Design of A Channel Robust Radio Frequency Fingerprint Identification Scheme

Yuexiu Xing, Aiqun Hu, Junqing Zhang, *Member, IEEE,* Linning Peng, and Xianbin Wang, *Fellow, IEEE*

***Abstract*—Radio frequency fingerprint (RFF) identification is an emerging device authentication technique that exploits the hardware imperfections resulting from the manufacturing process. Due to the varying impact of the wireless channel during RFF training and test stages, it is challenging to design channel-independent RFF techniques. This paper designs a channel robust RFF identification scheme by leveraging the different spectrum of adjacent signal symbols, named the difference of the logarithm of the spectrum (DoLoS), which does not rely on a single RFF feature or requires additional manipulation of the devices under test. Specifically, DoLoS exploits the fact that two different symbols in a packet exhibit different RFF features but have a similar channel response during the channel coherence time. We implemented the DoLoS with the IEEE 802.11 orthogonal frequency division multiplexing (OFDM) system as a case study. We carried out extensive experiments using 7 Wi-Fi devices of the same model in different wireless channel environments, including 12 data collection positions in two completely different environments. Compared with conventional RFF identification schemes that do not eliminate channel effects, our scheme is robust to channel variations and the highest identification accuracy is 99.02% in the single-environment evaluation and 97.05% in the cross-environment evaluation.**

***Index Terms*—Device authentication, radio frequency fingerprint, 802.11, OFDM, wireless channel**

I. Introduction

WIRELESS communication technologies are rapidly evolving, leading to 5G-and-beyond network, Internet of things (IoT) and many applications enabled by them. However, the widespread deployment of radio transmissions are accompanied by increasingly serious security breaches [1], [2], due to the broadcast nature of wireless communication signals. Device authentication is an essential part of achieving communication security by authorizing legitimate users and rejecting malicious ones. Traditional cryptography-based authentication schemes, such as password-based authentication and certificate-based authentication, have some limitations when applied to IoT devices [3], [4]. These schemes require computational and energy resources, which may not be suitable for resource-constrained IoT devices, e.g., radio-frequency identification (RFID) chips. In addition, the secure storage of passwords is challenging and it is at the risk of being cracked by high-computing attackers or intercepted during login [5], [6]. Finally, the public key infrastructure (PKI) in certificate-based authentication may increase the initial deployment cost. Therefore, it is desirable to design an effective and low-cost device identification scheme for IoT.

Radio frequency fingerprint (RFF) identification has emerged as an effective and lightweight solution for device authentication [7]–[9], which is particularly suitable for IoT. In any wireless communication system, the baseband signal is processed by the transmitter components including the digital to analog converter (DAC), filter, mixer, oscillator, power amplifier, etc., and then becomes a radio frequency signal. The hardware involved has unavoidable imperfections during the manufacturing process, including the mismatch between the In-phase (I) and Quadrature (Q) branches of the mixer, power amplifier nonlinearity, etc. However, these imperfections are usually within the tolerance of the nominal values, which only slightly distort transmitted signals without severely impact the communication functions [10]. These hardware impairments are collectively referred to as RFF. RFF is device-specific and difficult to forge and tamper. Furthermore, RFF has good environmental robustness and long-term stability [11], [12] Therefore, it can be extracted for device identification.

RFF identification consists of two stages, namely training and identification stages [13]. In the training stage, a receiver extracts the RFF features of each legitimate device under test (DUT) and then trains them using a classifier such as the convolutional neural network (CNN) or distance-based classifiers, etc. In the identification stage, the authenticator collects signals from a device, extract RFF features, and infer its identity using the trained classifier.

RFF identification has been investigated for several wireless systems, such as Wi-Fi [14]–[18], ZigBee [11], [19], radar [20]–[22], LoRa [23], etc. Among them, Wi-Fi is one of the most popular wireless technologies and much RFF identification work uses Wi-Fi as case studies. For example, Brik *et al.* [14] utilized several RFF features including carrier frequency offset (CFO), in-phase/quadrature (I/Q) offset, and

This work was supported in part by Research Foundation for Advanced Talents, Nanjing University of Posts and Telecommunications (XK0160921022); in part by Research Fund of Jiangsu Provincial Double-Innovation Doctor Program. The work of J. Zhang was in part supported by UK Royal Society Research Grants under grant ID RGS/R1/191241. The associate editor coordinating the review of this paper and approving it for publication was xx. (*Corresponding author: Y. Xing.*)

Y. Xing is with the School of Internet of Things, Nanjing University of Posts and Telecommunications, 210003 Nanjing, China. (e-mail: yxxing@njupt.edu.cn).

A. Hu is with the School of Information Science and Engineering, Southeast University, 210096 Nanjing, China. (e-mail: aqhu@seu.edu.cn).

J. Zhang is with the Department of Electrical Engineering and Electronics, University of Liverpool, Liverpool, L69 3GJ, United Kingdom. (email: junqing.zhang@liverpool.ac.uk).

L. Peng is with the School of Cyber Science and Engineering, Southeast University, 210096 Nanjing, China. (e-mail: pengln@seu.edu.cn.).

A. Hu and L. Peng are also with the Purple Mountain Laboratories for Network and Communication Security, Nanjing, 210096, China.

X. Wang is with the Department of Electrical and Computer Engineering, Western University, London, Ontario, N6A 5B9, Canada. (email: xianbin.wang@uwo.ca)

Digital Object Identifier xxx

phase error. They evaluated 130 Wi-Fi devices and achieved 99% accuracy. In practical applications, wireless channels of training data and test data are usually different due to the varying environments and locations of data collection. Furthermore, the wireless channel has a severer effect to the signal distortion than RFF. Then, the RFF identification accuracy will be greatly affected by the varying wireless channels. For example, Al-Shawabka *et al.* [17] carried out extensive experiments on 20 Wi-Fi devices and found out that the wireless channel significantly affected the classification accuracy, which dropped from 85% (train-and-test-one-day) to 9% (train-one-day-test-another). The experiments in [18] also showed a similar phenomenon.

Therefore, designing a channel robust RFF identification scheme is challenging but highly desirable. The current research efforts can be divided into three categories. The first category is to extract RFF features that are independent from channels such as CFO. Vo-Huu *et al.* [24] evaluated the RFF-based Wi-Fi device identification using CFO and transients on an in-the-wild testbed. Hua *et al.* [25] demonstrated that CFO obtained from the channel state information (CSI) is an effective RFF feature, which remains stable over time and locations. However, it requires a large number of signals to extract a CFO, which cannot realize the device identification of single-frame signals. Hou *et al.* [26] proposed a physical layer authentication scheme utilizing CFO. It states that CFO includes a constant bias of the oscillator mis-match and a variable Doppler shift, which is time-varying. Similarly, we also found that the CFO of the same Wi-Fi device has deviations among different frame signals, mainly due to the variable Doppler shift and the instability of the device oscillator. In addition, our experiment showed that the CFOs of different Wi-Fi devices overlapped with each other, which means that CFO-based device identification is prone to misidentification (Section IV). Liu *et al.* [27] extracted the nonlinear phase offset between different subcarriers from CSI as RFF features. Experiments indicated this phase feature is robust to location, environment, and time. However, the types, brands, and models of Wi-Fi terminals in their experiments were different, which means that the RFF differences among devices are more obvious. The identification performance of the same model of devices requires further investigation.

The second category is to manipulate transmitters to construct channel robust features. Sankhe *et al.* [18] amplified the RFF features by adding device hardware impairments, such as I/Q imbalance and direct current (DC) offset. However, this approach requires a secure feedback channel between the transmitter and the receiver, which may not be available. The interaction will also increase additional overhead. Restuccia *et al.* [28] designed a digital finite input response filter at the transmitter to resist channel interference, which is achieved by slightly modifying transmitted signals based on the known current channel. This also requires the receiver to send the designed filter information to DUTs, which brings communication overhead and delay.

The last category is to eliminate channel effects by signal processing algorithms. Kennedy *et al.* [29] and Fadul *et al.* [15] presented to eliminate channel interference through channel estimation and channel equalization. However, the channel estimation process will be influenced by the RFF. In theory, such schemes require data without channel effects as the training set, which may be difficult to obtain in practical applications. Liu *et al.* [30] estimated the channel coefficients by using known training sequences to approximate the symbols with low-amplitude levels. It was mainly based on the fact that symbols with lower amplitude levels have relatively lower distortion levels. However, this approach was only evaluated on the identification of two simulated transmitters, hence the performance requires further experimental verification. Li *et al.* [31] proposed to extract the different features between two long training symbols (LTSs) in IEEE 802.11 OFDM signals. This method requires signals collected from multiple locations to generate the RFF features, which is difficult in practical applications. Zheng *et al.* [32] proposed an $\mathcal{F}(\cdot)$ function as the RFF to model the modulation and timing errors, CFO, and power amplifier noise of the device. However, its channel estimation is affected by RFF and noise, so the algorithm may not learn exactly the channel.

In order to address the above challenges and limitations, this paper designs a channel robust RFF identification scheme, which does not rely on a single feature or requires extra resources to manipulate DUTs. Specifically, we proposed an RFF extraction algorithm, which exploits the Difference of the Logarithmic Spectra (DoLoS) of the received signals. The main contributions are summarized as follows:

- We proposed a DoLoS algorithm to extract channel-independent RFF features. The algorithm first obtains two different symbols with different amplitudes and phases from the received signals; these symbols exhibit different RFF characteristics. When the two symbols are within the channel coherence time, during which the channel can be assumed stationary, the difference between the logarithmic spectrum of the two symbols can effectively eliminate the channel response but retain the RFF features.
- We implemented the proposed DoLoS algorithm with IEEE 802.11 OFDM as a case study. Specifically, we use the short training symbol (STS) and LTS in the preamble of the physical waveform which have different amplitudes and phases. In addition, we leverage the repeated symbols to denoise the received signals and further refine the received data by removing anomaly ones.
- We carried out extensive experimental evaluation and demonstrated our algorithm can effectively extract channel-independent RFF features. We have collected 84,000 packets from 7 Wi-Fi devices of the same model. Specifically, 1,000 data packets were collected from each position of each WiFi router for experiment evaluation. We used DoLoS algorithm to extract the channel robust RFF features and employed a CNN classifier for identification. Compared with the method without removing channel effects, the highest increase in the identification rate is 68.75%. In addition, denoising and data refining algorithms have brought 7.30% and 2.75% performance improvement on average, respectively.

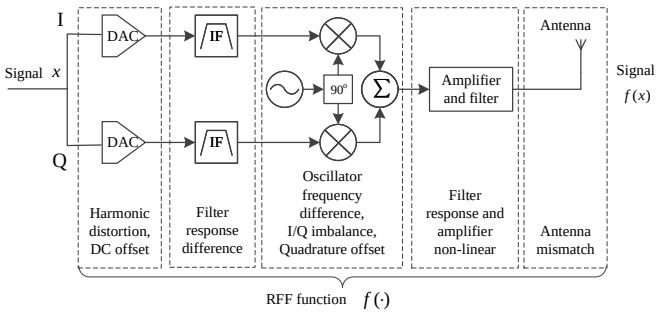


Fig. 1. System module of RFF sources.

The remainder of this paper is organized as follows. Section II gives the channel robust RFF identification scheme and the DoLoS algorithm. Section III introduces the preamble structure of IEEE 802.11 OFDM systems. Section IV presents a case study of implementing the DoLoS algorithm on IEEE 802.11 OFDM devices. Section V and Section VI show the experimental setup and performance evaluation, respectively. Finally, Section VII concludes this paper.

II. Channel Robust RFF Identification

A. System Model

RFF is the collective term for device hardware impairments. It can be seen from Fig. 1 that the hardware impairments in a typical transmitter mainly come from DAC, intermediate frequency (IF) filter, I/Q modulation block, amplifier, and antenna, including harmonic distortion, DC offset, poor filter response, oscillator frequency difference, I/Q imbalance, quadrature offset, amplifier non-linear, antenna mismatch, etc. Considering the transmitter as a black box, the effect of RFF on the signal to be transmitted x can be denoted as a function $f_i(\cdot)$, and the $f(x)$ is the signal after hardware distortion.

As shown in Fig. 2, there are N legitimate devices to be classified by a receiver. A CNN model is adopted as the classifier.

The received signal can be written as

$$y_{i,p} = f_i(x) * h_p + n_p,\ i = 1, 2, \cdots, N, \tag{1}$$

where $f_i(x)$ is the signal of device i with RFF, $*$ represents linear convolution operation, $p = \{T, I\}$ represents the training and identification stage, respectively, h_p is the wireless channel effect, and n_p denotes the additive white Gaussian noise (AWGN).

It can be seen in (1) that the received signal consists of both the hardware imperfection $f_i(\cdot)$ and the channel effect h_p. As the hardware imperfection is usually very slight, the wireless channel has a more dominant effect. In addition, the wireless channel varies with the environment, location, and time. Thus, h_T and h_I will be different for training and identification stages because they will probably be carried out at different places and time in practical applications. Therefore, it is essential to design a robust algorithm to eliminate channel effects and extract channel-independent RFF.

B. DoLoS Algorithm

We proposed a channel robust RFF feature extraction algorithm based on the Difference of the Logarithmic Spectra of received signals, named DoLoS.

There are three conditions for the transmitted signal x to be met, required by the DoLoS algorithm.

- There should be at least two fixed and different symbols x^A and x^B in the signal x, as shown in Fig. 2. The hardware components, such as filters and power amplifiers, have different responses to signals with different amplitudes and phases, hence the RFF of different symbols will also be different, i.e., $f_i(x^A) \neq f_i(x^B)$.
- Symbols x^A and x^B both have the cyclic prefix (CP), which refers to the prefixing of a symbol, with a repetition of the end. Multiple repetitive symbols can also form the CP structure. In some techniques, e.g., OFDM, the CP is intentionally designed as a guard interval to eliminate inter-symbol interference. As a CP repeats the end of the symbol, the linear convolution of the symbol and the multipath channel can be modeled as the circular convolution between them. Thus, the received signal can be transformed into the frequency domain via the fast Fourier transform (FFT).
- The symbols x^A and x^B should be within the channel coherence time, during which wireless channels experienced by the symbols x^A and x^B can be considered the same.

Thanks to the CP, linear convolution operation can be converted to circular convolution operation. The received signals in the time domain can be given as

$$y_{i,p}^{sym} = f_i(x^{sym}) \circledast h_p + n_p^{sym}, \tag{2}$$

where $sym = \{A, B\}$ represents symbols A and B, respectively, $\circledast$ donates circular convolution.

The time-domain signal, $y_{i,p}^{sym}$, can be transformed to the frequency domain by FFT, expressed as

$$\begin{aligned} Y_{i,p}^{sym} &= \mathcal{FFT}(y_{i,p}^{sym}) \\ &= \mathcal{FFT}(f_i(x^{sym}))\mathcal{FFT}(h_p) + \mathcal{FFT}(n_p^{sym}), \end{aligned} \tag{3}$$

where $\mathcal{FFT}(\cdot)$ represents FFT operation.

Next, without considering the noise, we can convert the amplitude of the frequency domain signal from a linear scale to the logarithmic scale, which can be given as

$$\begin{aligned} Y_{i,p,\log}^{sym} &= \log[|Y_{i,p}^{sym}|] \\ &= \log[|\mathcal{FFT}(f_i(x^{sym}))|] + \log[|\mathcal{FFT}(h_p)|], \end{aligned} \tag{4}$$

where $\log(\cdot)$ denotes natural logarithm and $|\cdot|$ represent absolute value operation.

Finally, we can remove the channel effect through a simple subtraction operation as

$$\begin{aligned} RFF_{i,p} &= Y_{i,p,\log}^{A} - Y_{i,p,\log}^{B} \\ &= \log[|\mathcal{FFT}(f_i(x^A))|] - \log[|\mathcal{FFT}(f_i(x^B))|]. \end{aligned} \tag{5}$$

It can be observed that the $RFF_{i,p}$ is only affected by x^A, x^B, and the hardware effect $f_i(\cdot)$. Different devices will

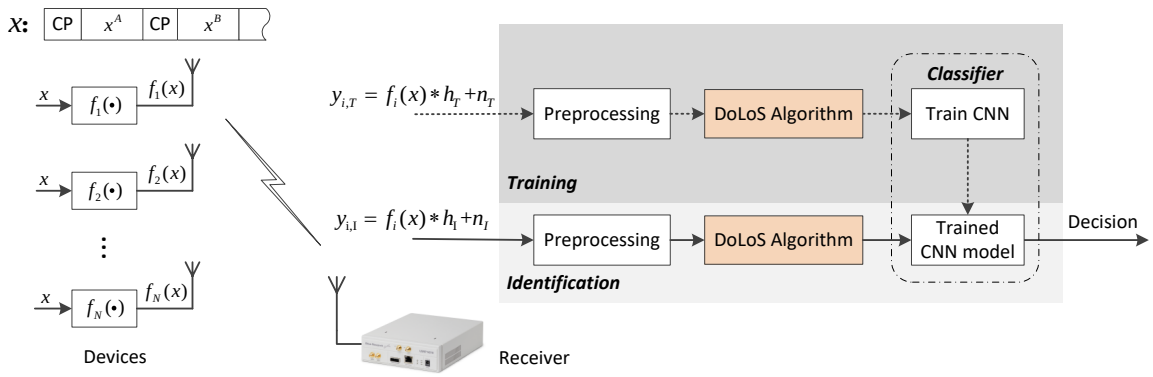


Fig. 2. DoLoS-based RFF identification.

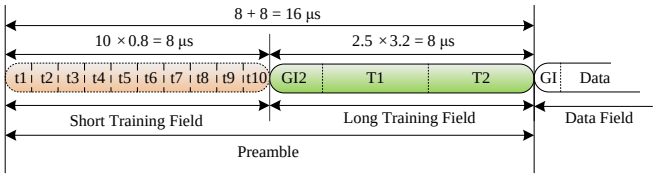


Fig. 3. The preamble structure of the IEEE 802.11 OFDM.

transmit the same symbols x^A and x^B while the hardware imperfection, $f_i(\cdot)$, is different among devices. Therefore, $RFF_{i,p}$ can represent the device's RFF features for device identification, which is channel independent.

III. Preliminary: IEEE 802.11 OFDM

IEEE 802.11 OFDM is chosen as a case study to verify the proposed channel robust RFF identification scheme. In this section, we will introduce the IEEE 802.11 OFDM physical layer packet format. The DoLoS algorithm implementation will be introduced in Section IV.

The Wi-Fi devices used in our experiments are in the IEEE 802.11n legacy mode, i.e., the IEEE 802.11 OFDM. OFDM is first employed by IEEE 802.11a (1999) and becomes very successful because of the high spectrum efficiency and robust to inter-symbol interference. Hence, it is adopted by the IEEE 802.11g/n/ac. Wi-Fi has become one of the most popular communication technologies, which is widely used in laptops, tablets, smartphones, etc.

There are 64 sub-carriers over a 20 MHz OFDM channel. Among them, there are 52 active sub-carriers, i.e., sub-carrier [-26 -1] and [1 26], while the rest are used as guard bands. As shown in Fig. 3, IEEE 802.11 OFDM standard defines a preamble at the beginning of the packet, which consists of a short training field (STF) and a long training field (LTF). STF and LTF are predefined public sequences and all the Wi-Fi compliant devices should follow. The STF is used for packet detection, CFO estimation, and automatic gain control while the LTF is employed for symbol alignment and channel estimation [33].

Specifically, the STF is composed of ten repetitive STSs, t1, t2, ..., t10. Each STS is generated as follows. A frequency-domain STS utilizes 12 sub-carriers with indices

$$\varsigma = [-24, -20, -16, -12, -8, -4, 4, 8, 12, 16, 20, 24] \quad (6)$$

and each subcarrier is quadrature phase shift keying (QPSK) modulated, which can be defined as

$$\begin{aligned}\mathcal{S} =& 1.472 \times \{0, 0, 1+j, 0, 0, 0, -1-j, 0, 0, 0, 1+j, \\ & 0, 0, 0, -1-j, 0, 0, 0, -1-j, 0, 0, 0, 1+j, 0, 0, 0, \\ & 0, 0, 0, 0, -1-j, 0, 0, 0, -1-j, 0, 0, 0, 1+j, \\ & 0, 0, 0, 1+j, 0, 0, 0, 1+j, 0, 0, 0, 1+j, 0, 0\}.\end{aligned} \quad (7)$$

$\mathcal{S}$ is transformed into the time domain using a 64-point FFT operation. The output contains four identical sequences, t, each with 16 samples. Then, one sequence is repeated 10 times to obtain a complete STF.

There are 52 active subcarriers in the LTS and the frequency domain LTS is defined as

$$\begin{aligned}\mathcal{L} =& \{1, 1, -1, -1, 1, 1, -1, 1, -1, 1, 1, 1, 1, 1, \\ & 1, -1, -1, 1, 1, -1, 1, -1, 1, 1, 1, 1, 0, 1, -1, \\ & -1, 1, 1, -1, 1, -1, 1, -1, -1, -1, -1, -1, 1, \\ & 1, -1, -1, 1, -1, 1, -1, 1, 1, 1, 1\},\end{aligned} \quad (8)$$

which is binary phase shift keying (BPSK) modulation. $\mathcal{L}$ is also transformed to the time domain LTS using a 64-point FFT operation. The time-domain LTF is constructed by one CP (GI2), and two LTSs (T1, T2).

The STF and LTF meet the three conditions required by the DoLoS algorithm.

- The STF and LTF are present in all the IEEE 802.11 OFDM packets. In addition, STF (QPSK modulated) and LTF (BPSK modulated) have different amplitudes and phases, which will lead to different RFF.
- The LTF has a designated CP (GI2) and the STF has ten repetitions of STS which can form the CP structure.
- STF and LTF are adjacently contained in a preamble and their duration is 16 μs, which is much smaller than the channel coherence time in most scenarios, such as Vehicle-to-Vehicle scenario (includind suburban, highway and rural) , walking scenario, the static indoor scenario [34], [35]. Hence, their channel responses can be assumed the same.

Therefore, we used Wi-Fi as a case study to evaluate our

proposed DoLoS algorithm. In addition, multiple repetitive symbols can also form a CP structure.

IV. Case Study: IEEE 802.11 OFDM-Based RFF Identification

In this section, the RFF-based identification of IEEE 802.11 OFDM devices is introduced as a case study of the proposed channel robust RFF identification scheme. Corresponding to Fig. 2, the preprocessing in this case study includes packet detection, CFO compensation, and denoising. In the training stage, the channel-independent RFF features extracted by the DoLoS algorithm are used to train a two-layer CNN as the classifier. In the identification stage, the RFF features of the unknown signal will be identified by the trained CNN model.

A. Preprocessing

1) Packet Detection: In a standard IEEE 802.11 OFDM system, the receiver employs the autocorrelation algorithm using the repeated STS to detect the signal arrival and then the cross-correlation algorithm using LTS to locate the starting point of the packet. We used these standard algorithms and interested readers please refer to [33] for details.

The preamble part of a received signal is illustrated in Fig. 4(a). There are 10 STSs (r1, r2, ..., r10) in STF and two LTSs (R1, R2) in LTF. As shown in Fig. 4(a), the received signals differ greatly from the local standard preamble due to the channel effect and noise, but their periodic characteristics maintain (10 repeated STSs in STF and 2.5 LTSs in LTF). The normalized autocorrelation coefficient is illustrated in Fig. 4(b), which clearly shows the plateau of high autocorrelation coefficients. Then we can roughly estimate the start of the packet. The start of the first LTS can be accurately detected from the correlation coefficients.

The first STS is discarded as there is no signal before it, which does not satisfy the condition of CP. In addition, a 64-point FFT operation requires four STS (each has 16 samples) as input, hence we concatenated four consecutive STSs as a valid time-domain OFDM symbol. We can then extract y_i^{sym} from the packets, where $sym = \{\{sts1, sts2\}, \{lts1, lts2\}\}$ denote STS and LTS, respectively.

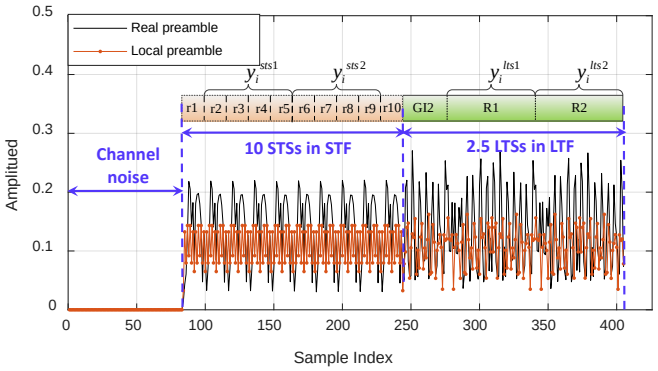
2) CFO Compensation: Influenced by the oscillator drift of transmitter and receiver as well as the Doppler shift of the wireless channel [26], there will be CFO between the transmitter and receiver, which brings distortion to the signals.

In this paper, we used the ten repeated STSs to estimate the CFO, as described in [33]. As shown in Fig. 5, even if the Wi-Fi device has been running for half an hour in advance, the collected CFO of different Wi-Fi devices vary in a short time and overlap with each other. The main reason is the variable Doppler shift and the instability of the device oscillator. Hence, it is necessary to estimate and compensate CFO before the RFF feature extraction.

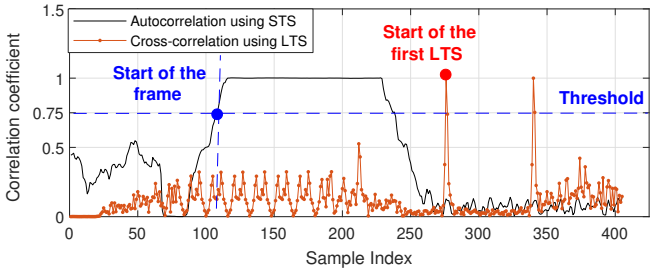
The symbols after CFO compensation can be given as

$$\hat{y}_i^{sym}(n) = y_i^{sym}(n) e^{j2\pi \Delta f n T_s}, \tag{9}$$

where Δf is the estimated CFO and T_s is the sampling interval, which is 50 ns in this paper.



(a) Real received preamble and local standard preamble.



(b) Correlation coefficient.

Fig. 4. Packet detection.

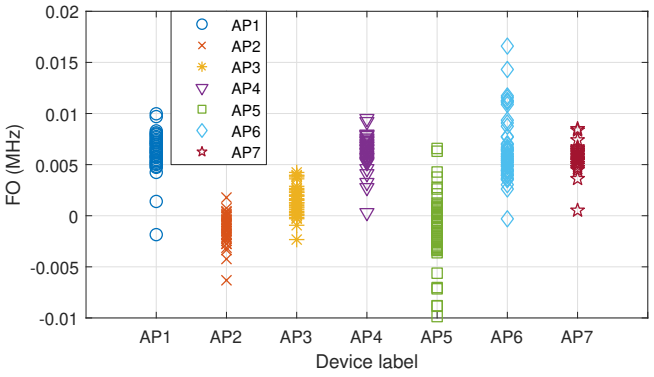


Fig. 5. CFO distribution of 7 Wi-Fi devices.

3) Denoising: In order to suppress noise, we consider a denoising method designed in [36], which leverages the repeatability of STS and LTS, given as

$$\begin{aligned} \hat{y}_i^{sts} &= \frac{1}{2}\left(\hat{y}^{sts1} + \hat{y}^{sts2}\right), \\ \hat{y}_i^{lts} &= \frac{1}{2}\left(\hat{y}^{lts1} + \hat{y}^{lts2}\right). \end{aligned} \tag{10}$$

Therefore, the SNR for STS and LTS can be increased by up to 2 times.

B. RFF Extraction Using DoLoS Algorithm

The logarithmic spectrum of the extracted symbol $\hat{y}_i^{sym}$ can be given as

$$Y_{i,\log}^{sym} = \log\left[\left|\left(\mathcal{FFT}(\hat{y}_i^{sym})\right|\right]\right. . \tag{11}$$

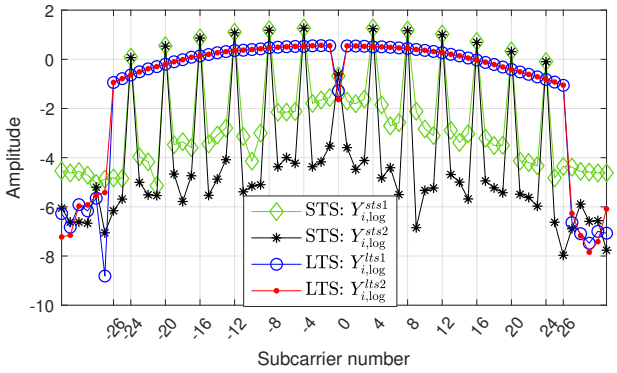


Fig. 6. Logarithmic spectrum of the valid symbols of STS and LTS.

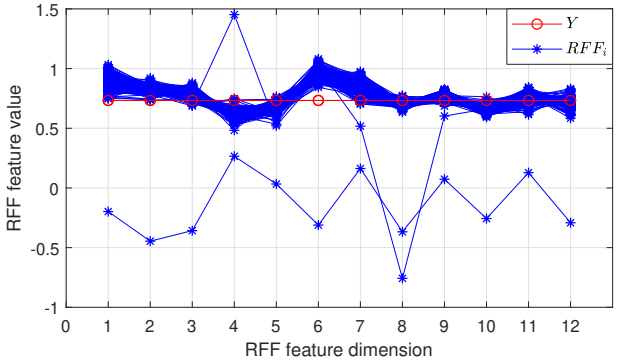


Fig. 7. Comparison of actual signal's RFF features of i^{th} device, RFF_i, with the theoretical results without considering RFF, Y.

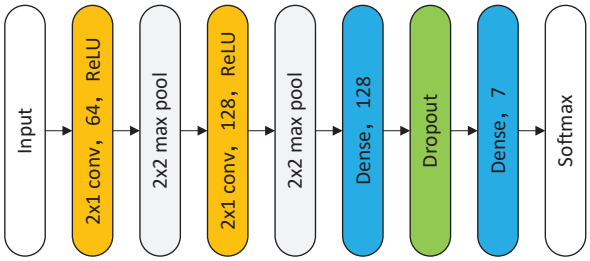


Fig. 8. The architecture of CNN model.

An example is given in Fig. 6. It can be seen that the subcarriers used by STS and LTS are not the same, which is in accordance with the 802.11 OFDM protocol introduced in Section III. We need to extract a common subset of subcarriers, namely ς defined in (6), from $Y^{sym}_{i,\log}$. Specifically, $Y^{sym}_{i,\log}$ contains 64 data points, which can be numbered [1 64]. Then, the point $[9, 13, 17, 21, 25, 29, 37, 41, 45, 49, 53, 57]$ of $Y^{sym}_{i,\log}$ corresponds to the subcarrier numbered $\varsigma = [-24, -20, -16, -12, -8, -4, 4, 8, 12, 16, 20, 24]$. It can be seen from Fig. 6 that there is a good match between $Y^{sts1}_{i,\log}$ and $Y^{sts2}_{i,\log}$ and between $Y^{lts1}_{i,\log}$ and $Y^{lts2}_{i,\log}$. Hence, it is valid to carry out the denoising algorithm.

We extract the data corresponding to these subcarriers from $Y^{sym}_{i,\log}$, carry out denoising and obtain the final RFF features, given as

$$\begin{aligned} RFF_i =& Y^{sts}_{i,\log}(\varsigma) - Y^{lts}_{i,\log}(\varsigma) \\ =& \log\left[|\mathcal{FFT}(\hat{y}^{sts}_i)|\right](\varsigma) - \log[|\mathcal{FFT}(\hat{y}^{lts}_i)|](\varsigma), \end{aligned} \tag{12}$$

which is a vector with 12 dimensions. Some examples are shown in Fig. 7, where the signals were captured from the same Wi-Fi device.

C. Data Refining

According to the 802.11 OFDM protocol, the theoretical amplitudes of the STS and LTS of the common subcarriers in the frequency domain are 1.472 and 1, respectively. Without considering the RFF, the theoretical amplitude of the difference of logarithm spectra should be

$$Y = \log(|\mathcal{S}'|) - \log(|\mathcal{L}'|)| = 0.7332I, \tag{13}$$

where

$$\begin{aligned} \mathcal{S}' =& 1.472[1+j, -1-j, 1+j, -1-j, -1-j, \\ & 1+j, -1-j, -1-j, 1+j, 1+j, 1+j, 1+j] \end{aligned}$$

and $\mathcal{L}' = [-1, -1, 1, 1, -1, 1, 1, -1, -1, 1, -1, 1]$ are the values of STS and LTS on the common subcarriers, respectively, I is a 12 dimensions unit vector.

Fig. 7 displays the RFF features obtained from actual signals and the theoretical amplitudes. Firstly, it is clear that theoretical results Y is 0.7332 for all dimensions, whose mean and variance are 0.7332 and 0, respectively. However, due to the existence of RFF in the actual signal, the value of RFF_i for one device has a small and relatively stable deviation from the theoretical value Y in various dimensions.

The extracted RFF features of different packets are not exactly the same due to the residual channel effects and noise. It is possible some packets have poor quality and the extracted RFF features will be noisy, as shown in Fig. 7. We can refine RFF features which satisfy the following conditions:

$$\begin{aligned} \mu_l \le mean(RFF_i) \le \mu_h; \\ \delta_l \le var(RFF_i) \le \delta_h, \end{aligned} \tag{14}$$

where $mean(\cdot)$ and $var(\cdot)$ denote the mean and variance operations, μ_l, μ_h and δ_l, δ_h are the lower and upper thresholds of mean and variance, respectively. Thereby, the packets whose quality is too poor can be removed.

In practical applications, the distribution of the mean and variance values of target devices with different brands or models will vary. Hence, different thresholds are required. Fortunately, the training data set can always be obtained in advance. We can select reasonable thresholds based on the mean and variance distribution of the training set.

D. RFF Identification Using CNN

After data refining, we use the training data to train a CNN model. The final RFF features RFF_i is a 12-dimensional vector, which is small size. Hence, we choose a two-layer CNN model, whose network depth is basically the same as a well-run network on the MNIST dataset [37].

The network architecture are given in Fig. 8. There are two convolutional layers, two dense layers, and a softmax classifier.

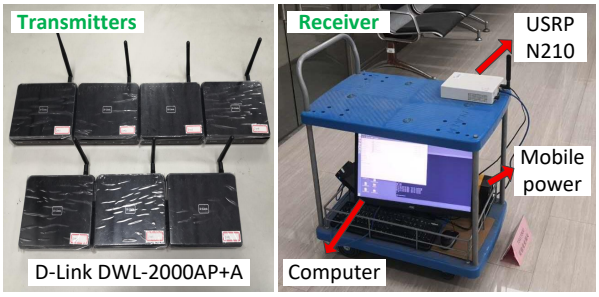


Fig. 9. Photo of Wi-Fi devices and the receiver.

The rectifying linear unit (ReLU) activation function is used. To train the CNN, the categorical cross-entropy is used as the loss function.

We define the identification accuracy rate ξ as

$$\xi = \frac{N_c}{N_{all}}, \tag{15}$$

where N_{all} is the number of packets to be identified and N_c is the number of correctly identified packets. We also use the confusion matrix to visualize the classification performance.

V. Experimental Setup

A. Devices

The devices involved in the experiment include the WiFi device to be identified and the receiver.

Wi-Fi DUT: As shown in Fig. 9(a), seven Wi-Fi routers of the same model, namely DWL-2000AP+A, were tested as DUTs, which were purchased in bulk from D-Link manufacturers. In the experiments, their working protocol, carrier frequency, and bandwidth were configured as IEEE 802.11n, 2.4 GHz, and 20 MHz, respectively.

Receiver: As shown in Fig. 9(b), we used a software-defined radio (SDR) device, namely Ettus universal software radio peripheral (USRP) N210 with a UBX daughterboard, to collect signals from DUTs. The sampling rate was set to 20 MS/s. In addition, we placed it on a mobile cart equipped with a mobile power supply to facilitate movement. The data collected by the USRP N210 was stored in the host computer for our RFF identification algorithm. The data processing and RFF extraction were carried out by MATLAB R2018b. The CNN model was trained and tested using NVIDIA GeForce GTX 1660 Ti GPU on TensorFlow 1.13.1 and Keras 2.2.4.

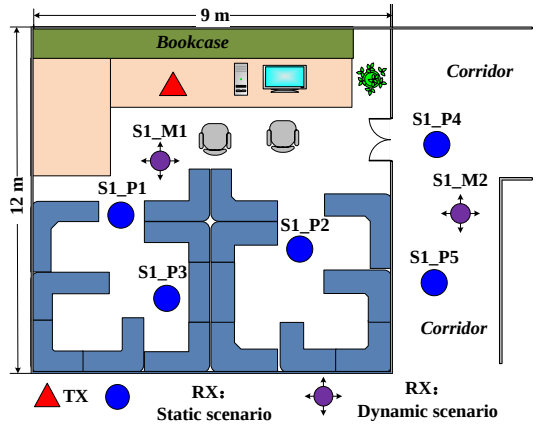
B. Experimental Environments

The main purpose of this paper is to study the impact of wireless channels on RFF identification. Therefore, we evaluated our approach under two experiments with different wireless environments. Their photos and layout are displayed in Fig. 10 and Fig. 11, respectively.

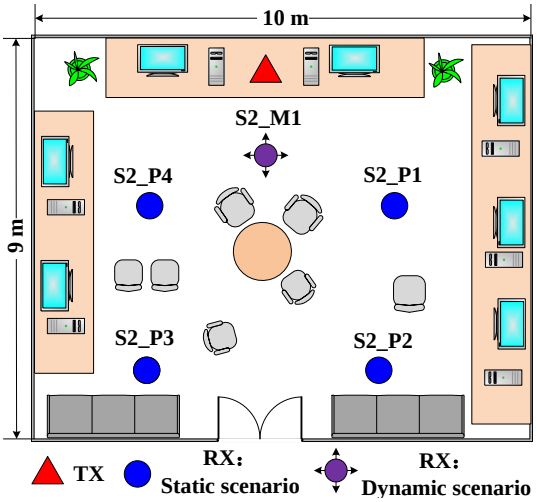
Experiment Environment 1 includes an office and a corridor, as shown in Fig. 10(a) and Fig. 11(a). The size of the office is 9 m $\times$ 12 m, and there is a large bookcase, two laboratory tables, several tables with partitions, chairs

(a) Environment 1. (b) Environment 2.

Fig. 10. Photos of the experiment environments.



(a) Environment 1.



(b) Environment 2.

Fig. 11. Layout of the experiment environments.

and a lot of sundries. The environment is crowded and the multipath effect is severe. The corridor is simply furnished, with only two rows of tables and chairs. In addition, the iron door connecting the office and the corridor was closed during the experiment.

Experiment Environment 2 is a laboratory with a size of 9 m $\times$ 10 m. Compared with Environment 1, the laboratory is relatively empty. A table and a few chairs are scattered in the middle of the room while other obstacles are distributed around the room, such as tables, sofas, computers and monitors.

C. Experimental Scenarios

There are two scenarios considered regarding the receiver movement, namely a static scenario and a dynamic scenario.

Static Scenario: A Wi-Fi router (DUT) and the USRP receiver were placed at the TX and RX positions, respectively. For each data collection process, the receiver remained stationary at a fixed position. As shown in Fig. 11(a), for Environment 1, the receiver collected data at five fixed positions, where S1_P1, S1_P2, and S1_P3 were located in the office, and S1_P4 and S1_P5 were set on the corridor. Due to the closed iron door, when the receiver was located at the positions of S1_P4 and S1_P5, there is no direct line-of-sight (LOS) path between the DUT and the receiver. For Environment 2 shown in Fig. 11(b), the fixed positions are S2_P1, S2_P2, S2_P3, and S2_P4. The router and receiver always have a direct line-of-sight (LoS) path. There were random movement in the lab and the wireless channel was varying.

Dynamic Scenario: A Wi-Fi router (DUT) was placed in the position TX and the USRP receiver moved at an average speed of 1 m/s. The movement route and direction were random. As shown in Fig. 11(a), Environment 1 contained two dynamic data collection areas, namely the office room (S1_M1) and the corridor (S1_M2). Environment 2 demonstrated in Fig. 11(b) had one dynamic scenario, i.e., the entire laboratory room. There were people walking around the room, which might occasionally block the LoS between the router and the receiver.

D. Data Collection

The data sets used in this paper were collected in two different environments (Environment 1 and Environment 2), and the data collection took place four months apart. In a data collection experiment, one DUT was fixed at the TX position and the receiver was placed in different RX positions (including fixed positions in the static scenario and moving areas in the dynamic scenario) to collect data. We collected 1,000 data packets from each position of each WiFi router, for a total of 1,000*7*12=84,000 packets. The recorded data set of 7 Wi-Fi routers, hereinafter referred to as AP1-AP7.

VI. Experimental Results

To evaluate the performance of our scheme, we conducted data collection and analysis at multiple positions in two different environments, respectively. First, we analyzed the channel characteristics of the original signal and the extracted RFF features after using the DoLoS algorithm. Then, we presented the RFF identification results, including the evaluation of DoLoS algorithm, the evaluation of denoising and data refining method, and the evaluation of cross-environment identification. Finally, we compared the performance of our scheme with solutions using IQ data and FFT data.

A. Results of Channel and RFF Features

1) Channel Characteristics: Fig. 12 shows the logarithmic spectrum of STS, $Y^{sts}_{i,\log}(\varsigma)$, and LTS, $Y^{lts}_{i,\log}(\varsigma)$, extracted from

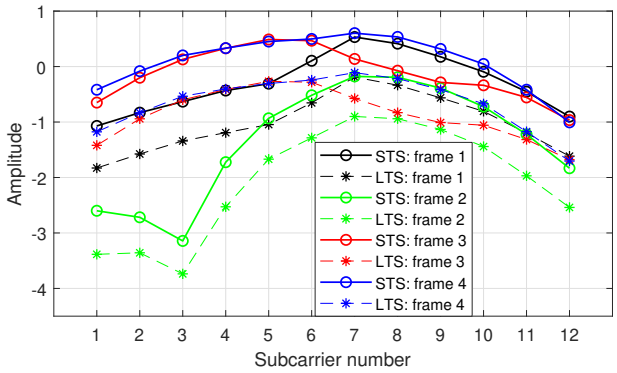


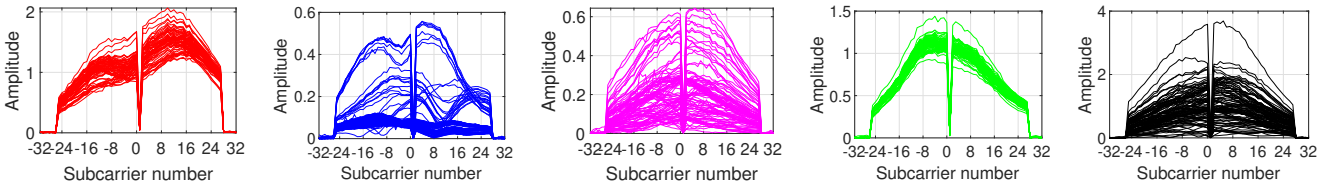
Fig. 12. Comparison of the logarithmic spectrum of STS and LTS in 12 valid subcarriers, i.e., $Y^{sts}_{i,\log}(\varsigma)$ and $Y^{lts}_{i,\log}(\varsigma)$.

four different frames of the same device. It is obvious that these four packets differ greatly in amplitude and trend, which indicates that the channel has a great influence on the spectrum. However, the STS and LTS of the same packet show a highly similar contour. Furthermore, the amplitude difference between STS and LTS on each subcarrier is close to the theoretical value (0.7332). This demonstrates that the STS and LTS in a packet are within the channel coherence time. Their channel responses can be considered unchanged in the same packet.

In order to visually observe the channel changes, we calculated the spectrum of two LTSs, $\hat{y}_i^{lts1}$ and $\hat{y}_i^{lts2}$, and took their average. Fig. 13 illustrates the spectrum curves of the signals collected from AP1 at different positions, S1_P1, S1_P4, S1_M2, S2_P2, and S2_M1. As can be observed from the figures, the curves of the five positions vary greatly in amplitude and shape. Even in some static scenarios, such as S1_P4, the amplitude and shape of the spectrum curve have changed a lot, which may be caused by people walking in the office. In other static positions, the spectral curves are relatively concentrated, but the curves at different positions still vary greatly. In addition, the spectrum curves variations in dynamic scenarios (S1_M2 and S2_M1) were more significant than those in static scenarios. This demonstrates that the channel characteristics of the Wi-Fi signal are affected by different locations and environments.

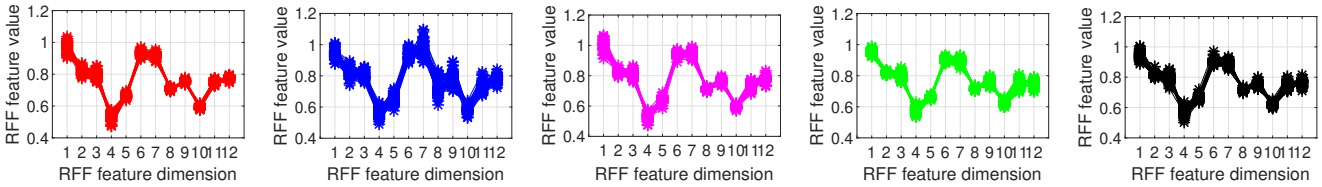
2) RFF Features: Our goal is to eliminate the channel effect in the signal without compromising the RFF information. In other words, for the same device, the RFF features collected at different positions (or different channel environments) should remain the same.

Fig. 14 presents the extracted RFF feature sets of AP1 in S1_P1, S1_P4, S1_M2, S2_P2, and S2_M1. In order to quantify the similarity among the extracted RFF features, we calculated the variance of their RFF features in each dimension and the results are given in Table I. It can be found that the RFF features were stable in static scenarios S1_P1 and S2_P2, whose variances in each dimension only ranges from 0.07 $\times 10^{-3}$ to 0.88 $\times 10^{-3}$. In contrast, the variances of dynamic scenarios S1_M2 and S2_M1 have increased a lot in all dimensions, with the biggest variance, 6.72×10^{-3}, in dimension 1 (S1_M2). This is mainly because the channel



(a) S1_P1 (b) S1_P4 (c) S1_M2 (d) S2_P2 (e) S2_M1

Fig. 13. Y_1^{lts}, the spectrum (linear scale, all 52 subcarriers) of AP1 in positions S1_P1, S1_P4, S1_M2, S2_P2, and S2_M1.

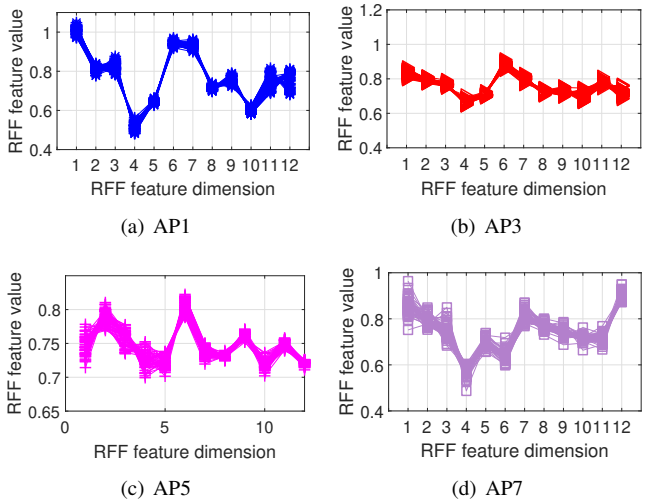


(a) S1_P1 (b) S1_P4 (c) S1_M2 (d) S2_P2 (e) S2_M1

Fig. 14. RFF_1, the RFF feature set of AP1 in positions S1_P1, S1_P4, S1_M2, S2_P2, and S2_M1.

TABLE I
VARIANCE OF RFF FEATURES IN DIFFERENT DIMENSIONS (AP1, ALL VALUES $\times 10^{-3}$).

Dimension	S1_P1	S1_P4	S1_M2	S2_P2	S2_M1
1	0.74	4.31	**6.72**	0.44	1.93
2	0.37	2.54	3.33	0.13	0.69
3	**0.88**	1.56	2.25	0.41	1.41
4	0.57	1.93	2.30	0.35	1.11
5	0.16	1.11	1.68	0.12	0.35
6	0.18	1.81	1.46	0.30	0.32
7	0.29	3.52	3.21	0.49	0.49
8	**0.07**	2.69	0.94	0.11	0.23
9	0.13	2.14	1.56	0.33	0.42
10	0.09	0.76	0.79	0.15	0.34
11	0.20	1.47	1.15	0.84	1.04
12	0.15	0.80	1.60	0.46	1.32



(a) AP1 (b) AP3 (c) AP5 (d) AP7

Fig. 15. The RFF feature set of four different APs at position S1_P2.

changes drastically in the dynamic scenario and has a greater impact on the extracted RFF. Similarly, due to the influence of human walking in the experiment, the channel at the position S1_P4 also changed drastically, which results in the dispersion of its RFF features.

However, even the dispersion of RFF feature values in some dimensions is relatively obvious, the absolute amplitude differences are small, as the maximum amplitude difference is about 0.2 in dimension 1 of S1_M2. In addition, although the absolute values of the RFF features are different, their trends and shapes are similar. Compared with the huge channel characteristics difference in Fig. 13, it demonstrates that the proposed DoLoS algorithm can effectively eliminate the channel influence.

In Fig. 15, we displayed the RFF features extracted from four Wi-Fi devices (AP1, AP3, AP5, and AP7) in the position S1_P2. The channel characteristics at the same location should be similar. Therefore, the differences in Fig. 15 are caused by hardware imperfections, which represent RFF features. In addition, the degree of dispersion of values in various dimensions is a kind of RFF feature because the severity of the RFF jitter of different devices is not the same.

B. Results of RFF Identification in Single-Environment

CNN was used for RFF-based device classification. We sequentially selected the data of one position as training data (80% as the training set and 20% as the verification set) and the data of other locations were used for test to verify the identification performance.

1) Evaluation of DoLoS Algorithm: We performed RFF identification on the data collected in different positions in Environment 1 to evaluate the DoLoS algorithm. The identification accuracy of the DoLoS algorithm, ξ, is shown in Table II.

TABLE II
RFF IDENTIFICATION PERFORMANCE OF ENVIRONMENT 1 DATA SET. (ξ: ACCURACY OF ORIGINAL DATA WITH DOLOS ALGORITHM; ξ_d: ACCURACY OF DENOISED DATA WITH DOLOS ALGORITHM; $\xi_{d,r}$: ACCURACY OF DENOISED AND REFINED DATA WITH DOLOS ALGORITHM; ξ_{IQ}: ACCURACY BASED ON RAW I/Q DATA IN THE TIME DOMAIN; ξ_{FFT}: ACCURACY BASED ON RAW I/Q DATA AFTER FFT; ξ_{AoQ}: ACCURACY OF THE AOQ ALGORITHM.)

Train	Test	Identification rate (%)					
		ξ	ξ_d	$\xi_{d,r}$	ξ_{IQ}	ξ_{FFT}	ξ_{AoQ}
S1_P1	S1_P2	65.77	77.49	82.98	27.97	7.17	45.30
	S1_P3	76.09	84.04	89.44	28.37	54.45	55.34
	S1_P4	68.39	75.63	80.29	14.29	24.10	37.73
	S1_P5	72.97	80.62	82.78	14.43	14.37	43.12
	S1_M1	**72.33**	**86.16**	90.87	28.04	28.67	56.22
	S1_M2	56.24	66.45	**70.65**	15.41	19.16	35.24
S1_P2	S1_P1	83.24	94.08	94.31	42.00	32.63	63.93
	S1_P3	71.14	79.54	83.57	17.98	31.66	47.21
	S1_P4	65.07	78.26	80.43	14.29	14.29	31.14
	S1_P5	66.12	79.05	78.01	14.43	14.43	35.01
	S1_M1	78.45	88.04	**90.00**	28.26	29.36	60.15
	S1_M2	64.87	71.41	71.90	14.58	14.58	33.67
S1_P3	S1_P1	88.44	91.96	95.87	**42.71**	42.31	64.93
	S1_P2	83.16	90.40	94.43	18.90	17.36	55.71
	S1_P4	71.89	80.41	**80.52**	17.90	17.93	38.17
	S1_P5	74.24	81.46	81.66	14.53	19.39	40.22
	S1_M1	81.39	88.29	92.64	34.47	27.98	58.28
	S1_M2	63.39	69.00	71.01	18.84	19.54	34.34
S1_P4	S1_P1	81.13	85.43	91.24	13.93	30.13	37.80
	S1_P2	74.81	76.24	77.98	28.73	33.81	30.20
	S1_P3	89.31	92.11	92.59	20.97	29.95	43.16
	S1_P5	71.31	82.80	86.12	33.15	40.38	35.56
	S1_M1	77.94	83.78	90.42	26.03	28.77	38.54
	S1_M2	62.96	70.09	74.57	23.07	21.42	31.35
S1_P5	S1_P1	**90.83**	94.70	95.98	27.66	28.44	45.59
	S1_P2	65.17	70.56	74.52	27.71	28.14	38.49
	S1_P3	77.50	85.71	88.55	**12.67**	8.75	41.58
	S1_P4	58.46	69.97	81.10	20.14	28.73	30.27
	S1_M1	72.15	78.94	88.81	22.94	23.12	39.70
	S1_M2	60.12	68.82	74.71	21.22	24.73	32.84
S1_M1	S1_P1	95.29	98.81	**99.02**	70.47	76.77	73.51
	S1_P2	89.94	98.57	98.43	76.06	77.70	72.10
	S1_P3	92.19	98.40	98.64	74.53	80.98	65.27
	S1_P4	85.10	86.67	88.43	39.83	51.94	41.86
	S1_P5	82.19	90.85	91.80	16.71	62.87	40.65
	S1_M2	72.08	79.97	80.44	25.82	52.32	37.34
S1_M2	S1_P1	**96.44**	98.61	98.80	68.86	78.16	54.77
	S1_P2	93.57	98.76	98.65	78.37	83.53	57.30
	S1_P3	89.15	93.69	95.42	71.02	73.63	51.46
	S1_P4	77.89	86.33	89.39	65.76	72.43	39.60
	S1_P5	86.32	93.00	93.30	89.88	90.16	45.25
	S1_M1	90.75	97.40	97.96	76.12	80.79	55.57

In the static scenario (Train: S1_P1-P5), the average performance of ξ is 72.83% and the highest accuracy is 90.83%. Fig. 13 has illustrated that the channel characteristics of the Wi-Fi signal collected in different positions/environments are very different. When the training data and test data are collected in different locations, the results of our method, ξ, are still acceptable. This indicates that the DoLoS operation can mitigate the channel response of the received signal.

In the dynamic scenario (Train: S1_M1-M2), the average identification rate of ξ is 87.58%, and the highest accuracy is 96.44%. It is relatively higher compared with the static scenario. The main reason is that the training data collected in the dynamic scenarios contained channel effects at different fixed positions, which means it also included channels of most of the test signals. Therefore, the influence of the channel on CNN learning RFF becomes smaller.

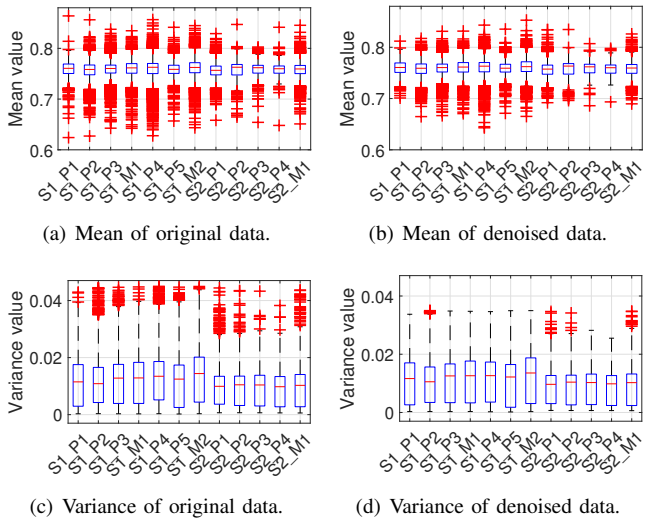
2) Evaluation of Denoising and Data Refining: Fig. 16 shows the distribution of the mean and variance of the original data and denoised data in different positions. Compared with the original data, the average distribution of the denoising data is more concentrated near the theoretical value, and the outliers are significantly reduced. This phenomenon explains the improvement in signal quality. Similarly, the variance trend of the denoised data is closer to 0 and most outliers have entered between the upper and lower limits.

For the data refining, based on the mean distribution in Fig. 16(b) and the theoretical mean (0.7332), we set the mean thresholds as [0.72, 0.77]. It can be seen that most data is concentrated within the mean threshold. Only about 8000 signal packets are filtered from the all signal packets (about 300,000). Furthermore, we set the variance thresholds as [0, 0.0017] according to Fig. 16(d), and about 10,000 packets are outside the threshold range. In addition, some packets outside the threshold have reached the quality requirements of RFF identification after denoising. Finally, about 6% of signal packets have been removed after denoising and data refining.

At the same time, it can be found that even if the received signal power is different for the data collected at different locations, the mean and variance distributions of the obtained RFF features are similar. In other words, even if the test data is collected under completely different conditions, the threshold in the data refining can still work.

Furthermore, we tested the effects of denoising and data refining on RFF identification performance, denoted as ξ_d and $\xi_{d.r}$, respectively, in Table II. Compared with ξ, the denoising algorithm brought an average of 7.30% improvement on the accuracy. The highest performance improvement was 13.84% (86.16% of ξ_d and 72.33% of ξ) when the data from S1_P1 was training and the data from S1_M1 was testing. The improvement demonstrated that the denoising algorithm is a simple but effective method for noise elimination and RFF stabilization. In addition, we refined the data reasonably to obtain the final recognition performance of $\xi_{d,r}$. The overall identification rate has increased by 2.75% on average. It is clear that the data refinement is helpful to improve the precision of RFF identification by removing signals with bad qualities.

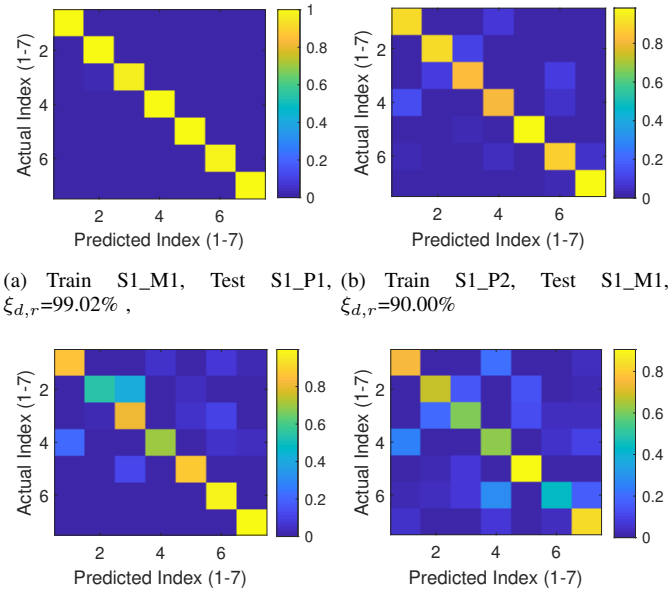
Fig. 17 shows the confusion matrix of the best, worst and two intermediate cases of $\xi_{d,r}$. The distribution of



(a) Mean of original data. (b) Mean of denoised data.

(c) Variance of original data. (d) Variance of denoised data.

Fig. 16. Mean and variance distribution of the RFF feature set.



(a) Train S1_M1, Test S1_P1, $\xi_{d,r}$=99.02% , (b) Train S1_P2, Test S1_M1, $\xi_{d,r}$=90.00%

(c) Train S1_P3, Test S1_P4, $\xi_{d,r}$=80.52% (d) Train S1_P1, Test S1_M2, $\xi_{d,r}$=70.65%

Fig. 17. Confusion matrixes in different cases for the Wi-Fi devices identification problem.

identification errors of other devices is relatively uniform, which may be caused by the residual noise and channel information.

C. Results of RFF Identification in Cross-Environment

In order to further improve the data diversity, we added the RFF cross-recognition evaluation based on the data collected in different environments. In this paper, the data sets under the two environments were collected four months apart and their collection environments were completely different. Table III shows the results of RFF identification using Environment 1 data for training and Environment 2 data for testing.

TABLE III
RFF IDENTIFICATION PERFORMANCE OF TWO ENVIRONMENT DATA SETS.

Train	Test	Identification rate (%)			
		$\xi_{d,r}$	ξ_{IQ}	ξ_{FFT}	ξ_{AoQ}
S1_P1	S2_P1	83.17	26.00	19.00	49.64
	S2_P2	83.88	21.03	20.41	40.10
	S2_P3	87.39	16.20	18.43	54.09
	S2_P4	97.05	28.50	26.56	56.27
	S2_M1	87.88	22.06	31.01	50.96
S1_P2	S2_P1	70.31	14.29	14.01	45.84
	S2_P2	80.07	14.29	14.29	51.27
	S2_P3	86.47	14.44	20.59	45.33
	S2_P4	88.98	28.63	38.40	50.31
	S2_M1	79.05	20.09	22.10	49.93
S1_P3	S2_P1	92.20	44.53	25.83	56.29
	S2_P2	84.76	34.89	29.50	48.40
	S2_P3	85.92	28.74	13.96	57.81
	S2_P4	91.86	24.00	45.37	55.56
	S2_M1	81.86	31.69	27.09	52.59
S1_P4	S2_P1	91.96	32.56	40.46	41.23
	S2_P2	83.48	46.66	37.03	29.46
	S2_P3	83.48	35.60	37.19	41.99
	S2_P4	91.57	30.83	27.69	34.27
	S2_M1	89.02	33.26	33.06	35.06
S1_P5	S2_P1	84.21	35.67	33.84	43.23
	S2_P2	78.30	28.84	19.20	28.59
	S2_P3	89.45	44.03	37.29	40.36
	S2_P4	73.18	28.31	41.27	38.60
	S2_M1	78.38	27.21	26.60	35.84
S1_M1	S2_P1	84.03	55.84	35.34	58.47
	S2_P2	69.63	14.13	1.91	53.13
	S2_P3	76.14	30.04	36.04	59.89
	S2_P4	71.29	18.10	14.29	60.61
	S2_M1	72.95	19.16	18.36	57.63
S1_M2	S2_P1	84.88	27.79	27.96	48.34
	S2_P2	79.89	32.00	34.69	42.94
	S2_P3	84.31	27.44	28.89	48.57
	S2_P4	88.51	28.36	28.49	51.74
	S2_M1	83.55	28.63	30.01	46.87

It can be seen that in the static scenario, the average identification rate of our scheme $\xi_{d,r}$ in Table III is around 85%, which is consistent with the results in Table II. It turns out that the good performance of our scheme $\xi_{d,r}$ is indeed because of the mitigation of channel characteristics on RFF identification, rather than assuming that channel characteristics may be similar at different locations in the same room.

In the dynamic scenario, the average identification rate of $\xi_{d,r}$ is also a acceptable result (around 80%). However, it is a little worse compared with the single-environment. This is because all the data used in the single-environment are collected in a similar environment, which means that the dynamically collected training data contains most of the channel characteristics in the test data. Therefore, CNN can

perform RFF recognition more easily.

D. Comparison with Existing Solution

The work in [17] has carried out extensive WiFi-based experimental evaluation by using raw IQ samples in the time domain and the data after FFT operation, i.e., the frequency domain data, respectively, as the input for the CNN model. Both methods do not specifically adopt channel elimination. These two methods are compared in this paper as baseline, and their identification accuracy are denoted as ξ_{IQ} and ξ_{FFT}, given in Table II (single-environment) and Table III (cross-environment). Specifically, the IQ-based solution took the time domain I/Q data, $\hat{y}_i^{sts1}$ and $\hat{y}_i^{lts1}$, which is a 128*2 vector. The FFT-based solution used FFT coefficients of the raw-data $\hat{y}_i^{sts1}$ and $\hat{y}_i^{lts1}$, which is also a 128*2 vector.

In addition, three categories methods of channel robust RFF identification are discussed in Section I. For the first category, CFO-based RFF feature is investigated in this paper. The results in Fig. 5 show that CFO is unstable and overlap with each other, which implies poor identification performance. The second category requires manipulation of the emitter, which is not suitable for the scenario in this paper. For the third category, we compared our solution with the AoQ algorithm in [31], whose identification accuracy is shown in Table II (single-environment) and Table III (cross-environment) denoted as ξ_{AoQ}. Specifically, the AoQ algorithm extracts two LTSs in the same frame signal and calculates the amplitude quotient of the two LTS spectrums (named AoQ) to eliminate the channel response. The RFF feature is constructed by collecting AoQ from multiple locations. The signals from multiple locations used to generate the RFF are considered to be sent by the same device. This process lacks device authentication, which is a security vulnerability. Our scheme performs RFF identification utilizing a single frame signal, which does not have the aforementioned security risks. For a fair performance comparison, we tested the identification performance of the AoQ algorithm with a single frame signal.

1) Single-Environment: As shown in Table II, the average performance of ξ_{IQ} in the static scenario is poor, whose highest accuracy is only 42.71% and the lowest value is 12.67%. The main reason is that the channel influence was dominant and the tiny RFF features were completely swamped when the channels of the training and test sets are different. This is echoed in [17], the accuracy obtained by IQ data is only 1.7% when training and test sets were collected in different environments. Similarly, the identification rate ξ_{FFT} was also quite bad, which shows that the FFT operations cannot eliminate the channel response of the received signal. In contrast, the identification rate of our scheme ξ in the static scenario has been greatly improved. Especially, the maximum value of ξ (90.83%) is more than 3 times the value of ξ_{FFT} (28.44%). The channel effect is mitigated by the DoLoS algorithm, thus CNN can effectively learn the tiny RFF features as the device identity.

Regarding the dynamic scenario, the average identification rate of ξ_{IQ} are 50.57% of S1_M1 and 75.00% of S1_M2, and the average identification rate of ξ_{FFT} are 67.10% of S1_M1 and 79.78% of S1_M2, which have significant improvement compared with their counterparts in the static scenarios. The training data in the dynamic scenarios included channels of most of the signals collected at the fixed positions. Then, in the identification stage, the fixed position data can easily find similar samples in the training set to identify the corresponding device. However, it is difficult to obtain a data set containing all channel effects in practical applications. Furthermore, the environment and channel characteristics are likely to change with time or site. Thus, device identification based on certain fixed channel characteristics does not have long-term stability. However, ξ_{IQ} and ξ_{FFT} are still much lower than our approach, i.e., average $\xi_{d,r}$: 92.79% of S1_M1 and 95.59% of S1_M2), .

Compared with ξ_{IQ} and ξ_{FFT}, the performance of ξ_{AoQ} has small improvement in the static scenario. However, its performance is much lower than our scheme in both static and dynamic scenario. The main reason may be that the RFF difference between two identical symbols is smaller than that between two different symbols.

2) Cross-Environment: As shown in Table III, the identification rates of ξ_{IQ} and ξ_{FFT} in the static scenario are also too low to meet the requirements of device identification. In the dynamic scenario, the ξ_{IQ} and ξ_{FFT} did not show a significant improvement. The main reason is that the training and test data for the dynamic scenario were collected in completely different environments, which resulted in varied channel characteristics. Compared to ξ_{IQ} and ξ_{FFT}, the average performance improvement of $\xi_{d,r}$ exceeds 55%. This phenomenon demonstrates that our RFF identification scheme can effectively remove the most influence of channel characteristics. In addition, the identification performance obtained by training on data from different locations is very similar. In other words, even if the data collection time and environment are very different, our scheme still shows great channel robustness. Compared with ξ_{AoQ}, our algorithm also show satisfied performance improvement.

VII. Conclusion

This paper proposed a channel robust RFF identification scheme to address the serious interference of the channel on RFF identification in practical applications. Our proposed DoLoS algorithm leverages the different spectra of signal symbols as the RFF features. We implemented the algorithm with the IEEE 802.11 OFDM system as a case study. We found that when the training set and the test set are collected in different channel environments, the RFF-based device identification cannot work well without an effective method to process variable channels. Then, after using the DoLoS algorithm, the channel interference on the RFF features is effectively eliminated. In the single-environment evaluation, DoLoS algorithm can bring a significant improvement compared to the raw IQ-based RFF identification, up to 68.75% in the best case. Furthermore, the denoising and data refining methods proposed for the IEEE 802.11 devices can also bring about 10% performance improvement on average in the experiments. In cross-environment evaluation, our scheme

also showed excellent RFF identification performance with the highest accuracy of 97.05%.

REFERENCES

[1] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, "Overview of 5G security challenges and solutions," *IEEE Commun. Standards Mag.*, vol. 2, pp. 36–43, Apr. 2018.

[2] H. M. J. Almohri, L. T. Watson, and D. Evans, "An attack-resilient architecture for the Internet of Things," *IEEE Trans.Inf. Forensics Security*, pp. 3940–3954, May 2020.

[3] W. Wu, S. Hu, D. Lin, and Z. Liu, "DSLN: Securing Internet of Things through RF fingerprint recognition in Low-SNR settings," *IEEE Internet Things J.*, vol. 9, pp. 3838–3849, Jul. 2022.

[4] K. Xue, W. Meng, H. Zhou, D. S. L. Wei, and M. Guizani, "A lightweight and secure group key based handover authentication protocol for the software-defined space information network," *IEEE Trans. Wireless Commun.*, pp. 3673–3684, Feb. 2020.

[5] Y. Li, H. Wang, and K. Sun, "Personal information in passwords and its security implications," *IEEE Trans.Inf. Forensics Security*, vol. 12, pp. 2320–2333, May 2017.

[6] S. Holtmanns and I. Oliver, "SMS and one-time-password interception in LTE networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Paris, France, Jul. 2017, pp. 1–6.

[7] Y. Lin, Y. Tu, Z. Dou, L. Chen, and S. Mao, "Contour stella image and deep learning for signal recognition in the physical layer," *IEEE Trans. Cogn. Commun. Netw.*, vol. 7, pp. 34–46, Sep. 2021.

[8] Q. Tian, Y. Lin, X. Guo, J. Wen, Y. Fang, J. Rodriguez, and S. Mumtaz, "New security mechanisms of high-reliability IoT communication based on radio frequency fingerprint," *IEEE Internet Things J.*, vol. 6, pp. 7980–7987, Apr. 2019.

[9] J. Zhang, R. Woods, M. Sandell, M. Valkama, A. Marshall, and J. Cavallaro, "Radio frequency fingerprint identification for narrowband systems, modelling and classification," *IEEE Trans.Inf. Forensics Security*, pp. 3974–3987, Jun. 2021.

[10] B. Chatterjee, D. Das, S. Maity, and S. Sen, "RF-PUF: Enhancing IoT security through authentication of wireless nodes using in-situ machine learning," *IEEE Internet Things J.*, vol. 6, pp. 388–398, Feb. 2019.

[11] X. Zhou, A. Hu, G. Li, L. Peng, Y. Xing, and J. Yu, "A robust radio-frequency fingerprint extraction scheme for practical device recognition," *IEEE Internet Things J.*, vol. 8, pp. 11 276–11 289, Jan. 2021.

[12] B. Danev, D. Zanetti, and S. Capkun, "On physical-layer identification of wireless devices," *ACM Comput. Surv. (CSUR)*, vol. 45, no. 1, pp. 1–29, 2012.

[13] J. Yu, A. Hu, G. Li, and L. Peng, "A Robust RF Fingerprinting Approach Using Multisampling Convolutional Neural Network," *IEEE Internet Things J.*, vol. 6, no. 4, pp. 6786–6799, 2019.

[14] V. Brik, S. Banerjee, M. Gruteser, and S. Oh, "Wireless device identification with radiometric signatures," in *Proc. 14th ACM Int. Conf. Mobile Comput. Netw.*, New York, NY, USA, Sep. 2008, pp. 116–127.

[15] M. Fadul, D. Reising, T. D. Loveless, and A. Ofoli, "Nelder-mead simplex channel estimation for the RF-DNA fingerprinting of OFDM transmitters under rayleigh fading conditions," *IEEE Trans.Inf. Forensics Security*, pp. 2381–2396, Jan. 2021.

[16] S. Hanna, S. Karunaratne, and D. Cabric, "Open set wireless transmitter authorization: Deep learning approaches and dataset considerations," *IEEE Trans. on Cogn. Commun. Netw.*, pp. 59–72, Dec. 2021.

[17] A. Al-Shawabka, F. Restuccia, S. D'Oro, T. Jian, B. C. Rendon, N. Soltani, J. Dy, K. Chowdhury, S. Ioannidis, and T. Melodia, "Exposing the fingerprint: Dissecting the impact of the wireless channel on radio fingerprinting," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, Toronto, Canada, Jul. 2020, pp. 1–10.

[18] K. Sankhe, M. Belgiovine, F. Zhou, L. Angioloni, F. Restuccia, S. D'Oro, T. Melodia, S. Ioannidis, and K. Chowdhury, "No radio left behind: Radio fingerprinting through deep learning of physical-layer hardware impairments," *IEEE Trans. Cogn. Commun. Netw.*, pp. 165–178, Oct. 2020.

[19] L. Peng, J. Zhang, M. Liu, and A. Hu, "Deep learning based RF fingerprint identification using differential constellation trace figure," *IEEE Trans. Veh. Technol.*, vol. 69, pp. 1091–1095, Otc. 2020.

[20] Y. Xing, A. Hu, J. Yu, G. Li, L. Peng, and F. Zhou, "A robust radio frequency fingerprint identification scheme for LFM pulse radars," in *Proc. 15th Int. Conf. Wireless Mobile Comput. Netw. Commun. (WiMob)*, Barcelona, Spain, Oct. 2019, pp. 1–6.

[21] G. Gok, Y. K. Alp, and O. Arikan, "A new method for specific emitter identification with results on real radar measurements," *IEEE Trans.Inf. Forensics Security*, vol. 15, pp. 3335–3346, Apr. 2020.

[22] Y. Xing, A. Hu, J. Zhang, J. Yu, G. Li, and T. Wang, "Design of a robust radio frequency fingerprint identification scheme for multi-mode LFM radar," *IEEE Internet Things J.*, vol. 7, no. 10, pp. 10 581–10 593, Jun. 2020.

[23] G. Shen, J. Zhang, A. Marshall, and J. R. Cavallaro, "Towards scalable and channel-robust radio frequency fingerprint identification for lora," *IEEE Trans.Inf. Forensics Security*, pp. 774–787, Feb. 2022.

[24] T. D. Vo-Huu, T. D. Vo-Huu, and G. Noubir, "Fingerprinting Wi-Fi devices using software defined radios," in *Proc. 9th ACM Conf. Secur. Privacy Wireless Mobile Netw.*, New York, USA, Jul. 2016, pp. 3–14.

[25] J. Hua, H. Sun, Z. Shen, Z. Qian, and S. Zhong, "Accurate and efficient wireless device fingerprinting using channel state information," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, Apr., Honolulu, HI, USA 2018, pp. 11 700–1708.

[26] W. Hou, X. Wang, J.-Y. Chouinard, and A. Refaey, "Physical layer authentication for mobile systems with time-varying carrier frequency offsets," *IEEE Trans. Commun.*, vol. 62, pp. 1658–1667, Apr. 2014.

[27] P. Liu, P. Yang, W. Song, Y. Yan, and X. Li, "Real-time identification of rogue WiFi connections using environment-independent physical features," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, Paris, France, Jun. 2019, pp. 190–198.

[28] F. Restuccia, S. D'Oro, A. Al-Shawabka, M. Belgiovine, L. Angioloni, S. Ioannidis, K. Chowdhury, and T. Melodia, "DeepRadioID: Real-time channel-resilient optimization of deep learning-based radio fingerprinting algorithms," in *Proc. Twentieth ACM Int. Symposium Mobile Ad Hoc Netw. Comput.*, New York, NY, USA, 2019, pp. 51–60.

[29] I. O. Kennedy and A. M. Kuzminskiy, "RF fingerprint detection in a wireless multipath channel," in *Proc. 7th Int. Symposium Wireless Commun. Systems*, York, UK, nov. 2010, pp. 820–823.

[30] M. Liu and J. F. Doherty, "Nonlinearity estimation for specific emitter identification in multipath channels," *IEEE Trans.Inf. Forensics Security.*, vol. 6, pp. 1076–1085, Apr. 2011.

[31] G. Li, J. Yu, Y. Xing, and A. Hu, "Location-invariant physical layer identification approach for WiFi devices," *IEEE Access*, vol. 7, pp. 106 974–106 986, Aug. 2019.

[32] T. Zheng, Z. Sun, and K. Ren, "FID: Function modeling-based data-independent and channel-robust physical-layer identification," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, Paris, France, Jun. 2019, pp. 199–207.

[33] B. Bloessl, M. Segata, C. Sommer, and F. Dressler, "Performance assessment of IEEE 802.11p with an open source SDR-based prototype," *IEEE Trans. Mobile Comput.*, vol. 17, pp. 1162–1175, Sep. 2018.

[34] H. Jung, T. â. Kwon, K. Cho, and Y. Choi, "REACT: Rate adaptation using coherence time in 802.11 WLANs," *Comput. Commun.*, vol. 34, pp. 1316–1327, Feb. 2011.

[35] Z. Li, F. Bai, J. A. Fernandez, and B. V. K. Vijaya Kumar, "Tentpoles scheme: A Data-Aided channel estimation mechanism for achieving reliable Vehicle-to-Vehicle communications," *IEEE Trans. Wireless Commun.*, vol. 14, no. Jan., pp. 2487–2499, 2015.

[36] Y. Xing, A. Hu, J. Zhang, L. Peng, and G. Li, "On radio frequency fingerprint identification for DSSS systems in low SNR scenarios," *IEEE Commun. Lett.*, vol. 22, no. 11, pp. 2326–2329, Nov. 2018.

[37] D. C. Ciresan, U. Meier, L. M. Gambardella, and J. Schmidhuber, "Convolutional neural network committees for handwritten character classification," in *Proc. Int. Conf. Document Analysis and Recognition*, Beijing, China, Nov. 2011, pp. 1135–1139.