DOI: 10.19884/j.1672-5220.202411003

Security Defenses for Cross-Technology Communication in IoT Control System

LI Tianyun, ZHANG Anqi, ZHANG Guanglin *
College of Information Science and Technology, Donghua University, Shanghai 201620, China

Abstract: To solve security problems in cross-technology communication (CTC), we take the Internet of Things (IoT) control system as an example, and propose a comprehensive solution against the attack on the physical layer CTC from ZigBee to Wi-Fi. Specifically, we propose a noise interference strategy by adding an appropriate amount of dedicated noise signals, which can interfere with the eavesdropping and simulation of ZigBee signals without affecting the reception of the receiver. Moreover, we also propose a regression modeling strategy which collects data, extracts features, and trains a binary logistic regression model so that the receiver can actively distinguish simulated attack signals. We build the experimental platform by using GNU Radio and USRP devices. Experimental results demonstrate that the security defense strategies can identify and distinguish the signals from the attacker with a high accuracy, effectively solving the signal emulation attack on the physical layer CTC from ZigBee to Wi-Fi.

Keywords: cross-technology communication; Internet of Things (IoT); intelligent control; security defense strategy
CLC number: TN918.91 **Document code**: A
Article ID: 1672-5220(2025)05-0503-10

Open Science Identity (OSID)

0 Introduction

Wi-Fi[1-2], ZigBee[3-4], Bluetooth[5], LoRa[6], RFID[7] and other wireless technologies are widely used in various fields such as smart home, smart wearable, smart medical and smart industry. However, due to their operation in the same frequency band, the coexistence of these technologies in the same application field often leads to serious interference problems such as channel competition, signal collision and throughput reduction. As shown in Fig. 1, especially in the 2.4 GHz frequency band, the spectrum overlap phenomenon of various wireless signals is severe. It has been proven that Wi-Fi and ZigBee interfere with each other in the real-world environment, and the packet loss rate of ZigBee fluctuates between 0% and 85% depending on various Wi-Fi traffic loads[8].

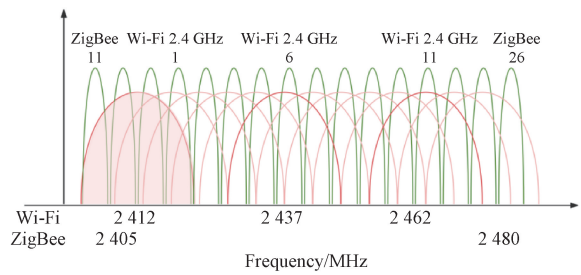


Fig. 1 Spectrum distribution of Wi-Fi and ZigBee in 2.4 GHz frequency band

Cross-technology communication (CTC) is emerged to solve the above interference problem that is caused by the coexistence of multiple technologies, and to achieve the connection and collaborative work between different wireless technologies without the need for gateways. Recently, CTC has shown broad application prospects in various fields.

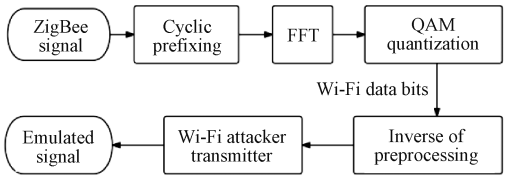
Specifically, Wi-Fi access points in a smart home environment can dynamically assign priorities to sensor nodes based on different scenarios, effectively managing and coordinating the coexistence of multiple heterogeneous wireless devices[9-10]. The PTrack platform of health monitoring utilizes CTC to not only accelerate the upload speed of health data, but also broaden the monitoring scope[11].

Although CTC has brought many conveniences to the development of the Internet of Things (IoT), it still has new security risks. Specifically, CTC allows heterogeneous devices to communicate without gateway authentication, such as bypassing the gateway to invade the smart home system and opening the smart door lock. Moreover, a malicious device would mimic normal devices in CTC, making it impossible to distinguish between homogeneous devices and heterogeneous devices. For example, in agricultural automatic control systems, attackers can eavesdrop on and mimic ZigBee signals from sensors, which causes the Wi-Fi receiver to obtain incorrect parameters and thus make wrong decisions.

Recently, most related works have studied the security issue in CTC. JamCloak raised security and privacy issues such as advertisement pushing and data

Received date: 2024-11-05
* Correspondence should be addressed to ZHANG Guanglin, email: glzhang@dhu.edu.cn
Citation: LI T Y, ZHANG A Q, ZHANG G L. Security defenses for cross-technology communication in IoT control system[J]. *Journal of Donghua University (English Edition)*, 2025, 42(5): 503-512.

stealing[12]. Attackers can also use heterogeneous communication technique to conduct mimicry attacks, stealing or tampering with sensor data to control IoT devices, which can lead to serious security issues[13]. As shown in Fig. 2, an attacker can use Wi-Fi to imitate ZigBee signals and tamper with the data collected by sensors, causing the Wi-Fi control device to obtain incorrect information and then issue wrong instructions after intelligent decision-making. In Fig. 2, quadrature amplitude modulation (QAM) is a modulation method that modulates the amplitude of two orthogonal carriers.



FFT—fast Fourier transform.

Fig. 2 Signal simulation attack in IoT

Existing CTC research focuses on the enhancement of the data transmission rate, synchronisation capability, and anti-jamming capability in data sharing and fusion of wireless heterogeneous devices. Strip-Comm[14] and FreeBee[15] employed strategies such as Manchester coding and folding technologies to resist noise, respectively. AdaComm[16] and C-chirp[17] improved the reliability of channel state information (CSI). PRComm adopted a related decoding strategy to improve the synchronization and anti-interference of CTC[18]. X-burst contributed to optimizing the energy transmission efficiency of CTC[19]. G-Bee was proposed to synchronise the transmission of ZigBee signals[20]. NETCTC provided a feedback mechanism for cross protocol data transmission[21]. However, these related studies focus on the implementation and optimization of CTC, and neglect the security issue, which is our main consideration.

Based on these, we propose a strategy combining noise interference and detection to defend against cross-technology signal emulation attacks. The noise interference uses ZigBee's direct sequence spread spectrum (DSSS) coding error tolerance, misleading attackers into eavesdropping on distorted signals after QAM quantization. The regression modeling strategy extracts features from signals using time-domain cyclic prefix and frequency-domain constellation features, training a binary logistic regression model. This model recognizes signal sources at the Wi-Fi receiver, continuously improves performance, and distinguishes emulated signals. The GNU Radio 3.8, USRP 2953R and DHT11 sensor are used in the experiment, and the data from the DHT11 sensor is transmitted through a ZigBee transmitter.

Our contributions are summarized as follows.

1) We present a comprehensive solution against cross-technology attacks in IoT intelligent control systems, which can significantly reduce the risk of receiving imitation data from attackers at the decision-making end and improve the security and reliability of data transmission.

2) We employ a noise interference strategy to interfere with the eavesdropping of attackers. Meanwhile, we employ a regression modeling strategy to enable the Wi-Fi receiving decision devices to distinguish attack signals.

3) We conduct experiments on GNU Radio 3.8 and USRP 2953R devices to verify the effectiveness and practicality of the proposed security defense strategies by simulating the CTC process.

1 Related Work

1.1 Packet-level CTC

Packet-level CTC utilizes packet-level features to construct a side channel that can effectively communicate data information across protocols between heterogeneous devices by simultaneously addressing both the sender and receiver.

1.1.1 CTC based on received signal strength indicator (CTC-RSSI)

The transmitter and receiver create recognizable sequences by using the signal strength for cross-technology data. Packet energy, length, interval, etc., are adjusted to form received signal strength indicator (RSSI) features. Wi-Fi transmit packet transmission causes ZigBee to receive a 1-bit high RSSI, and no transmission results in a 0-bit low RSSI. WiZig boosts data rates by varying Wi-Fi transmit power[22]. HoWiES establishes a mapping table between the sender and receiver[23]. EMF alters the signal duty cycle by the packet order, using the Morse code for bit transfer[24].

1.1.2 CTC based on channel state information (CTC-CSI)

The overlapping of heterogeneous wireless signals in the frequency domain supports CTC based on CSI. Wi-Fi 802.11a/g/n uses 20 MHz channels that are divided into 64 sub-channels, with CSI indicating states (amplitude and phase) on sub-carriers[25]. CSI is more stable and resistant to interference than RSSI. CTC via CSI features, waveform and frequency bias at Wi-Fi Rx is feasible. The use of support vector machines to make judgments on CSI sequences is proposed in ZigFi[25]. C-chirp sends packets on ZigBee channels, varying the CSI linearly at the Wi-Fi receiver within 60 m[17].

However, packet-level CTC is relatively simple and compatible, and its data transmission rate is significantly limited, i.e., only a few hundred bits per second to a few kilobits per second. In our paper, we focus on physical-layer-level CTC, which can further improve the transmission efficiency and has been widely studied in recent years.

1.2 Physical-layer-level CTC

Transparent CTC at the receiver side is a method that

allows the receiver side to directly decode other heterogeneous wireless signals without any modifications. WeBee provided a physical-layer waveform simulation-based approach[26]. If the transmitter does not require any modifications, it is a transparent CTC on the transmitter. It fully utilizes the computing power of the receiver to achieve reverse transmission of CTC from low-end wireless devices to high-end wireless devices, and its core idea is cross mapping[27]. Non-transparent CTC is the scenario in which both the transmitter and the receiver make hardware modifications or firmware upgrades. These techniques can be used to improve the performance of CTC or to achieve concurrent transmission of multiple cross-technology data. For TwinBee, the distribution of symbol errors was explored by decoding Wi-Fi analogue signals at the ZigBee receiver side, and a code-slice combining approach was proposed to recover the erroneous decoded bits at the receiver side[28].

In practice, the physical-layer-level CTC may cause decoding errors once it receives the waveform or phase effects of noise and attacks. Therefore, it is more susceptible to noise or attacks. Unfortunately, these related studies do not consider the security issue in CTC.

2 Background

2.1 Transparent CTC on transmitter

Transparent CTC at the transmitter end implies that the transmitter requires no modifications and fully leverages the computing power of the receiver to achieve reverse cross-technology information transmission from low-end wireless devices to high-end wireless devices. The core idea of this technology is cross-mapping[27], which realizes the transmission and decoding of cross-technical information through the mapping relationship between the signal at the transmitter and the signal decoded by the receiver. SymBee is a novel ZigBee-to-Wi-Fi CTC method with symbolic-level encoding[29]. It is one of the transparent CTC at the transmitter end. After investigating the existing research at home and abroad, it is found that the scenario of imitating ZigBee to attack ZigBee data link through Wi-Fi has occurred from time to time. This attack technique has been described in detail in the IoT house published by Zhang et al.[13]. It can be inferred that SymBee also has the risk of ZigBee being imitated.

2.2 Software and hardware platform construction

GNU Radio is a framework designed to assist wireless communication developers in designing, building and implementing wireless communication systems. It offers comprehensive processing modules for complex signal processing applications. GNU Radio has been applied to a wide range of practical systems, including audio processing, mobile communications, satellite communications, radar systems and software-defined radio systems.

USRP is a software defined radio device that can be used to flexibly build individual signal processing functions. The USRP 2953R used in this paper (shown in Fig. 3) provides high bandwidth and high dynamic processing capability, consists of a Xilinx field programmable gate array (FPGA) module, dual analog-to-digital converters (ADCs) with a transmission rate of 200 million samples per second (MS/s), dual digital-to-analog converters (DACs) with a transmission rate of 200 MS/s and Gigabit Ethernet ports or 10 Gigabit Ethernet ports. The device is capable of operating between 1.2 GHz and 6.0 GHz, and can be extended to support multiple-input multiple-output (MIMO) configurations. We use the 120 MHz version for the system.

Fig. 3 USRP 2953R used in experiment

3 IoT Intelligent Control System Design

Most existing IoT intelligent control systems rely on gateways to convert different communication protocols and restrict the access of illegal devices. Gateways can effectively prevent information leakage and malicious tampering, thereby ensuring the security of IoT intelligent control systems. However, in this paper, the IoT intelligent control system that we design is based on the SymBee CTC mode without gateways, which increases the risk of being attacked.

We illustrate a general diagram of IoT intelligent control system in Fig. 4. In an IoT intelligent control system, the ZigBee transmitters of ZigBee sensors (such as temperature sensors and humidity sensors) utilize the SymBee CTC method to send the collected data to the Wi-Fi receiver (such as smartphones) for processing and analysis.

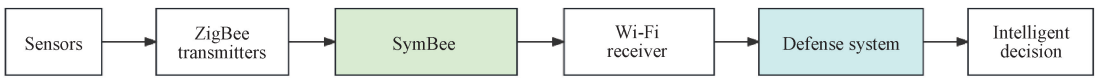


Fig. 4 General diagram of IoT intelligent control system

3.1 ZigBee transmitters

In the IoT intelligent control system, the sensors use the ZigBee transmitters to send collected data to the Wi-Fi receiver for processing and analysis.

1) Data source. DHT11 is a digital sensor that can detect humidity and temperature simultaneously. The internal structure of DHT11 is demonstrated in Fig. 5. GND represents ground. VDD provides positive voltage to the power supply. MCU is an integrated circuit chip.

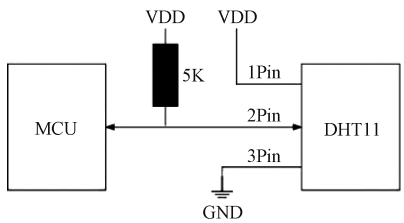
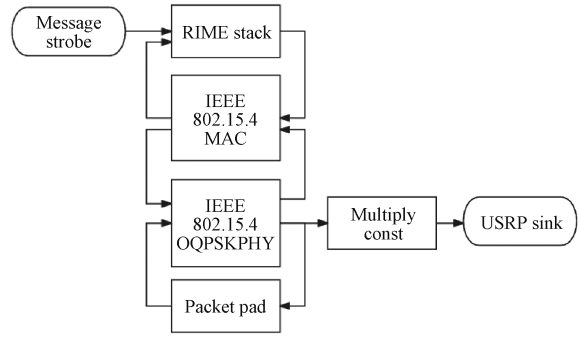


Fig. 5 Internal structure of DHT11

2) ZigBee signal transmission. The data format is specifically composed of unencoded binary data output by sensors[30]. When processing the data, each part is processed separately by the GNU Radio companion (GRC) of the ZigBee transmitter that we built on the GNU Radio platform as shown in Fig. 6.



RIME— a layered protocol stack; const—constant; OQPSKPHY—offset quadrature phase shift keying physical layer.

Fig. 6 Structure diagram of ZigBee transmitter

3.2 Wi-Fi receiver

At the receiving end of the system, the Wi-Fi receiver processes the received signal and loads the data into smart devices for analysis and decision-making.

1) Wi-Fi signal reception. A Wi-Fi signal's symbol is 80-bit complex data consisting of 16-bit cyclic prefix data and 64-bit valid data. Figure 7 shows the flowchart of the Wi-Fi receiver built for the test environment in GNU Radio.

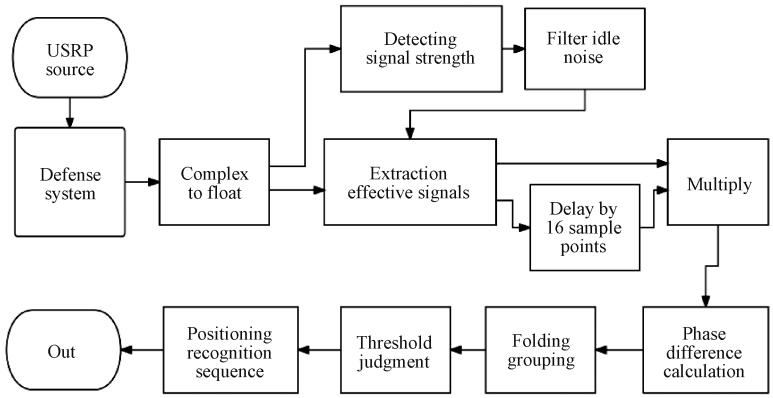
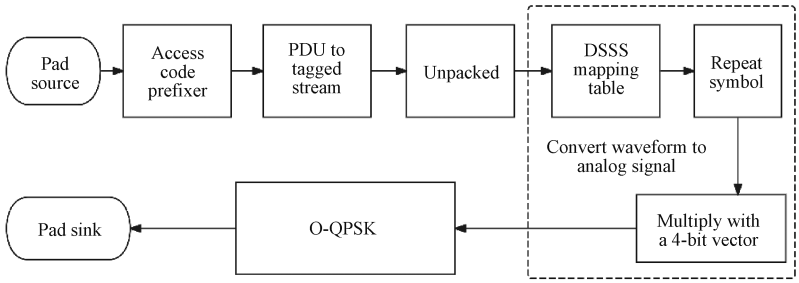


Fig. 7 Flowchart of Wi-Fi receiver

The testing environment was built by using two USRP 2953R and GNU Radio 3.8 in the Ubuntu virtual machine of VMware Workstation. One USRP 2953R is used as a ZigBee transmitter, and the other is used as a Wi-Fi receiver. Figure 8 shows the physical layer of the transmission system. The protocol data unit (PDU) refers to a single unit of information transmitted between peer entities in a computer network. Offset quadrature phase shift keying (O-QPSK) is an improved QPSK modulation method that uses phase modulated reference signals for data transmission.



DSSS—direct sequence spread spectrum.

Fig. 8 Physical layer flowchart of transmission system

2) Intelligent decision. Received data are sent to the monitor node's program entry and visualized via matplotlib plots; an easy GUI is used for the user interface and Pickle is used for variable serialization. As

shown in Fig. 9, the entered temperature threshold is displayed as a straight line on the interface at runtime. When the temperature exceeds the set threshold, a warning is given by adding a label. The intelligent decision-making system can send the corresponding instructions to the ZigBee node to respond to the operation through the Wi-Fi transmitter.

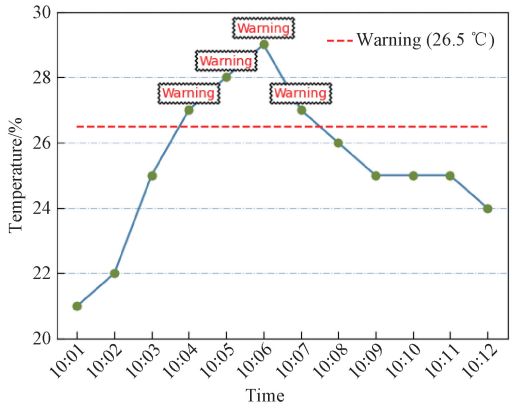


Fig. 9 Temperature interface

4 Defense against Cross-Technology Attacks

We focus on the security issues during the signal transmission in Fig. 4 and design two security defense strategies to ensure the signal is not tampered by attackers.

4.1 Noise interference strategy

Based on the carrier frequency offset characteristics of attacks, this section proposes a physical-layer defense scheme. By introducing additive white Gaussian noise (AWGN) during signal transmission, attackers can eavesdrop on and simulate ZigBee signals, resulting in significant quantization errors after Fourier transform and quantization, leading to signal distortion and reducing the success rate of attacks.

1) AWGN. AWGN represents a common communication noise model. It has a uniform power spectral density and Gaussian power distribution, and is widely used in simulating real communication environments. AWGN is generated by configuring Gaussian noise source parameters in our experiment.

2) FFT. FFT is a highly efficient algorithm for performing the discrete Fourier transform (DFT). It is a basic tool for analyzing signal transformation from the time domain to the frequency domain[29].

$$Z'(m, n) = Z(m, n) + N_Z(m, n), \tag{1}$$

where $Z(m, n)$ represents the frequency-domain expression of the ZigBee signal after FFT; $N_Z(m, n)$ represents the added AWGN noise; $Z'(m, n)$ represents the frequency-domain expression of the ZigBee signal after applying noise interference strategy. Figure 10 shows the image of the noisy ZigBee signal sent in our experiment after FFT.

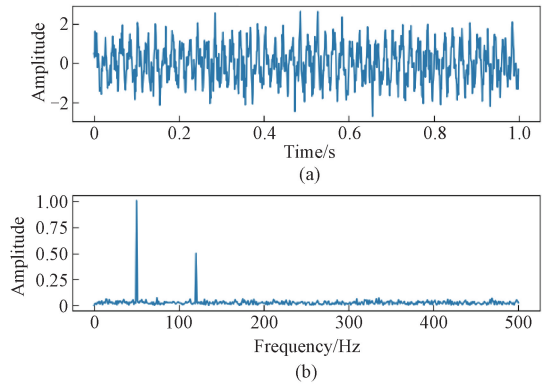


Fig. 10 Images of ZigBee signal: (a) time-domain signal with noise; (b) frequency-domain signal after FFT

3) QAM quantization error. The FFT processed signals $Z(m, n)$ and $Z'(m, n)$ are quantized, and the quantized constellation coordinates are denoted as $Q(m, n)$ and $Q'(m, n)$. After quantification, the quantization errors are labelled as $e(m, n)$ and $e'(m, n)$, respectively:

$$e(m, n) = (Z_{\mathrm{Re}}(m, n) - \alpha Q_{\mathrm{Re}}(m, n))^2 + (Z_{\mathrm{Im}}(m, n) - \alpha Q_{\mathrm{Im}}(m, n))^2, \tag{2}$$

$$e'(m, n) = (Z_{\mathrm{Re}}(m, n) - \alpha Q'_{\mathrm{Re}}(m, n))^2 + (Z_{\mathrm{Im}}(m, n) - \alpha Q'_{\mathrm{Im}}(m, n))^2, \tag{3}$$

where $Z_{\mathrm{Re}}(m, n)$ and $Z_{\mathrm{Im}}(m, n)$ represent the real part and imaginary part of the FFT signals, respectively; α is the optimal scalar; $Q_{\mathrm{Re}}(m, n)$ and $Q_{\mathrm{Im}}(m, n)$ are the real part and imaginary part of the quantized constellation coordinates without AWGN, respectively; $Q'_{\mathrm{Re}}(m, n)$ and $Q'_{\mathrm{Im}}(m, n)$ are the real part and imaginary part of the quantized constellation coordinates with AWGN, respectively. They can be used to compare the differences in the presence or absence of AWGN. Moderate AWGN noise can cause signals to be quantized to different QAM points, resulting in larger quantization errors.

4.2 Regression modeling strategy

Wi-Fi attackers possess sufficient computing power to execute signal emulation attacks through exhaustive searches of their constellations. Consequently, this subsection introduces a regression modeling strategy designed to differentiate in real time between signals from Wi-Fi attackers and those from ZigBee transmitters, as illustrated in Fig. 11.

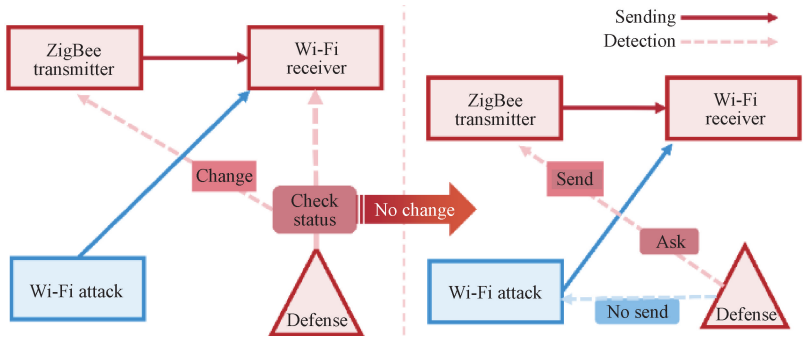


Fig. 11 Flowchart of regression modeling strategy

1) Feature extraction. The regression modeling strategy leverages wireless network protocol traits. To differentiate ZigBee from attacks, the receiver analyzes time and frequency features. In the time domain, cyclic prefix of Wi-Fi is verified by the cosine distance and high cosine distance values mean strong similarity. Comparing the average distance can analyze whether it is an attack signal. In the frequency domain, eavesdropped signals differ in constellation structure from analog ones.

2) Data collection and labeling. At the beginning of the run, the system records whether the transmitter sends a signal when the receiver receives a signal, so that the system can continuously classify it based on the historical learning results, as shown in Fig. 11. When receiving a signal, the first step is to check for any changes in the Wi-Fi receiver. If no change occurs, the signal is deemed an analog signal. If a signal has already been sent, the ZigBee transmitter is queried. If the sensor indicates that no signal is transmitted, the signal is classified as the analog. If a transmitter on the sensor side sends a signal, it is identified as the source.

3) The logistic regression model. The regression model categorizes data by formulating a boundary based on features[31]. Advantages of logistic regression in this paper are easy implementation due to simple formulas and clear parametric models, high efficiency with a fast calculation speed and low delay, and rich output offering probabilities for different events instead of an absolute 0 or 1.

The receiver in this paper needs to divide the sources of the received signal into two categories, so the binary logistic regression model is used. By comparing the magnitude of the two probabilities to determine the signal source, it can be determined that the signal comes from the transmitter with a higher probability.

$$P(Y=1 \mid \boldsymbol{x}) = \frac{\exp(\hat{\boldsymbol{w}} \cdot \boldsymbol{x} + \hat{\boldsymbol{b}})}{1 + \exp(\hat{\boldsymbol{w}} \cdot \boldsymbol{x} + \hat{\boldsymbol{b}})}, \tag{4}$$

$$P(Y=0 \mid \boldsymbol{x}) = \frac{1}{1 + \exp(\hat{\boldsymbol{w}} \cdot \boldsymbol{x} + \hat{\boldsymbol{b}})}, \tag{5}$$

where event "$Y=1$" indicates that the signal is from a Wi-Fi attacker; event "$Y=0$" indicates the transmitter; $\boldsymbol{x}$ denotes a feature vector; $\hat{\boldsymbol{\omega}}$ is the estimated weight veetor, and $\hat{\boldsymbol{\omega}} \in \mathbf{R}^n$; $\hat{\boldsymbol{b}}$ is the estimated bias term obtained by maximizing log-likelihood.

4.3 Selection design

To verify the performance of the proposed security defense strategies, this section shows the defense system selection design set in GRC, which can easily and quickly select the security defense strategy to be compared. We use the variables above to select the defense strategy.

In this system, after selecting the security defense strategies, the two selectors in the system will be synchronized, and open the corresponding port to receive data streams. To select the security defense strategies to be used, the route of the data flow can be automatically selected, simplifying the complexity of the GRC flow diagram, and avoiding repeated operations and excessive equipment performance consumption.

5 Performance Analysis of Security Defense Strategies

5.1 Experiment setup

We use one USRP 2953R equipped with IEEE 802.15.4 physical layer to send messages and another USRP 2953R equipped with IEEE 802.11 PHY to receive messages and perform a signal emulation attack on them in the GNU Radio 3.8 environment. The USRP 2953R receives the wireless signals through the radio frequency (RF) front-end and converts them into a digital signal stream for transmission to the connected computers.

5.2 Interference performance

After interference by noise, the signal emulated by the Wi-Fi attacker is quantized to a different constellation point than the one emitted by the transmitter. Figure 12 shows the original constellation performance. After adding AWGN, points that are more reddish indicate points with higher quantification errors, while green ones are points with lower quantification errors, as shown in Fig. 13.

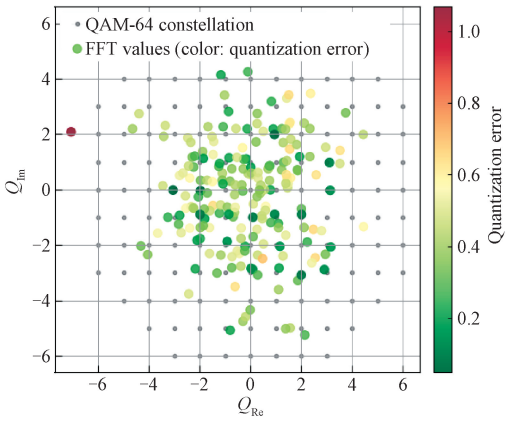


Fig. 12 Original constellation performance

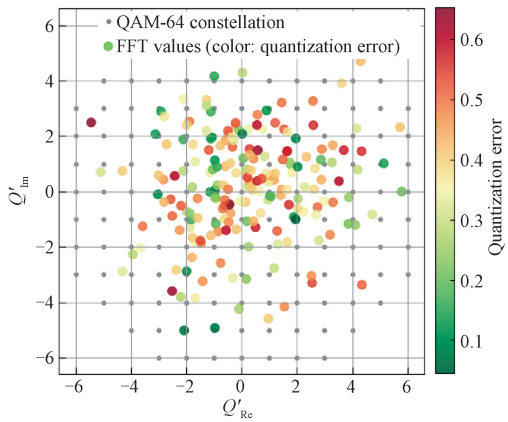


Fig. 13 New constellation performance

The QAM points on the constellation are shown in Table 1. For example, considering the point $m = 10$, when no noise is present, the point m quantizes to the QAM point $-1+j$; however, after adding noise, it quantizes to $-1-j$, deviating from the original FFT point. This erroneous quantization results in increased quantization errors, demonstrating that adding AWGN to the ZigBee transmit signal amplifies the quantization error in the attacker's simulation.

Table 1 Comparison of constellation performance

Sub-carrier	$Q(m, n)$	$e(m, n)$	$Q'(m, n)$	$e'(m, n)$
10	−1+j	0.647 8	−1−j	2.625 4
11	−1+2j	0.387 8	−1+j	0.648 1
12	−1+5j	0.121 7	−1+5j	0.122 3
13	1+j	0.831 5	1−j	1.812 5
14	1+2j	0.501 3	1+2j	0.524 5
15	1+5j	0.451 4	1+4j	0.625 1
16	2+3j	0.544 7	2+2j	0.924 5
17	5−3j	1.104 2	5−3j	1.135 4
18	−7+j	0.425 1	−5+j	2.512 4

5.3 Recognition performance

The trained model of the regression modeling strategy predicts points in the sample space, observes classifications, draws category boundaries and creates a decision boundary graph. In binary classification, this graph splits the vector space into two parts, and the decision boundary is a straight line, serving as the binary classification threshold. We use Matplotlib and SciKit-Learn to calculate prediction probabilities on a grid, set a threshold to distinguish attacker and sensor signals, and draw the decision boundary, as shown in Fig. 14.

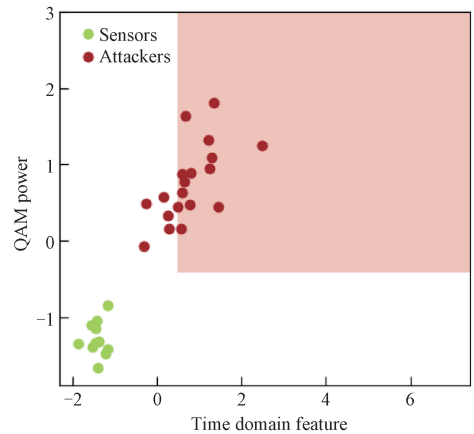


Fig. 14 Model decision boundary of regression modeling strategy

Signals are received continuously in the application, so a large number of fast data input and processing speeds need to be considered to distinguish signal sources in time based on the feature classification learned by the model. The accuracy of the model gradually tends to "1" with the increase of the amount of model training data. Figure 15 shows the accuracy of the model of the regression modeling strategy.

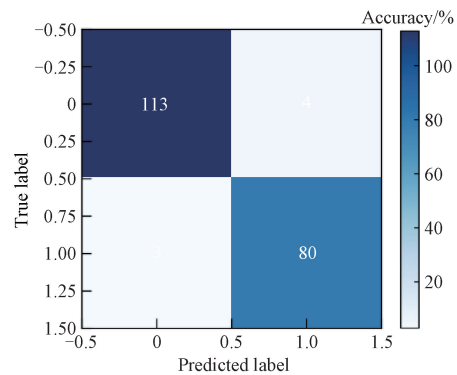


Fig. 15 Model performance accuracy

To verify the stability of the security defense strategies under different network loads, a series of tests are conducted within the traffic rate range of the ZigBee transmitter. The control of the traffic rate is achieved by adding a throttle module to the ZigBee transmitter. The results are shown in Fig. 16. From the experimental results, it can be seen that our security defense strategies

have good stability under heavy traffic conditions.

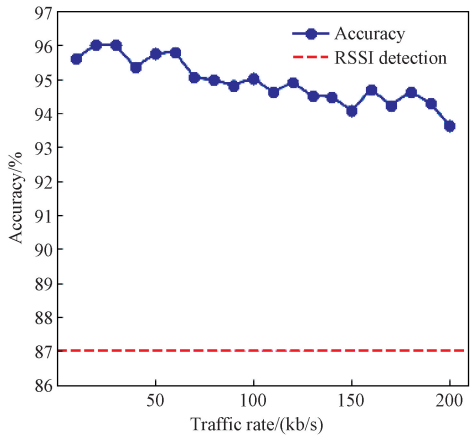


Fig. 16 Accuracy on different traffic rates

6 Conclusions

In this paper, a comprehensive solution is proposed, which combines a noise interference strategy and a regression modeling strategy to counteract CTC attacks at the physical-layer communication from ZigBee to Wi-Fi. On the receiver side, dedicated noisy signals are added to raw signals. Subsequently, data collection and feature extraction are performed. By training a binary logistic regression model, the recognition ability of attackers' simulated signals is continuously enhanced. Exhaustive experiments verify the superior defense performance of our proposed strategies, which plays an important role in the secure and reliable development of IoT. In future research, the processing efficiency and other performance of the regression model can be further improved to defend against replay attacks and DoS attacks. At the same time, conducting in-depth research on the characteristics of Bluetooth and long-term evolution signals and identifying parameters that can be used for feature extraction can help to apply the security defense strategies to more situations of heterogeneous wireless signals coexist.

References

[1] IEEE Standard Association. IEEE Standard 802.11[S]. New York: IEEE, 2012.

[2] ZHANG D A, WANG J X, JANG J, et al. On the feasibility of Wi-Fi based material sensing [C]//The 25th Annual International Conference on Mobile Computing and Networking. New York: ACM, 2019: 1-16.

[3] IEEE Standard Association. IEEE Standard 802.15.4[S]. New York: IEEE, 2003.

[4] PARK Y, HA J H, KIM H, et al. Enabling sensor network to smartphone interaction using software radios[J]. *ACM Transactions on Sensor Networks*, 2017, 13(1): 1-26.

[5] SHESHADRI R, SUNDARESAN K, CHAI E. BLU: blueprinting interference for robust LTE access in unlicensed spectrum [C]//Proceeding of the 13th ACM CONEXT. New York: ACM, 2017: 15-27.

[6] SEMTECH R. LoRa Standard [EB/OL]. [2020-10-12] (2024-10-11). https://lora-alliance.org.

[7] HAN J S, DING H, QIAN C, et al. CBID: a customer behavior identification system using passive tags [J]. *ACM Transactions on Networking*, 2016, 24(5): 2885-2898.

[8] ANGRISANI L, BERTOCCO M, FORTIN D, et al. Experimental study of coexistence issues between IEEE 802.11b and IEEE 802.15.4 wireless networks [J]. *IEEE Transactions on Instrumentation and Measurement*, 2008, 57(8): 1514-1523.

[9] CHI Z C, LI Y, HUANG Z C, et al. Simultaneous bi-directional communications and data forwarding using a single ZigBee data stream [C]//2019 IEEE Conference on Computer Communications. New York: IEEE, 2019: 577-585.

[10] JIANG W C, YIN Z M, KIM S M, et al. Transparent cross-technology communication over data traffic [C]//2017 IEEE Conference on Computer Communications. New York: IEEE, 2017: 1-9.

[11] LIU R F, YIN Z M, JIANG W C, et al. WiBeacon: expanding BLE location-based services via WiFi[C]//Proceedings of the 27th Annual International Conference on Mobile Computing and Networking. New York: ACM, 2021: 83-96.

[12] CHEN G L, DONG W. JamCloak: reactive jamming attack over cross-technology communication links [C]//2018 IEEE 26th International Conference on Network Protocols (ICNP). New York: IEEE, 2018: 34-43.

[13] ZHANG X N, YU S H, ZHOU H S, et al. Signal emulation attack and defense for smart home IoT[J]. *IEEE Transactions on Dependable and Secure Computing*, 2023, 20(3): 2040-2057.

[14] ZHENG X L, HE Y, GUO X Z. Strip-Comm: interference-resilient cross-technology communication in coexisting environments[C]//Proceeding of IEEE INFOCOM. New York: IEEE, 2018: 171-179.

[15] KIM S M, HE T. FreeBee: cross-technology communication via free side-channel [C]// Proceeding of the 21st ACM MobiCom. New York: ACM, 2015: 317-330.

[16] WANG W G, ZHENG X L, HE Y, et al. AdaComm: tracing channel dynamics for reliable cross-technology communication[C]//2019 16th

Annual IEEE International Conference on Sensing, Communication, and Networking (SECON). New York: IEEE, 2019: 1-9.
[17] XIA D, ZHENG X L, LIU L, et al. C-chirp: towards symmetric cross-technology communication over asymmetric channels [C]//2020 17th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON). New York: IEEE, 2020: 1-9.
[18] WANG W, HE D S, JIA W, et al. PRComm: anti-interference cross-technology communication based on pseudo-random sequence [C]// Proceedings of the 20th International Conference on Information Processing in Sensor Networks. New York: ACM, 2021: 163-175.
[19] HOFMANN R, BOANO C A, ROMER K. X-burst: enabling multi-platform cross-technology communication between constrained IoT devices [C]//2019 16th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON). New York: IEEE, 2019: 1-9.
[20] CHAE Y, WANG S, KIM S M. Exploiting WiFi guard band for safeguarded ZigBee [C]// Proceedings of the 16th ACM Conference on Embedded Networked Sensor Systems. New York: ACM, 2018: 172-184.
[21] WANG S, YIN Z M, LI Z J, et al. Networking support for physical-layer cross-technology communication [C]//2018 IEEE 26th International Conference on Network Protocols (ICNP). New York: IEEE, 2018: 259-269.
[22] GUO X Z, ZHENG X L, HE Y. WiZig: cross-technology energy communication over a noisy channel [C]//Proceeding of IEEE INFOCOM. New York: IEEE, 2020: 2449-2460.
[23] ZHANG Y F, LI Q. HoWiES: a holistic approach to ZigBee assisted WiFi energy savings in mobile devices [C]//2013 Proceedings IEEE INFOCOM. New York: IEEE, 2013: 1366-1374.
[24] CHI Z C, HUANG Z C, YAO Y, et al. EMF: embedding multiple flows of information in existing traffic for concurrent communication among heterogeneous IoT devices [C]//IEEE INFOCOM 2017-IEEE Conference on Computer Communications. New York: IEEE, 2017: 1-9.
[25] GUO X Z, HE Y, ZHENG X L, et al. ZIGFI: harnessing channel state information for cross-technology communication [C]//IEEE INFOCOM 2018-IEEE Conference on Computer Communications. New York: IEEE, 2018: 360-368.
[26] LI Z J, HE T. WeBee: physical-layer cross-technology communication via emulation [C]// Proceeding of the 23rd ACM MobiCom. New York: ACM, 2017: 2-14.
[27] LI L G, CHEN Y R, LI Z J. Physical-layer cross-technology communication with narrow-band decoding [C]//Proceeding of the 27th IEEE ICNP. New York: IEEE, 2019: 1-2.
[28] CHEN Y R, LI Z J, HE T. TwinBee: reliable physical-layer cross-technology communication with symbol-level coding [C]//IEEE INFOCOM 2018-IEEE Conference on Computer Communications. New York: IEEE, 2018: 153-161.
[29] WANG S, KIM S M, HE T. Symbol-level cross-technology communication via payload encoding [C]//2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS). New York: IEEE, 2018: 500-510.
[30] HIDAYAT T, MAHARDIKO R, SIANTURI TIGOR F D. Method of systematic literature review for Internet of Things in ZigBee smart agriculture [C]//2020 8th International Conference on Information and Communication Technology (ICoICT). New York: IEEE, 2020: 1-4.
[31] CHEN Y R, WANG S, LI Z J, et al. Reliable physical-layer cross-technology communication with emulation error correction [J]. *ACM Transactions on Networking*, 2020, 28(2): 612-624.

物联网控制系统中跨技术通信的安全防御

李天韵，张安琪，张光林*
东华大学 信息科学与技术学院，上海 201620

摘　要：为解决跨技术通信（cross-technology communication，CTC）安全问题，以物联网（Internet of Things，IoT）智能控制系统为例，提出了一种从 ZigBee 到 Wi-Fi 的物理层 CTC 攻击综合解决方案。具体而言，提出了一种噪声干扰策略，通过添加适量的专有噪声信号来干扰攻击者对 ZigBee 信号的窃听和仿真，而不影响接收端的信号接收；提出了一种回归建模策略来收集数据、提取特征，并训练二进制逻辑的回归模型，使接收器能够主动区分模拟的攻击信号。使用 GNU Radio 和 USRP 设备构建了一个实验平台。实验结果表明，所提出的安全防御策略能够高精度地识别和区分攻击者的信号，有效地防御了从 ZigBee 到 Wi-Fi 的物理层 CTC 上的信号仿真攻击。

关键词：跨技术通信；物联网；智能控制；安全防御策略