Multi-Channel CNN-Based Open-Set RF Fingerprint Identification for LTE Devices

Pengcheng Yin, Linning Peng, *Member, IEEE,* Guanxiong Shen, *Member, IEEE,* Junqing Zhang, *Member, IEEE,* Ming Liu, *Member, IEEE,* Hua Fu, *Member, IEEE,* Aiqun Hu, *Senior Member, IEEE,* and Xianbin Wang, *Fellow, IEEE*

***Abstract*—Radio frequency fingerprint identification (RFFI) is a promising technique that exploits the transmitter-specific characteristics of the RF chain for identification. Disregarding its massive deployment, long-term evolution (LTE) systems have not fully benefited from RFFI. In this paper, an RFFI technique is designed to authenticate LTE devices. Three segments of the LTE physical layer random access channel (PRACH) preambles are captured, namely the transient-on, transient-off, and modulation parts. The segments are first converted into differential constellation trace figures (DCTFs), and then a specific type of neural network called multi-channel convolutional neural network (MCCNN) is used for identification. Additionally, the protocol is able to be applied for open-set identification, i.e., unknown device detection. Experiments are conducted with ten LTE mobile phones. The results show that the proposed RFFI scheme is robust against location changes. In the known device classification problem, the classification accuracy can reach 98.70% in the line-of-sight (LOS) scenario and 89.40% in the non-line-of-sight (NLOS) scenario. In the open-set unknown device detection problem, the identification equal error rate (EER) and area under the curve (AUC) reach 0.0545 and 0.9817, respectively, among six known devices and four unknown devices.**

***Index Terms*—LTE, Radio Frequency Fingerprint, Open-Set Recognition, MCCNN, Maxmin-loss**

I. Introduction

WITH dramatic evolution of the proliferation of wireless technologies, wireless communication has become an indispensable part of modern life. For instance, long-term evolution (LTE) systems have been deployed at a massive scale for our daily communication. According to the report of the global mobile suppliers association (GSA) in March 2022, the number of global LTE subscribers has reached 6.83 billion by the end of 2021, accounting for 67.1% of global mobile communication users [1].

While bringing great convenience to users worldwide, LTE networks are vulnerable to malicious attacks due to the broadcast nature of wireless transmissions [2]. Various security threats to LTE systems have been exposed. Most of them are due to the loophole of the protocol standard defined by 3GPP [3], especially the network access process [4]. Firstly, LTE networks are vulnerable to physical layer threats including radio frequency (RF) jamming, spoofing, and sniffing [5], [6]. Secondly, the LTE authentication protocol, i.e., the evolved packet system authentication and key agreement (EPS-AKA) protocol, is not sufficiently secured. More specifically, the EPS-AKA protocol relies on the international mobile subscriber identity (IMSI) and the encryption protocol in the universal subscriber identity module (USIM) card [7]. However, previous studies have demonstrated that USIM is subject to side-channel attacks [8]. Moreover, the EPS-AKA protocol also makes the LTE network vulnerable to denial of service (DoS) [9] attacks because the core network has to handle every access request from UEs [10], [11]. To prevent these attacks, a reliable device identification scheme is essential to enhance the security of the LTE network access process.

Radio frequency fingerprint identification (RFFI) is a physical layer security mechanism to authenticate wireless devices [12]. It performs identification by analyzing transmitter-specific distortion of the captured communication signal, which is caused by the minor deviation in the electronic components of a transmitter in the production process [13]. Applying RFFI to LTE systems can effectively reduce the risk of USIM cracking and device spoofing, and further prevent DoS attacks in the EPS-AKA process. Previous RFFI studies are mainly focused on identifying IoT devices, such as RFID [14]–[17], WiFi [18], LoRa [19], [20], ZigBee [21], [22], and

Manuscript received xxx; revised xxx; accepted xxx. Date of publication xxx; date of current version xxx. This work was supported in part by the National Key Research and Development Program of China (2022YFB4300300), National Natural Science Foundation of China under Grant 62171120, 62001106, 61971029, and 62221001, Jiangsu Provincial Key Laboratory of Network and Information Security No. BM2003201, Guangdong Key Research and Development Program under Grant 2020B0303010001, Chongqing Natural Science Joint Fund Project under Grant No. CSTB2023NSCQ-LZX0121, and Purple Mountain Laboratories for Network and Communication Security. The work of J. Zhang was in part supported by the UK Engineering and Physical Sciences Research Council (EPSRC) New Investigator Award under grant ID EP/V027697/1. For the purpose of open access, the authors have applied a Creative Commons Attribution (CC BY) licence to any Accepted Manuscript version arising. This paper was presented in part at the 2021 IEEE Global Communications Conference (GLOBECOM). The associate editor coordinating the review of this paper and approving it for publication was xx. (*Corresponding author: L. Peng.*)

P. Yin, L. Peng, G. Shen and H. Fu are with School of Cyber Science and Engineering, Southeast University, 210096 Nanjing, China. (e-mail: pcyin@aa.seu.edu.cn;pengln@seu.edu.cn;gxshen@seu.edu.cn;hfu@seu.edu.cn)

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

M. Liu is with the Engineering Research Center of Network Management Technology for High Speed Raiway of Ministry of Education, Collaborative Innovation Center of Railway Traffic Safety, Beijing Jiaotong University, Beijing, China. (email: mingliu@bjtu.edu.cn)

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

L. Peng, H. Fu, and A. Hu are also with the Purple Mountain Laboratories, Nanjing, 210096, China.

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

Digital Object Identifier xxx

Bluetooth [23]. For instance, Khadka *et al.* presented a robust technology for detecting RFID tags using both the amplitude and phase information of the frequency signature and used a deep learning model to prevent the cloning of tags [17]. Sankhe *et al.* showed how their feedback-driven transmitter-side modifications can increase differentiability for bit-similar WiFi devices on fingerprinting identification problem [18]. Aghnaiya *et al.* extracted higher-order statistical features to identify Bluetooth devices [23]. In the meanwhile, authentication of cellular devices is largely neglected. There have been some recent efforts attempting to identify mobile phones using their global system for mobile communication (GSM) signals [24]–[28]. Disregarding its massive deployment scale, RFFI for LTE systems has not been fully explored, with only very few attempts [29].

Existing RFFI studies usually leverage the advanced deep learning technique for its superior feature extraction capability [18], [30]. However, most of them focus on closed-set classification problems, which means the system can only identify devices that are present in the training stage. An unknown device is always misclassified as an existing class with the most similar features. This is unacceptable for security systems because malicious devices can never be accessed during training. There should be a mechanism to reject malicious/unknown wireless devices getting access to the network. Specifically, an RFFI system should implement the following functionalities:

- *Known Device Classification*: Classifying a known device that has been trained and registered before. This is a traditional multi-class classification problem with the closed-set assumption.
- *Unknown Device Detection*: Identifying an unknown device, which is an open-set recognition problem [31].

There have been some studies investigating the open-set RFFI system, e.g., One vs All (OvA) [32], OpenMax [32], heuristics for slices [33], generative adversarial network (GAN) [34], instance-generation-based methods [35], [36], and deep metric learning-based approach [19]. Specific to LTE-RFFI systems, current studies only consider the case of closed-set *known device classification* and their performance under open-set recognition is unknown.

In this paper, an open-set RFFI scheme is proposed to identify LTE devices, which can be employed for both *known device classification* and *unknown device detection* tasks. The designed RFFI system can detect the presence of an unknown/malicious mobile phone, and further predict the identity of the known/legitimate phone. The transient-on, transient-off, and modulation parts of the LTE PRACH preamble are exploited to generate separate DCTFs to improve the RFFI performance, considering the overlap of transient and modulation parts and the inhibition of the visibility of transient characteristics in a single DCTF. The RFF is extracted from PRACH preambles to ensure that the device identification is done before the device establishes connections to the core network to prevent attacks. A multi-channel convolutional neural network scheme, namely MCCNN, is designed that takes DCTFs as the input for the LTE device identification. To enhance the unknown device detection ability of the RFFI system, a custom loss function called maxmin-loss is proposed to ensure that the neural network learns a mapping where the feature representations of the same device are close to each other, while those from different devices are separated farther. Experiments are conducted using multiple LTE mobile phones and a software-defined radio (SDR) platform to emulate LTE eNodeB. The main contributions of this work are summarized as follows.

- A multi-DCTF-based RFFI protocol is proposed. More specifically, we convert the transient-on, modulation, and transient-off parts of the LTE PRACH signal into three DCTFs, respectively. Then the MCCNN is specially designed for identification, which extracts features from the three DCTFs separately and then combines them to achieve a higher identification accuracy.
- We propose an open-set approach for LTE-RFFI systems. It first detects whether the received signal is from an unknown device. If it is determined that the signal is not from an unknown device, the RFFI system will further classify the received signal. To the best knowledge of the authors, it is the first work considering the RFF open-set recognition for LTE mobile phones.
- To enhance the open-set RFFI performance, a custom loss function named maxmin-loss is designed to train the MCCNN along with the cross-entropy loss. It aims to cluster the intraclass representations while separating the interclass ones. Specific to RFFI, it can lead a relatively optimal performance on unknown device detection and known device classification at the same time with one model.
- The proposed LTE-RFFI system is evaluated with extensive experiments. A USRP N210 SDR platform was used to capture real-world transmissions from ten commercial-off-the-shelf (COTS) LTE mobile phones for evaluation. Experimental results show that the designed RFFI system can successfully detect unknown devices and classify the known devices with high accuracy. The area under the curve (AUC) of unknown device detection reaches 0.9817 and the accuracy for known device classification reaches 98.70%.

The DCTF-based MCCNN scheme for closed-set LTE device classification has been proposed in our prior work [37]. In this work, we extended it to the open-set unknown device detection. The signal preprocessing and DCTF generation details are introduced and more extensive experiments are carried out in this paper.

The rest of the paper is organized as follows. Section II gives an introduction to the LTE PRACH signal. Section III illustrates the system overview. Section IV introduces the signal preprocessing methods. Section V and Section VI present the designed multi-DCTF and open-set MCCNN-based LTE RFFI approaches. The experimental setup and results discussion are presented in Section VII. Section VIII introduces the related works in RFFI and LTE-RFFI. Section IX finally concludes the paper.

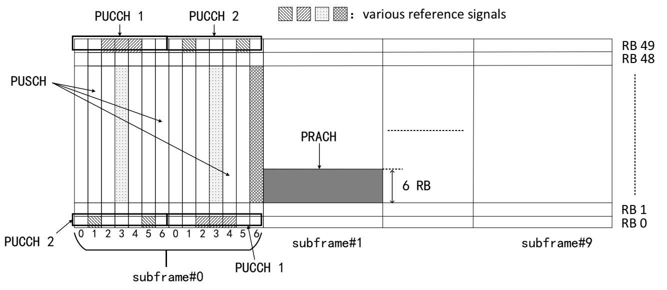


Fig. 1. The structure of LTE uplink physical channels and reference signals.

II. LTE PRACH Preliminary

The LTE uplink multiple access technologies are known as single-carrier frequency-division multiple access (SC-FDMA). The LTE PRACH is one of the uplink physical channels which carries the signal called random access preamble, i.e., PRACH preamble. The LTE PRACH occupies six resource blocks (RBs), spanning 1.08 MHz in the frequency domain. In addition to the PRACH, the uplink physical channels also include the physical uplink shared channel (PUSCH), the physical uplink control channel (PUCCH), and various reference signals. An example of LTE uplink physical channels and reference signals with 50 RBs is shown in Fig. 1.

Among PRACH, PUSCH, and PUCCH, the PRACH preamble is more suitable for RFFI. Firstly, the PRACH occupies less bandwidth compared to PUSCH, which is less affected by the multi-path effect of wireless channels. Secondly, the PRACH location is stable when the eNodeB parameters are determined, while the PUCCH location can change frequently because of the employed frequency hopping mechanism. Moreover, when a phone accesses an LTE network, the PRACH preamble is the first transmitted signal in the radio resource control (RRC) connection without any identity information. Moreover, a PRACH spoofing attack might be feasible while the 3GPP specifications do not specify the countermeasures in this situation [38]. The introduction of RFFI based on PRACH can offer a potential workaround.

The RFFI system proposed in this work identifies devices by analyzing the physical layer characteristics of PRACH preambles. The PRACH preamble consists of a cyclic prefix (CP) and a sequence part, which is generated by one or several root Zadoff-Chu sequences. The u^{th} Zadoff-Chu root sequence $x^u[n]$ is defined as

$$x^u[n] = e^{-j\frac{\pi u n(n+1)}{N_{ZC}}}, \tag{1}$$

where N_{ZC} is the length of $x^u[n]$ which equals 839 in an LTE frequency division duplex (LTE-FDD) system. The index u ranges from 1 to 838 according to the eNodeB setup. In each eNodeB with u^{th} root sequence, 64 different PRACH preambles could be generated using the following function

$$x_v^u[n] = x^u[(n + C_v) \bmod N_{ZC}], \tag{2}$$

where C_v is the cyclic shift value of the v^{th} preamble defined by the eNodeB. The LTE terminals can randomly choose C_v and generate orthogonal PRACH preambles. The generated baseband PRACH preamble signal is given as

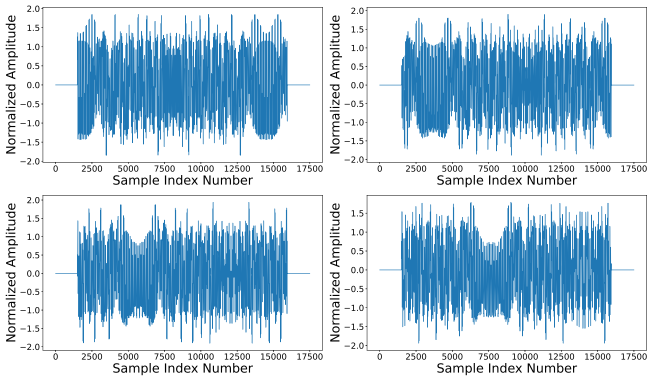


Fig. 2. An illustration of different PRACH preambles in one typical cell setup.

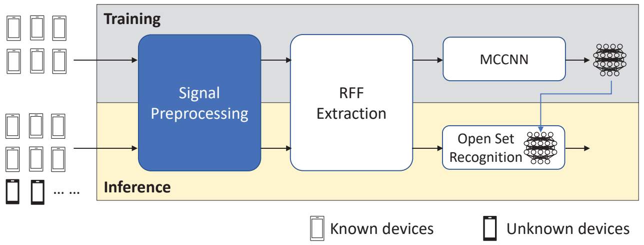


Fig. 3. System overview.

$$s(t) = \beta \sum_{k=0}^{N_{ZC}-1} X_v^u[k] e^{j2\pi(k+\varphi+\frac{\Delta f}{\Delta f_{RA}}(k_0+\frac{1}{2}))\Delta f_{RA}(t-T_{CP})} \tag{3}$$

where β is the amplitude gain factor, k_0 is used to determine the location in the frequency domain, Δf is the subcarrier interval of SC-FDMA symbols, Δf_{RA} is the subcarrier interval of PRACH preambles, and T_{CP} is the time duration of the cyclic prefix in the PRACH preamble. According to the setup in this work, Δf is 15 kHz, Δf_{RA} is 1.25 KHz and φ is seven. $X_v^u[k]$ represents the N_{ZC} points DFT of $x_v^u[n]$. Some example PRACH preambles are shown in Fig. 2.

III. System Overview

The system overview is illustrated in Fig. 3. The designed protocol consists of two stages, namely training and inference. In the training stage, we collect signals from available known devices. The signal preprocessing and collection algorithms are elaborated in Section IV. The RFFs, i.e., multiple DCTFs, are then extracted using the scheme presented in Section V. Finally, an MCCNN is trained with a custom loss function to predict the device identity. The design details can be found in Section VI. In the inference stage, the RFF is extracted from the received signal, and then the trained MCCNN can correctly predict from which device the signal is sent. Note that the RFFI system can first determine whether the signal is sent from a legitimate known device before predicting the device label. In other words, it has open-set recognition capability.

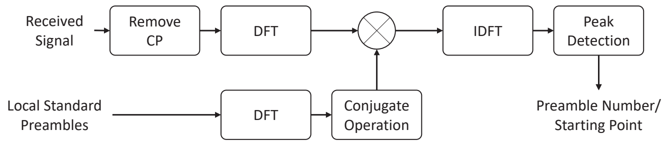


Fig. 4. Frequency domain correlation algorithm for fine time synchronization.

IV. Signal Preprocessing

This section describes the algorithm for LTE signal acquisition, which includes preamble detection, coarse and fine synchronization.

A. Preamble Detection

A sliding-window-based energy detection algorithm is applied to detect the presence of PRACH preambles, which is formulated as

$$\frac{A_{center}}{A_{sum}} > \lambda_{pd}, \tag{4}$$

where A_{sum} is the amplitude sum of the spectrum in the window, and A_{center} is the amplitude sum of the spectrum in the middle of the window. The preamble is detected when the result exceeds a pre-defined threshold λ_{pd}.

The detected PRACH preamble is filtered by an eighth-order Butterworth filter with a cut-off frequency of 1 MHz. Then its power is normalized. To reduce the computing complexity, the detected signal is down-sampled by a rate of 3/25, which is denoted as $r[n]$.

B. Time Synchronization

After a PRACH preamble is detected, the time synchronization algorithm is performed to accurately locate its starting point. It includes two steps, namely coarse and fine synchronization.

1) Coarse Time Synchronization: The coarse time synchronization is performed by detecting the peak in the correlation result $M[n]$ between duplicated CP and tail signal of the preamble sequence, given as

$$M[n] = \sum_{j=0}^{L_{CP}-1} r[n+j]r^*[n+j+L_{SEQ}], \tag{5}$$

where L_{CP} and L_{SEQ} are the lengths of the CP in the PRACH preamble and preamble sequence, respectively. The index of the start point d' is calculated by finding the peak in $M[n]$, expressed as

$$d' = \underbrace{\arg\max}_{n}(M[n]). \tag{6}$$

2) Fine Time Synchronization: A fine time synchronization is required since the coarse one is sensitive to multipath effects. The utilized fine time synchronization algorithm is based on the standard preamble correlation in the frequency domain, which is illustrated in Fig. 4.

Firstly the CP is removed according to the assumed start point d' and the rest of the signal is then converted to the frequency domain using DFT. The result is denoted as $R[w]$. Standard CP-free PRACH preambles are generated and converted to the frequency domain as well, denoted as $R_v^{std}[w]$, v is the preamble number.

The mobile phone would send one of the pre-defined 64 PRACH preambles in one access attempt. The correlation sequence can be expressed as

$$\begin{aligned}\boldsymbol{Corr^f}_v &= \left\{Corr^f{}_{v0}, Corr^f{}_{v1}, \cdots, Corr^f{}_{vj}\right\} \\ &= \text{IDFT}\left(R_v^{std*} \cdot R\right),\end{aligned} \tag{7}$$

where $v \in [0, 63]$, $j \in [0, N_{\text{SEQ}}-1]$. For each $\boldsymbol{Corr^f}_v$, the peak index can be calculated as

$$\text{Index}^p{}_v = \underbrace{\arg\max}_{j\in[0,N_{\text{SEQ}}-1]} \left|Corr^f{}_{vj}\right|. \tag{8}$$

Note Index^s is the peak index calculated by two standard preambles according to (7) and (8). Then the preamble number v' in the cell preamble set can be calculated as

$$v' = \underbrace{\arg\min}_{v\in[0,63]} \left|\text{Index}^p{}_v - \text{Index}^s\right|. \tag{9}$$

After obtaining the preamble number v', the fine starting point can be searched in the range of $[d'-N_s, d'+N_s]$ where N_s can be selected by prior knowledge. For $s \in [d'-N_s, d'+N_s]$, calculate that

$$\boldsymbol{Corr^f}_s = \text{IDFT}\left(R_{v'}^{std*} \cdot R_s\right), \tag{10}$$

where R_s is the DFT of $r\left[s+N_{\text{CP}}, s+N_{\text{CP}}+N_{\text{SEQ}}\right]$. The peak index in $\boldsymbol{Corr^f}_s$ can be expressed as

$$\text{Index}^p{}_s = \underbrace{\arg\max}_{j\in[0,N_{\text{SEQ}}-1]} \left|Corr^f{}_{sj}\right|. \tag{11}$$

Therefore, the estimated fine starting point d'' of the PRACH preamble can be calculated as

$$d'' = \left(\underbrace{\arg\min}_{s\in[d'-N_s,d'+N_s]} \left|\text{Index}^p{}_s - \text{Index}^s\right|\right) - N_s. \tag{12}$$

With the help of an estimated fine starting point, the transient parts of the received PRACH preamble can be extracted. Note that coarse time synchronization is required before fine time synchronization. This design can greatly narrow down the search range in fine time synchronization and effectively reduce the amount of computation.

The processed signals and corresponding labels are then saved in a training dataset $\mathcal{T}$, given as

$$\mathcal{T} = \{(y^m, l^m)\}_{m=1}^{M_{train}}, \tag{13}$$

where y^m is the m^{th} processed signal, i.e., I/Q samples, and l^m is the corresponding one-hot encoded device label.

V. Multi-DCTF

Previous work demonstrates that converting the received I/Q samples into an appropriate signal representation can enhance RFFI performance [20]. In this work, we designed multi-DCTF for LTE PRACH preambles as the input to the RFFI system.

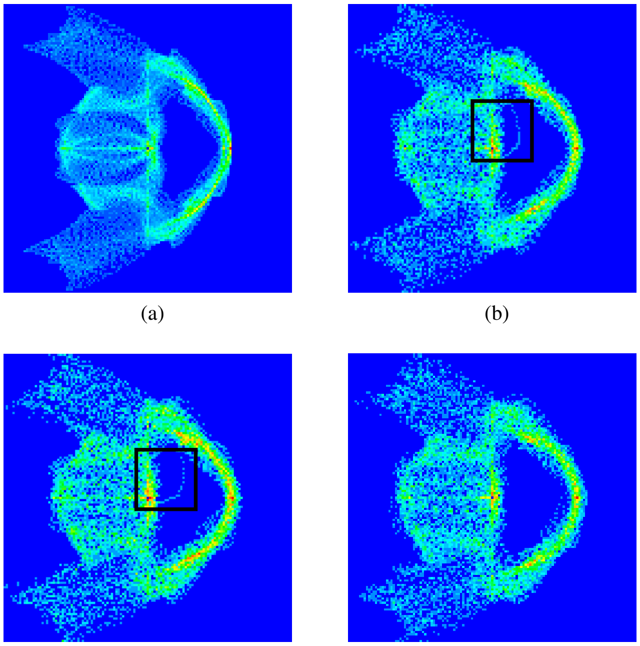


Fig. 5. DCTFs. (a) The DCTF of a standard preamble. (b)-(d) DCTFs of preambles from different real phones.

A. DCTF Generation

The DCTF is a specially designed feature in previous RFFI studies [21]. We first perform a differential operation on the received I/Q samples $y[n]$, given as

$$D[n] = y[n] \cdot y[n + L_{DF}], \tag{14}$$

where L_{DF} is the differential interval and $D[n]$ is the result which is a complex vector. $D[n]$ can then be mapped to the I/Q complex plane to generate a constellation diagram, namely DCTF. More specifically, a two-dimensional matrix Γ with a size of $[n \times n]$ is defined. The coordinate (i, j) of $D(t)$ in Γ is given by

$$\begin{aligned} i &= \left\lceil \frac{D_I[n] + T}{2T} \right\rceil \cdot n, \\ j &= \left\lceil \frac{D_Q[n] + T}{2T} \right\rceil \cdot n, \end{aligned} \tag{15}$$

where $D_I[n]$ and $D_Q[n]$ are real and imaginary part of $D[n]$, respectively. Then the DCTF can be generated by the density of the sampling points in each pixel $\Gamma[i, j]$.

B. Multi-DCTF Generation

Fig. 5 illustrates DCTFs. Fig. 5a is transformed from the simulated standard PRACH preamble, while Figs. 5b, 5c, and 5d are generated from the real collected ones. As illustrated in the figures, there are thin curves in the central of Fig. 5b and Fig. 5c (highlighted in the box), which is converted from the signal transient part. In contrast, the thin curves do not exist in Fig. 5a and Fig. 5d. For Fig. 5a, the reason is that there is no transient part in the simulated standard PRACH preamble. While for Fig. 5d, this is probably because the trace of the transient part is similar to that of the modulation part and is therefore obscured. In addition, the transient part may be faded and be suppressed after normalization and mapping of the most concentrated regions in the entire 2D plane [37]. Since the transient part has much fewer samples compared to the modulation part. For example, as shown in Fig. 6, the length of transient parts is less than 100 while the signal modulation part contains 14450 samples. Hence, it is necessary to process the transient and modulation parts in DCTF separately to make full use of the signal transient part.

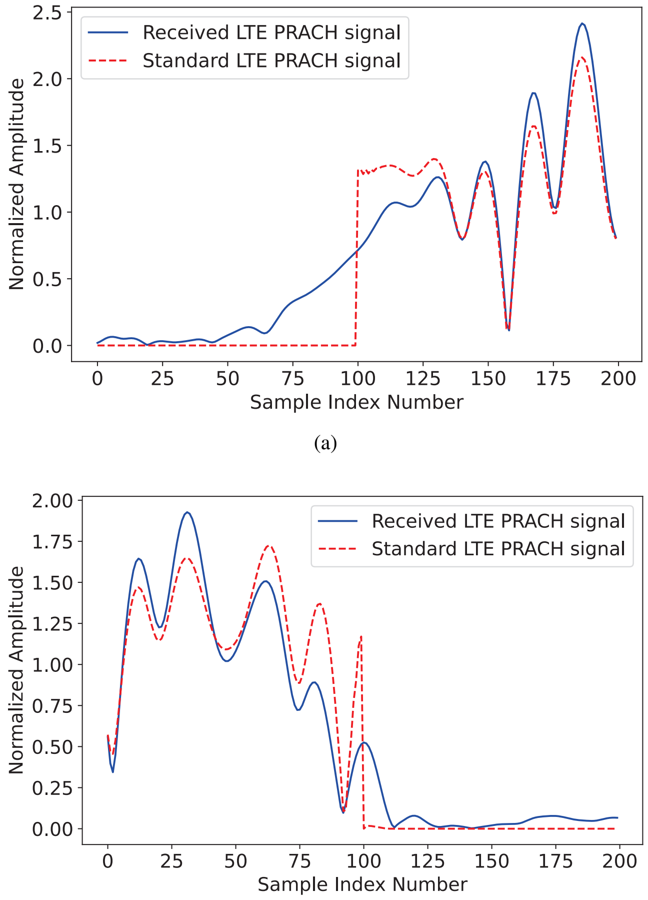
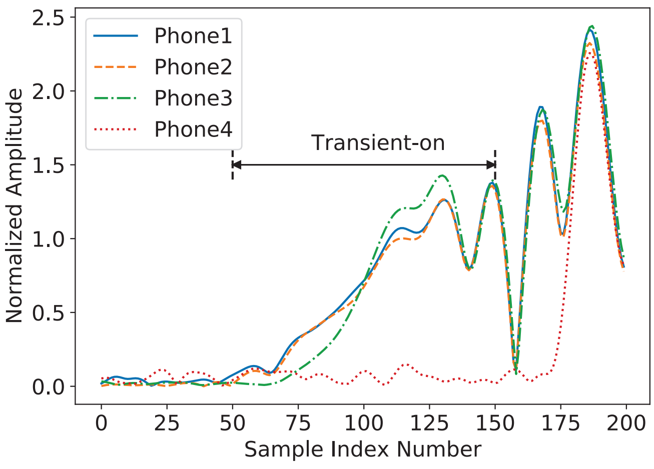


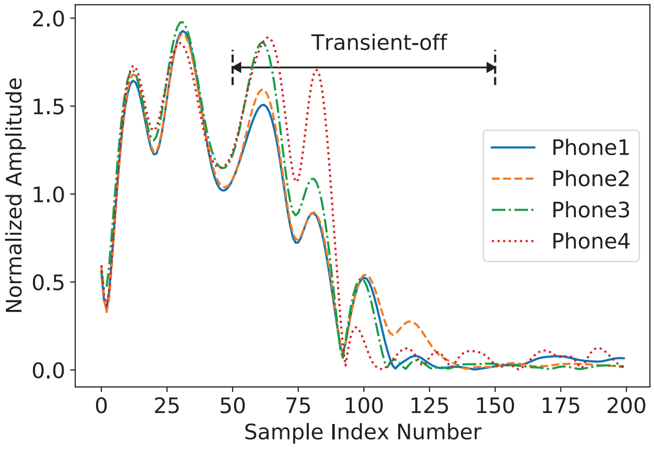
Fig. 6. An illustration of LTE PRACH transient parts (a) Transient-on part. (b) Transient-off part.

Fig. 7 demonstrates the transient-on and off waveforms from four different phones. It is obvious that the transient parts vary among LTE phones. As annotated in Fig. 7, the transient-on signal is constructed with samples from index 50 to index 150, where the starting point of the packet is index 100. After we detect the signal ending point, we will take a segment. As illustrated in Fig. 7, the ending point of the packet in the segment is index 100, and the transient-off signal is created with samples from index 50 to index 150. Other parts are considered as modulation parts. Transient-on, transient-off, and modulation parts of the LTE PRACH preamble are used to generate DCTFs respectively as shown in Fig. 8 for later recognition.

After multi-DCTF generation, the training dataset $\mathcal{T}$ can be

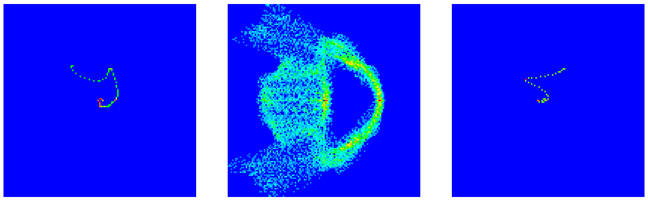


(a)



(b)

Fig. 7. Normalized amplitudes of PRACH preambles with the same preamble index from four different phones. (a) Transient-on waveforms (the starting point of the packet is index number 100). (b) Transient-off waveforms (the ending point of the packet is index number 100).



(a) (b) (c)

Fig. 8. DCTFs of different parts of the LTE PRACH preamble. (a) DCTF of the transient-on part. (b) DCTF of the modulation part. (c) DCTF of the transient-off part.

constructed as

$$\mathcal{T} = \{(\{\Gamma_{\text{on}}^m, \Gamma_{\text{mod}}^m, \Gamma_{\text{off}}^m\}, l^m)\}_{m=1}^{M_{train}}, \tag{16}$$

where Γ_{on}^m, Γ_{mod}^m, and Γ_{off}^m are DCTFs generated from the transient-on, modulation, and transient-off parts of y^m, respectively.

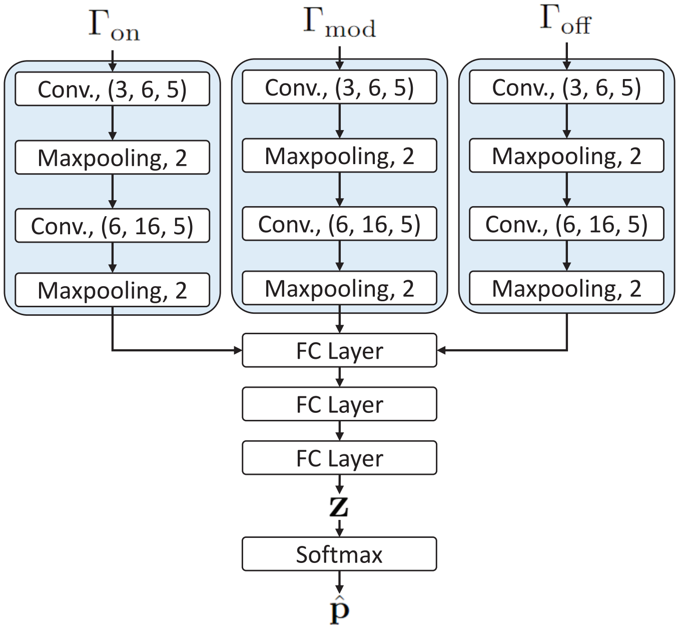


Fig. 9. Architecture of the MCCNN.

VI. MCCNN Based LTE Device Identification

A. Neural Network Architecture

An MCCNN is proposed as a feature extractor to process the multi-DCTF, whose architecture is shown in Fig. 9. The three DCTFs, $\{\Gamma_{\text{on}}, \Gamma_{\text{mod}}, \Gamma_{\text{off}}\}$, act as different MCCNN input channels. The output of the three convolutional branches is flattened and concatenated as a 1D vector, which is then processed by three fully connected (FC) layers. The output of the third FC layer, denoted as $\mathbf{z} = \{z^1, ..., z^k, ..., z^K\}$, is deemed to be the feature representations extracted from the multi-DCTF input. K is the number of categories. After that, a softmax function is applied to convert $\mathbf{z}$ to a probability vector $\hat{\mathbf{p}} = \{\hat{p}^1, ..., \hat{p}^k, ..., \hat{p}^K\}$, which is mathematically given as

$$\hat{p}^k = \frac{e^{z^k}}{\sum_{k=1}^{K} e^{z^k}}. \tag{17}$$

B. Loss Function

We designed a combined loss function to train the proposed MCCNN, which is composed of cross entropy and maxmin losses. Cross entropy loss is often used to train a classification neural network, given as

$$\mathcal{L}_{CE} = -\sum_{k=1}^{K} p^k \log(\hat{p}^k), \tag{18}$$

where $\mathcal{L}_{CE}$ is the cross entropy loss function, $p^k = \{1 \text{ if sample belongs to category } k, 0 \text{ otherwise}\}$. Note that it aims to distinguish representations among different categories but not to cluster intraclass representations or to separate interclass representations. The output probability vector $\hat{\mathbf{p}}$ is leveraged for classification, which does not mean that the distances among different categories are large when the classification probability is maximized. Therefore, the cross-entropy loss cannot lead to discriminative representations that are well separated among categories, which can be further improved.

The maxmin loss is proposed to learn discriminative representations, which is inspired by the work in [39], [40]. It is anticipated that during the training stage, intraclass representations will be clustered and interclass representations will be separated. We define the mean maximal intraclass distance d_{max} in feature representations as

$$d_{\text{max}} = \frac{1}{K}\sum_{k=1}^{K} \max_{\mathbf{z}_i \in C_k} \|\mathbf{z}_i - \mathbf{u}_k\|_2, \tag{19}$$

where $\mathbf{u}_k$ is the mean feature representation of category C_k, given as

$$\mathbf{u}_k = \frac{1}{|C_k|}\sum_{i=1}^{|C_k|} \mathbf{z}_i, \tag{20}$$

where $|C_k|$ denotes the number of training instances in category C_k. We define the minimal interclass distance d_{min} as the distance between the closest two categories

$$d_{\text{min}} = \min_{\substack{1 \le a \le K \\ a+1 \le b \le K}} \|\mathbf{u}_a - \mathbf{u}_b\|_2. \tag{21}$$

Then the maxmin loss $\mathcal{L}_{MM}$ is defined as

$$\mathcal{L}_{MM} = \frac{d_{\text{max}}}{d_{\text{min}}}. \tag{22}$$

The cross-entropy and maxmin losses are finally combined to train the designed MCCNN, given as

$$\mathcal{L}_{comb} = \mathcal{L}_{CE} + \alpha \mathcal{L}_{MM}, \tag{23}$$

where $\mathcal{L}_{comb}$ is the combined loss and α is a hyperparameter that determines the weight between cross entropy and maxmin loss, which is set to 0.5 in this paper.

C. Open-Set Recognition

With the learned well-separated feature representations, the open-set recognition task can be performed by distance measurement. Mahalanobis distance is adopted in the proposed RFFI system, given as

$$d_j = \sqrt{(\mathbf{z} - \mathbf{u}_j)^T \Sigma_j^{-1} (\mathbf{z} - \mathbf{u}_j)}, \tag{24}$$

where Σ_j is the covariance matrix of $\mathbf{z}_j$ in the training instances. Then the similarity score S_f is defined as

$$S_f = \frac{\|d\|_2}{\min\limits_{1 \le j \le K} d_j}, \tag{25}$$

where d is the set of d_j. The decision can be made by comparing S_f with a pre-defined threshold λ, given as

$$\hat{C} = \begin{cases} \text{Unknown device}, & \text{when } S_f < \lambda \\ \operatorname*{argmax}_k(\hat{\mathbf{p}}), & \text{when } S_f \ge \lambda \end{cases} \tag{26}$$

where $\hat{C}$ is the predicted device label.

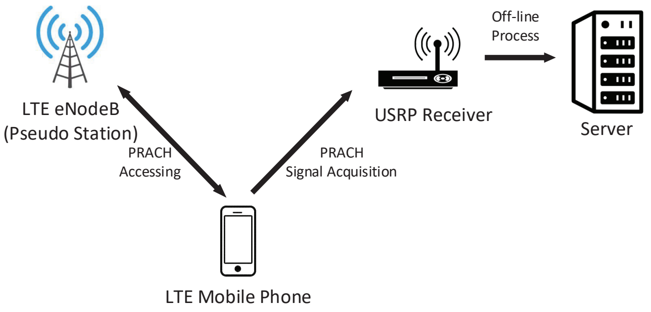


Fig. 10. Experimental setup. An LTE eNodeB pseudo station is established for communications between the LTE mobile phone. The USRP receiver is collecting PRACH preamble for RFFI.

Fig. 11. (a) Photo of the ten LTE mobile phones. (b) Photo of the pseudo-LTE eNodeB station and the USRP receiver.

VII. Experimental Evaluation

A. Experimental Setup

1) Experimental Hardware Settings: Fig. 10 shows the diagram of the designed experimental platform. The photos of experimental devices are shown in Fig. 11. The platform consists of three components, namely an LTE eNodeB station, some LTE mobile phones and a USRP receiver.

LTE eNodeB Station: We used a USRP B205 to build a pseudo-LTE eNodeB station with the open source srsLTE [41], which can establish communication links with LTE mobile phones. The uplink center frequency is set to 2,565 MHz, which is a spare frequency channel to avoid interference. The number of RB in the uplink channel is 50. The frequency domain offset is set to two, which means the preamble is at the edge of the uplink channel. Our pseudo eNodeB parameter setup makes sure that the available preambles are generated by one root sequence.

LTE Mobile Phones (DUTs): Ten COTS phones of four models are employed as devices under test (DUTs) to be identified, whose information is detailed in Table I. We consider phones 1-6 as known DUTs while the rest as unknown ones. The transmission of PRACH preambles is enabled by manually switching on/off the flight mode. The center frequency of PRACH preambles is calculated as 2,561.4 MHz according to the setup of the pseudo eNodeB station.

USRP Receiver: A USRP N210 SDR platform is used for signal collection for RFFI since the srsLTE-based pseudo-eNodeB station does not support access to physical layer signals. The center frequency of USRP N210 is set to 2,561.4 MHz, the same as the carrier frequency of PRACH

TABLE I
DUT INFORMATION

Category	Name	Model
Known DUTs	Phone 1	XIAOMI Redmi 5A
	Phone 2	Google Nexus 5
	Phone 3	Google Nexus 6P
	Phone 4	HUAWEI P9
	Phone 5	Google Nexus 5
	Phone 6	Google Nexus 5
Unknown DUTs	Phone 7	Google Nexus 5
	Phone 8	Google Nexus 5
	Phone 9	HUAWEI P9
	Phone 10	HUAWEI P9

TABLE II
DATASET INFORMATION

	DUT Index	Channel Condition	# Signals
Dataset 1	DUT 1 to 10	LOS	6,535
Dataset 2	DUT 1 to 10	NLOS	5,030
Dataset 3	DUT 1 to 6	LOS & NLOS	2,540

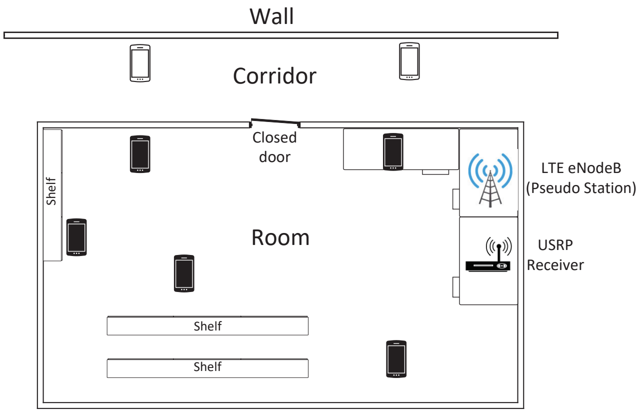


Fig. 12. Layout of the dataset collection environment.

preambles. The sampling rate of the USRP N210 platform is 20 MSamples/s.

2) Dataset Collection Settings: Three datasets are collected for different evaluation purposes, which are summarized in Table II. The layout of the dataset collection environment is illustrated in Fig. 12. Five collection positions are set for the LOS scenario, while two collection positions are set for the NLOS scenario.

Dataset 1 contains signals collected from DUT 1-10. The signal collection is carried out in an LOS scenario with a distance of less than 6 m. This dataset includes both known and unknown DUTs, which are used to evaluate the performance of unknown device detection described in Section VII-B. There are 6,535 preambles in total, among which 4,258 are from known DUTs and the rest 2,277 are from unknown DUTs.

Dataset 2 contains signals collected from DUT 1-10. The signal collection is carried out in an NLOS scenario with a distance of more than 10 m. This dataset includes both known and unknown DUTs, which are also used to evaluate the performance of unknown device detection described in Section VII-B. There are 5,030 preambles in total, among which 3,315 are from known DUTs and the rest 1,715 are from unknown DUTs.

Dataset 3 contains signals collected from DUTs 1-6. It only includes known DUTs and is thus mainly used to evaluate known device classification. The signal collection is conducted in both LOS and NLOS scenarios therefore the system robustness against channel variations can be evaluated as well. The distance between transceivers is 6 m and 13 m in LOS and NLOS scenarios, respectively. Dataset 3 is used to assess the known device classification performance in Section VII-C. There are 2,540 preambles in total. Among them, 1,946 preambles are collected in LOS scenarios and others are collected in NLOS scenarios.

3) Neural Network Training Settings: The training was carried out on a PC with Ubuntu 18.04 system and GeForce RTX 2080 Ti GPU. The PyTorch framework was used. During the training process, the Adam optimizer was used, the initial learning rate was 0.001 and the batch size was 64. For Unknown device detection, the number of epochs was set to 100 and for known device classification the number of epochs was 50 considering the dataset size.

B. Evaluation of Unknown Device Detection

1) Evaluation Metrics and Benchmarks: Essentially, unknown device detection is a binary classification problem. Accuracy is the most common performance metric, which is the proportion of correctly classified samples to the total number of samples. The receiver operating characteristic (ROC) curve is often used to evaluate unknown device detection [19], which shows the relationship between false positive rate (FPR) and true positive rate (TPR) under different threshold settings. It could reflect the performance of a learner based on weights of precision and recall. Two scalar metrics can be further derived from the ROC curve, namely AUC and equal error rate (EER). The AUC refers to the area under the plotted ROC curve and the EER is the location where the FPR equals 1-TPR. The larger the AUC or the smaller the EER, the better the unknown device detection performance.

We leverage the neural network proposed in [24] as the first benchmark for comparison. Additionally, OpenMax is applied to it to enable the open-set identification capability, which has been proven to be effective in RFFI [32], [42]. Finally, we use the designed maxmin loss to train the neural network as the third benchmark.

2) Results of Unknown Device Detection: Dataset 1 is leveraged to evaluate the unknown device detection performance. We aim to evaluate whether the RFFI system can successfully detect the signals sent from the unknown DUTs, i.e., Phone 7-10. The training and test data are summarized as follows:

- **Training**: Random 80% of the signals from DUTs 1-6, i.e., known DUTs, in Dataset 1.
- **Test**: All the remaining signals in Dataset 1, including signals from DUTs 1-10, i.e., known and unknown DUTs.

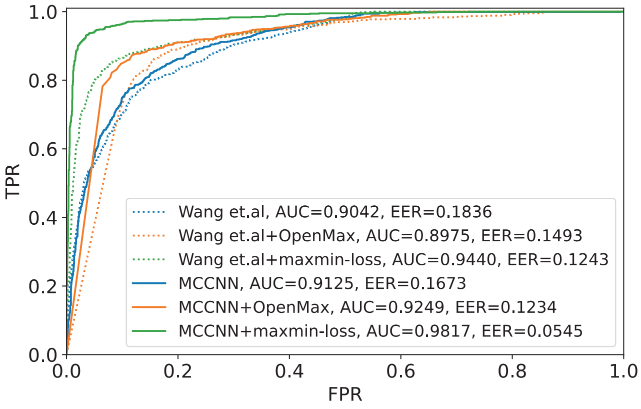


Fig. 13. ROC curves of unknown LTE device detection.

The ROC curves are shown in Fig. 13. OpenMax is based on the extreme value theory, correcting the softmax output of training process by fitting extreme value models. In contrast, MCCNN with maxmin loss trains the various parameters and updates them under the supervision of both softmax function and maxmin loss to drive the scheme to get high performance. It is clear that the proposed MCCNN with maxmin loss scheme reaches the best detection performance, with an AUC of 0.9817 and an EER of 0.0545.

3) Results Discussion at Various Scenarios: To evaluate unknown device detection performance at different levels of SNR, additive white Gaussian noise (AWGN) is added to the collected signals. The training and test data are detailed as follows:

- **Training**: Random 80% of the signals from DUTs 1-6, i.e., known DUTs, in Dataset 1. Different power levels of AWGN are used to create different SNR levels.
- **Test**: All the remaining signals in Dataset 1, including signals from DUTs 1-10, i.e., known and unknown DUTs. AWGN with different powers is added.

In order to evaluate the performance of the proposed method in the NLOS scenario, Dataset 2 is used. The details are as follows:

- **Training**: Random 80% of the signals from DUTs 1-6, i.e., known DUTs, in Dataset 2.
- **Test**: All the remaining signals in Dataset 2, including signals from DUTs 1-10, i.e., known and unknown DUTs.

The unknown device detection results are shown in Table III. OpenMax method is also evaluated for comparison. As can be observed from Table III, the scheme with the maxmin-loss has better unknown device detection performance than the OpenMax loss in both LOS and NLOS scenarios, i.e., the maxmin-loss approach achieved higher AUC and lower EER. The performances of both methods reduce when SNR decreases. One reason is that DCTF can be affected by the noise, as shown in Fig. 14. Compared to the high SNR scenario, the feature is significantly blurry.

4) The Effect of Maxmin-Loss: As discussed in Section VI-B, the proposed maxmin loss can decrease the intraclass while increasing the interclass distances relatively, leading to a better separation between the intraclass and interclass distance. Fig. 15 verifies this by showing the histogram of the normalized intraclass and interclass distances between the feature representations in the training dataset. It can be seen that after the application of maxmin loss, the feature representations of different categories are well separated, so an unknown device is more likely to be detected since it would tend to be away from all known categories in the feature space. And this leads to better performance in the unknown device detection problem.

TABLE III
LTE DEVICE DETECTION PERFORMANCES AT VARIOUS SCENARIOS

Scenario		MCCNN w/ maxmin-loss		MCCNN w/ OpenMax	
		AUC	EER	AUC	EER
LOS	40dB	0.9817	0.0545	0.9249	0.1234
	35dB	0.9421	0.1199	0.8857	0.1611
	30dB	0.8685	0.2108	0.7514	0.3509
	25dB	0.8546	0.2121	0.8503	0.2090
	20dB	0.8458	0.2257	0.7906	0.2683
NLOS	35dB	0.7531	0.2945	0.6231	0.4723
	30dB	0.7571	0.3044	0.6549	0.4496
	25dB	0.7050	0.3563	0.6092	0.5102
	20dB	0.5306	0.4659	0.5476	0.5393

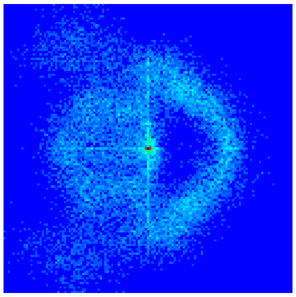


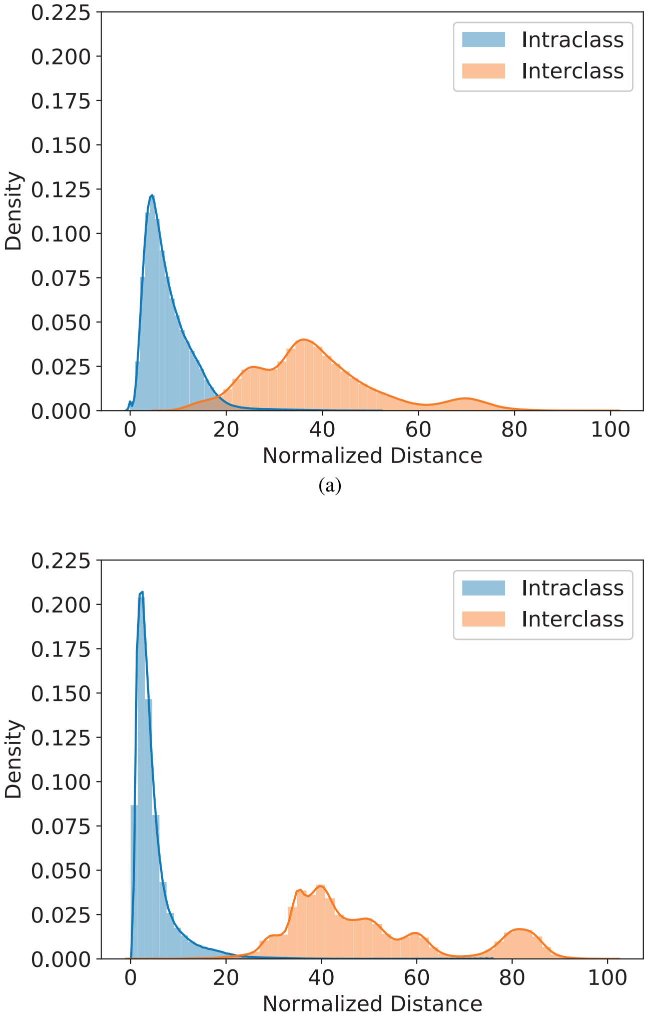
Fig. 14. A DCTF generated at SNR of 20dB.

C. Evaluation of Known Device Classification

1) Evaluation Metrics and Benchmarks: Classification accuracy is often used to evaluate the performance of a classification problem, which is the ratio between the correctly classified instances and the total number of test instances.

We took the schemes proposed in [24], [29] as the benchmarks for known device classification. Although the work in [24] is originally designed for the identification of GSM mobile phones, we can use the same CNN structure to process the LTE PRACH preambles. The RFFI system in [29] uses an SVM model to classify feature vectors consisting of IQ imbalances and variances extracted PRACH preambles.

2) Results in LOS and NLOS Scenarios: Dataset 3 is leveraged to evaluate the performance of known device classification. We trained the MCCNN with signals collected in LOS scenarios and test it with signals collected in both LOS and NLOS scenarios. This allows us to evaluate the system's robustness to DUT position changes. The training and test data are detailed as follows:



(a)

(b)

Fig. 15. Normalized Intraclass and interclass distances of the training RFF representations. (a) Trained without maxmin loss. (b) Trained with maxmin loss.

- **Training**: Random 80% of the signals collected in LOS scenarios in Dataset 3.
- **Test**: The remaining 20% signals of LOS scenarios and all the signals of NLOS scenarios in Dataset 3.

The results are shown in Table IV. It can be seen that the proposed MCCNN-based schemes outperform previous schemes in [24], [29]. The MCCNN without maxmin loss reaches slightly higher classification accuracy. The system performance in the NLOS scenario is lower than that in the LOS scenario due to changes in wireless channel conditions. It is clear that the MCCNN-based schemes are still superior to others.

3) Results at Various SNRs: The RFFI performance is evaluated at different SNR conditions, which is achieved by adding AWGN to the collected signals. The training and test data are listed as follows:

- **Training**: Random 80% of the signals collected in LOS scenarios in Dataset 3. AWGN is added.
- **Test**: The remaining signals are in both LOS and NLOS scenarios in Dataset 3. AWGN is added.

TABLE IV
RESULTS OF KNOWN DEVICE CLASSIFICATION

Methods	Test of Accuracy in LOS Scenarios	Test of Accuracy in NLOS Scenarios
Ding *et al.* [29]	37.40%	30.60%
Wang *et al.* [24]	95.34%	80.47%
MCCNN	98.70%	89.40%
MCCNN+maxmin loss	96.11%	88.55%

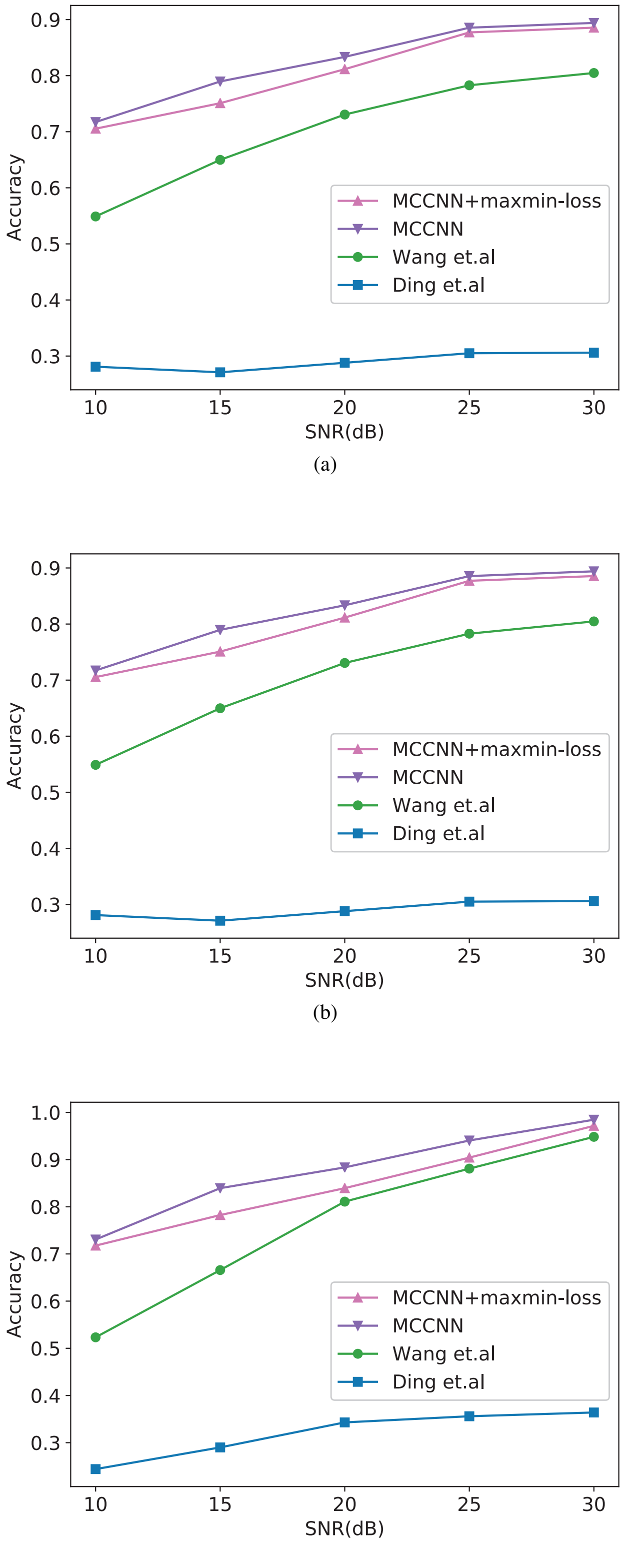
To evaluate the classification performance in certain applications or environments, the signals in NLOS scenarios are added to the training set. The details are as follows:

- **Training**: Random 80% of the signals collected in both LOS and NLOS scenarios in Dataset 3. AWGN is added.
- **Test**: The remaining signals in LOS scenarios in Dataset 3. AWGN is added.

The classification results are shown in Fig. 16. It is clear that the proposed MCCNN-based schemes achieve better performance than those proposed in [24], [29] in both LOS and NLOS scenarios. The method in [24] is inferior to the proposed MCCNN scheme, and the performance gap grows as the SNR decreases. The classification accuracy of the method proposed in [29] is lower than 40%, which is unacceptable for an RFFI system. The segmentation mechanism for DCTF of LTE RACH signal gives higher performance, especially when the DCTF gets vague at a low level of SNR. And for the scenarios with a training set including both LOS and NLOS signals, the performance seems no significant change for all the schemes. At the SNR of 30dB, classification accuracy with MCCNN is 98.45%, and the accuracy is 97.15% when MCCNN with maxmin loss is used.

The classification confusion matrices with MCCNN at different levels of SNRs are illustrated in Fig. 17. Wrong predictions would be more frequent at low SNR levels. The incorrect predictions occur more often among devices of the same model. It leads to a variety of classification performance among different devices, e.g., at the level of 10dB SNR, the classification accuracy of phone 2, 5 and 6 declines sharply while that of others tends to decrease slightly.

4) Discussion on Performance with Maxmin-Loss: As previously discussed, the maxmin-loss is expected to enhance performance in unknown device detection by creating a clear separation between samples belonging to different categories. In contrast, the cross entropy loss primarily emphasizes the relationship between samples and their respective category labels, making it advantageous for classification problem. However, the combination of these two losses in classification may lead to a decrease in performance. In the context of open-set identification, our aim is to achieve a relatively optimal performance between unknown device detection and known device classification at the same time with one model. In fact, both MCCNN and MCCNN with maxmin-loss exhibit superior classification performance compared to the other two methods.



(a)

(b)

(c)

Fig. 16. Classification performance at different SNRs. (a) Train in LOS scenarios. Test in LOS scenarios. (b) Train in LOS scenarios. Test in NLOS scenarios. (c) Train in LOS & NLOS scenarios, test in LOS scenarios.

VIII. Related Work

RF fingerprints can be extracted from both the transient and modulation segments of the received signals. The RF fingerprints extracted from the transient signals include fractal dimension [43], high-order statistical features [23], energy property [44]–[46], and the frequency, phase, amplitude of transient signals [46]–[48]. Transient-based methods require precise starting point detection and signal interception algorithms since the transient signal duration is extremely short. In addition to the transient features, the RF fingerprints can also be extracted from the modulation part. The designed features include signal spectrum [49], estimated carrier frequency offset and I/Q offset [50], [51], and transform domain features [52], [53]. Peng *et al.* propose an RFF extraction method based on DCTF, which can reflect both transient and modulation characteristics at the same time without prior information of the signal [21], [54]. A DCTF-based RFFI scheme for mobile phone identification was proposed in [24]. However, it is unclear whether the visibility of the transient and modulation parts in one figure will affect each other given the fact that the duration of transient signals is much shorter than that of the steady-state signal part.

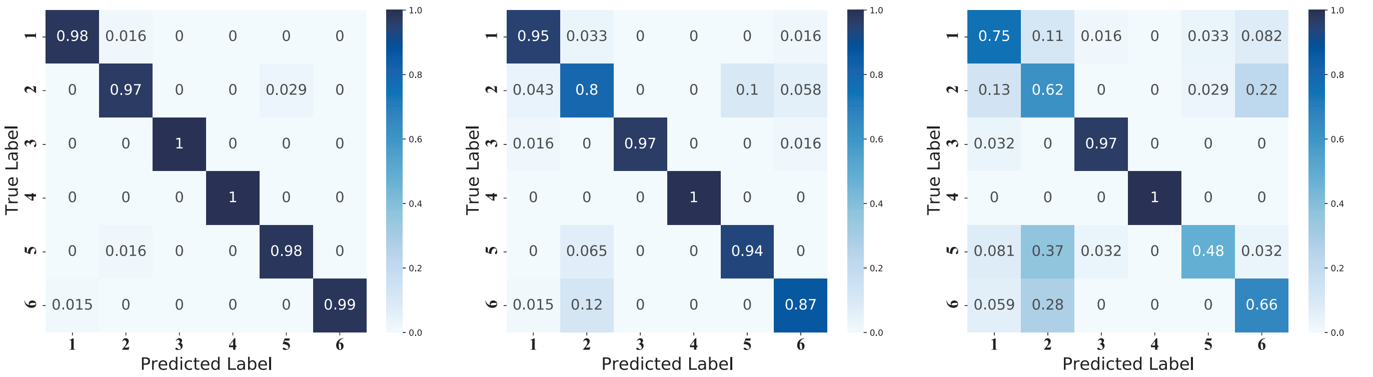
Despite the fact that LTE is now among the most widely used wireless technologies in our daily lives. Prior research has not focused much on using RFFI to identify LTE mobile phones. To the best knowledge of the authors, there are only two papers investigating LTE-RFFI. In our prior work [29], the I/Q imbalance of the random access preamble is extracted as the feature and a support vector machine (SVM) is used as the classifier. Zhang *et al.* design an LTE-RFFI system using ResNet and evaluate it with 15 COTS mobile phones [55]. Further research is needed to investigate the effectiveness of using RFFI to identify LTE devices.

IX. Conclusion

In this paper, an open-set recognition scheme for RFF-based LTE device identification was proposed. The feasibility of using RFF to identify LTE mobile phones was verified. DCTF features from transient-on, modulation and transient-off parts of LTE PRACH preamble signals were extracted. An MCCNN scheme was proposed using these features from different parts of the signals to reach a high level of performance on RFFI. To maximize the interclass distances and minimize the intraclass distances of the RFF representations, a custom maxmin-loss was proposed to be used during the training process of the MCCNN scheme. Extensive experiments were carried out including ten mobile phones from four models. The dataset was constructed with waveforms collected from different locations including LOS and NLOS scenarios. In known LTE device classification problems, the accuracy can reach 98.70% in the LOS scenario at an SNR level of 30 dB among six LTE mobile phones. In the unknown LTE device detection problems, the EER is as low as 0.0545 and the AUC reaches 0.9817 considering six known phones and four unknown phones.

References

[1] "4G-5G Subscribers March 2022 - Quarterly update." [Online]. Available: https://gsacom.com/paper/4g-5g-subscribers-march-2022-quarterly-update/



(a) (b) (c)

Fig. 17. Classification confusion matrices with the MCCNN scheme. (a) SNR is 30 dB. (b) SNR is 20 dB. (c) SNR is 10 dB.

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

[3] Y. Park and T. Park, “A survey of security threats on 4G networks,” in *Proc. IEEE Global Commun. Conf. Workshop (Globecom)*, 2007, pp. 1–6.

[4] L. He, Z. Yan, and M. Atiquzzaman, “LTE/LTE-A network security data collection and analysis for security measurement: A survey,” *IEEE Access*, vol. 6, pp. 4220–4242, 2018.

[5] M. Lichtman, R. P. Jover, M. Labib, R. Rao, V. Marojevic, and J. H. Reed, “LTE/LTE-A jamming, spoofing, and sniffing: threat assessment and mitigation,” *IEEE Commun. Mag.*, vol. 54, no. 4, pp. 54–61, 2016.

[6] R. P. Jover, J. Lackey, and A. Raghavan, “Enhancing the security of LTE networks against jamming attacks,” *EURASIP Journal on Information Security*, vol. 2014, no. 1, p. 7, 2014. [Online]. Available: https://doi.org/10.1186/1687-417X-2014-7

[7] J. Cao, M. Ma, H. Li, Y. Zhang, and Z. Luo, “A survey on security aspects for LTE and LTE-A networks,” *IEEE Commun. Surveys Tuts.*, vol. 16, no. 1, pp. 283–302, 2014.

[8] C. Jin, Y. Zhou, X. Qiu, Q. Feng, and Q. Zhang, “Breaking real-world COTS USIM cards with unknown side-channel countermeasures,” *Computers & Security*, vol. 113, p. 102531, 2022.

[9] R. Bassil, A. Chehab, I. Elhajj, and A. Kayssi, “Signaling oriented denial of service on LTE networks,” in *Proc. ACM Int. Symposium Mobility Management wireless Access*, 2012, pp. 153–158.

[10] J. Henrydoss and T. Boult, “Critical security review and study of DDoS attacks on LTE mobile network,” in *Proc. IEEE Asia Pacific Conf. Wireless Mob.*, 2014, pp. 194–200.

[11] R. Piqueras Jover, “Security attacks against the availability of LTE mobility networks: Overview and research directions,” in *Proc. Int. Symposium Wireless Personal Multimedia Commun. (WPMC)*, 2013, pp. 1–9.

[12] G. Shen, J. Zhang, A. Marshall, L. Peng, and X. Wang, “Radio frequency fingerprint identification for LoRa using spectrogram and CNN,” in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, 2021, pp. 1–10.

[13] S. Dolatshahi, A. Polak, and D. L. Goeckel, “Identification of wireless users via power amplifier imperfections,” in *Proc. Conf. Asilomar Conf. Signals Systems Comput. (Asilomar)*, 2010, pp. 1553–1557.

[14] H. P. Romero, K. A. Remley, D. F. Williams, and C.-M. Wang, “Electromagnetic measurements for counterfeit detection of radio frequency identification cards,” *IEEE Transactions on Microwave Theory and Techniques*, vol. 57, no. 5, pp. 1383–1387, 2009.

[15] D. Zanetti, B. Danev, and S. Capkun, “Physical-layer identification of UHF RFID tags,” in *Proceedings of the Sixteenth Annual International Conference on Mobile Computing and Networking*, ser. MobiCom’10. New York, NY, USA: Association for Computing Machinery, 2010, p. 353–364. [Online]. Available: https://doi.org/10.1145/1859995.1860035

[16] S. Chinnappa Gounder Periaswamy, D. R. Thompson, and J. Di, “Fingerprinting RFID tags,” *IEEE Transactions on Dependable and Secure Computing*, vol. 8, no. 6, pp. 938–943, 2011.

[17] G. Khadka, B. Ray, N. C. Karmakar, and J. Choi, “Physical-layer detection and security of printed chipless RFID tag for internet of things applications,” *IEEE Internet of Things Journal*, vol. 9, no. 17, pp. 15 714–15 724, 2022.

[18] K. Sankhe, M. Belgiovine, F. Zhou, L. Angioloni, F. Restuccia, S. D’Oro, T. Melodia, S. Ioannidis, and K. Chowdhury, “No radio left behind: Radio fingerprinting through deep learning of physical-layer hardware impairments,” *IEEE Trans. on Cogn. Commun. Netw.*, vol. 6, no. 1, pp. 165–178, 2019.

[19] G. Shen, J. Zhang, A. Marshall, and J. R. Cavallaro, “Towards scalable and channel-robust radio frequency fingerprint identification for LoRa,” *IEEE Trans. Inf. Forensics Security*, vol. 17, pp. 774–787, 2022.

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

[21] L. Peng, A. Hu, J. Zhang, Y. Jiang, J. Yu, and Y. Yan, “Design of a hybrid RF fingerprint extraction and device classification scheme,” *IEEE Internet Things J.*, vol. 6, no. 1, pp. 349–360, 2019.

[22] J. Shi, L. Peng, H. Fu, and A. Hu, “Robust rf fingerprint extraction based on cyclic shift characteristic,” *IEEE Internet of Things Journal*, pp. 1–1, 2023.

[23] A. Aghnaiya, A. M. Ali, and A. Kara, “Variational mode decomposition-based radio frequency fingerprinting of bluetooth devices,” *IEEE Access*, vol. 7, pp. 144 054–144 058, 2019.

[24] S. Wang, L. Peng, H. Fu, A. Hu, and X. Zhou, “A convolutional neural network-based RF fingerprinting identification scheme for mobile phones,” in *Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, 2020, pp. 115–120.

[25] M. D. Williams, M. A. Temple, and D. R. Reising, “Augmenting bit-level network security using physical layer RF-DNA fingerprinting,” in *Proc. IEEE Global Commun. Conf. (Globecom)*, 2010, pp. 1–6.

[26] D. Zanetti, V. Lenders, and S. Capkun, “Exploring the physical-layer identification of GSM devices,” *Technical Report*, vol. 763, 2012.

[27] J. Hasse, T. Gloe, and M. Beck, “Forensic identification of GSM mobile phones,” in *Proc. ACM Info. Hiding Multimedia Security*, 2013, pp. 131–140.

[28] E. Ener and T. Çıloğlu, “Specific emitter identification of mobile phones using transient features,” in *Proc. Signal Processing Commun. Applications Conf. (SIU)*, 2017, pp. 1–4.

[29] T. Ding, L. Peng, Y. Qiu, Z. Wu, and H. Fu, “A research of I/Q imbalance based RF fingerprint identification with LTE-RACH signals,” in *Proc. Int. Conf. Signal Image Processing (ICSIP)*, 2021, pp. 66–71.

[30] W. Wang and L. Gan, “Radio frequency fingerprinting improved by statistical noise reduction,” *IEEE Trans. on Cogn. Commun. Netw.*, 2022.

[31] C. Geng, S.-J. Huang, and S. Chen, “Recent advances in open set recognition: A survey,” *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 43, no. 10, pp. 3614–3631, 2021.

[32] S. Hanna, S. Karunaratne, and D. Cabric, “Open set wireless transmitter authorization: Deep learning approaches and dataset considerations,” *IEEE Trans. on Cogn. Commun. Netw.*, vol. 7, no. 1, pp. 59–72, 2021.

[33] A. Gritsenko, Z. Wang, T. Jian, J. Dy, K. Chowdhury, and S. Ioannidis, “Finding a ‘new’ needle in the haystack: Unseen radio detection in large populations using deep learning,” in *Proc. IEEE Int. Symposium Dynamic Spectrum Access Netw. (DySPAN)*, 2019, pp. 1–10.

[34] D. Roy, T. Mukherjee, M. Chatterjee, E. Blasch, and E. Pasiliao, “Rfal: Adversarial learning for rf transmitter identification and classification,” *IEEE Trans. on Cogn. Commun. Netw.*, vol. 6, no. 2, pp. 783–801, 2019.

[35] S. Karunaratne, S. Hanna, and D. Cabric, “Open set RF fingerprinting using generative outlier augmentation,” in *Proc. IEEE Global Commun. Conf. (Globecom)*, 2021, pp. 01–07.

[36] R. Xie, W. Xu, Y. Chen, J. Yu, A. Hu, D. W. K. Ng, and A. L. Swindlehurst, “A generalizable model-and-data driven approach for open-set RFF authentication,” *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 4435–4450, 2021.

[37] P. Yin, L. Peng, J. Zhang, M. Liu, H. Fu, and A. Hu, “LTE device identification based on RF fingerprint with multi-channel convolutional neural network,” in *Proc. IEEE Global Commun. Conf. (Globecom)*, 2021, pp. 1–6.

[38] M. Lichtman, R. Rao, V. Marojevic, J. Reed, and R. P. Jover, “5G NR jamming, spoofing, and sniffing: Threat assessment and mitigation,” in *2018 IEEE International Conference on Communications Workshops (ICC Workshops)*, 2018, pp. 1–6.

[39] J. Deng, J. Guo, N. Xue, and S. Zafeiriou, “Arcface: Additive angular margin loss for deep face recognition,” in *Proc. IEEE Conf. Comput. Vision Pattern Recog. (CVPR)*, 2019, pp. 4685–4694.

[40] Y. Wen, K. Zhang, Z. Li, and Y. Qiao, “A discriminative feature learning approach for deep face recognition,” in *European Conf. Comput. Vision (ECCV)*. Springer, 2016, pp. 499–515.

[41] Open-source LTE software radio suite. [Online]. Available: https://www.srslte.com/

[42] A. Bendale and T. E. Boult, “Towards open set deep networks,” in *Proc. IEEE Conf. Comput. Vision Pattern Recog. (CVPR)*, 2016, pp. 1563–1572.

[43] S. Guo, S. Akhtar, and A. Mella, “A method for radar model identification using time-domain transient signals,” *IEEE Trans. Aerosp. Navig. Electron.*, vol. 57, no. 5, pp. 3132–3149, 2021.

[44] F. Zhuo, Y. Huang, and J. Chen, “Specific emitter identification based on linear polynomial fitting of the energy envelope,” in *Proc. Int. Conf. Elec. Info. Emergency Commun. (ICEIEC)*, 2016, pp. 278–281.

[45] M. Köse, S. Taşcioğlu, and Z. Telatar, “RF fingerprinting of IoT devices based on transient energy spectrum,” *IEEE Access*, vol. 7, pp. 18 715–18 726, 2019.

[46] J. Yue, L. Gao, and N. Zheng, “Research on C-E fingerprint extraction of emitter,” in *Proc. IEEE Info. Tech. Electronic Automation Control Conf. (IAEAC)*, vol. 1, 2019, pp. 1088–1093.

[47] J. Hall, M. Barbeau, and E. Kranakis, “Enhancing intrusion detection in wireless networks using radio frequency fingerprinting.” *Communications, internet, and information technology*, vol. 1, 2004.

[48] ——, “Detecting rogue devices in bluetooth networks using radio frequency fingerprinting,” in *Proc. Int. Conf. Commun. & Comput. Netw.*, 2006.

[49] I. O. Kennedy, P. Scanlon, F. J. Mullany, M. M. Buddhikot, K. E. Nolan, and T. W. Rondeau, “Radio transmitter fingerprinting: A steady state frequency domain approach,” in *Proc. IEEE Vehicular Tech. Conf. (VTC)*, 2008, pp. 1–5.

[50] V. Brik, S. Banerjee, M. Gruteser, and S. Oh, “Wireless device identification with radiometric signatures,” in *Proc. Int. Conf. Mobile Comput. Netw. (MobiCom)*, San Francisco, CA, USA, Sep. 2008, pp. 116–127.

[51] A. Ali and G. Fischer, “The phase noise and clock synchronous carrier frequency offset based RF fingerprinting for the fake base station detection,” in *Proc. IEEE Wireless Microwave Tech. Conf. (WAMICON)*, 2019, pp. 1–6.

[52] L. Zong, C. Xu, and H. Yuan, “A RF fingerprint recognition method based on deeply convolutional neural network,” in *Proc. IEEE Info. Tech. Mechatronics Engineering Conf. (ITOEC)*, 2020, pp. 1778–1781.

[53] Y. Yang and T. Yan, “Radio frequency fingerprint recognition method based on generative adversarial net,” in *Proc. Int. Conf. Commun. Software Netw. (ICCSN)*, 2021, pp. 361–364.

[54] L. Peng, J. Zhang, M. Liu, and A. Hu, “Deep learning based RF fingerprint identification using differential constellation trace figure,” *IEEE Trans. Veh. Technol.*, vol. 69, no. 1, pp. 1091–1095, 2020.

[55] T. Zhang, P. Ren, and Z. Ren, “Deep radio fingerprint resnet for reliable lightweight device identification,” in *Proc. IEEE Vehicular Tech. Conf. (VTC)*. IEEE, 2021, pp. 1–6.