Security and Safety, Vol. 3, 2023022 (2024)
https://doi.org/10.1051/sands/2023022
sands.edpsciences.org

Security and Safety in Physical Layer Systems

Review OPEN ACCESS

Information Network

Radio frequency fingerprint identification for Internet of Things: A survey

Lingnan Xie[1], Linning Peng[1,2,*], Junqing Zhang[3], and Aiqun Hu[2,4]

[1] *School of Cyber Science and Engineering, Southeast University, Nanjing 210096, China*
[2] *Purple Mountain Laboratories for Network and Communication Security, Nanjing 211111, China*
[3] *Department of Electrical Engineering and Electronics, University of Liverpool L69 3GJ, Liverpool, UK*
[4] *School of Information Science and Engineering, Southeast University, Nanjing 210096, China*

Received: 28 April 2023 / Revised: 12 July 2023 / Accepted: 2 August 2023 / Published online: 18 September 2023

Abstract Radio frequency fingerprint (RFF) identification is a promising technique for identifying Internet of Things (IoT) devices. This paper presents a comprehensive survey on RFF identification, which covers various aspects ranging from related definitions to details of each stage in the identification process, namely signal preprocessing, RFF feature extraction, further processing, and RFF identification. Specifically, three main steps of preprocessing are summarized, including carrier frequency offset estimation, noise elimination, and channel cancellation. Besides, three kinds of RFFs are categorized, comprising I/Q signal-based, parameter-based, and transformation-based features. Meanwhile, feature fusion and feature dimension reduction are elaborated as two main further processing methods. Furthermore, a novel framework is established from the perspective of closed set and open set problems, and the related state-of-the-art methodologies are investigated, including approaches based on traditional machine learning, deep learning, and generative models. Additionally, we highlight the challenges faced by RFF identification and point out future research trends in this field.

Keywords Radio frequency fingerprint (RFF), Internet of Things (IoT), physical layer security, closed set identification, open set identification, deep learning

Citation Xie L, Peng L and Zhang J et al. Radio frequency fingerprint identification for Internet of Things: A survey. Security and Safety 2024; **3**: 2023022. https://doi.org/10.1051/sands/2023022

1 Introduction

The Internet of Things (IoT) is widely regarded as one of the most important technological innovations of the 21st century, propelling the world towards an era of greater openness and interconnectivity [1]. IoT connects various kinds of sensors into communication networks, enabling end-to-end connectivity through information transfer and sharing [2]. As illustrated in Figure 1, IoT applications have proliferated in every aspect of human society. Many exciting applications are enabled by tens of billions of IoT devices [3], from smart homes [4], healthcare monitoring [5], logistics management [6], to smart factories [7], smart transportation [8], and smart city [9]. With further development of wireless communication networks and the application of technologies such as 5G and 6G, it is predictable that IoT will gain more advanced iterations and progress.

[*] Corresponding author (email: pengln@seu.edu.cn)

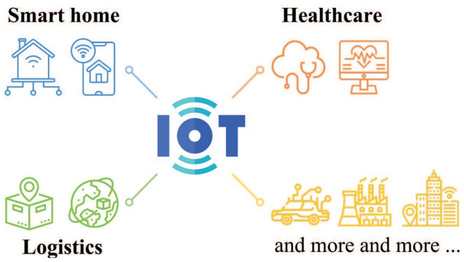

Figure 1. IoT applications

However, owing to the openness of wireless communication networks and the continuously increasing number of terminal nodes, malicious attacks such as jamming, spoofing, and sniffing are possible, which bring threats to information security and system stability [10]. Traditionally, the high cost of an RF transceiver required to generate such attacks has prevented extensive research into related security issues in the technology base that has driven the development of communication standards [11]. Nonetheless, the advent of software-defined radio (SDR) has brought low-cost programmable RF and baseband modules, exposing communication systems to a significantly higher risk of malicious attacks [12]. Therefore, how to achieve wireless network security has become a pressing issue.

Traditional security mechanism relies on the assumption that the time and computational resources consumed to decode the key are much greater than the importance of information, thus utilizing long keys is a feasible way to ensure the security of information transmission. However, the heavy power consumption and the strict requirement for computing capacity brought by this traditional security mechanism make many wireless network devices unaffordable. Additionally, malicious attacks against IoT, such as spoofing attacks and distributed denial-of-service (DDoS) attacks, would consume substantial computing resources if intercepted at the upper layer of the network, thus degrading the efficiency of the whole security system.

Different from traditional cryptographic-based authentication methods, physical layer identification relies on the unique hardware characteristics of devices, based on which the concept of radio frequency fingerprint (RFF) is proposed [13]. The RFF refers specifically to the hardware features contained in the received signal, which typically originate from manufacturing imperfections. Similar to human biometrics, these features are unique and unclonable.

It should be noted that the features extracted from the RF signal must have the following basic characteristics to be considered as RFF.

(1) **Uniqueness:** the extracted features should present differences in different devices to be identified.
(2) **Relative stability:** the extracted features should remain unchanged within a certain period of time, and the long-term stable RFFs are more valuable for research.
(3) **Independence:** the extracted features are only related to the hardware features of the transceiver, rather than to the signal modulation method, the transmitted information, or the features of the wireless channel.

In recent years, the RFF identification technique has evolved rapidly, and the application of machine learning and deep learning algorithms, in particular, injected fresh vitality into related research. Nevertheless, the physical layer security technology based on RFF still has some deficiencies, including (1) Most of the existing studies are based on relatively ideal experimental conditions, and the relevant techniques cannot be effectively applied to more severe environments such as scenarios with low signal-to-noise ratio (SNR). (2) As a physical layer authentication technology, RFF is required to cope with more open and variable application scenarios, yet common problems in practical scenarios such as registration of new devices and detection of unknown devices have not been adequately studied. Therefore, these gaps motivate us to write a comprehensive survey to summarize the existing studies and anticipate future research trends in this field.

This paper focuses on investigating the cutting-edge research findings in the past five years, where a four-step process for RFF identification is proposed and a framework from the perspective of closed and open set problems is presented. Furthermore, we innovatively propose three basic features of RFF, and to the best of our knowledge, the systematic and comprehensive nature of this paper is unprecedented in

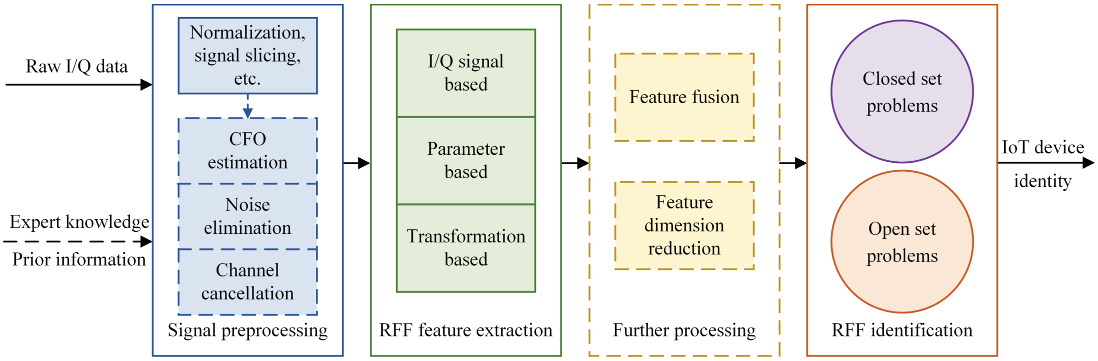

Figure 2. Overview of RFF-based IoT device identification. Note that the black dotted arrow indicates that expert knowledge and prior information may not be available, while the blue and yellow dotted boxes indicate that these signal preprocessing and further processing steps may sometimes be unnecessary. Besides, the purple and orange circles illustrate the distinction between closed set and open set problems

exploring the solution to open set RFF identification. Therefore, this paper is instructive for propelling RFF identification technique to application scenarios.

The remainder of this paper is organized as follows. Section 2 gives a brief overview of the entire RFF identification system, with an emphasis on the definition of closed set and open set problems and the introduction of evaluation metrics. Section 3 demonstrates the role of signal preprocessing in RFF identification. Section 4 summarizes three categories of RFF features. Section 5 introduces two main further processing methods. Section 6 reviews the closed set RFF identification methods with a focus on the adverse factors affecting classification accuracy, such as non-ideal environments and large-scale devices. Section 7 outlines the development of studies on the RFF open set problem with an emphasis on investigating state-of-the-art methods. Section 8 points out the challenges faced by RFF identification technology and the direction of future research. Section 9 concludes this paper.

2 Overview of RFF identification system

The process of RFF identification is usually divided into four steps, which are signal preprocessing, RFF feature extraction, further processing, and RFF identification. Additionally, according to the characteristics of datasets and application scenarios, RFF identification problems can be classified as closed set and open set problems.

Figure 2 demonstrates the details of the RFF identification process. The preprocessing step consists of operations such as normalization and signal slicing without the requirement for prior information or expert knowledge, as well as operations such as compensation of frequency and phase offsets that demand prior information. It should be noted that in the application scenarios, the choice of preprocessing method is determined by the requirements of the identification scheme. Besides, the RFF feature extraction step focuses on mining latent hardware features from the received signal, while the further processing step can be summarized into two main methods, namely feature fusion and feature dimension reduction. Furthermore, in the last step of RFF identification, effective classifiers are constructed to accomplish IoT device identification in closed set and open set problems.

2.1 Signal preprocessing

Signal preprocessing is the first step of RFF-based IoT device identification, which aims at converting received raw I/Q data into a practical form for the identification model. It should be noted that expert knowledge and prior information are not always available during this step, which also brings effect the selection of preprocessing method. Therefore, depending on the availability of expert knowledge and prior information, preprocessing methods can be simply divided into two types: simple operations consist of normalization, signal slicing, *etc.*, and complex operations include frequency and phase compensation, signal stacking, *etc.* In general, simple preprocessing operations are performed to convert received data

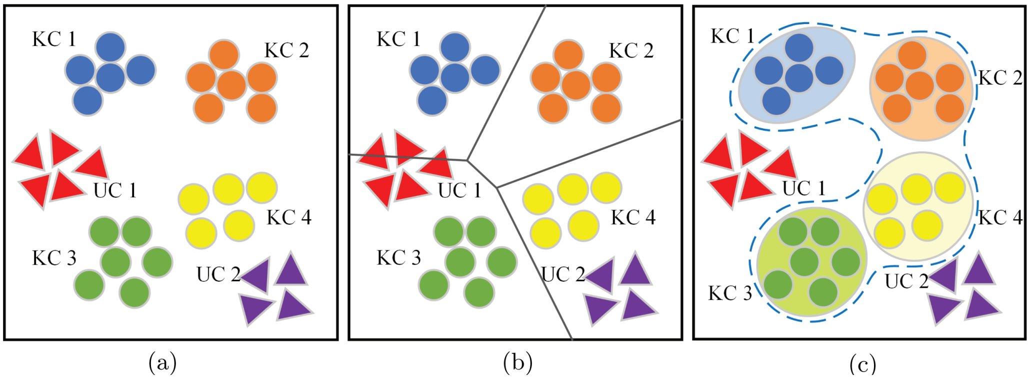

Figure 3. Comparison between closed set and open set problem. Figure 3a demonstrates the distribution of original dataset including 4 known classes (KC) and 2 unknown classes (UC). Figure 3b shows the traditional solution to closed set problem, where the decision boundary is learned and utilized to classify KCs without considering UCs. Figure 3c illustrates open set identification, where the decision boundary either limits the whole scope of KCs to accomplish a two-class classification problem (also known as anomaly detection) or distinguishes among all the KCs and rejects UCs

into training and testing datasets, while the purposes of complex operations can be summarized into three classes, namely carrier frequency offset (CFO) estimation, noise elimination, and channel cancellation. This part will be elaborated on Section 3.

2.2 RFF feature extraction

Following signal preprocessing is the RFF feature extraction, which can be classified into three categories, namely I/Q signal-based, parameter-based, and transformation-based feature extraction methods. I/Q signal-based RFFs rely on the inherent hardware features contained in transmitted I/Q signals, and parameter-based RFFs mainly refer to the basic one-dimensional parameters that can reflect the effects of non-ideal hardware characteristics on modulated signals, while transformation-based RFFs refer to features extracted by various transformation methods. Details will be provided in Section 4.

2.3 Further processing

While the RFF feature extraction step focuses on the physical meaning of extracted features, further processing is an optional step that purely aims at converting extracted RFF features into more applicable forms to accomplish IoT device identification, and thus the preferred methods do not belong to traditional signal processing. It should be noted that the choice of further processing methods is dependent on not only the feature extraction step but also the classifier design in the RFF identification step, thus serving as a connecting link between the preceding and the following procedures. Generally, further processing consists of algorithms such as feature fusion and feature dimension reduction. Details will be demonstrated in Section 5.

2.4 RFF identification

RFF-based device identification is a universal definition that includes both closed set and open set problems. As illustrated in Figure 3, the closed set problem can be summarized as *known device classification*, while the open set problem can be summarized as *unknown device detection*. Known device classification uses the same devices in the training and testing stage and can be considered a multi-class classification problem. Comparatively, unknown device detection could be a two-class classification problem since the receiver only needs to identify signals from known device classes and detect signals from unknown device classes. Specifically, the addition of unknown devices during testing whose samples do not exist in the training stage, is what distinguishes open set problems from closed set problems, and creates additional requirements for the design of classifiers since the output shall cover the prediction of added unknown devices. Furthermore, in this paper, the scenario conditions corresponding to closed set problems are referred to as closed set environments, and those corresponding to open set problems are referred to as open set environments.

Moreover, since many early studies prefer simple scenarios with ideal conditions (*e.g.*, high SNR and constant channels), where the accuracy of RFF identification is more likely to stabilize at high levels, this paper refers to the opposite scenarios as non-ideal environments. Notably, the RFF features utilized in the identification step are only determined by the requirements of specific experimental scenarios (*e.g.*, no prior information, resource limitation, low SNR) and the design of the identification scheme (*e.g.*, choice of RFF extraction method), rather than the problem category (closed set or open set). However, owing to the different preferences for experimental hypotheses in the existing studies on closed set and open set problems, it seems that these two problems require different RFF features. In fact, both closed set and open set problems demand RFF features of great validity as well as generalization ability, and the greater the better.

Details of closed set and open set RFF identification will be demonstrated in Sections 6 and 7, respectively.

2.5 Evaluation metric

2.5.1 Closed set problem

The closed set problem of RFF identification requires no consideration of the effects generated by unknown devices, instead mainly concerns the classification task of known devices, expecting to accurately classify every sample in the test set under different conditions, therefore the classification accuracy (CA) is the most important evaluation metric. Given the number of testing samples that are correctly predicted, T, and the number of samples incorrectly predicted, F, the CA is defined as

$$\mathrm{CA} = \frac{T}{T+F}. \tag{1}$$

2.5.2 Open set problem

The open set problem of RFF identification focuses on the detection of unknown devices whose signal samples do not appear in the training set and therefore can reflect the openness of the real-world environment.

For the evaluation metric of the RFF identification scheme in the open set problem, the receiver operating characteristic (ROC) curve can be used, which reveals the trade-off between false-positive rate (FPR) and true-positive rate (TPR) at various threshold settings. Given the true positive (TP), the true negative (TN), the false positive (FP), and the false negative (FN) rates, TPR and FPR are respectively defined as:

$$\mathrm{TPR} = \frac{\mathrm{TP}}{\mathrm{TP}+\mathrm{FN}}, \quad \mathrm{FPR} = \frac{\mathrm{FP}}{\mathrm{FP}+\mathrm{TN}}, \tag{2}$$

where TPR reflects the proportion of correctly classified positive samples to all positive samples, and FPR reflects the proportion of incorrectly classified negative samples to all negative samples. Here positive and negative samples represent signals from the known and unknown devices, respectively. Meanwhile, the area under the curve (AUC) and the equal error rate (EER) calculated from the ROC curve are also important evaluation metrics, among which the EER refers to the point where FNR and FPR are equal. Here $\mathrm{FNR} = 1 - \mathrm{TPR}$. It is worth noting that the closer the AUC and EER are to one and zero respectively, the better the detection performance is. Figure 4 illustrates the concepts of the ROC curve.

Furthermore, this paper introduces *openness* as a metric to characterize the composition of the dataset in open set problems [14, 15]. Let C_{tr} and C_{te} respectively represent the number of devices used in training and testing, then the openness of the corresponding identification task is:

$$\mathrm{Openness} = 1 - \sqrt{\frac{2 \times C_{tr}}{C_{tr} + C_{te}}}. \tag{3}$$

In most cases, C_{te} is equal to the total number of known and unknown devices, therefore the openness in (3) can be further expressed as:

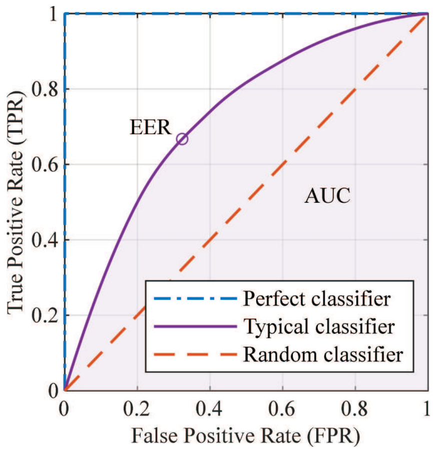

Figure 4. ROC curves for different kinds of classifiers. A perfect classifier is what we always want, and a random classifier is equivalent to a random guess

$$\text{Openness} = 1 - \sqrt{\frac{2 \times A}{2 \times A + O}}, \tag{4}$$

where A and O represent the number of known devices and unknown devices (also can be considered outliers), respectively. Obviously, larger openness corresponds to more open problems, whereas an openness of zero means that the identification task is actually a closed set problem, therefore the difficulty of open set identification increases with openness in a certain range. However, when openness is very large (*e.g.*, close to 1), the decision boundary for known and unknown devices is instead easier to determine because there are only a very small number of known devices. In fact, apart from openness, the total number of devices and the sample imbalance are also dataset characteristics that affect the difficulty of the open set problem.

3 Signal preprocessing

During the process of RFF identification, the function of preprocessing can be summarized as two points. (1) Build up the dataset. Corresponding preprocessing methods are relatively simple, such as normalization, signal slicing, *etc.* (2) Serve the extraction of RFF by choosing different preprocessing methods or simply no preprocessing operations according to the specific requirements of the feature extraction step.

It is worth noting that, however, under some circumstances, RFF feature extraction can also be performed without additional preprocessing operations. For example, the method of using RF-DNA as RFF only requires the accomplishment of zero-meaning and normalization for transient feature sequences without other preprocessing steps [16].

In summary, the main purposes of preprocessing can be categorized into three types, namely CFO estimation, noise elimination, and channel cancellation, which will be discussed below.

3.1 CFO estimation

Although CFO is one of the parameter-based RFFs, it is unstable in many IoT devices and application scenarios and is inclined to change rapidly due to factors such as temperature [17, 18]. This property makes the CFO detrimental to the RFF identification, especially when the population of devices is large [19]. Moreover, the terminal in the 4G/5G/Vehicle to Everything (V2X) system will synchronize its crystal oscillator based on the broadcast signal from the base station or GPS signal (V2X), in which conditions the CFO can no longer be used as an RFF feature [20].

Merchant *et al.* [21] and Qiu *et al.* [22] first accomplished the estimation and compensation of frequency offsets, then extracted the RFF features from I/Q samples. Xie *et al.* [23] utilized deep learning-based methods to improve the process of carrier synchronization and proposed a novel preprocessing module named neural synchronization to reduce the loss of RFF features caused by traditional carrier synchronization techniques, and then extracted the RFF features with the preamble of ZigBee signals. Yin *et al.* [20] completed coarse synchronization on the cyclic prefix of the PRACH preamble before extracting the DCTF features. Shen *et al.* [24] performed synchronization and carrier frequency offset (CFO) compensation before extracting RFF features with STFT. Cekic *et al.* [19] estimated and corrected the CFO using knowledge of the periodic structure of the preamble, where a two-step approach [25] involving a coarse estimation and a fine estimation was performed. In the case of 19 WiFi devices, CFO compensation improved the classification accuracy from 9.86% to 96.37%. Shen *et al.* [26] also applied a two-step approach, where the instantaneous frequency sequences of the preamble were averaged to reach the coarse estimation, and then the fine estimation was completed using the same approach as in [19]. In the simulation experiment, the residual CFO after coarse and fine compensation is between 5 Hz to 20 Hz and between -1 Hz to $+1$ Hz, respectively, when original CFOs uniformly distributed from $-10\,000$ Hz to $+10\,000$ Hz at a signal-to-noise ratio (SNR) of 20 dB. Consequently, based on the RFF identification method proposed in this paper, the CFO compensation improved the classification accuracy from 83.53% to 95.35%.

CFO compensation relies on the prior information of the signal protocol and thus suffers from limitations in practical applications. In particular, for the cases where prior information on the signal protocol is unavailable, Cekic *et al.* [19] suggested that data augmentation can be utilized to reduce the impact of CFO on the results of RFF identification.

3.2 Noise elimination

The performance of RFF-based device identification is relevant to the SNR of the received signal [27]. Low SNR will cause the useful signal to be swamped by noise, thus affecting the extraction of RFF. In fact, extremely low SNR is commonly found in applications related to wireless communication scenarios, such as satellite communication and ocean-going underwater communication. Therefore, the elimination of noise is of great necessity in the preprocessing step. Among the cutting-edge research achievements in recent years, the signal stacking method as well as the wavelet threshold method have been widely used.

3.2.1 Signal stacking method

The signal stacking method relies on the assumption that the noise in the received signal is uncorrelated or partially correlated. In the process of signal stacking, the energy of a useful signal with coherence is enlarged, while the incoherent noise compensates for each other due to its randomness, thus achieving the purpose of improving the SNR with an enhancement ratio equal to the number of stacked signals [28–30].

Based on the above, Xing *et al.* [29] stacked 900 spread spectrum sequences and obtained a classification accuracy of 98.5% at an SNR of -15 dB. However, there was a lack of further exploration of the signal stacking method, as the excessive number of spreading sequences involved in the stacking was an important factor limiting the application value of the scheme. Xie *et al.* [28] completed the stacking of signals based on coherent accumulation and proposed two optimized methods that can reduce the demand for signal length. In the experiment, for the classification task of 10 nRF24 transmitters, they obtained an accuracy close to 100% at 0 dB SNR based on 100 stacked signals and achieved an accuracy of 90% at -5 dB SNR. Inspired by Xing *et al.* [29], Yu *et al.* [31] applied signal stacking to the preamble of the ZigBee signal and accomplished the classification task for 27 devices with 71.5% and 95.7% accuracy at 0 dB and 10 dB SNR, respectively. With regard to the specific operation of signal stacking, they pointed out that the RFF features embedded in the staked signals should be identical and stable, therefore only the steady-state portion of the preamble was stacked and then connected to the semi-steady portion to constitute a complete training sample. Wang and Gan [30] summarized the application of signal stacking methods in denoising, highlighting the limitations of rapid channel variations on the length of signals involved in stacking, and pointing out that the signal stacking method is not effective for partially coherent noise such as colored noise. In addition, they discussed the effects of sampling rate and sampling time on recognition accuracy and concluded that the enhancement of these two parameters within a certain range can increase the features contained in the signal, thus effectively improving the recognition accuracy.

To summarize, the signal stacking method can effectively improve the SNR of the received signal, but its performance is still limited by the length of the stacked signals and the incoherent nature of the noise. Furthermore, for some of the improved stacking methods [28, 30], although they reduce the need for signal length, the similarity between different signal samples inevitably increases after stacking, which therefore raises the possibility of overfitting.

3.2.2 Wavelet threshold method

The wavelet threshold method is a classical denoising method [32, 33], the core of which is that after the wavelet transform of received signals, the wavelet coefficient of the useful signal is larger than that of the noise, so a reasonable threshold can be set to achieve the purpose of noise elimination. Xie *et al.* [28] applied the wavelet threshold method to the field of RFF identification and obtained 98% classification accuracy for 10 nRF24 transmitters at 15 dB SNR and 80% at 5 dB SNR.

The wavelet analysis-based denoising method relies on the setting of a threshold value, and the threshold-based segmentation method tends to eliminate the useful information in the received signal along with the noise, which leads to the reduction in the validity of the extracted RFF features and indirectly degrades the identification accuracy. In fact, in the comparison experiments between these two methods of signal stacking and wavelet threshold proposed in [28], the classification accuracy based on the wavelet threshold method dropped to less than 80% at SNRs below 5 dB, while the classification accuracy based on signal stacking method remained around 80% at −7 dB and −1 dB SNR, with the stacking number of 100 and 10 respectively.

3.3 Channel cancellation

The basic characteristic, *Independence*, determines the necessity to eliminate the influence of channel features on RFF extraction. As a matter of fact, however, whether the variation of distance and direction between transmitter and receiver, or the variation of factors such as ambient humidity and air particulate density will cause the change of channel, thus increasing the difficulty of obtaining stable and effective RFFs from the received signal. Additionally, multipath effects caused by factors such as atmosphere, buildings, and natural terrain will also pose a challenge to the extraction of RFFs. Therefore, in [34], mitigation of channel impacts was performed on the I/Q signals before extracting the RFF features. In [35], the channel response was estimated in advance, and afterwards the I/Q Imbalance was used as the RFF.

Currently, the research on preprocessing methods for canceling channel features is still in the early stage, where the most common method is to construct a mathematical model that characterizes the influence of channel features on the RFF and then separate or eliminate the influence. If channel features can be perfectly canceled in the preprocessing step, the extracted RFF will no longer be affected by channel variations and multipath effects, and then it can be called a channel robust RFF.

To address the effect of channel variation on RFF, Zheng *et al.* [36] utilized a non-parametric function estimation method that correlates the distance variation between the transceiver and the received signal amplitude, equating the polarization mismatch as multiplying the received signal by a projection factor. Restuccia *et al.* [37] partially counteracted phase and amplitude variations caused by the channel based on a blind channel equalization method. Xing *et al.* [38] proposed a channel-robust RFF identification scheme by leveraging the different spectrum of adjacent signal symbols, exploiting the fact that two different symbols in a packet exhibit different RFF features while having similar channel responses during the channel coherence time.

Moreover, to address the impact of multipath channels on RFF, Zheng *et al.* [36] presented that if there are multiple receivers, the channel taps can be estimated using linear regression and the useful information of the received signal can be extracted using the deconvolution method. Wang *et al.* [39] proposed a channel reciprocity-based RFF estimation method and a main path decomposition-based RFF estimation method, completing the separation of channel features from RFFs. Shen *et al.* [24] took the quotient of adjacent frequency units of the spectrogram as the RFF, which partially eliminated the

Table 1. Brief comparison of RFF feature extraction methods

Methods	Prior information requirement	Challenges
I/Q signal-based	Low (raw I/Q) Median (RF-DNA)^a High (the others)	Low identification accuracy. (RF-DNA) Strict demands on classifier design and the possibility of overfitting. (I/Q sample)
Parameter-based	High	Dependence on manually selected features and accurate estimation
Transformation-based	Median^b	Dependence on expert knowledge

Note: $^{(a)}$Requires the information of signal protocol. $^{(b)}$Sometimes the prior information is required for signal preprocessing.

effect of multipath. Rajendran and Sun [40] performed a reverse analysis of a typical RFIC and created a parametric RFF distribution model, together with a blind source separation filter to eliminate the channel effects including multipath fading.

As to the construction of mathematical models, it is worth noting that nonparametric methods often bring the possibility of overfitting, while the validity of parametric models relies on expert knowledge. Furthermore, how to maintain the generalizability of mathematical models under different communication protocols is also an urgent issue to be addressed.

4 RFF feature extraction

At present, the prevailing RFF feature extraction methods can be roughly divided into three categories, namely I/Q signal-based, parameter-based, and transformation-based feature extraction, where different methods rely on different degrees of prior information and expert knowledge. A brief comparison of these three feature extraction methods is presented in Table 1.

4.1 I/Q signal-based RFF feature extraction

The I/Q signal inherently contains many RFF features that can reflect the hardware characteristics, such as the shape of signal envelopes. Therefore, the envelope derived from the transient part of the I/Q signal can be used as RFF [41–44]. However, this method is extremely sensitive to the device position and antenna polarization direction [45].

Moreover, the statistical characteristics of I/Q signals can be used as RFF, with the representative method named RF-DNA (Distinctive Native Attributive) [16, 46–49], which extracts instantaneous amplitude, phase, and frequency responses from the I/Q signal, and calculates variance, skewness, and kurtosis using these corresponding response sequences.

With the improvement of classification algorithms, some researchers directly utilize the preprocessed I/Q signals as RFF [50–53] and then accomplish device identification using machine learning algorithms. It is worth noting that special structures of I/Q signals have been favored by researchers, such as preamble [20, 23, 31]. These structures contain the same content under identical standards and are suitable for extracting RFF features because they can avoid the effects of modulation methods. As illustrated in Figure 5, with respect to different ZigBee devices, the preambles of in-phase signals have distinct characteristic differences, and thus can be used as RFF. In fact, methods that directly use I/Q signals as RFF are less dependent on prior information and expert knowledge, and the ones without requirements of complex preprocessing are suitable for more application scenarios because of their end-to-end characteristics.

4.2 Parameter-based RFF feature extraction

The parameter-based RFF features mainly refer to the basic parameters such as I/Q imbalance [54], sampling frequency offset (SFO) [55], carrier frequency offset (CFO) [47, 56, 57], *etc.* which reflect the

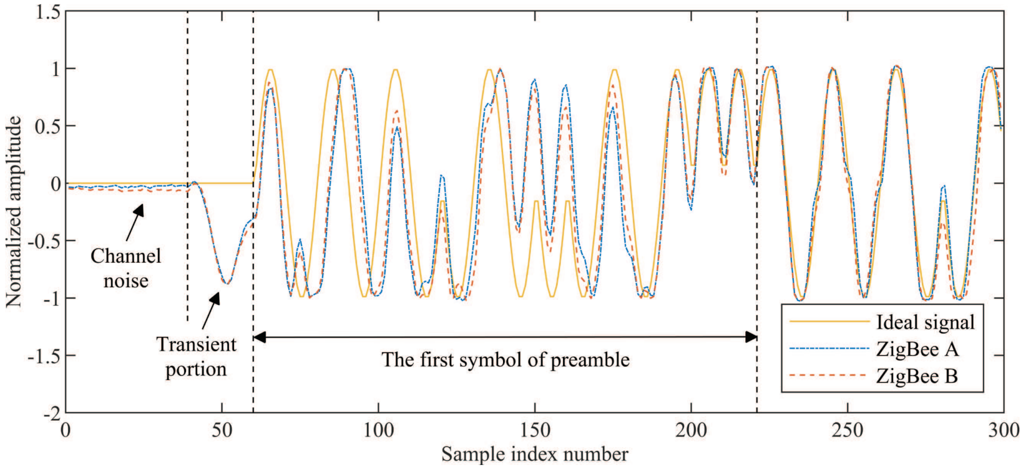

Figure 5. Comparison of in-phase signals from different ZigBee devices

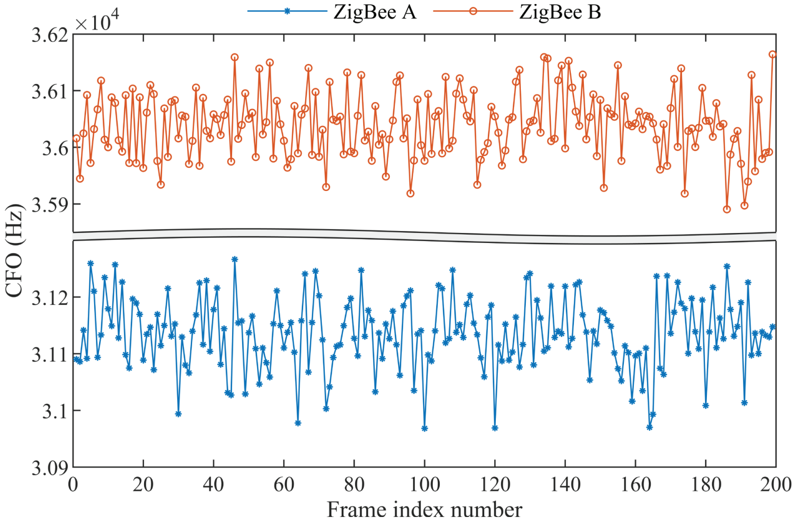

Figure 6. Comparison of CFOs from different ZigBee devices

effects of various non-ideal characteristics of devices on modulated signals. These parameters represent characteristics of the signal in the time domain or frequency domain, which are commonly found in various signal processing procedures. Figure 6 chooses CFO as an example of parameter-based RFFs, where CFOs from different ZigBee devices oscillate in their respective small ranges within a short period of time. It should be noted that the parameter-based methods rely on manual selection and accurate estimation of representative parameters, and the extraction process is highly dependent on prior information of the signal as well as expert knowledge, thus suffering from various limitations in the application.

4.3 Transformation-based RFF feature extraction

Besides the above methods, researchers have also used various feature transformation methods to extract RFFs from the received signal, such as short-time Fourier transform (STFT) [24, 26, 58, 59], discrete wavelet transform (DWT) [28, 41], bi-spectrum transform [59, 60], Hilbert-Huang transform (HHT) [61, 62], *etc.* Among them, time-frequency domain analysis methods like STFT and DWT are commonly used to obtain the RFFs of non-stationary signals, while the bi-spectrum analysis can be employed to extract RFFs with non-Gaussian distribution. Additionally, for steady-state signals, the shape of the constellation diagram is preferred by researchers for its visualization of modulation errors (*e.g.*, I/Q offset, frequency offset, and amplifier nonlinearity). In 2008, Brik *et al.* [54] accomplished the definition for

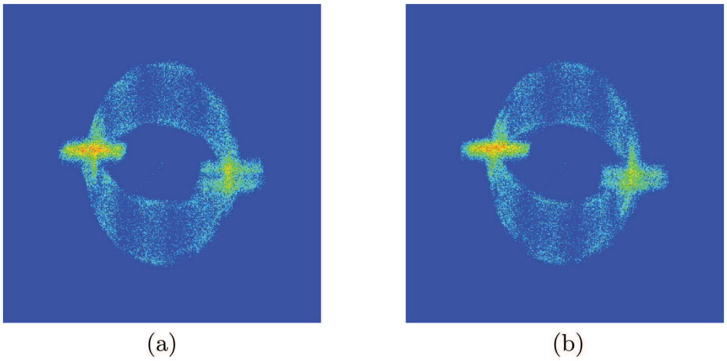

Figure 7. Comparison of DCTFs from different ZigBee devices. (a) DCTF of ZigBee A. (b) DCTF of ZigBee B

different types of modulation errors using the characteristics of the scatter distribution on the constellation diagram and proposed the RFF based on modulation errors. In 2016, Peng *et al.* [63, 64] proposed a feature transformation method named differential constellation trace figure (DCTF). In 2022, the authors in [65] proposed a heat constellation trace figure (HCTF), which further mined the information carried in the constellation diagram from the perspective of distribution density. Figure 7 shows DCTF as an example of transformation-based RFFs, where the DCTFs from ZigBee A and B show different clustering patterns.

Compared to parameter-based RFF feature extraction methods, some feature transformation methods, such as STFT and DCTF, do not require prior information on the signal and are therefore more widely applicable. However, at the same time, these methods still rely on expert knowledge to set some of the parameters and thus are not adequate for some practical scenarios such as end-to-end.

5 Further processing

Further processing is an optional step that directly serves the RFF identification by transforming the extracted RFF features into suitable forms for machine learning classifiers. In contrast to the step of RFF feature extraction which relies on various signal processing methods, further processing always relies on methods such as feature fusion and feature dimension reduction which relatively lack physical meaning but simultaneously have the possibility to enhance the representation capability of features.

5.1 Feature fusion

Feature fusion aims to combine different kinds of RFFs with each other to improve the effectiveness as well as generalization ability. For example, Peng *et al.* [27] obtained more stable and higher classification accuracy by combining four feature parameters, namely DCTF, CFO, modulation offset, and I/Q offset, compared to the method using individual parameters as RFFs. Liu *et al.* [59] proposed an RFF recognition scheme that fused four kinds of signal representation into a four-channel image and fed it into a neural network. These features were respectively obtained by employing HHT, STFT, ambiguity function, and bi-spectrum transform. The experimental results validated the effectiveness of the proposed feature fusion method.

5.2 Feature dimension reduction

Feature dimension reduction (FDR) is intended to cope with the problem that a poor classification result may be obtained when classifiers are fed with features that have high dimensional characteristics or low representation capability. Inspired by Ray *et al.* [66], this paper categorizes the FDR methods adopted in RFF identification into two classes, namely Feature Selection Algorithm (FSA) and Feature Extraction Algorithm (FEA).

Table 2. Comparison of different FSA methods

Methods	Description	Classifier dependency	Computational cost	Applicable scenarios	Challenges
Filter	Complete feature selection based on evaluation function before classification.	Independent	Low	High-dimensional datasets and data preprocessing	No guarantee to find the optimal subset.
Wrapper	Select the optimal feature subset based on training results of classifier.	Dependent	High	Not applicable to high-dimensional datasets	Poor generalization ability and long computation time.
Embedded	Integrate the feature selection and model training.	Dependent	Low	High-dimensional datasets	Possibility of overfitting.

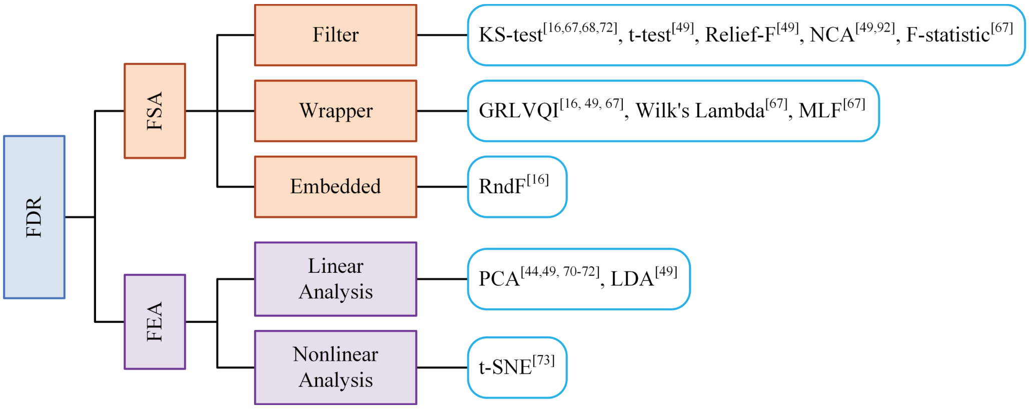
FDR
FSA
FEA
Filter
Wrapper
Embedded
Linear Analysis
Nonlinear Analysis
KS-test[16,67,68,72], t-test[49], Relief-F[49], NCA[49,92], F-statistic[67]
GRLVQI[16, 49, 67], Wilk's Lambda[67], MLF[67]
RndF[16]
PCA[44,49, 70-72], LDA[49]
t-SNE[73]

Figure 8. Brief hierarchy of FSA methods

5.2.1 Feature Selection Algorithm

Feature Selection Algorithm (FSA) is aimed at selecting the optimal feature subset by eradicating the irrelevant features from the original dataset without any data transformation. Furthermore, FSA can be classified into three categories, namely filter, wrapper, and embedded methods.

- Filter methods perform feature selection before classification, which often employs parameters such as distance, mutual information, and correlation coefficient as discrimination criteria to filter out features with strong relevance to the category.
- Wrapper methods rely on the learning results of the classifier to select feature subsets and discriminate the importance of features based on classification performance.
- Embedded methods integrate the feature selection process with the model training process, which often complete the feature selection while training discriminative model such as SVM, tree/forest-based model.

Table 2 briefly summarizes and compares these three methods. It should be noted that due to the relationship between the rationale for feature selection and the classifier training results, filter methods and wrapper methods were also referred to as pre-classification dimensional reduction analysis and post-classification feature ranking [67].

Various FSA methods have been employed in RFF identification. Dubendorfer *et al.* [68] accomplished dimension reduction of RFF features for ZigBee signals using KS (Kolmogorov–Smirnoff)-test and Generalized Relevance Learning Vector Quantization Improved (GRLVQI) relevance ranking. Bihl *et al.* [67] proposed a dimension reduction method named MDA Loadings Fusion (MLF) to enhance RFF identification accuracy. Reising *et al.* [49] employed Relief-F for feature dimension reduction to identify RFFs from WiMAX devices. A brief hierarchy of FSA is demonstrated in Figure 8.

Table 3. Comparison of closed set RFF identification mechanisms

Mechanisms	Classifier	Against non-ideal environment	Against large-scale identification	Classification accuracy
TML-based	Simple[a]	Most rely on preprocessing	Applicable to tens of devices	Low[b]
DL-based	Complex[c]	Most rely on neural network design	Applicable to more than 10 000 devices	High

Note: [a]Most are TML-based classifiers. [b]Well-designed RFF features may perform better than some of the DL-based methods. [c]Both TML and DL algorithms are applicable as classifiers.

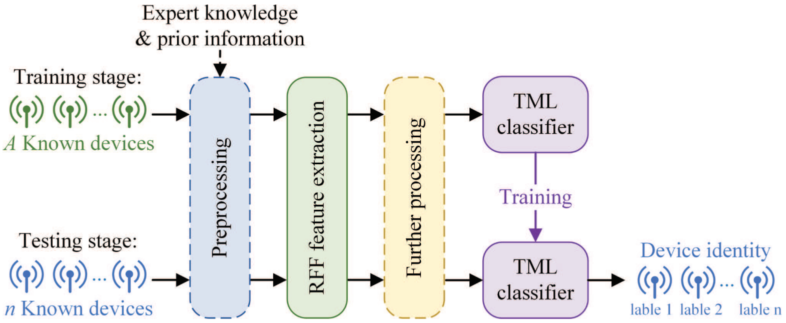

Figure 9. Pipeline of traditional machine learning-based closed set RFF identification. Note that although the devices in training and testing datasets are always the same, signals of known devices used during testing should be sampled later than those used during training. Therefore devices are illustrated with different colors. Besides, here $n \leq A$

5.2.2 Feature Extraction Algorithm

Feature Extraction Algorithm (FEA) is essentially the transformation of data [69], which can be further classified as linear analysis methods such as PCA [44, 49, 70–72] and LDA [49], as well as nonlinear analysis methods such as *t*-SNE [73]. It should be noted that since *t*-SNE does not learn a specific function from the original space to the new dimensional space, it is generally used for visualization rather than in classification models.

5.2.3 Comparison analysis

From a general standpoint, both FEA and FSA can improve the learning efficiency of the discriminative model. However, since FEA involves the transformation of the feature space, some original RFF features are inevitably converted into new features with the possible omission of useful information, which can also trigger the problem of overfitting. Compared with FEA, FSA simplifies the model while providing greater interpretability, and often results in higher identification accuracy [49, 66].

It is worth mentioning that although the FEA method is inferior to FSA in most cases, FEA still has the unique advantage of simplifying the signal processing steps and enhancing the effectiveness of machine learning classifiers, and thus remains valuable for research.

In the field of RFF identification, several studies have been performed to compare various methods belonging to FSA and FEA [16, 49, 67, 68]. Bihl *et al.* [67] performed a comparison of 5 FSA methods, namely KS-test and F-statistic which belong to the filter method, along with Wilk's Lambda, GRLVQI and the proposed MLF which belong to the wrapper method. Reising *et al.* [49] not only took GRLVQI, NCA, POEACC, BC, *t*-test, and Relief-F which belong to FSA into consideration but also compared the performance of LDA and PCA which belong to FEA, extending the categories of feature dimension reduction methods to a number of 8. These two papers compared and analyzed the performance of different FDR methods in the task of identifying ZigBee and WiMAX devices, respectively, where the F-statistic and MLF in [67], as well as the Relief-F in [49], achieved the best result in respective experiments. It should be noted that Relief-F is one of the most advanced feature dimension reduction algorithms by accomplishing feature selection through the computation of feature weight vectors and the solution of a convex optimization problem, and is more effective than any wrapper method [66].

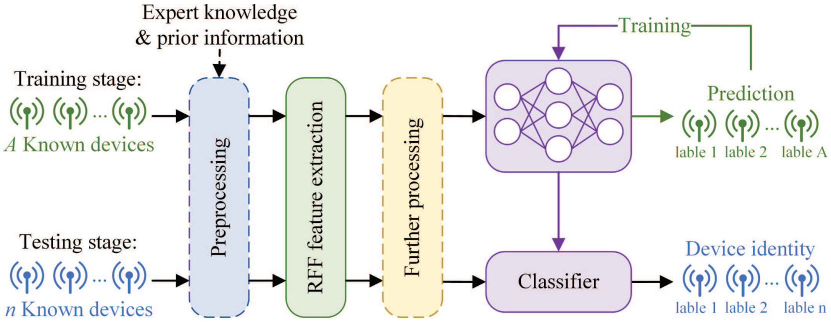

Figure 10. Pipeline of deep learning-based closed set RFF identification

6 Closed set RFF identification

In the closed set environment, RFF identification can be summarized as a classification task for known devices, and classification accuracy is a direct criterion to evaluate the effectiveness of the identification method. Therefore, how to establish a suitable classifier to complete the classification task is the key research point. According to the construction method of classifier, the approaches of closed set RFF identification can be divided into two branches based on traditional machine learning (TML) and deep learning (DL), and a brief comparison of these two approaches is presented in Table 3. Moreover, data augmentation has been successfully implemented in closed set RFF identification, which has been proven effective in several studies.

6.1 Traditional machine learning-based closed set RFF identification

The pipeline of TML-based closed set RFF identification is demonstrated in Figure 9. Generally, the classification accuracy obtained by the closed set identification method based on TML is highly dependent on the validity of features. Therefore, in some cases, further processing such as feature fusion [27] and feature dimension reduction [44, 49, 70, 71] have been applied to the RFFs obtained from the feature extraction step to further enhance the representation capability of them.

In the face of well-processed RFF features, the main part of TML-based RFF identification lies in the classifier design. TML-based methods often utilize simple machine-learning algorithms for classification tasks. Cobb *et al.* [74] employed a linear Bayesian classifier and completed the classification of 40 16-bit PIC24F micro-controllers with unintentional RF emissions. Lin *et al.* [44] compared four machine learning classifiers, namely Random Forest (RndF), Support Vector Machine (SVM), Artificial Neural Network (ANN), and Grey Relational Analysis (GRA), to accomplish a closed set classification task for 10 Motorola walkie-talkies. Additionally, machine learning algorithms such as K-Nearest Neighbor (KNN) [75] and Multiple Discriminant Analysis (MDA) [76] are commonly used to construct classifiers for closed set RFF identification.

6.2 Deep learning-based closed set RFF identification

In recent years, the development and application of DL-based methods have injected new vitality into the research of RFF identification. DL-based RFF identification methods significantly rely on the construction of neural networks. For one thing, neural networks that contain structures such as fully connected layers, as well as softmax activation functions, can be inherently employed as classifiers. For another thing, with regard to the features obtained from the previous RFF extraction and further processing step, latent features with effectiveness can be learned by a well-designed neural network. To be specific, the function of neural networks can be seen as automatic feature representation and classification, where the high-dimensional output from a hidden layer of the trained network is treated as latent feature representation and then fed into the last several layers for device identification. Besides, it is worth noting that as to the deep latent features obtained from the hidden layer, TML algorithms can also be used to construct the final classifier [65]. In summary, a pipeline of DL-based closed set RFF identification is presented in Figure 10.

Notably, DL-based methods are capable of reducing pressure on feature design in the previous steps, where the information loss due to manual screening and signal processing such as traditional compensation of frequency and phase offset can be avoided [23]. In fact, since advanced neural networks models such as CNN, RNN, Transformer, and corresponding variants such as ResNet [77] and LSTM [78], have been widely used in closed set RFF identification, these DL-based methods tend to achieve higher classification accuracy compared to TML-based methods, maintaining performance stability under severe experimental conditions such as non-ideal environments (*e.g.*, environments with low SNR and channel variations) and large-scale device identification.

6.2.1 Non-ideal environment

In Sections 3.2 and 3.3, several approaches to eliminating the effect of noise and channel on RFF identification have been presented, and similar results can be obtained based on DL methods. A brief comparison of these two approaches to overcoming identification problems under a non-ideal environment is given in Table 4. In fact, neither preprocessing nor DL-based methods in existing research can completely eliminate the influence of a non-ideal environment on identification results, therefore they can be used as a complement to each other in practice. Additionally, data augmentation is another supplementary measure to improve identification accuracy under a non-ideal environment, which will be discussed in Section 6.3.

Yu *et al.* [79] proposed a specially structured CNN that uses signals with different sampling rates as input to the neural network in order to obtain short-term features in signals with high sampling rates and long-term features in signals with low sampling rates, obtaining a classification accuracy of 78.2% in LOS scenario for 54 ZigBee devices at 10 dB SNR. Reus-Muns *et al.* [51] introduced triplet loss into a CNN with four convolutional layers and obtained a classification accuracy of about 93% when tested with a dataset collected on a different day than the training dataset, to some extent reducing the effect of channel variations on the identification results. Agadakos *et al.* [58] proposed a recurrent complex-valued neural network and achieved an accuracy close to 100% for a classification task of 100 classes of ADS-B signals at 2 dB SNR. Liu *et al.* [59] successfully applied feature fusion in a DL-based RFF identification scheme. They transformed the ADS-B signal into a four-channel image and extracted the RFF from it using CNN. For 10 transmitters to be classified, an accuracy of about 90% was obtained at an SNR of 0 dB. Wu *et al.* [80] proposed a neural network called DSLN based on the ResNet structure, where the activation function was designed based on a dynamic threshold to set the near-zero features to zero and preserve the negative features in order to obtain a higher classification accuracy under low SNR scenarios. In comparison with traditional CNN and RNN, the proposed DSLN yielded accuracy improvement of 10% and 20% respectively, while reducing the running time by up to 60%. Zhang *et al.* [81] proposed a scattering network that combined the fractional wavelet scattering transform and the structure of ResNet, obtaining a classification accuracy of 99.5% for LTE signals collected from 15 mobile phones at different dates and channel states. Inspired by ensemble learning, Peng *et al.* [65] employed Inception V3 to obtain RFFs from multiple signal slices and adopted CNN as a classifier based on the strategies such as majority voting and weighted averaging, which achieved classification accuracy of 91.07% and 99.88% for 7 devices at 0 dB and 5 dB SNR, respectively.

6.2.2 Large-scale device identification

The above cutting-edge research achievements demonstrate the effectiveness of DL-based methods in the closed set RFF identification problem, especially the robustness under a non-ideal environment. However, in practical application scenarios, the number of devices to be classified is also an essential factor that influences DL-based RFF identification.

In contrast to TML-based methods which are often employed for identification problems involving tens of devices, DL-based methods are capable of accomplishing classification tasks when faced with hundreds [37, 58, 80, 83] or even 10 000 [34, 84] devices. Restuccia *et al.* [37] accomplished a closed set classification task for 100 WiFi devices using a CNN with 8 convolutional and 4 fully connected layers and improved the accuracy by 27% compared to the TML-based method proposed by Vo *et al.* [55]. Al-Shawabka *et al.* [83]

Table 4. Brief comparison of methods for addressing non-ideal environment

Methods	Explainability	Resource consumption	Challenges
Preprocessing	Strong	Low	Possibility of losing useful feature information.
Deep learning	Weak[a]	High (computing resources)	High requirements for neural network design.
Data augmentation	Median	High (storage resources)	Some methods rely on known ideal signal.

Note: [a] Due to the lack of interpretability [82] of neural networks.

employed CNN with one-dimension convolutional layers and CNN with two-dimension convolutional layers, obtaining classification accuracy of 99% and 97% for 100 LoRa devices, respectively.

However, as the number of devices increased further, neural networks with simple structures become unable to provide sufficiently descriptive power. Soltani *et al.* [85] adopted CNN with 10 one-dimension convolutional layers to explore the task of classifying WiFi devices under channel variations, where the classification accuracy decreased from nearly 80% to less than 20% when the number of devices increased from 50 to 5000. Agadakos *et al.* [58] proposed a simple complex-valued CNN named CDCN and a model named RDCN which combined LSTM and CNN. They explored the effect of the number of devices on the classification accuracy using an equal mix of data from both the WiFi and ADS-B datasets, with the experimental results demonstrating that RDCN achieved a precision of 82% for 100 devices while 72% and 62% for 500 and 1000 classes respectively when the accuracy achieved by CDCN dropped from 73% to about 52%. Additionally, they tested the performance of real-valued CNN and observed a rapid decline, which indicated that real-valued neural networks are more difficult to cope with large-scale device identification compared to complex-valued neural networks when adopting I/Q sample-based RFF.

To improve the accuracy of DL-based RFF identification methods in large-scale device classification tasks, there is a way to increase the depth of the network and utilize very complex structures to learn RFF features. Robinson *et al.* [84] used signals from the RFMLS dataset [86], and proposed an augmented dilated causal convolution (ADCC) network which combined a stack of dilated causal convolution layers with traditional convolutional layers, accomplishing the classification of large-scale devices with the population ranging from 100 to 10 000. With the same dataset, a neural network containing 50 layers called ResNet-50-1D was proposed in [34], which accomplished the classification for 10 000 devices. The dataset was equally split between WiFi and ADS-B, and the experimental results demonstrated that for the ADS-B dataset, ResNet-50-1D obtained 77% and 90% accuracy over 5000 and 500 devices, while for the WiFi dataset obtained only 26% and 61% accuracy, respectively. It should be noted that the relationship between classification accuracy and the population of devices depends on the complex influence of neural network structure, RFF characteristics, and other factors, which makes it difficult to summarize a universal law. For example, when the population of devices exceeds 100, interestingly, the classification performance is linear in the logarithm of the device population in [84], while [34, 58] only present a nonlinear relationship.

In summary, there are two challenges faced by DL-based large-scale device identification: (1) The increase in computational complexity brings greater resource consumption. (2) Existing research still cannot guarantee high classification accuracy when the number of devices is significantly large. To address these challenges, more effective RFF features and new advanced neural networks are promising solutions. Besides, for the advancement of research in this area, new open source large-scale datasets are necessary.

6.3 Data augmentation in closed set RFF identification

In the training stage of neural networks, the lack of training samples would increase the possibility of overfitting. Meanwhile, RFF features are highly susceptible to noise, multipath interference, and other complex factors, which can be reflected in the inconsistent distribution of training and testing samples, thus reducing the robustness of the neural network model and eventually leading to the degradation of classification accuracy. To address the problems above, increasing the number of samples in the RFF dataset is an effective solution. However, in practical application scenarios, it is difficult and costly to collect large-scale signal data. In this case, data augmentation is likely to be an effective solution.

The data augmentation method can effectively alleviate the problem of lacking training samples at a relatively low cost, meanwhile, it can simulate the effects of noise, CFO shifts, channel variations, multipath effects, and other complex factors on the RFF features, improving the robustness of the identification model. Soltani *et al.* [85] added white Gaussian noise to the training samples to simulate the received signals with different SNRs, aiming to enhance the robustness of the neural network model against noise. They also simulated different channel effects using multi-tap FIR filters and passed the training samples through filters with different parameter settings. The experimental results demonstrated that for 50 to 5000 WiFi transmitters, the data augmentation improved the classification accuracy by up to 51%. Al-Shawabka *et al.* [83] generated a wide variety of International Telecommunication Union (ITU) standard multipath channels and employed them as FIR filter taps, then accomplished the data augmentation with signals acquired under ideal conditions. In the classification task of 100 LoRa devices, the data augmentation improved the accuracy from 82% to 91% when the training set and test set were collected on the same day. However, when the training set and test set were collected on different days, it only improved the accuracy from 19% to 36%, which indicated that the data augmentation is ineffective in the face of significant channel variations. Cekic *et al.* [19] accomplished data augmentation using randomly generated CFOs and wireless channels, and obtained higher classification accuracy by employing it in conjunction with CFO compensation, inspiring us to combine data augmentation with preprocessing methods in closed set RFF identification. Shen *et al.* [24] described multipath and Doppler shift utilizing power delay profile and Doppler spectrum, respectively, based on which the construction of different channel parameters was accomplished and the signals were passed through these channels for data augmentation. In the classification task of 30 LoRa devices, the data augmentation improved the classification accuracy from about 98% to almost 100% in the static indoor scenario with a multipath effect. Moreover, in high-speed mobile scenarios, the proposed data augmentation improved the classification accuracy significantly as the Doppler shift increased, from 68.6% to more than 80% when the Doppler shift was 100 Hz compared to the data augmentation method without considering the Doppler effect.

The above data augmentation methods can be summarized as the same process, where the factors that need to be mitigated are first modeled and analyzed, and random variables are then designed to simulate more RFFs affected by different target factors. The scheme is cost-effective and can enable the neural network to learn more information, thus enhancing the generalization ability and robustness of the network model. However, it should be noted that some of the data augmentation methods rely on conditions where the ideal received signal is known [24, 85], therefore lacking generalizability in practical applications. Besides, generative models such as GAN and Autoencoder can be performed for data augmentation, which will be demonstrated in Section 7.4.

7 Open set RFF identification

Compared with a closed set environment, an open set environment is closer to the practical application scenario, where signal samples from unknown devices are introduced during the testing stage of RFF identification. These samples not only come from transmitters without access authority but also come from spoofing attacks with malicious intent. Therefore, accurately detecting unknown devices is a key research point to ensure the security of the RFF identification scheme. This section will focus on the open set problems of RFF identification, thoroughly investigate the relevant research achievements and provide brief summary and prospect.

7.1 Overview of open set RFF identification

The existing open set RFF identification methods can be summarized into three categories, which are traditional machine learning (TML)-based methods, deep learning (DL)-based methods, and generative model (GM)-based methods. Figure 11 presents an overview of open set RFF identification, where the important elements of each method, namely feature engineering, classifier design, and model selection, are summarized and demonstrated.

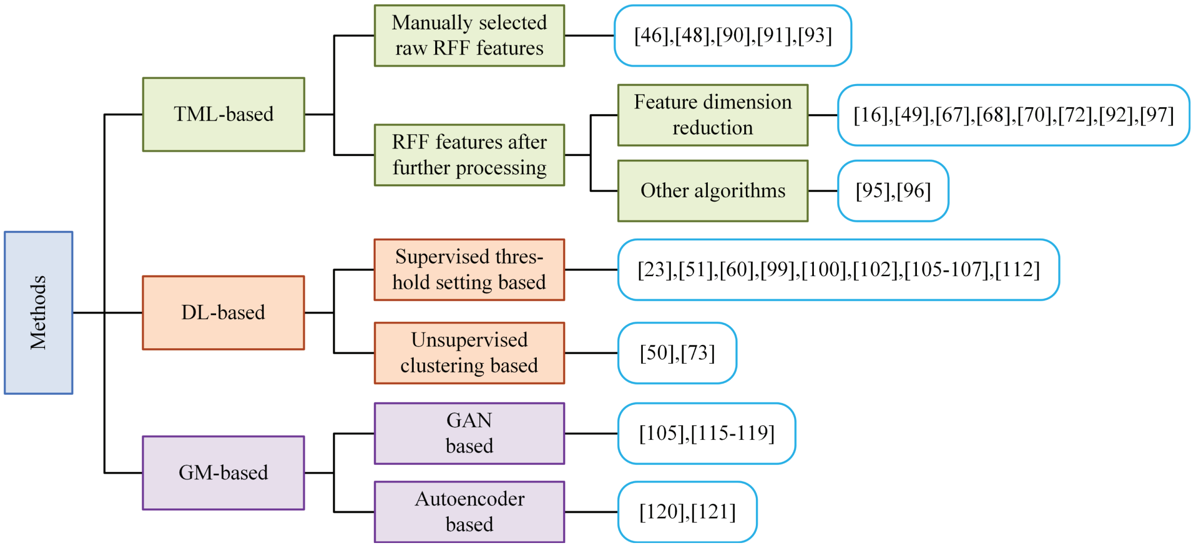

Figure 11. Overview of open set RFF identification methods

TML-based methods emphasize the category selection and further processing of the features obtained in the RFF extraction step, as well as the utilization of a simple machine learning classifier to complete the open set identification. DL-based methods, however, focus on the construction of classifiers based on DL, adopting advanced algorithms for the purpose of detecting unknown devices. GM-based methods, in turn, employ methods such as Generative Adversarial Network (GAN) and Autoencoder to generate additional signal samples and complete data augmentation with the objective of improving the accuracy of open set identification.

It is worth mentioning that the non-ideal environment discussed in Section 6.2.1, as well as the large-scale device identification scenario discussed in Section 6.2.2, are also the research points in open set problems. However, there are still research gaps in these points and there is a lack of feasibility verification to directly transfer existing methods applied in closed set problems to open set problems, therefore this section does not contain related contents, which also include traditional data augmentation methods discussed in Section 6.3.

7.2 Traditional machine learning-based open set RFF identification

7.2.1 Feature design

Traditional machine learning (TML)-based methods for open set RFF identification always rely on the validity and generalization ability of the extracted RFF features. The validity mainly refers to the capability of accurately reflecting the difference between various devices, while the generalization ability refers to the extensive existence of distinctions between different devices, even if the environmental conditions or communication protocols change. Therefore, the selection of RFF features and further processing methods are key elements of the research on TML-based open set RFF identification. A brief pipeline is illustrated in Figure 12.

Hall *et al.* [41] employed the envelope characteristics of the transient signals to accomplish the detection of unauthorized Bluetooth devices, which obtained a detection rate of 93% under the condition of a 5% false alarm rate. Chouchane *et al.* [87] theoretically combined the wavelet-based RFFs with the previously proposed CODERA [88] to accomplish the detection of illegal base stations. Dubendorfer *et al.* [46] completed open set identification for 7 known and 2 unknown ZigBee devices using the prevailing RF-DNA as RFF. Although the application scenarios of these researches are relatively simple, they pioneered the path for TML-based open set RFF identification.

In recent years, several RFF features with high validity and generalization ability have been discovered and applied to open set problems. Talbot *et al.* [48] conducted experiments to compare the effectiveness of time domain (TD) based RFF and Slope-Based Frequency Shift Keyed (SB-FSK) based RFF, where two

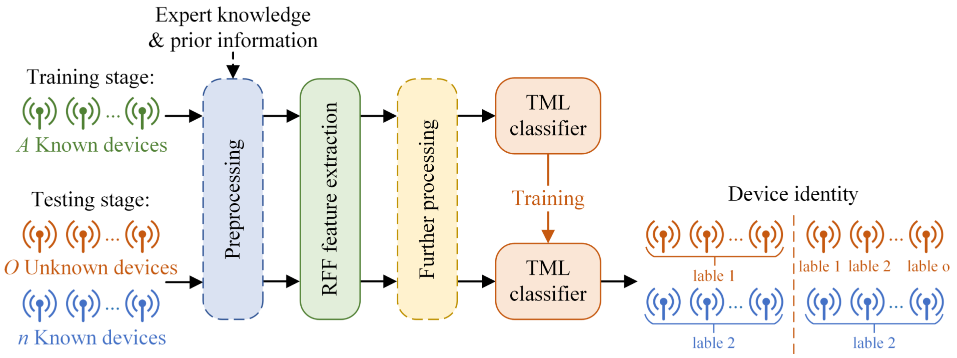

Figure 12. Pipeline of traditional machine learning-based open set RFF identification. Note that unknown devices can be classified into one class or o classes (determined by the classifier design). Here o and O are not always equal (determined by the prior information of unknown device population and classifier design). Besides, the classification of known devices is a closed set problem, therefore these devices only receive one label in this pipeline, which means that they are distinguished from unknown devices

kinds of commercial communication devices were involved in the open set problem. In the experiment, the SB-FSK-based RFF demonstrated stronger computational efficiency due to the lower feature dimension, based on which a detection rate of 94.9% was obtained as to the open set problem including 4 known and 2 unknown devices. Inspired by the studies of Rondeau *et al.* [89] and Peng *et al.* [27], Rondeau *et al.* [90] employed constellation-based RFF to accomplish open set identification for Wireless HART adapters. Wang *et al.* [91] used the SNR traces obtained from the sector level sweep (SLS) process as RFF, accomplishing open set identification for mmWave 60-GHz IEEE 802.11ad devices, with an unknown device detection rate up to 99% when false alarm rate was less than 1% under NLOS scenario with a 3-meter distance between transmitter and receiver.

From the research above, it is evident that the TML-based open set RFF identification is highly dependent on expert knowledge as well as prior information, and the detection performance is associated with the dimension of feature space [36]. For one thing, RFFs based on low-dimensional features are often incapable of accurately characterizing the difference between known and unknown devices, so there are limitations on the number of transmitters and the type of signal. For another thing, RFFs based on high-dimensional features tend to bring high computational complexity, which does not always lead to satisfactory identification results in the case of limited computational and storage resources [48]. Therefore, as a further processing method, feature dimension reduction is recommended in this research field [49, 67]. Bihl *et al.* [67] proposed a dimension reduction method named MDA Loadings Fusion (MLF), achieving a 97.2% detection rate of unknown devices with a TPR of 100% when there were 4 known and 9 unknown ZigBee devices. Reising *et al.* [49] employed Relief-F for feature dimension reduction and obtained a 90% detection rate at 3 dB SNR for 6 known and 12 unknown WiMAX devices.

7.2.2 Classifier design

TML-based open set RFF identification mainly relies on threshold setting to detect unknown devices, which is often a one-*vs*-one verification process, *i.e.*, a binary classification is completed for each device to be identified. Popular machine learning classifiers include MDA/ML [16, 46, 68, 90], KNN [70, 72], SVM [49, 91], SVDD [92], RndF [16, 93], *etc.* These machine learning methods either have special variants (*e.g.*, one-class SVM, isolation forest) or rely on clustering (*e.g.*, KNN) to adapt to the requirements of unknown device detection. It should be noted that machine learning methods based on clustering mechanisms are inherently adaptable to application scenarios where new devices are constantly registered, and even have the possibility to accomplish incremental learning, due to their compatibility with newly added samples.

Cobb *et al.* [74] proposed an identification scheme based on MDA and linear Bayesian classifier with RF-DNA as fingerprint, where the fingerprints of devices to be identified were compared with that of authorized devices according to the claimed identity. The whole process was referred to as one-*vs*-one verification. Furthermore, Reising *et al.* [94] highlighted the effectiveness of one-*vs*-one verification, and proposed an identification scheme for WiMAX signals based on MDA/ML. Although these two papers did not discuss in detail the impact brought by unknown devices on RFF identification, the MDA-based classifier and the proposed one-*vs*-one verification scheme laid the foundation for the research on open set problems in the following years.

Inspired by Reising *et al.* [94], Dubendorfer *et al.* [46] employed MDA/ML and a one-*vs*-one verification scheme to accomplish the open set identification of 7 known and 2 unknown ZigBee devices, where a detection rate of 90% was obtained at 10 dB SNR. However, the experimental results also presented low detection rates for individual unknown devices, which indicated that the generalization ability of RFF features is of significant importance. Therefore, Dubendorfer *et al.* [68] introduced feature dimension reduction and accomplished the open set identification task for ZigBee devices utilizing MDA/ML. The combination of MDA/ML, feature dimension reduction, and one-*vs*-one verification scheme established an early framework of TML-based open set RFF identification. In recent years, the classifier for open set problems based on MDA/ML has been improved with methodology iterations. Rondeau *et al.* [90] combined multivariate normal probability density function with MDA/ML, achieving performance beyond the traditional Euclidean distance-based unknown device detection approach, where unknown device detection rates ranged from 83.4% to 99.9% were obtained in the face of 6 known and 2 unknown WirelessHART adapters.

Apart from MDA/ML, several TML-based methods have been researched in early studies. Patel *et al.* [93] employed RndF as a classifier and tested the unknown device detection rate when receiving signals with a high-end receiver (NI PXIe-1085 system) and a low-end receiver (NI USRP-2921) from 3 known and 3 unknown ZigBee devices, achieving results of 67.11% and 57.11%, respectively. The authors in [16] pointed out that statistical analysis methods such as MDA rely on the assumption of Gaussian distribution compliance of feature parameters, while multipath conditions in practical scenarios and interference from other devices often result in received signals that do not strictly obey Gaussian distribution, thus leading to a decrease in the effectiveness of MDA/ML methods. To solve this problem, they introduced an integrated classifier constructed based on nonparametric RndF and Multi-Class AdaBoost (MCA), and compared this method with the parametric-based MDA/ML method and GRLVQI classifier-based method. In the experiment, there were 36 scenarios where 4 known and 9 unknown ZigBee devices were randomly chosen, and the RndF, MDA/ML, and GRLVQI methods obtained a TPR $\geq$ 90% and an FPR $\leq$ 10% in 31, 20, and 25 scenarios, respectively.

Since 2019, more and more TML-based methods have been applied to open set RFF identification. Tian *et al.* [70] applied RFF technology to the Industrial Internet of Things (IIoT) and accomplished open set identification for 8 known and 2 unknown devices using KNN, obtaining close to 100% detection rate of unknown devices at 10 dB SNR. The authors in [92] employed the classical one-class classifier Support Vector Data Description (SVDD) and achieved a detection rate of 90% in the case of 8 known devices and 2 unknown devices at an SNR of 15 dB. Kokalj-Filipovic *et al.* [95] proposed an algorithm named Deep-delay Loop Reservoir Computing (DLR), based on which the classification of 10 known WiFi transmitters was completed, followed by transfer of parameters to Multilayer Perceptron (MLP) and using the softmax value as a criterion to detect unknown devices, obtaining more than 99% detection rate with the addition of 10 unknown devices and keeping the false alarm rate less than 1%. Medaiyese *et al.* [96] proposed a semi-supervised learning method based on the Local Outlier Factor (LOF) algorithm, which was able to detect UAV signals from Bluetooth signals and WiFi signals with an accuracy of 96.7% at 30 dB SNR. Inspired by research on face recognition, Zhou *et al.* [97] applied the Gaussian Probabilistic Linear Discriminant Analysis (GPLDA) to the open set RFF identification, with an equal error rate (EER) of only 0.63% in an experimental scenario involving 6 known and 6 unknown ZigBee devices.

7.3 Deep learning-based open set RFF identification

In Section 6.2, the application of deep learning (DL)-based methods to the closed set RFF identification is demonstrated, where the DL-based methods tend to achieve higher classification accuracy in comparison to TML-based methods. However, when samples of unknown devices are added to the test set, classical neural networks based on cross-entropy loss as well as softmax activation function always misclassify the tested sample to a known device with the highest probability [98]. Therefore, the innovation of neural network-based classifiers is of great importance in order to address open set problems. A brief pipeline is presented in Figure 13.

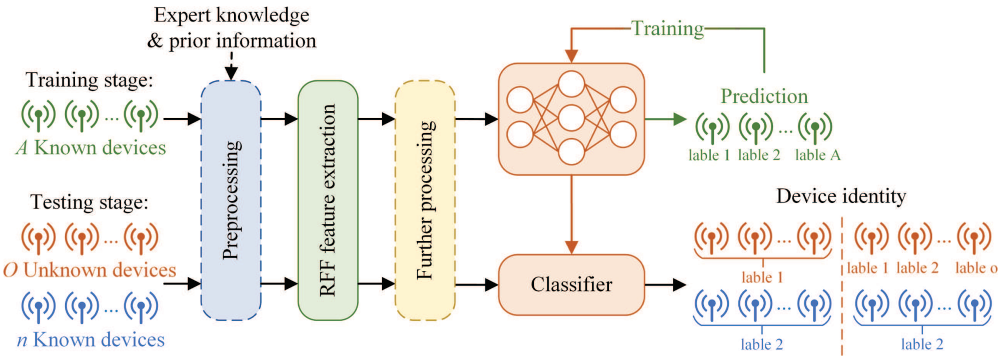

Figure 13. Pipeline of deep learning-based open set RFF identification

7.3.1 Classifier design and case studies

Hanna *et al.* explored different structures of neural network classifiers for the open set problem in 2020 [99] and 2021 [100], respectively. They replaced the original classification layer of ResNet with One *vs* All (OvA) or OpenMax classifier and performed the open set identification using I/Q samples of WiFi signals. The OvA method constructs binary classifiers for every legal device, performing one-*vs*-one verification for unknown signal samples, while OpenMax is a classical method for solving the open set problem [101], where a separate category is added to the output as a representation of negative samples.

The above method is based on the threshold setting to determine whether the target sample belongs to a known device or an unknown device, but it cannot directly determine the number of unknown devices classes. For this problem, Wong *et al.* [50] proposed a semi-supervised learning method that combined supervised RFF extraction with unsupervised clustering for the purpose of detecting unknown devices. In the experiment, I/Q signal-based RFF was further processed by CNN, and Density-Based Spatial Clustering of Applications with Noise (DBSCAN) was employed to perform the clustering, reaching an adjusted mutual information (AMI) of more than 0.8, and the determination of 24 existing devices in the case of 15 known and 15 unknown USRP devices.

Based on the research above, we can summarize the classifier design of open set RFF identification based on DL, which can be categorized into supervised threshold setting-based and unsupervised clustering-based methods. The former mainly relies on the dataset of labeled known devices to learn an effective decision threshold to precisely distinguish between known and unknown devices. Here labels of known devices can be either known conditions or obtained from unlabeled data with the designed algorithm. The latter primarily relies on unsupervised clustering algorithms to complete the category determination, which is generally combined with supervised training of neural network-based representers.

In research based on the pipeline demonstrated in Figure 13, only a few employed unsupervised clustering-based classifiers. Inspired by the proposed method in [50], Bassey *et al.* [73] employed CNN as the representer of RFF features, and utilized DBSCAN to perform clustering, reaching an AMI of 0.79 in the case of 5 known and 1 unknown ZigBee devices. From the experimental results of these two papers, it can be observed that the open set identification method based on clustering is able to detect the number of unknown devices to a certain extent, but it is not satisfactory in terms of accuracy.

Actually, in many application scenarios, the number of unknown device categories is not very valuable, therefore methods based on supervised threshold setting have received more attention. Reus-Muns *et al.* [51] proposed an authentication algorithm for 5G open RANs, which utilized CNN to extract RFFs from the I/Q samples of the base station signals, and accomplished one-*vs*-one verification based on softmax score. Also employing CNN to extract RFFs, Xie *et al.* [23] further enlarged the inter-class difference of the obtained RFF features using hyperspherical projection, and employed the cosine distance to portray the similarity of these features, reaching an AUC of 0.999 when EER was only 0.012, in the case of 45 known and 9 unknown ZigBee devices. Xu *et al.* [102] employed the intra-class splitting (ICS) technique where the known devices that are difficult to classify were used as the determination boundary to detect unknown devices. Transformer-based representer was also utilized to extract latent RFF features and to accomplish the open set identification task, reaching a detection rate that surpassed alternative open

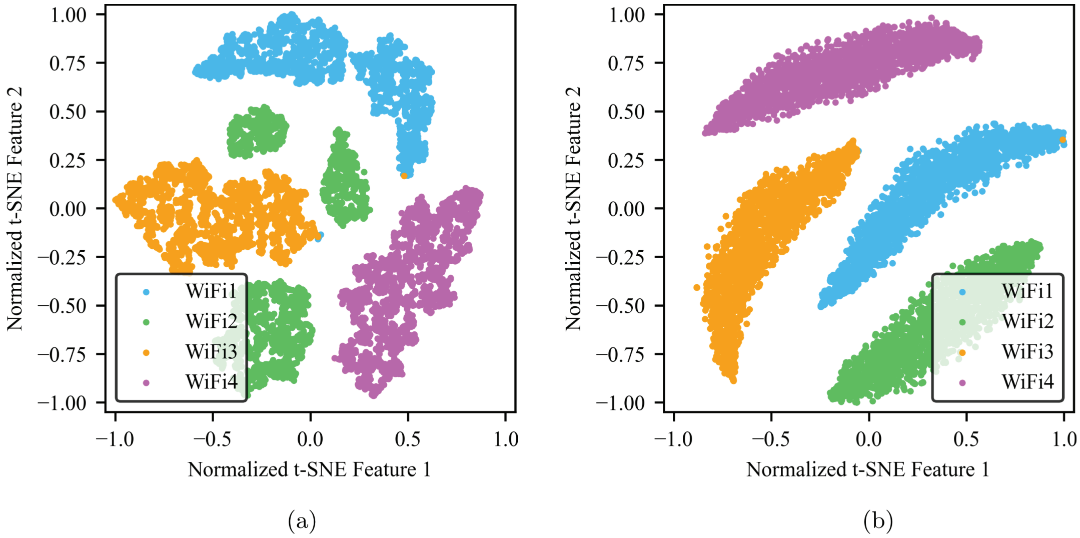

Figure 14. 2D feature visualization using *t*-SNE. (a) Network is trained without triplet loss. (b) Network is trained with triplet loss

set identification schemes such as Modified ICS [103], CROSR [104], and Hybrid OvA [100], under the experimental condition of 20 known and 10 unknown USRP devices.

In addition to the above research, Wang *et al.* [105] proposed an unknown device detection scheme based on a Siamese network, which utilized SLS SNR traces of 5G signals as RFF, obtaining a detection rate of 99% in different experimental scenarios. Xie *et al.* [60] replaced the softmax classifier of CNN with an intrinsic feature memorizer which was used for detecting unknown signals. Huang *et al.* [106] extracted RFFs in ADS-B signals with zero-bias CNN and employed the OpenMax classifier for open set identification. Zhao *et al.* [107] employed ResNet to extract RFFs from civil aviation radar signals and accomplished open set identification using Softmax-threshold and OpenMax-based approaches, respectively. The experimental results demonstrated that the Softmax-threshold approach is more advantageous in the classification of known devices, while the OpenMax-based approach is more applicable to the detection of unknown devices.

7.3.2 Application of metric learning

In the research of DL-based open set RFF identification, various types of neural networks have been employed to extract latent features with validity and generalization ability. Meanwhile, the identification mechanism based on these high-dimensional features often relies on the difference between sample pairs, which implies that for a discriminative model based on threshold setting, it makes sense to increase the inter-class gap and decrease the intra-class gap, and this is consistent with the nature of metric learning. Xie *et al.* [23] mapped the extracted features to the hypersphere to further enlarge the distinctions in RFF features between different known devices. Moreover, the loss function of the neural network is able to describe the distance between different feature parameters, such as contrastive loss [108], triplet loss [109], center loss [110], large-margin softmax loss [111], *etc.* At present, there are still few studies that apply these loss functions to the open set RFF identification. Reus-Muns *et al.* [51] combined triplet loss with cross-entropy loss in order to enlarge the difference between sample pairs during the training stage. Lei *et al.* [112] improved triplet loss by adding a penalty for intra-class distance and obtained an accuracy improvement of about 1% in the experiments.

Based on the dataset and method provided in [51], we visualized the high-dimensional RFF features using *t*-SNE, which is demonstrated in Figure 14. It is apparent that the high-dimensional RFF features of 4 WiFi devices are converted by triplet loss from the original 7 clusters in Figure 14a to 4 clusters in Figure 14b, and the distinction between clusters of different categories becomes more evident. This case vividly demonstrates the positive effects of metric learning on the training stage of RFF identification.

Table 5. Methods for data augmentation in RFF identification

Methods	Description	Application scenarios	Advantages	Disadvantages
Traditional signal processing	Use signal processing to simulate device samples in designed condition.	Most in closed set problems	• High explainability. • Low time consumption. • Easy to combine with other methods.	• Narrow scope of application. • Dependence on prior information and expert knowledge.
GAN	Train GAN model to generate device samples.	Most in open set problems	• The best sample quality. • Useful latent feature representation.	• High complexity of design. • Unstable training results. • Low explainability.
Autoencoder	Train Autoencoder model to generate device samples.	Most in open set problems	• Good sample quality. • Useful latent feature representation.	• High complexity of design. • Low explainability.

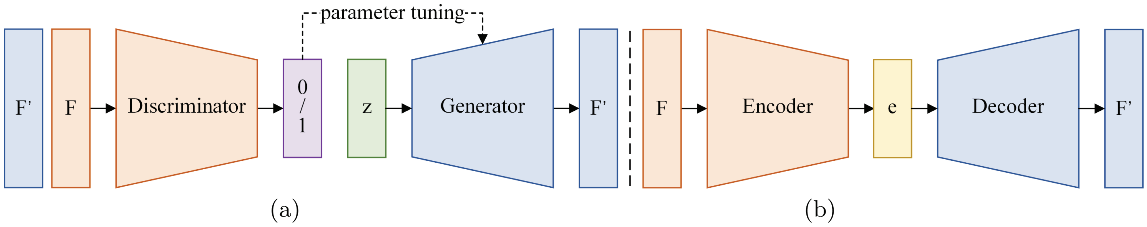

Figure 15. Typical architectures of generative models. Note that F, F′, z, and e represent input RFF features, generated/decoded features, random noise and encoded vector, respectively. (a) GAN. (b) Autoencoder

It should be noted that metric learning has a promising application prospect in RFF identification (*e.g.*, RFF against channel variation [51]), but the performance still remains to be verified.

7.4 Generative model-based open set RFF identification

In the open set problem, since the training set only contains known device samples and the test set merely consists of unknown device samples, their data do not satisfy the assumption of identical distribution, which is the main reason for the decrease in the accuracy of open set identification. In this regard, the generative model (GM) is an effective countermeasure, which can improve the identification accuracy to a certain extent by generating unknown device samples for training. Existing data augmentation methods utilized in RFF identification are summarized in Table 5, among which, however, traditional signal processing methods such as rotation, flipping, and adding Gaussian noise [113], are unable to meet the demand of generating effective unknown device samples because of the difficulty to portray complex channel condition in practical scenarios and differences of RFFS between known and unknown devices. Therefore, researchers turned their attention to DL-based data augmentation methods, such as GAN and Autoencoder. Typical architectures of GAN and Autoencoder are illustrated in Figure 15. In fact, generative models are usually able to accurately describe the feature distribution of known devices [114], and thus can obtain high detection rate of unknown devices.

7.4.1 GAN-based generative model

Zhao *et al.* [115] proposed an improved GAN model to generate samples of unknown devices in a two-dimensional feature space surrounding clusters of known device features, enhancing both identification accuracy and recall in the experiments. Roy *et al.* [116, 117] generated rogue device samples with GAN and I/Q signals of USRP devices, based on which the detection of counterfeit was successfully performed. Han *et al.* [118] obtained an unknown device detection rate of 99.98% based on Wasserstein GAN with gradient penalty (WGAN-GP) and multi-classifier. Chen *et al.* [119] utilized GAN to generate unknown device samples and randomly selected 1 out of 54 ZigBee devices as known devices and the remaining 53 as unknown devices, achieving 95% open set identification accuracy at an SNR of 30 dB. Wang *et al.*

Table 6. Current state-of-the-art open set RFF identification methods

Methods	Reference	Openness	Device/ Protocol	Signal preprocessing[a]	Category of RFF/ Further processing	Classifier	Experimental result
Traditional machine learning based	IEEE IoT 2021 [49]	29.29%	WiMAX	Raw	RF-DNA/ Relief-F for FDR	SVM	TPR $\geq 90\%$, FPR $\leq 10\%$ at 6 dB SNR
	IEEE IoT 2021 [97]	18.35%	ZigBee	Frequency/ phase offset compensation	I/Q data/ LDA for FDR	GPLDA	EER $= 0.0063$ at 30 dB SNR
Deep learning based	IEEE TIFS 2021 [23]	4.65%	ZigBee	Neural synchronization	I/Q data/ Hypersphere representation	Auxiliary linear classifier	EER $= 0.020$, AUC $= 0.998$ at 30 dB SNR with device aging[b]
Generative model-based	IEEE GLOBECOM 2021 [120]	50.00%	WiFi	Raw	I/Q data/ Blind outlier generation with Autoencoder	OvA classifier and $\lvert A\rvert + 1$ classification network[c]	Testing accuracy: $\geq 84\%$

Note: [a] Specifically refers to preprocessing other than basic operations such as normalization and signal slicing, which does not require prior information. [b] Also known as parameter drift, which will be discussed in Section 8.1.1. [c] $|A|$ denotes the number of known devices.

[105] proposed an open set identification scheme for 5G mmWave, which was based on GAN and RFFs named SLS SNR trace.

7.4.2 Autoencoder-based generative model

Utilizing Autoencoder, Karunaratne *et al.* [120] proposed two blind outlier generation schemes based on the ellipsoidal method and optimization method, respectively. The former relies on experience in the setting of hyperparameters, while the latter requires more resources in the computation of gradient descent. In the experiment, 30 unknown WiFi transmitters were set, together with a different number of known transmitters. The experimental results showed that the accuracy improvement obtained by the ellipsoidal method and optimization method was up to 15% and 25%, respectively, compared to the case without data augmentation. Nosouhi *et al.* [121] performed the detection of unknown 5G devices using beam pattern as RFF and deep Autoencoder as data augmentation method, obtaining a detection rate of 98.6% when there were 100 known devices.

7.5 Summary

This section presents a comprehensive survey on the open set RFF identification and clarifies the development of related research, pointing out three approaches to solving the open set problem, which are methods based on traditional machine learning, deep learning, and generative model. The current state-of-the-art methodologies are summarized in Table 6. It is worth mentioning that researches related to open set problems are much less than that related to closed set problems, and various effective methodologies are yet to be further explored by researchers.

8 Challenges and future research directions

This paper demonstrates that RFF identification is an important technique in the field of physical layer security for the identification of IoT devices. However, this technique is still in the development stage and there are still remaining challenges. This section summarizes the challenges faced by RFF identification and future research trends.

8.1 Challenges in RFF identification

8.1.1 Effectiveness and robustness of features

(1) Parameter drift

IoT devices generally have a long duration of service, therefore the aging of the device is an unavoidable issue, and the resultant changes in the RFF will also have an impact on the performance of identification [23, 27, 97].

(2) Manufacturing technology
IoT devices produced by the same manufacturer often have similar RFFs, which poses a direct threat to the fundamental characteristic of *Uniqueness*. To address this problem, current research either adopts deep learning methods to explore latent RFF features or utilizes the special properties of certain feature parameters, such as the long-term stability of CFO [17]. Moreover, with the improvement of the manufacturing process, the representation ability of some RFF features inevitably decreases, which causes difficulties in distinguishing IoT devices. For this problem, injectable RFFs seem to be a promising solution [122].

8.1.2 Sample composition of identification model

(1) Complexity
In the open set RFF identification schemes presented in this paper, the unknown devices are unauthorized devices that appear only in the test set. However, in practical application scenarios, samples of unauthorized devices are sometimes available in the training stage [100, 120, 123–125], which can be called Universum data. Therefore, how to effectively utilize these samples to enhance the security of the physical layer is a question worth investigating.

(2) Diversity
Currently, the diversity of data samples can be summarized into three main types. The first is the case where the number of samples is small, such as few-shot [60, 105], one-shot [97], and even zero-shot conditions. The second is the case of imbalanced samples, which is mainly reflected by the difference in the number of samples from different devices (also known as the problem of long-tailed distribution), or the difference between the number of positive and negative samples. The third is the case of large-scale samples [34, 84]. All three of these cases have an impact on the performance of RFF identification.

8.1.3 Requirements of application scenarios

(1) Scalability
In practical scenarios, devices are often constantly registered and can be logged out at any time [24], therefore the requirements for RFF identification could be constantly changing, which poses a challenge to the scalability of the identification model. Thankfully, the methodologies based on semi-supervised learning, transfer learning [96, 125], and incremental learning [59, 126, 127], which have been applied in RFF identification, provide guidance to address this challenge.

(2) Multi-task
Practical application scenarios for RFF identification often have requirements for multi-task, such as the simultaneous execution of known device classification and unknown device detection. A simple solution is to complete every task separately, but such an approach may result in a waste of resources. Therefore, how to obtain optimal results for multiple tasks simultaneously is a valuable research point.

(3) Unsupervised learning
The lack of labeled datasets is a possible challenge in practical scenarios, especially under non-cooperative conditions [128]. As to IoT device identification, traditional machine learning algorithms such as K-Means and DBSCAN often meet with problems of low accuracy, while the studies based on deep learning methods are currently sparse.

8.1.4 Resource limitation

(1) Measurement accuracy
Compared to low-end receivers (*e.g.*, USRP), RFFs obtained based on high-end receivers (*e.g.*, PXIe system [93]) tend to be more effective. In fact, the sampling rate of the received signal tends to be positively correlated with the performance of RFF identification within a certain range [30, 64, 79]. In practice, however, low-cost receivers usually have lower measurement accuracy, which poses a challenge to the design of the RFF identification scheme.

Table 7. Open source RFF datasets

Reference	Device/ Protocol	Transmitter population	Receiver	Sample rate	Frequency	Real-world (R)/ Generated (G)
[129]	ZigBee	60	USRP N210	10 MS/s	2.505 GHz	R
[130]	LoRa	10	USRP N210	250 kS/s	868.1 MHz	R
[131]	Bluetooth	10	USRP X300	2 MS/s	2.414 GHz	R
[132]	WiFi	174	USRP B210/N210/X310	25 MS/s	2.462 GHz	R
[133]	ADS-B	>140	USRP B210	8 MS/s	1.090 GHz	R
[134]	DJI M100 UAV	7	USRP X310	10 MS/s	2.4 GHz	R
[34]	USRP N210/X310	20	USRP N210	20 MS/s	2.432 GHz	G
[51]	USRP X310	4	USRP B210	5 and 7.68 MS/s	2.685 GHz	G

(2) Computing and storage resources

Computing and storage resources are also constraints for RFF identification, especially for lightweight application scenarios. Therefore, the trade-off between identification accuracy and resource consumption can be added as an optimization problem in the process of scheme design.

(3) Open source RFF datasets

A quality dataset can not only facilitate the training of deep learning-based RFF identification methods to obtain effective neural network models, but also serve as a benchmark to measure the strengths and weaknesses among different methods. However, there is still a lack of open source RFF datasets, which slows down the progress of related research to some extent.

For convenience, Table 7 lists some of the datasets that have been made open source after 2020. Nevertheless, many of them have a limited number of transmitter population and there still remains a lack of high-quality RFF datasets of real-world LTE and 5G-NR signals.

8.2 Future research directions

8.2.1 RFF applications in practical scenarios

Currently, there are research gaps in RFF identification technology with respect to two aspects: (1) In Narrow Band Internet of Things (NB-IOT), 5G massive Machine Type Communications (mMTC), and Internet of Vehicles (IoV), there exist terminals whose operating frequency points and bandwidths are dynamically changing. However, most previous research on RFF was focused on devices with fixed bandwidth and frequency points, which are not applicable to the scenarios above. (2) In scenarios such as IoV, WiFi, *etc.*, terminals may have multiple antennas and the transmitted signals will exhibit different RFF features from terminals with single antenna due to MIMO diversity or space-time coding, which has been rarely investigated.

8.2.2 Universal RFF

Compared with the current RFF technologies, a universal RFF no longer needs to construct features with specificity based on information such as the modulation mode of the signal. Instead, it can be applied to communication scenarios of different protocols and environments, requiring only subtle or even no additional scheme adjustments. It is a difficult but prospective problem to find such a universal RFF and apply it to closed set and open set environments.

8.2.3 Application of interpretable neural networks

There have been many research achievements demonstrating the important role of neural networks in RFF identification, but most of them encounter bottlenecks in accuracy improvement. The major reason lies in the incapability to accurately describe the discriminative process and boundary conditions of neural networks, therefore effective adjustment of the model cannot be accomplished. In this case, research related to interpretable neural networks is promising to promote the improvement of RFF identification technology.

9 Conclusion

This paper provides a comprehensive survey on RFF identification, which is a promising technique for IoT device identification. The relevant research achievements, especially the frontier studies in recent years, are discussed thoroughly. We clarify the process of RFF identification and the details of each stage, specifying the role of signal preprocessing, current schemes of RFF feature extraction, and further processing methods. We refine the framework of RFF identification from the perspective of closed set and open set problems, aiming to propel the technology based on RFF towards practical application scenarios. Furthermore, we summarize the research challenges and point out that RFF applications in practical scenarios, the universal RFF, and the application of interpretable neural networks are promising subsequent research directions in this field.

Conflict of Interest

The authors declare that they have no conflict of interest.

Data Availability

No data are associated with this article.

Authors' Contributions

Lingnan Xie mainly surveyed the RFF identification schemes under closed and open set environments. Linning Peng mainly surveyed the RFF feature extraction techniques. Junqing Zhang helped construct the architecture of the RFF identification system and improved its readability by language polishing and grammar modification. Aiqun Hu mainly surveyed the future research directions of RFF-based IoT device identification. All authors participated in the design of the paper structure.

Acknowledgements

We thank the anonymous reviewers for their helpful comments.

Funding

This work was supported in part by the National Natural Science Foundation of China under Grant 62171120 and 62001106, National Key Research and Development Program of China (2020YFE0200600), Jiangsu Provincial Key Laboratory of Network and Information Security No. BM2003201, Guangdong Key Research and Development Program under Grant 2020B0303010001, and Purple Mountain Laboratories for Network and Communication Security.

References

[1] Zhang JQ, Li GY and Marshall A et al. A new frontier for IoT security emerging from three decades of key generation relying on wireless channels. IEEE Access 2020; **8**: 138406–46.

[2] Pan JL and McElhannon J. Future edge cloud and edge computing for Internet of Things applications. IEEE Internet Things J 2018; **5**: 439–49.

[3] Statista. Number of IoT connected devices worldwide 2019–2021, with forecasts to 2030. https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/ (accessed on 10 September 2022).

[4] Zielonka A, Sikora A and Wozniak M et al. Intelligent Internet of Things system for smart home optimal convection. IEEE Trans Ind Inform 2021; **17**: 4308–17.

[5] Qadri YA, Nauman A and Bin Zikria Y et al. The future of healthcare Internet of Things: a survey of emerging technologies. IEEE Commun Surv Tutor 2020; **22**: 1121–67.

[6] Song YX, Yu FR and Zhou L et al. Applications of the Internet of Things (IoT) in smart logistics: a comprehensive survey. IEEE Internet Things J 2021; **8**: 4250–74.

[7] Houda ZAE, Brik B and Ksentini A et al. When federated learning meets game theory: a cooperative framework to secure IIoT applications on edge computing. IEEE Trans Ind Inf 2022; **18**: 7988–97.

[8] Abdel-Basset M, Moustafa N and Hawash H et al. Federated intrusion detection in blockchain-based smart transportation systems. IEEE Trans Intell Transp Syst 2022; **23**: 2523–37.

[9] Gharaibeh A, Salahuddin MA and Hussini SJ et al. Smart cities: a survey on data management, security, and enabling technologies. IEEE Commun Surv Tutor 2017; **19**: 2456–501.

[10] Lichtman M, Rao R and Marojevic V et al. 5G NR jamming, spoofing, and sniffing: threat assessment and mitigation. In: 2018 IEEE International Conference on Communications Workshops (ICC Workshops). IEEE, Kansas City, MO, USA, May 2018, 1–6.

[11] SWAN white paper – Radio frequency vulnerabilities. https://cpb-eu-w2.wpmucdn.com/blogs.bristol.ac.uk/dist/6/635/files/2021/05/SWANWH2.pdf (accessed on 8 March 2023).

[12] Li W, Wang J and Li L et al. Countermeasure for smart jamming threat: a deceptively adversarial attack approach. In: ICC 2021-IEEE International Conference on Communications. IEEE, Canada, June 2021, doi: 10.1109/ICC42927.2021.9500773.

[13] Hall J, Barbeau M and Kranakis E. Detection of transient in radio frequency fingerprinting using signal phase. Wireless Opt Commun 2003; **9**: 13–8.

[14] Scheirer W, Jain LP and Boult TE. Probability models for open set recognition. IEEE Trans Pattern Anal Mach Intell 2014; **36**: 2317–24.

[15] Geng C, Huang SJ and Chen S. Recent advances in open set recognition: a survey. IEEE Trans Pattern Anal Mach Intell 2021; **43**: 3614–31.

[16] Patel HJ, Temple MA and Baldwin RO. Improving ZigBee device network authentication using ensemble decision tree classifiers with radio frequency distinct native attribute fingerprinting. IEEE Trans Reliab 2015; **64**: 221–33.

[17] Shen GX, Zhang JQ and Marshall A et al. Radio frequency fingerprint identification for LoRa using spectrogram and CNN. In: IEEE INFOCOM 2021 – IEEE Conference on Computer Communications. IEEE, Vancouver, BC, Canada, May 2021, 1–10.

[18] Andrews SD. Extensions to radio frequency fingerprinting. Ph.D. Dissertation, Virginia Tech, 2019.

[19] Cekic M, Gopalakrishnan S and Madhow U. Wireless fingerprinting via deep learning: the impact of confounding factors. In: 2021 55th Asilomar Conference on Signals, Systems, and Computers. IEEE, Pacific Grove, CA, USA, November 2021, 677–84.

[20] Yin PC, Peng LN and Zhang JQ et al. LTE device identification based on RF fingerprint with multi-channel convolutional neural network. In: 2021 IEEE Global Communications Conference (GLOBECOM). IEEE, Madrid, Spain, December 2021, 1–6.

[21] Merchant K, Revay S and Stantchev G et al. Deep learning for RF device fingerprinting in cognitive communication networks. IEEE J Sel Top Signal Process 2018; **12**: 160–7.

[22] Qiu YJ, Peng LN and Zhang JQ et al. Signal-independent RFF identification for LTE mobile devices via ensemble deep learning. In: GLOBECOM 2022 – 2022 IEEE Global Communications Conference. IEEE, Rio de Janeiro, Brazil, December 2022, 37–42.

[23] Xie RJ, Xu W and Chen YZ et al. A generalizable model-and-data driven approach for open-set RFF authentication. IEEE Trans Inf Forensic Secur 2021; **16**: 4435–50.

[24] Shen GX, Zhang JQ and Marshall A et al. Towards scalable and channel-robust radio frequency fingerprint identification for LoRa. IEEE Trans Inf Forensic Secur 2022; **17**: 774–87.

[25] Sourour E, El-Ghoroury H and McNeill D et al. Frequency offset estimation and correction in the IEEE 802.11a WLAN. In: IEEE 60th Vehicular Technology Conference, 2004. VTC2004-Fall. IEEE, Los Angeles, CA, USA, September 2004, 4923–7.

[26] Shen GX, Zhang JQ and Marshall A et al. Radio frequency fingerprint identification for LoRa using deep learning. IEEE J Sel Areas Commun 2021; **39**: 2604–16.

[27] Peng LN, Hu AQ and Zhang JQ et al. Design of a hybrid RF fingerprint extraction and device classification scheme. IEEE Internet Things J 2019; **6**: 349–60.

[28] Xie FY, Wen H and Li YS et al. Optimized coherent integration-based radio frequency fingerprinting in Internet of Things. IEEE Internet Things J 2018; **5**: 3967–77.

[29] Xing YX, Hu AQ and Zhang JQ et al. On radio frequency fingerprint identification for DSSS systems in low SNR scenarios. IEEE Commun Lett 2018; **22**: 2326–9.

[30] Wang WD and Gan L. Radio frequency fingerprinting improved by statistical noise reduction. IEEE Trans Cogn Commun Netw 2022; **8**: 1444–52.

[31] Yu JB, Hu AQ and Zhou F et al. Radio frequency fingerprint identification based on denoising Autoencoders. In: 2019 International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob). IEEE, Barcelona, Spain, October 2019, 1–6.

[32] Diedrich A, Charoensuk W and Brychta RJ et al. Analysis of raw microneurographic recordings based on wavelet de-noising technique and classification algorithm: wavelet analysis in microneurography. IEEE Trans Biomed Eng 2003; **50**: 41–50.

[33] Johnstone IM and Silverman BW. Wavelet threshold estimators for data with correlated noise. J R Stat Soc Ser B-Stat Methodol 1997; **59**: 319–51.

[34] Al-Shawabka A, Restuccia F and D'Oro S et al. Exposing the fingerprint: dissecting the impact of the wireless channel on radio fingerprinting. In: IEEE INFOCOM 2020 – IEEE Conference on Computer Communications. IEEE, Toronto, ON, Canada, July 2020, 646–55.

[35] Ding TY, Peng LN and Qiu YJ et al. A research of I/Q imbalance based RF fingerprint identification with LTE-RACH signals. In: 2021 IEEE 6th International Conference on Signal and Image Processing (ICSIP). IEEE, Xi'an, China, April 2021, 66–71.

[36] Zheng TH, Sun Z and Ren K. FID: function modeling-based data-independent and channel-robust physical-layer identification. In: Proc IEEE INFOCOM, Paris, France, April 2019, 199–207.

[37] Restuccia F, D'Oro S and Al-Shawabka A et al. DeepRadioID: real-time channel-resilient optimization of deep learning-based radio fingerprinting algorithms. In: Proceedings of the Twentieth ACM International Symposium on Mobile Ad Hoc Networking and Computing. ACM, Catania, Italy, July 2019, 51–60.

[38] Xing YX, Hu AQ and Zhang JQ et al. Design of a channel robust radio frequency fingerprint identification scheme. IEEE Internet Things J 2022; **10**: 6946–59.

[39] Wang D, Hu AQ and Wang Y. Radio frequency fingerprint estimation in multi-path transmission environment. J Cryptol Res 2020; **7**: 249–60.

[40] Rajendran S and Sun Z. RF impairment model-based IoT physical-layer identification for enhanced domain generalization. IEEE Trans Inf Forensic Secur 2022; **17**: 1285–99.

[41] Hall J, Barbeau M and Kranakis E. Detecting rogue devices in bluetooth networks using radio frequency fingerprinting. In: Proceedings of the 3rd IASTED International Conference on Communications and Computer Networks, Lima, Peru, 2006, 108–13.

[42] Klein RW, Temple MA and Mendenhall MJ. Application of wavelet-based RF fingerprinting to enhance wireless network security. J Commun Netw 2009; **11**: 544–55.

[43] Yuan HL and Hu AQ. Preamble-based detection of Wi-Fi transmitter RF fingerprints. Electron Lett 2010; **46**: 1165–6.

[44] Lin Y, Zhu XL and Zheng ZG et al. The individual identification method of wireless device based on dimensionality reduction and machine learning. J Supercomput 2019; **75**: 3010–27.

[45] Danev B and Capkun S. Transient-based identification of wireless sensor nodes. In: 2009 International Conference on Information Processing in Sensor Networks. IEEE, San Francisco, CA, USA, April 2009, 25–36.

[46] Dubendorfer CK, Ramsey BW and Temple MA. An RF-DNA verification process for ZigBee networks. In: MILCOM 2012 – 2012 IEEE Military Communications Conference. IEEE, Orlando, FL, USA, November 2012, 1–6.

[47] Wheeler CG and Reising DR. Assessment of the impact of CFO on RF-DNA fingerprint classification performance. In: 2017 International Conference on Computing, Networking and Communications (ICNC). IEEE, Silicon Valley, CA, USA, January 2017, 110–4.

[48] Talbot CM, Temple MA and Carbino TJ et al. Detecting rogue attacks on commercial wireless Insteon home automation systems. Comput Secur 2018; **74**: 296–307.

[49] Reising D, Cancelleri J and Loveless TD et al. Radio identity verification-based IoT security using RF-DNA fingerprints and SVM. IEEE Internet Things J 2021; **8**: 8356–71.

[50] Wong LJ, Headley WC and Andrews S et al. Clustering learned CNN features from raw I/Q data for emitter identification. In: MILCOM 2018 – 2018 IEEE Military Communications Conference (MILCOM). IEEE, Los Angeles, CA, USA, July 2018, 26–33.

[51] Reus-Muns G, Jaisinghani D and Sankhe K et al. Trust in 5G open RANs through machine learning: RF fingerprinting on the POWDER PAWR platform. In: GLOBECOM 2020 – 2020 IEEE Global Communications Conference. IEEE, Taipei, Taiwan, December 2020, 1–6.

[52] Sankhe K, Belgiovine M and Zhou F et al. No radio left behind: radio fingerprinting through deep learning of physical-layer hardware impairments. IEEE Trans Cogn Commun Netw 2020; **6**: 165–78.

[53] McGinthy JM, Wong LJ and Michaels AJ. Groundwork for neural network-based specific emitter identification authentication for IoT. IEEE Internet Things J 2019; **6**: 6429–40.

[54] Brik V, Banerjee S and Gruteser M et al. Wireless device identification with radiometric signatures. In: Proceedings of the 14th ACM International Conference on Mobile Computing and Networking. ACM, San Francisco, CA, USA, September 2008, 116–27.

[55] Vo-Huu TD, Vo-Huu TD and Noubir G. Fingerprinting Wi-Fi devices using software defined radios. In: Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks. ACM, Darmstadt, Germany, July 2016, 3–13.

[56] Nguyen NT, Zheng GB and Han Z et al. Device fingerprinting to enhance wireless security using nonparametric Bayesian method. In: 2011 Proceedings IEEE INFOCOM. IEEE, Shanghai, China, April 2011, 1404–12.

[57] Rahbari H, Krunz M and Lazos L. Security vulnerability and countermeasures of frequency offset correction in 802.11a systems. In: IEEE INFOCOM 2014-IEEE Conference on Computer Communications. IEEE, Toronto, ON, Canada, April 2014, 1015–23.

[58] Agadakos I, Agadakos N and Polakis J et al. Chameleons' oblivion: complex-valued deep neural networks for protocol-agnostic RF device fingerprinting. In: 2020 IEEE European Symposium on Security and Privacy (EuroS&P). IEEE, Genoa, Italy, September 2020, 322–38.

[59] Liu MQ, Wang JK and Zhao N et al. Radio frequency fingerprint collaborative intelligent identification using incremental learning. IEEE Trans Netw Sci Eng 2022; **9**: 3222–33.

[60] Xie CX, Zhang LM and Zhong ZG. Meta learning-based open-set identification system for specific emitter identification in non-cooperative scenarios. KSII Trans Internet Inf Syst 2022; **16**: 1755–77.

[61] Lv YY, Liu YN and Liu F et al. Automatic modulation recognition of digital signals using CWT based on optimal scales. In: 2014 IEEE International Conference on Computer and Information Technology. IEEE, Xi'an, Shaanxi, China, September 2014, 430–4.

[62] Zhang JW, Wang FG and Dobre OA et al. Specific emitter identification via Hilbert–Huang transform in single-hop and relaying scenarios. IEEE Trans Inf Forensic Secur 2016; **11**: 1192–205.

[63] Peng LN, Hu AQ and Jiang Y et al. A differential constellation trace figure based device identification method for ZigBee nodes. In: 2016 8th International Conference on Wireless Communications & Signal Processing (WCSP). IEEE, Yangzhou, China, October 2016, 1–6.

[64] Peng LN, Zhang JQ and Liu M et al. Deep learning based RF fingerprint identification using differential constellation trace figure. IEEE Trans Veh Technol 2020; **69**: 1091–5.

[65] Peng Y, Liu PF and Wang Y et al. Radio frequency fingerprint identification based on slice integration cooperation and heat constellation trace figure. IEEE Wirel Commun Lett 2022; **11**: 543–7.

[66] Ray P, Reddy SS and Banerjee T. Various dimension reduction techniques for high dimensional data analysis: a review. Artif Intell Rev 2021; **54**: 3473–515.

[67] Bihl TJ, Bauer KW and Temple MA. Feature selection for RF fingerprinting with multiple discriminant analysis and using ZigBee device emissions. IEEE Trans Inf Forensic Secur 2016; **11**: 1862–74.

[68] Dubendorfer C, Ramsey B and Temple MA. ZigBee device verification for securing industrial control and building automation systems. In: Critical Infrastructure Protection VII: 7th IFIP WG 11.10 International Conference, ICCIP 2013, Washington, DC, USA, March 18–20, 2013, Revised Selected Papers 7. Springer Berlin Heidelberg, 2013, 47–62.

[69] Gedik N. A new feature extraction method based on multi-resolution representations of mammograms. Appl Soft Comput 2016; **44**: 128–33.

[70] Tian Q, Lin Y and Guo XH et al. New security mechanisms of high-reliability IoT communication based on radio frequency fingerprint. IEEE Internet Things J 2019; **6**: 7980–7.

[71] Ureten O and Serinken N. Wireless security through RF fingerprinting. Can J Electr Comp Eng-Rev Can Genie Electr Inf 2007; **32**: 27–33.

[72] Leonardi M and Gerardi F. Aircraft mode S transponder fingerprinting for intrusion detection. Aerospace 2020; **7**: 30.

[73] Bassey J, Adesina D and Li XF et al. Intrusion detection for IoT devices based on RF fingerprinting using deep learning. In: 2019 Fourth International Conference on Fog and Mobile Edge Computing (FMEC). IEEE, Rome, Italy, June 2019, 98–104.

[74] Cobb WE, Laspe ED and Baldwin RO et al. Intrinsic physical-layer authentication of integrated circuits. IEEE Trans Inf Forensic Secur 2012; **7**: 14–24.

[75] Huang GQ, Yuan YJ and Wang X et al. Specific emitter identification for communications transmitter using multi-measurements. Wirel Pers Commun 2017; **94**: 1523–42.

[76] Paul AJ, Collins PJ and Temple MA. Enhancing microwave system health assessment using artificial neural networks. IEEE Antennas Wirel Propag Lett 2019; **18**: 2230–4.

[77] Gritsenko A, Wang ZF and Jian T et al. Finding a "new" needle in the haystack: unseen radio detection in large populations using deep learning. In: 2019 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN). IEEE, Newark, NJ, USA, November 2019, 430–9.

[78] He BF and Wang FG. Cooperative specific emitter identification via multiple distorted receivers. IEEE Trans Inf Forensic Secur 2020; **15**: 3791–806.

[79] Yu JB, Hu AQ and Li GY et al. A robust RF fingerprinting approach using multisampling convolutional neural network. IEEE Internet Things J 2019; **6**: 6786–99.

[80] Wu WW, Hu S and Lin D et al. DSLN: securing internet of things through RF fingerprint recognition in low-SNR settings. IEEE Internet Things J 2022; **9**: 3838–49.

[81] Zhang TT, Ren PY and Ren ZY et al. FWSResNet: an edge device fingerprinting framework based on scattering and convolutional networks. In: 2022 IEEE 95th Vehicular Technology Conference (VTC2022-Spring). IEEE, Helsinki, Finland, June 2022, 1–6.

[82] Monga V, Li YL and Eldar YC. Algorithm unrolling: interpretable, efficient deep learning for signal and image processing. IEEE Signal Process Mag 2021; **38**: 18–44.

[83] Al-Shawabka A, Pietraski P and Pattar SB et al. DeepLoRa: fingerprinting LoRa devices at scale through deep learning and data augmentation. In: Proceedings of the Twenty-second International Symposium on Theory, Algorithmic Foundations, and Protocol Design for Mobile Networks and Mobile Computing. ACM, Shanghai, China, July 2021, 251–60.

[84] Robinson J, Kuzdeba S and Stankowicz J et al. Dilated causal convolutional model for RF fingerprinting. In: 2020 10th Annual Computing and Communication Workshop and Conference (CCWC). IEEE, Las Vegas, NV, USA, January 2021, 157–62.

[85] Soltani N, Sankhe K and Dy J et al. More is better: data augmentation for channel-resilient RF fingerprinting. IEEE Commun Mag 2020; **58**: 66–72.

[86] Defense Advanced Research Projects Agency (DARPA). Radio Frequency Machine Learning Systems (RFMLS). https://www.darpa.mil/program/radio-frequency-machine-learning-systems (accessed on 15 January 2023).

[87] Chouchane A, Rekhis S and Boudriga N. Defending against rogue base station attacks using wavelet based fingerprinting. In: 2009 IEEE/ACS International Conference on Computer Systems and Applications. IEEE, Rabat, Morocco, May 2009, 523–30.

[88] Rekhis S, Chouchane A and Boudriga N. Detection and reaction against DDoS attacks in cellular networks. In: 2008 3rd International Conference on Information and Communication Technologies: From Theory to Applications. IEEE, Damascus, Syria, April 2008, 2520–5.

[89] Rondeau CM, Betances JA and Temple MA. Securing ZigBee commercial communications using constellation based distinct native attribute fingerprinting. Secur Commun Netw 2018; 1489347.

[90] Rondeau CM, Temple MA and Betances JA et al. Extending critical infrastructure element longevity using constellation-based ID verification. Comput Secur 2021; **100**: 102073.

[91] Wang N, Li WW and Jiao L et al. Orientation and channel-independent RF fingerprinting for 5G IEEE 802.11ad devices. IEEE Internet Things J 2022; **9**: 9036–48.

[92] Tian Q, Lin Y and Guo X et al. An identity authentication method of a MIoT device based on radio frequency (RF) fingerprint technology. Sensors 2020; **20**: 1213.

[93] Patel H, Temple MA and Ramsey BW. Comparison of high-end and low-end receivers for RF-DNA fingerprinting. In: 2014 IEEE Military Communications Conference. IEEE, Baltimore, MD, USA, October 2014, 24–29.

[94] Reising DR and Temple MA. WiMAX mobile subscriber verification using Gabor-based RF-DNA fingerprints. In: 2012 IEEE International Conference on Communications (ICC). IEEE, Ottawa, Canada, June 2012, 1005–10.

[95] Kokalj-Filipovic S, Toliver P and Johnson W et al. Reservoir-based distributed machine learning for edge operation of emitter identification. In: MILCOM 2021 – 2021 IEEE Military Communications Conference (MILCOM). IEEE, San Diego, CA, USA, November 2021, 96–101.

[96] Medaiyese OO, Ezuma M and Lauf AP et al. Semi-supervised learning framework for UAV detection. In: 2021 IEEE 32nd Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC). IEEE, Helsinki, Finland, September 2021, 1185–90.

[97] Zhou XY, Hu AQ and Li GY et al. A robust radio-frequency fingerprint extraction scheme for practical device recognition. IEEE Internet Things J 2021; **8**: 11276–89.

[98] Liu YX, Wang J and Li JQ et al. Machine learning for the detection and identification of Internet of Things devices: A survey. IEEE Internet Things J 2022; **9**: 298–320.

[99] Hanna S, Karunaratne S and Cabric D. Deep learning approaches for open set wireless transmitter authorization. In: 2020 IEEE 21st International Workshop on Signal Processing Advances in Wireless Communications (SPAWC). IEEE, Atlanta, GA, USA, May 2020, 1–5.

[100] Hanna S, Karunaratne S and Cabric D. Open set wireless transmitter authorization: deep learning approaches and dataset considerations. IEEE Trans Cogn Commun Netw 2021; **7**: 59–72.

[101] Bendale A and Boult TE. Towards open set deep networks. In: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition. IEEE, Las Vegas, NV, USA, June 2016, 1563–72.

[102] Xu HF and Xu XD. A transformer based approach for open set specific emitter identification. In: 2021 7th International Conference on Computer and Communications (ICCC). IEEE, Chengdu, China, December 2021, 1420–5.

[103] Xu YJ, Qin XW and Xu XD et al. Open-set interference signal recognition using boundary samples: a hybrid approach. In: 2020 International Conference on Wireless Communications and Signal Processing (WCSP). IEEE, Nanjing, China, October 2020, 269–74.

[104] Yoshihashi R, Shao W and Kawakami R et al. Classification-reconstruction learning for open-set recognition. In: Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. IEEE, Long Beach, CA, USA, June 2019, 4011–20.

[105] Wang N, Jiao L and Wang P et al. Exploiting beam features for spoofing attack detection in mmWave 60-GHz IEEE 802.11ad networks. IEEE Trans Wirel Commun 2021; **20**: 3321–35.

[106] Huang K, Yang J and Hu P et al. A novel framework for open-set authentication of Internet of Things using limited devices. Sensors 2022; **22**: 2662.

[107] Zhao YR, Wang X and Lin ZY et al. Multi-classifier fusion for open-set specific emitter identification. Remote Sens 2022; **14**: 2226.

[108] Chopra S, Hadsell R and LeCun Y. Learning a similarity metric discriminatively, with application to face verification. In: 2005 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR'05). IEEE, San Diego, CA, USA, June 2005, **1**: 539–46.

[109] Schroff F, Kalenichenko D and Philbin J. FaceNet: a unified embedding for face recognition and clustering. In: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition. IEEE, Boston, MA, USA, June 2015, 815–23.

[110] Luo H, Gu YZ and Liao XY et al. Bag of tricks and a strong baseline for deep person re-identification. In: Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops. IEEE, Long Beach, CA, USA, June 2019, 1487–95.

[111] Liu WY, Wen YD and Yu ZD et al. Large-margin softmax loss for convolutional neural networks. Int Conf Mach Learn 2016, **48**: 7.

[112] Lei Y, Zhao CD and Wang YL et al. Security authentication of smart grid based on RFF. In: Lai Y, Wang T and Jiang M et al. (eds.). Algorithms and Architectures for Parallel Processing. ICA3PP 2021. Lecture Notes in Computer Science. Springer, Cham, Vol. 13157, December 2021, 362–75.

[113] Huang L, Pan WJ and Zhang Y et al. Data augmentation for deep learning-based radio modulation classification. IEEE Access 2020; **8**: 1498–506.

[114] Yang HM, Zhang XY and Yin F et al. Convolutional prototype network for open set recognition. IEEE Trans Pattern Anal Mach Intell 2020; **44**: 2358–70.

[115] Zhao CD, Shi MX and Cai ZB et al. Research on the open-categorical classification of the Internet-of-Things based on generative adversarial networks. Appl Sci-Basel 2018; **8**: 2351.

[116] Roy D, Mukherjee T and Chatterjee M et al. Detection of rogue RF transmitters using generative adversarial nets. In: 2019 IEEE wireless communications and networking conference (WCNC). IEEE, Marrakesh, Morocco, April 2019, 1–7.

[117] Roy D, Mukherjee T and Chatterjee M et al. RFAL: adversarial learning for RF transmitter identification and classification. IEEE Trans Cogn Commun Netw 2020; **6**: 783–801.

[118] Han H, Cui L and Li W et al. Radio frequency fingerprint based wireless transmitter identification against malicious attacker: an adversarial learning approach. In: 2020 International Conference on Wireless Communications and Signal Processing (WCSP). IEEE, Nanjing, China, October 2020, 310–5.

[119] Chen ZK, Peng LN and Hu AQ et al. Generative adversarial network-based rogue device identification using differential constellation trace figure. EURASIP J Wirel Commun Netw 2021; **2021**: 72.

[120] Karunaratne S, Hanna S and Cabric D. Open Set RF fingerprinting using generative outlier augmentation. In: 2021 IEEE Global Communications Conference (GLOBECOM). IEEE, Madrid, Spain, December 2021, 1–7.

[121] Nosouhi MR, Sood K and Grobler M et al. Towards spoofing resistant next generation IoT networks. IEEE Trans Inf Forensic Secur 2022; **17**: 1669–83.

[122] Mohanti S, Soltani N and Sankhe K et al. AirID: injecting a custom RF fingerprint for enhanced UAV identification using deep learning. In: GLOBECOM 2020 – 2020 IEEE Global Communications Conference. IEEE, Taipei, Taiwan, December 2020, 1–6.

[123] Wang ZF, Salehi B and Gritsenko A et al. Open-world class discovery with kernel networks. In: 2020 IEEE International Conference on Data Mining (ICDM). IEEE, Sorrento, Italy, November 2020, 631–40.

[124] Karunaratne S, Hanna S and Cabric D. Real-time wireless transmitter authorization: adapting to dynamic authorized sets with information retrieval. In: 2021 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN). IEEE, USA, December 2021, 302–8.

[125] Feng YT, Wang GL and Liu ZP et al. An unknown radar emitter identification method based on semi-supervised and transfer learning. Algorithms 2019; **12**: 271.

[126] Morehouse T, Montes C and Bisbano M et al. Incremental learning-based jammer classification. In: Artificial Intelligence and Machine Learning for Multi-Domain Operations Applications III. SPIE, USA, Vol. 11746, April 2021, 624–33.

[127] Liu YX, Wang J and Li JQ et al. Class-incremental learning for wireless device identification in IoT. IEEE Internet Things J 2021; **8**: 17227–35.

[128] Gong JL, Xu XD and Lei YK. Unsupervised specific emitter identification method using radio-frequency fingerprint embedded InfoGAN. IEEE Trans Inf Forensic Secur 2020; **15**: 2898–913.

[129] Shi JX, Peng LN and Fu H et al. Robust RF fingerprint extraction based on cyclic shift characteristic. IEEE Internet Things J 2023, doi: 10.1109/JIOT.2023.3281644.

[130] Shen GX, Zhang JQ and Marshall A et al. Toward length-versatile and noise-robust radio frequency fingerprint identification. IEEE Trans Inf Forensic Secur 2023; **18**: 2355–67.

[131] Jagannath A and Jagannath J. Embedding-assisted attentional deep learning for real-world RF fingerprinting of Bluetooth. IEEE Trans Cogn Commun Netw 2023, doi: 10.1109/TCCN.2023.3269764.

[132] Hanna S, Karunaratne S and Cabric D. WiSig: a large-scale WiFi signal dataset for receiver and channel agnostic RF fingerprinting. IEEE Access 2022; **10**: 22808–18.

[133] Liu YX, Wang J and Li JQ et al. Zero-bias deep learning for accurate identification of Internet-of-Things (IoT) devices. IEEE Internet Things J 2021; **8**: 2627–34.

[134] Soltani N, Reus-Muns G and Salehi B et al. RF fingerprinting unmanned aerial vehicles with non-standard transmitter waveforms. IEEE Trans Veh Technol 2020; **69**: 15518–31.

Lingnan Xie received the B.Eng. degree from Nanjing University of Science and Technology, Nanjing, China, in 2021. He is currently pursuing a Ph.D. degree at Southeast University, Nanjing, China. His current research interests include the Internet of Things and physical layer security in wireless communications.

Linning Peng received a Ph.D. degree from the IETR (Electronics and Telecommunications Institute of Rennes) Laboratory, INSA (National Institute of Applied Sciences) of Rennes, Rennes, France, in 2014. Since 2014, he has been a Research Associate with Southeast University, Nanjing, China. He is also a part-time researcher with the Purple Mountain Laboratories, Nanjing, China. His research interests include the Internet of Things and physical layer security in wired and wireless communications.

Junqing Zhang received a Ph.D. degree in electronics and electrical engineering from Queen's University Belfast, U.K., in 2016. He is currently a Lecturer (Assistant Professor) at the University of Liverpool, U.K. His research interests include the Internet of Things, wireless security, physical layer security, key generation, radio frequency fingerprint identification, and wireless sensing.

Aiqun Hu received a Ph.D. degree from Southeast University, Nanjing, China, in 1993. He is a Full Professor a Southeast University. He is also a part-time professor with the Purple Mountain Laboratories, Nanjing, China. His research interests are in wireless network technology and physical layer security of wireless communications.