Channel-Agnostic Radio Frequency Fingerprint Identification Using Spectral Quotient Constellation Errors

Jiashuo He, *Graduate Student Member, IEEE*, Sai Huang, *Senior Member, IEEE*, Zheng Yang, Kan Yu, *Member, IEEE*, Hao Huan, and Zhiyong Feng, *Senior Member, IEEE*

***Abstract*— Radio frequency fingerprint identification (RFFI) is a physical layer security methodology to recognize individual devices by leveraging hardware imperfections inevitably induced in the manufacturing process. However, the performance degradation caused by the time-varying channel impacts and interferences has severely restricted the development of RFFI. To this end, we present a channel-agnostic RFFI system, which consists of three modules, i.e., signal preprocessing module, feature extraction module, and classification module. In the signal preprocessing module, we first propose a novel approach, referred to as limiter-based spectral circular shift bidirectional division (LB-SCSBD), to generate two parallel spectral quotient (SQ) sequences. Then, we define the spectral quotient constellation (SQC) symbols according to different modulation formats, and thereby transform the SQ sequences into four magnitude-based sequences in terms of two channel-robust signal representations, i.e., the SQ magnitude (SQM) and SQC error vector magnitude (SQC-EVM). In the feature extraction module, we present a moment-based statistical feature extractor (MB-SFE) to extract the device-specific information from the above four sequences. In the classification module, the extracted statistics are fed into the multi-class support vector machine (SVM) for training and testing. We take WiFi as a case study and evaluate the performance of the proposed RFFI system by classifying eight simulated device models and six universal software radio peripheral (USRP) transmitter radios. Experimental results show that (i) the proposed method achieves the accuracies of 99.84% and 98.26% with eight devices in QPSK and 16QAM cases, as well as the accuracy of 92.42% with six USRP devices (ii) the proposed method exhibits superior classification performance in comparison to some existing RFFI methods, leading to a significant accuracy improvement of at least 38.33%.**

***Index Terms*— High-order moments, multipath fading channel, radio frequency fingerprint identification, spectral quotient constellation errors, WiFi.**

Manuscript received 9 January 2023; revised 21 March 2023; accepted 3 May 2023. Date of publication 22 May 2023; date of current version 9 January 2024. This work was supported in part by the National Natural Science Foundation of China under Grant 62171045 and in part by the National Key Research and Development Program of China under Grant 2019YFB1804404 and Grant 2020YFB1807602. The associate editor coordinating the review of this article and approving it for publication was W. Ni. *(Corresponding author: Sai Huang.)*

Jiashuo He, Sai Huang, Zheng Yang, Kan Yu, and Zhiyong Feng are with the Key Laboratory of Universal Wireless Communications, Ministry of Education, Beijing University of Posts and Telecommunications (BUPT), Beijing 100876, China (e-mail: jiashuohe@bupt.edu.cn; huangsai@bupt.edu.cn; yz2016@bupt.edu.cn; kanyu1108@126.com; fengzy@bupt.edu.cn).

Hao Huan is with the Beijing Institute of Technology, Beijing 100081, China (e-mail: huanhao@bit.edu.cn).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TWC.2023.3276519.

Digital Object Identifier 10.1109/TWC.2023.3276519

I. Introduction

In RECENT years, the Internet of Things (IoT) has gained great popularity and achieved unprecedented growth in both the number and variety of applications, such as connected healthcare, smart home and industrial control [1], [2]. With the explosive growth of IoT device numbers, safeguarding IoT systems in wireless connectivity will be accompanied by more challenges. Conventional authentication techniques including cryptographic schemes on software addresses and pre-shared keys are effective strategies for physical layer security authentication [3]. However, cryptography-based authentication techniques usually consume massive computing resources, which makes them difficult to deploy in the limited power and computation resources, such as IoT devices, and their effectiveness can be impacted by robustly detecting and revoking compromised keys [4].

Radio frequency fingerprint identification (RFFI) has emerged as an effective physical layer security methodology, which employs the distinctive transmitter imperfections extracted from the received signals to recognize individual devices. Since the hardware imperfections are unintentionally introduced in the manufacturing process, the radio frequency fingerprints (RFF) resulting from them are nearly impossible to mimic. For this reason, RFFI has attracted great interest and has been widely investigated in WiFi [5], ZigBee [6], LoRa [7], and Bluetooth [8].

Generally speaking, RFF can be extracted from both the transient and steady-state portions of a signal. The corresponding transient-based method involves recognizing distinctive RFF presented in the transient turn-on waveforms. The challenging issue is how to properly capture the transient signal portion in a short time [9], [10], [11]. In contrast, the steady-state signals are comparatively simple to capture and detect. Therefore, RFFI based on the steady-state signals has been investigated in many works [12], [13], [14], [15], [16], [17]. Since a vast majority of existing wireless communication systems send the preambles for synchronization, the attention to feature extraction is initially transferred into the preamble of the steady-state signals. In [12] and [13], the mean, variance, skewness, and other statistics extracted from the time-frequency analysis of preambles are utilized as the discriminative features for identification. Subsequently, the RFF research on the payload instead of the preamble has been a hotspot. According to the literature [4], [14], [15],

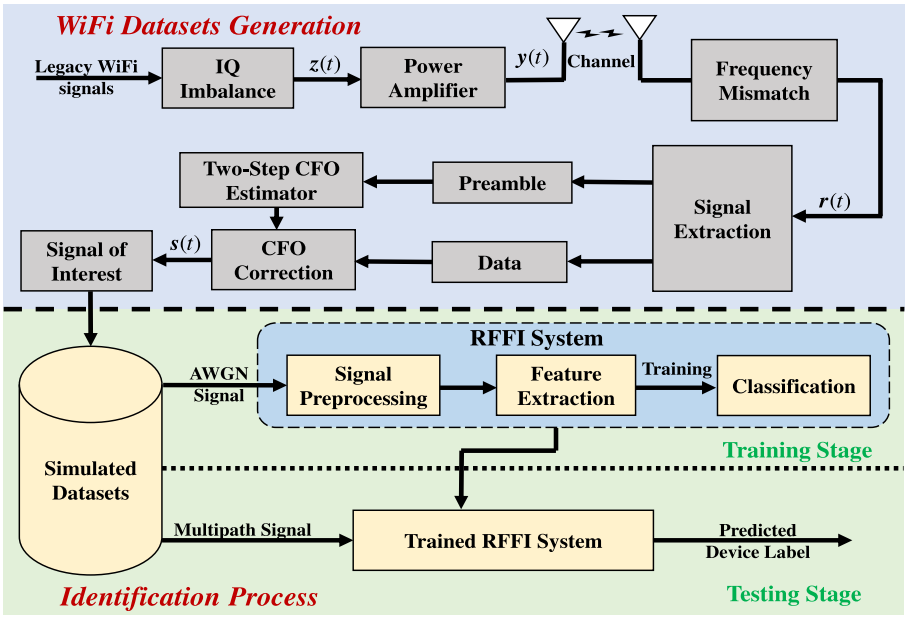


Fig. 1. The flow chart of the WiFi datasets generation and identification.

[16], and [17], the synchronization correlation, mixer offset, constellation error as well as some statistics are employed as distinct RFF and achieve significant classification performance. Moreover, other RFFI methods like the deep neural network (DNN) and conventional neural network (CNN) also have been conducted in many works [18], [19], [20], [21], [22], [23], [24], as this end-to-end approach can directly process the raw signal and make predictions without feature engineering. However, these approaches require intensive computational complexity and have poor generalizability. Considering the limited computation resources on the low-cost IoT devices, our goal is to extract the handcraft features from the payload as the distinct RFF for device recognization.

A major challenge for RFFI is that the time-varying channel effects can result in unreliable classification performance. At present, most current RFFI works only consider the noise effects without the channel or simply assume the static channels in the controlled environment [15], [16], [17], [18], [19], [20], [21], [22], [23], [24], and only a few works have considered the time-varying impacts of the multipath fading channel [26], [27], [28], [29], [30]. For instance, Tugnait added the Gaussian artificial noise to the received signal in order to compensate for the channel changes [26]. Besides, Zhou et al. also proposed an artificial noise adding algorithm to improve the classification accuracy by regularization and channel adaptation [27]. However, the level of artificial noise required to add is still uncertain. In [28], Sankhe et al. proposed the ORACLE framework to mitigate the channel effects through the undercomplete demodulation approach. However, this method requires channel estimation and equalization, which can induce extra errors and additional computational complexity. Shen et al. in [29] first employed the short-time Fourier transform (STFT) to construct the channel-independent spectrogram, and then fed it into the CNN for devices recognization. Their RFFI framework successfully achieved excellent classification performance and effective channel mitigation. However, this method only focuses on the preambles and neglects the phase information of the spectrogram. In our prior work [30], we attempted to use the signal preprocessing method named spectral circular shift division (SCSD) to generate the channel-robust spectral quotient (SQ) signals. However, the SQ signals generated by the SCSD method fluctuate heavily, and this decreases the stability of the extracted RFF as well as degrades the classification performance.

In this paper, a channel-agnostic RFFI system is designed, which consists of three modules, i.e., signal preprocessing module, feature extraction module, and classification module. To combat the time-varying channel effects, our approach first converts the received signals to other channel-robust representations in the signal preprocessing module and then uses the moment-based statistical feature extractor (MB-SFE) to extract the device-specific RFF in the feature extraction module. After that, the extracted feature samples are fed into the multi-class support vector machine (SVM) for training and testing in the classification module. During the training stage, we train the SVM using the feature samples without any channel effects. During the testing stage, we evaluate the classification performance of the trained SVM using the feature samples extracted under different channel conditions. In our experimental evaluation, we take WiFi as a case study and employ eight simulated device models and six universal software radio peripheral (USRP) transmitters (in an open dataset) for classification. The main contributions of this work are summarized as follows:

- We propose a novel approach, referred to as limiter-based spectral circular shift bidirectional division (LB-SCSBD), to generate two parallel SQ sequences in the submodule of the signal preprocessing module. Moreover, we show that the proposed RFFI system using

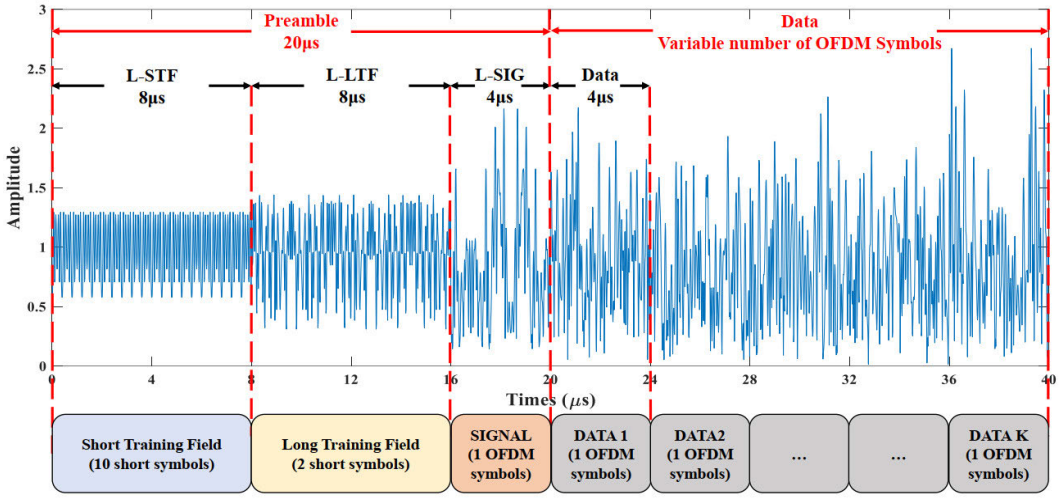


Fig. 2. The legacy WiFi frame structure.

the LB-SCSBD method can enhance the classification accuracies of 14% - 47% in comparison to that using the SCSD method at SNR = 27 dB.

- We define the spectral quotient constellation (SQC) symbols in terms of the quadrature amplitude modulation (QAM) constellation symbols and then construct the SQC error vectors by performing the minimum Euclidean distance between the SQ sequences and the SQC symbols. It is worth noting that the SQC symbols don't contain any hardware imperfections, which suggests that the SQC error vectors have abundant RFF.
- We investigate two novel channel-robust signal representations, namely SQ magnitude (SQM) and SQC error vector magnitude (SQC-EVM), to generate four magnitude-based sequences in another submodule of the signal preprocessing module. Later, we present an effective RFF extractor named MB-SFE in the feature extraction module, which can extract four moments (i.e., first, second, third, and fourth moments) from each observed sequence as the distinct RFF.
- We carry out extensive experiments to evaluate the classification performance of the proposed RFFI system. In comparison to the RFFI methods given in [17] and [30], our method exhibits the best classification performance, with at least 38.33% accuracy improvements when the signal-to-noise ratio (SNR) level is equal to 30 dB. Moreover, the proposed RFFI system can achieve the accuracies of 99.84% and 98.26% with eight devices in QPSK and 16QAM cases at SNR = 32 dB, as well as the accuracy of 92.42% with six USRP devices in the open dataset.

The rest of the paper is organized as follows. Section II details the generation of the WiFi datasets used in our experiments. The identification process of the proposed channel-agnostic RFFI system is briefly given in Section III. In Section IV, we first introduce the experimental setup and then analyze the experiment results of the proposed RFFI system. Finally, we conclude this paper in Section V.

II. Dataset Generation and Signal Model

As shown in Fig. 1, the overall work can be divided into two steps: the WiFi datasets generation and the identification process. In this section, we first introduce the generation of the simulated datasets, where the standard-compliant IEEE 802.11a WiFi frames are generated as the transmitted signals. Then, we give the impairments modeling of the transmitter with a special focus on the in-phase (I) and quadrature (Q) imbalance, power amplifier (PA) nonlinearity, frequency and phase mismatch, typically seen in actual hardware implementations. Finally, the received signal model is given, where the carrier frequency offset (CFO) estimation and correction are performed to decrease the impacts of oscillator imperfection. The detailed operations are provided in the following.

A. WiFi Frame Structure

Fig. 2 shows the IEEE 802.11a WiFi OFDM frame structure [28], which consists of a legacy short training field (L-STF, 8 microseconds, i.e., μs), legacy long training field (L-LTF, 8 μs), legacy signal field (L-SIG, 4 μs), and data field. The data field contains K random OFDM symbols and each OFDM symbol lasts for 4 μs. The L-STF is primarily used for coarse CFO estimation, while the L-LTF is mainly used for fine CFO estimation.

For simplicity, the WiFi signals are represented in the complex form as follows

$$x(t) = x_I(t) + jx_Q(t); 0 \leq t \leq T, \tag{1}$$

where $x_I(t)$ and $x_Q(t)$ denote the WiFi signals on the I and Q branches, respectively; T (in μs) is the duration of each WiFi full frame.

B. IQ Imbanlance

Quadrature mixers are used for upconversion and are often impaired by IQ imbalances, which is one of the main aspects of the transmitter's impairments. Considering the distortion

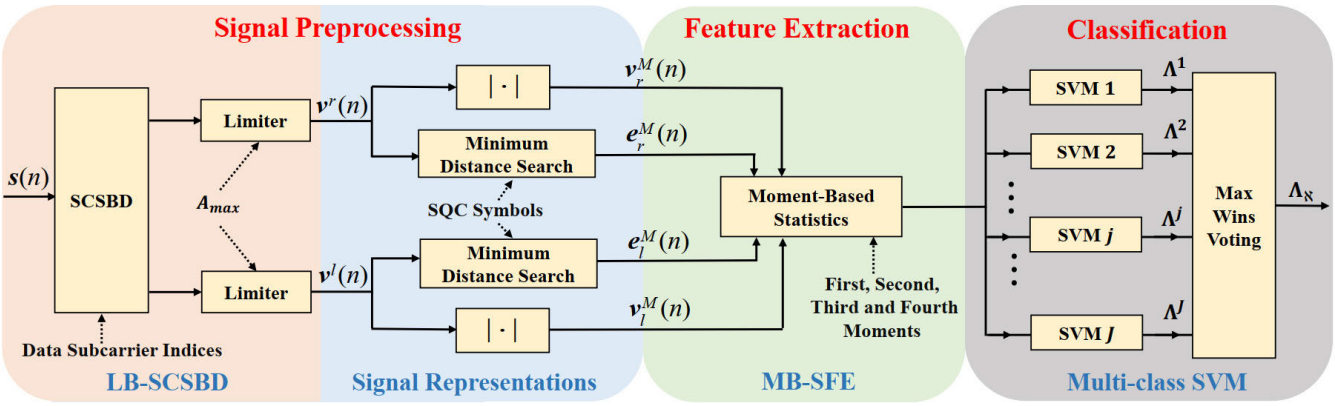


Fig. 3. The detailed architecture of channel-agnostic RFFI system.

caused by the IQ imbalances, the corrupted baseband signal can be modeled as

$$z(t) = g_I^{tx} x_I(t) e^{\frac{j\theta^{tx}}{2}} + j g_Q^{tx} x_Q(t) e^{\frac{-j\theta^{tx}}{2}}, \quad (2)$$

where θ^{tx} (in rad) is the phase mismatch; g_I^{tx} and g_Q^{tx} denote the gain on the I and Q branches, respectively. As referred from [24], the IQ gains in the linear scale can be denoted as

$$g_I^{tx} = 10^{0.5\frac{G^{tx}}{20}}, \quad (3)$$

$$g_Q^{tx} = 10^{-0.5\frac{G^{tx}}{20}}, \quad (4)$$

where G^{tx} (in dB) is the gain imbalance.

C. Power Amplifier Nonlinear Distortion

Generally speaking, a power amplifier in a communication system is used to boost a signal to a power level suitable for transmission. Due to the demand for PA efficiency, nonlinearity is caused in the process of power amplification and plays a key role in the generation of transmitter imperfection. Considering the memoryless nonlinearity caused by PA, the distorted baseband signal can be expressed as

$$y(t) = \mathscr{F}(z(t)), \quad (5)$$

where $y(t)$ is the PA output at t time, and $\mathscr{F}(\cdot)$ is the power amplifier transfer function. Several memoryless PA models including the Saleh model, Rapp model, and polynomial model are employed, and the detailed descriptions are given in Appendix A.

D. Received Signal Model

The transmitted signal attached by the distinct RFF will be captured at the receiver after passing through the wireless channel. Due to the frequency mismatch between the transmitter and receiver, CFO and phase offset (PO) occur in the process of downconversion. Hence, the continuously received baseband signal interrelated with the transmitter RFF and these time-varying distortions can be represented as

$$r(t) = e^{-j(2\pi B\varepsilon t+\Phi)} \sum_{i=1}^{I} h_{\tau_i}(t) y(t-\tau_i) + w(t); \quad 0 \le t < T, \quad (6)$$

where B (in MHz) is the transmission bandwidth and ε is the normalized CFO with respect to B; Φ is the PO within $[-\pi, \pi]$; I is the maximum channel delay taps and τ_i denotes the channel delay of the i^{th} tap; $h_{\tau_i}(t)$ is the channel coefficient of the i^{th} delay tap at t time; $w(t)$ is the additive white Gaussian noise (AWGN) and $w(t) \sim \mathcal{CN}(0, \sigma_n^2)$.

Synchronization is often employed to detect the accurate start of the received packet so that we can extract the signal of interest easily with the prior information of the signal configuration. The well-known Schmidl-Cox algorithm [31] can be implemented when there is a need for synchronization. Since synchronization is unnecessary in the simulated WiFi frames (because the start of the WiFi signal is already known in the simulated cases), we straightly divide the received WiFi frame into two parts: preamble and OFDM data. As referred from the literature [32], we can use the L-STF ($t \in [0, 8)\mu s$) and L-LTF ($t \in [8, 16)\mu s$) signals in the preamble for the coarse and fine CFO estimation according to the conventional two-step CFO estimator. Assuming the overall estimated CFO is Δf, after performing the CFO correction, the corrected baseband signal without oversampling in the data field can be expressed as

$$s(n) = e^{-j(2\pi\varepsilon' n+\Phi')} \sum_{i=1}^{I} h_{\tau_i'}(n) y(n-\tau_i') + \hat{w}(n); \quad 0 \le n \le N-1, \quad (7)$$

where n is the discrete-time index of the sampling signal and $n = (t-20)B$ (i.e., the start of the data field); N is the length of the sampling signal in the WiFi data field; Φ' denotes the residual PO; ε' is the normalized residual CFO and $\varepsilon' = \varepsilon - \Delta f/B$; τ_i' is the discrete-time channel delay of the i^{th} path and $h_{\tau_i'}(n)$ is the corresponding n^{th} channel coefficient; $\hat{w}(n)$ is the AWGN after performing the CFO correction.

After performing the above operations, the simulated WiFi frames will be kept in several datasets according to the channel conditions and modulation formats. Meanwhile, this completes the generation of the simulated WiFi datasets.

III. Channel-Agnostic RFFI System

A. System Overview

As shown in Fig.1, the identification process comprises two essential stages, namely training and inference stages. In the training stage, we only use the noise-affected dataset

to train the proposed RFFI system. In the testing stage, the well-trained RFFI system will predict the device label according to the received samples of the multipath fading channel datasets. Fig. 3 shows the detailed architecture of the proposed channel-agnostic RFFI system, where three modules, i.e., signal preprocessing module, feature extraction module, and classification module are illustrated. In the signal preprocessing module, we first generate two parallel SQ sequences through the LB-SCSBD submodule. Then, we convert the SQ sequences to two channel-robust signal representations, i.e., the SQM and the SQC-EVM, so that we can obtain four magnitude-based sequences in the next submodule. In the feature extraction module, we present the MB-SFE to explore the hardware-introduced information from these sequences, where the first, second, third, and fourth moments are extracted from each sequence and then applied as the RFF features. At last, the multi-class SVM classifiers are trained and tested with the extracted feature samples in the classification module.

B. Limiter-Based Spectral Circular Shift Bidirectional Division

Since the division-based algorithm is sensitive to the denominator value, the SQ signal value generated by the SCSD method is unstable and fluctuates heavily. This characteristic decreases the statistical stability with a small amount of data and then degrades the identification accuracy of the statistical features-based RFFI system. On these bases, we propose a novel approach named LB-SCSBD to generate two parallel SQ signal sequences within a limited range. Additionally, we take into account the null and pilot subcarriers of the WiFi OFDM data in the proposed method.

Let $\boldsymbol{s}_k = [s_k(0), s_k(1), \ldots, s_k(I_1-1)]$ denote the k^{th} corrected OFDM signals in the data field of a WiFi frame and $\boldsymbol{ID} = [id(0), id(1), \ldots, id(I_2-1)]$ denote the data subcarrier indices, where I_1 is the length of an OFDM symbol after removing the cyclic prefix (CP) and I_2 is the total number of the data subcarriers. Then, we can derive the OFDM symbol $\boldsymbol{S}_k = [S_k(0), S_k(1), \ldots, S_k(I_1-1)]$ by performing the fast Fourier transform (FFT) as

$$S_k(n_1) = \sum_{i_1=0}^{I_1-1} s_k(i_1) e^{-j2\pi i_1 n_1/I_1}; 0 \le n_1 \le I_1 - 1. \quad (8)$$

Due to the fact that the duration of an OFDM symbol is 4 μs, the slow fading channel behaves in a correlated manner during such a short period. Thus, we can expect the channel coefficients to remain unchanged during the transmission of each OFDM symbol. In this case, according to [30], $S_k(n_1)$ can be approximated as

$$S_k(n_1) \approx \lambda \cdot H(n_1) \cdot Y_k(n_1) + \hat{W}(n_1), \quad (9)$$

where λ is a constant factor related to the PO and residual CFO; $H(n_1)$ is the n_1^{th} channel frequency response; $Y_k(n_1)$ is the n_1^{th} element of the k^{th} OFDM symbol distorted with the transmitter imperfections; $\hat{W}(n_1)$ is the n_1^{th} frequency-domain noise. Moreover, λ, $H(n_1)$ and $Y_k(n_1)$ can be expressed as

$$\begin{aligned} \lambda &= e^{-j(\pi\varepsilon' I_1 + \Phi')}, \\ H(n_1) &= \sum_{i=1}^{I} h_{\tau_i'} W_{I_1}^{\tau_i' n_1}, \\ Y_k(n_1) &= \sum_{i_1=0}^{I_1-1} y_k(i_1) W_{I_1}^{i_1 n_1}, \end{aligned} \quad (10)$$

where $W_{I_1} = e^{-j2\pi/I_1}$ and $y_k(i_1)$ is the i_1^{th} element of the k^{th} transmitted OFDM signal.

It is clear that the hybrid impacts caused by the multipath fading channel, PO and residual CFO can be roughly deemed as the multiplicative interferences in the frequency domain. Hence, by leveraging the strong correlations of the channel frequency responses at the neighboring subcarriers, the multiplicative interferences can be significantly suppressed in the SQ domain [30].

Hence, we first perform the right circular shift by one step on $\boldsymbol{ID}$ vector, then a new vector of the data subcarrier indices can be obtained as

$$\begin{aligned} \boldsymbol{ID}^{rcs} &= [id^{rcs}(0), id^{rcs}(1), \ldots, id^{rcs}(I_2-1)] \\ &= [id(I_2-1), id(0), \ldots, id(I_2-2)]. \end{aligned} \quad (11)$$

Thereafter, we can generate the index pairs of the data subcarriers as $\{id(i_2), id^{rcs}(i_2)\}, (0 \le i_2 \le I_2-1)$. Let $\boldsymbol{\Upsilon}_k^r = [\Upsilon_k^r(0), \ldots, \Upsilon_k^r(i_2), \ldots, \Upsilon_k^r(I_2-1)]$ denote the right circular shift SQ signal vector, then its i_2^{th} element can be calculated as

$$\Upsilon_k^r(i_2) = \frac{S_k(id(i_2))}{S_k(id^{rcs}(i_2))}. \quad (12)$$

To effectively mitigate the channel effects, we extract the SQ signals that can satisfy the condition of $id(i_2) - id^{rcs}(i_2) =$

Algorithm 1 Limiter-Based Spectral Circular Shift Bidirectional Division (LB-SCSBD)

Input: A complete OFDM signal without CP, $\boldsymbol{s}_k$; the data subcarrier indices, $\boldsymbol{ID}$; the maximum limiter output, A_{max}; the initial index of output, $i_3 = 0$;
Output: The spectral quotient signal sequences: $\boldsymbol{v}_k^r$; $\boldsymbol{v}_k^l$;

```
Performing the FFT operation on s_k to derive S_k;
Generating the shifted data subcarrier indices vector ID^rcs by Eq. (11);
Calculating the SQ vector Υ_k^r with Eq. (12);
for i_2 = 0; i_2 < I_2; i_2 ++ do
    if id(i_2) − id^rcs(i_2) = 1 then
        Extracting the qualified SQ signal as:
                Υ̂_k^r(i_3) = Υ_k^r(i_2);
        Deriving the SQ signal of left circular shift as:
                Υ̂_k^l(i_3) = 1/Υ̂_k^r(i_3);
        Generating v_k^r(i_3) and v_k^l(i_3) by Eq. (14)
        i_3 ++;
    else
    end if
end for
return v_k^r, v_k^l.
```

1 from $\boldsymbol{\Upsilon}_k^r$, and then the extracted SQ vector is denoted as $\hat{\boldsymbol{\Upsilon}}_k^r = [\hat{\Upsilon}_k^r(0), \ldots, \hat{\Upsilon}_k^r(i_3), \ldots, \hat{\Upsilon}_k^r(I_3 - 1)]$, where I_3 is the total number of the qualified SQ signals. Meanwhile, we also generate the left circular shift SQ signal vector $\hat{\boldsymbol{\Upsilon}}_k^l = [\hat{\Upsilon}_k^l(0), \ldots, \hat{\Upsilon}_k^l(i_3), \ldots, \hat{\Upsilon}_k^l(I_3 - 1)]$ via the above steps. It is noted that the elements in $\hat{\boldsymbol{\Upsilon}}_k^l$ are exactly the reciprocal of that in $\hat{\boldsymbol{\Upsilon}}_k^r$, which can be expressed as

$$\hat{\Upsilon}_k^l(i_3) = \frac{1}{\hat{\Upsilon}_k^r(i_3)}. \tag{13}$$

After passing through a limiter with the maximum output amplitude of A_{max}, we can derive the parallel SQ sequences, i.e., $\boldsymbol{v}_k^r = [v_k^r(0), \ldots, v_k^r(i_3), \ldots, v_k^r(I_3 - 1)]$ and $\boldsymbol{v}_k^l = [v_k^l(0), \ldots, v_k^l(i_3), \ldots, v_k^l(I_3 - 1)]$, and their elements can be calculated as

$$v_k^{\wp}(i_3) = \begin{cases} \hat{\Upsilon}_k^{\wp}(i_3), & |\hat{\Upsilon}_k^{\wp}(i_3)| \le A_{max} \\ \frac{A_{max} \cdot \hat{\Upsilon}_k^{\wp}(i_3)}{|\hat{\Upsilon}_k^{\wp}(i_3)|}, & \text{otherwise}, \end{cases} \tag{14}$$

where the superscript $\wp$ denotes r or l.

The detailed steps of the LB-SCSBD are summarized in Algorithm 1. After K times repetitive operations on different OFDM data, we can derive the following parallel SQ signal vectors from a complete WiFi frame as

$$\begin{aligned} \boldsymbol{v}^r &= [\boldsymbol{v}_1^r, \boldsymbol{v}_2^r, \ldots, \boldsymbol{v}_K^r], \\ \boldsymbol{v}^l &= [\boldsymbol{v}_1^l, \boldsymbol{v}_2^l, \ldots, \boldsymbol{v}_K^l], \end{aligned} \tag{15}$$

where the length of each vector is KI_3.

C. Channel-Robust Signal Representations

Considering the need for signal analysis, we first define the SQC symbols as follows:

Definition 1: Given Q is the complex-valued set comprised of M-QAM symbols, then it can be used to generate a second-dimension space $\mathbb{D} = \{(\mathscr{A}, \mathscr{B}) | \mathscr{A} \in Q, \mathscr{B} \in Q\}$. Let $f : \mathbb{D} \mapsto P$ denote a function of two variables, which can also be written in the following form:

$$f(\mathbb{D}) = \{\mathscr{P} | \mathscr{P} = \mathscr{A}/\mathscr{B}, \mathscr{A} \in Q, \mathscr{B} \in Q\}, \tag{16}$$

where P is the set of spectral quotient constellation symbols based on M-QAM and $\mathscr{P} \in P$.

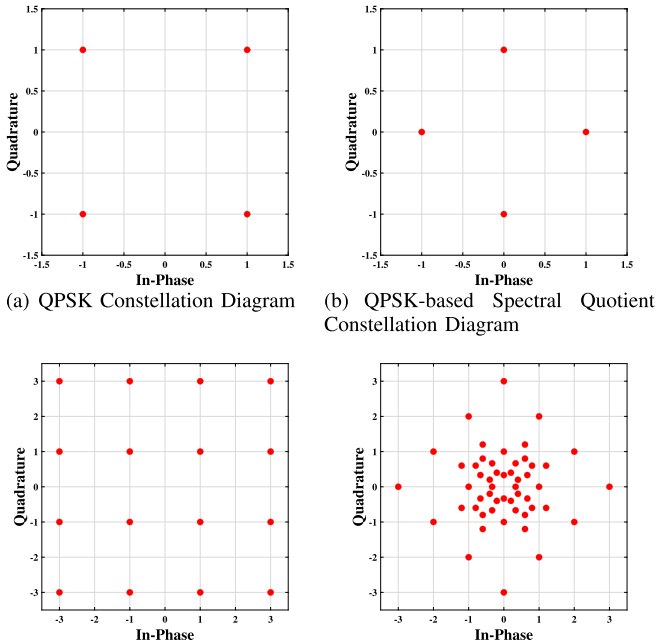
Fig. 4 provides the spectral quotient constellation diagrams in terms of QPSK and 16QAM. It should be noted that the SQC symbols are the transformation of the QAM symbols and don't contain any imperfections. Hence, the variations between the SQ signal and SQC symbols can be attributed to the hybrid effects of the transmitter impairments and interferences (noise, residual channel effects, etc.).

The SQC error vector is a measure of how accurately the generated SQ signal is within its constellation, which can be obtained as

$$\begin{aligned} \boldsymbol{e}^r &= \boldsymbol{v}^r - \boldsymbol{p}^r, \\ \boldsymbol{e}^l &= \boldsymbol{v}^l - \boldsymbol{p}^l, \end{aligned} \tag{17}$$

where $\boldsymbol{p}^r$ and $\boldsymbol{p}^l$ are the vectors of decided symbols after performing the minimum Euclidean distance between each SQ signal and the SQC symbols in P, and their n^{th} elements are derived as

$$\begin{aligned} p^r(n) &= \underset{\mathscr{P} \in P}{\operatorname{argmin}} |v^r(n) - \mathscr{P}|, \\ p^l(n) &= \underset{\mathscr{P} \in P}{\operatorname{argmin}} |v^l(n) - \mathscr{P}|. \end{aligned} \tag{18}$$



(a) QPSK Constellation Diagram (b) QPSK-based Spectral Quotient Constellation Diagram

(c) 16QAM Constellation Diagram (d) 16QAM-based Spectral Quotient Constellation Diagram

Fig. 4. The scatterplot of the QAM constellation diagrams and the corresponding spectral quotient constellation diagrams.

In the following, we investigate two channel-robust and magnitude-based signal representations that can be fed into the subsequent feature extractor.

1) Spectral Quotient Magnitude: The SQ signal, especially its magnitude, contains abundant device-specific information, which can be used for device identification. The SQM sequences are expressed as

$$\begin{aligned} \boldsymbol{v}_r^M &= |\boldsymbol{v}^r|, \\ \boldsymbol{v}_l^M &= |\boldsymbol{v}^l|. \end{aligned} \tag{19}$$

2) Spectral Quotient Constellation Error Vector Magnitude: EVM is a popular system-level performance metric that helps gauge the impacts of all impairments simultaneously from a single value. Therefore, the signal representation of the SQC-EVM vectors can be derived as

$$\begin{aligned} \boldsymbol{e}_r^M &= |\boldsymbol{e}^r|, \\ \boldsymbol{e}_l^M &= |\boldsymbol{e}^l|. \end{aligned} \tag{20}$$

D. Moment-Based Statistical Feature Extractor

In the feature extraction module, we propose a novel feature extractor named MB-SFE to exploit the discriminant information induced by transmitter imperfections. Specifically, a total of sixteen moment-based statistics (i.e., first, second,

TABLE I
IMPAIRMENTS OF EIGHT DEVICES USED IN SIMULATIONS

Device Code	IQ Imbalance	Power Amplifier		Normalized CFO Ranges (ppm)
		Model	Normalized Parameters	
Λ_1	$G^{tx}=0.10$dB $\theta_d^{tx}=2.12°$	Saleh	$\alpha_1=2.1587$ $\beta_1=1.1517$ $\alpha_2=4.0033$ $\beta_2=9.1040$	[-36,7]
Λ_2	$G^{tx}=-0.78$dB $\theta_d^{tx}=-9.57°$		$\alpha_1=1.2000$ $\beta_1=0.3600$ $\alpha_2=0.3744$ $\beta_2=0.3600$	[16,37]
Λ_3	$G^{tx}=1.00$dB $\theta_d^{tx}=11.39°$		$\alpha_1=18.5338$ $\beta_1=1.0594$ $\alpha_2=14.0668$ $\beta_2=45.4472$	[-2,22]
Λ_4	$G^{tx}=0.82$dB $\theta_d^{tx}=9.64°$		$\alpha_1=6.6492$ $\beta_1=0.8832$ $\alpha_2=2.4528$ $\beta_2=5.5296$	[78,98]
Λ_5	$G^{tx}=-0.06$dB $\theta_d^{tx}=-2.05°$	Rapp	$a=1.2$ $b=2.0$ $c=1.0$	[-114,-101]
Λ_6	$G^{tx}=0.64$dB $\theta_d^{tx}=7.76°$		$a=1.0$ $b=1.0$ $c=2.0$	[44,60]
Λ_7	$G^{tx}=0.46$dB $\theta_d^{tx}=5.88°$		$a=7.5$ $b=6.5$ $c=3.5$	[-82,-56]
Λ_8	$G^{tx}=-0.96$dB $\theta_d^{tx}=-11.42°$	Polynomial	$a_1=0.9798-0.2887i$ $a_3=-0.2901+0.4350i$	[12,27]

Notation: The input saturation threshold of PA is set to 1; the output power of each device is normalized in the transmitter; $\theta^{tx}=\theta_d^{tx}\pi/180$.

third and fourth moments) are extracted from four magnitude-based sequences, and then they are employed to serve as the discriminative features in the proposed RFFI system. Let $\mathbf{\Psi}=[\mathbf{\Psi}^1,\mathbf{\Psi}^2,\mathbf{\Psi}^3,\mathbf{\Psi}^4]$ denote the extracted statistical feature vector and $\mathbf{\Psi}^\lambda=[\Psi_{r,\lambda}^v,\Psi_{l,\lambda}^v,\Psi_{r,\lambda}^e,\Psi_{l,\lambda}^e]$ is the λ-order moment vector. Then, the elements of $\mathbf{\Psi}^\lambda$ can be calculated as follows

$$\Psi_{r,\lambda}^v=\frac{1}{KI_3}\sum_{n=1}^{KI_3}|v_r^M(n)|^\lambda, \tag{21}$$

$$\Psi_{l,\lambda}^v=\frac{1}{KI_3}\sum_{n=1}^{KI_3}|v_l^M(n)|^\lambda, \tag{22}$$

$$\Psi_{r,\lambda}^e=\frac{1}{KI_3}\sum_{n=1}^{KI_3}|e_r^M(n)|^\lambda, \tag{23}$$

$$\Psi_{l,\lambda}^e=\frac{1}{KI_3}\sum_{n=1}^{KI_3}|e_l^M(n)|^\lambda. \tag{24}$$

E. SVM Classifier

SVM is originally designed for binary classification. Broadly, RFFI is used for multi-class classification scenarios. The conventional way to extend binary-classification SVM to multi-class scenarios is to decompose a multi-class problem into several two-class classification problems, and then we can implement the one-against-one strategy for the multi-class SVM classifier training [33].

Considering a γ-class classification scenario in an RFFI system, where we have L training samples: $\{\mathbf{\Psi}_1^{train},\Lambda_{i_1}\},\ldots,\{\mathbf{\Psi}_L^{train},\Lambda_{i_L}\}$. Here Λ_i is the device code and $i\in[1,2,\ldots,\gamma]$. According to the one-against-one strategy, we should construct $J=\gamma(\gamma-1)/2$ binary-classification SVM classifiers. During the SVM training stage, the polynomial is chosen as the kernel function and the hyperparameters of each SVM are independently updated in terms of the training samples. Supposing that we have trained J binary-classification SVM$_j$ ($j\in[1,2,\ldots,J]$) and a testing sample $\{\mathbf{\Psi}_l^{test},\Lambda_{i_l}\}$ is fed into the well-trained classifier, then each SVM classifier will make a prediction on the testing sampling label Λ^j (prediction of SVM$_j$). Obviously, J prediction results of the testing sampling will be obtained in the meanwhile. To make the final prediction, we adopt a voting approach named max wins strategy [17] to decide the predicted device code $\Lambda_\aleph$ ($\aleph\in[1,2,\ldots,\gamma]$).

TABLE II
THE DELAY TAPS AND NORMALIZED POWER OF THE MULTIPATH FADING CHANNEL MODELS IN SIMULATIONS

Power \ Channels / Path Delay	C_1	C_2	C_3	C_4	C_5
50 ns	0.8	0.83	0.86	0.86	0.86
100 ns	0.2	0.17	0.14	0.10	0.10
150 ns	–	–	–	0.04	0.02
200 ns	–	–	–	–	0.014
250 ns	–	–	–	–	0.006

Notation: ns is the abbreviation of the nanosecond.

IV. EXPERIMENTAL RESULTS

In this section, we first introduce the experimental setup for the WiFi datasets generation and multi-class SVM training as well as the evaluation metrics. Then, we will validate the effectiveness of the LB-SCSBD method. Meanwhile, the classification performance of the proposed channel-agnostic RFFI system is investigated by experimental evaluations. Moreover, we compare the performance of our methods with some other existing RFFI methods on the simulated datasets. Finally, we use the data originating from an open dataset [28] to evaluate the proposed RFFI system in the face of the real-world collected signals. The detailed experimental designs and results are given in the following.

A. Experimental Setup

This subsection will introduce the configuration parameters used for the generation of the datasets in terms of the device

TABLE III
THE GENERATED CONDITIONS OF TWELVE SIMULATED DATASETS

Dataset Code \ Conditions	Impairments	Modulation	Channel
DAT_0^1	✓	QPSK	AWGN
DAT_1^1	✓	QPSK	C_1
DAT_2^1	✓	QPSK	C_2
DAT_3^1	✓	QPSK	C_3
DAT_4^1	✓	QPSK	C_4
DAT_5^1	✓	QPSK	C_5
DAT_0^2	✓	16QAM	AWGN
DAT_1^2	✓	16QAM	C_1
DAT_2^2	✓	16QAM	C_2
DAT_3^2	✓	16QAM	C_3
DAT_4^2	✓	16QAM	C_4
DAT_5^2	✓	16QAM	C_5

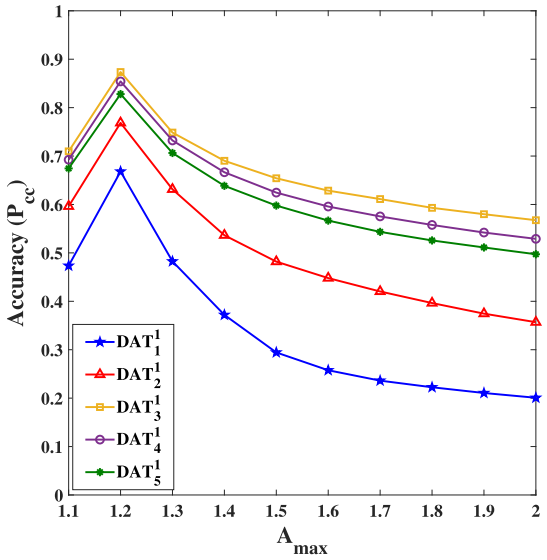
impairments and WiFi signal settings as well as the multipath fading channel models. Meanwhile, the evaluation metrics are also provided in this part.

1) Device Impairments: To generate the simulated datasets, eight device models with different impairments are configured in this subsection. As reported from [24], the phase imbalance usually ranges from 2 to 11.42 degrees and the absolute gain imbalance generally runs from 0.02 to 1 dB, so we use a set of gain and phase imbalances within these ranges. Moreover, the utilized power amplifier models are referred from the literature [34], [35], [36], [37], [38], [39]. Since the OFDM technique will cause a large peak-to-average power ratio (PAPR) in waveforms, the input back-off (IBO) technique[1] prior to PA is adopted to keep the simulated signals away from severe nonlinear distortions (especially the saturated distortions). Furthermore, the CFO values of different devices are set within limited ranges[2] and follow the uniform random distribution [42], while the PO values follow the same distribution within $[-\pi, \pi]$. The detailed parameters of the device impairments used in our simulations are summarized in Table I.

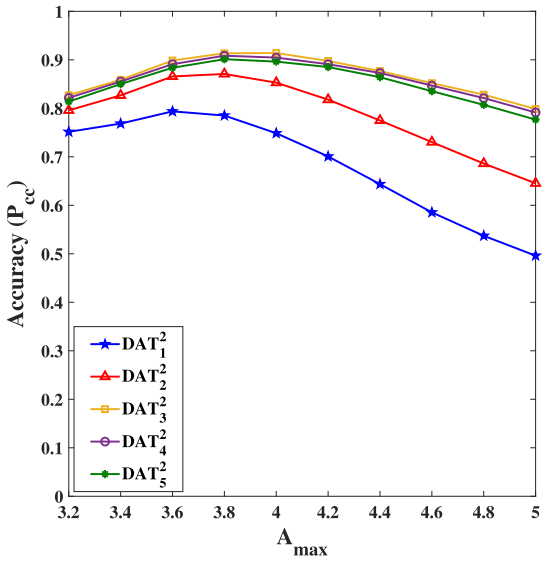
2) WiFi Signal Settings: The carrier frequency and transmission bandwidth are set to 5GHz and 80MHz, respectively. The preamble duration is 20 μs, including 8 μs of L-STF, 8 μs of L-LTF, and 4 μs of L-SIG. We adopt both the QPSK and 16QAM modulation techniques to generate the OFDM symbols in the WiFi data field. On the one hand, the WiFi frame modulated with QPSK lasts for 0.48 milliseconds (ms) and contains 115 OFDM symbols (3.2 μs) with CP (0.8 μs). On the other hand, the WiFi frame modulated with 16QAM lasts for 0.364 ms and contains 86 OFDM symbols with CP. After removing the CP, the length of each OFDM symbol in the data field is 256.

3) Multipath Fading Channel Models: As shown in [43], the varying channel will interfere with the transmitter impairments and degrade the classification performance of the RFFI system. In order to focus on the channel-agnostic RFFI system, we take the Rician multipath fading channel into consideration, where five different channel conditions are detailed in Table II. In the first delay tap, there is a line-of-sight (LOS) component and a complex Gaussian variable, while the envelope follows the Rayleigh distribution in other delay taps. Since the channel's coherence time is almost always larger than the duration of 8 μs in wireless local area network (WLAN) settings [44], it is reasonable to assume that the channel is time-invariant in each 8 μs duration. Therefore, for each WiFi frame, the channel fading coefficients are randomly and periodically regenerated every 8 μs.

4) Datasets Description: To test the proposed RFFI method with different channel conditions and modulation types, eight simulated datasets are generated in terms of Table III, where the WiFi datasets under the AWGN channel are also included due to the need for the RFFI system training. Each dataset



(a) QPSK, SNR = 27 dB

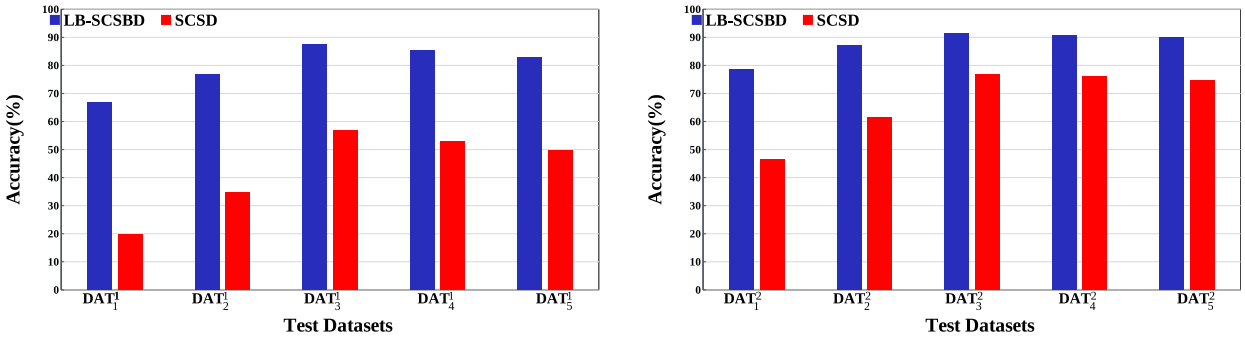


(b) 16QAM, SNR = 27 dB

Fig. 5. The classification performance with different A_{max}.

[1]According to [40], the IBO level is defined as $10\lg\frac{P_{sat}}{P_{in}}$, where P_{sat} is the input saturation power and P_{in} is the average input power. Since the average PAPR is about 7.8 dB, we set the IBO level to 12 dB for all simulated models in this paper.

[2]According to the IEEE 802.11a specification [41], the CFO tolerance with respect to f_c is equal to ± 20 parts per million (ppm, 10^{-6}), hence the maximum tolerable value of ε in Eq. (6) is $\pm 40 \cdot f_c/B$ ppm.



(a) QPSK, SNR = 27 dB, $A_{max} = 1.2$ (b) 16QAM, SNR = 27 dB, $A_{max} = 3.8$

Fig. 6. The performance comparison of P_{cc} considering different SQ-generation methods.

contains 800 samples of the WiFi frames, where the preamble (after performing the CFO correction) and CP (in the data field) are deliberately neglected. In other words, 100 samples of each device are kept in each dataset.

5) Multi-Class SVM Training: To investigate the performance of the proposed RFFI method, we run LIBSVM[3] [45] to train the multi-class SVM classifiers in the following experiments. It should be noted that the moment-based features are extracted from the complete data field (i.e., 115/86 OFDM symbols of QPSK/16QAM) of a single WiFi frame.

6) Evaluation Metrics: The confusion matrix and the overall classification accuracy are used as evaluation metrics, which allow visualization of the classification performance. Generally, the probability of correct classification P_{cc} can be measured as

$$P_{cc} = \sum_{i=1}^{\gamma} P(\Lambda_i) P(\Lambda_{\aleph} = \Lambda_i | \Lambda_i), \tag{25}$$

where $P(\Lambda_i)$ is the prior probability of the device Λ_i and $P(\Lambda_i) = 1/\gamma$; $P(\Lambda_{\aleph} = \Lambda_i | \Lambda_i)$ is the conditional probability of the event that the predicted device code of testing sample $(\Lambda_{\aleph})$ is Λ_i given that the device code of testing sample is Λ_i.

B. Effectiveness of the LB-SCSBD Method

First of all, we explore the impacts of the maximum output amplitude (A_{max}) employed in the LB-SCSBD submodule on the classification performance of the proposed RFFI system. As shown in Fig. 5, the classification results with different A_{max} are provided at SNR = 27 dB. It is clear that we can obtain the best P_{cc} performance when $A_{max} = 1.2$ in the QPSK cases. Meanwhile, all of the P_{cc} values are close to the best performance when $A_{max} = 3.8$ in the 16QAM cases. Hence, the A_{max} values are set to 1.2 (QPSK) or 3.8 (16QAM) in the following simulations, respectively.

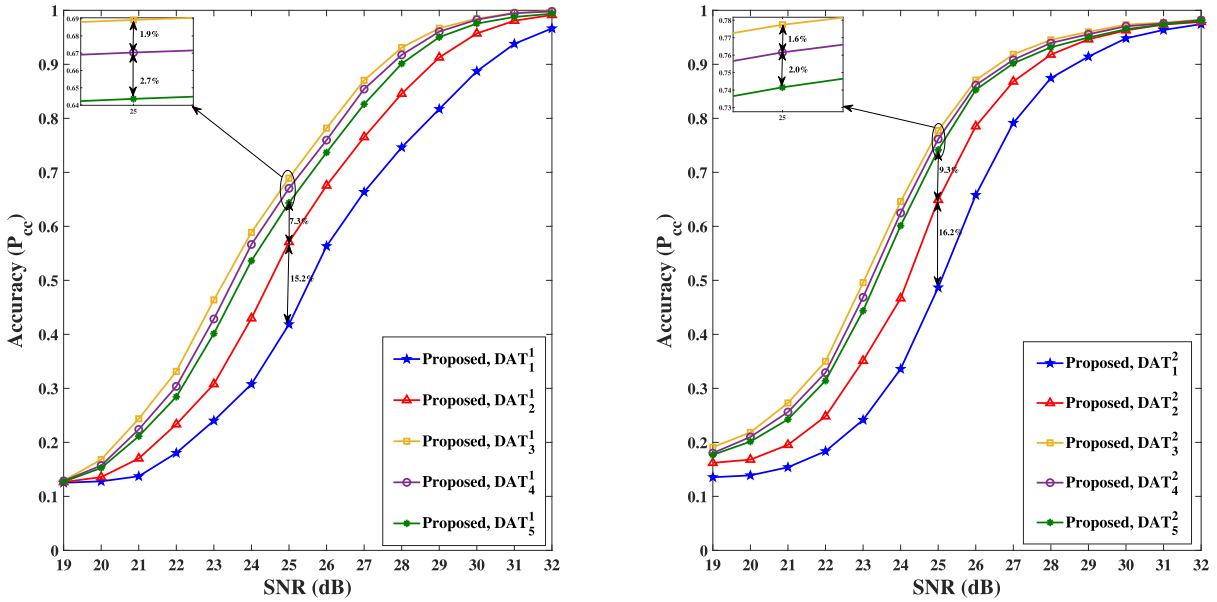
As mentioned in Section III, the LB-SCSBD is a novel method to generate parallel SQ signals within a limited range. To validate its effectiveness, we compare the classification performance of the proposed system under different SQ-generation methods, i.e., the SCSD and LB-SCSBD. The comparison results are provided in Fig. 6, where the SCSD and LB-SCSBD methods are tested in the proposed RFFI system, respectively. We can find that the proposed RFFI system using the LB-SCSBD method leads to the best classification performance in these cases, with 14% – 47% accuracy improvements in comparison to that using the SCSD method. Therefore, we can conclude that the LB-SCSBD method is effective in the experimental scenarios.

C. Evaluation of the Proposed RFFI System

In this subsection, we evaluate the proposed channel-agnostic RFFI system. To investigate the noise effect on classification accuracy, we add artificial AWGN of different SNR levels to the simulated datasets. Since the channel-mitigation effect of the SQ signal degrades severely at high noise levels [30], we simulate the SNR range within 19 dB to 32 dB and the classification results are given in Fig. 7.

It can be observed from Fig. 7(a) and Fig. 7(b) that the overall identification accuracies are dependent on the channel conditions when the noise level is fixed, especially in the medium-level SNR regions (i.e., 23 dB – 29 dB). For instance, there are 1.6% – 29.1% gaps among the accuracy results tested under different channels at SNR = 25 dB. Moreover, when SNR is equal to 32 dB, it is clear that the recognization accuracy of our RFFI system can reach up to 99.84% and 98.26% in the QPSK and 16QAM cases, respectively. Meanwhile, focusing on the SNR regions within 21 dB to 29 dB, we can clearly observe two interesting phenomena from these curves. On the one hand, in terms of the curves marked with the blue pentagram, red triangle, and yellow square, it is apparent that the recognition accuracies will rise up as the normalized power in the main fading path increases when the path delay taps are fixed. On the other hand, according to the curves marked with the yellow square, violet circle, and green snowflake, the recognition accuracies can be degraded with the increase of the path delay taps when the normalized power in the main fading path is fixed. These phenomena can be explained by the fact that the concentration of the channel power distribution will increase the channel frequency correlation between the adjacent subcarriers, then the channel effects can be suppressed more significantly in the generated

[3]In our training process, the type of SVM is C-SVC and the type of kernel function is the polynomial base function, where the gamma is equal to 60 and other hyperparameters are defaults. Moreover, we only use the feature samples without any channel effects to train the SVM.



(a) QPSK cases, $A_{max} = 1.2$ (b) 16QAM cases, $A_{max} = 3.8$

Fig. 7. The overall classification accuracy curves of the proposed RFFI system on different datasets (i.e., collected under different channel conditions).

SQ signals, and hence improving the overall identification accuracies.

D. Performance Comparison With Existing Methods

In this subsection, we further compare the classification performance of our method with other two existing RFFI methods based on statistical features:

1) In [17], the skewness and kurtosis extracted from the first two decomposed signals of empirical mode decomposition (EMD) are served as RFF under the fading channels. For simplicity, this method is referred to as EMD-SK.
2) In [30], the root mean square, variance, skewness, and kurtosis are extracted from I and Q branches of the spectral quotient sequences generated by the SCSD method, and then they can be employed for devices classification. This approach is called SQ-RVSK.

Note that the EMD-based RFFI method is operated with the baseband signal of the WiFi data field in our experiment. In detail, we first use the EMD algorithm to decompose the I and Q branches of the baseband signals, respectively. Then, we extract the skewness and kurtosis from the first two decomposed signals in each branch. Finally, the extracted features will be fed into the SVM for training and testing.

Table IV shows the classification results of these methods with respect to different datasets at SNR = 30 dB, where the same training conditions are considered. Obviously, the proposed method achieves the best performance in all experiments. However, the accuracy of EMD-SK can only reach 12.71% – 13.81%, which means this method is inefficient in the simulated scenarios. This is because EMD can't alleviate the multipath fading channel effects and then the decomposed signals are heavily impacted by the channel effects. Although the SQ-RVSK method is effective, its accuracies have significant gaps (38.33% – 60.44%) in comparison to the accuracies of the proposed method. Hence, we can draw the conclusion that the proposed method exhibits robustness and superiority in comparison to the SQ-RVSK and EMD-SK methods for the channel-agnostic RFFI tasks.

TABLE IV
THE CLASSIFICATION RESULTS OF THREE RFFI SCHEMES UNDER DIFFERENT DATASETS

Datasets \ Method	Proposed	EMD-SK [17]	SQ-RVSK [30]
DAT$^1_1$	88.65%	12.85%	28.21%
DAT$^1_2$	95.78%	12.99%	42.98%
DAT$^1_3$	98.53%	13.81%	60.20%
DAT$^1_4$	98.38%	13.42%	54.15%
DAT$^1_5$	97.57%	12.95%	51.42%
DAT$^2_1$	94.81%	12.71%	38.87%
DAT$^2_2$	96.29%	12.83%	44.35%
DAT$^2_3$	97.34%	13.51%	51.81%
DAT$^2_4$	97.05%	13.12%	50.44%
DAT$^2_5$	96.50%	12.99%	50.66%

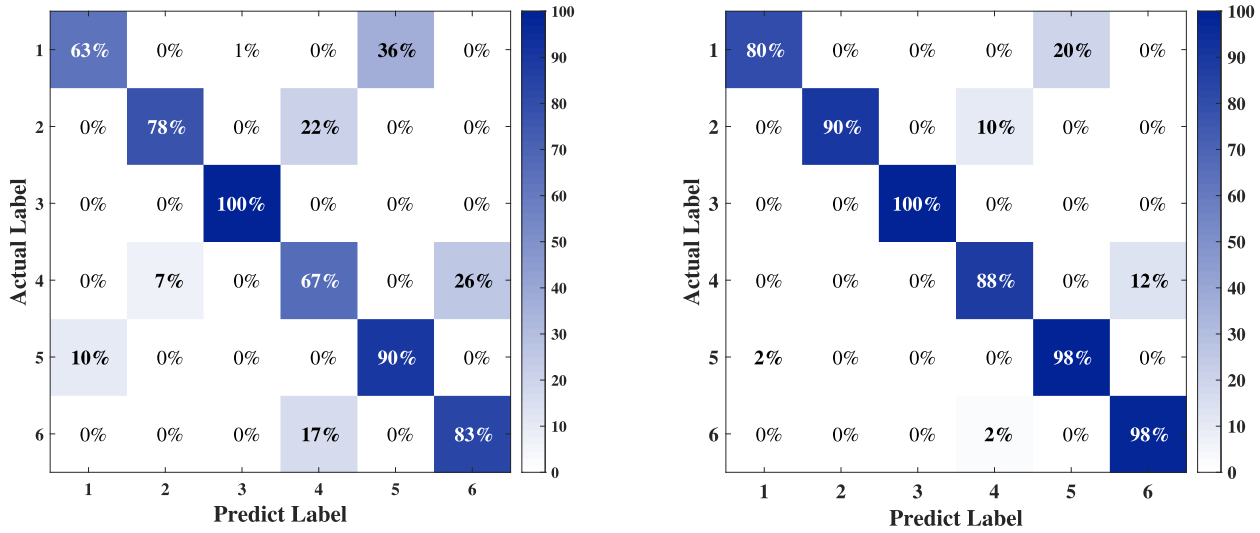
Notation: All of the RFFI schemes are trained using the dataset generated under the AWGN channel, where SNR = 30 dB.

E. Performance on the Open Dataset

In [28], the authors first use the B210 radio receiver to collect the raw IQ samples from over-the-air transmissions of different USRP X310 transmitter radios and then release this dataset online. As can be learned from their work, it is hard to classify raw samples collected from the same devices but at different times (due to the dynamic channel), and the classification result will be unpredictable even for four devices.

In this part, we use the six devices' data collected at different times[4] to verify the effectiveness of our RFFI system.

[4]The data used in our experiments is saved in the "ft" folder, and their device codes are 3124E4A, 3123D7B, 3123D64, 3123D65, 3123D78, 3123D89. Moreover, we use the data recorded in the first run for training and then use the data recorded in the second run for testing.



(a) $L_f = 1$, $A_{max} = 1.08$

(b) $L_f = 5$, $A_{max} = 1.08$

Fig. 8. Classification results on the open dataset with different L_f.

Specifically, we first implement the Schmidl-Cox algorithm to detect the start of the WiFi frame in the received data streams. Then, the CFO estimation and correction should be performed by the two-step CFO estimator. Afterward, we use L_f WiFi frames to generate the parallel SQ sequences according to the proposed LB-SCSBD method, where the A_{max} is 1.08. After extracting the moment-based features, we will feed them into the multi-class SVM classifier for training. Finally, we test the classification performance of the trained SVM by predicting the feature vectors extracted from the samples collected at different times. Fig. 8 shows the confusion matrixes of the classification results using the proposed RFFI system with different L_f, where the overall classification accuracies are 80.17% at $L_f = 1$ and 92.42% at $L_f = 5$, respectively. A significant improvement of the overall accuracy can be made with the growth of L_f, since in this case the statistical stability can be enhanced, and then the extracted statistical features are more separable in multi-class SVM. Finally, we can make a conclusion that our RFFI system is still effective on the real-world collected dataset.

V. Conclusion

In this paper, we proposed a channel-agnostic RFFI method and employed the legacy WiFi frame as a case study for experimental evaluation. We first configured eight device models of the transmitter with different IQ imbalances and PA nonlinearity. Then, we generated the simulated WiFi datasets in terms of these models under different channel conditions, where two types of modulation formats were considered. The AWGN datasets were used for training the multi-class SVM, while others were used for testing. In our experimental evaluation, we showed that the proposed RFFI system using the LB-SCSBD method outperformed that using the SCSD method, resulting in 14% – 47% accuracy improvements at SNR = 27 dB. Moreover, when SNR = 32 dB, our RFFI system can reach up to 99.84% and 98.26% accuracies in the QPSK and 16QAM cases, respectively. In comparison to two existing RFFI methods based on statistical features, our method provided the superior and the most robust classification performance when facing channel-agnostic RFFI tasks. At last, we tested the proposed method on the open datasets collected at different times, the experimental results showed that our method was also effective and achieved an accuracy of 92.42% with six USRP devices.

Appendix A
Power Amplifier Models

A. Saleh Model

Saleh model [34] is one of the typical PA models used to characterize both the amplitude-modulation-to-amplitude-modulation (AM-AM) and amplitude-modulation-to-phase-modulation (AM-PM) distortions. which is denoted as

$$y(t) = \mathscr{F}(z(t)) = A(|z(t)|)e^{j(\phi(z(t))+\varphi(|z(t)|))}, \tag{26}$$

where $\phi(\cdot)$ is the phase operator, respectively; $A(\cdot)$ denotes the AM-AM function and $\varphi(\cdot)$ is the function used to describe the AM-PM effects. Besides, $A(\cdot)$ and $\varphi(\cdot)$ can be denoted as

$$A(|z(t)|) = \frac{\alpha_1|z(t)|}{1+\beta_1|z(t)|^2}, \tag{27}$$

$$\varphi(|z(t)|) = \frac{\alpha_2|z(t)|^2}{1+\beta_2|z(t)|^2}, \tag{28}$$

where α_1, β_1, α_2 and β_2 are the hyperparameters.

B. Rapp Model

Rapp model is a memoryless semi-physical behavioral model, which only considers the AM-AM effects. Hence, the Rapp model can be expressed as [37]

$$y(t) = \mathscr{F}(z(t)) = \frac{az(t)}{(1+(\frac{a|z(t)|}{b})^{2c})^{\frac{1}{2c}}}, \tag{29}$$

where a is the weak-signal gain; b is the saturation output amplitude; c controls the smoothness of the transition from a linear region to a saturated region.

C. Memoryless Polynomial Model

Memoryless polynomial model is a widely used PA model for describing memoryless nonlinear behavior. This model can individually describe both the AM-AM and AM-PM distortions of PA, which is given as [39]

$$y(t) = \mathscr{F}(z(t)) = \sum_{q=1}^{Q} a_{2q-1} z(t)|z(t)|^{2q-1}, \qquad (30)$$

where Q is the number of polynomial terms and $2Q-1$ denotes the maximum order of nonlinear terms; a_{2q-1} is the complex coefficient of the $(2q-1)^{th}$ order nonlinearity.

REFERENCES

[1] F. Meneghello, M. Calore, D. Zucchetto, M. Polese, and A. Zanella, "IoT: Internet of Threats? A survey of practical security vulnerabilities in real IoT devices," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8182–8201, Oct. 2019.

[2] G. Gui, M. Liu, F. Tang, N. Kato, and F. Adachi, "6G: Opening new horizons for integration of comfort, security, and intelligence," *IEEE Wireless Commun.*, vol. 27, no. 5, pp. 126–132, Oct. 2020.

[3] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proc. IEEE*, vol. 104, no. 9, pp. 1727–1765, Sep. 2016.

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

[5] W. Nie, Z. Han, M. Zhou, L. Xie, and Q. Jiang, "UAV detection and identification based on WiFi signal and RF fingerprint," *IEEE Sensors J.*, vol. 21, no. 12, pp. 13540–13550, Jun. 2021.

[6] H. Patel, "Non-parametric feature generation for RF-fingerprinting on ZigBee devices," in *Proc. IEEE Symp. Comput. Intell. Secur. Defense Appl. (CISDA)*, Verona, NY, USA, May 2015, pp. 1–5.

[7] G. Shen, J. Zhang, A. Marshall, L. Peng, and X. Wang, "Radio frequency fingerprint identification for LoRa using deep learning," *IEEE J. Sel. Areas Commun.*, vol. 39, no. 8, pp. 2604–2616, Aug. 2021.

[8] A. Jagannath, Z. Kane, and J. Jagannath, "RF fingerprinting needs attention: Multi-task approach for real-world WiFi and Bluetooth," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Rio de Janeiro, Brazil, Dec. 2022, pp. 4607–4612.

[9] S. Guo, R. E. White, and M. Low, "A comparison study of radar emitter identification based on signal transients," in *Proc. IEEE Radar Conf. (RadarConf)*, Oklahoma City, OK, USA, Apr. 2018, pp. 0286–0291.

[10] A. Jagannath, J. Jagannath, and P. S. P. V. Kumar, "A comprehensive survey on radio frequency (RF) fingerprinting: Traditional approaches, deep learning, and open challenges," 2022, *arXiv:2201.00680*.

[11] N. Soltanieh, Y. Norouzi, Y. Yang, and N. C. Karmakar, "A review of radio frequency fingerprinting techniques," *IEEE J. Radio Freq. Identificat.*, vol. 4, no. 3, pp. 222–233, Sep. 2020.

[12] D. R. Reising, M. A. Temple, and J. A. Jackson, "Authorized and rogue device discrimination using dimensionally reduced RF-DNA fingerprints," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 6, pp. 1180–1192, Jun. 2015.

[13] H. J. Patel, M. A. Temple, and R. O. Baldwin, "Improving ZigBee device network authentication using ensemble decision tree classifiers with radio frequency distinct native attribute fingerprinting," *IEEE Trans. Rel.*, vol. 64, no. 1, pp. 221–233, Mar. 2015.

[14] Y. Huang and H. Zheng, "Radio frequency fingerprinting based on the constellation errors," in *Proc. 18th Asia–Pacific Conf. Commun. (APCC)*, Jeju, South Korea, Oct. 2012, pp. 900–905.

[15] A. Ali and G. Fischer, "Symbol based statistical RF fingerprinting for fake base station identification," in *Proc. 29th Int. Conf. Radioelektronika (RADIOELEKTRONIKA)*, Pardubice, Czech Republic, Apr. 2019, pp. 1–5.

[16] J. Zhang, F. Wang, O. A. Dobre, and Z. Zhong, "Specific emitter identification via Hilbert–Huang transform in single-hop and relaying scenarios," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 6, pp. 1192–1205, Jun. 2016.

[17] B. He and F. Wang, "Cooperative specific emitter identification via multiple distorted receivers," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 3791–3806, 2020.

[18] Y. Wang, G. Gui, H. Gacanin, T. Ohtsuki, O. A. Dobre, and H. V. Poor, "An efficient specific emitter identification method based on complex-valued neural networks and network compression," *IEEE J. Sel. Areas Commun.*, vol. 39, no. 8, pp. 2305–2317, Aug. 2021.

[19] Y. Peng, P. Liu, Y. Wang, G. Gui, B. Adebisi, and H. Gacanin, "Radio frequency fingerprint identification based on slice integration cooperation and heat constellation trace figure," *IEEE Wireless Commun. Lett.*, vol. 11, no. 3, pp. 543–547, Mar. 2022.

[20] 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, Aug. 2019.

[21] L. Ding, S. Wang, F. Wang, and W. Zhang, "Specific emitter identification via convolutional neural networks," *IEEE Commun. Lett.*, vol. 22, no. 12, pp. 2591–2594, Dec. 2018.

[22] S. Huang, C. Lin, W. Xu, Y. Gao, Z. Feng, and F. Zhu, "Identification of active attacks in Internet of Things: Joint model- and data-driven automatic modulation classification approach," *IEEE Internet Things J.*, vol. 8, no. 3, pp. 2051–2065, Feb. 2021.

[23] Y. Wang, G. Gui, Y. Lin, H. Wu, C. Yuen, and F. Adachi, "Few-shot specific emitter identification via deep metric ensemble learning," *IEEE Internet Things J.*, vol. 9, no. 24, pp. 24980–24994, Dec. 2022.

[24] 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*, vol. 16, pp. 3974–3987, 2021.

[25] Q. Xu, R. Zheng, W. Saad, and Z. Han, "Device fingerprinting in wireless networks: Challenges and opportunities," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 1, pp. 94–104, 1st Quart., 2016.

[26] J. K. Tugnait, "Using artificial noise to improve detection performance for wireless user authentication in time-variant channels," *IEEE Wireless Commun. Lett.*, vol. 3, no. 4, pp. 377–380, Aug. 2014.

[27] 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, no. 14, pp. 11276–11289, Jul. 2021.

[28] K. Sankhe et al., "No radio left behind: Radio fingerprinting through deep learning of physical-layer hardware impairments," *IEEE Trans. Cognit. Commun. Netw.*, vol. 6, no. 1, pp. 165–178, Mar. 2020.

[29] 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*, vol. 17, pp. 774–787, 2022.

[30] J. He, S. Huang, S. Chang, F. Wang, B.-Z. Shen, and Z. Feng, "Radio frequency fingerprint identification with hybrid time-varying distortions," *IEEE Trans. Wireless Commun.*, early access, Feb. 22, 2023, doi: 10.1109/TWC.2023.3245070.

[31] T. M. Schmidl and D. C. Cox, "Robust frequency and timing synchronization for OFDM," *IEEE Trans. Commun.*, vol. 45, no. 12, pp. 1613–1621, Dec. 1997.

[32] P. H. Moose, "A technique for orthogonal frequency division multiplexing frequency offset correction," *IEEE Trans. Commun.*, vol. 42, no. 10, pp. 2908–2914, Oct. 1994.

[33] C.-W. Hsu and C.-J. Lin, "A comparison of methods for multiclass support vector machines," *IEEE Trans. Neural Netw.*, vol. 13, no. 2, pp. 415–425, Mar. 2002.

[34] A. A. M. Saleh, "Frequency-independent and frequency-dependent nonlinear models of TWT amplifiers," *IEEE Trans. Commun.*, vol. COM-29, no. 11, pp. 1715–1720, Nov. 1981.

[35] S. V. Kulygin and V. O. Kazachkov, "Modeling of nonlinear distortions in 5G NR systems," in *Systems of Signals Generating and Processing in the Field of On-Board Communications*. Moscow, Russia: IEEE, Mar. 2021.

[36] P. Plotnikov and D. Dolgikh, "Joint compensation of power amplifier nonlinear distortions on transmitter and receiver sides," in *Proc. IEEE Int. Black Sea Conf. Commun. Netw. (BlackSeaCom)*, Sochi, Russia, Jun. 2019, pp. 1–5.

[37] A. E. Jayati and M. Sipan, "Impact of nonlinear distortion with the Rapp model on the GFDM system," in *Proc. 3rd Int. Conf. Vocational Educ. Electr. Eng. (ICVEE)*, Surabaya, Indonesia, Oct. 2020, pp. 1–5.

[38] R. V. S. Devi, C. S. P. Kumar, M. K. Chaitanya, M. V. Deepak, and D. G. Kurup, "Modeling broadband RF power amplifiers using a modified Hammerstein model," in *Proc. Int. Conf. Commun. Signal Process. (ICCSP)*, Chennai, India, Apr. 2018, pp. 186–189.
[39] H. Ku and J. S. Kenney, "Behavioral modeling of nonlinear RF power amplifiers considering memory effects," *IEEE Trans. Microw. Theory Techn.*, vol. 51, no. 12, pp. 2495–2504, Dec. 2003.
[40] Z. Alina and O. Amrani, "On digital post-distortion techniques," *IEEE Trans. Signal Process.*, vol. 64, no. 3, pp. 603–614, Feb. 2016.
[41] 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, no. 5, pp. 1658–1667, May 2014.
[42] K. Iqbal, J. Ahmed, and A. Rafique, "Analysis of carrier frequency offset distribution on efficiency of multicarrier spread spectrum techniques," in *Proc. Int. Conf. Frontiers Inf. Technol. (FIT)*, Islamabad, Pakistan, Dec. 2016, pp. 125–129.
[43] P. Robyns, E. Marin, W. Lamotte, P. Quax, D. Singelée, and B. Preneel, "Physical-layer fingerprinting of LoRa devices using supervised and zero-shot learning," in *Proc. 10th ACM Conf. Secur. Privacy Wireless Mobile Netw.*, Boston, MA, USA, Jul. 2017, pp. 58–63.
[44] H. Rahbari and M. Krunz, "Exploiting frame preamble waveforms to support new physical-layer functions in OFDM-based 802.11 systems," *IEEE Trans. Wireless Commun.*, vol. 16, no. 6, pp. 3775–3786, Jun. 2017.
[45] C.-C. Chang and C.-J. Lin, "LIBSVM: A library for support vector machines," *ACM Trans. Intell. Syst. Technol.*, vol. 2, no. 3, pp. 1–27, Apr. 2011.

Jiashuo He (Graduate Student Member, IEEE) received the M.S. degree in communication engineering from Xidian University, Xi'an, China, in 2021. He is currently pursuing the Ph.D. degree with the Beijing University of Posts and Telecommunications (BUPT), Beijing, China. His current research interests include signal processing, automatic modulation classification, and radio frequency fingerprint identification.

Sai Huang (Senior Member, IEEE) is currently an Associate Professor with the Department of Information and Communication Engineering, Beijing University of Posts and Telecommunications (BUPT), and serves as an Academic Secretary for the Key Laboratory of Universal Wireless Communications, Ministry of Education, China. His research interests include machine learning assisted intelligent signal processing, statistical spectrum sensing and analysis, fast detection and depth recognition of universal wireless signals, millimeter wave signal processing, and cognitive radio network. He is a Reviewer of international journals, such as IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, IEEE WIRELESS COMMUNICATIONS LETTERS, and IEEE TRANSACTIONS ON COGNITIVE COMMUNICATIONS AND NETWORKING and international conferences, such as IEEE ICC and IEEE GLOBECOM.

Zheng Yang received the B.S. degree from the Beijing University of Posts and Telecommunications (BUPT), Beijing, China, in 2020, where he is currently pursuing the Ph.D. degree. His current research interests include automatic modulation classification and security in 5G/B5G.

Kan Yu (Member, IEEE) received the M.S. degree from the School of Information Science and Engineering, Qufu Normal University, in 2016, and the Ph.D. degree from the College of Computer Science and Engineering, Shandong University of Science and Technology, in 2019. He is currently pursuing the second Ph.D. degree with the Key Laboratory of Universal Wireless Communications, Ministry of Education, Beijing University of Posts and Telecommunications (BUPT), Beijing, China. His main research interests include wireless networks, the IoT security, and distributed algorithm design and analysis. He is a member of the China Computer Federation (CCF).

Hao Huan received the B.E. degree in information engineering from Zhengzhou University, Zhengzhou, China, in 2006, and the Ph.D. degree in information and communication engineering from the Beijing Institute of Technology, Beijing, China, in 2013. He was a Visiting Researcher with the University of Delaware, Newark, DE, USA, in 2017. He is currently an Assistant Professor with the School of Information and Electronics, Beijing Institute of Technology, Beijing, China. His research interests include wireless communications and emitter location.

Zhiyong Feng (Senior Member, IEEE) received the B.S., M.S., and Ph.D. degrees in information and communication engineering from the Beijing University of Posts and Telecommunications (BUPT), Beijing, China. She is currently a Full Professor. She is also the Director of the Key Laboratory of Universal Wireless Communications, Ministry of Education. Her main research interests include wireless network architecture design and radio resource management in 5th generation mobile networks (5G), spectrum sensing and dynamic spectrum management in cognitive wireless networks, universal signal detection and identification, and network information theory. She is a Technical Advisor of NGMN. She is active in ITU-R, IEEE, ETSI, and CCSA standards. She is the Editor of *IET Communications* and *KSII Transactions on Internet and Information Systems*, and a Reviewer of IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, and IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS.