


RESEARCH

Open Access



# Generative adversarial network-based rogue device identification using differential constellation trace figure

Zekun Chen<sup>1</sup> , Linning Peng<sup>1,2\*</sup>, Aiqun Hu<sup>2,3</sup> and Hua Fu<sup>1,2</sup>

\*Correspondence:

pengln@seu.edu.cn

<sup>2</sup> Purple Mountain

Laboratories, Nanjing, China

Full list of author information

is available at the end of the

article

## Abstract

With the dramatic development of the internet of things (IoT), security issues such as identity authentication have received serious attention. The radio frequency (RF) fingerprint of IoT device is an inherent feature, which can hardly be imitated. In this paper, we propose a rogue device identification technique via RF fingerprinting using deep learning-based generative adversarial network (GAN). Being different from traditional classification problems in RF fingerprint identifications, this work focuses on unknown accessing device recognition without prior information. A differential constellation trace figure generation process is initially employed to transform RF fingerprint features from time-domain waveforms to two-dimensional figures. Then, by using GAN, which is a kind of unsupervised learning algorithm, we can discriminate rogue devices without any prior information. An experimental verification system is built with 54 ZigBee devices regarded as recognized devices and accessing devices. A universal software radio peripheral receiver is used to capture the signal and identify the accessing devices. Experimental results show that the proposed rogue device identification method can achieve 95% identification accuracy in a real environment.

**Keywords:** Physical layer security, RF fingerprint, DCTF, GAN, Device identification

## 1 Introduction

The internet of things (IoT) connects various independent devices into a network and provides a possibility to interact with different machines at any time and anywhere, which brings tremendous convenience to our lives. With the increasing use of IoT technology, new security risks have emerged: criminals can attack the network by connecting illegal devices with malicious programs. Therefore, identifying IoT accessing devices and preventing intrusion is an imperative issue currently facing IoT networks [1, 2].

Traditional wireless systems primarily rely on high-level-based authentication information in terminal devices such as service set identifiers (SSID) [3], universal subscriber identity module (USIM) [4], and internet protocol (IP) or message authentication code (MAC) addresses [5]. However, some authentication information, such as SSID, MAC address, are not highly reliable since they can be easily forged. Besides, we can authenticate the identity of accessing devices via cryptography-based algorithms, such as

one-way hash functions-based schemes [6] or elliptic curve cryptography (ECC)-based authentication methods [7]. However, these algorithms mainly rely on complex protocols and mathematical calculations, which require high-cost in terminals. IoT devices are generally designed with low-cost consideration for which they are not suitable for high-complexity security algorithms or additional security modules such as USIM. Therefore, a kind of secure and terminal cost-free authentication method is required to ensure the security of the IoT systems. It is worth noting that most devices connect to the IoT through wireless channels. The radio frequency (RF) waveform contains unique features due to the manufacturing deviations of these devices. This kind of feature is called RF fingerprint or RF distinct and native attributes (DNA). RF fingerprint is an inherent feature of wireless devices in the physical layer which can hardly be forged. Moreover, the identity authentication system based on RF fingerprint, whose computational complexity is mainly borne by the receiving device at the base station, is not limited by the computing power and the battery capacity of the devices. Therefore, RF fingerprint-based identification technology has become a new solution to identify wireless devices [8–10].

In an RF fingerprint identification system, the legitimate device should initially communicate with the receiver so that the receiver can register the RF features, then the receiver will be able to verify the authenticity of the accessing device with the declared identity. Therefore, the process of rogue device identification using RF fingerprint can be divided into two steps: feature extraction and fingerprint identification.

### 1.1 Related works

Features such as relative carrier frequency offset [11], sampling offset, and constellation deviation [12] are named as modulation features, which can be used for RF fingerprint identifications. Danev et al. [13] used Fourier transform and linear discriminant analysis (LDA) to extract turn-on transient features as RF fingerprints. Polak et al. [14] proposed to use imperfections embedded in the digital-to-analog converter (DAC) and nonlinearity of power amplifier as RF fingerprints. Reising et al. [15] collected discrete Gabor transform features from WiFi and World Interoperability for Microwave Access (WiMAX) signals and used dimensional reduction analysis (DRA) to remove less-relevant features. Li et al. [16] used the time series composed of signal strength as fingerprints to distinguish wireless devices by calculating the similarity between time series. Besides, Bertoni et al. [17] used dynamic wavelet fingerprint (DWFP) and higher-order statistics as a significant basis for device identifications.

However, these methods have certain shortcomings. The transient signal-based RF fingerprint can seriously be affected by the position of the devices and the polarization direction of the antennas. Also, to capture slight variations in the transient part, the receiver requires high sensitivity, linearity, and over-sampling rate, thereby increasing the cost of RF fingerprint identifications [13]. Furthermore, the extraction of modulation features requires detailed information about the transmitted signal, including transmission frequency and synchronization information [18].

In the fingerprint identification process, the receiver will compare the extracted feature to that previously registered. It is worth noting that most of the existing RF fingerprint identification works deal with the classification problem, which is a goal of finding the minimal feature distance to the specified class. However, the rogue device identification

requires to exclusively confirm the identity of the accessing device with an unknown distance, which should be an unsupervised learning process with a different goal.

In existing RF fingerprint classification systems, traditional classification methods, e.g., multiple discriminant analysis (MDA) [19] and support vector machines (SVM) [20] are commonly used. Tian et al. [21] used K-nearest neighbor classifier (KNN) to classify the RF fingerprint extracted through principal component analysis (PCA) preprocessing. Kroon et al. used SVM to identify mobile phones accessed to the cellular base station. They compared the performance of one-class classifiers (OCC) and customized ensemble classifiers. However, the true negative rate and the true positive rate can not simultaneously reach a high level [22].

With the help of the rapid development of deep learning technologies, deep learning-based methods have been widely used in the field of wireless communication, such as channel estimations, waveform angle estimations, and modulation type identifications [23]. Many studies have used them for RF fingerprint-based device classification problems [24–30]. In our previous work, a DCTF-based convolutional neural network (CNN) system was designed to classify 54 Zigbee devices [30]. Schmidt et al. [25] classified wireless devices by assigning frequency channels and types of wireless technologies using CNN. Merchant et al. [26] operated on the time-domain complex baseband error signal by CNN to classify different devices without the need to manually select relevant features. Li et al. [27] authenticated the amplitude of quotient (AoQ) of WiFi signals using Euclidean distance and deep neural network (DNN) to classify different devices. Kose et al. [28] used probabilistic neural network (PNN) to classify the RF fingerprints extracted from transient signals of WiFi devices. Pan et al. [29] used deep residual networks to train the Hilbert spectrum images of received signals to classify specific emitters. Yu et al. [31, 32] used Multi-Sampling convolutional neural network (MSCNN) to identify ZigBee. Al-Shawabka et al. [33] used CNN to identify WiFi signal fragments, and Shen et al. [34] used spectrogram and CNN to identify Lora system. Reising et al. used generalized relevance learning vector quantization-improved (GRLVQI) method to identify WiMAX device features after dimensional reduction.

## 1.2 Method used in our work

In this paper, a differential constellation trace figure (DCTF)-based RF fingerprint extraction method is employed for rogue device identification. The DCTF extraction does not require time and frequency synchronization, which can be directly obtained in RF baseband [35]. The DCTF process converts time-domain variant I/Q sequences into a stable figure with a fixed size, which can be used as an effective basis for identifying different target devices. Besides, the baseband-based DCTF generation requires moderate equipment accuracy and therefore does not need the support of high-cost receivers. Experiments show that the accuracy of classifying 54 ZigBee devices using DCTF-based CNN in 30dB environment can reach more than 98%. This accuracy is 91.4% using I/Q samples-based CNN, 81.4% using bispectrum-based CNN and 41.7% using Hilbert–Huang transform (HHT)-based CNN in the same experiment condition [30].

Most of the mentioned fingerprint identification measures perform well in classifying different devices. However, there exists a limitation when using them to identify rogue devices, that is, CNN is a kind of supervised learning algorithm that requires labeled

samples with prior information for training. In reality, it is impossible to obtain the rogue device RF fingerprint in advance. Therefore, CNN-based algorithms can only classify recognized devices, but have difficulty in identifying unknown devices.

To solve this problem, we propose a novel generative adversarial network (GAN)-based rogue device identification method. GAN is a recent emerging unsupervised deep learning algorithm, which has received extensive attentions [36–40]. It is characterized by identifying the authenticity of data without the need for negative samples. Therefore, GAN is more practical than traditional CNN in identifying rogue devices. Ferdowsi et al. [41] utilized a distributed GAN-based intrusion detection system (IDS) to detect the data collected by IoT devices to prevent the invasion of abnormal data sent from cyber attackers. Our method used GAN to identify the RF fingerprint collected from accessing devices to prevent rogue devices accessed by attackers.

The device identification method proposed in this paper is mainly based on GANomaly, which is an improved GAN model proposed by Akcay et al. [37]. This is a kind of semi-supervised learning algorithm. We improve the updating algorithm of GANomaly, making it a completely unsupervised learning algorithm that is suitable for the field of unknown device identification. We train GANomaly using the features extracted from DCTF to obtain discriminators that can effectively identify the rogue devices. By this method, we can distinguish them from legitimate devices without obtaining any prior information of rogue devices.

### 1.3 Contributions

In the IoT system, the attacker uses a rogue device similar to a legitimate one to impersonate it and access the network. The rogue device has the same type as the legitimate one and can forge RF information such as MAC and SSID, which makes it difficult for traditional identification methods to identify them. The rogue device can perform attacks such as information theft and illegal data injection after accessing, thereby endangering the security of the IoT system. In this paper, we propose a GAN-based rogue device identification method to solve this problem. The main contributions of this work are shown as follows:

- A DCTF-based rogue device identification method is firstly proposed in this work. We demonstrate that the 2D DCTF is a promising feature for unknown device identification with low complexity and high precision.
- The existing applications of DCTF [30, 35, 42, 43] are for the classification of known devices, while this paper solves the problem of rogue device identification. This problem is more challenging since we cannot obtain any prior information about rogue devices.
- We introduce the GAN for rogue device identification and improve the GANomaly to a completely unsupervised model. With the help of the proposed DCTF-GAN method, we can identify rogue devices with only the fingerprint characteristics of legitimate devices.
- We used a much larger number of devices and conducted more experiments than any other relevant study of this kind. There has been no research on the true negative rate and true positive rate of such a large number of devices identification.

- We design a novel threshold selection algorithm and rogue device identification strategy to ensure the accuracy of distinguishing rogue devices from legitimate devices. The accuracy of identifying rogue devices can exceed 90% and 95%, respectively, in 20 dB and 30 dB signal-to-noise ratio (SNR) environments through our method.

The devices used in our experiments include the following categories:

- Recognized devices, which are known devices used to train the discriminator.
- Accessing devices, which are unknown devices to be identified, including legitimate devices and rogue devices.
- Legitimate devices, that is legal devices that should be allowed to access.
- Rogue devices, that is, invading devices disguised as legitimate ones. Our main purpose is to distinguish the accessing devices into legitimate ones and rogue ones.

This paper consists of the following sections: Section 2 introduces the principles of DCTF and its extraction methods. Section 3 describes the GAN model structure and the method of device identification. Section 4 provides an overview of the experimental design. Section 5 gives the experimental results and analysis. Section 6 summarizes the paper.

## 2 DCTF-based RF fingerprint extraction

DCTF is the fingerprint we use in this paper. Researches have shown that DCTF can achieve very high accuracy in the classification of devices with different protocols. Peng et al. [30] used DCTF for the classification of ZigBee. Wang et al. [44] used DCTF for the classification of Global System for Mobile Communications (GSM) devices, and Jiang et al. [45] used it for the classification of Lora devices. In these experiments, the accuracy of wireless device classification using DCTF can reach more than 95%. According to the IEEE 802.15.4 protocol, the ZigBee signal uses offset quadrature phase-shift keying (OQPSK), half sinusoidal pulse shaping, direct sequence spread spectrum (DSSS) modulation, with a data rate of 250 kbps and operates in the 2.4 GHz band. The transmitted signal is represented by the following equation considering only the I/Q channel offset without the nonlinear characteristics:

$$T(t) = ((\alpha X_I(t) + D_I) + (\beta X_Q(t + \varphi) + D_Q)j)e^{-j2\pi f_{cTx}t} \quad (1)$$

where  $X_I(t)$  and  $X_Q(t)$  represent real and imaginary parts of the OQPSK signal  $X(t)$ , namely the I-channel part and the Q-channel part, respectively.  $\alpha$ ,  $\beta$  are I/Q signal gains,  $D_I$  and  $D_Q$  are direct current (DC) offsets of the I/Q signals, respectively.  $\varphi$  is the normalized I/Q phase mismatch factor. These coefficients are related to hardware characteristics that vary with different devices, hence they can be used to identify different devices. With oversampling, this feature could be reflected in a constellation trace figure (CTF).  $f_{cTx}$  is the carrier frequency of the transmitter. Assuming the transmission channel is ideal, the received signal will be equal to the transmitted signal, i.e.:

$$R(t) = T(t) \quad (2)$$

The demodulated signal can be expressed as:

$$\begin{aligned}
Y(t) &= R(t)e^{-j2\pi f_{cRx}t + \Psi} \\
&= ((\alpha X_I(t) + D_I) \\
&\quad + (\beta X_Q(t + \varphi) + D_Q)j)e^{-j2\pi\theta t + \Psi}
\end{aligned} \tag{3}$$

where  $f_{cRx}$  is the receiver carrier frequency. In real systems,  $f_{cRx}$  can hardly be equal to  $f_{cTx}$ . Therefore,  $\theta = f_{cRx} - f_{cTx}$  represents the frequency difference between the transmitter and the receiver.  $\Psi$  is the phase difference between the transmitter and the receiver. When  $\theta \neq 0$ , the baseband signal at the receiver will have a phase rotation factor  $e^{j2\pi\theta t}$  compared to the transmitter, resulting in a rotation of the CTF without synchronization. To further enhance the fingerprint characteristics, we differentially process the receiver signal. This procedure can be formulated as follows:

$$d(t) = (Y_I(t) + Y_{t+\varphi}j) \cdot (Y_I(t + \lambda) + Y_Q(t + \lambda + \varphi))^* \tag{4}$$

That is, the  $I/Q$  channel signal at a certain time is conjugate-multiplied with the  $I/Q$  channel signal at the next time. Where  $Y_I(t)$  and  $Y_Q(t)$  are the real and imaginary parts of the  $I/Q$  channel of received signal  $Y(t)$ , respectively.  $\lambda$  is the differential time interval, and  $\varphi$  is phase mismatch distortion. Since frequency and phase offset are useful for device identification, We directly plot  $d(t)$  on the  $I/Q$  graph without synchronization to obtain a DCTF.

The carrier frequency and time synchronization will be required if we process directly on complex numbers, otherwise, the disturbance of frequency offset will make it difficult to identify the data. Conjugation will change the disturbance of the frequency offset into a fixed phase selection which forms a feature in the image and is easier to identify [30]. Therefore, we use DCTF as the input to complex neural networks instead of the complex numbers.

DCTF does not require any prior synchronization information about the receiver, which makes it a kind of stable transmitter feature that can be extracted at the receiver. Besides, The research in [42] verified that DCTF is a stable RF fingerprint through experimental measurements for 18 months, which will not vary significantly over time. Moreover, this method is also effective for signals modulated in other ways. A detailed explanation of RF fingerprint representation in DCTF is shown in [35].

### 3 GAN model construction

#### 3.1 Advantages and basic structure of GAN model

Traditional methods can effectively solve the problem of device classification. The work in [43] uses CNN and Long Short-Term Memory (LSTM) network to classify unknown devices. The experiment based on LSTM used  $I/Q$  sampling data for classification. However, it is found through experimental comparison that the classification accuracy of LSTM is not as good as image-based CNN after the statistical features of  $I/Q$  data have been obtained.

In classification, all of the samples are known and trained in advance. The classifier only needs to find the boundary between each device. The identification, by contrast, is more challenging. This is because that receivers only know information from a few devices and most of the devices are unknown. What's more, the boundary of each

recognized device suffers from noise variations, which leads to a trade-off between the accuracy of rogue device detection and legitimate device acceptance.

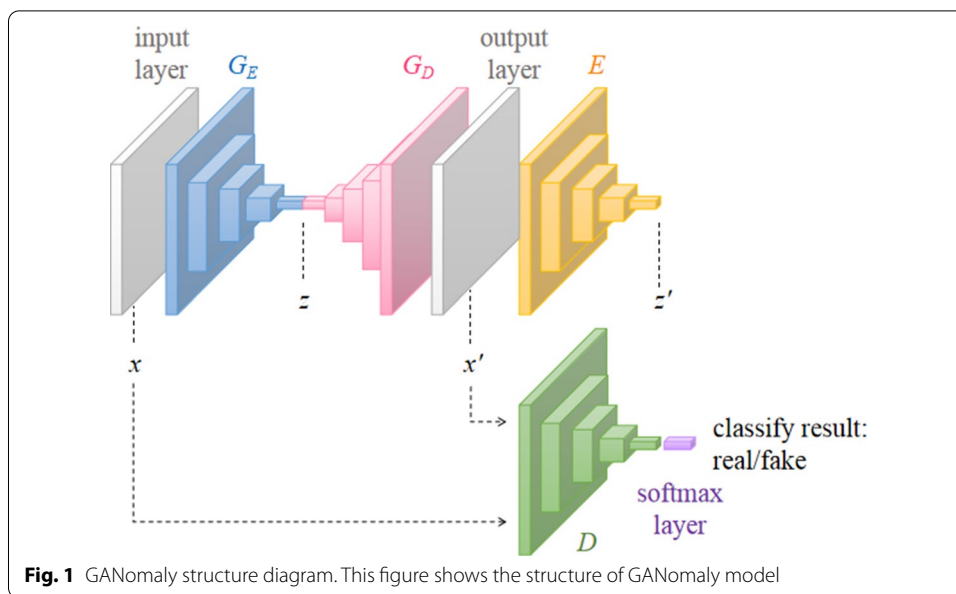
In actual situations, attacks of rogue devices are sudden and contingent, most of which cannot be sampled in advance. Recently, traditional methods such as LDA, SVM and  $K$ -means clustering have been used to identify rogue ZigBee devices. The work in [35] used  $K$ -means clustering to identify 10 recognized devices and 6 rogue devices, and both the true positive rate and true negative rate can reach nearly 100% under 10dB.

The limitation of these traditional methods is that sophisticated design need to be carried out when identifying a large number of input samples. The distribution of the samples should be converted into a Gaussian distribution through preprocessing in order to obtain better identification accuracy [46]. GAN can solve the problem of unknown device identification better for it is an unsupervised machine learning algorithm that was first proposed by Goodfellow et al. [36]. There have been many studies using this algorithm to generate images, while we use it to accomplish an identification task. Compared to other deep learning algorithms or fingerprint identification techniques, the advantage of GAN is that we do not need to obtain fingerprint samples of rogue devices in advance. This method trains the fingerprint samples of the recognized devices to enable the discriminators to learn the data distribution of legitimate devices' fingerprints, thereby identifying the accessing devices whose fingerprint does not match the legitimate devices as illegal ones.

The basic idea of GAN model is to train two neural networks at the same time: The first one is the generator network  $\mathcal{G}$  which can capture input data distribution and generating forged data following this distribution; the second one is the discriminator network  $\mathcal{D}$  which can be used to estimate the probability of a certain sample from raw data rather than generated by the generator  $\mathcal{G}$ .

Deep convolution generative adversarial network (DCGAN) is one of the most influential GAN structures proposed by Radford et al. [38] in 2016, which solved the problem of training instability that occurred in the original GAN. The GAN scheme adopted in this paper is the GANomaly model that further improved by Akcay et al. [37] based on DCGAN, which was first proposed in 2018. The primary goal of GANomaly is to generate fake images by learning the features of real images. The advantage of this model is that the training results will not be affected when a few abnormal images are mixed in the training set. Therefore, this model greatly reduces the interference of abnormal input data. The model consists of three sub-networks, whose structure is shown in Fig. 1. The GANomaly model consists of the following sub-networks:

- *Bow-tie automatic encoder  $G$*  This network is the generator part of the entire model, spliced with an encoder network that maps from a high-dimensional tensor  $x$  to a low-dimensional tensor  $z$ , and a decoder network that remaps  $z$  to a high-dimensional tensor  $x'$ . This generator learns the distribution of the input data and reconstructs them through the networks.
- *Encoder  $E$*  The role of this part is to downsample the reconstructed image  $x'$  into a low-dimensional tensor  $z'$ , whose dimension is consistent with  $z$ . It learns to mini-



**Fig. 1** GANomaly structure diagram. This figure shows the structure of GANomaly model

mize the distance between  $z$  and  $z'$  by parameterization. This distance, as a part of the total loss, serves as feedback to the entire learning process, which is utilized to calculate the model loss.

- *Discriminator D* This network receives the original data  $x$  from the input and the forged data  $x'$  from the generator and distinguishes them. The structure of this part is the same as the previously mentioned decoder network with an extra softmax layer added at the end.

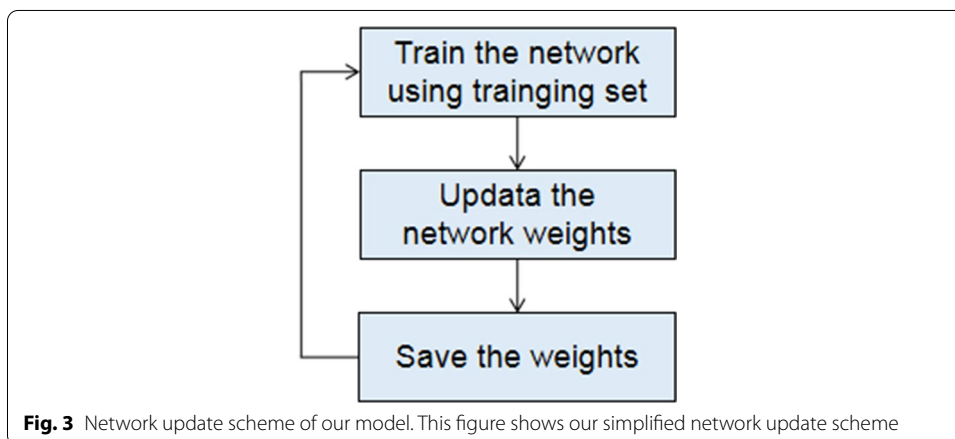
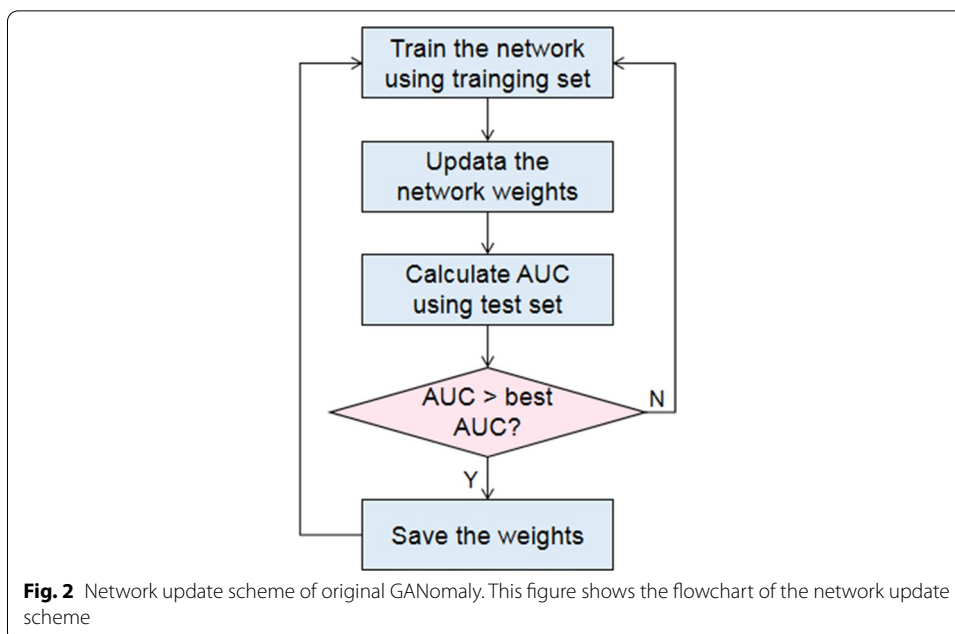
### 3.2 Model improvement

Our goal of using GANomaly is different from that of the original work of Akcay's. The main goal of the original work is to generate fake images using the trained generator, while our goal is to judge whether an unknown image sent to the trained discriminator is legitimate or not. For this purpose, we need to make some improvements to GANomaly.

The original GANomaly is a kind of semi-supervised machine learning scheme in which the networks are tested by calculating the area under the curve (AUC) of the receiver operating characteristic (ROC) of each current network using the data from the test set after each epoch of training, where ROC is a function of true positive rate (TPR) on the false positive rate (FPR) [37]. The weights of the network are saved only when the current AUC is higher than the best-AUC. The data in the test set used to obtain AUC, however, is labeled with "normal" or "abnormal". That is to say, although the training process is unsupervised, the test and weights preservation process are supervised, for which it is called a semi-supervised scheme. The flow chart of the network update scheme is shown in Fig. 2.

In the context of our work, due to the unavailability of accessing device RF fingerprint acquisition in advance, our approach needs to be completely unsupervised. Therefore, we save the current latest network weights after each epoch of training and the





discriminator obtained after the last epoch of training. Our simplified network update scheme is shown in Fig. 3.

### 3.3 Threshold selection

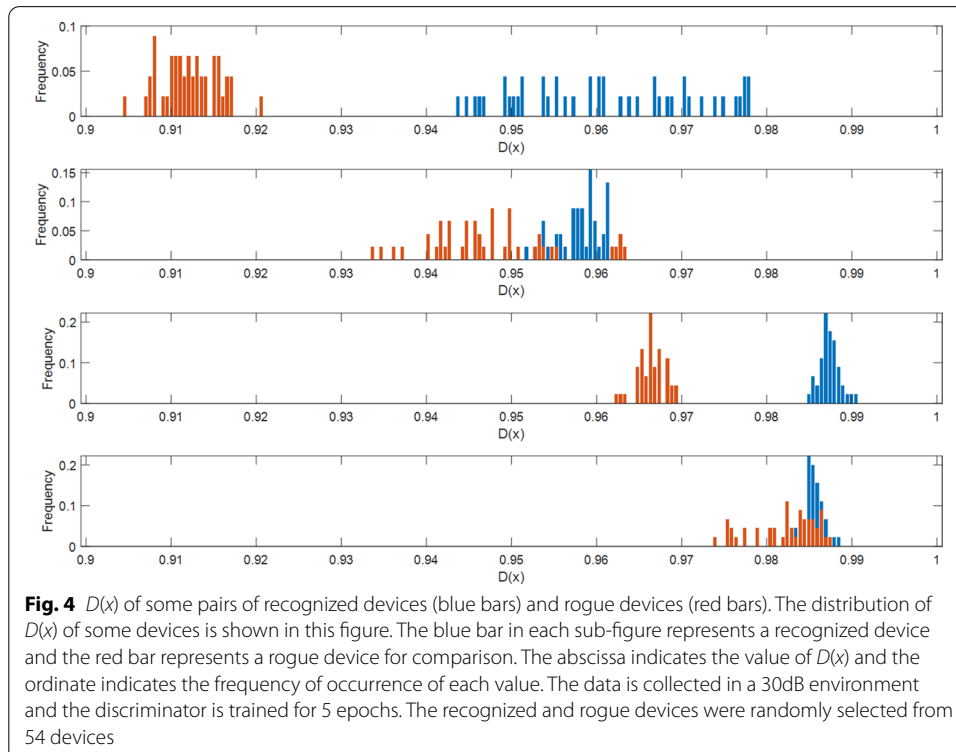
We need to determine a threshold  $\gamma$  for the discriminator to determine whether a DCTF image is from a legitimate device or a rogue device. The discriminant result of an image  $x$  obtained from the discriminator is  $D(x)$ , where  $D(x) \in [0, 1]$ . A larger  $D(x)$  indicates that the DCTF is more likely to come from a legitimate device. We judge that the DCTF image is from a legitimate device when  $D(x) \geq \gamma$ . In most of the existing systems, a specific threshold is always selected as a fixed value. Experiments have shown that discriminators trained by the same set of DCTF from a recognized device will give different  $D(x)$  to an unknown DCTF image because of the randomness of network training. It is unreasonable to set a fixed value threshold for determining whether the device is legal.

In practical systems, we are unable to achieve any prior information on the rogue device in advance. Therefore we can only determine  $\gamma$  based on the information of recognized devices. After we obtain the discriminator, a batch of DCTFs from recognized devices are sent to it and  $\gamma$  is determined according to  $D(x)$  of this batch of DCTF. The distribution of  $D(x)$  of some devices is shown in Fig. 4. The blue bar in each sub-figure represents a recognized device and the red bar represents a rogue device for comparison. The abscissa indicates the value of  $D(x)$  and the ordinate indicates the frequency of occurrence of each value. The data is collected in a 30dB environment and the discriminator is trained for 5 epochs. The recognized and rogue devices were randomly selected from 54 devices.

An intuitive approach to distinguish rogue devices is to compare the mean value of  $D(x)$  of the accessing device and the recognized device. However, this approach will easily cause an accessed legitimate device to be judged as a rogue one. It is difficult to determine  $\gamma$  according to statistical parameters such as the mean or the standard deviation for  $D(x)$  have no obvious distribution, as can be seen from Fig. 4. Therefore, we take the minimum value of  $D(x)$  of the recognized device as  $\gamma$ .

Another confronting problem is that  $D(x)$  of a legitimate device sometimes overlaps that of a rogue one, as shown in Fig. 4. Given this situation, we define another threshold  $\delta$  and stipulate that when the proportion of DCTF that satisfies  $D(x) \geq \gamma$  exceeds  $\delta$  in all DCTF images of an accessing device, this accessing device is considered to be legitimate.

The larger  $\delta$  is, the higher the accuracy of rogue device detection (i.e., true negative rate) is. Otherwise, the accuracy of legitimate device acceptance (i.e., true positive rate) is higher. We need a reasonable  $\delta$  to make a trade-off between the true negative rate and



the true positive rate. To find the best  $\delta$ , we take an interval of 0.1 within the scope of (0, 1] for testing, and the two kinds of accuracy reach equilibrium when  $\delta = 0.7$ . This experiment is performed in a 30dB environment and the discriminator is trained for 5 epochs.

In general, our threshold selection scheme is as follows:

We take a portion from the DCTF images set obtained from the recognized device denoted as  $x_r$  and send them to the trained discriminator to obtain  $\gamma$ . The discriminant result denoted as  $D(x_r)$  and the minimum value of  $D(x_r)$  is recorded as  $\gamma$ . The acquisition of  $\gamma$  can be formulated as:

$$\gamma = \min_i D(x_{r,i}) \quad (5)$$

The DCTF images set obtained from the accessing device is denoted as  $x_a$  and the basis for judging whether the  $j$ th image in  $x_a$  comes from a legitimate device can be formulated as:

$$T_j = \begin{cases} 1, & D(x_{a,j}) \geq \gamma, \text{ Legitimate device} \\ 0, & D(x_{a,j}) < \gamma, \text{ Rogue device} \end{cases} \quad (6)$$

The device is considered as legal when  $x_a$  meet the following conditions:

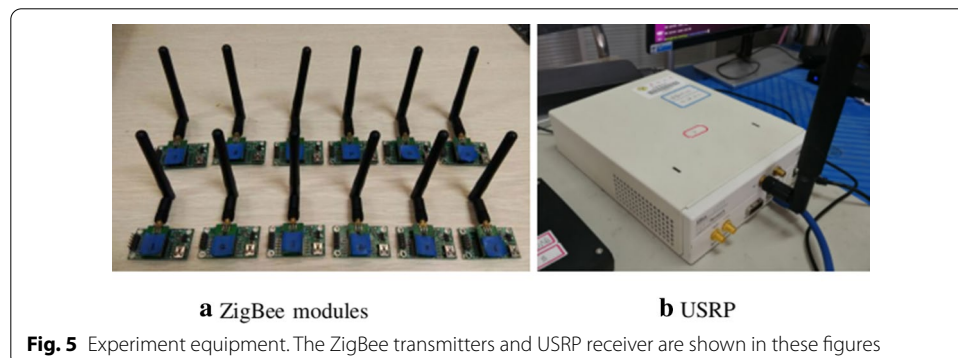
$$\sum_{i=1}^J T_j \geq \delta J = 0.7J \quad (7)$$

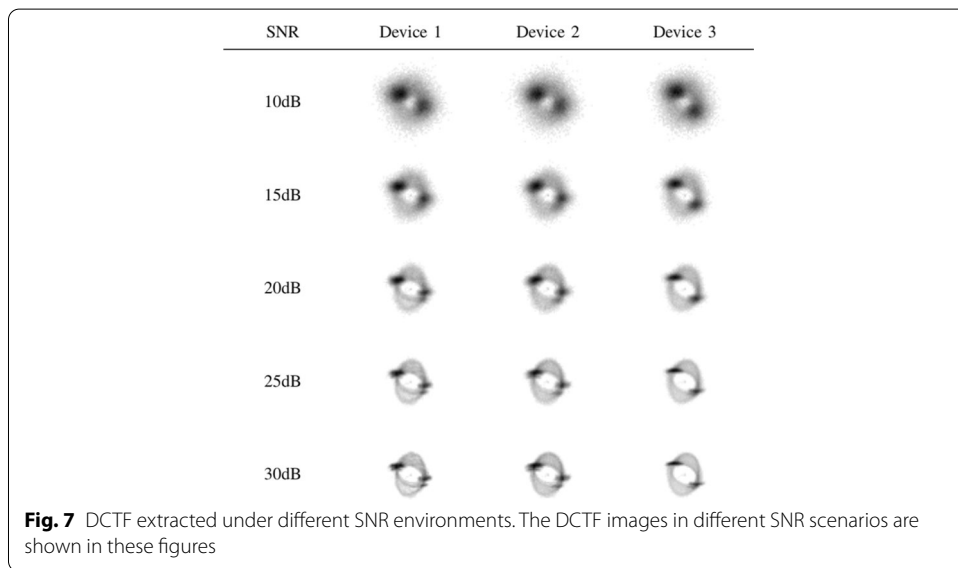
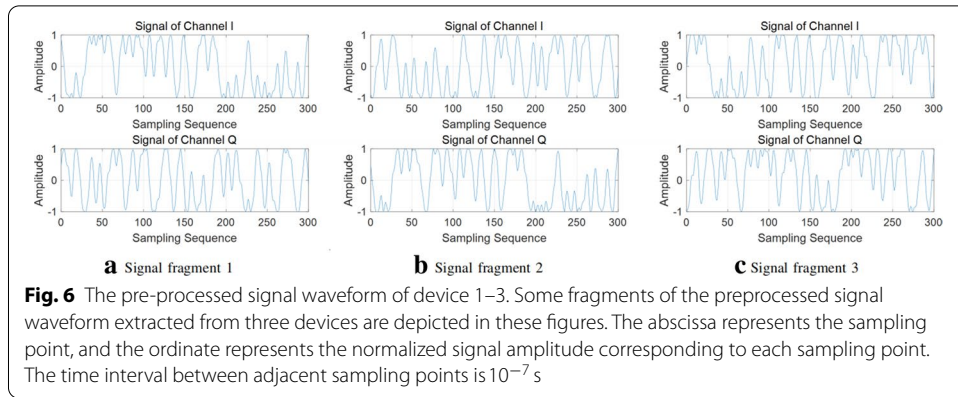
## 4 Experimental design

In our experiment, we use 54 TI CC2530 ZigBee modules as transmitters and a USRP N210 software radios platform as the RF signal receiver. The ZigBee transmitters and USRP receiver are shown in Fig. 5. We collect the RF signals transmitted by ZigBee devices and plot their DCTFs, which are used as fingerprints of different devices. We use GAN to identify rogue devices. The steps of this scheme are shown as follows.

### 4.1 Data extraction and plotting DCTF

We use USRP N210 to collect OQPSK signals from the ZigBee modules. ZigBee modules work at 2505 MHz with 1 MS chip rate. The USRP N210 sampling rate is 10 Mbps





and a total of about 400-k samples are captured from each device for feature extraction. The transmitted power is 21dBm, which is the maximum transmit power that the cc2530 can reach. The experiment is carried out in a real open environment with line-of-sight (LOS) transmission. We record the time domain signals in complex form and process them by MATLAB. We divide each set of data into several segments and normalize them with average absolute values. Some fragments of the pre-processed signal waveform extracted from three devices are depicted in Fig. 6. The abscissa represents the sampling point, and the ordinate represents the normalized signal amplitude corresponding to each sampling point. The time interval between adjacent sampling points is  $10^{-7}$  s.

To compare the results of the proposed scheme in different SNR scenarios, additive white Gaussian noise (AWGN) is added with the SNR at 15 dB, 20 dB, 25 dB, and 30 dB, respectively. These signals are processed and then plotted onto complex planes to obtain the DCTF, which are  $65 \times 65$  pixel greyscale images, where 20 k samples of a signal from one device are used in each image. The DCTF images in different SNR scenarios are shown in Fig. 7.

As can be seen from Fig. 7, although we cannot get any RF features directly from the original IQ waveform shown in Fig. 6, the DCTF plotted by them has distinct characteristics. Each DCTF has two gathering centers, respectively on the left and right sides of the image, each of which has a certain deviation and dispersion. These characteristics reflect the phase mismatch distortion and DC offset of the transmitted signals. Besides, the positions of gathering centers have certain rotation angles instead of locating in the exact right and left positions of the images, which reflects the differences in carrier frequency between transmitters and receivers. It can be seen that these features of different devices are subtly different, which can be used as characters for distinguishing devices.

#### 4.2 Discriminator training

We build a GAN model using PyTorch to identify rogue devices and use a computer with four GeForce RTX 2080 Ti graphics processing units (GPU) to train the model. The GAN construction consists of two parts:

- *NetG* It generates forged images and then downsamples it into a low-dimensional tensor. It consists of the bow-tie automatic encoder  $G$  and the encoder  $E$ , which are two sub-networks of GANomaly mentioned above.
- *NetD* It determines whether an input image is a real one. It corresponds to the discriminator  $D$  in GANomaly mentioned above.

The network architectures of *NetG* and *NetD* are listed in Tables 1 and 2, respectively. Two points need to be explained:

- Since the input image dimension of GANomaly must be an integer multiple of 16, we crop the  $65 \times 65$  pixel images to  $64 \times 64$  pixels.
- Unlike CNN, fully connected layers and pooling layers are not used in DCGAN and GANomaly which is developed based on DCGAN.

In *NetG*, *Input*— $x$  is DCTF from a recognized device, which is called a “real image”. *Output*— $x'$  is the “forged image” generated by the generator. The similarity of *Output*— $z$  and *Output*— $z'$  reflect the similarity of *Input*— $x$  and *Output*— $x'$ . In *NetD*, *Input* is DCTF from an accessing device and *Output* is a scalar that reflects the probability that the input DCTF came from a legitimate device.

After the network is built, we send the DCTF of different devices into GAN for training. The generator learns its distribution based on the characteristics of input data and produces forged images. Here we use Adam optimization algorithm for training. Starting from 0.00005, we gradually increase the initial learning rate for testing and finally set it to 0.0002, when the model can converge quickly. A larger learning rate may cause the model to fail to converge. 180 DCTFs are prepared for each device to form a training set and the batch size is set to 90. During the identification phase, 45 DCTFs from an accessing device are sent to the discriminator to determine whether this device is legitimate.

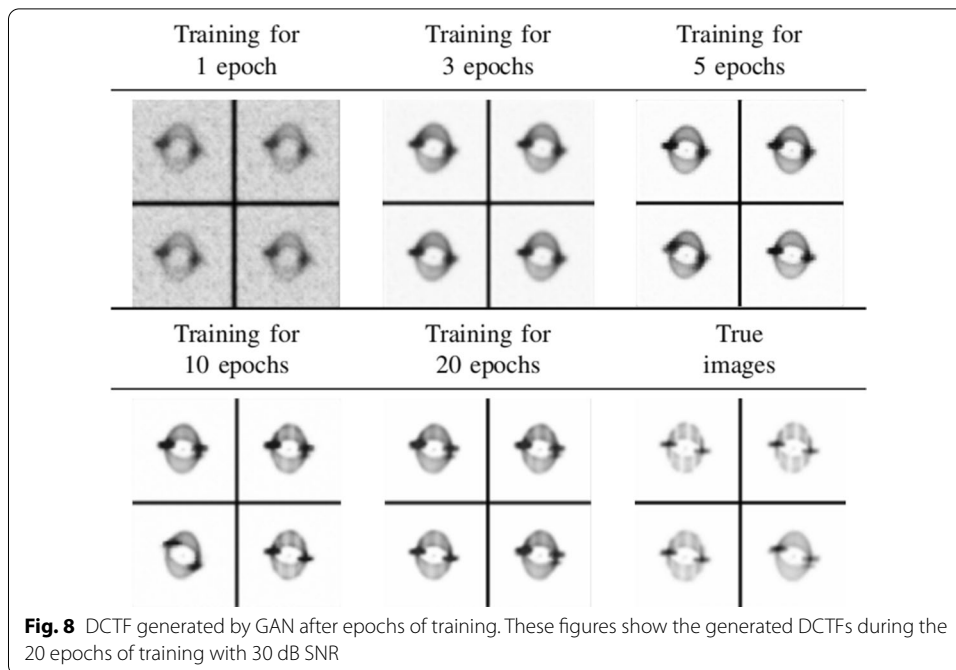
**Table 1** The network architectures of *NetG*

Layer	Output channels	Output dimension	Kernel, stride, padding	Parameters	Activation
<i>Input</i> — <i>x</i>	1	[64,64]	–	–	–
Convolution-2D	64	[32,32]	[4,4], 2, 1	1024	LeakyReLU
Convolution-2D	128	[16,16]	[4,4], 2, 1	131,072	–
BatchNorm-2D	128	[16,16]	–	256	LeakyReLU
Convolution-2D	256	[8,8]	[4,4], 2, 1	524,288	–
BatchNorm-2D	256	[8,8]	–	512	LeakyReLU
Convolution-2D	100	[5,5]	[4,4], 1, 0	409,600	Sigmoid
<i>Output</i> — <i>z</i>	100	[5,5]	–	–	–
Convolution transpose-2D	256	[8,8]	[4,4], 1, 0	409,600	–
BatchNorm-2D	256	[8,8]	–	512	ReLU
Convolution transpose-2D	128	[16,16]	[4,4], 2, 1	524,288	–
BatchNorm-2D	128	[16,16]	–	256	ReLU
Convolution transpose-2D	64	[32,32]	[4,4], 2, 1	131,072	–
BatchNorm-2D	64	[32,32]	–	128	ReLU
Convolution transpose-2D	1	[64,64]	[4,4], 2, 1	1024	Tanh
<i>Output</i> — <i>x'</i>	1	[64,64]	–	–	–
Convolution-2D	64	[32,32]	[4,4], 2, 1	1024	LeakyReLU
Convolution-2D	128	[16,16]	[4,4], 2, 1	131,072	–
BatchNorm-2D	128	[16,16]	–	256	LeakyReLU
Convolution-2D	256	[8,8]	[4,4], 2, 1	524,288	–
BatchNorm-2D	256	[8,8]	–	512	LeakyReLU
Convolution-2D	100	[5,5]	[4,4], 1, 0	409,600	–
<i>Output</i> — <i>z'</i>	100	[5,5]	–	–	–

**Table 2** The network architectures of *NetD*

Layer	Output channels	Output dimension	Kernel, stride, padding	Parameters	Activation
<i>Input</i>	1	[64,64]	–	–	–
Convolution-2D	64	[32,32]	[4,4], 2, 1	1024	LeakyReLU
Convolution-2D	128	[16,16]	[4,4], 2, 1	131,072	–
BatchNorm-2D	128	[16,16]	–	256	LeakyReLU
Convolution-2D	256	[8,8]	[4,4], 2, 1	524,288	–
BatchNorm-2D	256	[8,8]	–	512	LeakyReLU
Convolution-2D	1	[5,5]	[4,4], 1, 0	4,096	Sigmoid
<i>Output</i>	1	1	–	–	–

The weights of the latest *NetG* and *NetD* are saved after each epoch of training. During the 20 epochs of training with 30 dB SNR, the generated DCTFs are shown in Fig. 8. It can be seen that when the quantity of training epochs reaches a certain number, the position of gathering centers can be clearly distinguished although there is still a certain gap between the forged images and the real ones. In other words, the RF fingerprint characteristics of different devices have been adequately reflected in these



images. Correspondingly, the current discriminators should theoretically be able to distinguish DCTF generated by different devices.

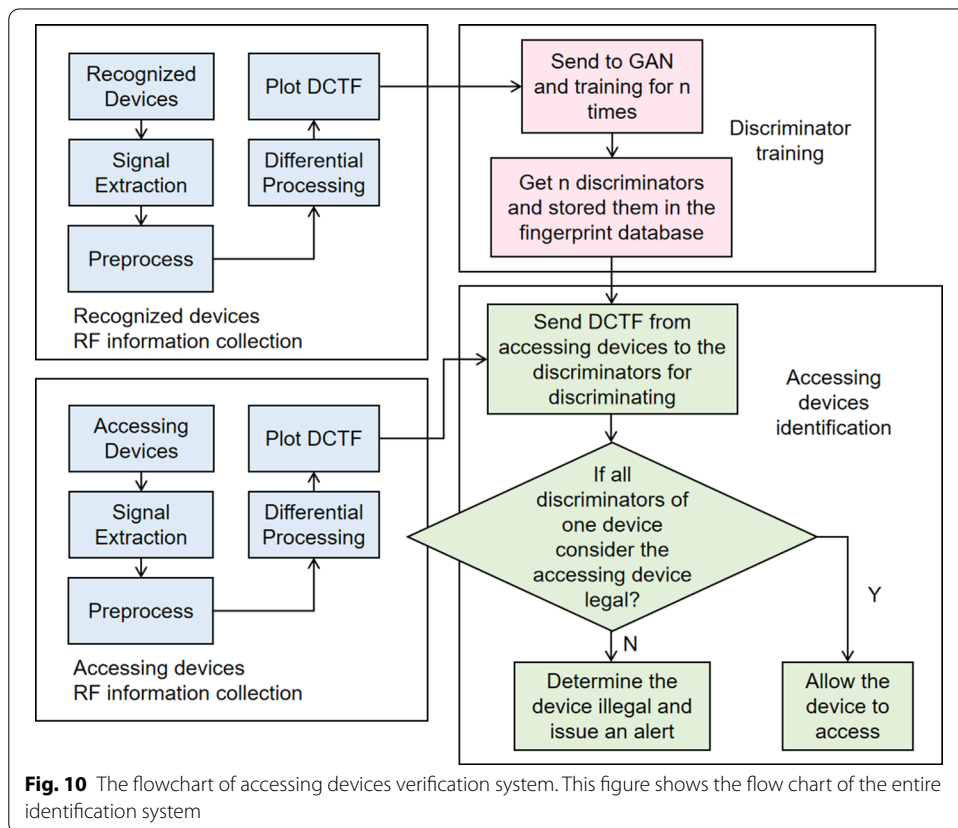
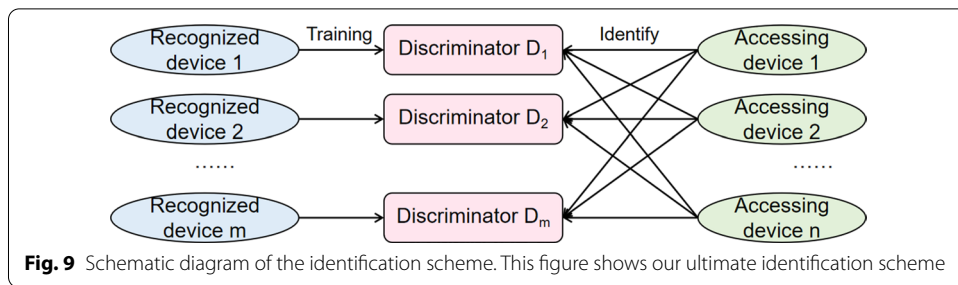
The similarity of these generated forged images represents the performance of the generator, while in the identification scheme proposed in this paper, the discriminator portion is mainly used.

In the experiment, we extract  $M$  devices as recognized ones and  $N$  devices as accessing ones. The DCTFs of one legitimate device are divided into two groups: the training set and the test set, while the DCTFs of a rogue device are only used in the test set. We only use the legal DCTFs to train the generators and the discriminators. After several epochs of training, the legal and illegal DCTFs in the test set are sent into the obtained discriminators for identification. It defines a real score for the input images according to the credibility of them. When the real score of an image exceeds the threshold, it is determined to come from a legitimate device.

### 4.3 Device identification

We first study the case when  $M = 1$  and  $N = 1$  since GAN is generally used to solve a two-class problem. In practical applications, this case assumes that in each time, only one accessing unknown device will imitate the legitimate device. This accessing unknown device will be sent to the GAN and the authenticity of its identity will be judged. Therefore, it is essentially a one-to-one identification issue. In this case, when  $M = 1$  legitimate device is selected, the residual  $54 - M$  devices are considered as rogue devices. In each identification, the target device  $N = 1$  and we evaluate the rogue device identification performance via  $54 - M$  times one-to-one identification.

We further extend the scheme to the case where  $M > 1$ ,  $N > 1$ . We select  $M$  ( $M > 1$ ) devices from 54 ZigBee modules as recognized devices, extracting their DCTF that are then sent to GAN for training. After training, we save the obtained



discriminators as fingerprints. Then we select  $N$  ( $N > 1$ ) ones as unknown devices. We send their DCTF to the discriminators in the fingerprint database in turn for identifying. If all the discriminators of one recognized device consider that an accessing device is legal, it is treated as a legitimate device. Our ultimate identification scheme is shown in Fig. 9 and can be described as follows:

- Train DCTFs of each recognized device to a discriminator as the fingerprint of each device, which are stored in the white list fingerprint database;
- The DCTFs of each accessing device are sent to the discriminator in the fingerprint database for identification. When one recognized device is considered as legitimate, it is allowed to access.



The flowchart of the entire identification system is shown in Fig. 10. As shown in the figure, the entire identification is consists of four main parts:

- *Recognized devices RF information collection* Extract the signal from recognized devices and perform pre-processing such as segmentation and normalization. Then differentially process it and plot DCTF.
- *Discriminator training* The DCTF from recognized devices are sent to GAN and training for multiple times to obtain multiple discriminators. These discriminators are stored in a database to discriminate DCTF from accessing devices.
- *Recognized devices RF information collection* Collect the signal from accessing devices and plot DCTF. This process is the same as plotting DCTF of recognized devices.
- *Accessing devices identification* The DCTF from accessing devices are sent to multiple trained discriminators for discrimination. An accessing device is allowed to access only if all the discriminators believe that it is legitimate. Otherwise, it is considered rogue.

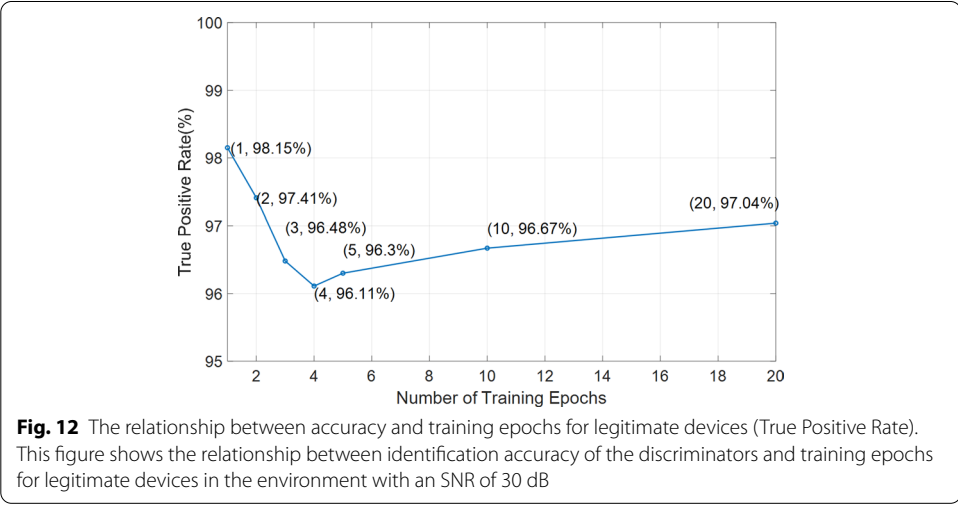
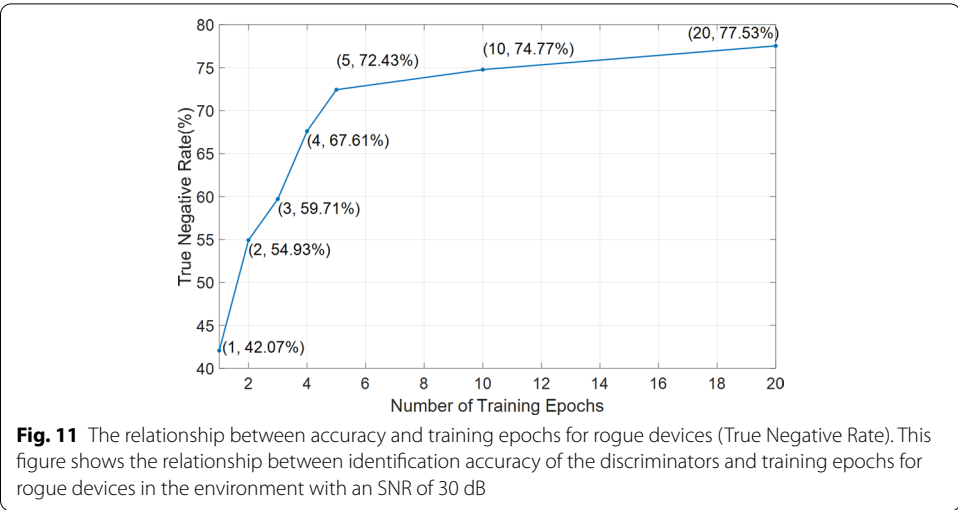
## 5 Experimental results and analysis

We change the training times for each pair of devices and the number of epochs per training in the same experimental environment to test the identification accuracy under different SNR conditions. The experiment is divided into two parts to test the accuracy of the proposed scheme to identify rogue and legitimate devices, respectively. The specific implementation of the two-part experiment is as follows:

- *Identification of rogue devices* From the 54 devices used in the experiment, one of them is selected as a recognized device whose DCTFs are used to train the discriminator. The remaining 53 are considered as rogue devices whose DCTFs are sent to the discriminator for identification in turn. In the following rogue device identification experiment, we conducted a round of aforesaid one-to-one experiments, that is, a total of  $54 \times 53 = 2862$  experiments under each condition to obtain the true negative rate of device identification under different conditions.
- *Identification of legitimate devices* From the 54 devices used in the experiment, the DCTF of one of the selected devices are divided into two sets. One training is used for training the discriminator, and one test set which is sent to the discriminator for testing. Since we only have 54 devices, the experimental results will lack universality if only one round of legitimate device identification experiments is carried out under each condition. Therefore, we conducted 10 rounds of repeated experiments, that is, a total of  $54 \times 10 = 540$  experiments under each condition to obtain the true positive rate under different conditions.

### 5.1 Identification accuracy analysis

We set the initial learning rate to 0.0002. The accessing device will be considered legal if 70% of the DCTF image set is judged to be from a recognized device. In the



environment with an SNR of 30 dB, the relationship between identification accuracy of the discriminators and training epochs are shown in Figs. 11 and 12, which are for rogue devices and legitimate devices, respectively.

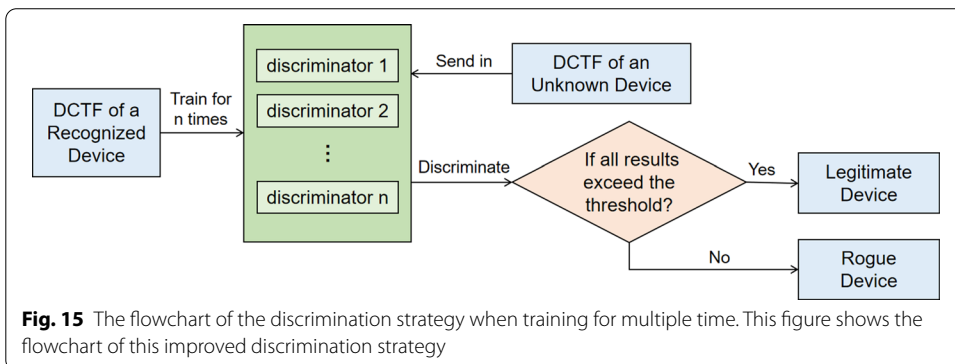
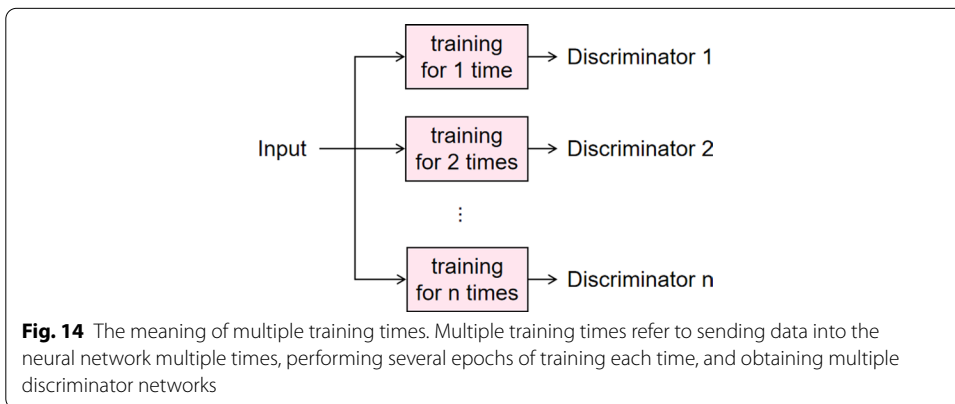
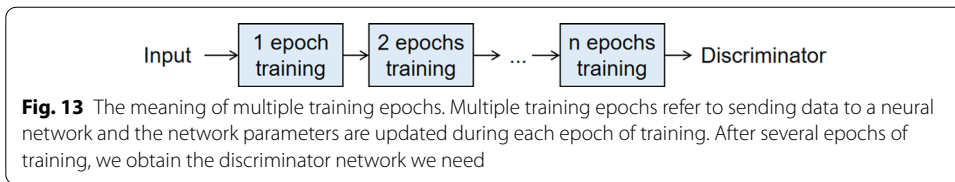
As can be found in the figure, however, when the accuracy for rogue devices exceeds 70%, it will hardly continue to rise as the number of training epochs rises. For legitimate devices, the identification accuracy is not visibly affected by the number of training epochs and can always above 96%. This is because the discriminators are more inclined to think that different DCTF sets come from the same device caused by the strong similarities of different DCTF.

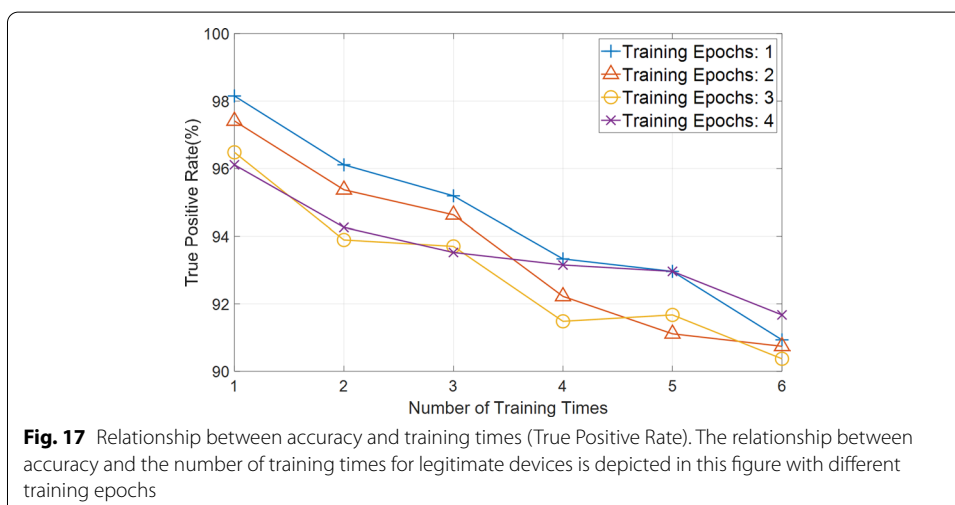
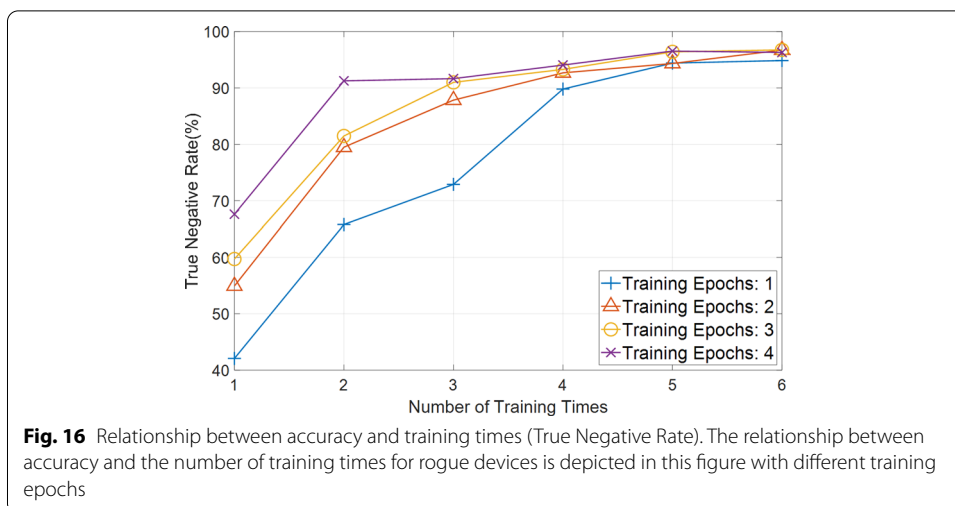
It is found through many experiments that one discrimination may misjudge the rogue device as a legitimate one, however, the probability of error in multiple discrimination is quite low. That is to say, we can train multiple times and get multiple discriminators for each device. Only when all discriminators of one certain device consider an accessing device to be legitimate, it is allowed to access.

The difference between the meanings of multiple training epochs and multiple training times can be described as follow:

- Multiple training epochs refer to sending data to a neural network and the network parameters are updated during each epoch of training. After several epochs of training, we obtain the discriminator network we need. Its block diagram is shown in Fig. 13.
- Multiple training times refer to sending data into the neural network multiple times, performing several epochs of training each time, and obtaining multiple discriminator networks. Its block diagram is shown in Fig. 14.

Another advantage of performing multiple training compared to performing one training for many epochs is that multiple training can be performed simultaneously and the number of epochs for each training is small, thereby effectively reducing the time cost. The flowchart of this improved discrimination strategy is shown in Fig. 15.



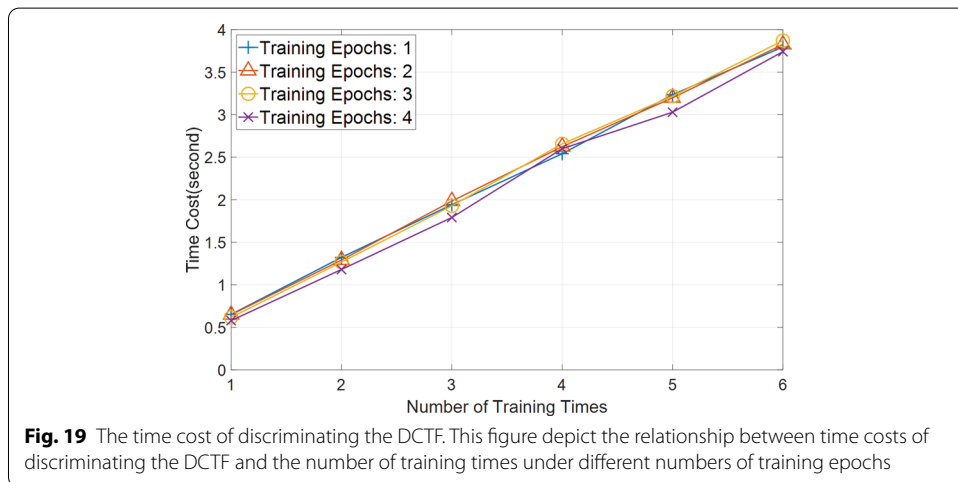
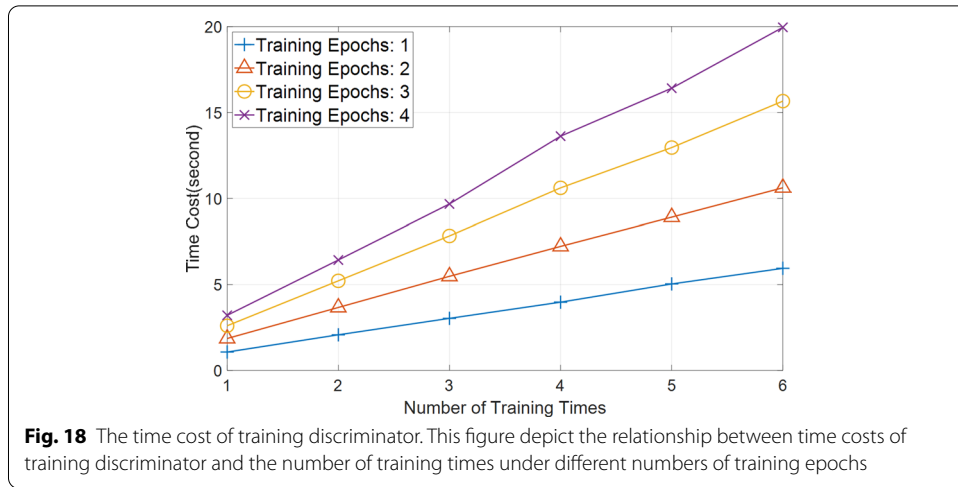


**5.2 Trade-off between rogue device detection and legitimate device acceptance**

We increase the number of training times with the other conditions remaining constant. The relationship between accuracy and the number of training times for rogue devices is depicted in Fig. 16 with different training epochs. It can be seen from the figure that the accuracy of identifying rogue devices can reach a degree of more than 90% when training 2 times and more than 95% when training 5 times at an SNR of 30dB.

The relationship between accuracy and the number of training times for legitimate devices under the same conditions is depicted in Fig. 17. It can be seen that the accuracy of legitimate devices decreases with the increase of training times. This is because a DCTF set is judged to be from a legitimate device only when it is deemed to be legal for every time of training.

The proposed discrimination strategy causes a trade-off between rogue device detection and legitimate device acceptance. The increase of training time will enhance the accuracy of rogue device detection while also resulting in a decrease in the accuracy of

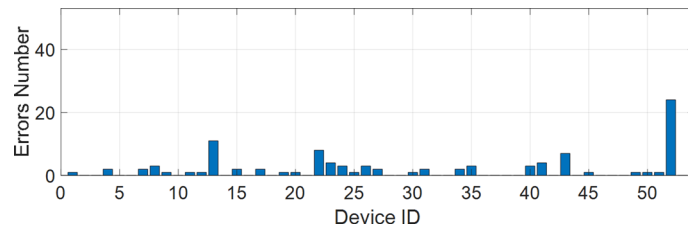


legitimate device acceptance. We should adjust the number of training to balance the true positive rate and true negative rate according to different needs.

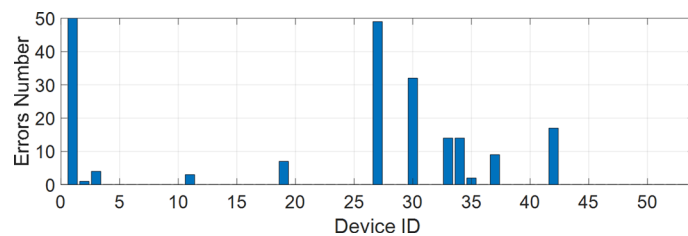
Figures 18 and 19 depict the relationship between time costs and the number of training times under different numbers of training epochs. It can be seen that the time costs of training discriminator are proportional to the product of the number of training times and the number of epochs, and the time costs of discriminating the DCTF are proportional to the number of training times.

### 5.3 Misjudged devices distribution

The number of identification errors for device 1 to device 54 under the conditions of training for 5 times and 4 epochs per time in a 30dB SNR environment are shown in Figs. 20 and 21. Figure 20 shows the number of errors that occurred when one device is selected as legal and the remaining 53 ones are selected as rogue devices in turn. Figure 21 shows the number of errors in 50 repeated experiments for each device in turn.



**Fig. 20** The number of errors for rogue devices. The figure shows the number of errors that occurred when one device is selected as legal and the remaining 53 ones are selected as rogue devices in turn



**Fig. 21** The number of errors for legitimate devices. The figure shows the number of errors in 50 repeated experiments for each device in turn

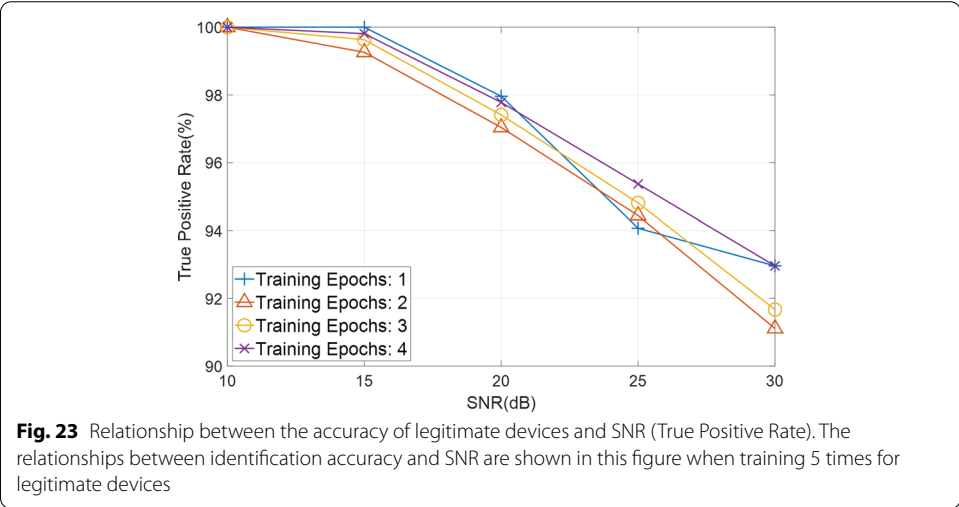
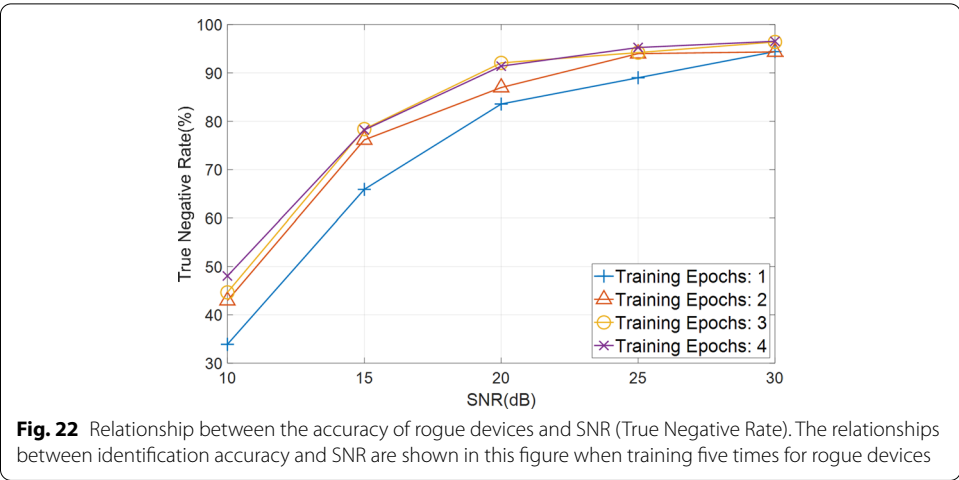
In these experiments, the training images set and test images set are extracted from the same device.

As can be seen from the figures, the distribution of the number of errors of each device is very uneven, especially in the experiments of legitimate devices identification. Some devices with insignificant characteristics, such as device 1 and device 27, the discrimination results are almost completely wrong. However, most of the testing device can be successfully recognized with our proposed method. For rogue devices identification, 96.3% of the devices can reach an accuracy of 80% and 92.6% of the devices can reach an accuracy of 90%. For legitimate devices identification, 88.9% of the devices can reach an accuracy of 80% and 85.2% of the devices can reach an accuracy of 90%.

#### 5.4 Influence of SNR on accuracy

Then we test the performance of our proposed scheme in low SNR scenarios. The relationships between identification accuracy and SNR are shown in Figs. 22 and 23 when training 5 times for rogue and legitimate devices respectively. The rogue devices can hardly be identified when the SNR is relatively low, while the accuracy of legitimate devices reaches 100% as can be seen from the figures. This is because the obtained DCTF is so blurry when serious noise is added. In this case, the discriminator can hardly distinguish rogue and legitimate DCTFs and judge them all from the same device.

To trade-off the accuracy for legitimate devices and rogue devices, the number of training times can be appropriately increased in a low SNR environment to increase the accuracy of rogue devices detection. Experiments show that when the training times exceed 20, the identification accuracy can reach 90% under the 15dB environment. However, the accuracy of legitimate devices will decrease in a high SNR environment. Therefore, to ensure the accuracy of both legitimate and rogue devices, the training times



should be decreased with the increase of SNR. It is because that the discriminator is more likely to recognize the difference between fingerprints when the SNR is high, thus helping to identify rogue devices. In contrast, the discriminator can not easily identify the difference between fingerprints when the SNR is low, so the misdiagnosis rate for rogue devices is increased. The improvement of training times makes the conditions of legitimate devices identification more stringent, thus counteracting the effect of low SNR.

**5.5 Accuracy analysis on multiple devices**

We further evaluate the accuracy when  $M, N > 1$ , where  $M, N$  are the numbers of recognized devices and accessing devices, respectively. The value of  $M$  ranges from 1 to 5 and  $N$  ranges from 2 to 5. We take 500 experiments for each pair of  $M$  and  $N$  and the experiments are taken under the conditions of training for 5 times and 4 epochs per time in a 30dB SNR environment.

In multiple device analysis, we randomly select  $M$  devices from 54 experimental devices as recognized devices. After that, we randomly select  $N$  devices from 54

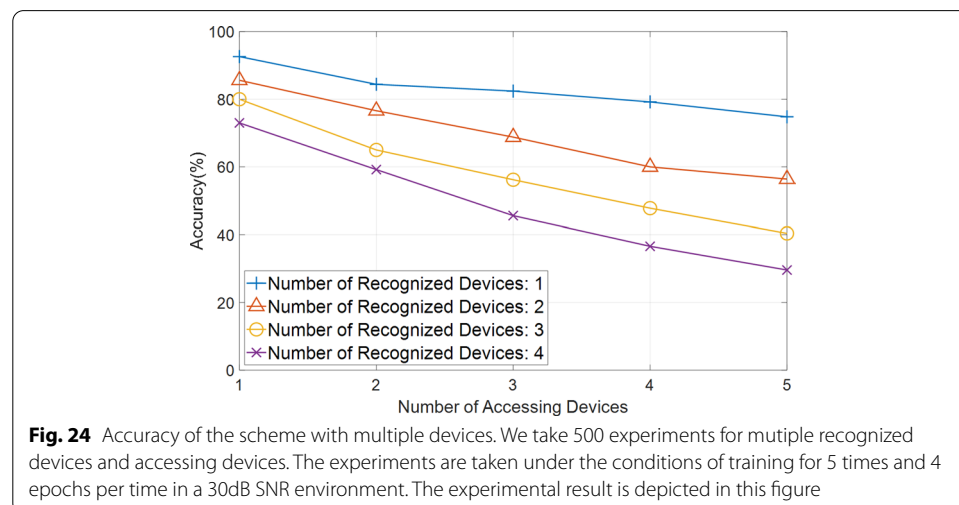
devices as accessing devices, which includes legitimate devices and rogue devices. For each experiment, the selection of  $M$  and  $N$  devices is also random. In this experiment, a device may appear in both the set of  $M$  recognized devices and  $N$  accessing devices. However, the DCTF images sets for training are different from that for testing though they may come from the same device. The evaluation has been taken by comparing the DCTF of the recognized devices and accessing devices one by one. Due to the reason that recognized devices have no prior information about accessing devices, if one of the recognized devices determines that the accessing device is legal, it will be permitted to access. The experimental result is depicted in Fig. 24.

In the situation of  $M = 1$ , it is reasonable that when  $N$  increases, the accuracy decreases and be proportional to the power of  $N$ . The accuracy of  $M = 1$  could be roughly  $P_1^N$ , where  $P_1$  is the accuracy with  $M = 1, N = 1$ . This means that although we can obtain near 95% successful chance to detect the attack when one device is used to access the network. The chance of successful detection will continuously decrease when more accessing devices are used. In addition, it is also reasonable that when recognized device number  $M$  increases, the accuracy dramatically decreases. The relationship of accuracy deterioration and recognized devices number  $N$  increase is even worse than the power of  $M$ . Although in our RF-based identification problem (not classification problem), 54 targets are employed for the experiment, which is the largest device number as we know. The evaluated result indicates that when more legitimate devices are employed in the system, the challenge of RF fingerprint-based accessing control will be more serious than we expected.

## 6 Conclusion and future work

### 6.1 Conclusion

This paper proposes an rogue device identification scheme for IoT system based on DCTF-GAN. In this scheme, we employ the obtained DCTF from accessing devices as the RF fingerprint feature. A completely unsupervised GANomaly model is designed to distinguish rogue devices only from legal DCTFs. To ensure the identification accuracy, a novel threshold selection algorithm and rogue device identification strategy are





also designed in our DCTF-GAN scheme. An experimental verification system is built with a total of 54 ZigBee devices regarded as  $M$  recognized devices and  $N$  accessing devices. We initially study the elemental one-to-one identification case with  $M = 1$  and  $N = 1$  and get an accuracy of over 95% for identifying accessing devices under a 30dB SNR environment. Moreover, the accuracy of rogue devices detection decreases, while the accuracy of legitimate devices identification increases in the low SNR scenario. In this situation, we find that classifiers can slightly adjust the number of training times to achieve a trade-off between legitimate and rogue devices detection rates. We further extend experiments to the case when  $M > 1$ ,  $N > 1$  by comparing each pair of recognized devices and accessing devices in turn. Experimental results show that when  $M > 1$  in our 54 devices identification problem, the accuracy of the DCTF-GAN dramatically decreases with the increased number of recognized devices.

## 6.2 Future work

The future work will focus on the study of design DCTF-GAN in  $M > 1$  situations. In addition, the fading of the wireless channel is negligible which does not have a special impact on the experimental results in the current experimental environment. We will further study the effect of fading on the identification accuracy in future work. Besides, an attacker may be able to design counterfeit fingerprint features after collecting DCTF fingerprints of legitimate devices. The method to resist this kind of attack will be our future research direction.

### Abbreviations

IoT: Internet of Things; RF: Radio frequency; GAN: Generative adversarial network; DCTF: Differential constellation trace figure; 2D: Two-dimensional; USRP: Universal software radio peripheral; SSID: Service set identifiers; IP: Internet protocol; MAC: Message authentication code; USIM: Universal subscriber identity module; ECC: Elliptic curve cryptography; DNA: Distinct and native attributes; LDA: Linear discriminant analysis; DAC: Digital-to-analog converter; WiMAX: World interoperability for microwave access; DRA: Dimensional reduction analysis; DWFP: Dynamic wavelet fingerprint; MDA: Multiple discriminant analysis; SVM: Support vector machines; KNN: K-nearest neighbor classifier; PCA: Principal component analysis; OCC: One-class classifiers; CNN: Convolutional neural network; AoQ: Amplitude of quotient; DNN: Deep neural network; PNN: Probabilistic neural network; MSCNN: Multi-sampling convolutional neural network; GRLVQI: Generalized relevance learning vector quantization-improved; HHT: Hilbert–Huang transform; IDS: Intrusion detection system; SNR: Signal-to-noise ratio; GSM: Global system for mobile communications; OQPSK: Offset quadrature phase-shift keying; DSSS: Direct sequence spread spectrum; DC: Direct current; CTF: Constellation trace figure; LSTM: Long short-term memory; DCGAN: Deep convolution generative adversarial network; AUC: Area under the curve; ROC: Receiver operating characteristic; TPR: True-positive rate; FPR: False-positive rate; LOS: Line-of-sight; AWGN: Additive white Gaussian noise; GPU: Graphics processing unit.

### Acknowledgements

Not applicable.

### Authors' contributions

ZC utilized DCTF to train the discriminators by GAN and verify the accuracy of the discriminators. In addition, he was responsible for writing the first draft of this paper. LP collected ZigBee signals and plotted DCTF to obtain the characteristics of different devices. In addition, he wrote part of this paper. AH and HF were responsible for the revision and polishing of this paper. All authors read and approved the final manuscript.

### Author information

**Zekun Chen** received the B.S. degree from School of Information Science and Engineering, Southeast University, China in 2019 and is currently pursuing the M.S. degree in School of Cyber Science and Engineering, Southeast University. His research interests include radio frequency fingerprint, physical layer security, and deep learning.

**Linling Peng** received his PhD degrees from IETR (Electronics and Telecommunications Institute of Rennes) laboratory at INSA (National Institute of Applied Sciences) of Rennes, France, in 2014. From 2014, he has been a research associate with Southeast University, China. His research interests include Internet of Things, physical layer security in wired and wireless communications.

**Aiqun Hu** received the PhD degree from Southeast University, China in 1993. He is a full Professor at Southeast University now. His research interests are in wireless network technology and physical layer security of wireless communications. He has published many papers on high-quality transactions and possessed many Chinese patents in wireless technology.

**Hua Fu** received the M.Eng. degree from the École nationale supérieure délectronique, informatique, télécommunications, mathématique et mécanique de Bordeaux(ENSEIRB-MATMECA), France, in 2011, and the Ph.D. degree from the National Institute of Applied Sciences (INSA), Rennes, France, in 2015, all in electrical engineering. She was with the Electrical and Computer Engineering Department, Université de Sherbrooke, QC, Canada, as a Postdoctoral Fellow. She is currently with the School of Cyber Science and Engineering, Southeast University, Nanjing, China, as a lecturer. Her research interests include multiple-input multiple-output (MIMO) systems with large antenna arrays, performance analysis of fading channels and physical layer security.

#### Funding

This work was supported in part by the National Natural Science Foundation of China under Grants 61941115, Jiangsu Province's key Research and Development Program under Grant BE2019109, Funding Supported: National key research and development program of China, Joint research of IoT security system and key technologies based on quantum key (2020YFE0200600) and in part by the Purple Mountain Laboratories for Network and Communication Security.

#### Availability of data and materials

The datasets used and/or analysed during the current study are available from the corresponding author on reasonable request.

#### Declaration

##### Competing interests

The authors declare that they have no competing interests.

##### Author details

<sup>1</sup> School of Cyber Science and Engineering, Southeast University, Nanjing, China. <sup>2</sup> Purple Mountain Laboratories, Nanjing, China. <sup>3</sup> School of Information Science and Engineering, Southeast University, Nanjing, China.

Received: 21 October 2020 Accepted: 11 March 2021

Published online: 01 April 2021

#### References

1. S. Baker, X. Wei, I. Atkinson, Internet of things for smart healthcare: technologies, challenges, and opportunities. *IEEE Access* **5**, 26521–26544 (2017)
2. Y. Zou, J. Zhu, X. Wang, L. Hanzo, A survey on wireless security: technical challenges, recent advances, and future trends. *Proc. IEEE* **104**(9), 1727–1765 (2016)
3. Z. Akram, M.A. Saeed, M. Daud, Real time exploitation of security mechanisms of residential WLAN access points, in *Proceedings of International Conference on Computing, Mathematics and Engineering Technologies (ICOMET)* (2018)
4. X. Huang, L. Shen, Y. Feng, A user authentication scheme based on fingerprint and USIM card, in *lihmsp 08 International Conference on Intelligent Information Hiding & Multimedia Signal Processing IEEE* (2008), pp. 1261–1264
5. K. Zhang, X. Liang, R. Lu, X. Shen, Sybil attacks and their defenses in the internet of things. *IEEE Internet Things J.* **1**(5), 372–383 (2014)
6. J. Lim, H. Oh, S. Kim, A new hash-based RFID mutual authentication protocol providing enhanced user privacy protection, in *Proceedings of 4th International Conference on Information Security Practice and Experience (ISPEC)* (2008), pp. 278–289
7. D. He, S. Zeadally, An analysis of RFID authentication schemes for internet of things in healthcare environment using elliptic curve cryptography. *IEEE Internet Things J.* **2**(1), 72–83 (2015)
8. O. Ureten, N. Serinken, Wireless security through RF fingerprinting. *Can. J. Electr. Comput. Eng.* **32**(1), 27–33 (2007)
9. Q. Xu, R. Zheng, W. Saad, Z. Han, Device fingerprinting in wireless networks: challenges and opportunities. *IEEE Commun. Surv. Tuts* **18**(1), 94–104 (2016)
10. Y. Tu, Z. Zhang, Y. Li, C. Wang, Y. Xiao, Research on the internet of things device recognition based on RF-fingerprinting. *IEEE Access* **7**, 37426–37431 (2019)
11. D.A. Knox, T. Kunz, Practical RF fingerprints for wireless sensor network authentication, in *Proceedings of 8th International Conference on Wireless Communications and Mobile Computing (IWCMC)* (2012)
12. N. Nguyen, G. Zheng, Z. Han, R. Zheng, Device fingerprinting to enhance wireless security using nonparametric bayesian method, in *Proceedings of IEEE INFOCOM* (2011)
13. B. Danev, S. Capkun, Transient-based identification of wireless sensor nodes, in *Proceedings of International Conference on Information Processing in Sensor Networks (IPSN)* (2009)
14. A.C. Polak, C. Dolatshahi, D.L. Goeckel, Identifying wireless users via transmitter imperfections. *IEEE J. Sel. Areas Commun.* **29**(7), 1469–1479 (2011)
15. D.R. Reising, M.A. Temple, J.A. Jackson, Authorized and rogue device discrimination using dimensionally reduced RF-DNA fingerprints. *IEEE Trans. Inf. Forensics Secur.* **10**(6), 1180–1192 (2015)
16. G. Li, J. Yu, Y. Xing, A. Hu, Location-invariant physical layer identification approach for WiFi devices. *IEEE Access* **7**, 106974–106986 (2019)
17. C. Bertoincini, K. Rudd, B. Noursain, M. Hinders, Wavelet fingerprinting of radio-frequency identification (RFID) tags. *IEEE Trans. Ind. Electron.* **59**(12), 4843–4850 (2012)

18. V. Brik, S. Banerjee, M. Gruteser, S. Oh, Wireless device identification with radiometric signatures. *14th ACM International Conference on Mobile computing and networking (MobiCom)* (2008)
19. H.J. Patel, M.A. Temple, R.O. Baldwin, Improving zigbee device network authentication using ensemble decision tree classifiers with radiofrequency distinct native attribute fingerprinting. *IEEE Trans. Reliab.* **64**(1), 221–233 (2015)
20. P. Robyns, E. Marin, W. Lamotte, P. Quax, D. Singele, B. Preneel, Physical-layer fingerprinting of LoRa devices using supervised and zero-shot learning, in *Proceedings of ACM Conference on Security Privacy in Wireless and Mobile Networks (WiSec)* (Boston, USA, 2017), pp. 58–63
21. Q. Tian, Y. Lin, X. Guo, J. Wen, Y. Fang, J. Rodriguez, S. Mumtaz, New security mechanisms of high-reliability IoT communication based on radio frequency fingerprint. *IEEE Internet Things J.* **6**(5), 7980–7987 (2019)
22. B. Kroon, S. Bergin, I. Kennedy, G.O. Zamora, Steadystate RF fingerprinting for identity verification: one class classifier versus customized ensemble, in *Conference on Artificial Intelligence and Cognitive Science* (2010)
23. H. Ye, G.Y. Li, B.H.F. Juang, Power of deep learning for channel estimation and signal detection in OFDM systems. *IEEE Wirel. Commun. Lett.* **7**, 114–117 (2017)
24. J. Bassey, D. Adesina, X. Li, L. Qian, A. Aved, T. Kroecker, Intrusion detection for IoT devices based on RF fingerprinting using deep learning, in *4th International Conference on Fog and Mobile Edge Computing (FMEC)* (2019)
25. M. Schmidt, D. Block, U. Meier, Wireless interference identification with convolutional neural networks. [arXiv:1703.00737](https://arxiv.org/abs/1703.00737) (2017)
26. K. Merchant, S. Revay, G. Stantchev, B. Noursain, Deep learning for RF device fingerprinting in cognitive communication networks. *IEEE J. Sel. Top. Signal Process.* **12**(1), 160–167 (2018)
27. Q. Li, H. Fan, W. Sun, J. Li, L. Chen, Z. Liu, Fingerprints in the air: unique identification of wireless devices using RF RSS fingerprints. *IEEE Sens. J.* **17**(11), 3568–3579 (2017)
28. M. Kose, S. Tascioglu, Z. Telatar, RF fingerprinting of IoT devices based on transient energy spectrum. *IEEE Access* **7**, 18715–18726 (2019)
29. Y. Pan, S. Yang, H. Peng, T. Li, W. Wang, Specific emitter identification based on deep residual networks. *IEEE Access* **7**, 54425–54434 (2019)
30. L. Peng, J. Zhang, M. Liu, A. Hu, Deep learning based RF fingerprint identification using differential constellation trace figure. *IEEE Trans. Veh. Technol.* **69**(1), 1091–1095 (2020)
31. J. Yu, A. Hu, G. Li, L. Peng, A robust RF fingerprinting approach using multisampling convolutional neural network. *IEEE Internet Things J.* **6**(4), 6786–6799 (2019)
32. J. Yu, A. Hu, G. Li, L. Peng, A multi-sampling convolutional neural network-based RF fingerprinting approach for low-power devices, in *IEEE INFOCOM 2019—IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)* (2019)
33. A. Al-Shawabka, F. Restuccia, et al., Exposing the fingerprint: Dissecting the impact of the wireless channel on radio fingerprinting, in *IEEE INFOCOM 2020—IEEE Conference on Computer Communications Workshops* (2020)
34. G. Shen, J. Zhang, A. Marshall, L. Peng, X. Wang, Radio frequency fingerprint identification for LoRa using spectrogram and CNN, in *IEEE International Conference on Computer Communications* (2021)
35. L. Peng, A. Hu, Y. Jiang, Y. Yan, C. Zhu, A differential constellation trace figure based device identification method for ZigBee nodes, in *Proceedings of 8th International Conference on Wireless Communications & Signal Processing (WCSP)* (2016)
36. I.J. Goodfellow, J. Pouget-Abadie, M. Mirza, B. Xu, D. Warde-Farley, S. Ozair, A. Courville, Y. Bengio, Generative adversarial nets, in *Advances in Neural Information Processing Systems* (2014), pp. 2672–2680
37. S. Akcay, A. Atapour-Abarghouei, T.P. Breckon, GANomaly: semi-supervised anomaly detection via adversarial training. [arXiv preprint arXiv: 1805.06725](https://arxiv.org/abs/1805.06725) (2018)
38. A. Radford, L. Metz, S. Chintala, Unsupervised representation learning with deep convolutional generative adversarial networks, in *ICLR* (2016)
39. D. Berthelot, T. Schumm, L. Metz, BEGAN: boundary equilibrium generative adversarial networks. [arXiv: 1703.10717](https://arxiv.org/abs/1703.10717) (2017)
40. J. Zhu, T. Park, P. Isola, A.A. Efros, Unpaired image-to-image translation using cycle-consistent adversarial networks. [arXiv: 1703.10593](https://arxiv.org/abs/1703.10593) (2017)
41. A. Ferdowsi, W. Saad, Generative adversarial networks for distributed intrusion detection in the Internet of Things, in *Proceedings of the IEEE Global Communications Conference (GLOBECOM), Communication & Information System Security Symposium* (Waikoloa, HI, USA, 2019)
42. L. Peng, A. Hu, J. Zhang, Y. Jiang, J. Yu, Y. Yan, Design of a hybrid RF fingerprint extraction and device classification scheme. *IEEE Internet Things J.* **6**(1), 349–360 (2019)
43. L. Peng, A. Hu, A design of deep learning based optical fiber ethernet device fingerprint identification system, in *IEEE International Conference on Communications (ICC)* (2019)
44. S. Wang, L. Peng, H. Fu, A. Hu, X. Zhou, A convolutional neural network-based RF fingerprinting identification scheme for mobile phones, in *IEEE INFOCOM 2020—IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)* (2020), pp. 115–120
45. Y. Jiang, L. Peng, A. Hu, S. Wang, Y. Huang, Physical layer identification of LoRa devices using constellation trace figure. *EURASIP J. Wirel. Commun. Netw.* (2019)
46. X. Zhou, A. Hu, G. Li, L. Peng, Y. Xing, J. Yu, A robust radio frequency fingerprint extraction scheme for practical device recognition. *IEEE Internet Things J.* (2021)

## Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.