LoS case in USRP testbed and both the LoS and NLoS cases in prototype. In addition, in our smartphone testbed, a smartphone Nexus 5 equipped with NEXMON firmware, as an anchor, and an USRP N210 send the AWGN and the ZigBee signal respectively at the same time. The SNR ranges from -5dB to 20dB. Two USRP N210s next to each other, playing the role of the ZigBee receiver and the eavesdropper respectively, receive the noised ZigBee signal simultaneously. We use the USRP as the ZigBee receiver to better analyze the noise effect to benign ZigBee signal reception whereas the other USRP helps the attacker to eavesdrop the noised ZigBee signal. The eavesdropped signal is then given to the other smartphone Nexus 5 for launching the signal emulation attack.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2022.3169705, IEEE Transactions on Dependable and Secure Computing



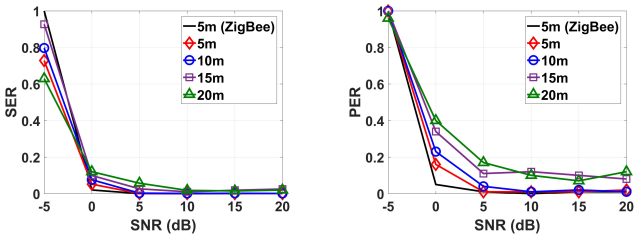
(a) CER (b) SER (c) PER (d) Hamming Distance

Fig. 14: Signal Emulation Attack on Smartphone Testbed



(a) α Vs. SNR (b) Average Square Error

Fig. 15: Quantization Performance



(a) CC26x2R SER (b) CC26x2R PER

Fig. 16: Effects on Error Rate

7.3.1 USRP Testbed

At the above locations, the WiFi attacker transmits 100 emulated noised signal 10 times. We show the effectiveness of the passive defense strategy from the following aspects.

Effect on the Quantization. We illustrate scalar α and the average square error associated with it in Fig.15a and Fig. 15b. When the SNR is under 0dB, a large scalar α is generated and results in a high average square error. This is because the noise with a high power brings a negative effect to the constellation quantization of the eavesdropped signal. Each FFT point of the eavesdropped signal is quantized to the 64-QAM point that is far away from itself.

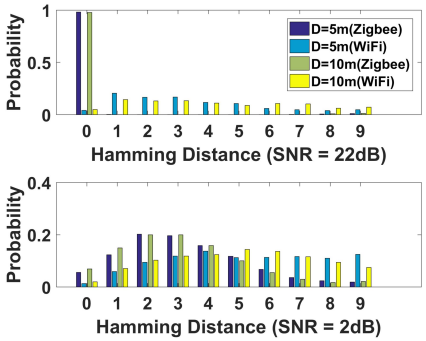


Fig. 17: Hamming Distance Performance

Effect on Hamming Distance. In Fig.17, we illustrate the Hamming distance distribution for both the received ZigBee signal and emulated signal when the anchor generates the AWGN with the high SNR (22dB) and low SNR (2dB). The threshold of Hamming distance is set to 10. When the SNR is 22dB, most Hamming distance of ZigBee signal is around 0 and 1 whereas that of emulated signal is distributed among $2-9$. The ZigBee receiver decodes all the chips correctly. As the distance increases, the Hamming distance of the emulated signal becomes larger. Due to noise tolerance, the ZigBee receiver still decodes the emulated signal to correct symbols. However, when the SNR is 2dB, many chips are incorrectly decoded. The ZigBee receiver cannot recognize the emulated signal. WiFi attacker do not control the ZigBee devices.

Effect on SER and PER. We evaluate the SER and PER from the receivers' perspective. As we can see in Fig.16, the SER and PER of both the ZigBee and emulated signal are very high when the SNR is below 0dB. The receiver decodes neither of them. When the SNR is above 5dB, the SER and PER of them approach to 0. The ZigBee receiver decodes both of them. When the SNR is between 0dB and 5dB, both SER and PER of ZigBee signal approach to 0 while the PER of the emulated signal is high, especially when the distance is larger. The receiver only decodes the ZigBee signal. The above analysis demonstrates that our passive defense strategy can effectively protect the ZigBee device from being attacked by WiFi attackers, particularly those who attempt to control the ZigBee device from a longer distance.

7.3.2 Prototype

The smartphone attempts to control the bulb from locations $L1$ to $L7$ in the building whose floor map is shown in Fig.18. Specifically, WiFi attacker locates at $L1$, $L2$ and $L4$ attacks the bulb in LoS. When the smartphone is at $L3$, $L5$, $L6$ or $L7$, it attempts to turn on the bulb without being found (NLOS). The SNR increases from -2dB to 30dB during the eavesdropping phase.

The success rate of turning on the bulb is illustrated in Fig. 19. When the SNR is low, e.g., -2dB and 2dB, WiFi attacker only turns on the bulb in LoS case. As the SNR increases, indicating the added AWGN is decreasing, the success rate also increases. When it increases to 26dB and 30dB, the noise variance is so small that it cannot bring any trouble to the WiFi attacker. WiFi attacker turns on the smart light prototype at all the marked locations, including many NLoS locations. The above observation also echos the

effectiveness of our signal emulation attack in both LoS and NLoS case.

Fig. 18: Building Map 1

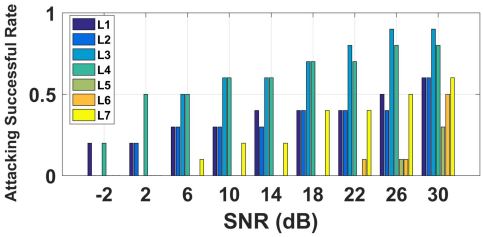
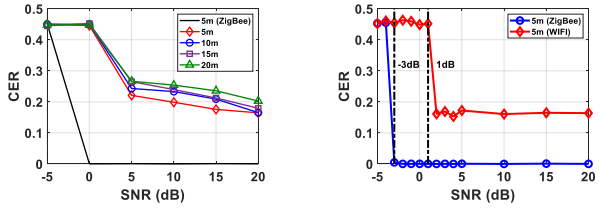
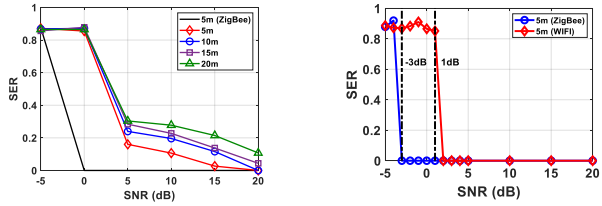


Fig. 19: Defensive Performance in Prototype



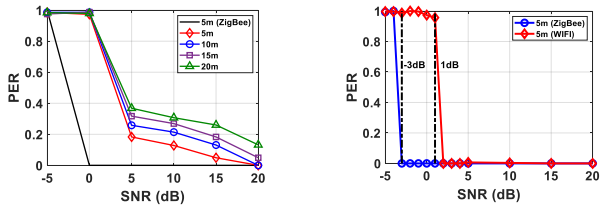
(a) (b)

Fig. 20: CER Performance



(a) (b)

Fig. 21: SER Performance



(a) (b)

Fig. 22: PER Performance

7.3.3 Smartphone Testbed

Similar to the USRP testbed, the smartphone transmit 100 emulated noised signal 10 times. We show the effectiveness of the passive defense strategy from the following aspects.

Effect on CER, SER, and PER. Strong noise carried by the anchor not only obstructs the eavesdropping procedure from the attacker but also brings the potential risk of overwhelming the benign ZigBee signal, causing a high

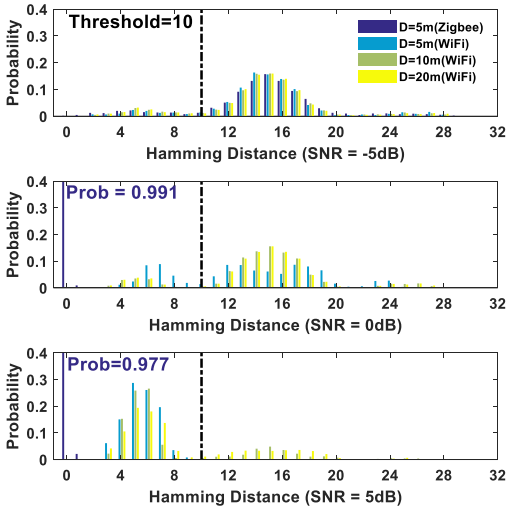


Fig. 23: Hamming Distance Performance

error rate at the Zigbee receiver. We calculate the CER, SER, and PER from the received noised ZigBee signal and the emulated signal. The distance between the ZigBee transmitter and receiver is 5m whereas the smartphone attacker launches the emulation attack from a distance of 5m, 10m, 15m, and 20m to the ZigBee receiver. The CER, SER, PER performance is shown in Fig. 20, 21, and 22 respectively.

We first consider the scenario where the distance from the ZigBee transmitter/the smartphone to the ZigBee receiver is 5m. When SNR is -5dB, the CER calculated from the received noised ZigBee signal and the emulated signal in Fig.20a is close to 0.45, resulting the high SER in Fig.22a and PER in Fig. 22a. In other words, with a higher-power noise, although our passive defensive strategy prevents the ZigBee device from being controlled, it deteriorates the benign ZigBee signal reception. The Hamming distance performance in Fig. 23 further proves the above observations, where the number of different chips between the predefined chip sequence and the received noised/emulated chip sequence mainly falls into the interval between 10 and 20. Given the threshold 10, the ZigBee receiver cannot decode the received signal. Fortunately, as depicted in Fig.20a, 21a, and 22a, when SNR is increased to 0dB, the CER, SER, and PER calculated from the noised ZigBee signal all decrease to 0, demonstrating that the ZigBee receiver is back to work. However, the smartphone fails to manipulate the ZigBee receiver as those error rates do not have any changes compared to their performance under the SNR -5dB. We can also tell the fact from the Hamming distance performance with SNR 0dB in Fig. 23 that the number of different chips under the noised ZigBee signal is equaled to 0 with the probability of 0.991 while that under the emulated signal is larger than the threshold 10 with a higher probability. When we continue to increase the SNR, the error rates calculated from the emulated signal begin to decrease, which means that the WiFi attacker has the opportunity to successfully launch the emulation attack. As a proof, from Fig. 23, we can see that most Hamming distance with SNR 5dB under the emulated signal runs into the threshold of 10, for which

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2022.3169705, IEEE Transactions on Dependable and Secure Computing

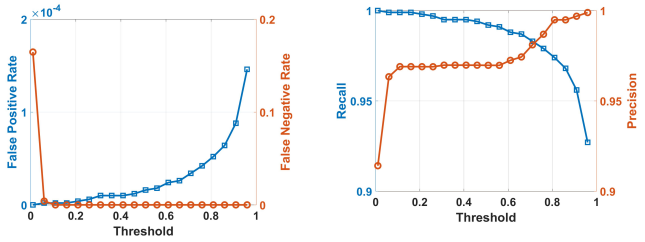
the ZigBee receiver can also decode the emulated signal. However, we can see from the Fig. 21a and 22a that the attacker cannot fully control the ZigBee device even at the SNR as high as 20dB over the distance of 10m, indicating that the passive defense strategy still works for defending against the long-range eavesdropping.

Boundary of effective defense. Fig. 20a, 21a and 22a demonstrate that the best SNR that enables the passive defensive strategy is within -5dB to 5dB. To find the optimal SNR, we investigate the error rate performance with the SNR set from -5dB to 5dB increased by 1dB every step. As illustrated in Fig. 20b, when the SNR is lower than -3dB, the CER of the benign ZigBee signal is around 0.45, resulting in a higher value in SER and PER shown in Fig.21b and Fig.22b respectively. The ZigBee receiver is significantly interfered by the noise and. As the SNR increases, all the error rates decrease to 0, illustrating that the ZigBee receiver can tolerant the noise and decode all the packets. However, the error rates of the emulated signal keeps high until the SNR reaches to 2dB, after which emulated signal can also be decoded by the ZigBee receiver.

From the experiment on smartphone testbed, we conclude the safe SNR range in our passive defensive strategy is $[-3dB, 2dB)$, within which the WiFi attacker fails to launch the emulation attack from a longer distance than 5m while the begin ZigBee signal reception is not interfered. It is necessary to mention that SNR within the safe range provides a robust guarantee of security to ZigBee receiver and the SNR higher than the upper bound can still somehow defend against the emulation attack from the smartphone.

7.4 Proactive Defense Strategy

In our proactive strategy, a USRP, as the anchor, is put next to ZigBee devices to help distinguish the signal source. Note that we consider the normalized maximum energy and minimized energy instead of extracting them directly.

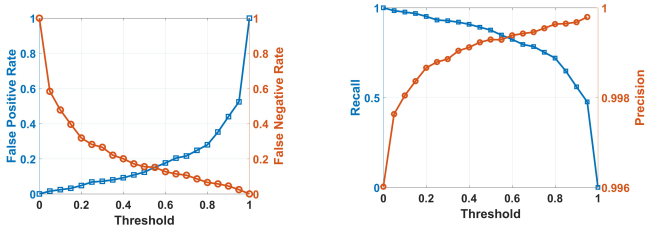


(a) ROC Curve (b) Recall and Precision

Fig. 24: Detection Performance in USRP Testbed

7.4.1 USRP Testbed

We randomly generate 1000 ZigBee signal, which are eavesdropped by the WiFi attacker. Then, it generates the corresponding emulated signal. The original ZigBee signal and the emulated ones are sent to the ZigBee device respectively. Half of the received emulated signal is put into the training set and the others are to be classified. The operation of the ZigBee signal is the same. The experimental results are shown as a Receiver Operating Characteristic (ROC) curve in Fig.24a. The false positive rate represents that the emulated signal is mistakenly considered to be from the ZigBee transmitter whereas the false negative rate denotes that the ZigBee signal is regarded as from the WiFi attacker. In the LoS case, both the false positive rate and false negative rate approach to 0 due to the existence of the powerful anchor. In addition, we demonstrate the recall and precision performance in Fig.24b. The recall value represents the capability of identifying the WiFi attacker whereas the precision value denotes the capability of recognizing the ZigBee transmitter from the received signal. When the detection threshold is set to around 0.7, both the recall and precision value are near to 1, in the sense that the anchor effectively identifies both the WiFi attacker and ZigBee transmitter.



(a) ROC Curve (b) Recall and Precision

Fig. 25: Detection Performance in Prototype

7.4.2 Prototype

The WiFi attacker attempts to control the bulb from the LoS locations $L1$ and $L2$ together with NLoS locations $C1$, $C2$ and $C3$. The USRP receives 500 emulated signals and ZigBee signal, respectively. Half of both received signals are put into the training set and the others are going to be classified. As we can see from Fig.25, when the detection threshold is set to 0.5, both false positive and negative rates approach to 0.2 while the precision is near to 0. The anchor can effectively identify the received signal source.

7.5 Results from Field Experiments

7.5.1 Experiment Settings

To further verify the effectiveness of emulation attack and defense strategies, we conduct field experiments in a larger space, where the end-to-end distance is more than two times of the previous building. Due to the complicated floor plan as given in Fig. 26, we can carry out more experiments in the extreme NLoS case.

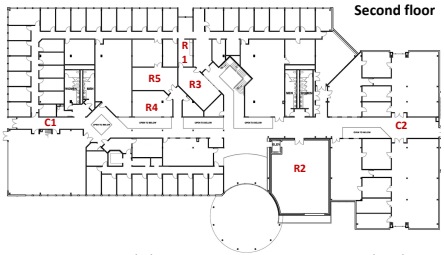


Fig. 26: Building Map 2 – Second Floor

Specifically, we test the results on emulation attack to the commodity Sylvania ZigBee LED. The launchpad CC26x2R is always placed close to LED to show the symbol/packet level performance. A USRP is placed at location C1 on the second floor. For the LoS case, we move LED from USRP location to the end of the hallway $C2$. The distance from $C1$ to $C2$ is 80m. For the NLoS, we place the LED in room R1, R2, R3, and the end of the hallway on the first floor C2′. The distance between R2 and C1 is around 60m. The emulation signal has to pass through other rooms, e.g., R3, R4, R5, before being received at R1. The USRP sends the

"TURNING ON" command that includes 49 ZigBee symbols 500 times to turn on the LED. As an attacker, the USRP sends the emulated command with the gain value 20dB, which indicates the amplification factor in hardware before sending the signal out [35]. As a ZigBee transmitter, the USRP transmits the received ZigBee command with the gain value 12dB. Since the maximum power of WiFi transmission on the smartphone (e.g., Samsung Galaxy series) is 13dBm whereas that on ZigBee devices is 5dBm, gain value settings are to ensure the maximum power ratio between WiFi and ZigBee.

7.5.2 Signal Emulation Attack Performance

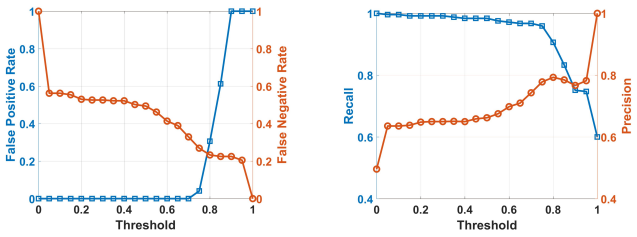
In the field experiment, the LED is turned on after receiving either emulated or ZigBee "TURNING ON" command in LoS case. In NLoS case, the LED is on for the above four locations only when the USRP sends emulated signals. The signal performance on CC26x2R gives similar results. As in Table.3, when the USRP sends the emulated command, the signals received by CC26x2R have a lower SER. The received packet is supposed to be incorrect if one of the symbols is not correctly received. Hence, the PER is relatively high. However, it is much smaller than that when the USRP sends the ZigBee. Even worse, being placed at R2, the CC26xR even cannot receive the ZigBee signal. The above results validate our intuition that ZigBee devices are more easily controlled by WiFi devices from NLoS locations.

TABLE 3: Symbol/Packet Level Performance

Location	C2	C2′	R1	R2	R3
SER (WiFi)	16.09%	9.15%	34.25%	23.09%	11.78%
PER (WiFi)	44.60%	44.30%	62.70%	57.60%	36.50%
SER (ZigBee)	16.07%	6.06%	53.81%	N/A	11.12%
PER (ZigBee)	44.30%	19.10%	83.20%	N/A	32.90%

7.5.3 Proactive Defense Strategy

To distinguish the signal source, a USRP is deployed next to the Smart LED. Similarly, it receives 500 emulated signals and original ZigBee signals (including both LoS and NLoS), respectively. The result is shown in Fig.27. When the detection threshold is lower than 0.8, the anchor would not ignore the emulated signal, but it is possible that the anchor mistakenly regards the ZigBee source as WiFi attacker. When the detection threshold is set above 0.8, the distinguishing result is reversed. When the threshold is set to around 0.8, the anchor gets a balance between the false positive rate and the false negative rate. Shown in Fig.27b, the recall and precision value approaches to 0.8 simultaneously when the threshold is set between 0.8 and 0.9, in the sense that the anchor can effectively identify both the ZigBee receiver and WiFi attacker.



(a) ROC Curve (b) Recall and Precision

Fig. 27: Detection Performance in Field Experiments

8 Related Work

8.1 Security in Smart Home IoT

The application of IoT in smart home have brought our lives substantial conveniences. However, it also introduces potential security threats. According to [36], those threats lie in the device firmware [37–39], communication protocols [40–42], and home automation applications [42–44]. Specifically, communication security research emphasizes the security and privacy issues in smart home communication protocols such as BLE, ZigBee, and Z-Wave [36]. In [42] a worm attack exploiting an implementation bug in the ZigBee Light Link protocols is descried, which has the potential of massive spread. Another security and privacy threat in communication protocols come from different types of traffic analysis. Abbas *et al.* in [45] detect and identify the types of IoT devices, their states, and ongoing user activities by only passively sniffing and analyzing the network traffic from smart home devices and sensors. OConnor *et al.* in [46] classify users' behaviors and the hidden activities performed by devices by extracting features of connection oriented application data unit exchanges. Different from the above work, our proposed security threat comes from the physical layer. By utilizing the fact of weak verification to the ZigBee data in MAC layer, the WiFi attacker can successfully launch the eavesdropping attack and further control the ZigBee device by sending the emulated signal. Compared with the above work, our proposed attack has the following two advantages: (1) it happens in the local environment without the need of the network; (2) it brings the direct detrimental effect to IoT devices.

8.2 Solutions to PHY Security Problems

Physical-layer security problems mostly focus on how to prevent attacks (e.g., eavesdropping and interception) during the communication. Corresponding defense strategies can be categorized into two groups. One is to theoretically discuss the secrecy capacity, which exploits the property of the wireless channel for secure communication [47, 48]. Many transmission strategies, such as cooperative transmission [49], artificial noise [50], and secure beamforming [51], are proposed to enhance the security capacity in the physical layer. The other group is to embed the private permit into the message to prevent it from being replayed, such as RF fingerprinting in [24, 52, 53] and authentication signal embedding in [54–60]. However, the above methods cannot prevent the signal from being eavesdropped and emulated.

8.3 Cross-Technology Communication

Cross-Technology Communication (CTC) is envisioned to serve as an effective approach to alleviate the cross-technology interference by allowing direct communication between devices with different protocols [31, 61–63]. B^2W^2 [9] enables the high throughput and long distance concurrent N-way CTC between BLE and WiFi by leveraging channel state information. In FreeBee [33], Esense [31] and GSense [64], the communication between WiFi and ZigBee devices is enabled by using RSS to measure the WiFi signal. Different from the above packet-level CTCs, Li *et. al* in [8] propose a physical-level emulation technique. Although the objective in above work is to increase the throughput in CTC, it leads to new security issues.

8.4 Security Challenges and Solutions in CTC

The research in CTC brings new security challenges. Wi-attack in [65] uses the WiFi device to conduct poisonous impersonation attacks to iBeacon services by emulating redundant iBeacon advertisements. The attack is based on WiFi to BLE communication. Since BLE and ZigBee deploy different protocols, e.g., IEEE802.15.1 for BLE and IEEE802.15.4 for ZigBee, Wi-attack cannot be used to attack ZigBee devices. Chen *et. al* in [66] present a active jamming attack on the CTC links from WiFi to ZigBee, the protocols over which construct the un-regular energy characteristics to embed CTC bits at packet level. The major difference between the jamming attack in [66] and our signal emulation attack is: the former attack degrades the CTC decoding performance by attacking existing packet-level CTC protocols [31, 67, 68] while the latter attack manipulates ZigBee devices based on the bit-level WiFi to ZigBee communication. The way to consider CTC as an attacking method has been taken into account in our previous work [69, 70]. Particularly, in [69], a defensive strategy is proposed to seek the WiFi attacker from the normal ZigBee devices based on constellation higher-order statistical analysis. In [70], we put more efforts on the authorization code embedding approach in order to differentiate whether the signal comes from a legitimate CTC device or an illegitimate CTC device. However, the ZigBee signal eavesdropping, as the foundation of attacking the ZigBee device, is missing in [69]. Meanwhile, the proposed defense approach only takes the constellation feature into consideration. As an extension, in this paper, we propose a ZigBee signal eavesdropping approach as well as two defensive strategies, where no actions have to be taken at the ZigBee receiver by using the passive defensive strategy and more features are considered to classify the ZigBee and emulated signals in the proactive strategy. The process of attacking ZigBee devices is improved as well. In addition, we implement the complete attacking process and defensive strategies on the real-world testbeds and our self-designed prototypes, where the distance between the WiFi attacker and the ZigBee receiver is up to 20m.

8.5 RF Fingerprinting

Most radio fingerprinting methods identify a device by considering various PHY layer classification approaches. Based on [24], RF features are broadly classified into: (1) channel-specific ones, e.g., channel impulse response, that characterize the wireless channel. They have been successfully adopted in robust location distinction [25, 26]; (2) Transmitter-specific ones that are independent of the channel, e.g., artifacts of individual wireless frames [24], unique features in the radio turn-on transients [27], and joint time-frequency Gaborand Gabor-Wigner Transform features [71]; and (3) Hardware properties like TCP and ICMP time stamp in [72]. All the above work apply radio fingerprint techniques to distinguishing different wireless devices whiles our proactive defense strategy is to differentiate signals generated based on different protocols. In other words, our strategy still works even if the ZigBee device is changed to a new (unknown to the classifier) one.

9 Conclusion

In this paper, we identify a new physical-layer based attack, cross-technology signal emulation attack, where the WiFi attacker controls the ZigBee device by emulating the eavesdropped ZigBee signal. To combat this attack, we introduce an anchor to safeguard the ZigBee communication. In the passive defense strategy, the anchor transmits the AWGN to prevent the WiFi attacker from successfully emulating the perfect ZigBee signal. Whereas in the proactive defense strategy, the anchor receives the signal and identifies the signal source in real time. We implement our design on USRP testbeds, the commodity smart LED, our self-designed prototype and the smartphone testbed. Extensive experiments are performed, demonstrating both the feasibility of signal emulation attack and the effectiveness of the defense strategies.

Acknowledgement

The work of L. Guo was supported by National Science Foundation under grant IIS-1949640 and CNS-2008049. The work of M. Li was partially supported by National Science Foundation under grant CNS-1943509.

References

[1] B. L. R. Stojkoska and K. V. Trivodaliev, "A review of internet of things for smart home: Challenges and solutions," *Journal of Cleaner Production*, vol. 140, pp. 1454–1464, 2017.

[2] "Iot report how internet of things technology is now reaching mainstream companies and consumers," https://www.businessinsider.com/internet-of-things-report, 2020.

[3] I. D. Corporation, "The growth in connected iot devices is expected to generate 79.4zb of data in 2025, according to a new idc forecast," https://www.idc.com/getdoc.jsp?containerId=prUS45213219, Jun. 2019.

[4] D. Tse and P. Viswanath, *Fundamentals of wireless communication*. Cambridge university press, 2005.

[5] D. Croce, N. Galioto, D. Garlisi, F. Giuliano, and I. Tinnirello, "An inter-technology communication scheme for wifi/zigbee coexisting networks," in *Proceedings of the 2017 International Conference on Embedded Wireless Systems and Networks*. Junction Publishing, 2017, pp. 305–310.

[6] F. Li, J. Luo, G. Shi, and Y. He, "Art: Adaptive frequency-temporal co-existing of zigbee and wifi," *IEEE Transactions on Mobile Computing*, vol. 16, no. 3, pp. 662–674, 2017.

[7] Y. Li, Z. Chi, X. Liu, and T. Zhu, "Passive-zigbee: Enabling zigbee communication in iot networks with 1000x+ less power consumption," in *Proceedings of the 16th ACM Conference on Embedded Networked Sensor Systems*. ACM, 2018, pp. 159–171.

[8] Z. Li and T. He, "Webee: Physical-layer cross-technology communication via emulation," in *Proceedings of the 23rd Annual International Conference on Mobile Computing and Networking*. ACM, 2017, pp. 2–14.

[9] Z. Chi, Y. Li, H. Sun, Y. Yao, Z. Lu, and T. Zhu, "B2w2: N-way concurrent communication for iot devices," in *Proceedings of the 14th ACM Conference on Embedded Network Sensor Systems CD-ROM*. ACM, 2016, pp. 245–258.

[10] X. Guo, Y. He, X. Zheng, L. Yu, and O. Gnawali, "Zigfi: Harnessing channel state information for cross-technology communication," in *Proceedings of ACM INFOCOM*, 2018.

[11] Amazon, "Sylvania dimmable led lamp, a19," https://www.amazon.com/SYLVANIA-SmartThings-Required-Assistant-Packaging/dp/B0197840KQ/ref=sr_1_5?ie=UTF8&qid=1529017285&sr=8-5&keywords=zigbee+bulb, 2018.

[12] T. Instruments, "Simplelink multi-standard cc26x2r wireless mcu launchpad development kit," http://www.ti.com/tool/LAUNCHXL-CC26X2R1, Jun. 2017.

[13] "Wireshark," https://www.wireshark.org/, 2019.

[14] P. Jokar, N. Arianpoo, and V. C. M. Leung, "Spoofing prevention using received signal strength for zigbee-based home area networks," in *2013 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, Oct 2013, pp. 438–443.

[15] S. Michaels, K. Akkaya, and A. Selcuk Uluagac, "Inducing data loss in zigbee networks via join/association handshake spoofing," in *2016 IEEE Conference on Communications and Network Security (CNS)*, Oct 2016, pp. 401–405.

[16] Y. Sharaf-Dabbagh and W. Saad, "On the authentication of devices in the internet of things," in *2016 IEEE 17th International Symposium*

on A World of Wireless, Mobile and Multimedia Networks (WoWMoM), June 2016, pp. 1–3.
[17] X. Fan, F. Susan, W. Long, and S. Li, "Security analysis of zigbee," https://courses.csail.mit.edu/6.857/2017/project/17.pdf, 2017.
[18] "Ubiqua protocol analyzer," https://www.ubilogix.com/ubiqua/, 2019.
[19] A. Goldsmith, *Wireless communications*. Cambridge university press, 2005.
[20] T. H. Cormen, C. E. Leiserson, R. L. Rivest, and C. Stein, *Introduction to algorithms*. MIT press, 2009.
[21] S. Boyd and L. Vandenberghe, *Convex optimization*. Cambridge university press, 2004.
[22] E. W. Weisstein, ""parseval's theorem." from mathworld–a wolfram web resource," http://mathworld.wolfram.com/ParsevalsTheorem.html.
[23] "Ieee 802.15.4 stack user guide," https://www.nxp.com/docs/en/user-guide/JN-UG-3024.pdf, 2016.
[24] V. Brik, S. Banerjee, M. Gruteser, and S. Oh, "Wireless device identification with radiometric signatures," in *Proceedings of the 14th ACM international conference on Mobile computing and networking*. ACM, 2008, pp. 116–127.
[25] Z. Li, W. Xu, R. Miller, and W. Trappe, "Securing wireless systems via lower layer enforcements," in *Proceedings of the 5th ACM workshop on Wireless security*. ACM, 2006, pp. 33–42.
[26] N. Patwari and S. K. Kasera, "Robust location distinction using temporal link signatures," in *Proceedings of the 13th annual ACM international conference on Mobile computing and networking*. ACM, 2007, pp. 111–122.
[27] B. Danev and S. Capkun, "Transient-based identification of wireless sensor nodes," in *Proceedings of the 2009 International Conference on Information Processing in Sensor Networks*. IEEE Computer Society, 2009, pp. 25–36.
[28] A. Swami and B. M. Sadler, "Hierarchical digital modulation classification using cumulants," *IEEE Transactions on communications*, vol. 48, no. 3, pp. 416–429, 2000.
[29] N. M. Nasrabadi, "Pattern recognition and machine learning," *Journal of electronic imaging*, vol. 16, no. 4, p. 049901, 2007.
[30] A. Criminisi, J. Shotton, E. Konukoglu *et al.*, "Decision forests: A unified framework for classification, regression, density estimation, manifold learning and semi-supervised learning," *Foundations and Trends® in Computer Graphics and Vision*, vol. 7, no. 2–3, pp. 81–227, 2012.
[31] K. Chebrolu and A. Dhekne, "Esense: communication through energy sensing," in *Proceedings of the 15th annual international conference on Mobile computing and networking*. ACM, 2009, pp. 85–96.
[32] W. Jiang, Z. Yin, S. M. Kim, and T. He, "Transparent cross-technology communication over data traffic," in *IEEE INFOCOM 2017-IEEE Conference on Computer Communications*. IEEE, 2017, pp. 1–9.
[33] S. M. Kim and T. He, "Freebee: Cross-technology communication via free side-channel," in *Proceedings of the 21st Annual International Conference on Mobile Computing and Networking*. ACM, 2015, pp. 317–330.
[34] "The c-based firmware patching framework for broadcom/cypress wifi chips that enables monitor mode, frame injection and much more," https://github.com/seemoo-lab/nexmon, 2017.
[35] "Role of gain in usrp," http://lists.ettus.com/pipermail/usrp-users_lists.ettus.com/2017-May/053025.html, 2017.
[36] W. Zhou, Y. Jia, Y. Yao, L. Zhu, L. Guan, Y. Mao, P. Liu, and Y. Zhang, "Discovering and understanding the security hazards in the interactions between iot devices, mobile apps, and clouds on smart home platforms," in *28th {USENIX} Security Symposium ({USENIX} Security 19)*, 2019, pp. 1133–1150.
[37] S. Notra, M. Siddiqi, H. H. Gharakheili, V. Sivaraman, and R. Boreli, "An experimental study of security and privacy risks with emerging household appliances," in *2014 IEEE conference on communications and network security*. IEEE, 2014, pp. 79–84.
[38] S. A. Christiaens, "Evaluating the security of smart home hubs," 2015.
[39] Z. Ling, J. Luo, Y. Xu, C. Gao, K. Wu, and X. Fu, "Security vulnerabilities of internet of things: A case study of the smart plug system," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1899–1909, 2017.
[40] B. Fouladi and S. Ghanoun, "Honey, i'm home!!, hacking zwave home automation systems," *Black Hat USA*, 2013.
[41] R. Goyal, N. Dragoni, and A. Spognardi, "Mind the tracker you wear: a security analysis of wearable health trackers," in *Proceedings of the 31st Annual ACM Symposium on Applied Computing*, 2016, pp. 131–136.
[42] E. Ronen, A. Shamir, A.-O. Weingarten, and C. O'Flynn, "Iot goes nuclear: Creating a zigbee chain reaction," in *2017 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2017, pp. 195–212.
[43] E. Fernandes, J. Jung, and A. Prakash, "Security analysis of emerging smart home applications," in *2016 IEEE symposium on security and privacy (SP)*. IEEE, 2016, pp. 636–654.
[44] Z. B. Celik, L. Babun, A. K. Sikder, H. Aksu, G. Tan, P. McDaniel, and A. S. Uluagac, "Sensitive information tracking in commodity iot," in *27th {USENIX} Security Symposium ({USENIX} Security 18)*, 2018, pp. 1687–1704.
[45] A. Acar, H. Fereidooni, T. Abera, A. K. Sikder, M. Miettinen, H. Aksu, M. Conti, A.-R. Sadeghi, and S. Uluagac, "Peek-a-boo: I see your smart home activities, even encrypted!" in *Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, 2020, pp. 207–218.
[46] T. OConnor, R. Mohamed, M. Miettinen, W. Enck, B. Reaves, and A.-R. Sadeghi, "Homesnitch: behavior transparency and control for smart home iot devices," in *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*, 2019, pp. 128–138.
[47] A. D. Wyner, "The wire-tap channel," *Bell system technical journal*, vol. 54, no. 8, pp. 1355–1387, 1975.
[48] H. Fang, L. Xu, and X. Wang, "Coordinated multiple-relays based physical-layer security improvement: A single-leader multiple-followers stackelberg game scheme," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 1, pp. 197–209, 2018.
[49] Y. Zou, X. Wang, and W. Shen, "Optimal relay selection for physical-layer security in cooperative wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 10, pp. 2099–2111, 2013.
[50] S. Liu, Y. Hong, and E. Viterbo, "Practical secrecy using artificial noise," *IEEE Communications Letters*, vol. 17, no. 7, pp. 1483–1486, 2013.
[51] W.-C. Liao, T.-H. Chang, W.-K. Ma, and C.-Y. Chi, "Qos-based transmit beamforming in the presence of eavesdroppers: An optimized artificial-noise-aided approach," *IEEE Transactions on Signal Processing*, vol. 59, no. 3, pp. 1202–1216, 2011.
[52] W. Hou, X. Wang, and J.-Y. Chouinard, "Physical layer authentication in ofdm systems based on hypothesis testing of cfo estimates," in *2012 IEEE International Conference on Communications (ICC)*. IEEE, 2012, pp. 3559–3563.
[53] O. Ureten and N. Serinken, "Wireless security through rf fingerprinting," *Canadian Journal of Electrical and Computer Engineering*, vol. 32, no. 1, pp. 27–33, 2007.
[54] V. Kumar, J.-M. Park, and K. Bian, "Blind transmitter authentication for spectrum security and enforcement," in *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2014, pp. 787–798.
[55] L. Yang, Z. Zhang, B. Y. Zhao, C. Kruegel, and H. Zheng, "Enforcing dynamic spectrum access with spectrum permits," in *Proceedings of the thirteenth ACM international symposium on Mobile Ad Hoc Networking and Computing*. ACM, 2012, pp. 195–204.
[56] V. Kumar, J.-M. Park, T. C. Clancy, and K. Bian, "Phy-layer authentication by introducing controlled inter symbol interference," in *Communications and Network Security (CNS), 2013 IEEE Conference on*. IEEE, 2013, pp. 10–18.
[57] X. Jin, J. Sun, R. Zhang, Y. Zhang, and C. Zhang, "Specguard: Spectrum misuse detection in dynamic spectrum access systems," in *2015 IEEE Conference on Computer Communications (INFOCOM)*. IEEE, 2015, pp. 172–180.
[58] X. Jin, J. Sun, R. Zhang, and Y. Zhang, "Safedsa: Safeguard dynamic spectrum access against fake secondary users," in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2015, pp. 304–315.
[59] L. Y. Paul, J. S. Baras, and B. M. Sadler, "Physical-layer authentication," *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 1, pp. 38–51, 2008.
[60] X. Tan, K. Borle, W. Du, and B. Chen, "Cryptographic link signatures for spectrum usage authentication in cognitive radio," in *Proceedings of the fourth ACM conference on Wireless network security*. ACM, 2011, pp. 79–90.
[61] Y. Zhang and Q. Li, "Howies: A holistic approach to zigbee assisted wifi energy savings in mobile devices," in *INFOCOM, 2013 Proceedings IEEE*. IEEE, 2013, pp. 1366–1374.
[62] X. Zhang and K. G. Shin, "Cooperative carrier signaling: Harmonizing coexisting wpan and wlan devices," *IEEE/ACM Transactions on Networking (TON)*, vol. 21, no. 2, pp. 426–439, 2013.
[63] X. Zheng, Y. He, and X. Guo, "Stripcomm: Interference-resilient cross-technology communication in coexisting environments," in

IEEE Int. Conf. Comput. Commun.(INFOCOM), 2018, pp. 15–19.

[64] X. Zhang and K. G. Shin, "Gap sense: Lightweight coordination of heterogeneous wireless devices," in *INFOCOM, 2013 Proceedings IEEE*. IEEE, 2013, pp. 3094–3101.

[65] X. Na, X. Guo, Y. He, and R. Xi, "Wi-attack: Cross-technology impersonation attack against ibeacon services," in *2021 18th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)*. IEEE, 2021, pp. 1–9.

[66] G. Chen and W. Dong, "Jamcloak: Reactive jamming attack over cross-technology communication links," in *2018 IEEE 26th International Conference on Network Protocols (ICNP)*, Sep. 2018, pp. 34–43.

[67] Z. Chi, Z. Huang, Y. Yao, T. Xie, H. Sun, and T. Zhu, "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*. IEEE, 2017, pp. 1–9.

[68] X. Guo, X. Zheng, and Y. He, "Wizig: Cross-technology energy communication over a noisy channel," in *IEEE INFOCOM 2017-IEEE Conference on Computer Communications*. IEEE, 2017, pp. 1–9.

[69] X. Zhang, P. Huang, L. Guo, and Y. Fang, "Hide and seek: Waveform emulation attack and defense in cross-technology communication," in *2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS)*. IEEE, 2019, pp. 1117–1126.

[70] S. Yu, X. Zhang, P. Huang, L. Guo, L. Cheng, and K. Wang, "Authctc: Defending against waveform emulation attack in heterogeneous iot environments," in *Proceedings of the 15th ACM Asia Conference on Computer and Communications Security*, 2020, pp. 20–32.

[71] D. R. Reising, M. A. Temple, and M. E. Oxley, "Gabor-based rf-dna fingerprinting for classifying 802.16 e wimax mobile subscribers," in *2012 International Conference on Computing, Networking and Communications (ICNC)*. IEEE, 2012, pp. 7–13.

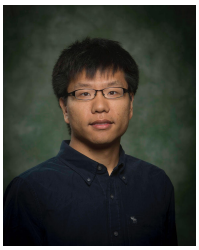
[72] T. Kohno, A. Broido, and K. C. Claffy, "Remote physical device fingerprinting," *IEEE Transactions on Dependable and Secure Computing*, vol. 2, no. 2, pp. 93–108, 2005.

Xiaonan Zhang received the M.S. degree in Electrical and Computer Engineering from Binghamton University, State University of New York, Vestal, NY, USA, in 2017, and the Ph.D. degree in Computer Engineering from Clemson University, Clemson, SC, USA, in 2020. She is currently an Assistant Professor in the Department of Computer Science at Florida State University, Tallahassee, FL, USA. Her research spans over general areas of wireless communication and networking, Internet of Things (IoT), and wireless security with an emphasis on interference mitigation, resource allocation, and physical-layer security in a heterogeneous wireless environment. She is a member of the IEEE and ACM.

Sihan Yu received the BE degree in computer science and technology from Liaoning University, Liaoning, China, in 2013, the ME degree in Control Engineering from University of Chinese Academy of Sciences, Beijing, China, in 2016, and the MS degree in Computer Engineering from Virginia Tech, VA, USA, in 2018. He is currently working toward the PhD degree at Clemson University, SC, USA. His research interests include cross-technology communication, physical layer security in wireless network and the Internet of Things. He is a student member of the IEEE.

Hansong Zhou received his B.E. degree in Information Technology from Xi'an Jiaotong University in 2019 and his M.S. degree in Electrical and Computer Engineering from the University of Florida in 2021, respectively. He is currently a Ph.D. student in the Department of Computer Science at Florida State University. His recent research interests are in the area of resource allocation in edge computing and the security in wireless network.

Pei Huang received her B.S degree from Xidian University, Xi'an, China in 2015 and M.S degree from SUNY at Binghamton in 2017. She got her doctorate degree in Computer Engineering at Clemson University in 2021. Her research interests cover the security and privacy in eHealth/mHealth system, wireless networks, machine learning, and crowdsensing, with a focus on the security problems regarding physical layer properties in the Internet of Things (IoTs) recently.



Linke Guo received the BE degree in electronic information science and technology from the Beijing University of Posts and Telecommunications in 2008. He received the MS and PhD degrees in electrical and computer engineering from the University of Florida in 2011 and 2014, respectively. From August 2014 to August 2019, he was an assistant professor at the Department of Electrical and Computer Engineering, Binghamton University, State University of New York. Starting from August 2019, he has been an assistant professor with Department of Electrical and Computer Engineering, Clemson University. His research interests include wireless network, IoT, security and privacy. He is currently serving as the editor of IEEE Transactions on Vehicular Technology. He also serves as the poster/demo chair of IEEE INFOCOM 2020-2021. He was the publication chair of IEEE Conference on Communications and Network Security (CNS) 2016 and 2017. He was the symposium co-chair of Network Algorithms and Performance Evaluation Symposium, ICNC 2016. He has served as the Technical Program Committee (TPC) members for several conferences including IEEE INFOCOM, ICC, GLOBECOM, and WCNC. He is the co-recipient of Best Paper Award of Globecom 2015, Symposium on Communication and Information System Security. He is a senior member of the IEEE and a member of ACM.

Ming Li received the B.E. degree in Electrical Engineering from Sun Yat-sen University, China, in 2007, the M.E. degree in Electrical Engineering from Beijing University of Posts and Communications, China, in 2010, and the Ph.D. degree in Electrical and Computer Engineering from Mississippi State University, Starkville, in 2014, respectively. She is currently an associate professor in the Department of Computer Science and Engineering, The University of Texas at Arlington. Her research interests include mobile computing, internet of things, security, and privacy-preserving computing. Her work won Best Paper Awards in Globecom 2015 and DASC 2017, respectively. She received the NSF CAREER Award in 2020 and is a member of the IEEE and the ACM.