Authorized and Rogue LTE Terminal Identification Using Wavelet Coefficient Graph with Auto-encoder

Zhenni Wu*, 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*—The wide popularity of 4G/5G mobile terminals increase the requirements of wireless security. Radio frequency fingerprint (RFF) technology can strengthen 4G/5G air interface accessing security at the physical layer. In this paper, a wavelet transform (WT) coefficient graphs RFF extraction with auto-encoder (AE) based rogue terminal detection scheme is proposed. At first, WT coefficients at 48 scales are extracted from the transient-power-off part of LTE physical random access channel (PRACH) preamble. Then, an AE network structure aimed for 2D WT coefficient graph is designed for rogue terminal detection. We successfully distinguish 7 mobile phones and 1 USRP under the proposed mechanism, where the authorized terminals from the same manufacturer can be identified with an accuracy of 90.08%. In addition, extensive experiments are carried out at LOS and NOLS scenarios, respectively, the proposed LTE identification scheme has demonstrated robustness in dynamic environments.**

***Index Terms*—Radio frequency fingerprinting, wavelet, auto-encoder, rogue terminal identification, LTE**

I. Introduction

The rapid growth of mobile communications raises heightened security concerns. The massive 4G/5G terminal accessing may cause denial of service (DoS) attacks. Traditional authentication method usually relies on the pre-shared key or digital identification. This can hardly handle DoS attacks from rogue terminals. Radio frequency fingerprint (RFF) is a physical layer solution for wireless terminal authentication, which can effectively identify rogue terminals without priori knowledge.

The LTE standard provides mutual mechanism for users and base stations by using authentication and key agreement (AKA) protocols, which provide enhanced security levels compared to their 2G and 3G counterparts. However, there are still many potential threats to LTE systems, which can be grouped into two broad categories: DoS attacks and information extraction [1]. RFF has a good characteristic of tamper resistance and measurability, which can well provide a reliable mechanism for the authentication of LTE terminals.

In previous studies on LTE RFF identification, Mondal *et al.* proposed a minimization of drive testing (MDT) method for LTE signals to identify different geographical locations [2]. Concerning mobile terminal identifications, Yin *et al.* extracted the differential constellation trace figure (DCTF) feature and classified 6 mobile phones, the classification accuracy can reach 98.96% in the line-of-sight (LOS) scenarios while greatly reduced in non-line-of-sight scenarios (NLOS) [4].

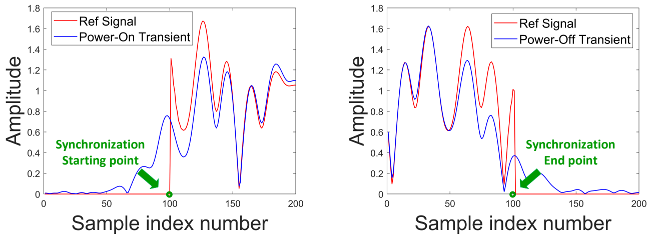
In RFF identification problem, the authorized terminal must be collected and stored at the initial training stage, signals from the known terminals are then used for classification testing [5]. In most of studies, convolutional neural network (CNN), long short-term memory (LSTM) and auto-encoder(AE) methods are used for classification, and the labels of the terminals to be classified can be predicted [4], [6]–[8]. However, rogue terminal identification can be applied to detect malicious terminals such as DoS attacks, which is of great significance. And unsupervised learning is more persuasive in these scenarios where the identity of rogue terminals is anonymous [9], [10].

Fast fourier transform(FFT) and wavelet transform(WT) are classical methods to analyze signals. Danev *et al.* used the feature of FFT spectra to identify the wireless sensor nodes [11]. Ho *et al.* used Haar wavelet, combined the identification results at 4 different scales [12], classified CDMA and GSM signals according to the selected threshold. Baldini *et al.* compared the effects of short-time Fourier features and WT features for 12 wireless devices identification, and the results present that WT features have better performance [13].

In this paper, we extracted wavelet coefficients of 48 scales in transient signals of physical random access chanel (PRACH) preamble of LTE terminals. An auto-encoder (AE) is designed to identify legitimate terminal from rogue ones. The main contributions of our work are as follows:

- A WT based RFF feature extraction method is proposed for the power-off transient part of the LTE PRACH preamble. This feature could distinguish slight difference between the LTE terminal from the same manufacturer.
- An AE network is designed for 2 dimension (2-D) WT feature. The AE network could identify unknown rogue LTE terminals without priori information.
- An experimental system is built including real LTE terminals. The robustness of the proposed RFF identification method is proved in both line-of-sight (LOS) and non-line-of-sight (NLOS) scenarios.

The rest of this paper is organized as follows. Section II describes the WT based RFF feature extraction for LTE PRACH preamble. Section III proposes the auto-encoder network for rogue terminal identification. Section IV introduces



(a)

(b)

Fig. 1. Semi-steady phenomenon of LTE PRACH preamble. (a) Power-on Transient. (b) Power-off Transient.

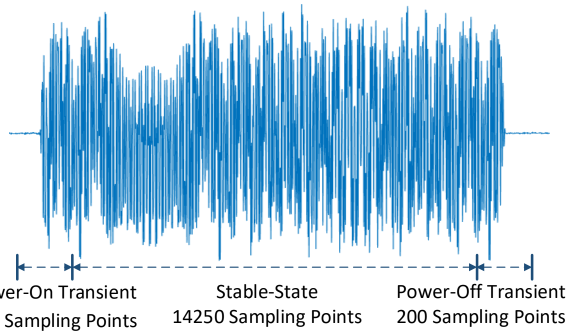


Fig. 2. The transient parts and stable-state part of PRACH preamble

the experimental setup for PRACH signal acquisition. Section V evaluates the performance of the proposed method. Section VI gives the conclusion of this paper.

II. WT Based RFF Feature Extraction

A. LTE PRACH Preamble

PRACH preamble is the first signal sent from an LTE terminal to Evolved Node B (eNB) for the network connection. The PRACH preamble is generated by cyclic shift of Zadoff-Chu (ZC) sequence, derived from one or more root sequences. In one eNB cell, 64 different PRACH preambles could be sent from a LTE terminal with random shift. This is the random access process in 4G/5G network. Generally, under the same eNB cell, the root sequence index and the cyclic shift interval remain constant over a period of time. When the base station coverage is small, using a small cyclic shift interval allows all 64 random PRACH preambles to be under one root sequence index. The first index of PRACH ZC root sequence can be controlled by the PRACH configuration parameters in the eNB, which could be used to generate 64 different preambles with random cyclic shift interval at LTE terminals [14].

Different from the ideal PRACH preamble defined in the 3GPP standard, our experiment demonstrated that the LTE terminal has semi-steady state characteristics in the PRACH preamble. Fig. 1 demonstrates the transient PRACH signal of one LTE terminal, the 100th point in the two subgraphs is the synchronization start point and end point respectively. There are some obvious differences compared with the standard reference signal to the collected signals before and after the synchronization points, which is caused by the semi-steady characteristics of LTE terminals. According to [14], the length of transient should not exceed 20 μs. Therefore, at the sampling rate of 16MS/s, 100 points before the synchronization start point and 100 points after the synchronization start point are selected to constitute the power-on transient part in our research, so does the power-off transient part. The relative position of transient parts and stable-state part of PRACH signal is shown in Fig. 2.

B. Wavelet Transform on Transient Signal

WT has superior time-frequency localization capability compared with the short time Fourier transform (STFT), which is a more suitable method for transient signal analysis [12]. It has very short base function time, supports simultaneous location of time and frequency information, and can be flexibly selected according to special scenarios. The WT is defined as

$$WT(\alpha,\gamma)=\int_{-\infty}^{\infty}S(t)*f\Big(\frac{t-\gamma}{\alpha}\Big)\mathrm{d}t, \qquad (1)$$

where $S(t)$ is the expression of signal in the time domain, $f(t)$ stands for the wavelet in time domain, α means the scale of the wavelet, and γ decides the translation of the wavelet. By stretching or compressing the wavelet, the length and frequency of the wavelet can be changed, so does the corresponding time window length. When at high frequency, the wavelet is compressed and the time window is narrowed, which makes the time resolution higher. These changes at low frequency are reversed. Hence, WT can not only express the frequency components of the signal, but also provides its specific position in the time domain. Ho *et al.* extracted 4 WT-scales of wavelet coefficients and applied histogram to measure the frequency of different energy occurrences at each WT scale, which is an improvement of extracting the wavelet coefficients at a single transform scale [12].

We propose a method to represent multi-scale WT coefficients in a 2-D graph. The CWT function in Matlab toolbox is employed to calculate the wavelet coefficient matrix, using Morse wavelets. Discretization is performed with a specified number of sounds per octave of 10. The minimum and maximum scales are determined automatically based on the energy spread of the wavelet in frequency and time [15]. After WT processing, a 48*200 coefficient matrix is generated due to 200 transient points and 48 WT-scales. According to the complex wavelet coefficient matrix of 48*200, we combine the real and imaginary parts to form a new matrix of 96*200, forming the corresponding size of the diagram. Fig. 3 shows the WT coefficient graphs of some LTE terminals after aforementioned feature extraction. Significant difference could been found among different LTE terminals.

III. Auto-encoder for Rogue Terminal Identification

In most RFF related works, deep learning methods such as CNN are mainly employed to solve multi-class classification

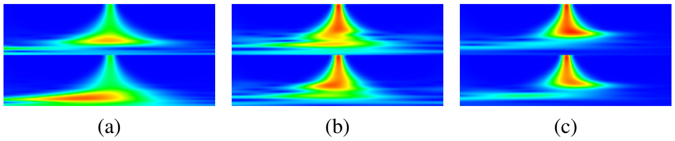


Fig. 3. WT coefficient graphs of LTE PRACH transient part.

problem, which usually requires the priori knowledge of all target terminals in the training stage. In the actual environment, eNB needs to judge whether it is an authorized terminal or a rogue terminal based on the first PRACH signal transmitted by the LTE terminal. Therefore, we design an auto-encoder (AE) with 2-D input for rogue terminal identification.

A. The Design of Auto-encoder

AE is an unsupervised neural network model designed to learn how to represent the input information by taking it as the learning object [8]. The input data is regarded as the supervision to guide the neural network to learn a mapping function, so as to obtain a reconstructed output. When the difference between the output reconstructed by the network and the original input exceeds a certain threshold, it is considered as an anomaly.

Assume $Pre(\cdot)$ represents the function of data preprocessing, which includes time synchronization, frequency offset compensation of the raw I/Q samples and WT feature extration. The input of AE network could be denoted as [8]

$$X = Pre(S(t)), X \in R^{s \times n}, \tag{2}$$

where n is the length of signal, s is the amount of WT-scales. In order to make the output of the subsequent decoder between 0 and 1, eliminate differences between data categories, min-max normalization is adopted, given as

$$X' = \frac{X - \min(X)}{\max(X) - \min(X)}, X' \in [0, 1]^{s \times n}. \tag{3}$$

Assume the function learned by the encoder is $\phi_{w,b}(\cdot)$, where w and b is the network parameters, the input after encoding can be expressed as

$$T = \phi_{w,b}(X'), T \in R^{s \times n}. \tag{4}$$

Similarly, the reconstructed output after decoding can be described as

$$Y = \varphi_{w,b}(T), Y \in R^{s \times n}, \tag{5}$$

where $\varphi_{w,b}(\cdot)$ represents the operations at decoding layer.

Then the mean square error (MSE) function is applied to evaluate the reconstruction error, defined as

$$MSE(X', Y) = \frac{1}{M} \sum_{i=1}^{M} \|Y - X'\|^2, \tag{6}$$

where M stands for the amount of training samples.

The WT coefficient graph is 2-D data, so we designed an AE network for 2-D input. Fig. 4 depicts the structure and detailed parameters of the AE network. The parameter selection is mainly according to [2] and [8]. Firstly, the 96*200 graph is used as input, three convolution layers, two max-pooling layers and four fully connected layers are added to the encoding layer. The kernel size are chosen as $[6 \times 6]$, $[5 \times 5]$, $[4 \times 4]$ for convolution, and $[2 \times 2]$ for max-pooling. Parameters of each fully connected layer are also presented in Fig. 4. Then, a completely symmetrical network structure forms the decoder, which is composed of four fully connected layers, two up-pooling layer and three deconvolution layers.

TABLE I
LTE TERMINAL INFORMATION

	Terminal Model	**Manufacturer**	**Serial Number**
LTE1	Google nexus5	Google	0921fd20027fd130
LTE2	Google nexus5	Google	0666e7ac00616f3a
LTE3	Google nexus5	Google	09218647027fe738
LTE4	Google nexus6P	Huawei	ENU7N16325682829
LTE5	Huawei P9	Huawei	PBV5T16827001165
LTE6	Huawei P9	Huawei	PBV7N16806010230
LTE7	Huawei P9	Huawei	PBV7N16519005122
LTE8	USRP B205	-	-

In the training phase, the AE network learns the information of the input graph at the encoding layers, then restores the same output as the input graph as much as possible at the decoding layers. In the subsequent testing phase, the MSE of the output and the original input graph is regarded as the judgment basis for authorized terminal and rogue terminal.

B. Power-off Transient Part for WT Extraction

In order to search the PRACH preamble part with the most distinguishable wavelet feature, we defined an MSE ratio to evaluate the discrimination effect for AE, which is shown as

$$R_{MSE} = \frac{MSE_{authorized}}{MSE_{rogue}}, \tag{7}$$

where $MSE_{authorized}$ and MSE_{rogue} represent the average MSE of authorized and rogue terminals, respectively. It is obviosu that the smaller the ratio is, the better the discrimination effect is. We extract WT features from the power-on transient, stable-state and power-off transient parts of LTE PRACH preamble, and calculated R_{MSE} for each part. The MSE ratio is 0.6935, 0.9811 and 0.5896, respectively. Therefore, we select power-off transient part to extract the wavelet coefficient graph in subsequent experiments.

IV. Experimental Setups

We use the pseudo eNB to build the experimental system. The corresponding uplink frequency is set to 2565MHz, PRACH root sequence index is set to 0, and cyclic shift interval is set to 13. As described in Section II-A, the 64 random PRACH preambles are all generated from the same root sequence with the specified cyclic shift interval.

There were eight LTE terminals under test, including seven mobile phones from two manufactures and one USRP B205. The parameters of each terminal information are shown in Table I. It is worth noting that Google Nexus6P is manufactured by Huawei.

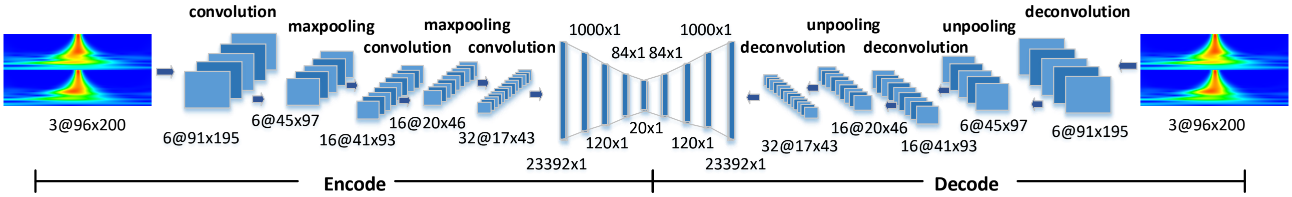


Fig. 4. Structure of auto-encoder for WT coefficient graph.

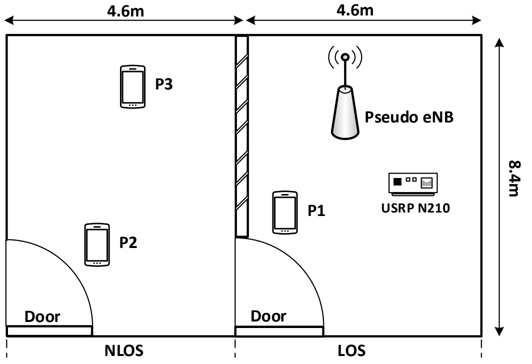


Fig. 5. The acquisition location of our experiment

To evaluate the robustness of our proposed RFF identification method, we captured the LTE terminal signals in LOS and NLOS scenarios. An USRP N210 software defined radio (SDR) platform was used for signal acquisition at the sampling rate of 20MS/s. The acquisition location of our experiment is shown in Fig. 5. We collected 4250 PRACH preambles including three positions (P1, P2, and P3). 800 frames from P1 are used as training dataset. The residual frames are used as testing dataset, which equally include 1150 collected PRACH preambles in P1, P2 and P3.

The server configuration for training AE network in our experiment is as follows: a GeForce RTX 2080 graphics card, 4 Intel(R) Xeon(R) E5-2678 V3 @ 2.50GHz CPU with 12 cores. And the version of CUDA is 11.0. The average training time is around 62.4s with 800 training frames and 100 iterations.

V. Experimental Results and Analysis

LTE terminal verification performance is assessed for each of the trials in Table I in which the selected 1 terminal constitutes the authorized terminal and the remaining 7 terminals as rogue terminals. According to Section III-A, the output MSE of unknown terminals can be calculated through trained AE network. After calculating the MSE of the input WT graph from testing dataset, the threshold can be settled. The accessing PRACH preamble could be considered as an authorized terminal when the MSE is lower than the threshold. Otherwise, the accessing PRACH preamble will be considered as a rogue terminal. It is obvious that the higher threshold value, the higher true positive rate (TPR), meanwhile the lower threshold value, the higher true negative rate (TNR). Therefore, we select the threshold value when TPR equals to TNR. The TPR at this threshold is defined as the verification accuracy of the current LTE terminal. The verification accuracy is calculated from the averaging result of 8 LTE terminals.

Two existing RFF extraction methods are compared as the reference. The first one is HWT proposed in [12], which extracts the wavelet coefficients at 4 scales, draws the histogram of the four groups of coefficients, and calculates the number of wavelet coefficients within each numerical interval as the input feature. The other one is PropFFT [11], which uses the adjacent spectral differences of frequency domain stable-state signal as the input feature. It is worth noting that features in [12] and [11] are both 1-dimensional (1-D) input. Therefore, we use 1-D convolution layer at the AE network. The kernel size are chosen as $[6 \times 1]$, $[5 \times 1]$, $[4 \times 1]$ for convolution, and $[2 \times 1]$ for max-pooling.

A. *Performance of Different Positions*

The results of different methods with training at P1 and testing at different positions are shown in Fig. 6, where WT is the method we introduced in this paper. It can be seen that the verification accuracy of LOS and NLOS positions both can reach nearly 90% by using our proposed method. The accuracy of training position P1 is almost the same as that of test positions P2 and P3. The average accuracy at three testing positions is around 90.08%. As for HWT, the verification accuracy can reach about 70%, but decline sharply at P2. While for PropFFT, the verification accuracy is less than 70%, and also decrease dramatically at P2. When compared to the PropFFT, WT provides the time-frequency localization capability, while compared to HWT, more wavelet coefficients are extracted in WT. In general, the proposed WT coefficient graph based method has the best verification accuracy.

B. *ROC Curve Analysis*

Fig. 7 depicts the receiver operating characteristic (ROC) curve for each terminal at P1. It can be seen that LTE4 and LTE8 show the best verification performance, and the ROC curves of them tend to be right-angle shape. According to Table I, LTE4 is a Google mobile phone manufactured by

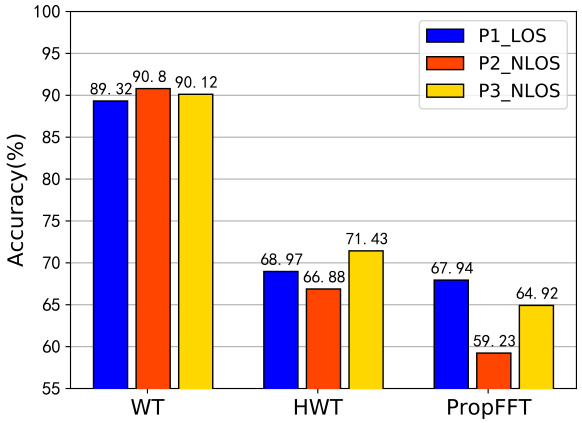


Fig. 6. Verification accuracy in LOS and NLOS scenarios

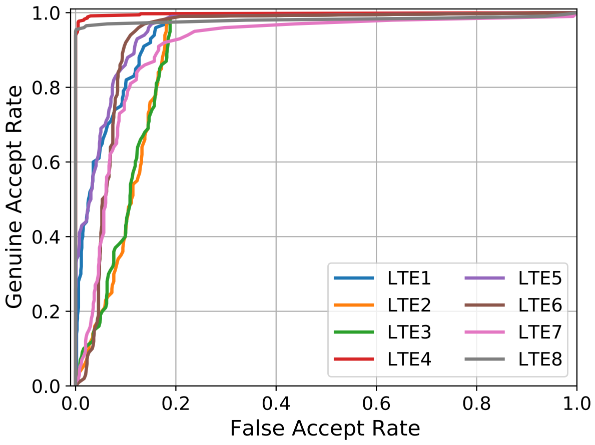


Fig. 7. ROC of 8 LTE terminals at P1

Huawei, compared with other mobile phones from Huawei. Similarly, LTE8 is a USRP device, which show great difference from mobile phones. It is also interesting that LTE2 and LTE3 own the worst verification performance. These two mobile phones are both manufactured from Google with the same model. Meanwhile, Huawei P9 phones tend to be easier to be distinguished compared with Google Nexus5 phones, the average verification accuracy of the former is 89.14% and the latter is 85.76%. It can be inferred that mobile phones from different manufacturers have different degrees of distinctiveness in RFF identifications.

VI. Conclusion

In this paper, a WT based LTE RFF feature extraction method is proposed. We select the power-off transient part of PRACH preamble with the lowest MSE ratio for rogue LTE terminal identification. A 2-D AE network is proposed for WT coefficient graph feature. Extensive experiments are carried out including 8 LTE terminals with 3 different locations. The average verification accuracy can reach 90.08%, showing great robustness both in LOS and NLOS scenarios, which significantly outperform existing methods.

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] 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 Communications Magazine*, vol. 54, no. 4, pp. 54-61, 2016.

[2] R. Mondal, J. Turkka, T. Ristaniemi and T. Henttonen, “Performance evaluation of MDT assisted LTE RF fingerprint framework,” in *2014 Seventh International Conference on Mobile Computing and Ubiquitous Networking (ICMU)*, pp. 33-37, 2014.

[3] D. Zanetti, V. Lenders, and S. Capkun, “Exploring the physical-layer identification of GSM devices,” *CTIT technical report*, vol. 763, 2012.

[4] 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”, *2021 IEEE Global Communications Conference (GLOBECOM)*, pp. 1-6, 2021.

[5] G. Baldini and G. Steri, “A Survey of Techniques for the Identification of Mobile Phones Using the Physical Fingerprints of the Built-In Components”, *IEEE Communications Surveys & Tutorials*, vol. 19, no. 3, pp. 1761-1789, 2017.

[6] J. H. Tyler, M. K. M. Fadul, D. R. Reising and E. Kaplanoglu, “Simplified Denoising for Robust Specific Emitter Identification of Preamble-based Waveforms,” *2021 IEEE Global Communications Conference (GLOBECOM)*, pp. 1-7, 2021.

[7] G. Shen, J. Zhang, A. Marshall, L. Peng and X. Wang, ”Radio Frequency Fingerprint Identification for LoRa Using Deep Learning,” in *IEEE Journal on Selected Areas in Communications*, vol. 39, no. 8, pp. 2604-2616, Aug. 2021.

[8] J. Yu, A. Hu, F. Zhou, Y. Xing, Y. Yu, G. Li and L. Peng, “Radio Frequency Fingerprint Identification Based on Denoising Autoencoders,” in *2019 International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, pp. 1-6, 2019.

[9] D. R. Reising, M. A. Temple and J. A. Jackson, “Authorized and Rogue Device Discrimination Using Dimensionally Reduced RF-DNA Fingerprints,” *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 6, pp. 1180-1192, 2015.

[10] Y. Liu, J. Wang, J. Li, S. Niu and H. Song, “Machine Learning for the Detection and Identification of Internet of Things Devices: A Survey,” *IEEE Internet of Things Journal*, vol. 9, no. 1, pp. 298-320, 2022.

[11] B. Danev and S. Capkun, “Transient-based identification of wireless sensor nodes”, in *2009 International Conference on Information Processing in Sensor Networks*, pp. 25–36, 2009.

[12] K. C. Ho, Haiqin Liu, and Liang Hong, “On improving the accuracy of a wavelet based identifier to classify CDMA signal and GSM signal”, in *1999 IEEE International Symposium on Circuits and Systems (ISCAS)*, vol.4, pp. 564–567, 1999.

[13] G. Baldini, C. Gentile, R. Giuliani and G. Steri, ”Comparison of techniques for radiometric identification based on deep convolutional neural networks”, *Electron. Lett.*, vol. 55, no. 2, pp. 90-92, 2018.

[14] 3GPP TS 36.211 version 14.2.0 Release 14. [Online]. Available: https://www.3gpp.org/ftp/Specs/archive/.

[15] Matlab wavelet toolbox. [Online]. Available: https://www.mathworks.com/help/wavelet/ref/cwt.html.