Frontiers in Computing and Intelligent Systems
ISSN: 2832-6024 | Vol. 6, No. 3, 2023

CSI-based WIFI Device Identification Solution

Yiming Li *

Department of Computer Science and Technology, Qingdao University, Qingdao, Shandong, China
* **Corresponding author Email:** l997999350@163.com

Abstract: In recent years, wireless devices such as WIFI routers have become increasingly common in various fields. Rogue access point (RAP) is one of the threats that has persisted in wireless LAN (WLAN) for many years and can cause varying degrees of property damage and privacy leaks. In response to these threats, we propose a new security mechanism, called Rdi, which uses environment-independent features extracted from channel state information (CSI) as fingerprints for device identification. We found that the phase errors between multiple antennas on a single MIMO-OFDM (Multiple Input Multiple Output-Orthogonal Frequency Division Multiplexing) transmitter are not the same. This phase offset is due to the I/Q imbalance and imperfect oscillator of each WiFi network card, and it will not change with factors such as environment and time. Therefore, we inferred and verified that there must be some relationship between the phase errors of multiple groups of antennas, that is, the relative phase error (RPE). In addition, RPE will also vary with different WiFi devices. Compared with some similar fingerprint detection methods in the past, the use of specific connections between group phase errors between antennas can better reveal the different attributes between devices, thereby enhancing the uniqueness of features. Therefore, we believe that RPE can be used as an effective fingerprint to detect RAP attacks. We conduct a large number of experimental demonstrations on this, and innovatively built a multi-modal convolutional neural network (CNN) model to perform efficient classification work for our solution. Experiments on 22 WiFi devices and various scenarios show that the detection rate of Rdi can reach more than 98% in both dynamic and static device states.

Keywords: Relative Phase Error; CSI; RAP.

1. Introduction

With the development of communication technology and the wide application of mobile devices, various fields are becoming more and more informatized. WiFi has become one of the most popular communication mediums for connecting wireless devices in the Internet of Things (IoT). However, in this scenario, various threats and security loopholes against wireless networks are also emerging, such as Denial of service (DOS) attacks, encryption cracking, WiFi Freeloading, etc. Among them, rogue access points (RAP) attacks have become one of the most serious attack threats.

RAPs already exist around the world, and they usually occur in public places such as coffee shops, stations, airports, government agencies, and schools. Attackers usually use the same identifiers like basic service set identifier (BSSID) and service set identifier (SSID) as the original AP to pretend to be a legitimate one, thereby making illegal and malicious connections, manipulating all network communications of the victims. This will cause serious consequences, such as user privacy disclosure, and property loss, and even threaten the development of society.

To cope with RAP attacks, strengthening the detection mechanism of the client is the most important key. The current RAP detection schemes can be divided into two categories: non-hardware-based RAP detection and hardware-based RAP detection. The initial research focuses on non-hardware device detection, such as 802.11i RSNA, etc., which has provided some traditional encryption methods to enhance authentication security, but Jana et al. [1] have confirmed that there are still some loopholes, which will cause users to still be lured to connect to RAPs. Current Non-hardware detection mainly uses traffic characteristics, behavior characteristics, topology structure, and some network-level characteristics to detect attacks. Unfortunately, these detection methods have gradually exposed shortcomings such as low efficiency, high cost, and insufficient detection rate. For example, Gao et al. estimate the packet interval time in the network layer as a feature of AP [2]. In [3], the transmission rate of the PHY layer is used to distinguish devices. Although these traffic analysis methods are effective in some scenarios, they require a large amount of data collection, even up to tens of gigabytes, leading to significant time consumption, storage overhead, computation cost.

Hardware-based RAP detection schemes use device hardware fingerprints to realize device identification and attack detection, and many related schemes have begun to be widely studied. Fingerprints on the hardware layer mainly refer to the defect on the internal hardware component of the transmitter, such as Tx-Rx oscillators, digital-to-analog converter (DAC) and the power amplifiers (PA), etc. This kind of defect is generally difficult to imitate and has strong independent differences because forging hardware defects requires high costs for attackers, so this is a promising direction for device identification and RAP detection. CSI becomes a suitable research object, which can provide context-independent features of devices to detect and identify rogue WiFi devices or APs. For example, due to the carrier frequency mismatch between the TX and RX oscillators, Hua et al. [4] extract the carrier frequency offset (CFO) from CSI to be a device fingerprint. Later in [5], a great improvement in detection speed was made to this detection method, but the sensitivity to the environment still limited the fingerprint. These disadvantages were well optimized in the phase error fingerprint extracted from CSI by [6] et al. The phase error is due to the I/Q imbalance and oscillator imperfections of each WiFi device, and it doesn't require additional equipment to extract phase features across subcarriers to build device fingerprints. Although the fingerprint has performed well in terms of stability, there is still room for improvement in

applicable scenarios.

To solve the above problems, we propose a lightweight continuous authentication scheme for wireless devices based on CSI fingerprints for modern MIMO devices. Our solution, RPE-MIMO, innovatively uses relative phase error (RPE) as a fingerprint to detect AP attacks and identify devices and exploits a novel CNN-based multi-modal neural network model framework for efficient identification and classification. The proposed fingerprint is independent of the environment and eliminates the multipath effect of mobile devices. This solution can improve detection accuracy and expand the scope of applications while maintaining good stability, allowing it to be integrated into today's intelligent and diversified application scenarios.

In summary, we make the following contributions:

- An innovative device physical layer fingerprint detection scheme is proposed. This work is based on the relative phase error of multiple links of the device, and the proposed fingerprint is independent of the environment.
- A CNN-based multimodal neural network models is proposed. It can efficiently perform device detection tasks such as classification and prediction.
- A lot of verification work has been done by using 22 routers. The experimental data shows that the accuracy rates in static and dynamic scenarios are 99.2% and 98.4% respectively.

The rest of the paper is organized as follows: Section II introduces the background knowledge used in some schemes. In Section III, we discuss related work. Section IV clarifies our detailed approach and presents the experimental implementation in Section V. Finally, a conclusion of the full text is given in Section VI.

2. BACKGROUND

2.1. CSI (Channel State Information)

In wireless communication systems, CSI reveals the channel response characteristics of transmission links, including the combined effects of scattering, fading, and power attenuation. On a 2.4Ghz frequency band with a bandwidth of 20Mhz, the CSI measurement consists of 30 complex values, where each complex value corresponds to a selected subcarrier. So, for the received 802.11 frame, there are 30×Ntx×Nrx CSI streams, where Ntx and Nrx are the number of transmit antennas and receive antennas, which also record the amplitude and phase of OFDM subcarriers. In the frequency domain, a wireless channel can be described as $Y = H \times X + W$, where X and Y are received and transmitted signal vectors, respectively, H is a channel matrix expressed in CSI format, and W is an additive Gaussian white noise vector. The CSI stream for the kth subcarrier between the ith transmit antenna and the jth receive antennas can be expressed as $H_{k,i,j} = |H|e^{-j\varphi_{k,i,J}}$,where |H| is the amplitude and φk, i,j is the phase part of subcarrier k.

2.2. Phase Error

For the OFDM system, due to reasons such as I/Q imbalance and an imperfect oscillator, the phases at the receiver and the transmitter exhibit a non-linear offset, that is, phase error occurs. A previous study [6] confirmed that the phase error θ caused by I/Q imbalance can be expressed as:

$$\theta = \phi - \omega - \alpha - \beta - \psi$$

where, ω and ϕ represent the signal phases at the transmitter and receiver of the device.

α is the phase shift due to sampling frequency offset (SFO).

β is the offset due to frame detection delay (FDD).

ψ is the phase shift due to time of flight (ToF).

2.3. OFDM System

OFDM: By turning high-speed large data streams into parallel low-speed data streams through several orthogonal subcarriers, OFDM has stronger anti-multipath interference capabilities, so the latest version of the 802.11 protocol also uses this technology.

WiFi RF components: This mainly includes the transmitter, antenna and receiver (Fig .1).

1) Transmitter: After receiving the data, it uses modulation technology to modify the AC signal, encodes the data into the signal and transmits it to the antenna through the cable. The fingerprint information such as CPE and CFO we mentioned records the initial state of the transmitter as the starting state, thereby describing the entire offset trajectory.

2) Antenna: The antenna is divided into a transmitter antenna and a receiver antenna. The transmitter antenna collects the AC signals transmitted by the transmitter and radiates the radio frequency waves; the receiver antenna captures the radio frequency waves in the air and conducts the AC signals to the receiver. In modern MIMO systems, devices often contain multiple sets of transmitter and receiver antennas.

3) Receiver: Obtain the carrier signal received by the antenna and convert the signal into data. During the signal transmission process, due to inevitable factors such as hardware defects or unstable transmission environment, some errors or offsets are often caused, and they are often recorded in the receiver of the wireless device.

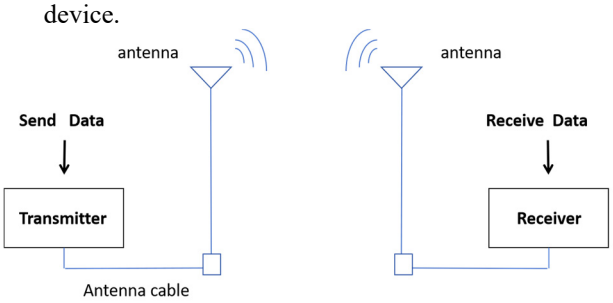


Fig 1. WiFi RF components

3. RELATED WORK

In recent years, more and more authentication schemes based on device fingerprints have been proposed. The key to achieving continuous authentication is to find a reliable and valid fingerprint. As mentioned above, current detection solutions are mainly studied from two aspects: non-hardware-based RAP detection and hardware-based RAP detection

The initial research work on RAP attack detection mainly focused on non-hardware-based device detection, mainly detecting devices through traffic characteristics, behavioral characteristics, topology structure, and other network layer or link layer characteristics. For example, Corbett et al. [3], utilized the transmission rate of the PHY layer as a fingerprint to distinguish devices. Moreover, Neumann et al. used a set of wireless parameters to fingerprint the target device, including inter-arrival time, frame size, transmission rate, etc. In another work [7], Gao et al used a black-box-based fingerprint identification method. The input to the black box

(AP) was a sequence of packets, different devices will take different actions on the packet sequence due to different architectures of the access points. This operating mode is unique to each AP, so it can be used as a device fingerprint, but the experiment was simply conducted using simulated traffic. Gao et al. estimated the packet arrival time (IAT) in the network layer as the fingerprint of AP [7], but IAT is easily affected by various factors such as network delay and retransmission. In summary, the above methods have various drawbacks. First, some of them are related to network traffic or other things, rather than to the device itself, so they can be easily counterfeited by attackers. Second, some of them require extensive data collection, which will cause a lot of time consumption, storage overhead, etc., making it difficult to implement in real-world applications. Furthermore, due to various other factors that have not been verified in real scenarios, some methods cannot be applied in practice and have poor robustness. Therefore, for advanced attackers, these non-hardware-based fingerprints can be easily forged and cannot be used as reliable fingerprints.

Later, the focus of research shifted to hardware-based RAP detection, which mainly used unique features on the physical layer to perform device identification or RAP detection. Such hardware differences are generally difficult to imitate and have strong distinguishability. For RAP attack detection, Jana et al. [1] proposed that the clock skews of the device can be used as the feature to characterize the physical device. They achieve the purpose of detecting RAP by calculating the target AP's clock skew and comparing it with the legitimate fingerprint recorded in the database. Then, Lanze et al. proposed a RAP detection scheme that can eliminate the impact between fingerprint collection devices, which uses the relative clock skews as the fingerprint of the device. This method calculated the relative clock skews of a device by collecting the clock skews of two APs, thus eliminating the impact of the collection device on the clock skews. However, this solution had only been simulated in a lab and lacks large-scale evaluation, so its robustness and practicality cannot be guaranteed. Brik et al.[8] adopted a hardware fingerprinting approach and used machine learning tools on collected modulation data to train classifiers that can distinguish arbitrary wireless network cards. In addition, Demirbas et al. proposed a lightweight RAP attack detection method based on the received signal strength indicator (RSSI). Although the above methods are related to the device hardware, most of them require specially custom detection equipment, and their systems are intolerant of mobile and dynamic multipath channels, affected by environmental factors, leading to an insufficient detection rate.

To eliminate expensive custom-built detection equipment, some researchers turned to CSI attribute analysis. Jiang et al. [9] fingerprinted wireless devices by measuring the CSI of WiFi management frames. Li et al. [10] used temporal soundings and multi-tone soundings extracted from channel estimates to verify legitimate transmitters. Liu et al. proposed a user-authentication framework that can build the user profile resilient to the presence of the spoofer, but devices were required to be static. In 2018, Hua et al. [4] extracted the carrier frequency offset (CFO) from CSI. They use the CFO between Tx-Rx oscillators as a device fingerprint, which could eliminate the need for customized hardware, and it achieved excellent performance in RAP detection. Moreover, on the basis of experimental results, Yu et al. proposed a lightweight solution based on CFO, the authentication time of CFO-based fingerprint detection was greatly shortened by additionally adding multiple features such as equal spacing and interception of CFO stripes[5]. However, due to sensitivity to the environment, these methods require the devices to remain stationary states, so they cannot achieve good recognition results in real-world scenes.

In 2019, Liu et al.[6] proposed a novel detection scheme, they used the phase error caused by the I/Q imbalance of the WiFi network card and the imperfect oscillator as a device fingerprint, which could adopt in a dynamic scene. Moreover, in Liu et al.'s scheme, it was proved that most other phase terms vary with time and/or frequency, while CFO and phase error are constant in both dimensions. When using a single Tx-Rx chain, the phase error as a fingerprint has eliminated the dependence on the environment, achieving good stability in device identification. However, there is still room for improvement in the detection rate of this solution in different scenarios.

All in all, current wireless device detection solutions can already achieve good attack detection using only ordinary collection devices (such as a laptop). However, the detection rate in dynamic and static environments is still not perfect, and there is still room for improvement. Inspired by this, we will propose a lightweight CSI-based RAP attack detection solution, which has a better detection rate in both dynamic and static environments. Its good robustness and stability features have been extensively verified in real-world scenarios.

4. METHODOLOGY

we propose a new solution Rdi to realize the identification of wireless devices. In this section, we introduce the specific principles and workflow of Rdi in detail.

4.1. Overview

We innovatively propose a lightweight solution Rdi for RAP attack detection, which uses the multi-antenna spatial dimensions provided by modern MIMO devices to extract phase errors within multiple groups of antennas as device features. Our method consists of three parts: estimating RPE From CSI, data processing, CNN multi-modal neural network.

Estimating RPE From CSI: This module is responsible for estimating RPE from CSI. The key innovation in Rdi is that we propose a new device fingerprint RPE. Specifically, RPE is a specific relationship between the phase errors of multiple sets of antennas in a wireless device, which can be output as a constant and unique device characteristic through calculation and other processing. We put the work of extracting unique features of fingerprints in the neural network model, and we only need to determine the input content.

Data processing: This module is responsible for the graphical processing of the obtained RPE so that we can visually observe the relationship between the phase errors of different antenna groups. More importantly, it is conducive to our efficient input in the subsequent CNN neural network classification.

CNN multi-modal neural network: In this module, we propose a multi-modal CNN model that can classify and predict wireless devices by taking the offset trajectory image of RPE as input, thereby achieving RAP attack detection.

Our solution completes RAP attack detection by extracting hardware fingerprint features and performing efficient classification, thereby identifying device identification. The

following parts of this section introduce the specific methods and details of each part.

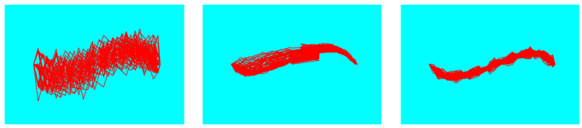


Fig 2. Phase error between three different sets of antennas

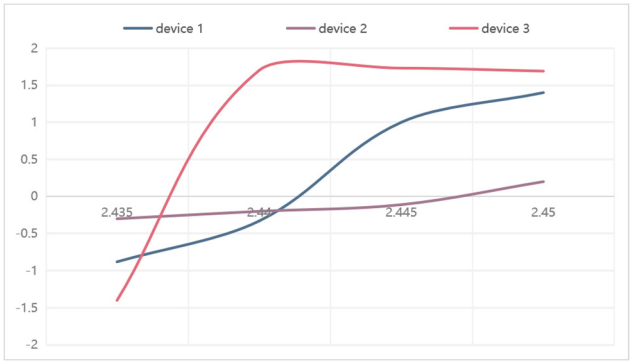


Fig 3. Fingerprint of three Different Devices

4.2. Estimating RPE From CSI

Since the phase errors between the antenna groups included in the same wireless device are inconsistent, as shown in the Fig. 2, and there is a constant relative relationship between them. Therefore, we study it and use Eq. (1) to obtain the phase error from CSI, and establish a new device fingerprint RPE to detect RAP attacks.

We select three groups of antennas, the transmitting antenna a and the receiving antennas $b1, b2,$ and $b3$, and extract the phase errors of the three groups of Tx-Rx in the device, recorded as $\theta1$,$\theta2$,$\theta3$. For example, $\theta1$ represents the phase error between the transmitting antenna a and the receiving antenna b1. We can express their relative relationship as:

$$\Delta\theta_{21} = \theta_2 - \theta_1$$
$$\Delta\theta_{32} = \theta_3 - \theta_2$$
$$\Delta\theta_{31} = \theta_3 - \theta_1$$

where $\Delta\theta_{21}$, $\Delta\theta_{31}$ and $\Delta\theta_{32}$ represent the RPE between multiple sets of antennas in a wireless device.

So in the end we use the relative phase errors $\Delta\theta_{21}$, $\Delta\theta_{31}$ and $\Delta\theta_{32}$ of the three links $\theta1$, $\theta2$ and $\theta3$ as our initial fingerprint data input. As shown in Fig. 3, the extracted fingerprints are different across devices. So the relative relationship between the phase errors between Tx-Rx is output as a device fingerprint, that is RPE, for identification of WIFI devices.

4.3. Processing of Data

This module is responsible for processing data of RPE. We reflect the obtained phase error and RPE in an intuitive two-dimensional space, which can also provide convenient and efficient input for subsequent neural network classification.

After obtaining the phase errors of the device from the CSI, it can be found through observation that they all have a deviation range determined by 30 subcarriers. To observe this deviation more intuitively and to study the deviation relationship between different groups of antennas more conveniently, we convert them into graphs and place them in two-dimensional space for the next step. Moreover, our subsequent detection work is based on the training and prediction in the neural network, so we need to convert the range of relative phase errors into graphs and use them as input to the model, which also makes it easier for us to carry out the work of the neural network in the future.

We take the measured 30 subcarriers as the abscissa of the graph, that is, K =[−28, −26, ..., −2, −1, 1, 3, ..., 27, 28], which corresponds to an offset value, thus forming a point set consisting of 30 points on the coordinate axis. These points are connected to form a region on the number axis, which may be a wide curved line segment or a section of up and down fold lines, or maybe a completely irregular shape.

After observation and comparison, the phase error shapes presented by different devices are different. This difference may be two completely different shapes, or it may be a very small difference. In the same device, the phase errors between three different groups of antennas also have completely different differences. We hypothesize and confirm that the connection between these three groups of phase errors, that is, the relative difference, is also unique to each WiFi device. We perform the same processing on $\Delta\theta_{21}$ and $\Delta\theta_{32}$ obtained in the previous section, get three corresponding RPE offset trajectories on the coordinate axis, and output them as graphs.

Therefore, the input of the fingerprint RPE mentioned in the previous section is also processed and becomes the phase error picture corresponding to the two links.

4.4. CNN Multi-modal Neural Network for Device Fingerprinting

We built a CNN neural network based on multi-modal technology (Fig. 4) to classify the RPE graph between multiple groups of antennas. CNN is a feed-forward neural network with a convolutional structure. It is a network that efficiently processes large amounts of image data classification and prediction, and can completely retain the original features. We take advantage of this feature, after several convolutions and pooling, the multi-dimensional data is "flattened" first, that is, the (height, width, channel) data is compressed into a one-dimensional array with a length of height × width × channel. Then it is connected to the fully connected layer, and the same workflow as the ordinary network is carried out until we get the training results we want for prediction and recognition.

The model is divided into three modules: Image processing, Feature extracting, and Attack detection.

Image processing: In the image processing stages, we provide a total of three channels of independent input. Taking the above three sets of relative phase error graphs in the same device as the only input, the neural network is used to label and preprocess them to carry out subsequent feature extraction and other work.

Feature extracting: After image processing, these three channels are independent and complementary to each other. Three sets of relative phase errors between different antenna groups of the same device provide rich information to the other set of images respectively, and are independent of each other. They can effectively fuse multiple images and classify them. After image processing, these three channels are independent and complementary to each other. Three sets of relative phase errors between different antenna groups of the same device provide rich information for another set of images, and are independent of each other. They can effectively fuse multiple images and classify them. Since the phase errors between different antenna groups of the same device may be very similar, this will cause the relative relationship between them to be very weak, making it difficult to identify their device characteristics during classification.

Therefore, to deeply learn more complex features and improve the accuracy of classification. In this part, we use the residual network ResNet50 as the backbone to construct a deep network, and use the first three residual blocks of the ResNet-50 network to extract and fuse fingerprint features. After the image is input, feature extraction is completed through convolution, pooling, etc. The difference and mutual influence of the three sets of phase offset graphs will be fully analyzed and extracted, and preliminary feature information F_a will be obtained.

Attack detection: In this module, we further strengthen the obtained features and finally complete the classification to achieve the detection of RAP attacks. We input the F_a obtained in the previous module into the channel attention, which re-constructs a series of feature graphs in the middle of the network, enhance the discriminative ability of image features, highlights some important features, and suppresses other general features, thereby extracting key information in the feature graph and obtaining feature F_b. Next, the fourth part of the residual block of the ResNet-50 network is used to enhance the features of $F_b$to obtain the final F_c. This feature F_c is used for the final classification prediction to achieve the best network performance.

This network model provides significant help for WIFI device fingerprint identification, making subsequent work more efficient and convenient, and can also be applied in more scenarios.

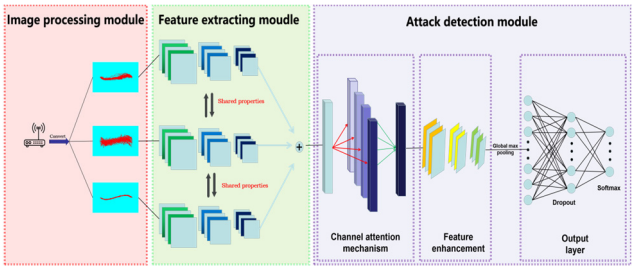


Fig 4. The overall framework of DL-QW

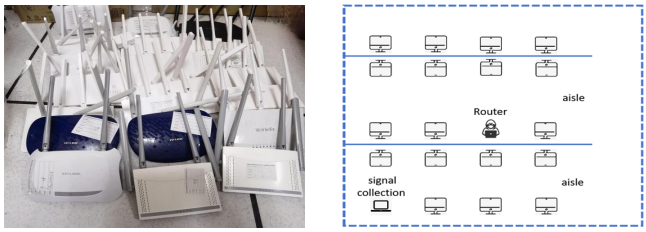
Our solution combines the excellent properties of CSI and the characteristics of MIMO-OFDM without using the traditional fingerprint method of a specific hardware defect in the device. In other words, our task shifts from estimating a specific fingerprint itself to estimating their constant relative relationship based on the phase error extracted from CSI. This relative relationship can more clearly reveal the difference in phase errors between devices, further improving the accuracy of device identification while maintaining good stability. This does not require additional hardware and cost, and can be well implemented in neural network models. In the next section we will demonstrate the specific experimental process.

5. EXPERIMENTS

This section introduces our experiments, including experimental settings, and experimental scenarios. Then, evaluate the performance of our proposed fingerprint mechanism, including an introduction from the aspects of data set collection, processing, device detection, and various parameters of the neural network.

Hardware: The testing device we use is a Thinkpad T340 laptop equipped with an Intel 5300 network card, and its CPU is an Intel i5-3320M. The created fingerprint library comes from 22 WIFI devices to be detected, which are composed of 22 routers of different brands and models in Fig. 5(a). The detailed data is shown in the TABLE I.

Software: The kernel of the detection terminal is Linux 4.2.0, and it runs the Ubuntu 14.0.4 LTS system. To collect CSI information, the system is installed with Linux 802.11n CSI Tool. Wi-Fi releases open networks to be tested for the CSI Tool's operational requirements.



(a) WiFi devices used in experiments (b) Experiment site

Fig 5. Experimental environment settings

Table 1. WiFi Routers

Brand	Model	Quantity
FAST	FW325R	4
360	360T2 2.0	4
TP-LINK	TL-WR842N	4
HONOR	XD16	2
TENDA	F3	4
MERCURY	MW325R	4

Experimental environment: Based on the test of stability, we will set up the experimental environment based on two aspects of: position stability and time stability. Our experimental environment is set in a dynamic experimental environment in a university laboratory. As shown in the Fig. 5(b), the laboratory area is 10m*10m, with 20 seats in it. One is to place the detection equipment and the equipment to be detected at both ends of the same aisle, without any obstructions and environmental changes in the middle. The other is to place the equipment to be tested (i.e., WIFI router) in the middle of the laboratory, and the testing equipment is placed in a corner, as shown in the Fig. 5(b), with various obstacles, including people and objects in the middle. During the experiment, the personnel in the laboratory can carry out any activities. The last one is that the equipment to be tested is still in the middle of the laboratory, and our Thinkpad T340 laptop is moving arbitrarily in the laboratory. Our testing equipment will measure the testing results every 6 hours within 72 hours.

Fingerprint library: We don't use the existing public data set, but collected the CSI data of 22 WIFI devices as our fingerprint library, including a total of 6 models, except Honor purchased two, and the other models each had four. Each device has collected 20M data, which contains about 50,000 pieces of CSI information, which record the fingerprints we need for detection, that is, the phase errors between all different TX-RX in the device. Then, we use the Linux802.11n CSI Tool to extract the CSI information from the AP's response. Finally, we use formula (1) to sequentially calculate the phase error between each group of antennas in each data frame.

Determine the fingerprint: We use the method described in the previous section to determine the fingerprint of the device, that is, the relative fingerprint error between the TX-RX chain of the device.

We respectively extract the phase errors between the transmitter antenna a and the receiver antenna b1, b2, and b3

of multiple wireless router devices from different brands, and obtain the corresponding three sets of RPE through the calculation of Eq. (1). Use them as fingerprints for our subsequent experiments to detect RAP attacks.

For our scheme, the main evaluation criteria are two indicators: (1) Accuracy: including the detection rate and false alarm rate of each known and unknown WIFI device. (2) Stability: The stability of device fingerprints over time and place.

Next, we will conduct detailed experiments around two indicators.

5.1. Accuracy

According to the Eq. (1) mentioned in the third section, and the method mentioned in the previous section, we extract the data frame of the corresponding RPE between the three sets of antennas in each WIFI device from the CSI. Next, we transform it into a drift fan-dimensional matrix. Each group of antennas in each device takes 100 offset values as a group to form a phase error drift range, and plots a group of RPE in a coordinate system. In the coordinate system, the subcarrier sequence is the x-axis (ie −28, −26, ..., −2, −1, 1, 3, ..., 27, 28), and the phase error value of each subcarrier is the y-axis. Because the variation range of the phase error is between -2 and 2, the maximum value of the y-axis is set to 2, and the minimum value is set to -2, so as to reflect the drift range fully. After reading the figure into a matrix, to speed up the network training, the matrix needs to be normalized. The part with a value of 1 in the matrix represents the non-phase error drift range, and the part with a value other than 1 in the matrix represents the phase error drift range. To highlight the phase error drift range and increase the contrast, we set the data within the drift range to 1, and set the data outside the drift range to 0. Next, we use the multimodal CNN neural network we built for testing.

In the experiments, we use a Lenovo PC with an Intel i7-1165g7 processor, and RTX 2080 Ti graphics card to train the deep learning model. The model is built by tensorflow version 2.10.0, using GPU acceleration to improve network training efficiency, and the Python version used is 3.97.

We use the ResNet-50-based model for network training, set the training round epochs to 100, the batch size to 16, the loss function to cross-entropy loss, the optimization algorithm to Adam, and the initial learning rate to 10-4. The output dimensions of the two fully connected layers are 512 and 256, respectively. The middle layer of the network uses the relu activation function, and the output layer uses the softmax activation function. The label of the data is converted into a one-hot value form.

The images generated by the three sets of antennas in each device are taken as a group (the three images have the same size and the same category) and are input into the neural network architecture for classification prediction. We use 500 images collected by each device, 400 for training and 100 for classification prediction. After training the model, the accuracy curve on the training set is obtained, as shown in Fig. 6.

We randomly selected 7 devices from 22 devices as illegal devices, and collected 1000 CSI samples for each device. Fig. 8 shows the detection accuracy of these seven detection devices as abnormal connections. CSI fingerprint collection was performed on 22 devices one by one to detect the legality of the devices. It can be seen from the Fig. 7 that the recognition accuracy of the 22 devices can reach 98%-99%, the loss curve shows a continuous downward trend, and finally approaches 0.05, and the false alarm rate is less than 2%. And for devices of different types, or multiple devices of the same type, our solution can accurately identify obvious or subtle differences between them.

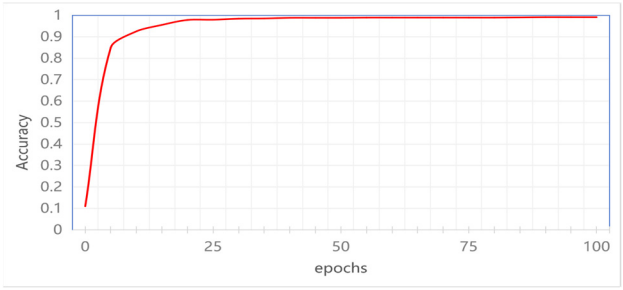


Fig 6. Accuracy changes with epochs

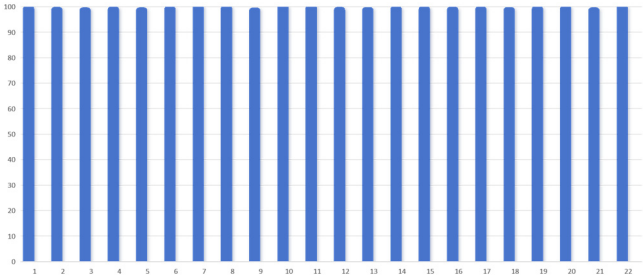


Fig 7. The accuracies of 22 wireless devices

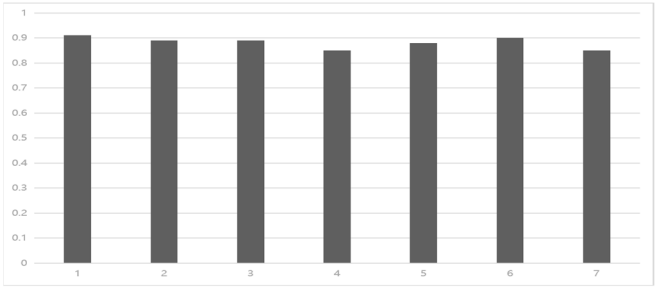


Fig 8. Identification accuracy of rogue connections.

5.2. Stability

5.2.1. Time Stability

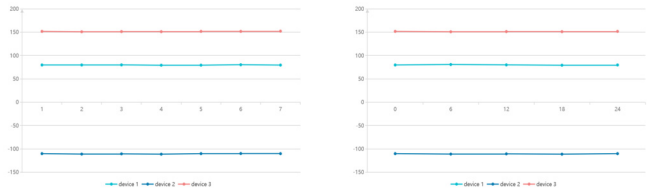
As a valid fingerprint for device identification, it must remain consistent over time. To prove that the relative phase error between the device antennas remains unchanged at different times of the day and for some time, we let the detection device record the CSI information of the three routers TPLINK_1, 360_1, and 360_2 every 6 o'clock in a week, and extract fingerprints. Fig. 9 shows the relative phase errors in the three sets of antennas in the three routers at different times. From the experimental results, it can be observed that regardless of the same type of different devices or different types of devices, their relative phase errors are quite consistent.

5.2.2. Site Stability

Due to the influence of TOF, CSI is sensitive to the location of the environment. Therefore, we need to conduct related experiments to verify whether our fingerprints are affected by location and environment. First, to introduce complex multipath effects, we set the conditions in the above-mentioned experimental environment indoors, and then added coffee shops, classrooms, and dormitories that are prone to malicious AP connections. We conduct multiple relative phase error device identifications in each location and

environment under conditions, record its CSI, and extract fingerprints. We record the relative phase error at different positions, and the TABLE II records the accuracy rate in different environments. The results in TABLE II show that, our fingerprints remain consistent with changes in position, and can still achieve 98% accuracy in dynamic environments.

A large number of experimental results have confirmed that our system can effectively detect malicious APs illegally connecting to WIFI devices.



(a) RPE of four deviceremain invariant across the one week

(b) RPE of four deviceremain invariant across the 24 hours

Fig 9. Invariance of fingerprints wıth respect to tıme

Table 2. Accuracy of WiFi devices in different scenes

Scene	Attack detection rates
coffee shops	98.3%
classrooms	99.1%
dormitories	98.6%
laboratory NLOS	98.8%
laboratory LOS	98.8%

6. Conclusion

This paper demonstrates that the relative phase error between TX chain carriers in the same device can be used as a valid fingerprint of the device. These fingerprints are fairly consistent across time and place, but vary across devices and are not affected by the mobile environment. Therefore, this mechanism can be used for device identification of WiFi devices supporting the 802.11n protocol. A large number of experiments using 22 WIFI devices in multiple scenarios and environments have shown that the accuracy of illegal connections is as high as 98%-99% in static and dynamic environments, and has a very efficient detection process under the multi-modal CNN neural network, which is also the first application of this kind of scheme. The experimental results show that we have significantly improved the accuracy and efficiency of this type of solution, and expanded the applicable background environment. In the future, we hope to use more experiments to prove the robustness and stability of the system to prove that it can be applied to more complex and wider scenarios.

References

[1] S. Jana and S. K. Kasera, “On fast and accurate detection of unauthorized wireless access points using clock skews.” in Proc. of the 14th ACM international conference on Mobile computing and networking (MobiCom’08), 2008, pp. 104–115.

[2] K. Gao, C. Corbett, and R. Beyah, “A passive approach to wireless device fingerprinting,” in 2010 IEEE/IFIP International Conference on Dependable Systems Networks (DSN), June 2010, pp. 383–392.

[3] C. L. Corbett, R. A. Beyah, and J. A. Copeland, “Passive classification of wireless nics during active scanning,” International Journal of Information Security, vol. 7, no. 5, pp. 335–348, Oct 2008.

[4] J. Hua, H. Sun, Z. Shen, Z. Qian, and S. Zhong, “Accurate and efficient wireless device fingerprinting using channel state information,” in IEEEINFOCOM 2018 - IEEE Conference on Computer Communications, April 2018, pp. 1–9.

[5] Boyao Y u*†, Chao Yang*†, and Jianfeng Ma* “Continuous Authentication for the Internet of Things Using Channel State Information”.

[6] Pengfei Liu, Panlong Yang, Wen-Zhan Song, Y ubo Yan, Xiang-Yang Li “Real-time Identification of Rogue WiFi Connections Using Environment-Independent Physical Features”.

[7] K. Gao, C. Corbett, and R. Beyah, “A passive approach to wireless device fingerprinting,” in 2010 IEEE/IFIP International Conference on Dependable Systems & Networks (DSN). IEEE, 2010, pp. 383–392.

[8] V . Brik, S. Banerjee, M. Gruteser, and S. Oh, “Wireless device identification with radiometric signatures,” in Proc. of the 14th ACM international conference on Mobile computing and networking (MobiCom’08), 2008, pp. 116–127.

[9] Z. Jiang, J. Zhao, X. Y . Li, J. Han, and W. Xi, “Rejecting the attack: Source authentication for wi-fi management frames using csi information,” in 2013 Proceedings IEEE INFOCOM, April 2013, pp.2544–2552.

[10] 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, ser. WiSe ’06. New Y ork, NY , USA: ACM, 2006, pp. 33–42. [Online]. Available: http://doi.acm.org/10.1145/1161289.1161297

[11] M. Young, The Techincal Writers Handbook. Mill Valley, CA: University Science, 1989.

[12] J. U. Duncombe, “Infrared navigation—Part I: An assessment of feasibility (Periodical style),” IEEE Trans. Electron Devices, vol. ED-11, pp. 34–39, Jan. 1959.

[13] S. Chen, B. Mulgrew, and P. M. Grant, “A clustering technique for digital communications channel equalization using radial basis function networks,” IEEE Trans. Neural Networks, vol. 4, pp. 570–578, Jul. 1993.

[14] R. W. Lucky, “Automatic equalization for digital communication,” Bell Syst. Tech. J., vol. 44, no. 4, pp. 547–588, Apr. 1965.

[15] S. P. Bingulac, “On the compatibility of adaptive controllers (Published Conference Proceedings style),” in Proc. 4th Annu. Allerton Conf. Circuits and Systems Theory, New York, 1994, pp. 8–16.

[16] G. R. Faulhaber, “Design of service systems with priority reservation,” in Conf. Rec. 1995 IEEE Int. Conf. Communications, pp. 3–8.

[17] J. G. Kreifeldt, “An analysis of surface-detected EMG as an amplitude-modulated noise,” presented at the 1989 Int. Conf. Medicine and Biological Engineering, Chicago, IL.

[18] J. Williams, “Narrow-band analyzer (Thesis or Dissertation style),” Ph.D. dissertation, Dept. Elect. Eng., Harvard Univ., Cambridge, MA, 1993.

[19] N. Kawasaki, “Parametric study of thermal and chemical nonequilibrium nozzle flow,” M.S. thesis, Dept. Electron. Eng., O.