Signal-independent RFF Identification for LTE Mobile Devices via Ensemble Deep Learning

Yanjin Qiu*, Linning Peng*†, Junqing Zhang‡, Ming Liu§, Hua Fu*†, Aiqun Hu¶†
*School of Cyber Science and Engineering, Southeast University, Nanjing, China
†Purple Mountain Laboratories for Network and Communication Security, Nanjing, China
‡Department of Electrical Engineering and Electronics, University of Liverpool, Liverpool, United Kingdom
§School of Computer and Information Technology, Beijing Jiaotong University, Beijing, China
¶School of Information Science and Engineering, Southeast University, Nanjing, China

***Abstract*—Radio frequency fingerprint (RFF)-based wireless device authentication is an emerging technique to prevent potential spoofing attacks in wireless communications. The random access preamble of the physical random access channel (PRACH) in Long Term Evolution (LTE) systems is the first message sent from a user equipment (UE). However, PRACH preambles change under different evolved Node B (eNB), which will affect the RFF extraction. In this paper, a signal-independent RFF extraction method is first proposed to extract varying LTE PRACH preambles under different LTE eNBs. Residual transient segment (RTS) features from the varying PRACH preambles are extracted for RFF identification. A convolutional neural network (CNN) based ensemble deep learning scheme is proposed to integrate benefits from different RFF features. An experimental system under real operator LTE eNB is designed to capture and identify real UE signals. Experimental results show that the classification accuracy of five UEs can reach more than 95% under the same eNB and 85% under different eNBs. Furthermore, longtime evaluations show that the UE RTS feature is robust over time.**

***Index Terms*—LTE, RFF, PRACH, residual transient segment, CNN, ensemble learning.**

I. Introduction

Radio frequency fingerprint (RFF)-based identification is an emerging technology for wireless device authentication [1]. There are subtle hardware differences between electronic components due to the manufacturing process, which will distort the emitted signals. RFF features are extracted from these distorted signals, which are unique, persistent, and difficult to clone or tamper with [2]. It can be used as an auxiliary mechanism for device access authentication to enhance system security from the physical layer without affecting the upper-layer protocols.

Long Term Evolution (LTE) is the primary global cellular standard, which has been employed by mobile operators worldwide. Though LTE offers higher spectral efficiency and better security mechanisms, it is still vulnerable to physical layer threats such as radio frequency (RF) jamming, spoofing and sniffing [3]. Therefore, it is of great significance to study the security scheme with practical application under LTE. Previous work on LTE signal identification was mainly based on other protocols, such as the Global System for Mobile Communications (GSM). Karami *et al.* proposed an algorithm based on the pilot-induced second-order cyclostationarity for the identification of GSM and LTE signals [4]. In [5]–[7], GSM mobile phone identification based on RFF was studied. Wang *et al.* proposed a differential constellation trace figure (DCTF) physical layer RFF extraction and convolutional neural network (CNN) based classification scheme to identify six GSM mobile phones, with accuracies of 99.77% at signal-to-noise ratio (SNR) levels of 50 dB [8]. In a recent work [9], Yin *et al.* extracted DCTF from the physical random access channel (PRACH) preambles under a pseudo base station implemented on the universal software radio peripheral (USRP) and completed effective classification of six mobile terminals using multi-channel CNN.

Generally, RFF extraction methods can be structured into three categories, namely transient-based, modulated-based and other signal-part based [10]. In this paper, the LTE random access preamble signals are segmented to extract RFF features. The wireless terminal will experience a transient process when switched on or off. In the transient phase, the signal converts between 0 and normal power, which does not contain data information, depends only on the hardware characteristics of the device [11]. The steady phase is the part of the signal sent when the received terminal power is stable, which is the modulated waveform of the specific symbol data. PRACH preambles emitted by user equipment (UE) are different due to the parameter change of the Zadoff-Chu (ZC) sequences [9]. Therefore, it is necessary to find a signal-independent RFF extraction method to adapt to the changing PRACH signals.

In this paper, an RFF-based CNN scheme is proposed for the LTE mobile phone identification under different evolved Node B (eNB) of real operators. To the best knowledge of the authors, the stability of RFF features of LTE terminals under different real operator eNBs has not been verified, which is related to the security performance in practical applications. The transient-on, steady, and transient-off parts of PRACH signals are extracted and adopted as RFF features to successfully distinguish five LTE UEs. The research results based on PRACH signals in LTE can be extended to 5G for the similar random access preamble. The main contributions of our work are as follows:

- We propose a residual transient segment (RTS) RFF extraction method for LTE PRACH preamble. With the

978-1-6654-3540-6/22/$31.00 ©2022 IEEE

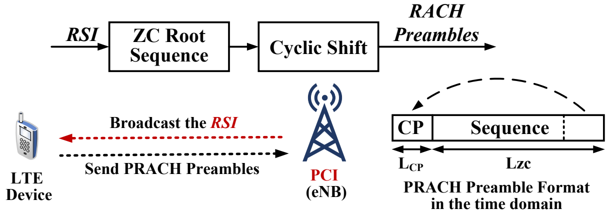


Fig. 1. Generation of the PRACH preamble.

help of the proposed synchronization process, we can obtain the difference between the received PRACH signal and the standard one, which enables signal-independent RFF extraction. We also discover the semi-steady phase of a received PRACH preamble, which varies with UE, can be combined with the traditional transient phase to contribute to terminal identification.

- We design a CNN based ensemble deep learning scheme for different RTS features. Classification advantages of single RFF feature can be combined to achieve the optimized identification effect.
- We implement an experimental system that can capture the UE signal communicating with real operator's eNBs. The RFF identification for LTE UE under the real operator eNB scenario is investigated, which is, to the best knowledge of the authors, the first work in this area.

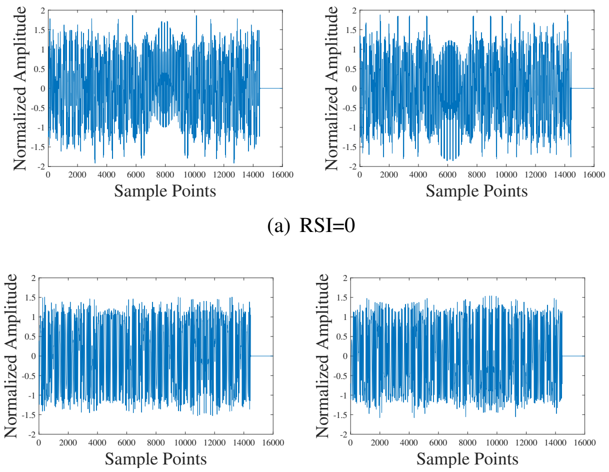
The rest of the paper is structured as follows. Section II introduces the LTE PRACH preamble. Section III introduces the semi-stable state of the PRACH preamble and the RTS RFF. Section IV describes the process of RFF identification. Section V introduces the collection of PRACH preambles and analyzes the experimental results. Section VI concludes the paper.

II. Preliminary: LTE PRACH Preamble

In LTE, PRACH preamble is the first message transmitted from the UE when accessing the eNB during the radio resource control (RRC) establishment, which is used to achieve the up-link synchronization and obtain resources from the eNB, e.g, RRC connection request.

As shown in Fig. 1, each eNB, represented by a physical cell identifier (PCI), sets a different root sequence index (RSI), which is broadcast as part of the system information from eNB. Once the UE receives the RSI, the UE will determine a root sequence from a pool of 839 sequences. It will then generate a set of 64 preambles through a cyclic shift of the root sequence. The generated preambles are orthogonal to avoid interference. Each PRACH preamble in the frequency domain occupies 6 resource blocks (RB) of up-link subframe, which is 1.08 MHz. In the time domain, the PRACH preamble consists of a cyclic prefix (CP) and a sequence part. CP is a segment taken from the back of the sequence part, as shown in Fig. 1. More specific generation principle of the PRACH preamble can be referred to [12].

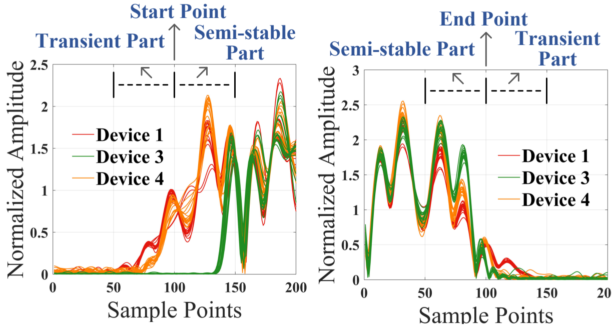
When a UE moves across different eNBs, PRACH preambles sent by the same UE will be significantly different due to the change of the root sequence. As shown in Fig. 2, the waveforms of the PRACH preambles under the same RSI are similar, while the waveforms between RSIs are obviously different. It indicates that the waveform is mainly affected by RSI changes compared with the shift under the same RSI.



(a) RSI=0

(b) RSI=50

Fig. 2. Different PRACH preambles with a specific RSI.



(a) Beginning of PRACH signals (b) End of PRACH signals

Fig. 3. Part of PRACH signals under self-built USRP base station (RSI=0, bandwidth=1.08 MHz, R_S=16 MHz, 20 signals per device).

III. PRACH Residual Transient Segment

As shown in Fig. 3, the received PRACH preamble is well synchronized at the 100^{th} sample. It is the logical start point of the signal unit impulse response in the digital circuit, found by correlating with the standard signal. The transient state only exists before the start point [11], and the signal region after the 100^{th} point in Fig. 3(a) should be the steady state to the traditional understanding. However, an unstable region of the PRACH signal from start point to the normal power is exist, which could be named as semi-steady state and it is varying with different UE. This paper forms the transient RFF feature using the semi-steady part as well as the classical transient part. And we call the combined parts transient-on and transient-off at the beginning and end of the signal respectively.

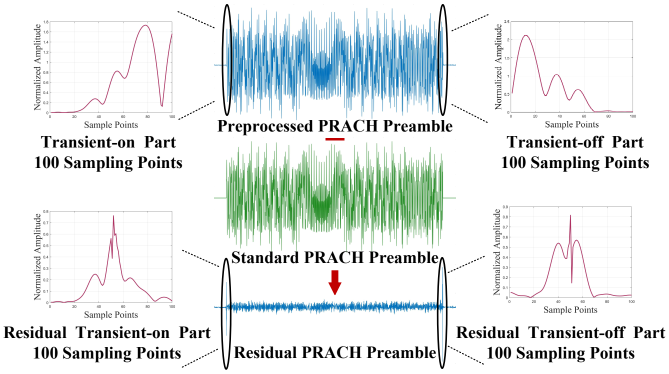
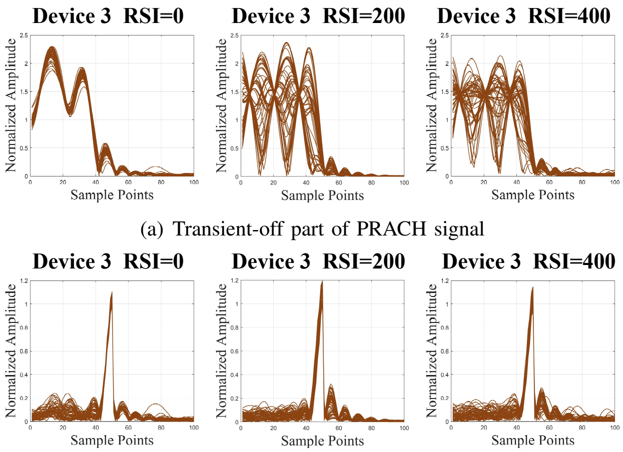


Fig. 4. RFF features extraction process.



(a) Transient-off part of PRACH signal

(b) Transient-off part of RTS PRACH signal

Fig. 5. Comparison of transient-off features under different RSI (60 signals per figure).

As indicated in Section II, the PRACH preamble will be different and orthogonal. As discussed in [13], different data patterns will interfere with the RFF extraction. Therefore, it is not ideal to extract RFF from the received signal directly. Instead, a residual signal $r(n)$ can be obtained by the subtraction of the normalized received PRACH preamble $\tilde{y}(n)$ and the standard PRACH preamble $s(n)$, given as:

$$r\left(n\right) = \tilde{y}\left(n\right) - s\left(n\right), \quad 1 \le n \le L_{CP} + L_{ZC}\ , \tag{1}$$

RTS is the transient-on or transient-off part of the residual signal. Fig. 4 illustrates the RTS extraction process. The areas circled in black are the classical transient and semi-steady regions of the signal. Table I explains the abbreviation of different RFF features used in this paper. Fig. 5 shows the stability of RTS feature from the same device under different RSI. As RSI changes, the semi-steady part in Fig. 5(a) varies, while the corresponding RTS feature is stable in Fig. 5(b). Therefore, RTS extraction is a method to eliminate the difference of PRACH signal under different eNB setups.

IV. RFF Identification

As shown in Fig. 6, the proposed LTE RFF identification scheme includes signal preprocessing, RFF extraction, CNN classification and ensemble learning with multiple features. The process of RFF extraction has been introduced in Section III.

TABLE I
Abbreviation of Each RFF

Abbreviation	RFF Feature
ON	*Transient-on Segment*
OFF	*Transient-off Segment*
RON	*Transient-on RTS*
ROFF	*Transient-off RTS*
RS	*Residual Steady Segment (Without RTS)*
RC	*Residual Complete Signal (Including all RTS and RS)*

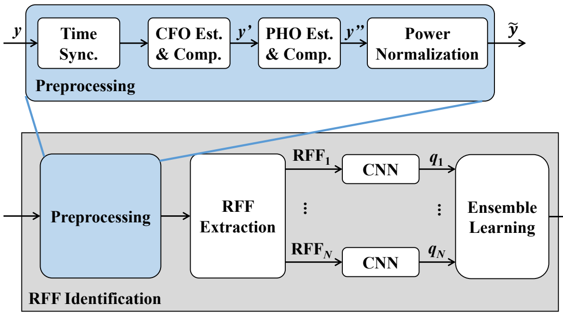


Fig. 6. Process of LTE RFF identification.

A. Preprocessing of PRACH Preamble

As shown in Fig. 6, the preprocessing process invovles time synchronization, carrier frequency offset (CFO) and phase offset (PHO) estimation and compensation, and power normalization.

1) Time Synchronization: The CP of PRACH preamble can be used for time synchronization, given as:

$$D = \arg\max_{i} \left(\sum_{n=0}^{L_{CP}-1} y\left(i+n\right) \cdot y^{*}\left(i+n+L_{ZC}\right) \right), \tag{2}$$

where D refers to the position of the synchronization point in the signal, $y(n)$ represents the received signal, $(\cdot)^*$ is the conjugate operation, L_{ZC} and L_{CP} are the length of the ZC sequence and the CP in the time domain, respectively.

2) Carrier Frequency Offset Estimation: CFO is caused by different oscillator frequencies at the transmitter and receiver. It is also estimated based on the CP of PRACH preamble. The CFO is calculated as follows:

$$\Delta f = \frac{\sum_{n=1}^{L_{CP}} angle\left(y(n) \cdot y^{*}\left(n+L_{ZC}\right)\right)}{2\pi \cdot L_{CP} \cdot L_{ZC}} \cdot R_S, \tag{3}$$

where R_S is the sampling frequency of received signal. The *angle* operation refers to the calculation of an angle. The compensated signal is given as:

$$y'\left(n\right) = y\left(n\right) e^{-j2\pi\Delta f n \frac{1}{R_S}}, \tag{4}$$

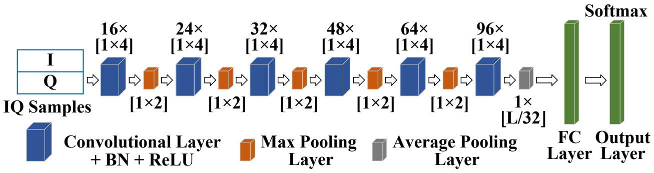


Fig. 7. Proposed CNN structure.

3) Phase Offset Estimation: PHO can be estimated as:

$$\varphi = angle\left(\frac{1}{L_{CP}+L_{ZC}}\sum_{n=1}^{L_{CP}+L_{ZC}} y'(n)\cdot s^{*}(n)\right), \tag{5}$$

where $s(n)$ represents the corresponding standard PRACH preamble. The PHO compensated signal becomes:

$$y''(n) = y'(n)\, e^{-j\varphi}, \tag{6}$$

4) Power Normalization: Finally, the signal is normalized as:

$$\tilde{y}(n) = \frac{y''(n)}{\frac{1}{L_{CP}+L_{ZC}}\sum_{n=1}^{L_{CP}+L_{ZC}}(|y''(n)|)}. \tag{7}$$

The bandwidth of PRACH signal is only 1.08 MHz, which is relatively narrow. Thus, flat fading can be assumed and the channel effect can be compensated by power normalization.

B. CNN Design

For each RFF feature, a specific CNN model is trained, though the same CNN structure is used. The training dataset consists of the real and imaginary parts of the RFF feature whose length is L. Fig. 7 illustrates the structure of the adopted CNN model, which consists of six 2D convolutional layers and a fully connected (FC) layer. The convolutional layer is used to extract local features of input data and the kernel size is set to $[1 \times 4]$. Channel numbers were chosen to 16, 24, 32, 48, 64 and 96 to accommodate higher level features. The batch normalization (BN) layer is added to accelerate the convergence rate of the network. The rectified linear unit (ReLU) is employed to increase the nonlinear relation between layers of neural network and alleviates overfitting. Five $[1 \times 2]$ max pooling layers are applied after the first five convolutional layers and a $1 \times \lfloor L/32 \rfloor$ average pooling layer after the last convolutional layer to reduce the size of parameter matrix and speed up the calculation. In the classification stage, the feature is mapped to the label space through the FC layer. Then the softmax layer calculates confidence level of each class, given as a list of probabilities, $\mathbf{q}$.

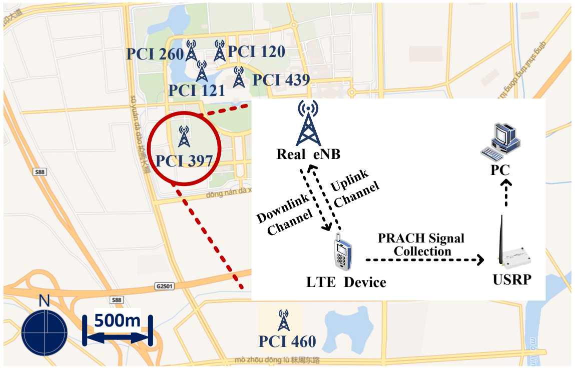


Fig. 8. Location of real eNBs and experimental setup under each eNB.

C. Ensemble Learning with Multiple Features

Multiple features of the same terminal can be arbitrarily combined according to respective classification effects to improve the accuracy based on the idea of ensemble learning. Multiple RFFs extracted from the same training set of PRACH signals trains models separately. When an RFF extracted from a test sample is put into the corresponding model, a set of classification probability scores $\mathbf{q}$ can be obtained, representing the similarity between the sample and each label under this RFF feature. A merged prediction score set $\mathbf{q}'$ can be derived by summing up score sets of N RFF features obtained under the same test sample, mathematically expressed as:

$$\mathbf{q}' = \sum_{n=1}^{N} \mathbf{q}_n, \tag{8}$$

where $\mathbf{q}_n$ is the prediction score set of the n^{th} RFF. Then the predicted label can be derived by selecting the index with the highest probability, formulated as:

$$label = \arg\max_{k}(\mathbf{q}'). \tag{9}$$

V. Experimental Evaluation

A. Data Collection and Training Setup

As shown in Fig. 8, our experiments involved six real operator eNBs. Five mobile phones including Google Nexus 5, XIAOMI MCT3B, HUAWEI P9, Google Nexus 6P and HONOR 30 Lite were employed. Since the PRACH preamble is transmitted when the mobile phone is initially connected to the core network, we switched the flight mode manually to trigger the PRACH signal. A B205 USRP was used to capture the PRACH signal. When collecting under each eNB, the straight-line distance between USRP and UE was 1 to 2 meters and the placement of each UE was randomly selected. The sampling frequency was 16 MHz. Table II shows the specific information of data collected. The same amount of training PRACH preambles are collected for each UE to ensure fairness. Fig. 9 shows PRACH preambles collected under different eNB PCI setups.

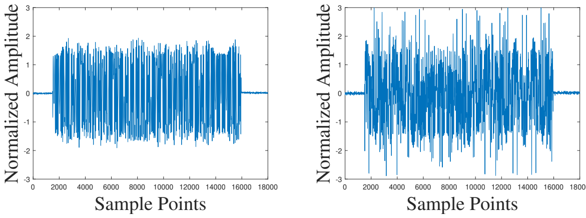
Training set and verification set are divided with a ratio of 7:3. The training learning rate is 2×10^{-2}. The training time is 100 epochs and the batch size is 64.

B. Experimental Results and Analysis

1) Performance of Classification under the Same eNB: When the UE moves in a small range, it will be served by the same eNB, i.e., the PRACH preambles will be generated with the same root sequence. The classification accuracy of 5 terminals is given in Table III when training and testing

TABLE II
INFORMATION OF DATA COLLECTED

Function	**PCI**	**Quantity (per phone)**	**Acquisition Time**	**Initial SNR (dB)**
Training set	397	200	Sept. 2021	44.48
	439		Jan. 2022	39.83
	120			39.72
	260			44.53
Test set	397	60	Sept. 2021	44.39
	439			43.94
	120			38.04
	260			42.92
	460		Nov. 2021	37.7
	397		Jan. 2022	39.31
	121			39.63



(a) PCI=260, j=9 (b) PCI=439, j=9

Fig. 9. PRACH signals under different eNBs (where j is the index number among the 64 standard ZC preambles).

TABLE III
IDENTIFICATION ACCURACY UNDER THE SAME ENB

Dataset	**PCI**			
Training Set	397	439	120	260
Test Set	397	439	120	260
Feature	**Test Accuracy (%)**			
ON	75.00	77.33	71.67	72.33
RON	81.67	85.00	78.33	86.00
OFF	89.67	93.00	92.00	97.67
ROFF	**96.00**	**96.33**	**93.67**	**98.00**
RS	89.00	78.67	55.67	60.33
RC	95.33	80.67	66.33	67.67
ON+OFF	93.33	98.00	93.00	98.00
RON+ROFF	98.33	98.00	96.67	99.00
RS+RC	93.33	80.33	63.67	64.33
ON+RON+ROFF	96.33	97.67	95.67	98.67
RON+ROFF+OFF	96.67	98.33	**97.33**	**99.33**
ON+RON+OFF+ROFF	96.67	99.33	**97.33**	99.00
ON+RON+OFF +ROFF+RS+RC	**99.33**	**100**	96.33	98.67

TABLE IV
IDENTIFICATION ACCURACY UNDER DIFFERENT ENBS

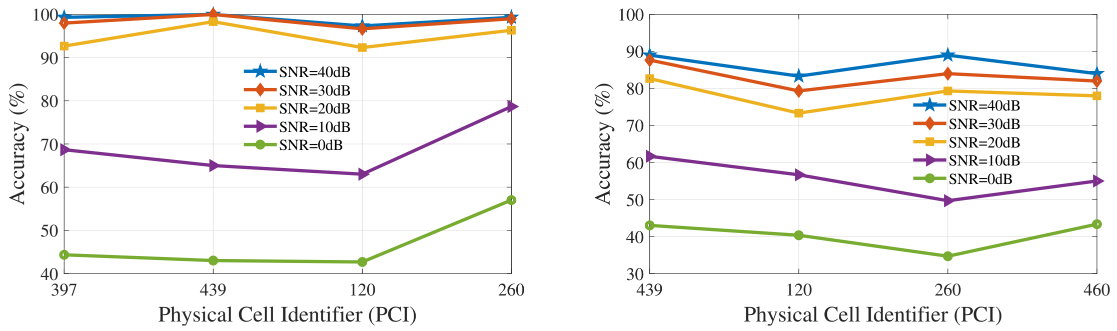
Dataset	**PCI**			
Training Set	397	397	397	397
Test Set	439	120	260	460
Feature	**Test Accuracy (%)**			
ON	41.67	50.00	35.67	49.00
RON	69.33	56.00	60.00	**70.67**
OFF	59.00	57.33	59.67	54.33
ROFF	**73.67**	**79.67**	**75.33**	**70.67**
RS	48.33	38.00	39.67	37.67
RC	46.00	41.00	44.00	46.67
ON+OFF	64.33	63.00	51.33	59.67
RON+ROFF	80.33	76.00	74.67	**84.00**
RS+RC	49.00	41.67	41.67	43.33
ON+RON+ROFF	76.67	71.33	74.00	80.33
RON+ROFF+OFF	81.00	**83.33**	**89.00**	79.33
ON+RON+OFF+ROFF	82.33	76.33	79.33	81.33
ON+RON+OFF +ROFF+RS+RC	**89.00**	72.67	74.33	72.33

PRACH preambles are collected under the same eNB. Totally 4 different eNBs cases are presented to show the universality of the experimental results. As shown in Table III, feature ROFF performs better than other single RFF feature, nearly with an accuracy of over 95% under each eNB. The accuracy with ensemble learning could be significantly higher than that with single RFF feature, which could achieve nearly 100%.

2) Performance of Classification under Different eNBs: In the UE moving state, cell switching causes the change of PRACH root sequence due to the different PCI setups. The classification accuracy of 5 terminals is compared in Table IV when training and testing PRACH preambles are collected under different eNBs. The ROFF feature also has better classification performance than other single features with an accuracy of over 70%. With the help of ensemble learning, the multi-feature of "$RON + ROFF + OFF$" can reach the accuracy at 89% and average accuracy around 85%, which has a significant improvement compared with a single feature. Summarily, the RTS feature owns the benefits of signal-independent and provides better performance than classical transient and steady features.

3) Performance of Identification Stability Over Time: In practical applications, UE can register the RFF feature when they access the network for the first time. The eNB needs to continuously identify the UE in different days. Therefore, the training and testing data of PRACH will probably be collected in different days. We collected PRACH signals in the campus of Southeast University with an interval of three months. Table V illustrates identification results by the multi-feature of "$RON + ROFF + OFF$". Accuracy was 98.67% and 85% under the same eNB and different eNBs, respectively, indicating that the RFF feature extraction and identification scheme is robust over time.

4) Performance With Different SNR: The initial SNR of collected signals is measured around 40 dB, as shown in Table II. In order to evaluate performance under low SNR scenarios, additive white Gaussian noise (AWGN) is added to the original data samples from 0 to 40 dB. As shown in



(a) With the same eNB

(b) With different eNBs

Fig. 10. Classification accuracy under different SNR levels.

TABLE V
IDENTIFICATION STABILITY OVER TIME

Training Set	Test Set	Accuracy (%)
PCI=397: Sept. 2021	PCI=397: Sept. 2021	99.33
	PCI=397: Jan. 2022	98.67
	PCI=260: Sept. 2021	89.00
	PCI=121: Jan. 2022	85.67

Fig. 10, when SNR is higher than 20 dB, accuracy rates only decrease slightly, while in extremely low SNR scenarios, the classification accuracy reduces significantly.

VI. CONCLUSION

In this paper, a signal-independent RFF extraction method for LTE PRACH preamble is proposed. The RTS feature could be extracted by subtracting the synchronized PRACH preamble from the standard PRACH preamble. The semi-steady differences among different PRACH preambles from the same UE due to the eNB PCI changes can be eliminated in RTS feature. An ensemble deep learning scheme combining multiple RFF features is proposed to enhance the RFF identification accuracy. We collect the UE PRACH preambles under real operator eNBs among three months. The experimental results show that the proposed method can effectively distinguish real mobile phones. The highest classification accuracy under the same eNB can reach more than 95% among 5 UEs, which is better than that under different eNBs with the best accuracy around 85%. The RTS feature performs better than classical transient and steady features. Furthermore, multi-feature ensemble learning can effectively improve the classification accuracy, and the proposed scheme has strong time and noise robustness. In general, the ROFF performs better than other single feature, while the combination of "$RON + ROFF + OFF$" is the best multi-feature. Future work includes the detection of unknown UE PRACH preambles via RTS features.

ACKNOWLEDGMENT

This work was supported in part by the National Key Research and Development Program of China (2020YFE0200600, 2021YFE0110500), National Natural Science Foundation of China under Grant 62171120, 62001106 and 61971029, Jiangsu Natural Science Foundation under Grant BK20200350, Jiangsu Provincial Key Laboratory of Network and Information Security No. BM2003201, Guangdong Key Research and Development Program under Grant 2020B0303010001, and Purple Mountain Laboratories for Network and Communication Security.

REFERENCES

[1] G. Shen, J. Zhang, A. Marshall, L. Peng, and X. Wang, "Radio frequency fingerprint identification for LoRa using deep learning," *IEEE Journal on Selected Areas in Communications*, vol. 39, no. 8, pp. 2604–2616, 2021.

[2] N. Xie, Z. Li, and H. Tan, "A survey of physical-layer authentication in wireless communications," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 1, pp. 282–310, 2020.

[3] 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.

[4] E. Karami, O. A. Dobre, and N. Adnani, "Identification of GSM and LTE signals using their second-order cyclostationarity," in *Proc. International Instrumentation and Measurement Technology Conference (I2MTC)*, 2015, pp. 1108–1112.

[5] J. Hasse, T. Gloe, and M. Beck, "Forensic identification of GSM mobile phones," in *Proc. first ACM workshop on Information Hiding and Multimedia Security*, 2013, pp. 131–140.

[6] D. Zanetti, V. Lenders, and S. Capkun, "Exploring the physical-layer identification of GSM devices," *Technical report*, vol. 763, 2012.

[7] E. Ener and T. Çıloğlu, "Specific emitter identification of mobile phones using transient features," in *2017 25th Signal Processing and Communications Applications Conference (SIU)*, 2017, pp. 1–4.

[8] 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 INFOCOM Workshops*, 2020, pp. 115–120.

[9] 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 GLOBECOM*, 2021, pp. 1–6.

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

[11] Z. Shi, M. Liu, and L. Huang, "Transient-based identification of 802.11b wireless device," in *Proc. WCSP*, 2011, pp. 1–5.

[12] "Evolved Universal Terrestrial Radio Access (E-UTRA); Physical Channels and Modulation (3GPP TS 36.211 version 14.2.0 Release 14)," 2017.

[13] J. Zhang, R. Woods, M. Sandell, M. Valkama, A. Marshall, and J. Cavallaro, "Radio frequency fingerprint identification for narrowband systems, modelling and classification," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 3974–3987, 2021.