A Robust Radio Frequency Fingerprint Extraction Scheme for Practical Device Recognition

Xinyu Zhou, Aiqun Hu, Guyue Li, Linning Peng, Yuexiu Xing, and Jiabao Yu

***Abstract*—Radio frequency fingerprinting (RFF) exploiting hardware characteristics has been employed for device recognition to enhance the overall security. However, the performance unreliability in long-term experiments, channel fading interference and unauthorized devices verification are three open problems that restrict the development of RFF recognition. To address these issues, a robust RFF extraction scheme based on three corresponding algorithms is studied. For the first problem, a long-term stacking of repetitive symbols (LSRS) algorithm is proposed to reduce the acquired signal variance, which contributes to the identification accuracy and long-term stability. For the second issue, we propose an artificial noise adding (ANA) algorithm to enhance the recognition robustness through regularization and channel adaptation. For the third issue, a verification algorithm based on the generative Gaussian probabilistic linear discriminant analysis (GPLDA) model is developed to handle unauthorized devices. Our robust RFF extraction scheme is verified in the experiments with 54 CC2530 ZigBee devices. It enables reliable node identification with the accuracy of 99.50% in the short rang line-of-sight (SLOS) scenarios for signals collected over 18 months, and 95.52% in the extensive multipath fading experiments. The equal error rate (EER) of the verification experiments with six authorized devices versus six unseen unauthorized devices is as low as 0.63%.**

***Index Terms*—Radio frequency (RF) fingerprint, physical layer identification, ZigBee, artificial noise, security.**

I. INTRODUCTION

THE deployment of Internet of Things (IoT) has gained great popularity in various applications [1] because of energy efficiency, such as smart city [2], smart healthcare [3], industrial control [4] etc. However, the openness of signal transmission has brought about a series of security challenges such as IP or MAC spoofing, replay and DoS attacks [5], [6]. What's worse, classical cryptography-based authentication techniques usually consumes massive computing resources. It is challenging for the energy-limited IoT devices to work for many year with these techniques. Therefore, a lightweight recognition technique is urgently needed for the IoT.

The vulnerability of IoT devices has motivated researches in physical layer to enhance the overall security, especially the radio frequency fingerprinting (RFF) technique utilizing inherent characteristics of device during transmission. These device-specific features are originated from tolerated hardware variations in the analog circuitries [7] and can be extracted from the transmitted signals, which adds no extra costs to existing IoT devices. Hence, RFF identification can be a potential solution for IoT devices. Despite the recent advancement of RFF, there are still many challenges on the practical level. The performance unreliability in long-term experiments, channel fading interference and unauthorized devices verification are open problems restricting the development of RFF.

Feature extraction has a pivotal role in an RFF scheme. It is worth noting that the feature space may vary with the change of time. Previous studies have reported that the ring oscillator's frequency may decrease while aging [8]. In [9], the stability of RFF is verified over a 25-hour period and the performance is mainly affected by the temperature variations. Although the average classification accuracy varies less than 1%, some nodes suffer a great loss of 7.7% degradation in accuracy. To compensate for RFF variations, in [10], a transfer learning algorithm to update the instance weights has been proposed to alleviate the problem. The authors use transfer learning based on rejection sampling to merge signals from different time, and there is a 10% increase in the accuracy. Difficulties arise, however, when an attempt is made to collect enough signals for transfer learning to update the weights after training since these devices have been deployed in vast fields and share massive connections. It is thus indispensable for an RFF scheme to work in long-term applications without extra training.

Another problem with current RFF schemes is that they are not robust in the presence of channel changes. Little work has been done with considering the impact of channel fading in a real-world environment. Recent evidences suggest that RFF features are sensitive to device position, antenna polarization, multipath channel and other environmental conditions [11] [12]. In [13], a hybrid RFF extraction and device classification scheme is evaluated in various channel conditions. Results show that there is a 4% to 9% loss of classification accuracy under multipath fading scenarios. To address these challenges, some algorithms have been proposed. In [14], Gaussian artificial noise is added to the received signals under time variant Rayleigh channel to compensate for the channel changes via simulation. The outcome shows that artificial noise leads to

This paper was presented in part at the IEEE Conference on Communications and Network Security (CNS), Washington D.C., USA, June 2019. This work was supported in part by the National Natural Science Foundation of China under Grant 61941115 and Purple Mountain Laboratories for Network and Communication Security. (Corresponding author: A. Hu.)

A. Hu, Y. Xing, and J. Yu are with the School of Information Science and Engineering, Southeast University, Nanjing 210096, China. (e-mail: {aqhu, yxxing, yujiabao}@seu.edu.cn.)

X. Zhou, G. Li and L. Peng are with the School of Cyber Science and Engineering, Southeast University, 210096 Nanjing, China. (e-mail:{zhouxinyu, guyuelee, pengln}@seu.edu.cn).

A. Hu, J. Yu, L. Peng and G. Li are also with the Purple Mountain Laboratories for Network and Communication Security, Nanjing, 210096, China.

obvious improvements in false alarm rate with a small increase in the miss detection rate. However, adding artificial noise to both training set and test set every time is not practical and how much artificial noise to add remains uncertain. Therefore, a channel robust RFF scheme is urgently required for practical applications.

What's more, many researches only consider closed set recognition where all the devices are known in the training stage. They are not eligible for handling unseen devices in a realistic scenario. The verification algorithm learns a mapping from received signals to a feature space where features from the same device cluster together while features from different devices spread out [15]. However, due to the lack of priori knowledge of rogue devices, the verification algorithm has a high chance to accept rogue devices similar to the existing devices. In [16], RF distinct native attribute (RF-DNA) and multiple discriminant analysis (MDA) are used for ZigBee devices verification with seven authorized devices (device 1-7) and two unseen rogue devices (device 8-9). The statistical posterior likelihood values are calculated as the similarity metric between the device under test and its claimed identity. In the experiments, the rogue device 9 has a high chance (around 85%) to be accepted by claiming itself as device 5. Handling new devices plays a vital role for the device recognition scheme that aims to work in a real environment.

This paper introduces three algorithms to address the arduous problems of performance unreliability, channel fading interference and unauthorized devices, and on this basis, a robust RFF extraction scheme is developed for practical device recognition. The main contributions of this paper are summarized as follows:

- We propose a long-term stacking of repetitive symbols (LSRS) algorithm to alleviate the long-term RFF variations. This algorithm can reduce the variances caused by the time-varying device noise and channel noise, which is beneficial for the long-term stability of RFF.
- We present an artificial noise adding (ANA) algorithm to enhance the identification robustness in various channel scenarios. To adapt to the diversity of transmission channels, artificial noise through theoretical calculation is added, so that the training set and the test set share similar channel conditions. Besides, we prove that ANA is an equivalent regularization method, and therefore it is able to form a robust model.
- We design a robust RFF verification scheme based on the generative Gaussian probabilistic linear discriminant analysis (GPLDA) model. The received feature vector is decomposed into the device identity vector and the noise vector with independent Gaussian distributions. By modelling the generation processes of identity vectors, this model is also applicable to identify unseen devices.
- We verify the effectiveness of the proposed scheme by real-world experiments conducted with 54 CC2530 ZigBee devices. The long-term identification experiments last over 18 months, and the accuracy varies less than 1%. We have achieved an identification accuracy of 99.49% in the non-line-of-sight (NLOS) scenario and 95.52% in the long-distance line-of-sight (LLOS) multipath scenario. Our scheme enables reliable and accurate sensor node verification and the equal error rate (EER) is as low as 0.63% with six authorized devices versus six unseen unauthorized devices.

TABLE I
NOTATIONS USED

Notation	Definition
$FR(\cdot)$	Representation extraction function
F	Representation/feature vector of the device
$r(t)$	Original received payload signal
$y(t)$	Processed baseband payload signal
$S(\cdot)$	Scoring function for similarity calculation
$x(t)$	Ideal transmitting payload signal
$f(t)$	Fingerprint of the device
$n(t)$	Gaussian channel noise
h_i	Multipath channel tap
$\tau_i(t)$	Propagation delay of channel
N	Stacking number for LSRS
T	Duration of a received symbol
Ts	The sampling interval
P_i	Position of the i-th target symbol
$a(t)$	Artificial noise adding function
$\mathcal{H}_s$	Hypothesis of the same device
$\mathcal{H}_\mu$	Hypothesis of different devices
μ	Device identity vector
z	Noise offset vector
Φ_b	Between-device covariance matrix
Σ	Within-device covariance matrix
m	overall device mean
$\mathcal{M}$	Probabilistic linear discriminant analysis model
N_d	The number of the device
$\mathcal{O}$	Computational complexity
D	The number of feature dimension
N_s	The number of samples
Q	The eigenvector matrix of Σ
Λ	The eigenvalue matrix of Σ

An initial stacking algorithm and a fixed artificial noise adding algorithm have been proposed in our previous work [17]. Whereas in this paper, we considerably extend and complement this work by improving the original algorithms and additionally providing a verification scheme for unauthorized devices. Furthermore, the initial fixed artificial noise adding algorithm is updated to a channel adaptive one.

The notations used in this paper and their definitions are summarized in Table I. The remaining parts of this paper are organized as follows: Section III introduces the experimental setup. After that, there is an illustration of our identification scheme in Section IV including the LSRS and ANA algorithms. In Section V, we present our verification scheme based on GPLDA. Our experimental results are demonstrated in Section VI. Finally, we conclude our work in Section VII.

II. Related Work

A common RFF scheme usually consists of three parts, including data acquisition, feature extraction and recognition.

Data acquisition is the first step. Recently, more and more RFF researches are completed with cheap software defined radio (SDR) devices other than high-end oscilloscopes or spectrum analyzers. Although a medium receiver will add to the difficulty for RFF authentication [18], it is more promising for practical applications.

After data acquisition, a feature extraction module is needed to extract characteristics. Divided by the part of collected signal for feature extraction, off-the-shelf approaches fall into two main categories: transient-based features and modulation-based features [7]. Transient-based RFF techniques focus on discriminating features when turning on or off the transmitters. Wavelet transforms [19], the signal power envelope, FFT [11] and reconstructed phase space [20] have been employed in different transient-based RF fingerprint techniques for feature extraction. However, the short duration of the transients adds up to the implementation cost of acquisition devices. The modulation-based RFF schemes leverage the errors between ideal data and real data. Errors in modulation domain such as phase error, magnitude error, frequency error, SYNC correlation are common hand-crafted features to form RF fingerprint [21]. Besides, statistical time-frequency analysis has also been proved to be effective in [22] and [23]. The effectiveness of most feature extraction methods are usually verified in a dataset collected in the same day or week. Short-term studies such as these do not necessarily show subtle feature changes over time, which leads to the performance degradation in the working period of the RFF system.

The recognition module is the key step to provide feedbacks for a particular application. There are typically two modes for a device recognition module: either identification of one device among many, or verification whether the received signal matches its claimed identity [24]. Previous studies have tended to focus on the identification problem. Traditional machine learning classifiers such as Random Forest [25] and support vector machine (SVM) [26] have reached relatively good identification results. With the development of artificial intelligence, a considerable literatures have grown up around the theme of deep learning based classifiers such as deep neural network (DNN) [27], convolutional neural network (CNN) [28] [29] and long short-term memory network (LSTM) [30]. This end to end model is promising without hand-crafted feature engineering, and it has been proved to be effective in related physical layer automatic modulation classification (AMC) [31]–[33]. However, most identification studies have only been carried out in additive white Gaussian noise (AWGN) channels without considering other channel distortions. Little attention has been paid to the verification problem. In [28], one CNN is trained per device to provide an Accepted/Rejected decision. However, these results are based upon 7 known devices and the high training cost is unacceptable. Besides, the verification process in existing works are not suitable for practical applications.

This paper aims to bridge the above gaps by proposing a robust RFF recognition scheme. The performance will be validated by extensive experimental data.

III. Experimental System

Our RFF recognition process is illustrated in Fig. 1. In the training stage, after the pre-processing and LSRS of acquired signals, parameters for recognition are calculated and stored in the database. In the test stage, based on the chosen mode, the system will give the answer to the identification problem: is the device one of the authorized devices or the verification problem: does the devices RFF match its claimed identity. The parameters of the system will be adjusted by the ANA algorithm to adapt to the transmission channels. The data acquisition system can be implemented with edge devices, and the subsequent processing are usually completed with a powerful local network center (e.g., gateway) or a remote server. In this section, we give the details of the experimental system for data acquisition.

ZigBee devices with IEEE 802.15.4 protocol implemented have been widely used in IoT applications given their low cost and low power. The protocol uses direct sequence spread spectrum coding and half-sine chip shaping offset-quadrature phase shift keying (O-QPSK) modulation. It divides each byte into 2 symbols (4 bits each) and maps 1 symbol to 32 chips. Thus, there are 16 types of symbols in the protocol. The transmitting frame format is described in Fig. 2, which is made up of 4 bytes of 0x00 (8 zero symbols) for synchronization, one byte with value 0xA7 for start-of-frame delimiter (SFD), one byte for frame length and the remainder for data unit.

Candidate devices have a population of 54 CC2530 ZigBee nodes from the same manufacturer running at 2.4GHz. A universal software radio peripheral (USRP) N210 with a UBX daughterboard acts as the receiver and the sampling rate is 10 Msample/s (10 times oversampling), that is, a typical symbol with the period T consists of 160 complex in-phase (I) and quadrature (Q) components. Acquired baseband signal is then transferred to a PC for further processing.

After data acquisition, there are usually a few data pre-processing steps and RFF has put forward higher requests on the fidelity of pre-processing. Our pre-processing steps are the same as [13], which consist of signal detection, energy normalization, time synchronization, frequency offset compensation and phase offset compensation. After frequency offset and phase offset compensations for the received payload signal $r(t)$, we can get the processed baseband payload signal $y(t)$.

IV. RFF Identification Using LSRS and ANA

In this section, we first build the signal model according to the observations of existing signals. Then based on the model, we detail the identification scheme using LSRS and ANA. The verification method is discussed in the next section.

A. Signal Modelling

The processed baseband in-phase signals of three zero symbols from device 1 are depicted in Fig. 3(a) with a standard symbol for reference. The ZigBee devices and the USRP were positioned close to each other in a range of 0.3-2m. The differences between the ideal signal and the received signal are shown in Fig. 3(c). To give an intuition, the middle parts (5000-10000 ns) are zoomed in and plotted in Fig. 3(b) and Fig. 3(d). What can be clearly seen is that the differences share the same period T with the symbols although there are some fluctuations at certain sampling points. What's more, the received half-sine waves are significantly different from the reference.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2021.3051402, IEEE Internet of Things Journal

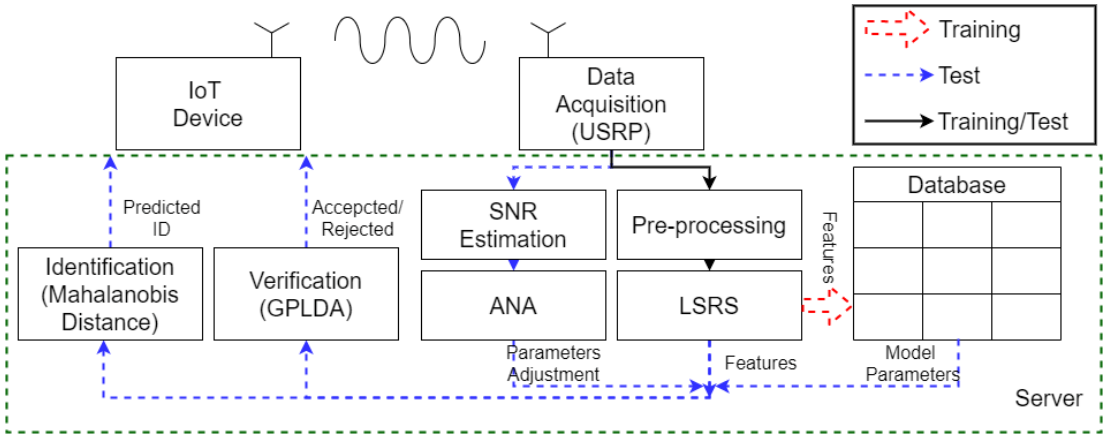

Fig. 1. System model of the RFF recognition scheme.

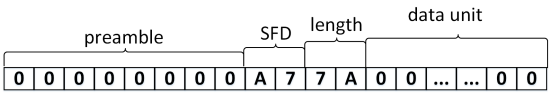

Fig. 2. Frame format.

We deem that the differences between the ideal signal and the received signal arise form the channel noise and the device hardware imperfection. Because of the short range between the USRP and the ZigBee devices, the channel is often modelled as an AWGN channel. The device hardware imperfection is a combination of circuit element characteristics such as the integral nonlinearity (INL) of the digital-to-analog converter (DAC) [34], implementation of shaping filters [35], and memory effects of power amplifiers caused by the electrical and electro-thermal effects [36]. Therefore, devices can be identified by extracting the hardware characteristic coefficients based on some nonlinear regression models [34] [37]. However, due to various device noise arising from DAC [34], RF oscillators [38], power amplifiers [39] or other components [40], observed device hardware imperfection is a joint result of circuit element characteristics and device noise. Thus, a stochastic model is adopted for describing this phenomenon and the received signal at close range is modelled as

$$y(t) = x(t) + f(t) + n(t) \tag{1}$$

where $y(t)$ is the received signal, and $x(t)$ is the ideal signal, $n(t)$ is the AWGN channel noise with a mean of 0 and a variance of δ^2, and $f(t)$ is the device fingerprint. As a joint result of circuit element characteristics and device noise, the device fingerprint of the i-th symbol $[f(T_s + iT), f(2T_s + iT), ..., f(T + iT)]$, where T_s is the sampling interval, obeys a certain multivariate distribution. And according to the results in Fig. 3, the same symbols share similar fingerprints. Previous researches [34] [37] try to find an approximate generative model from x to y, while this stochastic model focuses on the behavior of the discrete time vector of RFF f instead of the complex mapping relationship.

And in the multipath scenario, the model is:

$$y(t) = \sum_{i=0}^{N_p-1} h_i(t)[x(t - \tau_i(t)) + f(t - \tau_i(t))] + n(t) \tag{2}$$

where N_p is the number of paths, h_i is the channel tap and τ_i is the propagation delay for the i-th path.

Therefore, it is significant to find an algorithm to alleviate the channel noise and the device noise. In this case, LSRS is one possible solution.

B. Long-term Stacking of Repetitive Symbols Algorithm

Most existing systems send fixed repetitive symbols for synchronization. Based on this fact, inspired by the information data estimation based stacking (IDES) algorithm in [41] and the crowdsourced measurements in [42], our proposed LSRS algorithm exploits this specific structure to reduce the interference of time, environment and device noise. Since the major part of the device hardware characteristics remain similar with time changing, the reduction in the variance contributes to the long-term stability of the fingerprint.

After data pre-processing, the same symbols are gathered and can be stacked together:

$$LSRS(y(t)) = \sum_{i=0}^{N-1} b_i y(t + P_i T), 0<t \leq T, \tag{3}$$

$$\sum_{i=0}^{N-1} b_i = 1, \tag{4}$$

where N is the stacking number, P_i is the position of the i-th target symbol and b_i is the weight for stacking, which depends on the stacking algorithm. In this paper, the uniform algorithm where $b_i = \frac{1}{N}$ is deployed and thus our LSRS algorithm in the signal domain is

$$\begin{aligned} LSRS(y(t)) =& \frac{1}{N} \sum_{i=0}^{N-1} y(t + P_i T) \\ =& x(t) + \frac{1}{N} \sum_{i=0}^{N-1} f(t + P_i T) + \frac{1}{N} \sum_{i=0}^{N-1} n(t + P_i T) \\ =& x(t) + f'(t) + n'(t) \end{aligned} \tag{5}$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2021.3051402, IEEE Internet of Things Journal

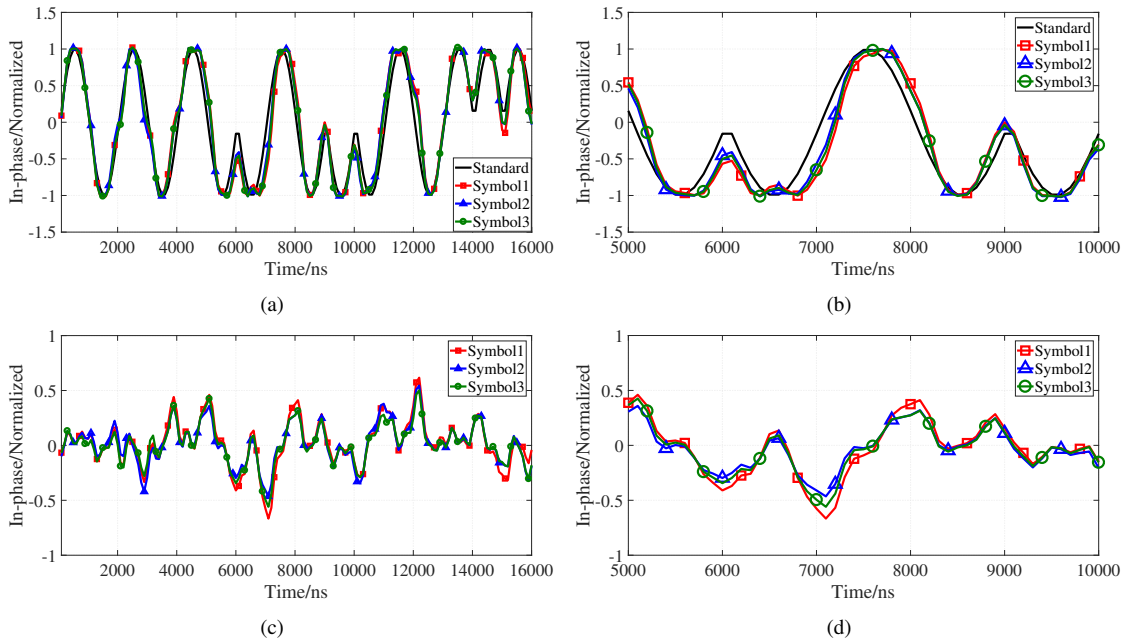

Fig. 3. The in-phase signals of three consecutive symbols zeros are plotted. (a) Three zeros symbols after pre-proceesing. (b) Middle parts of the three symbols after pre-proceesing. (c) The differences between received signal and ideal signal. (d) Middle parts of the differences between received signal and ideal signal.

where $f'(t)$ is the fingerprint after stacking, $x(t) = x(t+P_iT)$ because of the same symbol, and $n'(t)$ is the channel noise after stacking. The SNR before LSRS is

$$SNR_{n(t)} = 10 \cdot log_{10}(p/\delta^2), \tag{6}$$

and after LSRS, it becomes

$$SNR_{n'(t)} = 10 \cdot log_{10}(Np/\delta^2) \tag{7}$$

where p is the signal power and δ^2 is the noise power. Thus there is a $10 \cdot log_{10}(N)$ dB improvement in SNR because of LSRS.

The final unfolding RFF feature vector F in discrete form is:

$$\begin{aligned}&[real(LSRS(y(T_s))), imag(LSRS(y(T_s))),\\ &real(LSRS(y(2T_s))), imag(LSRS(y(2T_s))),\\ &.....,\\ &real(LSRS(y(T))), imag(LSRS(y(T)))]\end{aligned} \tag{8}$$

According to the central limit theorem (CLT), normalized sum of independent random variables tends to subject to a normal distribution. Thus the device noise after LSRS tends toward an approximate Gaussian distribution with smaller variances. The distribution of the fifth dimension after stacking, $real(LSRS(y(3T_s)))$, is shown in Fig. 4. A Gaussian curve based on the estimated variance is also plotted for reference. When the stacking number N is smaller than 20, the distribution is left-skewed because of the channel noise and some device noise. While with the increase of N, the distribution becomes more concentrated with a smaller variance. Fig. 5 presents results of the first two dimensions, $real(LSRS(y(T_s)))$ and $imag(LSRS(y(T_s)))$ when $N = 50$, and the Gaussian curves in these figures are still effective approximate methods. In this paper, the multivariate Gaussian distribution is adopted as an approximate model for the signals after LSRS and whether other models such as the heavy-tailed model will contribute to the recognition results remains further studies.

C. Identification after LSRS

Based on the approximate Gaussian distribution model after the LSRS algorithm, we can get the identification scheme through theoretical deduction.

After LSRS, the conditional distribution $p(F|k)$ for device k, where F is the feature vector after LSRS, obeys a multivariate Gaussian distribution with mean μ_k and covariance Σ_k:

$$p(F|k) = \frac{1}{(2\pi)^{\frac{n}{2}}|\Sigma_k|^{\frac{1}{2}}} exp[-\frac{1}{2}(F-\mu_k)^T\Sigma_k^{-1}(F-\mu_k)] \tag{9}$$

where Σ_k^{-1} is the inverse of Σ_k.

According to the the Bayes' rule [43] [44]:

$$p(k|F) = \frac{p(F|k)p(k)}{p(F)}, \tag{10}$$

we need to find the device k which maximizes the discriminant function

$$g_k(F) = \ln p(F|k) + \ln p(k). \tag{11}$$

As all devices are sending the same symbols and they are from the same manufacturer, it is reasonable to assume that their fingerprints share a similar covariance Σ. Then the discriminant function is

$$g_k(F) = -\frac{1}{2}(F-\mu_k)^T\Sigma^{-1}(F-\mu_k) + \ln p(k). \tag{12}$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2021.3051402, IEEE Internet of Things Journal

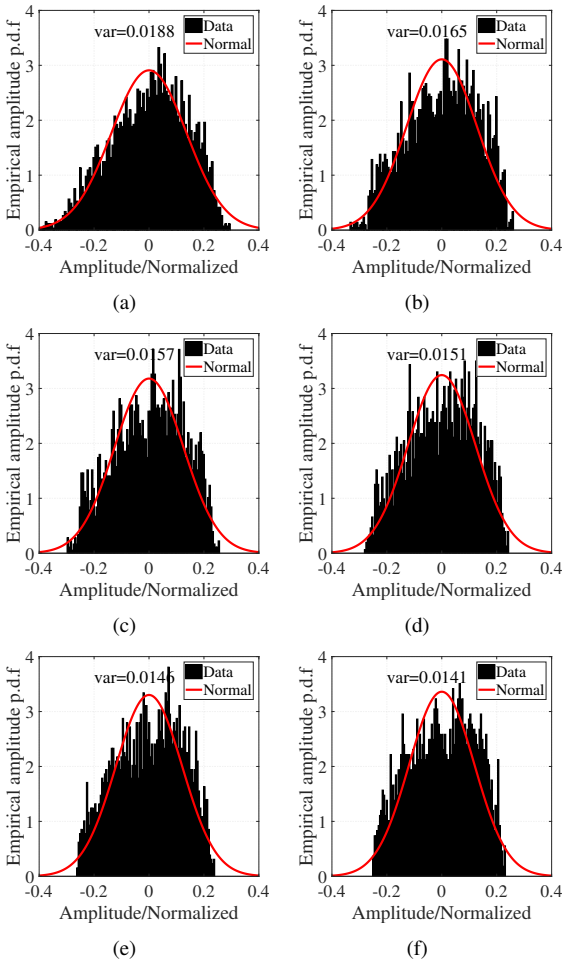

Fig. 4. Empirical amplitude of probability density function (p.d.f) after LSRS. (a)N=1. (b) N=10. (c) N=20.(d)N=30. (e) N=40. (f) N=50.

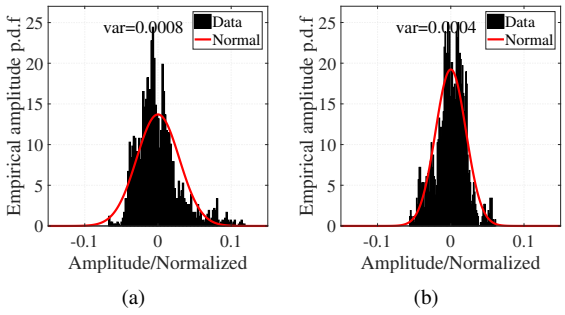

Fig. 5. Empirical amplitude of probability density function (p.d.f) after LSRS of other dimensions where $N = 50$. (a)$real(LSRS(y(T_s)))$. (b) $imag(LSRS(y(T_s)))$.

The prior probability of each device is equal:

$$p(k) = \frac{1}{N_d} \tag{13}$$

where N_d is the number of devices. Thus, for identification, the goal of our scheme is to find the device k to minimize the Mahalanobis distance between μ_k stored in local database and RFF of the received signal $F_{test,i}$ under test. And the Mahalanobis distance is calculated by

$$Mah(F_{test,i}, \mu_k) = (F_{test,i} - \mu_k)^T \Sigma^{-1} (F_{test,i} - \mu_k). \tag{14}$$

Some items in the Mahalanobis distance are independent of device k, and the Mahalanobis distance can also be written in

$$Mah'(F_{test,i}, \mu_k) = 2\Sigma^{-1}\mu_k F_{test,i} - \mu_k^T \Sigma^{-1} \mu_k \tag{15}$$

after dropping these items. This form can help us understand the decision of the system better.

D. Artificial Noise Adding Algorithm

This identification scheme after LSRS is able to work in a range of SNR due to the SNR improvement of stacking. However, the limitation of stacking number prevents the system from working in low SNR. Besides, LSRS can be hardly used to distinguish devices in multipath fading channel conditions. ANA is one promising method to enhance the robustness in these situations.

ANA arises from the belief that when the training set and the test set share a similar channel condition, the performance of recognition scheme is much better with similar channel information. And adding Gaussian artificial noise to the training set is one effective method to change the channel condition.

The processing of ANA is as below:

$$y^*(t) = \frac{y(t) + a(t)}{\sqrt{1+\sigma_a^2}} = \frac{x(t) + f(t) + a(t) + n(t)}{\sqrt{1+\sigma_a^2}} \tag{16}$$

where $a(t)$ is artificial additive Gaussian white noise with a variance of σ_a^2. SNR_a is used to denote the received signal to injected artificial noise ratio, so that $SNR_a = \infty$ corresponds to no artificial noise injection. The relationship between σ_a^2 and SNR_a is

$$\sigma_a^2 = 10^{-\frac{SNR_a}{10}}, \tag{17}$$

$\sqrt{1+\sigma_a^2}$ is the energy normalization factor.

After adding artificial noise, the SNR of the training set is

$$SNR_t = -10 \cdot log_{10}(\sigma_o^2 + \sigma_a^2(1+\sigma_o^2)) \tag{18}$$

where σ_o^2 is calculated with the orignal SNR of the training set SNR_o:

$$\sigma_o^2 = 10^{-\frac{SNR_o}{10}}, \tag{19}$$

Thus, the result after LSRS is:

$$\begin{aligned} LSRS(y^*(t)) =& \frac{x(t) + f'(t) + \frac{1}{N}\sum_{i=0}^{N-1} a(t + P_i T) + n'(t)}{\sqrt{1+\sigma_a^2}} \\ =& \frac{x(t) + f'(t) + a'(t) + n'(t)}{\sqrt{1+\sigma_a^2}}. \end{aligned} \tag{20}$$

In AWGN channels, artificial noise are added to make the training set share a similar SNR with the test set. That is, $SNR_t \approx SNR_e$, where SNR_e is the estimated SNR of the received signal. ANA enables the system to focus on the discriminative features in a specific SNR. However, adding artificial noise to the training set every time according to the SNR estimation of received signal consumes huge computation resources, and a lightweight ANA based identification scheme is in urgent need.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2021.3051402, IEEE Internet of Things Journal

Without ANA, the feature vector F after LSRS obeys the multivariate Gaussian distribution with mean μ_k and covariance Σ. ANA adds independent additive white Gaussian noise to the signal, so the feature vector with ANA in the training set, F^*, still obeys a multivariate Gaussian distribution. It is easy to get the new distribution of the feature vector,

$$p(F^*|k) = \frac{1}{(2\pi)^{\frac{n}{2}}|\Sigma^*|^{\frac{1}{2}}} exp[-\frac{1}{2}(F^* - \mu_k^*)^T \Sigma^{*-1}(F^* - \mu_k^*)], \tag{21}$$

$$\mu_k^* = \frac{\mu_k}{\sqrt{1+\sigma_a^2}}, \tag{22}$$

$$\Sigma^* = \frac{\Sigma + \frac{\sigma_a^2}{2N} I}{1+\sigma_a^2}, \tag{23}$$

where I is the identity matrix. For implementation, Σ is decomposed as $Q\Lambda Q^{-1}(Q^TQ = I)$, thus we can get the following results:

$$\Sigma^{-1} = Q\Lambda^{-1}Q^{-1}, \tag{24}$$

$$\Sigma^* = Q\frac{\Lambda + \frac{\sigma_a^2}{2N} I}{1+\sigma_a^2}Q^{-1}, \tag{25}$$

and

$$\Sigma^{*-1} = Q(\frac{\Lambda + \frac{\sigma_a^2}{2N} I}{1+\sigma_a^2})^{-1}Q^{-1} \tag{26}$$

Thus, for simplified calculation, the weighted Euclidean distance between $Q^{-1}F$ and $Q^{-1}\mu_k^*$ with the weight $(\frac{\Lambda + \frac{\sigma_a^2}{2N} I}{1+\sigma_a^2})^{-1}$ is adopted.

Thus, we can get our robust RFF identification Algorithm 1 in AWGN channels. When identifying a feature vector under test, we just need to change the SNR_a, corresponding μ_k^* and Σ^* according to the estimated SNR to compensate for the differences between the training set and the test set.

Besides compensation for the differences between AWGN channels, ANA is also an effective regularization method, and this makes ANA work in slight distorted channels with high SNR. When SNR_a is high, the energy normalization factor $\sqrt{1+\sigma_a^2}$ can be ignored, μ_k stays the same and

$$\Sigma^* = \Sigma + \frac{\sigma_a^2}{2N} I. \tag{27}$$

This is equivalent to a form of Tikhonov regularization [45]. There are two drawbacks of the original covariance matrix: it is arduous to collect sufficient signals to estimate the empirical matrix when its dimension is very high. Besides, due to the oversampling scheme, acquiring signals are highly correlated. Thus, the decision coefficient $\Sigma^{-1}\mu_k$ has a spatial rough contour [46] and slight deviations from training signals will significantly influence the identification outcomes. While after ANA, the identification scheme will be less sensitive to the channel noise. When the multipath fading is not very severe, ANA contributes to a robust performance of the system.

Algorithm 1 Robust RFF identification scheme in AWGN channels

Input: The received payload signal from USRP, $r(t)$; The stacking number, N; Identification parameters, μ_k and Σ;
Output: RFF: F; The identification result: k;

```
Preprocess r(t) to get the fine synchronization signal y(t) and its estimated SNR SNR_e, including signal detection, energy normalization, time synchronization, frequency offset compensation, phase offset compensation and SNR estimation;
F = ∅
Gather signals of the target symbol;
for each i ∈ [0, N − 1] do
    F = F + [y(T_s + P_iT), y(2T_s + P_iT), ..., y(T + P_iT)];
end for
F = F/N;
Unfold complex F to in-phase and quadrature sequences;
Calculate SNR_a to make SNR_t ≈ SNR_e;
Adjust μ_k^* and Σ^* based on SNR_a;
Find the device k minimize Mah(F, μ_k^*)
return F; k
```

V. RFF Verification Using GPLDA

Although the RFF identification scheme using LSRS and ANA in Algorithm 1 is channel robust for identification problems, one main drawback is that it can not handle the verification problem with unseen unauthorized devices. Its performance goes down sharply in this situation due to the lack of differences of μ_k between enrollment devices and imposters. This problem can be solved by making the device centers μ_k continuous and the device identity vector μ is used to describe the generation processes of μ_k. This solution is equivalent to a form of probabilistic linear discriminant analysis (PLDA) in [47] and it has been proved to be effective to make inference about the candidates not present during training in face recognition and speaker recognition. Therefore, the PLDA model is used in this paper to settle the verification problem with unseen unauthorized devices. We will first detail the whole process of verification and then try to build the generative model.

A. Verification Protocol

We implement the protocol widely used in face recognition [15] and speaker recognition [48] for verification. The protocol is divided into the three steps:

- Training: In the offline training stage, we find a suitable device representation extraction function $FR(\cdot)$ from the processed signal y and estimate basic parameters of the verification model.

$$F = FR(y) \tag{28}$$

- Enrollment: In the enrollment stage, the device k in the white list will have to provide signals for estimation of the reference template $F_{enroll,k}$. These devices are not in the training set and there are often not many signals for enrollment.

- Evaluation: For verification, a scoring function of similarity metric between the feature vector of the received signal $F_{test,i}$ and the feature vector of the enrollment device k $F_{enroll,k}$, $S(F_{test,i}, F_{enroll,k})$, is adopted. Euclidean distance and cosine similarity are common score functions. An accept/reject decision is then provided by comparing the similarity score with a pre-defined threshold value. The false reject and the false accept errors will occur in this protocol. The false acceptance rate (FAR) represents the ratio when a rogue device is accepted, while the false rejection rate (FRR) represents the ratio when a legitimate device is rejected. When the two error rates are equal, the common value is called EER. In this article, EER is used as a measurement metric for the verification model evaluation. Similarly, identification can be viewed as a k-NN problem to find the most similar reference templates, and clustering can be achieved using existing techniques such as k-means clustering.

It is always hard to collect enough signals for the model generation, especially in the enrollment stage. The one-shot recognition problems happen when there is only one sample for each device to be enrolled, and it remains a challenge for a face/speaker/device recognition system. In our experiments, only the first signal of each device is enrolled to simulate this situation.

B. Gaussian Probabilistic Linear Discriminant Analysis for Verification

Based on the PLDA model [47], the feature vector F is generated with the device identity vector μ and noise offset vector z:

$$F = \mu + z \tag{29}$$

μ remains constant for a device while z changes because of the channel and device noise. When assuming that the device identity vector and the noise vector subject to two independent Gaussian distributions, this model is called GPLDA. A heavy-tailed PLDA model (HT-PLDA) has also been proposed in [49] where the Gaussian priors are replaced by Students t distribution. One main advantage of GPLDA is that we can get a closed-form solution.

The GPLDA model $\mathcal{M}$ is defined by the following two probability distributions:

$$P(\mu|\mathcal{M}) = \mathcal{N}(\mu|m, \Phi_b), \tag{30}$$

$$P(F|\mu, \mathcal{M}) = \mathcal{N}(F|\mu, \Sigma), \tag{31}$$

where $\mathcal{N}$ denotes a Gaussian distribution, m is the overall device mean, Φ_b is the between-device covariance matrix and Σ is the within-device covariance matrix. The assumption that μ obeys the Gaussian distribution is the basis that GPLDA can be used for the presence of unauthorized devices. Expectation-maximization (EM) algorithm is needed for the estimation of m, Φ_b and Σ especially when collected signals are unbalanced, and detailed description of the model learning algorithm can be referred in [50].

After the model learning, the log likelihood ratio between the signal under test and the template of its claimed identity in the database is calculated. For a device verification task, we need to test two alternative hypotheses: $\mathcal{H}_s$ that the feature vector of the received signal $F_{test,i}$ and the feature vector of the enrollment device k $F_{enroll,k}$ are generated with the same identity vector μ, or $\mathcal{H}_\mu$ that the feature vectors are generated with different identity vectors μ_1 and μ_2. The closed-form solution is given in (32). As is discussed above, ANA is also able to help build a more robust GPLDA model.

C. Complexity Analysis

Now let us analyze the computational complexities of the proposed algorithms.

1) LSRS: To generate N_s samples with the feature dimension D and the stacking number N, there are $N_sD(N-1)$ additions and N_sD divisions in Equation 5. In total, the complexity is $\mathcal{O}(N_sND)$.

2) ANA: ANA adjusts the D eigenvalues of N_s samples through Equation 26. Thus, its complexity is $\mathcal{O}(N_sD)$.

3) Mahalanobis Distance: In the training stage, with N_s training samples, the calculation of mean vector is $\mathcal{O}(N_sD)$, the calculation of covariance is $\mathcal{O}(N_sD^2)$ and the decomposition is $\mathcal{O}(D^3)$. To get the covariance matrix, N_s should be much larger than D. Thus, the dominated term is $\mathcal{O}(N_sD^2)$. To store the parameters of N_d device: μ, Q^{-1} and Λ^{-1}, the memory requirement is $\mathcal{O}(N_dD + D^2 + D)$. In the test stage, with N_s candidate samples, the complexity is dominated by the projection of $Q^{-1}F$ with $\mathcal{O}(N_sD^2)$.

4) GPLDA: With a balanced data set, the training stage of GPLDA is similar to the Mahalanobis distance, its complexity is also $\mathcal{O}(N_sD^2)$ with extra memory requirement is $\mathcal{O}(2D^2 + 2D)$ for m, Φ_b and the eigenvalues and eigenvectors of Σ. In the enrollment stage, $\mathcal{O}(N_dD)$ extra memory requirement for the N_d authorized devices. In the evaluation stage, with N_s candidate samples, the complexity is also $\mathcal{O}(N_sD^2)$ in Equation 32 according to [51].

To conclude, the computational complexity and the memory requirement are mainly determined by the number of samples and the square of the feature dimension. In our scheme, the feature dimension D of Equation 8 is $2\frac{T}{T_s}$. That is, D is

$$\begin{aligned} score &= log\frac{p(F_{test,i}, F_{enroll,k}|\mathcal{H}_s)}{p(F_{test,i}|\mathcal{H}_\mu)p(F_{enroll,k}|\mathcal{H}_\mu)} \\ &= log\mathcal{N}\left(\begin{bmatrix} F_{test,i} \\ F_{enroll,k} \end{bmatrix}; \begin{bmatrix} m \\ m \end{bmatrix}, \begin{bmatrix} \Sigma + \Phi_b\Phi_b^T & \Phi_b\Phi_b^T \\ \Phi_b\Phi_b^T & \Sigma + \Phi_b\Phi_b^T \end{bmatrix}\right) \\ &- log\mathcal{N}\left(F_{test,i}; m, \Sigma + \Phi_b\Phi_b^T\right) - log\mathcal{N}\left(F_{enroll,k}; m, \Sigma + \Phi_b\Phi_b^T\right) \end{aligned} \tag{32}$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2021.3051402, IEEE Internet of Things Journal

determined by the sampling rate. When they are large, the system may require a certain computation. But in our system the computation mainly occurs at the powerful network center (e.g., gateway) without any extra computation cost of the IoT devices.

VI. EXPERIMENTAL IMPLEMENTATION AND RESULTS

In this section, we present the performance of our scheme through different experiments, and we mainly focus on the identification performance in long-term experiments and different channels and the verification performance with the presence of unseen unauthorized devices.

A. Dataset Generation

Using the aforementioned signal collection setup, we captured samples continuously over 22 months. For the exploration of repetitive symbols, the payload of the data unit is set to zeros. That is, the symbol zero is chosen as the target symbol for LSRS. The layout of the experimental environment is shown in Fig. 6 where RX is the receiver (USRP N210) and TX denotes the transmitter (ZigBee CC2530 devices). The information of the collected datasets is summarized in Table II.

In the short rang LOS (SLOS) scenarios where the ZigBee devices and the USRP were positioned close to each other, in a range of 0.3-2m (TX1 and RX1 in Fig. 6), 4 rounds experiments have been carried out on four different days across 22 months. The signals are collected device by device, and a device has only to work for minutes in each round of experiments. Acquired signals of the first experiment were partitioned into two sets: 80% as the training set SLOS1 and 20% as the test set SLOS2. Datasets SLOS3 and SLOS4 collected after 18 months were used to verify the long-term stability. Dataset SLOS5 with only 12 devices was used for later comparisons in various channel conditions because the first 12 devices with power amplifiers was able to transmit signals in long-range experiments. The SNR of SLOS situations was as high as 26 dB.

For the evaluation of channel distortions, we mainly focus on small scale fading in indoor environments. Due to the narrow band signals of ZigBee devices, the small Doppler shift and the device movement have little effects on the identification. Thus, multipath fading channels are our main considerations and two typical scenarios are chosen: the non-line of sight scenarios without a direct propagation line and the long distance line of sight scenario. In the non-line-of-sight (NLOS) scenarios, the ZigBee devices were placed in a corridor while the USRP was fixed in the same place as SLOS scenarios did without a direct propagation line. The distance between them was about 10-20 m in NLOS1 (TX2 and RX1) and NLOS2 (TX3 and RX1). As for the long-distance line-of-sight (LLOS) scenarios, the ZigBee devices and the USRP were located at the ends of the long corridor (TX4 and RX2). There was serious multipath fading due to the signals reflected by walls or pedestrians. The gain of the USRP was raised to properly receive and process the signals. The SNR was around

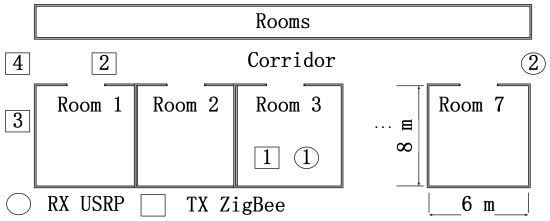

Fig. 6. Layout of the experimental environment.

20-25 dB in NLOS and 25 dB in LLOS. These datasets were used for the test of robustness in different channel conditions.

B. Baseline RFF Recognition Schemes

For comparison, we have implemented two typical RFF schemes: the radio frequency distinct native attribute (RF-DNA) in [25] and CNN in [28]. In [25], 8 contiguous symbols are used to calculate the instantaneous amplitude, phase, and frequency responses. Then each response sequence is divided into 80 equal length sub-sequences to obtain the statistical features consisting of variance, skewness, and kurtosis. In total, there are 3*3*80 features for one input sample. The Mahalanobis distance is used for recognition. To improve the performance in low SNR, the RF-DNA has to train a classifier in every SNR.

The convolutional neural network (CNN) of [28] is summarized in Table III. The input layer and output layer have been modified according to our datasets. The input sequence consists of 4 contiguous error signal symbols. Then all the estimated probabilities obtained by the network in one frame are gathered to calculate the probability that which device the frame belongs to. To improve the performance in low SNR, a network with more neurons, which is summarized in Table IV, is trained in a dataset of signals simulated in all SNRs. The verification scheme of CNN is incompatible with our protocol, so it is not implemented in the verification experiments. All the experiments are completed via a PC with Intel i7-7700, single thread at 2.8 GHz. An NVIDIA GeForce GTX 1060 GPU is used for training CNN with TensorFlow 2.1.0.

C. Identification Results in Long-term Experiments

For evaluating how the stacking number of LSRS will affect the long-term stability, experiments are carried out with MATLAB using datasets SLOS1, SLOS2, SLOS3 and SLOS4. SLOS1 acts as the training set and other datasets form the test sets. That is, the long-term stability is tested in a period around 18 months.

Table V describes the identification results with various stacking factors where $N = \{1, 8, 20, 30, 40, 50, 60\}$. When $N = 1$, although it performs well in SLOS2, the accuracies in SLOS3 and SLOS4 are significantly degraded by around 5% because of the long-term variation. As N continues to go up, there is a sharp rise in the performance of all test sets. When N grows to 60, there is only 0.43% loss of accuracy in SLOS3, which demonstrates the efficiency of LSRS on the reduction of the time-varying device noise and channel noise.

TABLE II
DESCRIPTION OF EXPERIMENTS

Location	Name	Population	Time	Frames	Remark
TX1 and RX1	SLOS1	54	2016.6	1728	Short range LOS (0.3-2m)
TX1 and RX1	SLOS2	54	2016.6	432	Short range LOS (0.3-2m)
TX1 and RX1	SLOS3	54	2017.12	864	Short range LOS (0.3-2m)
TX1 and RX1	SLOS4	54	2018.1	864	Short range LOS (0.3-2m)
TX1 and RX1	SLOS5	12	2018.4	360	Short range LOS (0.3-2m)
TX2 and RX1	NLOS1	12	2018.4	720	NLOS (10-20m)
TX3 and RX1	NLOS2	12	2018.4	360	NLOS (10-20m), more walls
TX4 and RX2	LLOS	12	2018.4	360	Long distance LOS (40m)

TABLE III
LAYERS, THE NUMBER OF PARAMETERS AND ACTIVATION FUNCTIONS OF THE CNN NETWORK

Layer	Dimension	Parameters	Activation
Input	640×2	-	-
Convolution 1D	128×19	4992	ELU
Max Pooling	2	-	-
Convolution 1D	32×15	61472	ELU
Max Pooling	2	-	-
Convolution 1D	16×11	5648	ELU
Max Pooling	2	-	-
Flatten	-	-	-
Dense	128	141440	ELU
Dropout(0.5)	-	-	-
Dense	16	2064	ELU
Dropout(0.5)	-	-	-
Dense	54	918	Softmax

TABLE IV
LAYERS, THE NUMBER OF PARAMETERS AND ACTIVATION FUNCTIONS OF THE CNN(NOISE) NETWORK

Layer	Dimension	Parameters	Activation
Input	640×2	-	-
Convolution 1D	128×19	4992	ELU
Max Pooling	2	-	-
Convolution 1D	32×15	61472	ELU
Max Pooling	2	-	-
Convolution 1D	16×11	5648	ELU
Max Pooling	2	-	-
Flatten	-	-	-
Dense	128	141440	ELU
Dropout(0.5)	-	-	-
Dense	64	8256	ELU
Dropout(0.5)	-	-	-
Dense	54	3510	Softmax

TABLE V
IMPACT OF STACKING FACTOR N IN LONG-TERM EXPERIMENTS

Accuracy/% Test Set / Scheme	SLOS2	SLOS3	SLOS4
LSRS ($N = 1$)	99.88	94.86	94.36
LSRS ($N = 8$)	100.00	97.99	98.15
LSRS ($N = 20$)	100.00	99.50	99.18
LSRS ($N = 30$)	100.00	99.54	99.40
LSRS ($N = 40$)	100.00	99.56	99.46
LSRS ($N = 50$)	100.00	99.58	99.45
LSRS ($N = 60$)	100.00	99.57	99.51
RF-DNA	99.74	94.19	93.54
CNN	100.00	63.15	76.07

Although increasing stacking number N leads to better performance, a practical system should choose appropriate parameters to match the security level of demand. When the data frame is not well-designed as ours, LSRS could still work by taking advantage of some fixed structures such as the preamble. It is practical for the system to collect around 10-20 zero symbols in one or two frames as there are already eight zero symbols in the preamble of a typical frame. As is shown in the Table V, when N reaches 20, the increase of stacking number leads to subtle improvement in accuracy. Considering the practicability and identification accuracy, 20 is a suitable choice.

As is illustrated in Table V, both CNN and RF-DNA work well in SLOS2. There are around 5% decrease in the accuracies of SLOS3 and SLOS4 for RF-DNA, which is similar to our scheme without stacking. Comparing RF-DNA and LSRS ($N = 8$), the results demonstrate the effectiveness of LSRS in long-term experiments. As for the CNN results in SLOS3 and SLOS4, the network is likely to overfit in SLOS1.

To summarize, although the time-varying device noise and channel noise leads to performance deterioration in long-term experiments, the proposed LSRS algorithm reduces the influences effectively, which contributes to the identification accuracy and time stability.

D. Identification Results in Different Channel Scenarios

Next, we evaluate the robustness of our scheme in different channel scenarios including AWGN channels and multipath channels.

1) Identification Results in AWGN channels: The robustness of our scheme in AWGN channels is evaluated through MATLAB simulation with the training set SLOS1 and the test set SLOS2, where the SNR of test set $SNR_e = \{0, 5, 10, 15, 20, 26\}$ dB.

Fig. 7(a) shows the identification results in AWGN channels with different stacking number after LSRS. It can be seen that without applying any scheme, the performance goes down sharply with the decline of SNR. Through the enhancement with LSRS, when N is over 20, the slight change of SNR has almost no effect on the identification results in $SNR_e >$ 20 dB. However, the large consumption of symbols of LSRS in low SNR is often difficult to meet. Compared with the results of RF-DNA and CNN, LSRS is able to improve the performance in AWGN more efficiently.

Fig. 7(b) shows the identification results in AWGN channels after ANA. Compared with results without ANA, when

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2021.3051402, IEEE Internet of Things Journal

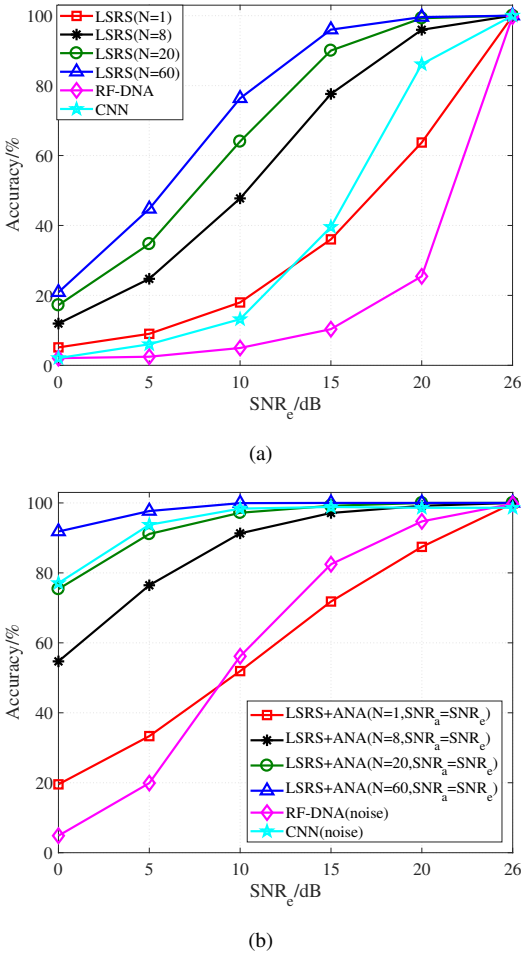

Fig. 7. Identification Results in AWGN channels. (a) Identification results with LSRS. (b) Identification results with LSRS+ANA.

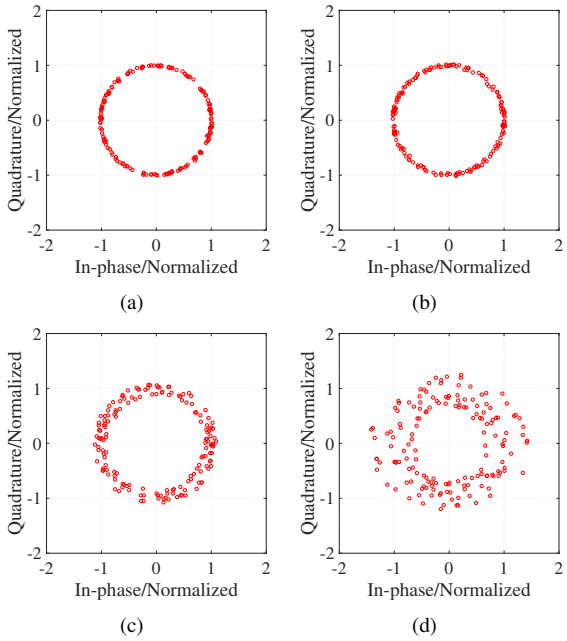

Fig. 8. Constellation of device 1 in different situation. (a) Constellation of SLOS1. (b) Constellation of SLOS5. (c) Constellation of NLOS1. (d) Constellation of LLOS.

$N = 1$, there are around 35% improvement in the accuracy of 15 dB. As N grows to 20, ANA improves the accuracy by 56.41% and 33.17% in 5 dB and 10 dB, respectively, which demonstrates the effectiveness of ANA. When $N = 60$, the system is able to work in the range of 5 dB to 26 dB with an acceptable identification accuracy. The adaptive ANA algorithm forces the system to find discriminative features in a specific SNR and this accounts for the good performance in the figure. There are obvious performance improvements for RF-DNA (noise) and CNN (noise) trained in simulated noise signals. And the accuracy of CNN (noise) is between that of LSRS+ANA ($N = 20, SNR_a = SNR_e$) and LSRS+ANA ($N = 60, SNR_a = SNR_e$). That is, our scheme is able to achieve better performance with less demand for the data. The main advantage of our scheme is that our parameters are calculated instead of simulation, which leads to less computation complexity and better performance.

2) Identification Results in multipath channels: The robustness of our scheme in various channel conditions is evaluated with the training set SLOS1 and test sets SLOS5, NLOS1, NLOS2, LLOS. To give an intuition of the channel conditions, in Fig. 8, the oversampling IQ samples in different test sets are plotted in the constellations. The long-term variation is not obvious in the constellation, while in NLOS1 and LLOS, noise and multipath shape the figures significantly. There are more than two circles in NLOS and LLOS caused by various propagation paths. The channel condition in LLOS is much worse because there are more obstacles in the long corridor between ZigBee and USRP.

In order to act as an effective regularization method, suitable artificial noise is needed to improve the performance in multipath fading channels without harming the results in SLOS situations. The original SNR of SLOS1 is around 26 dB, and adding artificial noise will change the actual SNR SNR_t of the training set. Fig. 9 shows the influence of SNR_a on the SNR_t. When SNR_a is over 40 dB, ANA has almost no influence on SNR_t because artificial noise is much smaller than the inherent noise of SLOS1. When SNR_a is below 20 dB, $SNR_t \approx SNR_a$. This leads to the performance degradation because of heavy Gaussian noise. When SNR_a is between 25 dB and 35 dB, the actual SNR is a little below 26 dB. Because of the SNR improvement resulting from LSRS, the slight change of SNR will not affect the identification results in short range LOS channels. Thus ANA with SNR_a between 25 dB and 35 dB could act as a regularization method, and in our scheme, we choose an intermediate value, 30 dB.

In Fig. 10, artificial noise of various $SNR_a = \{10, 20, 30, 40, 50, 60\}$ is added to the training set. Test sets of different channel situations are used to demonstrate how the regularization artificial noise works. When SNR_a is over 40 dB, artificial noise is small and the Tikhonov regularization is ineffective. The results in different channels is close to that without artificial noise ($SNR_a = \infty$). When SNR_a is much lower than the original SNR, jitter of artificial noise prevents the system from finding suitable representations in multipath channels in that SNR. The mismatch of SNRs brings about

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2021.3051402, IEEE Internet of Things Journal

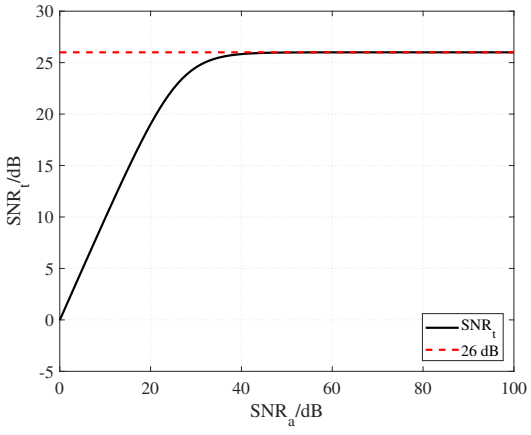

Fig. 9. SNR_a and SNR_t.

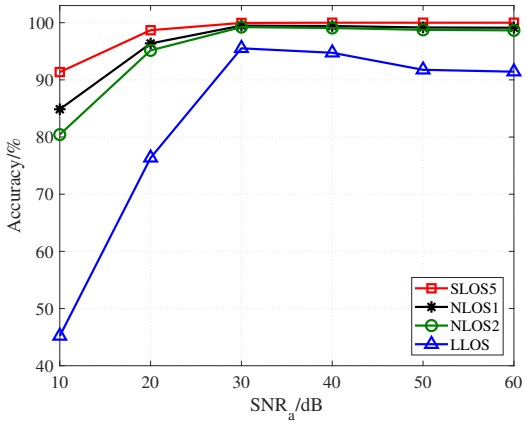

Fig. 10. Accuracy in test sets with different SNR_a, where the stacking number N is set to 20.

TABLE VI
RESULTS IN MULTIPATH CHANNELS

Accuracy/% Test Set / Scheme	SLOS5	NLOS1	NLOS2	LLOS
RF-DNA	99.69	90.47	67.37	25.72
CNN	83.05	62.50	61.42	26.97
LSRS ($N = 8$)	99.98	98.21	95.22	91.55
LSRS ($N = 20$)	100.00	99.12	98.65	91.36
LSRS+ANA ($N = 20$, $SNR_a = 30$ dB)	99.96	99.49	99.23	95.52

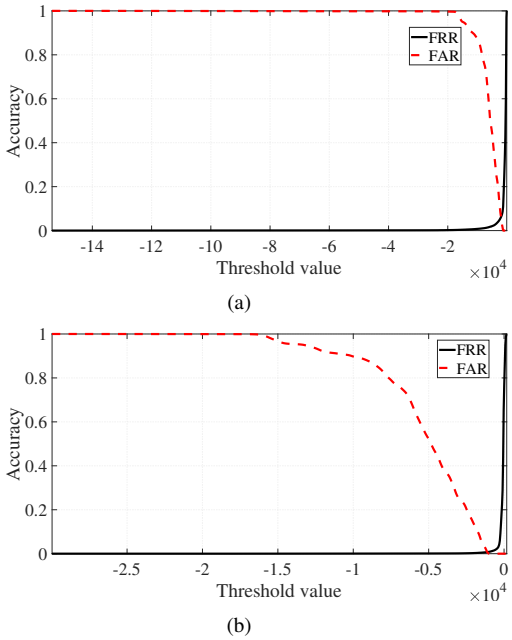

Fig. 11. FAR and FRR versus the threshold in the mixed test set. (a) LSRS+Mah ($N = 20$) (b) LSRS+GPLDA ($N = 20$).

the decline of accuracy. The identification accuracy rises to a high point and peaks when SNR_a of is around 30 dB. In this situation, ANA makes a good trade-off between regularization and effective device information. The artificial noise does not change the actual SNR significantly and forces the system to learn robust representations in multipath channels through regularization.

A thorough comparison is shown in Table VI. There is a significant decrease in the performance of RF-DNA in the multipath channels. Due to the overfitting, CNN does not have an acceptable performance even in SLOS5. Comparing with LSRS ($N = 8$) and LSRS ($N = 20$), large N contributes to the accuracies in NLOS while it is ineffective in LLOS. As is discussed above, to make sure ANA could acts as a regularization method, N should be large. Otherwise, the slight change of SNR will affect the identification accuracy because of the SNR mismatch. Thus, no regularization artificial noise is added when $N = 8$. After applying regularization artificial noise when $N = 20$, although there is slight decline in the accuracy of SLOS5, better performance is achieved in all multipath fading test sets. It is noticeable that ANA can improve the accuracy in LLOS by 4.16%.

To sum up, the ANA algorithm helps improve the performance in AWGN channels through adjusting the system parameters and enables robust device identification in multipath channels via regularization.

E. Verification Results

Finally, the performance of the verification problem is evaluated in this part based on the proposed verification protocol. In the training stage, device 13-54 in the training set SLOS1 are used to estimate the basic parameters for different models. In the enrollment stage, the first signals of device 1-6 in the training set are enrolled as the legal devices to simulate the one-shot problem. In the evaluation stage, devices 1-12 in the test sets SLOS2, SLOS3, SLOS4 and SLOS5 will try to get access to the system by claiming to be devices 1-6. One thing to note is that authorized devices can also access the system illegally by pretending to be other authorized devices. The similarity between the device representation under test $F_{test,i}$ and the representation of enrollment model $F_{enroll,k}$, $S(F_{test,i}, F_{enroll,k})$ is computed to give an accept/reject response, using the Mahalanobis distance or the likelihood ratio.

Table VII shows the verification results. Verification results of a mixed test set including all the data of SLOS2, SLOS3,

TABLE VII
VERIFICATION RESULTS WITH UNSEEN DEVICES

EER/% Situations / Schemes	SLOS2	SLOS3	SLOS4	SLOS5	Mixed
RF-DNA	10.37	10.73	10.55	13.09	11.72
LSRS+Mah ($N = 8$)	6.52	7.99	7.69	6.85	7.25
LSRS+Mah ($N = 20$)	5.28	6.46	6.86	5.82	6.13
LSRS+ANA+Mah ($N = 20$, $SNR_a = 30$ dB)	5.37	6.10	6.00	5.42	5.71
LSRS+GPLDA ($N = 8$)	1.06	1.25	1.48	1.05	1.20
LSRS+GPLDA ($N = 20$)	0.52	0.64	1.15	0.57	0.71
LSRS+ANA+GPLDA ($N = 20$, $SNR_a = 30$ dB)	0.60	0.51	1.01	0.52	0.63

SLOS4 and SLO5 are also presented. The EER of RF-DNA scheme is over 10%, and LSRS+Mah (N=8) is a bit better. When $N = 8$, the EER of GPLDA in the mixed test set is around one-sixth of our Mahalanobis verification result. When $N = 20$, the EER of GPLDA in the mixed test set is around one-ninth of our Mahalanobis verification result. This phenomenon is consistent with our expectations in consideration of the capacity of GPLDA to make inference of unseen devices. When calculating Mahalanobis distance, class centers μ_k are viewed as a finite set of points, which prevents the system from solving previously unseen devices. While in the generative GPLDA model, it is a simple hypothesis testing problem. Besides GPLDA, ANA also contributes to the low EER by making the system less sensitive to the perturbation caused by the jitter of input signals through regularization. Consistent with the analysis, the joint scheme of LSRS, ANA and GPLDA performs the best.

Fig. 11 shows the FAR and FRR versus the threshold for the LSRS+Mah ($N = 20$) scheme and LSRS+GPLDA ($N = 20$) scheme, respectively. For comparison, the x-axis in Fig. 11(a) represents the minus of the Mahalanobis distance. That is, the greater the distance/log likelihood ratio is, the more similar the devices are. With the increase of the threshold, the system is less likely to accept the device under test, which accounts for the rise in FRR and the opposite in FAR. The Y-axis value of the point at which the lines intersect is EER. The lower the EER, the better the system.

To conclude, in the experiments of six unauthorized devices, as a joint effect of LSRS, ANA and GPLDA, our scheme allows a device to be correctly verified with near-perfect performance.

VII. CONCLUSION

This paper presents a robust RFF extraction scheme based on LSRS, ANA and the GPLDA model. The LSRS algorithm alleviates the influence of time by reducing the variances of acquired signals. The ANA algorithm in the training stage enhances the identification robustness under time-variant channels through regularization and channel adaptation. Extracted RFF based on our scheme is stable over 18 months, and robust in AWGN or slight distorted multipath channels. For the verification problem with six unauthorized devices, the EER is as low as 0.63%.

The proposed scheme is based on repetitive symbols, and it can be applied to IoT technologies with specific repetitive symbols such as LoRaWAN. Our future work will focus on more advanced radio protocols like NB-IoT and 5G-NR. Besides, we will also further consider more complex multipath fading channels.

REFERENCES

[1] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Comput. Netw.*, vol. 54, no. 15, pp. 2787–2805, Oct. 2010.

[2] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of things for smart cities," *IEEE Internet Things J.*, vol. 1, no. 1, pp. 22–32, Feb. 2014.

[3] S. B. Baker, W. Xiang, and I. Atkinson, "Internet of things for smart healthcare: Technologies, challenges, and opportunities," *IEEE Access*, vol. 5, pp. 26 521–26 544, Nov. 2017.

[4] R. Squire and H. Song, "Cyber-physical systems opportunities in the chemical industry: A security and emergency management example," *Process. Saf. Program.*, vol. 33, no. 4, pp. 329–332, Dec. 2014.

[5] N. Vidgren, K. Haataja, J. L. Patino-Andres, J. J. Ramirez-Sanchis, and P. Toivanen, "Security threats in ZigBee-enabled systems: Vulnerability evaluation, practical experiments, countermeasures, and lessons learned," in *Proc. 46th Hawaii Int. Conf. Syst. Sci. (HICSS)*, Wailea, Maui, Hawaii, USA, Jan. 2013, pp. 5132–5138.

[6] P. Radmand, M. Domingo, J. Singh, J. Arnedo, A. Talevski, S. Petersen, and S. Carlsen, "ZigBee/ZigBee PRO security assessment based on compromised cryptographic keys," in *Proc. Int. Conf. P2P Parallel Grid Cloud Internet Comput. (3PGCIC)*, Fukuoka, Japan, Nov. 2010, pp. 465–470.

[7] B. Danev, D. Zanetti, and S. Capkun, "On physical-layer identification of wireless devices," *ACM Comput. Survys*, vol. 45, no. 1, pp. 1–29, Nov. 2012.

[8] T. Rahman, D. Forte, J. Fahrny, and M. Tehranipoor, "ARO-PUF: An aging-resistant ring oscillator PUF design," in *Proc. Design Autom. Test Eur. Conf. Exhibit. (DATE)*, Dresden, Germany, Mar. 2014, pp. 1–6.

[9] D. A. Knox and T. Kunz, "Wireless fingerprints inside a wireless sensor network," *ACM Trans. Sen. Netw.*, vol. 11, no. 2, p. 130, Feb. 2015.

[10] C. Zhao, Z. Cai, M. Huang, M. Shi, X. Du, and M. Guizani, "The identification of secular variation in IoT based on transfer learning," in *Proc. Int. Conf. Comput. Netw. Commun. (ICNC)*, Maui, HI, USA, Mar. 2018, pp. 878–882.

[11] B. Danev and S. Capkun, "Transient-based identification of wireless sensor nodes," in *Proc. Int. Conf. Inf. Process. Sensor Netw. (IPSN)*, San Francisco, CA, USA, Apr. 2009, pp. 25–36.

[12] D. Zanetti, "Exploring the physical-layer identification of GSM devices," *Zurich Eth Department of Computer Science*, 2012.

[13] 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, Feb. 2019.

[14] J. K. Tugnait, "Using artificial noise to improve detection performance for wireless user authentication in time-variant channels," *IEEE Wireless Commun. Lett.*, vol. 3, no. 4, pp. 377–380, Aug. 2014.

[15] F. Schroff, D. Kalenichenko, and J. Philbin, "Facenet: A unified embedding for face recognition and clustering," in *Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit. (CVPR)*, Boston, MA, USA, Jun. 2015, pp. 815–823.

[16] C. K. Dubendorfer, B. W. Ramsey, and M. A. Temple, "An RF-DNA verification process for ZigBee networks," in *Proc. IEEE Mil. Commun. Conf. (MILCOM)*, Orlando, FL, USA, Nov. 2012, pp. 1–6.

[17] X. Zhou, A. Hu, G. Li, L. Peng, Y. Xing, and J. Yu, "Design of a robust RF fingerprint generation and classification scheme for practical device identification," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, Jun. 2019, pp. 196–204.

[18] H. Patel, M. A. Temple, and B. W. Ramsey, "Comparison of high-end and low-end receivers for RF-DNA fingerprinting," in *Proc. IEEE Mil. Commun. Conf. (MILCOM)*, Baltimore, MD, USA, Oct. 2014, pp. 24–29.

[19] M. Barbeau, J. Hall, and E. Kranakis, "Detection of rogue devices in bluetooth networks using radio frequency fingerprinting," in *Proc. 3rd IASTED Int. Conf. Commun. and Computer Networks (CCN)*, Lima, Peru, Oct. 2006, pp. 4–6.

[20] Y. Yuan, Z. Huang, F. Wang, and X. Wang, "Radio specific emitter identification based on nonlinear characteristics of signal," in *Proc. IEEE Int. Black Sea Conf. Commun. Netw. (BlackSeaCom)*, Constanta, Romania, May 2015, pp. 77–81.

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

[22] 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 Telecommun. Conf. (GLOBECOM)*, Miami, FL, USA, Dec. 2010, pp. 1–6.

[23] D. R. Reising, M. A. Temple, and J. A. Jackson, "Authorized and rogue device discrimination using dimensionally reduced RF-DNA fingerprints," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 6, pp. 1180–1192, Jun 2015.

[24] R. M. Bolle, J. H. Connell, S. Pankanti, N. K. Ratha, and A. W. Senior, *Guide to biometrics*. Springer Science & Business Media, 2013.

[25] H. J. Patel, M. A. Temple, and R. O. Baldwin, "Improving ZigBee device network authentication using ensemble decision tree classifiers with radio frequency distinct native attribute fingerprinting," *IEEE Trans. Rel.*, vol. 64, no. 1, pp. 221–233, 2015.

[26] F. Demers and M. St-Hilaire, "Radiometric identification of LTE transmitters," in *Proc. IEEE Glob. Telecommun. Conf. (GLOBECOM)*, Atlanta, GA, USA, Dec. 2013, pp. 4116–4121.

[27] G. Li, J. Yu, Y. Xing, and A. Hu, "Location-invariant physical layer identification approach for wifi devices," *IEEE Access*, vol. 7, pp. 106 974–106 986, 2019.

[28] K. Merchant, S. Revay, G. Stantchev, and B. Nousain, "Deep learning for RF device fingerprinting in cognitive communication networks," *IEEE J. Sel. Topics Signal Process.*, vol. 12, no. 1, pp. 160–167, Feb. 2018.

[29] J. Yu, A. Hu, G. Li, and L. Peng, "A robust RF fingerprinting approach using multisampling convolutional neural network," *IEEE Internet Things J.*, vol. 6, no. 4, pp. 6786–6799, Aug. 2019.

[30] Q. Wu, C. Feres, D. Kuzmenko, D. Zhi, Z. Yu, X. Liu *et al.*, "Deep learning based RF fingerprinting for device identification and wireless security," *Electron. Lett.*, vol. 54, no. 24, pp. 1405–1407, Nov. 2018.

[31] Y. Lin, Y. Tu, and Z. Dou, "An improved neural network pruning technology for automatic modulation classification in edge devices," *IEEE Trans. Veh. Technol.*, vol. 69, no. 5, pp. 5703–5706, Mar. 2020.

[32] Y. Wang, J. Gui, Y. Yin, J. Wang, J. Sun, G. Gui, H. Gacanin, H. Sari, and F. Adachi, "Automatic modulation classification for MIMO systems via deep learning and zero-forcing equalization," *IEEE Trans. Veh. Technol.*, vol. 69, no. 5, pp. 5688–5692, Mar. 2020.

[33] Y. Wang, J. Yang, M. Liu, and G. Gui, "Lightamc: Lightweight automatic modulation classification via deep learning and compressive sensing," *IEEE Trans. Veh. Technol.*, vol. 69, no. 3, pp. 3491–3495, Feb. 2020.

[34] A. C. Polak, S. Dolatshahi, and D. L. Goeckel, "Identifying wireless users via transmitter imperfections," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 7, pp. 1469–1479, 2011.

[35] W. Wang, Z. Sun, S. Piao, B. Zhu, and K. Ren, "Wireless physical-layer identification: Modeling and validation," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 9, pp. 2091–2106, Sep. 2016.

[36] J. H. K. Vuolevi, T. Rahkonen, and J. P. A. Manninen, "Measurement technique for characterizing memory effects in RF power amplifiers," *IEEE Trans. Microw. Theory Tech.*, vol. 49, no. 8, pp. 1383–1389, Aug. 2001.

[37] T. Zheng, Z. Sun, and K. Ren, "FID: Function modeling-based data-independent and channel-robust physical-layer identification," in *Proc. IEEE Int. Conf. Comput. Commun. (INFOCOM)*, Paris, France, Apr. 2019, pp. 199–207.

[38] A. C. Polak and D. L. Goeckel, "Wireless device identification based on RF oscillator imperfections," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 12, pp. 2492–2501, Dec. 2015.

[39] N. Garmendia and J. Portilla, "Study of PM noise and noise figure in low noise amplifiers working under small and large signal conditions," in *Proc. IEEE MTT-S Int. Microw. Symp.*, Honolulu, HI, USA, Jun. 2007, pp. 2095–2098.

[40] F. Bonani, S. D. Guerrieri, and G. Ghione, "Noise source modeling for cyclostationary noise analysis in large-signal device operation," *IEEE Trans. Electron Devices*, vol. 49, no. 9, pp. 1640–1647, Sep. 2002.

[41] Y. Xing, A. Hu, J. Zhang, L. Peng, and G. Li, "On radio frequency fingerprint identification for DSSS systems in low SNR scenarios," *IEEE Commun. Lett.*, vol. 22, no. 11, pp. 2326–2329, Nov. 2018.

[42] S. Andrews, R. M. Gerdes, and M. Li, "Crowdsourced measurements for device fingerprinting," in *Proc. 12th ACM Conf. Security Privacy Wireless Mobile Netw. (WiSec)*, Miami, FL, USA, May 2019, pp. 72–82.

[43] R. O. Duda, P. E. Hart, and D. G. Stork, *Pattern classification*. John Wiley & Sons, 2012.

[44] F. Pedregosa, G. Varoquaux, A. Gramfort, V. Michel, B. Thirion, O. Grisel, M. Blondel, P. Prettenhofer, R. Weiss, V. Dubourg, J. Vanderplas, A. Passos, D. Cournapeau, M. Brucher, M. Perrot, and E. Duchesnay, "Scikit-learn: Machine learning in Python," *J. Mach. Learning Res.*, vol. 12, pp. 2825–2830, 2011.

[45] C. M. Bishop, "Training with noise is equivalent to tikhonov regularization," *Neural Comput.*, vol. 7, no. 1, pp. 108–116, Jan. 1995.

[46] T. Hastie, A. Buja, and R. Tibshirani, "Penalized discriminant analysis," *The Annals of Statistics*, pp. 73–102, Feb. 1995.

[47] N. Brümmer and E. De Villiers, "The speaker partitioning problem." in *Odyssey*, 2010, paper 034.

[48] G. Heigold, I. Moreno, S. Bengio, and N. Shazeer, "End-to-end text-dependent speaker verification," in *Proc. IEEE Int. Conf. Acoust. Speech Signal Process. (ICASSP)*, Shanghai, China, Mar. 2016, pp. 5115–5119.

[49] P. Kenny, "Bayesian speaker verification with heavy-tailed priors." in *Odyssey*, vol. 14, 2010, paper 014.

[50] A. Sizov, K. A. Lee, and T. Kinnunen, "Unifying probabilistic linear discriminant analysis variants in biometric authentication," in *Proc. Joint IAPR Int. Workshop Struct. Syntactic Statist. Pattern Recognit. (S+SSPR)*, Joensuu, Finland, Aug. 2014, pp. 464–475.

[51] P. Rajan, A. Afanasyev, V. Hautamäki, and T. Kinnunen, "From single to multiple enrollment i-vectors: Practical PLDA scoring variants for speaker verification," *Digital Signal Processing*, vol. 31, pp. 93–101, Aug. 2014.