

On the Use of Power Amplifier Nonlinearity Quotient to Improve Radio Frequency Fingerprint Identification in Time-Varying Channels

Lu Yang*, Seyit Camtepe[†], Yansong Gao[†], Vicky Liu[‡], and Dhammika Jayalath*

*Faculty of Engineering, Queensland University of Technology, Brisbane, Australia

[†]Data61, CSIRO, Sydney, Australia

[‡]Faculty of Science, Queensland University of Technology, Brisbane, Australia

Corresponding Author: Lu Yang (Email: l41.yang@hdr.qut.edu.au)

Abstract—Radio frequency fingerprint identification (RFFI) is a lightweight device authentication technique particularly desirable for power-constrained devices, e.g., the Internet of things (IoT) devices. Similar to biometric fingerprinting, RFFI exploits the intrinsic and unique hardware impairments resulting from manufacturing, such as power amplifier (PA) nonlinearity, to develop methods for device detection and classification. Due to the nature of wireless transmission, received signals are volatile when communication environments change. The resulting radio frequency fingerprints (RFFs) are distorted, leading to low device detection and classification accuracy. We propose a PA nonlinearity quotient and transfer learning classifier to design the environment-robust RFFI method. Firstly, we formalized and demonstrated that the PA nonlinearity quotient is independent of environmental changes. Secondly, we implemented transfer learning on a base classifier generated by data collected in an anechoic chamber, further improving device authentication and reducing disk and memory storage requirements. Extensive experiments, including indoor and outdoor settings, were carried out using LoRa devices. It is corroborated that the proposed PA nonlinearity quotient and transfer learning classifier significantly improved device detection and device classification accuracy. For example, the classification accuracy was improved by 33.3% and 34.5% under indoor and outdoor settings, respectively, compared to conventional deep learning and spectrogram-based classifiers.

Index Terms—Internet of things, device authentication, radio frequency fingerprinting identification, power amplifier nonlinearity, transfer learning.

I. INTRODUCTION

The rapid growth of the Internet of things (IoT) device population has sparked extensive demands on IoT security in recent years. Many security-critical IoT applications need more stringent security support [1]. Device authentication is one of the most important categories, which includes rogue device detection and the classification of registered devices [2]. Traditionally, device authentication is achieved by public-key cryptography (PKC). However, the implemented public key algorithms are not optimal for IoT devices because they are computationally costly. Further, PKC generally requires a certification authority when sharing keys. The authority may not always be available, considering the large volume and wide-area deployment of IoT devices [3].

A lightweight and reliable authentication technique is thus required for IoT security. Radio frequency fingerprint identification (RFFI) is a non-cryptographic authentication technique that attracted much research interest [4]–[7]. It exploits the intrinsic features brought by various hardware impairments resulting from imperfect manufacturing processes. The features manifested as slight distortions on transmitted signals. Like the biometric characteristics used for authentication, the subtle features are unique for different devices and hard to duplicate. Therefore, receivers can extract the features from received signals, followed by the verification with the pre-shared feature information for device authentication. The process does not involve computationally costly algorithms; hence, it consumes less energy and is suitable for power-constrained IoT devices.

An RFFI classifier is a machine learning model trained using radio frequency fingerprints (RFFs) for multi-class classification. Specifically, deep learning is leveraged as it minimizes the process of locating transient signal segments [8]–[12]. It automatically extracts RFFs from received signals, making it the technique requiring minimal manual selection to train RFFI classifiers. For the network architecture, convolutional neural network (CNN) is mostly implemented for image recognition tasks, which makes it especially suitable for device fingerprinting [13]–[18]. Among the feature selection, in-phase and quadrature (IQ) samples [19], FFT results [20], [21], and spectrogram [22] are widely studied. In [22], the spectrogram CNN model was shown to achieve the highest classification accuracy. Therefore, we adopt deep learning and spectrogram-based classifiers to benchmark proposed classifiers.

Due to the nature of wireless communications, RFFs are susceptible to environmental changes. Large-scale fading, multipath fading, and the Doppler effect affect wireless channels and modify received signal characteristics [23]–[25]. Traditional RFFs, e.g., spectrogram, extracted from the received signals are distorted and cannot be used for authentication [26]–[28]. We propose using a power amplifier (PA) nonlinearity quotient to mitigate the wireless channel effects introduced by environmental changes. The PA nonlinearity quotient is generated by taking division on the frequency domain of two consecutive signals transmitted with different power. The

division mitigates the wireless channel effects, and RFFI classifiers are trained to exploit the resulting RFFs.

Implementing environment-robust RFFs is limited when communication environments have many fast-moving objects because multipath fading and the Doppler effect mostly dominate wireless channels. Particularly, fast fading can happen when transmitters have low data rates, i.e., IoT devices. In [23], [28], [29], data augmentation is implemented to alleviate the impact of fast fading by training classifiers under channels with simulated multipath fading and the Doppler effect. However, the simulations had no pre-knowledge of the real deployment environments and significantly increased the required disk and memory storage for training classifiers.

Transfer learning can be implemented to combine RFFs resulting from different wireless channels [30]–[32]. Hence, distortions caused by multipath fading and the Doppler effect are acknowledged in device authentication. The required storage for transfer learning is less than data augmentation. Therefore, we implement transfer learning to alleviate the impact of fast fading. Specifically, a base classifier is trained with the original RFFs of the devices under test (DUTs); then, the classifier is retrained with the RFFs collected in real deployment environments.

This paper aims to design and validate an environment-robust RFFI system for IoT device authentication. The approach trains a classifier using the PA nonlinearity quotient. Transfer learning is adopted to alleviate the impact of fast fading and reduce training costs. Extensive experiments, including indoor and outdoor settings, were carried out using LoRa devices. The results show that the proposed PA nonlinearity quotient and transfer learning classifier significantly outperformed conventional deep learning and spectrogram-based classifiers. Our contributions are summarized as follows.

- We formalized the PA nonlinearity quotient and demonstrated that it is independent of environmental changes. The improvements in rogue device detection and device classification are backed by experimental validation.
- We developed data collection of real deployment, including indoor and outdoor environments. Further, we implemented transfer learning using the data to alleviate the impact of fast fading. The approach reduced the disk and memory storage requirements for training. The resulting classifiers have pre-knowledge of the real deployment environments compared to the data augmentation approach.
- We designed an RFFI system that involves the PA nonlinearity quotient and transfer learning. Samples resulting from natural multipath fading and the Doppler effect were implemented to validate the system.

II. POWER AMPLIFIER NONLINEARITY QUOTIENT

The PA is an indispensable component in any wireless device, with the implementation to amplify low-power signals to high-power ones. It is inherently nonlinear [33]. For low-power and narrowband systems, i.e., IoT devices, the PA is regarded as memoryless, meaning the nonlinear output depends only on the input at a particular time. The nonlinearity

can be characterized by an amplitude/amplitude (AM/AM) function and an amplitude/phase (AM/PM) function. Several models have been proposed to formulate the functions [33].

Implementing PA nonlinearity for RFFI is widely studied in the literature [34]–[39]. However, the implementation is often limited for static or semi-static channels. The RFFI performance drops significantly when communication environments change. We propose the PA nonlinearity quotient to design an environment-robust RFFI.

The signal of a narrowband system that reaches a receiver is given as

$$s(t) = h(\tau, t) * f[x(t)] + n(t), \quad (1)$$

where $x(t)$ is baseband signal, $h(\tau, t)$ is channel impulse response, $f[\cdot]$ denotes the nonlinear effect of hardware impairment at transmission power, and $n(t)$ is additive white Gaussian noise (AWGN). “*” denotes convolution operation.

When generating the PA nonlinearity quotient, two consecutive signals emitted with high and low transmission power correspondingly are received and developed an element-wise division on the frequency domain. The signal representation on the frequency domain is obtained through the short-time Fourier transform (STFT). The result of the STFT on the received signal is a matrix expressed as

$$S_p = \begin{bmatrix} S_p^{1,1} & S_p^{1,2} & \dots & S_p^{1,M} \\ S_p^{2,1} & S_p^{2,2} & \dots & S_p^{2,M} \\ \vdots & \vdots & \ddots & \vdots \\ S_p^{W,1} & S_p^{W,2} & \dots & S_p^{W,M} \end{bmatrix}, \quad (2)$$

where $p = \{h, l\}$ denotes high-power and low-power, respectively. The elements in the matrix are given as

$$S_p^{w,m} = \sum_{n=0}^{W-1} s_p[n] g[n - mR] e^{-j2\pi \frac{w}{W} n} \quad (3)$$

for $w = 1, 2, \dots, W$ and $m = 1, 2, \dots, M$,

where $s_p[n]$ is the discrete signal received by the receiver with a sampling interval, $g[n]$ is the window function with length W , and R is hop size. The experiments implement LoRa, hence M is given by LoRa configurations as

$$M = \frac{K \cdot \frac{2^{SF}}{B} \cdot f_S - W}{R} + 1, \quad (4)$$

where K is number of LoRa symbols, SF is LoRa spreading factor, B is bandwidth, and f_S is sampling frequency. The configurations are discussed in Section III-A. W is 1024 and R is 512. M is calculated to be 319.

The STFT result of the high-power signal is expressed as (5.1), where X denotes the ideal spectrum of the transmitted signal, H denotes the channel frequency response, and $F(\cdot)$ denotes the nonlinear hardware effect at the transmission power in the frequency domain. Only the preamble of the received signal is used to generate the PA nonlinearity quotient. The ideal spectrum of the low-power preamble is the same as the high-power one, i.e., $X^{w,m} = X^{w,M+m}$. Hence, the STFT result of the consecutive low-power signal is given as (5.2).

TABLE I
DUT CONFIGURATIONS

Carrier Frequency	Bandwidth (B)	Transmission Power (h/l)	Spreading Factor (SF)	Coding Rate
915 MHz	62.5 kHz	17/10 dBm	10	4/5

By removing the significantly distorted preambles caused by fast-moving objects nearby and implementing transfer learning, we assume intense multipath fading and the Doppler effect are mitigated. Slow fading mostly dominates the wireless channels. Therefore, the channel frequency response does not change significantly during one packet duration, i.e., $H^{w,m} \approx H^{w,M+m}$. The result of the element-wise division of received signals on the frequency domain (\mathbf{Q}) is given as

$$\mathbf{Q} = \mathbf{S}_h ./ \mathbf{S}_l = \begin{bmatrix} \frac{F_h(\mathbf{X}^1)}{F_l(\mathbf{X}^1)} & \frac{F_h(\mathbf{X}^2)}{F_l(\mathbf{X}^2)} & \dots & \frac{F_h(\mathbf{X}^M)}{F_l(\mathbf{X}^M)} \end{bmatrix}, \quad (6)$$

where “./” denotes the element-wise division operation and $\mathbf{X}^m = [X^{1,m} \ X^{2,m} \ \dots \ X^{W,m}]^T$. No channel frequency response (H) is present in \mathbf{Q} . The proposed environment-robust RFFI can be developed exploiting the PA nonlinearity quotient, which is \mathbf{Q} in dB scale, expressed as

$$\tilde{\mathbf{Q}} = 10 \log_{10}(|\mathbf{Q}|^2). \quad (7)$$

III. EXPERIMENTS

A. Experimental Settings

The experiments implemented 25 Arduino Nano-controlled LoRa SX1276 modules with the same circuit design and specifications as DUTs. 20 DUTs were randomly selected as legitimate devices (DUT: “A” to “T”), and 5 DUTs were selected as rogue devices (DUT: “Attacker 1” to “Attacker 5”). The device configurations are given in Table I. The LoRaWAN protocol supports 125 kHz, 250 kHz, and 500 kHz bandwidths, while LoRa supports bandwidths ranging from 7.8 kHz to 500 kHz. The proposed RSSI system does not focus on specific protocols. Therefore, a bandwidth of 62.5 kHz was used to reduce packet loss and maintain high throughputs. A universal software radio peripheral (USRP) platform with a 1 MS/s sampling frequency (f_s) was used to collect RF samples. Fig. 1 shows the devices used in the experiments.

The data collection was developed in three environments.

- **Anechoic chamber:** the collection of channel effect-free RFFs for training the base classifier required by transfer learning was carried out in the anechoic chamber on the top floor of the QUT GP campus S-block building. DUTs were placed 3 meters away from the USRP platform. The anechoic chamber was designed to absorb multipath signals. Therefore, RF samples collected in the environment can generate the PA nonlinearity quotient without the impact of multipath fading and the Doppler effect.
- **Indoor:** DUTs were placed in an office room for the indoor setting. The USRP platform was placed in the adjacent room, and DUT signals traveled through a wall. People were freely walking in the office during the data collection. The environment was considered to have moderate multipath fading and a slight Doppler effect.
- **Outdoor:** in the outdoor setting, DUTs were placed 104.5 meters away from the USRP platform, as shown in Fig. 2. Buildings blocked the line of sight, and people freely walked in the environment. The outdoor environment was considered to have more significant multipath fading and the Doppler effect than the indoor environment.

The DUTs transmit packets with alternating high-power and low-power modes, and the USRP platform passively receives the packets in the data collection. More than 2800 packets were collected for each DUT within one hour. Hence, more than 8400 packets were collected for each DUT in all three experimental environments.

B. Data Preprocessing

The data preprocessing includes synchronization, preamble extraction, normalization, and the PA nonlinearity quotient generation. The packets collected indoors and outdoors are required to go through the distorted preamble removal process before generating the PA nonlinearity quotient.

- 1) Synchronization: transmission power does not impact the data rate. Hence, the time-on-air for the DUT packets stays unchanged for the high-power and low-power transmission. The starting points of the packets are marked and used for synchronization to avoid inaccurate preamble extraction.

$$\mathbf{S}_h = \begin{bmatrix} H^{1,1} F_h(X^{1,1}) & H^{1,2} F_h(X^{1,2}) & \dots & H^{1,M} F_h(X^{1,M}) \\ H^{2,1} F_h(X^{2,1}) & H^{2,2} F_h(X^{2,2}) & \dots & H^{2,M} F_h(X^{2,M}) \\ \vdots & \vdots & \ddots & \vdots \\ H^{W,1} F_h(X^{W,1}) & H^{W,2} F_h(X^{W,2}) & \dots & H^{W,M} F_h(X^{W,M}) \end{bmatrix}, \quad (5.1)$$

$$\mathbf{S}_l = \begin{bmatrix} H^{1,M+1} F_l(X^{1,1}) & H^{1,M+2} F_l(X^{1,2}) & \dots & H^{1,2M} F_l(X^{1,M}) \\ H^{2,M+1} F_l(X^{2,1}) & H^{2,M+2} F_l(X^{2,2}) & \dots & H^{2,2M} F_l(X^{2,M}) \\ \vdots & \vdots & \ddots & \vdots \\ H^{W,M+1} F_l(X^{W,1}) & H^{W,M+2} F_l(X^{W,2}) & \dots & H^{W,2M} F_l(X^{W,M}) \end{bmatrix}. \quad (5.2)$$



Fig. 1. Devices used in the experiments. Left: a DUT in operation. Middle: 20 DUTs as legitimate devices and 5 DUTs as rogue devices. Right: a USRP-2922 platform as the receiver.



Fig. 2. Outdoor experimental environment.

- 2) Preamble extraction: preambles are payload-independent and have no software-defined features such as MAC addresses. Therefore, the intrinsic hardware features in the preamble symbols are the desirable source for RFFI. The preamble length is a flexible configuration for LoRa, with a minimum value of ten symbols. To study the worst-case scenario, we set and extracted ten symbols for one preamble per packet in the experiments.
- 3) Normalization: the process normalizes the received signal magnitude to remove the device-specific DC offset by dividing the root mean square. The PA nonlinearity feature is unaffected.
- 4) Distortion removal and PA nonlinearity quotient generation: we introduce Algorithm 1 to remove the severely distorted preambles caused by fast-moving objects nearby. The correlation between the high-power and low-power spectrogram should stay the same since PA nonlinearity is only affected by the input power [40]. The distorted preambles can be found by comparing the correlation of the channel-affected spectrogram to the correlation of the anechoic chamber spectrogram. The distortion is considered severe and can be removed if the difference is over a tolerance ($\theta = 0.2$ implemented in experiments). After the distortion removal, an element-wise division on the frequency domain is developed to generate the PA nonlinearity quotient. Fig. 3 shows the collected preamble spectrogram and the PA nonlinearity quotient generated by a DUT.

Algorithm 1: Distortion Removal and PA Nonlinearity Quotient Generation.

Input: $S_{h,k}, S_{l,k}$ %STFT results of indoor or outdoor preambles ($k = \text{indoor or outdoor}$)
Input: $S_{h,c}, S_{l,c}$ %STFT results of anechoic chamber preambles
Input: θ % Tolerance
Output: \tilde{Q} % PA nonlinearity quotient

- 1 $\rho_k = \text{corr}\{\max(S_{h,k}), \max(S_{l,k})\}$
- 2 $\rho_c = \text{corr}\{\max(S_{h,c}), \max(S_{l,c})\}$
- 3 $\rho_d = \|\rho_c - \rho_k\|$
- 4 **if** $\rho_d \leq \theta$ **then**
- 5 $\tilde{Q} = S_{h,k} / S_{l,k}$ % Element-wise division
- 6 $\tilde{Q} = 10 \log_{10}(|\tilde{Q}|^2)$
- 7 **else**
- 8 $_ _ \text{remove } S_{h,k}, S_{l,k}$

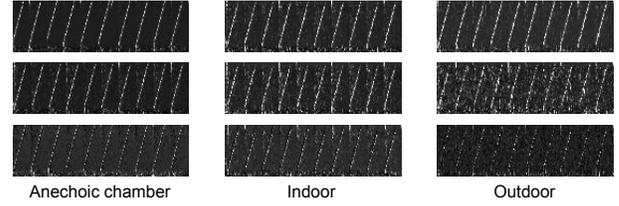


Fig. 3. Spectrogram and PA nonlinearity quotient of a DUT in the experiments. Top: high-power preamble spectrogram. Middle: low-power preamble spectrogram. Bottom: PA nonlinearity quotient, \tilde{Q} in (7).

C. Analytical Metrics

Device authentication exploiting RFFI involves two essential parts: device classification and rogue device detection. The classification accuracy and receiver operating characteristic (ROC) curve are implemented to evaluate the device classification and rogue device detection performance, respectively.

1) *Classification Accuracy*: The classification accuracy is defined as the number of correctly classified RFFs divided by the total number of tested RFFs. The results are obtained from the confusion matrix after developing classification tests.

2) *ROC Curve*: The rogue device detection was studied as binary classification in the experiments. The output values of the softmax function are compared to a threshold. The RFFs associated with the output values smaller than the threshold will be considered unauthorized. Since the threshold is configurable, it is hard to use a detection rate to analyze classifiers' performance. We adopted the ROC curve in the binary classifier study to overcome this. For each class of a classifier, ROC analysis applies threshold values in $[0,1]$ to calculate the true-positive rate (TPR) and the false-positive rate (FPR) for the outputs generated by each threshold. The area under the ROC curve (AUC) is the integral of a ROC curve with respect to FPR. The value of AUC is in the range of 0 to 1. A larger AUC indicates better classifier performance. In our experiments, a larger AUC indicates that the classifier is more capable of detecting rogue devices. A micro-averaging method is applied to generate the averaged AUC and ROC curves to analyze the rogue device detection for all classes.

TABLE II
LAYERS, PARAMETERS, AND ACTIVATION OF THE PROPOSED CLASSIFIER

Layer	Dimension	Parameters	Activation
Input	256×256	—	—
Convolution, BN	$8 \times (3 \times 3)$	80, 16	ReLU
MaxPooling	2×2	—	—
Convolution, BN	$16 \times (3 \times 3)$	1168, 32	ReLU
MaxPooling	2×2	—	—
Convolution, BN	$32 \times (3 \times 3)$	4640, 64	ReLU
FullyConnected	20	2304020	SoftMax

IV. CLASSIFIER ARCHITECTURE

The architecture of the PA nonlinearity quotient and transfer learning classifier is summarized in Table II. It consists of three convolution layers with 8, 16, and 32 3×3 filters, respectively. A batch normalization layer and the rectified linear unit (ReLU) activation follow each convolution layer. After the activation, a 2×2 max pooling layer with stride 2 is implemented. The output of the last ReLU activation is fed to a fully connected layer. An output layer with softmax function is implemented last to produce vectors of probabilities of outputs. The PA nonlinearity quotient is resized to 256×256 with 8-bit depth to go to the input layer. Adam optimizer is implemented to reduce the losses. The mini-batch size is 32. The initial training rate is 0.005 and remains unchanged.

Transfer learning retrains a pre-trained classifier on new datasets. In the experiments, the convolution layers of the pre-trained classifier recognize generic RFF patterns. We replaced the fully connected and output layers with new layers. For fine-tuning the transferred classifier, the training rate was configured to 0.0001, and the learning rate factor of the new layers was configured to 20.

V. RESULTS AND DISCUSSION

A. Device Classification

The base classifier was trained firstly using complete legitimate device (DUT: “A” to “T”) datasets in the anechoic chamber. Smaller training sets, including 50, 100, 150, and 200 packets, were randomly selected for each legitimate device from the indoor and outdoor datasets to implement the transfer learning. The conventional deep learning and spectrogram-based classifiers were trained as the comparison. The same test sets, including more than 1000 packets per DUT, were implemented to validate the proposed PA nonlinearity quotient and transfer learning classifier and the deep learning and spectrogram-based classifier. No training set packets were used in the test sets.

Fig. 4 shows the device classification results of indoor experiments. The proposed PA nonlinearity quotient and transfer learning classifier outperformed the conventional deep learning and spectrogram-based classifier with an improvement of 33.3% average classification accuracy. More training packets lead to higher classification accuracy. The highest accuracy is 99.4%, with 200 packets retraining the base classifier. The PA nonlinearity quotient improved the average classification accuracy by 19.4% compared to the spectrogram-based classifier.

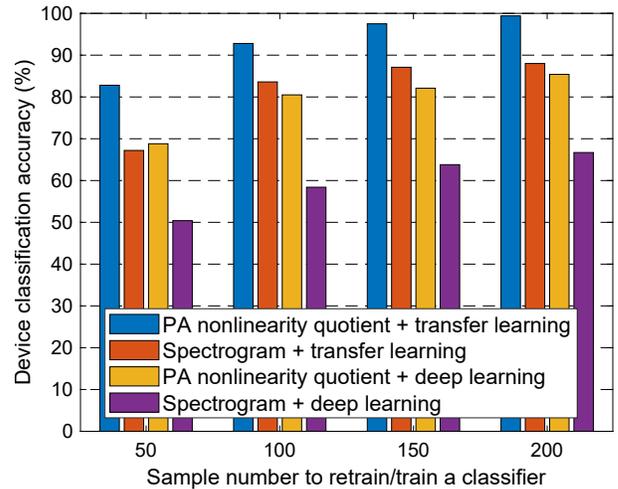


Fig. 4. Device classification results of the indoor experiments.

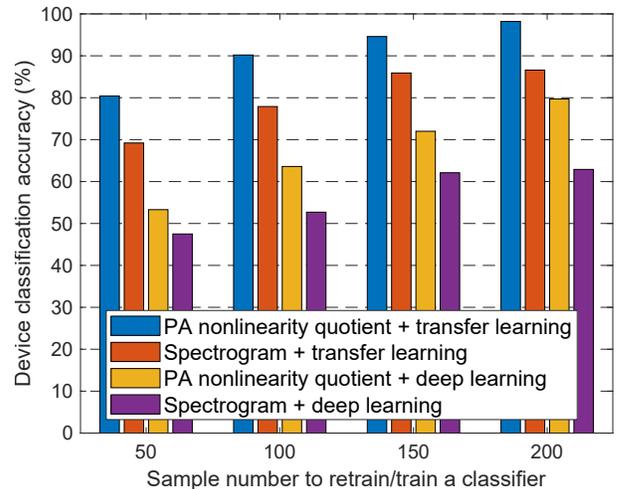


Fig. 5. Device classification results of the outdoor experiments.

Fig. 5 shows the classification results of outdoor experiments. The proposed PA nonlinearity quotient and transfer learning classifier outperformed the conventional deep learning and spectrogram-based classifier with an improvement of 34.5% average classification accuracy. The PA nonlinearity quotient improved the average classification accuracy by 10.9% compared to the spectrogram-based classifier.

Table III compares device classification performance among the proposed classifier and recent notable works in literature. The PA nonlinearity quotient and transfer learning classifier achieved high device classification accuracy while requiring fewer training samples and reducing the disk and memory storage requirements.

B. Rogue Device Detection

The training sets to retrain the base classifier included 100 randomly selected packets per DUT for studying the rogue device detection for the proposed classifier. Deep learning and spectrogram-based classifiers were trained for comparison.

TABLE III
DEVICE CLASSIFICATION COMPARISON WITH NOTABLE WORKS

Work	Experimental Environment	No. of Devices	Training Samples (Per Device)	Classification Accuracy
Ours	Indoor Outdoor	20	200	99.4% 98.2%
[23]	Indoor	30	100	98.4%
[41]	Indoor	54	698	84.6%
[42]	Indoor	7	800	99.0%

The test sets included more than 1000 packets per DUT and more than 1000 packets for each rogue device (DUT: "Attacker 1" to "Attacker 5"). No training set packets were used in the test sets.

Fig. 6 shows the ROC curves for the indoor experiments. The proposed PA nonlinearity quotient and transfer learning classifier outperformed the deep learning and spectrogram-based classifier, with an AUC value of 0.992 compared to 0.939. Fig. 7 shows the outdoor experiment results. Similar to the indoor experiments, the proposed classifier improved the AUC significantly. The PA nonlinearity quotient was more robust to environmental changes than the spectrogram, with larger AUC values in the indoor and outdoor experiments.

VI. CONCLUSION

In this paper, we investigated the technique to make RFFI resilient to environmental changes. We proposed the PA nonlinearity quotient and transfer learning classifier that mitigates channel effects to enhance the RFFI implementation for device classification and rogue device detection. Extensive experiments, including indoor and outdoor settings, were developed to evaluate the proposed classifier. The experiment results demonstrated that the proposed classifier significantly improved classification accuracy and rogue device detection for RFFI. The PA nonlinearity quotient outperformed the spectrogram to enhance RFFI in indoor and outdoor settings.

REFERENCES

- [1] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A survey on IoT security: Application areas, security threats, and solution architectures," *IEEE Access*, vol. 7, pp. 82 721–82 743, Jun. 2019.
- [2] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacy issues in Internet-of-Things," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1250–1258, Oct. 2017.
- [3] Q. Xu, R. Zheng, W. Saad, and Z. Han, "Device fingerprinting in wireless networks: Challenges and opportunities," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 1, pp. 94–104, Sep. 2015.
- [4] S. Riyaz, K. Sankhe, S. Ioannidis, and K. Chowdhury, "Deep learning convolutional neural networks for radio identification," *IEEE Commun. Mag.*, vol. 56, no. 9, pp. 146–152, Sep. 2018.
- [5] J. Zhang, S. Rajendran, Z. Sun, R. Woods, and L. Hanzo, "Physical layer security for the Internet of things: Authentication and key generation," *IEEE Wireless Commun.*, vol. 26, no. 5, pp. 92–98, May 2019.
- [6] K. Sankhe, M. Belgiovine, F. Zhou, L. Angioloni, F. Restuccia, S. D'Oro, T. Melodia, S. Ioannidis, and K. Chowdhury, "No radio left behind: Radio fingerprinting through deep learning of physical-layer hardware impairments," *IEEE Trans. Cognit. Commun. Netw.*, vol. 6, no. 1, pp. 165–178, Mar. 2020.
- [7] R. Xie, W. Xu, Y. Chen, J. Yu, A. Hu, D. W. K. Ng, and A. L. Swindlehurst, "A generalizable model-and-data driven approach for open-set RFF authentication," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 4435–4450, Aug. 2021.

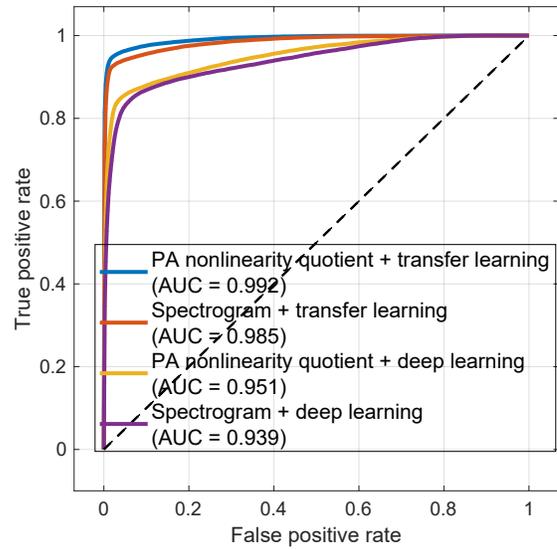


Fig. 6. ROC curves of rogue device detection in the indoor experiments.

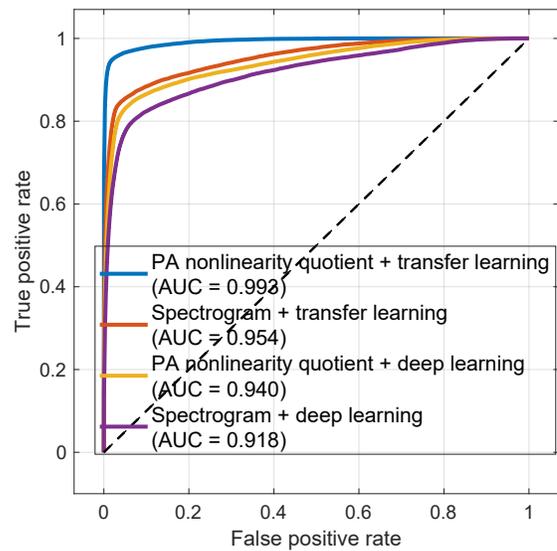


Fig. 7. ROC curves of rogue device detection in the outdoor experiments.

- [8] 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.
- [9] R. Das, A. Gadre, S. Zhang, S. Kumar, and J. M. Moura, "A deep learning approach to IoT authentication," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Kansas City, USA, May 2018, pp. 1–6.
- [10] L. Peng, J. Zhang, M. Liu, and A. Hu, "Deep learning based RF fingerprint identification using differential constellation trace figure," *IEEE Trans. Veh. Technol.*, vol. 69, no. 1, pp. 1091–1095, Jan. 2020.
- [11] D. Roy, T. Mukherjee, M. Chatterjee, E. Blasch, and E. Pasilio, "RFAL: Adversarial learning for RF transmitter identification and classification," *IEEE Trans. Cognit. Commun. Netw.*, vol. 6, no. 2, pp. 783–801, Jun. 2020.
- [12] B. He and F. Wang, "Cooperative specific emitter identification via multiple distorted receivers," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 3791–3806, Jun. 2020.
- [13] L. Ding, S. Wang, F. Wang, and W. Zhang, "Specific emitter identification via convolutional neural networks," *IEEE Commun. Lett.*, vol. 22, no. 12, pp. 2591–2594, Dec. 2018.
- [14] K. Sankhe, M. Belgiovine, F. Zhou, S. Riyaz, S. Ioannidis, and

- K. Chowdhury, "ORACLE: Optimized radio classification through convolutional neural networks," in *Proc. IEEE Int. Conf. Comput. Commun. (INFOCOM)*, Paris, France, Apr. 2019, pp. 370–378.
- [15] S. Rajendran, Z. Sun, F. Lin, and K. Ren, "Injecting reliable radio frequency fingerprints using metasurface for the Internet of Things," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 1896–1911, Dec. 2020.
- [16] T. Jian, Y. Gong, Z. Zhan, R. Shi, N. Soltani, Z. Wang, J. Dy, K. Chowdhury, Y. Wang, and S. Ioannidis, "Radio frequency fingerprinting on the edge," *IEEE Trans. Mobile Comput.*, vol. 21, no. 11, pp. 4078–4093, Nov. 2021.
- [17] Y. Qian, J. Qi, X. Kuai, G. Han, H. Sun, and S. Hong, "Specific emitter identification based on multi-level sparse representation in automatic identification system," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 2872–2884, Mar. 2021.
- [18] H. Li, K. Gupta, C. Wang, N. Ghose, and B. Wang, "RadioNet: Robust deep-learning based radio fingerprinting," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, Austin, USA, Oct. 2022, pp. 190–198.
- [19] X. Zhou, A. Hu, G. Li, L. Peng, Y. Xing, and J. Yu, "A robust radio-frequency fingerprint extraction scheme for practical device recognition," *IEEE Internet Things J.*, vol. 8, no. 14, pp. 11 276–11 289, Jul. 2021.
- [20] P. Robyns, E. Marin, W. Lamotte, P. Quax, D. Singelée, and B. Preneel, "Physical-layer fingerprinting of LoRa devices using supervised and zero-shot learning," in *Proc. 10th ACM Conf. Secur. Privacy Wireless Mobile Netw.*, Boston, USA, Jul. 2017, pp. 58–63.
- [21] S. Guo, Y. Xu, W. Huang, and B. Liu, "Specific emitter identification for WiFi devices via Bezier curve fitting," in *Proc. IEEE 32nd Int. Symp. Pers. Indoor Mobile Radio Commun. (PIMRC)*, Helsinki, Finland, Sep. 2021, pp. 1493–1499.
- [22] G. Shen, J. Zhang, A. Marshall, L. Peng, and X. Wang, "Radio frequency fingerprint identification for LoRa using deep learning," *IEEE J. Sel. Areas Commun.*, vol. 39, no. 8, pp. 2604–2616, Aug. 2021.
- [23] G. Shen, J. Zhang, A. Marshall, and J. R. Cavallaro, "Towards scalable and channel-robust radio frequency fingerprint identification for LoRa," *IEEE Trans. Inf. Forensics Security*, vol. 17, pp. 774–787, Feb. 2022.
- [24] N. Soltani, G. Reus-Muns, B. Salehi, J. Dy, S. Ioannidis, and K. Chowdhury, "RF fingerprinting unmanned aerial vehicles with non-standard transmitter waveforms," *IEEE Trans. Veh. Technol.*, vol. 69, no. 12, pp. 15 518–15 531, Dec. 2020.
- [25] L. Yang, Y. Gao, J. Zhang, S. Camtepe, and D. Jayalath, "A channel perceiving attack and the countermeasure on long-range IoT physical layer key generation," *Comput. Commun.*, vol. 191, pp. 108–118, Jul. 2022.
- [26] F. Restuccia, S. D'Oro, A. Al-Shawabka, M. Belgiovine, L. Angioloni, S. Ioannidis, K. Chowdhury, and T. Melodia, "DeepRadioID: Real-time channel-resilient optimization of deep learning-based radio fingerprinting algorithms," in *Proc. 20th ACM Int. Symp. Mobile Ad Hoc Netw. Comput.*, Catania, Italy, Jul. 2019, pp. 51–60.
- [27] A. Al-Shawabka, F. Restuccia, S. D'Oro, T. Jian, B. C. Rendon, N. Soltani, J. Dy, S. Ioannidis, K. Chowdhury, and T. Melodia, "Exposing the fingerprint: Dissecting the impact of the wireless channel on radio fingerprinting," in *Proc. IEEE Int. Conf. Comput. Commun. (INFOCOM)*, Toronto, Canada, Jul. 2020, pp. 646–655.
- [28] A. Al-Shawabka, P. Pietraski, S. B. Pattar, F. Restuccia, and T. Melodia, "DeepLoRa: Fingerprinting LoRa devices at scale through deep learning and data augmentation," in *Proc. ACM Int. Symp. Mobile Ad Hoc Netw. Comput. (MobiHoc)*, Shanghai, China, Jul. 2021, pp. 251–260.
- [29] N. Soltani, K. Sankhe, J. Dy, S. Ioannidis, and K. Chowdhury, "More is better: Data augmentation for channel-resilient RF fingerprinting," *IEEE Commun. Mag.*, vol. 58, no. 10, pp. 66–72, Oct. 2020.
- [30] Y. Sharaf-Dabbagh and W. Saad, "On the authentication of devices in the Internet of Things," in *Proc. IEEE 17th Int. Symp. World Wireless Mobile Multimedia Netw. (WoWMoM)*, Coimbra, Portugal, Jun. 2016, pp. 1–3.
- [31] X. Wang, Y. Zhang, H. Zhang, Y. Li, and X. Wei, "Radio frequency signal identification using transfer learning based on LSTM," *Circuits Syst. Signal Process.*, vol. 39, no. 11, pp. 5514–5528, Apr. 2020.
- [32] S. Kuzdeba, J. Robinson, and J. Carmack, "Transfer learning with radio frequency signals," in *Proc. IEEE 18th Annu. Consum. Commun. Netw. Conf. (CCNC)*, Las Vegas, USA, Jan. 2021, pp. 1–9.
- [33] Z. Zhu, H. Leung, and X. Huang, "Challenges in reconfigurable radio transceivers and application of nonlinear signal processing for RF impairment mitigation," *IEEE Circuits Syst. Mag.*, vol. 13, no. 1, pp. 44–65, Feb. 2013.
- [34] J. Gong, X. Xu, and Y. Lei, "Unsupervised specific emitter identification method using radio-frequency fingerprint embedded InfoGAN," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 2898–2913, Mar. 2020.
- [35] 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, Aug. 2011.
- [36] J. Zhang, F. Wang, O. A. Dobre, and Z. Zhong, "Specific emitter identification via Hilbert–Huang transform in single-hop and relaying scenarios," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 6, pp. 1192–1205, Jun. 2016.
- [37] S. S. Hanna and D. Cabric, "Deep learning based transmitter identification using power amplifier nonlinearity," in *Proc. Int. Conf. Comput., Netw. Commun. (ICNC)*, Honolulu, USA, Feb. 2019, pp. 674–680.
- [38] U. Satija, N. Trivedi, G. Biswal, and B. Ramkumar, "Specific emitter identification based on variational mode decomposition and spectral features in single hop and relaying scenarios," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 3, pp. 581–591, Mar. 2019.
- [39] Y. Li, Y. Ding, J. Zhang, G. Goussetis, and S. K. Podilchak, "Radio frequency fingerprinting exploiting non-linear memory effect," *IEEE Trans. Cognit. Commun. Netw.*, vol. 8, no. 4, pp. 1618–1631, Dec. 2022.
- [40] J. Zhang, R. Woods, M. Sandell, M. Valkama, A. Marshall, and J. Cavallaro, "Radio frequency fingerprint identification for narrowband systems, modelling and classification," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 3974–3987, Jun. 2021.
- [41] 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.
- [42] Y. Xing, A. Hu, J. Zhang, L. Peng, and X. Wang, "Design of a channel robust radio frequency fingerprint identification scheme," *IEEE Internet Things J.*, early access, Dec. 9, 2022, doi:<https://doi.org/10.1109/JIOT.2022.3228280>.