PUF-Assisted Radio Frequency Fingerprinting Exploiting Power Amplifier Active Load-pulling

Yuepei Li, Kai Xu, *Student Member, IEEE*, Junqing Zhang, Chongyan Gu, Yuan Ding*,
George Goussetis, *Senior Member, IEEE*, and Symon K. Podilchak, *Senior Member, IEEE*

***Abstract*—This paper presents a novel radio frequency fingerprint (RFF) enhancement strategy by exploiting the physical unclonable function (PUF) to tune the RF hardware impairments in a unique and secure manner, which is exemplified by taking power amplifiers (PAs) in RF chains as an example. This is achieved by intentionally and slightly tuning the PA non-linearity characteristics using the active load-pulling technique. The motivation driving the proposed research is to enlarge the RFF feature differences among wireless devices of same vendor, in order to massively improve their RFF classification accuracy in low to medium signal to noise ratio (SNR) channel conditions. PUF is employed to dynamically tune the PA's RFF feature which guarantees the security since the PUF response cannot be cloned. Specifically, a ring oscillator (RO)-based PUF is implemented to control the PA non-linearity by selecting unique but random configuration parameters. This approach is proposed to amplify the distinctions across same model PAs, thereby enhancing the RFF classification performance. In the meantime, our innovative strategy of PUF-assisted RFF does not noticeably compromise communication link performance which is experimentally tested. The resulting RFF features can be extracted from the received distorted constellation diagrams with the help of image recognition-based machine learning classification algorithms. Extensive experimental evaluations are carried out using both cable-connected and over-the-air (OTA) measurements. Our proposed approach, when classifying eight PAs from a same vendor, achieves 11% to 24% average classification accuracy improvement by enlarging the RFF feature differences arising from the PA non-linearity.**

***Index Terms*—Active load-pulling, convolution neural network (CNN), non-linear memory effect, physical unclonable function (PUF), radio frequency fingerprinting (RFF).**

I. Introduction

The Internet of Things (IoT) network has rapidly become a business enabler as their prevalence brings great convenience to people's daily lives. However, many IoT devices are low cost and only equipped with limited computational and energy resources. Such limitations result in various vulnerabilities to cyber attacks [1], as they cannot afford cryptographic schemes. For example, device authentication is usually achieved via cryptographic challenge response protocol, which will require a common key shared in advance. Unfortunately, such secure key distribution is quite challenging for IoT devices [2].

Radio frequency fingerprint identification (RFFI) is an emerging non-cryptographic solution for device authentication [3], [4]. In particular, the radio frequency fingerprint (RFF) refers to the unique hardware impairments inherently presented in analog transmit RF chains, which are fabricated subject to variations in the manufacturing process [5], [6]. These impairments are minute, which result in slight distortions of the transmit signal waveforms but do not compromise communication quality. Furthermore, they are unique to each transmitter, which can be extracted by the receiver and utilized as device identities (IDs) to facilitate secure network access authentications [7]. Compared to the traditional authentication methods, RFFI does not rely on shared secrets such as passwords or cryptographic keys, which makes it very suitable for low cost IoT devices. Hence, there have been active research efforts on studying RFFI with IoT technologies, including WiFi [8], ZigBee [9], [10], LoRa [11]–[13], Bluetooth [14], etc.

The hardware impairments of transmitters include I/Q imbalance [9], oscillator imperfection, i.e, frequency offset and phase noise [15], power amplifier (PA) non-linearity [16]–[20], antenna characteristics [13], [21], [22], etc. Among them, PAs exist in most wireless transmitter chains and are the major contributors to signal non-linearity, hence the PA non-linearity has been widely studied for RFFI [16]–[20]. However, these systems could operate only in high signal to noise ratio (SNR) conditions, hardly experienced in any practical wireless systems. Our previous work in [19] attempted to improve the RFFI performance in relatively low SNR regions by exploiting the non-linear memory effect of the transmission links consisting of matched pulse shaping filters and non-linear PAs.

There are usually multiple manufacturers and vendors for the same type of wireless technologies. It is more difficult to classify devices from the same manufacturer because they are from the same production line which results in very

Mr Yuepei Li's work was supported by Heriot-Watt University Doctoral Training Programme (DTP) scholarship. Dr Yuan Ding's work was supported by EPSRC (UK) under the Grant EP/V002635/1. Dr Junqing Zhang's work was supported by EPSRC (UK) under the Grant EP/V027697/1. Dr Chongyan Gu's work was supported by EPSRC (UK) under the Grant EP/X009602/1. (Corresponding author: *Yuan Ding*.)

Y. Li, K. Xu, Y. Ding, and G. Goussetis are with the Institute of Sensors, Signals and Systems (ISSS), Heriot-Watt University, UK (Emails: yl12; kx1; yuan.ding; gg35@hw.ac.uk). Y. Li, and K. Xu are also with the Institute of Digital Communications, School of Engineering, University of Edinburgh, UK.

J. Zhang is with the Department of Electrical Engineering and Electronic, University of Liverpool, UK (email: Junqing.Zhang@liverpool.ac.uk).

C. Gu is with the Centre for Secure Information Technologies (CSIT), Queen's University Belfast, U.K. (e-mail: c.gu@qub.ac.uk).

S. Podilchak is with the Institute of Digital Communications, School of Engineering, University of Edinburgh, UK (email: S.Podilchak@ed.ac.uk).

TABLE I
OUR PROPOSED WORK IN COMPARISON WITH THE EXISTING RFF ENHANCEMENT WORKS.

Works	RFF enhancement technique	Extra hardware?	Computational complexity	Cost	Identification method	Scalability
[8]	Metasurface circuit	Yes (Low-cost metasurface)	High	Medium	Shifting antenna resonant frequency	Low to medium
[23]	PUF assist RFFI	Yes (PUF circuit)	High	Low	PUF-controlled PA's out-band spectral regrowth	Low
[25]-[28]	RF-PUF	No	High	Low	Mutual authentication (Decrypted PUF response + RFF feature)	Medium
Our work	PUF assist RFFI	Yes (PUF & signal loopback circuits)	Medium	Low	PUF-controlled PA's non-linear memory effect	High

minute differences among them. Some dedicated experiments are designed to study the behavior of oscillator imperfection and PA non-linearity, which can focus on a particular type of hardware impairments. In [15], the unique characteristics of the phase noise that is generated in RF carrier oscillators were extracted for RFF. The reported classification performance for the cable-connected measurement among 8 oscillators of the same model indicated a low classification error at the SNR of 35 dB. The work in [19] demonstrated it is more difficult to classify PAs of the same model compared to PAs of different models, especially in low SNR scenarios. It achieved 90% classification accuracy at an SNR of about 10 dB among a mix of PAs from the same and different vendors. Observed from the confusion matrix presented in [19], most classification errors in low SNR regions occurred among devices of the same PA model. This will further deteriorate when a greater number of the same model devices are classified. There are also studies about commercial off-the-shelf IoT devices, which include all the hardware impairments. For example, the work in [11] classified 15 LoRa devices which were from three vendors. The misclassification mainly occurred among the devices of the same model. Such limitations result in challenges in practical applications as it is common to classify hardware platforms/components from the same manufacturer.

There are a few approaches proposed to introduce external impairments [8] and reconfigure existing hardware impairments [23]. These approaches adjust the operation condition of the RF devices slightly, hence, the unique RFF feature can be enlarged without compromising wireless link performance. In addition, in Table I our proposed work is compared with the existing works on RFF enhancement techniques. The RFF enhancement technique, computational complexity, cost, identification method and scalability of these works are presented. The work [8] embedded a metasurface to the transmitter antenna and this could inject new RFF features into radiated signals. In this topology, in order to reduce the insertion-loss the RF substrates and low-loss components have to be used in this metasurface, thus, inevitably increasing its cost. This approach is also susceptible to fabrication and component variations. For example, a variance of 0.1 pF capacitance within the metasurface elements can cause a frequency shift of approximately 150 MHz. In addition, this work requires complex electromagnetic (EM) simulations of large electric size and iterative optimization algorithms, which can be computationally intensive. In the work [23], the authors proposed to embed a PUF circuit to slightly adjust the PA bias through a digital to analog converter, so that the PA out-band spectrum regrowth became more distinguishable among the same-brand devices. The challenge here is that there are only very limited choices of PA biasing conditions that satisfy good in-band signal quality for maintaining wireless links and distinguishable out-band spectrum regrowth for RFF use. Thus, this may not be applicable in wireless networks wherein a large number of wireless devices need to be identified through RFF features. In addition, in some cases, the out-band spectrum regrowth may cause interference to other adjacent channels.

PUF is a hardware security technology, which is constructed using a digital circuit that is sensitive to minute variations in the semiconductor fabrication process, e.g., doping concentration [24]. Works in [25]–[28] utilized mutual authentication approach as referred to RF-PUF. However, those works treated their RFF schemes as the RF-based PUF but there was no PUF circuitry involved. The identification node in this approach needs to decrypt the PUF response and extract the RFF features from the received signals. The computational complexity depends on the size of the dataset used for training the machine learning algorithms, and also depends on the algorithms selected to decrypt the PUF output response and the RFF feature extraction for node identification.

To address the above-mentioned challenges, this paper exploits the active load-pulling technique and PUF to enlarge RFF feature differences for RF devices of the same brand/model in a unique and secure way, in order to significantly improve RFFI performance in low SNR scenarios. Specifically, the PA output load impedance in a traditional transmitter is commonly fixed to 50 Ω. This paper proposes to actively alter the output impedance of the PA as a means to enlarge RFF features, which is achieved by the active load-pulling technique. Such adjustment has to be individually fixed for each device while undisclosed to all nodes within the wireless networks (including the devices to be identified), which is imperative to mitigate security risks of being cloned, hence PUF is exploited. We built a testbed involving eight PAs with the same model and carried out a comprehensive experimental evaluation. To achieve this, only a low-cost PUF circuit and a signal loopback circuit (e.g., circulator) are required. The computational complexity of this work arises from the PUF implementations and the processing required to analyze transmitter non-linear memory effect RFF feature for node identification. All these can be done offline. The main contributions of our work are summarized as follows.

- The active load-pulling technique is leveraged to enlarge the PA RFF features, which can considerably improve the classification performance for the same brand devices. The PA output load impedance can be determined in PA load-pull contours, providing a broader range of options compared to the alteration of PA bias, without compromising communication qualities.
- PUF circuits are employed to select the active load-pulling configuration in a unique and secret manner. A ring oscillator-based PUF (RO-PUF) is used. An output is randomly generated, which is used to select a configuration for PAs.
- Extensive experimental evaluation has been carried out through both cable-connected and over-the-air (OTA) experiments. In the cable-connected experiments, the classification accuracy reached over 90% for the SNR of 13 dB. In the OTA experiments, the proposed approach achieved classification accuracies of 89% at the SNR of 26 dB for LOS and 64% at the SNR of 15 dB for non-line-of-sight (NLOS) transmission scenarios.
- Our proposed approach achieved a notable classification improvement in comparison to the conventional method without enlarging PA RFF features. Our approach achieved average classification accuracy improvements of approximately 22%, 17%, and 12% at SNRs of 0 dB, 5 dB and 10 dB in the cable-connected experiment, respectively, compared to the conventional method. The OTA experiment witnessed about 11% to 24% improvements in the average classification accuracy.

The rest of the paper is organized as follows. Section II introduces the overall architecture of the proposed PUF-assisted RFFI system. Section III elaborates the PA characteristics and the active load-pulling theory, as these are the main feature techniques for enhancing RFF feature for secure device identification. The PUF-control and RFFI protocol are discussed in Section IV and Section V, respectively. Section VI gives the experimental evaluation, both in cable-connected and OTA environments. Finally, conclusions are drawn in Section VII.

II. Overview of Proposed RFFI System

As portrayed in Fig. 1, an RFFI system includes N devices under test (DUTs) and a receiver. The DUT transmitter is subject to hardware impairments, resulting from variations of manufacturing processes. Such impairments distort the transmitted waveforms slightly but are generally unnoticeable with regard to wireless link performance. In an RFFI system, upon receiving the signals, a receiver aims to identify the DUTs' identity by exploiting the differences among the DUTs' hardware impairments.

A. Transmitters in RFFI Systems

From our previous work [19], the classification performance using the PA non-linearity is very limited in low SNR conditions, especially when the PAs are of the same model. In order to enhance the classification performance under such a challenging scenario, this paper proposes to use the active load-pulling technique to slightly adjust the PA characteristics, see the shaded area in Fig. 2. Here a module of PUF-controlled magnitude and phase tuner is added to assist in the adjustment of PA loads without compromising link quality. With the slight changes of the PA loads, the RFF features can be enlarged. The PA non-linearity characteristics as well as the active load-pulling technique will be explained in detail in Section III.

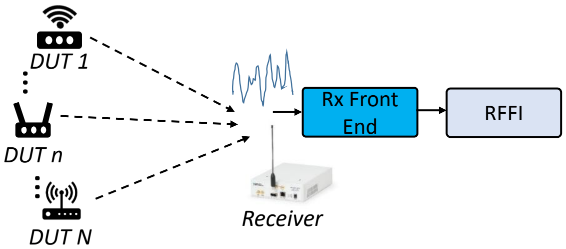


Fig. 1. Workflow of RFFI.

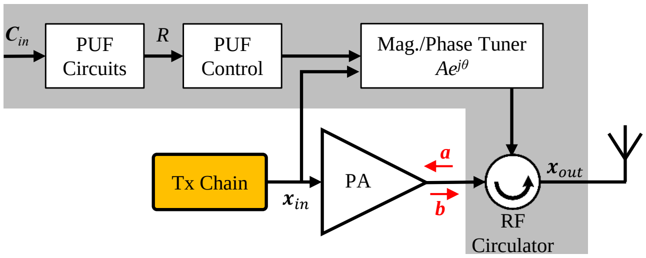


Fig. 2. PUF-assisted PA active load-pulling for RFFI.

The other key design consideration to ensure security is that once the pool of selectable loads is determined, the choice among these loads for a certain device has to be fixed but random, and unknown to any nodes in the network. This proposition rules out any chances of these settings being leaked and forged by malicious parties. This, fortunately, can be achieved by a PUF circuit whose uniqueness, producing fixed outputs, and unclonable, corresponding to random and unknown features, is a perfect fit. PUF is a digital circuit, commonly implemented in field programmable gate array (FPGA) or application-specific integrated circuit (ASIC), that exploits variations in the manufacturing process to generate unique unclonable digital fingerprints. Such variations exist in electronic components, particularly at the microelectronic level, which cannot be estimated or controlled. As depicted in Fig. 3, when the same challenge sequence, denoted as $\boldsymbol{C}_{in}$, is input to the same PUF design in the different digital boards, a unique unclonable digital fingerprint R for each individual device is generated. The PUF design used in our work will be further introduced in Section IV.

B. Receiver and RFFI Protocol

Once the receiver collects the signals from the DUT transmitter, the captured signals are down-converted and synchronized. After that, the RFFI protocol will carry out RFF feature extraction and classification. Deep learning has been widely adopted thanks to its excellent classification capability, such

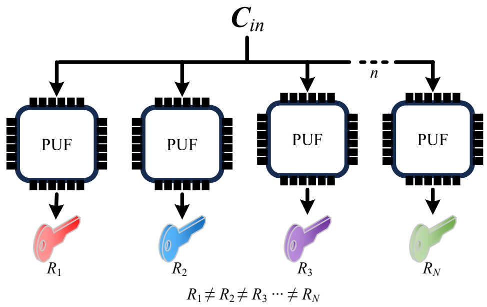


Fig. 3. PUF illustration.

as convolution neural network (CNN) [13], [19], [22], [29]. The RFFI protocol design will be given in Section V.

III. Power Amplifier Characteristics and Active Load-pulling Effect

In our work, we exploit the PA non-linearity, especially the dynamically adjusted non-linearity through active load-pulling technique, for the RFFI application, see Fig. 2 and the description in Section II. For a better understanding, the PA characteristics and the active load-pulling concept are presented in this section.

A. Power Amplifier Characteristics

The amplitude modulation to amplitude modulation (AM/AM) and amplitude modulation to phase modulation (AM/PM) are the important characteristics used to describe the PA input-to-output non-linear behaviors. The AM/AM (and AM/PM) quantifies the extent to which the output signal power (and phase) varies as a function of the input signal power. There are a number of PA behavioral models that provide a mathematical approximation to describe those AM/AM and AM/PM characteristics, such as Ghorbani [30], Saleh [31], Rapp [32], and Bessel-Fourier [33]. As reported in [33], [34], these models exhibit distinct strengths and limitations.

- The Rapp model fluctuates in the transition between linear and saturation regions;
- The Saleh model has great performance to fit the linear curves;
- The Ghorbani model is particularly well suited for the non-linear region;
- The Bessel-Fourier approach can accurately fit the entire PA operation region with a sacrifice on higher fitting complexity, i.e., more coefficients need to be determined.

Since the purpose of our work here is to study PA behavior for RFFI applications, and the PA behavior fitting can be performed offline, the more accurate Bessel-Fourier PA behavioral model is thus adopted in our work.

In our study, the AM/AM and AM/PM curves for the PAs under test are firstly measured using a Vector Network Analyzer (VNA), and they are subsequently Bessel-Fourier fitted using the model below

$$B(\rho)e^{jF(\rho)} = \sum_{l=1}^{L} \beta_l J_1(\alpha \cdot l \cdot \rho), \tag{1}$$

where ρ is the magnitude of the PA's input signal, $B(\cdot)$ and $F(\cdot)$ respectively represent the measured AM/AM and AM/PM of the PA under test, and $J_1(\cdot)$ refers to the Bessel function of the first kind with L being the length of the Bessel series. β_l and α are the coefficients to be determined, and l is the index of the Bessel terms. In this work, L of 30 is used hereafter to obtain accurate fitting results.

B. PA Load-pull

Load-pull is a method of evaluating PA performance, such as output power, efficiency, gain, linearity, etc, for a large number of PA output load impedances. The loads are commonly selected within a pre-defined region in the Smith chart, which is a graphic tool for microwave engineers that assists the transformation between impedance and reflection coefficients. The results, e.g., of output power, efficiency, or gain, are contour plotted in the Smith chart, within which every point is associated with a load impedance $\boldsymbol{Z}_L$ [35]. In our work, we used an automatic Maury load tuner [36] to conduct the PA load-pull measurement. 8 PAs of the same brand (PGA-105+ from Mini-Circuits [37]) are employed. As examples, the measured load-pull results at 2.4 GHz operation frequency for the output power at 1 dB compression point, denoted as P_{out_1dB}, are illustrated in Fig. 4 for the PA-1, PA-3, and PA-6. P_{out_1dB} refers to the output power at which the PA gain is 1 dB less than the PA gain in the linear region. It indicates the output power capacity of the PA. In Fig. 4, the x- and y- axes are the real and imaginary parts of the PA output reflection coefficient $\boldsymbol{\Gamma}_L$, which is defined as the voltage ratio of the reflected waveform $\boldsymbol{a}$ and the forward waveform $\boldsymbol{b}$, seen in Fig. 2. The waveforms $\boldsymbol{a}$ and $\boldsymbol{b}$ are the notations used in the RF microwave community. In physics, a signal wave describes the amplitude and phase (relative to a common phase reference) of an EM wave in a transmission line system. Given that the EM wave has a propagation direction (along the direction of the cross product of the electric field and the magnetic field), the waves $\boldsymbol{a}$ and $\boldsymbol{b}$ also have directions, which are labelled in Fig. 2. The mathematical expression of calculating the reflection coefficient $\boldsymbol{\Gamma}_L$ is

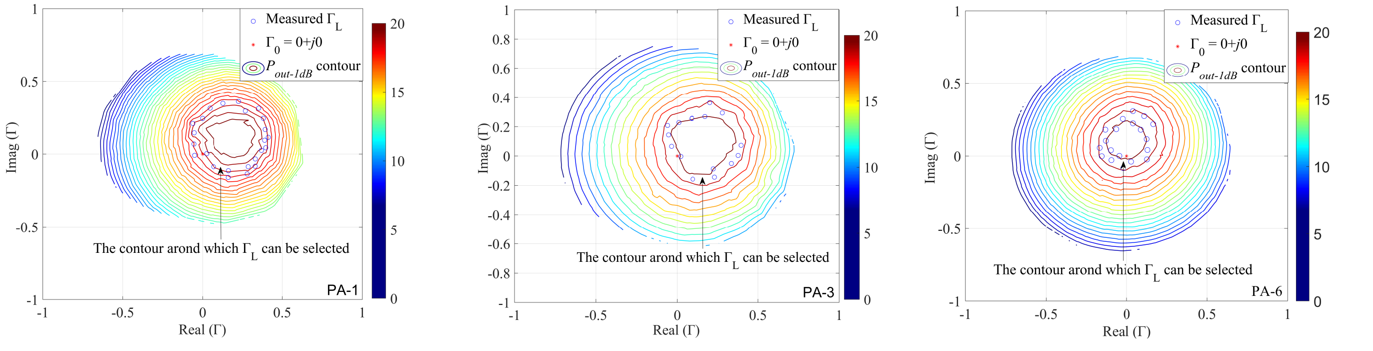
$$\boldsymbol{\Gamma}_L = \boldsymbol{a}/\boldsymbol{b}. \tag{2}$$

It is worth noting that here $\boldsymbol{a}$ and $\boldsymbol{b}$ are phasor representations, namely they are complex numbers containing only amplitude and initial phase of the corresponding waveforms at the operation frequency of interest. The PA load impedance $\boldsymbol{Z}_L$ can be calculated from the reflection coefficient $\boldsymbol{\Gamma}_L$, expressed as

$$\boldsymbol{Z}_L = \boldsymbol{Z}_0 \frac{1+\boldsymbol{\Gamma}_L}{1-\boldsymbol{\Gamma}_L}, \tag{3}$$

where $\boldsymbol{Z}_0$ is the system characteristic impedance. In this work, the commonly used 50 Ω is assumed. We choose P_{out_1dB} as the key PA characteristic, other than gain, efficiency or linearity, because in low-cost low-power IoT devices, the output power is most critical.

In Fig. 4, the color bar indicates the P_{out_1dB} in dBm. Thus, the PA with every load impedance on each contour in



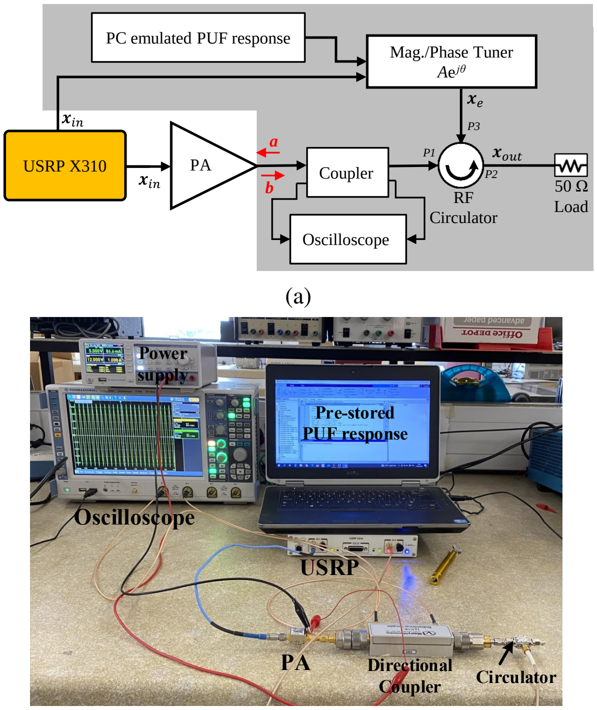
(a)

(b)

(c)

Fig. 4. Measured P_{out_1dB} load-pull contours associated with the (a) PA-1, (b) PA-3, and (c) PA-6. The gap between contour lines is 1 dB.

the load-pull plot can give identical output power. The center origin (0, 0) in the Smith chart is labeled as $\boldsymbol{\Gamma}_0 = 0$ (red solid dot in the graphs), which, using (3), also corresponds to the load impedance $\boldsymbol{Z}_0$. In these load-pull examples in Fig. 4, the 50 Ω load gives 19 dBm P_{out_1dB} to the PA-1 and the PA-3, and about 20 dBm to the PA-6. Though there are some differences among these load-pull plots for different PAs, as expected the overall performance distribution on the Smith chart looks similar.



(a)

(b)

Fig. 5. (a) Block diagram and (b) photograph of the active load-pulling experiment.

C. Active Load-pulling Effect

The load tuner equipment can be used for load-pull measurement, but it is impractical to be integrated into a transmitter. Hence, we explore an alternative approach of the active load-pulling technique, which adjusts the output impedance by injecting coherent signals at the PA output in the reverse direction, instead of altering the impedance of loads using reconfigurable devices in passive load tuners. This active load-pulling concept and block diagram, as well as the photograph of the experimental setup, are shown in Fig. 5. A universal software radio peripheral (USRP) X310, supporting two synchronized transmit chains, was used to generate two identical RF signals, one, denoted as $\boldsymbol{x}_{in}$, being injected into the PA input, and the other being scaled with $Ae^{j\theta}$ to produce the signal $\boldsymbol{x}_e$, which is expressed in (4). The module of PC emulated PUF response is used the stored PUF responses to control the 'Mag/Phase Tuner' required for PA active load-pulling. Since the purpose of the experiment in Fig. 5 is to demonstrate the PA active load-pulling concept and its impact on wireless link and RFF feature extraction, this PUF simplification is justifiable. In a practical system implementation, this, however, will be reverted back to the hardware PUF circuit to ensure security. More detailed information on PUF implementation can be found in Section IV.

$$\boldsymbol{x}_e = \boldsymbol{x}_{in} \cdot Ae^{j\theta} \tag{4}$$

This signal $\boldsymbol{x}_e$ is then routed to the PA output in the backward direction using an RF circulator. The RF circulator, a three-port component, ensures signals only travel in a certain direction, see the arrow inside the circulator in Fig. 5(a). In this example, the circulator only allows the PA output signal $\boldsymbol{b}$ to flow to the 50 Ω load (or the antenna as illustrated in Fig. 2), and it directs the $\boldsymbol{x}_e$ (the output of Mag/Phase Tuner) to only flow to the PA output in the reverse direction, i.e., generating the signal $\boldsymbol{a}$. A directional coupler is inserted at the PA output in the experiment to monitor and measure $\boldsymbol{a}$ and $\boldsymbol{b}$ using a two-port oscilloscope. In a practical design, this coupler can be removed.

The backward waveform $\boldsymbol{a}$ at the PA output, seen in Fig. 5(a) can be calculated as in

$$\boldsymbol{a} = \boldsymbol{x}_e \cdot \boldsymbol{S}_{cir\_13} \cdot \boldsymbol{S}_{cpl\_12}, \tag{5}$$

where $\boldsymbol{S}_{cir\_wo}$ and $\boldsymbol{S}_{cpl\_wo}$ are the S-parameters of the circulator and the coupler from port o to port w (o, $w \in \{1, 2, 3\}$ for the circulator and o, $w \in \{1, 2, 3, 4\}$ for the coupler).

Once the non-linear PA characteristics have been obtained using the Bessel-Fourier fitting via (1), the PA output $\boldsymbol{b}$ can

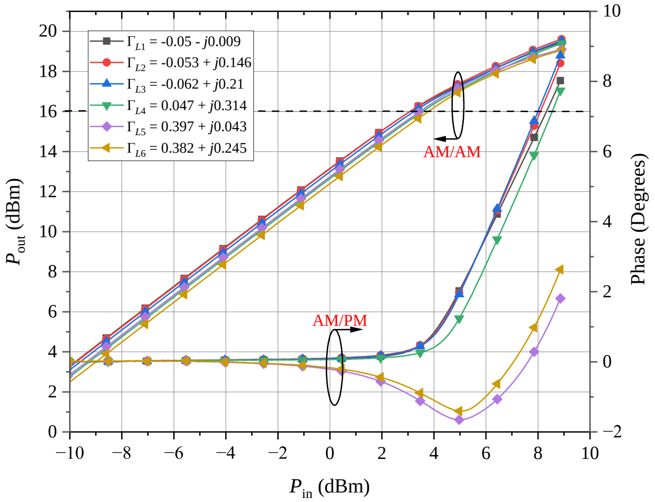


Fig. 6. Bessel-Fourier fitted AM/AM and AM/PM simulation curves associated with 6 varied $\boldsymbol{\Gamma}_L$ for PA-1. These 6 $\boldsymbol{\Gamma}_L$ are selected around 19 dBm P_{out_1dB} contour line, marked in Fig. 4(a).

be calculated using

$$\boldsymbol{b} = B\left(\rho_{in}\right) e^{j[(\varphi_{in}+F(\rho_{in})]}, \tag{6}$$

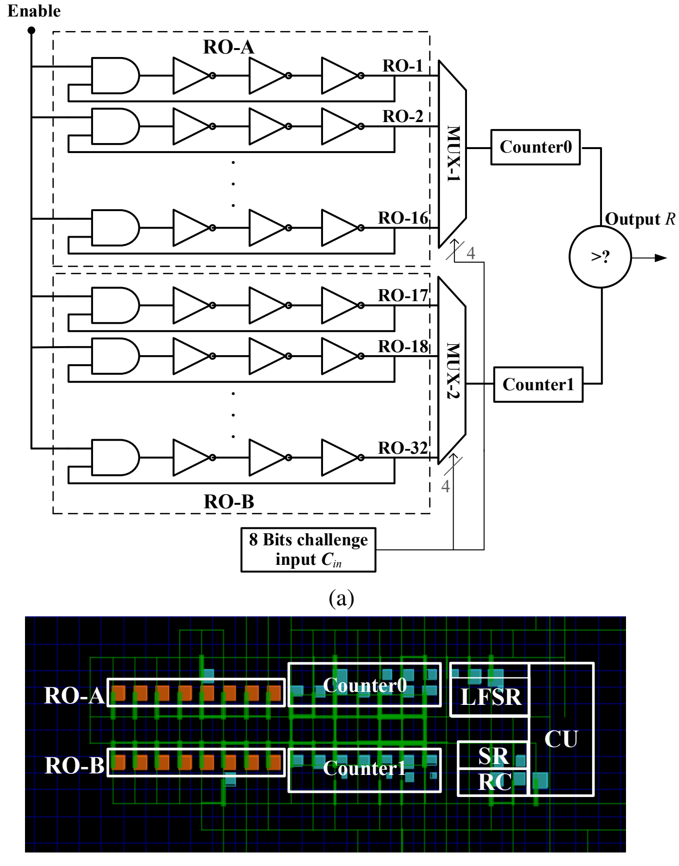
where ρ_{in} and φ_{in} represent the magnitude and the phase of the PA input signals $\boldsymbol{x}_{in}$.

From the above discussions and (2) to (6), we can see that the PA load impedance can be pulled around by choosing appropriate $Ae^{j\theta}$, i.e., active load-pulling. Even though the PA loads can be pulled anywhere, in order not to compromise the communication link quality, the selectable output reflection coefficients $\boldsymbol{\Gamma}_L$ needs to be located around the output power contour line that passes through the origin $\boldsymbol{\Gamma}_0$. This guarantees that the changes of PA loads do not affect the PA output power, comparing with the conventional 50 Ω system. Thus, in principle it can be infinite number of possible PA load choices, while in practice the number is limited by the resolution of magnitude and phase control of $Ae^{j\theta}$.

It is expected that the differences in the PA non-linear characteristics associated with these different loads are more distinct. Taking PA-1 as an example, the AM/AM and AM/PM characteristics were measured for 6 different selected $\boldsymbol{\Gamma}_L$, and the Bessel-Fourier fitted curves are shown in Fig. 6. It can be observed that different $\boldsymbol{\Gamma}_L$ affects PA characteristics, especially the AM/PM, which will eventually contribute to enlarged RFF features for secure device identification.

IV. PUF-assisted Active Load-pulling

In the above section, it has been shown that the active load-pulling technique can be used to adjust the PA non-linearity without compromising output power. In order for these changes of PA non-linearity characteristics to be used for RFFI, the control of the changes has to be secure. In our design we propose to use PUF circuitry in each DUT to generate a unique and unknown address for selecting a value of $Ae^{j\theta}$ that corresponds to a selectable $\boldsymbol{\Gamma}_L$ in a pre-stored look-up table.



(a)

(b)

Fig. 7. RO-PUF (a) circuit design and (b) FPGA implementation.

A. PUF Circuit

Numerous PUF designs have been developed, such as arbiter PUF, static random-access memory (SRAM) PUF, and RO-PUF [38]. Among them, the RO-PUF is one of the most widely studied PUF designs thanks to its simplicity and excellent reliability [38], and it is chosen for our application.

Our RO-PUF design is composed of 32 ROs, 2 multiplexers, 2 counters, one comparator, one shift register (SR), one reference counter (RC), one linear feedback shift register (LFSR) and one control unit (CU). The simplified block diagram and the implementation layout are shown in Fig. 7. Each RO delay line consists of 1 AND gate and 3 NOT gates. Overall, the proposed RO-PUF only requires a look-up table of a size of 269 and extra 170 flip-flops. Those digital resources can be readily available in many digital chips in low-cost IoT devices.

Algorithm 1 describes the operation of the developed RO-PUF for generating one output bit R. An 8-bits $\boldsymbol{C}_{in}$ is first initiated in CU module, and it is then divided into 4 most significant bits (MSB) and 4 least significant bits (LSB) by LFSR. The 4 MSB (and LSB), acting as the selection address, make multiplexer output the response from one of the selected ROs in the group RO-A (and RO-B). After counting the number of rising edges within the time period of which the RC reaches its maximum, the outputs of Counter0 and Counter1 are compared to generate one PUF output bit R of '0' or '1'. The above process is repeated for K times for different $\boldsymbol{C}_{in}$ in order to produce a random bit sequence of length K.

Algorithm 1 RO-PUF Operation for One Challenge Input

```
Input: 8-bit $\boldsymbol{C}_{in}$
Output: 1-bit $R$
Initialization: enable, reset, RC, Counter0, Counter1.
Divide 8-bit $\boldsymbol{C}_{in}$ into 4-bit $\boldsymbol{C}_{MSB}$ and $\boldsymbol{C}_{LSB}$ in LFSR.
Start 32 ROs.
Input $\boldsymbol{C}_{\{MSB,LSB\}}$ to select one out of 16 ROs in {RO-A; RO-B}.
while RC < maximum value do
    Count rising edges of selected ROs in {RO-A;RO-B} with Counter{0; 1}.
    RC = RC + 1.
end while
if Counter0 > Counter1 then
    $R$ = 0
else
    $R$ = 1
end if
Reset
```

TABLE II
MEASURED OUTPUT BIT *R* OF IMPLEMENTED RO-PUF AMONG 8 FPGA BOARDS.

$\boldsymbol{C}_{in}$ in Dec	*B*#1	*B*#2	*B*#3	*B*#4	*B*#5	*B*#6	*B*#7	*B*#8
1	1	1	1	0	0	1	1	0
2	0	1	1	1	1	0	1	0
3	1	1	0	0	1	0	0	1
4	1	0	0	1	1	1	1	0
5	0	0	0	1	1	1	0	1
6	0	1	1	1	0	1	1	0
7	1	1	1	0	1	0	0	0
8	0	1	1	1	1	0	1	0
9	1	0	0	1	0	0	0	0
⋮								
64	1	0	1	1	0	1	1	0
128	0	1	1	0	1	1	0	0
160	1	1	0	0	1	1	0	0
224	0	1	0	1	0	0	1	1

Note: $B\#u$ refers to the u^{th} FPGA board.

As examples, the output bit *R* of 8 PUF implementations for different $\boldsymbol{C}_{in}$ are listed in Table II.

The number of bits of C_{in} in our design is determined by the number of RO chains. Specifically, the designed RO-PUF consists of 32 ROs which are organized into two sets of 16 chains each. In order to select one of the 16 chains, a 4-bit input is required. Thus, in total, 8-bit $\boldsymbol{C}_{in}$ is needed to operate this designed PUF.

The PUF performance is evaluated through its uniqueness and reliability. The uniqueness evaluates how easily the responses of different PUF implementations can be differentiated when the same challenge input is used. The uniqueness is often calculated using the inter-Hamming Distance betweem the output bit sequence of different PUF instances, and it is expresses as follows

$$\text{Uniqueness} = \frac{2}{M(M-1)} \sum_{u=1}^{M-1} \sum_{j=u+1}^{M} \frac{HD\left(\vec{R}_u, \vec{R}_j\right)}{N} \times 100\%, \tag{7}$$

where M is the number of FPGA board, *HD* referrs to the Hamming Distance function to calculate the number of positions at which the corresponding bits are different, $\vec{R}_u = (R_{u1}, R_{u2}, ..., R_{u6})$ is the output bit sequence of the u^{th} PUF board of length N (N is selected to be 6 in our study), and $\vec{R}_j$ is the output bit sequence of the j^{th} PUF board. For an ideal PUF with completely random responses, the expected uniqueness value is 50%, indicating that any two responses are expected to differ in half of their bits.

The reliability assesses the robustness of a PUF design, i.e., the same input challenge applied on the PUF circuit is expected to always generate the same output. The metric for assessing the reliability of the PUF circuit is intra-Hamming Distance that compares multiple output bit sequences from the same PUF instance under different conditions. The calculation of the reliability can be expressed as follows

$$\text{Reliability} = \left(1 - \frac{1}{k} \sum_{i=1}^{k} \frac{HD\left(\vec{R}_u, \vec{R'}_{u,i}\right)}{N}\right) \times 100\%, \tag{8}$$

where k is the number of output bit sequences that have been collected from the same PUF, $\vec{R'}_{u,i}$ is the i^{th} sample of $\vec{R'}_u$. The ideal reliability of the PUF circuit is 100%.

In our PUF design among 8 FPGA implementations, the average uniqueness is around 54%, and the average reliability reaches up to 99%. The results show decent PUF performance. There are plenty of other PUF circuit topologies, and normally there is a trade-off between PUF performance and circuit complexity. We choose RO-PUF in our design due to its simplicity and decent performance, which is sufficient to be used as our proof-of-concept to demonstrate PUF-assisted RFF.

B. PUF Control

Upon identification of the $\boldsymbol{\Gamma}_L$ that can be selected from the poll, for example, the circles depicted on the contours in Fig. 4, it is imperative to adjust the different PA devices of the same brand to align with one of these loads by utilizing the active load-pulling technique as discussed in Section III-C. This adjustment needs to be fixed for each PA, but random and unknown to every party in the network, including the PAs themselves. This is achieved using our designed RO-PUF circuitry.

For our RFFI application, the minimum required number K of different $\boldsymbol{C}_{in}$ is determined by the number M of pre-determined selectable $\boldsymbol{\Gamma}_L$ for each DUT, namely $2^K \geq M$. In our study, we choose 6 selectable $\boldsymbol{\Gamma}_L$ for each DUT, so at least 3 different input challenges $\boldsymbol{C}_{in}$ are needed. In order to get more equal chances of each of the 6 $\boldsymbol{\Gamma}_L$ being selected, we choose 6 different input challenges $\boldsymbol{C}_{in}$ out of 256 possibilities, some of which are measured and listed in

Algorithm 2 The workflow of the PUF control for the active load-pulling at the transmitter. M = 8 and K = 6.

```
Input: $\vec{R} = (R_1, R_2, R_3, R_4, R_5, R_6)$
Output: Output: $Ae^{j\theta}$
Converting $\vec{R}$ to a decimal value, $d_R$
Mapping $d_R$ to $\Gamma_{Lk}$
    • 0 to 10 to $\Gamma_{L1}$
    • 11 to 21 to $\Gamma_{L2}$
    • 22 to 32 to $\Gamma_{L3}$
    • 33 to 43 to $\Gamma_{L4}$
    • 43 to 54 to $\Gamma_{L5}$
    • 55 to 63 to $\Gamma_{L6}$
Using (2), (4)-(6), mapping $\Gamma_{Lk}$ to $Ae^{\theta}$
```

Table II. In the design, 8-bit $\boldsymbol{C}_{in}$ means $2^8 = 256$ different challenge inputs. Since our RO-PUF circuit is symmetric, in terms of the first 16 ROs and the second 16 ones, statistically $\boldsymbol{C}_{in}$ can be randomly selected when the number of devices is large.

Due to the nature of anti-counterfeiting, for the same input, different devices will have different outputs although they have the same PUF design implemented. Therefore, the attacker has very limited opportunity of copying or cloning the PUF response to get access by mimicking a genuine wireless device.

The algorithm of our designed PUF control is given in Algorithm 2. After converting the PUF output bit sequence $(R_1, R_2, ..., R_6)$ to a decimal number, they are mapped to K = 6 pre-selected $\boldsymbol{\Gamma}_L$ by (quasi-) equally divide 2^6 into K sections. This selected $\boldsymbol{\Gamma}_{Lk}$, fixed but unknown, is then mapped to $Ae^{j\theta}$ using relationships as described in (2), and (4)-(6). In this way, the PA output load impedance is pulled to $\boldsymbol{\Gamma}_{Lk}$, which is unknown and different to different DUTs. As an example, Table III gives the mapping from $\vec{C_{in}} = (\boldsymbol{C}_{in1}, \boldsymbol{C}_{in2}, ..., \boldsymbol{C}_{in6})$ to $\vec{R} = (R_1, R_2, ..., R_6)$, to $\boldsymbol{\Gamma}_{Lk}$, and ultimately to $Ae^{j\theta}$ as required to control PA active load-pulling. In summary, what really affects the RFFI performance in our work is the selected PA active load impedance. As it is explained in Section IV and Algorithm 2, a PUF output is mapped to $\boldsymbol{\Gamma}_{Lk}$ which will alter the PA non-linearity. A list of selectable $\boldsymbol{\Gamma}_{Lk}$ is pre-generated, as explained in Section IV-B. Here, even if the PUF outputs are similar, e.g., with only one bit difference, these outputs can still be effectively mapped to totally different $\boldsymbol{\Gamma}_{Lk}$.

V. RFFI Protocol

A. Overview

As shown in Fig. 8, a deep learning-based RFFI protocol, adopted in our work, consists of two stages, training and classification. In the training stage, the receiver collects sufficient packets from each DUT to build a training dataset. The raw IQ samples are first converted to a colored-constellation diagram (CCD), which is a 2-D image in I/Q plane and it will be explained in Section V-B. A CNN classifier will then be trained, whose model details will be introduced in Section V-C. During the classification stage, the receiver captures a signal from a DUT, generates CCD, and then passes it to the trained classifier. The receiver will then predict the identity of the DUT.

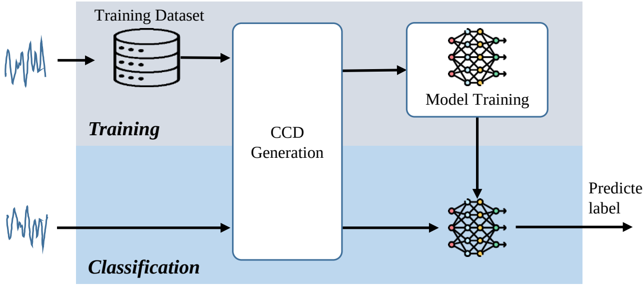


Fig. 8. Deep learning-based RFFI protocol.

B. CCD Generation

In our previous work [19], it was found that when non-linear PAs are cascaded with pulse shaping filters, the signals experience memory effects which result in irregular symbol clusters in constellation diagrams. When the data sequence is predetermined, extracting RFF features directly from raw I/Q samples in a time sequence becomes feasible. However, in our study, we aim to keep the method more generic, i.e., data sequence is dynamic and unknown. The raw I/Q data for each transmission thus are different because of the random nature of the symbols in the data streams. In this sense, using I/Q data in time domain for RFF becomes inapplicable.

Following similar link-level simulation procedures described in [19], the CDs in the I/Q plane, using 16-QAM as an example in this paper, were obtained. They are subsequently converted to colored density plots, referred to as CCDs. The CCDs are able to highlight the unique and irregular shapes, as well as the symbol cluster density distributions, of the constellation symbols for RFF classification [19]. The mathematical expression for the CCD generation can be described as

$$g\left[\frac{d_{\max}^{(q)}/2}{\left|P^{(q)} - z^{(q)}\right|}\right], \tag{9}$$

where $z^{(q)}$ are received symbols in the q^{th} constellation cluster (q = 1, ..., Q, with Q being 16 for the 16-QAM scheme) whose noiseless and interference-free reference constellation point is $P^{(q)}$. In the q^{th} constellation cluster, the maximum symbol offset is $d_{\max}^{(q)}$, with its half being taken as a ratio reference. $g[\cdot]$ is the heat map scale function, returning color density scale from 0 to 1 covering all $z^{(q)}$ distributions in the I/Q plane. In our work, the resulting CCDs are saved as JPEG image files. The dimension of CCD image determines the CNN training complexity. The larger the dimension, the more computation resources are required, see the CNN training times in Table IV. For this trail test, the CNN training network parameters were set as follows: initial learning rates of 0.1, maximal epoch of 60, and the minimum batch size of 64. Increasing the CCD image pixel size can improve validation accuracy to a certain extent. However, excess image details could potentially make CNN focus on non-important features, which is also evidenced in Table IV. Considering the results in the table, the CCD dimension of [295×295] was chosen in our study.

TABLE III

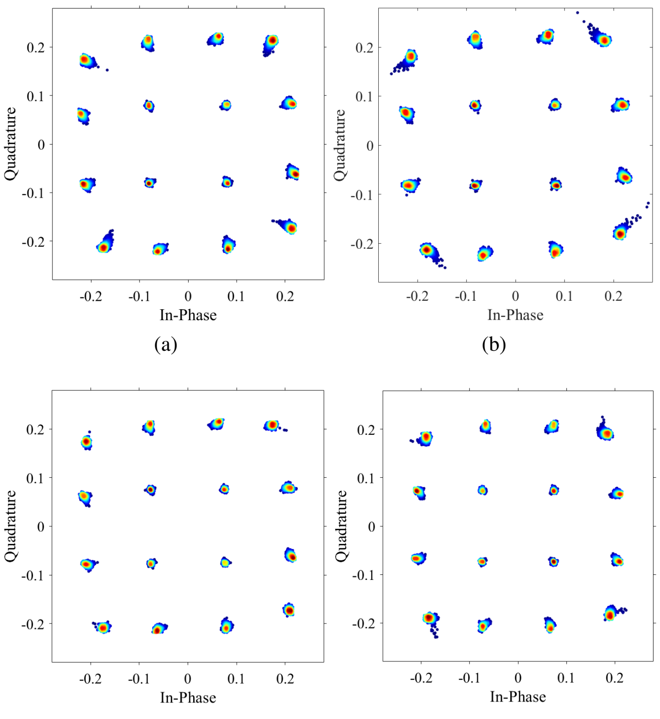
EXAMPLE OF MAPPING ($\boldsymbol{C}_{in1}, \boldsymbol{C}_{in2}, ..., \boldsymbol{C}_{in6}$), TO ($R_1, R_2, ..., R_6$), TO $\boldsymbol{\Gamma}_{Lk}$, AND ULTIMATELY TO $Ae^{j\theta}$ FOR PA-1 ACTIVE LOAD-PULLING.

($\boldsymbol{C}_{in1}, \boldsymbol{C}_{in2}, ..., \boldsymbol{C}_{in6}$) in Dec.	(6, 5, 2, 128, 1, 3)	(128, 1, 8, 9, 5, 6)	(224, 64, 3, 1, 2, 6)	(1, 6, 128, 7, 224, 3)	(160, 3, 5, 2, 6, 128)	(1, 9, 128, 3, 4, 7)
($R_1, R_2, ..., R_6$) in Dec.	3	16	28	37	48	55
k	1	2	3	4	5	6
$\boldsymbol{\Gamma}_{Lk}$	$-0.033 + j0.058$	$-0.044 - j0.054$	$-0.085 + j1.48$	$-0.333 - j0.008$	$-0.008 + j0.255$	$-0.0015 - j0.0.047$
$Ae^{j\theta}$	$0.845e^{j212^\circ}$	$0.85e^{j190^\circ}$	$0.75e^{j146^\circ}$	$0.63e^{j54.4^\circ}$	$0.75e^{j9.9^\circ}$	$0.93e^{j-131^\circ}$

TABLE IV

CNN TRAINING TIME AND VALIDATION ACCURACY WITH DIFFERENT CCD IMAGE SIZES.

Image size	Training time	Validation accuracy
[192×192]	775s	93.32%
[224×224]	948s	93.46%
[295×295]	1426s	94.68%
[350×350]	3021s	94.57%



(a)

(b)

(c)

(d)

Fig. 9. CCDs associated with the $\boldsymbol{\Gamma}_{L\{1,3,4,6\}}$ of PA-1. SNR is set to 30 dB in the simulation. (a) $\boldsymbol{\Gamma}_{L1}$. (b) $\boldsymbol{\Gamma}_{L3}$. (c) $\boldsymbol{\Gamma}_{L4}$. (d) $\boldsymbol{\Gamma}_{L6}$.

As examples, the simulated CCDs based on the measured AM/AM and AM/PM characteristics of the PA-1 for $\boldsymbol{\Gamma}_{L\{1,3,4,6\}}$ are plotted in Fig. 9. It can be seen that there are visible differences in CCDs, demonstrating the effectiveness of changing $\boldsymbol{\Gamma}_L$ on enlarging RFF features.

C. CNN Classifier

CNN is utilized to extract and classify the RFF feature exhibited in the CCDs. The resulting CCDs are input to the classification system, which performs feature weight calculation and outputs a class or probability of the input image belonging to a pre-trained class.

In our study, the constructed CNN classification system consists of 4 convolution layers, 3 max-pooling layers, and 1 fully connected layer. The input image size is set to (295, 295, 3), corresponding to (height, width, RGB). The Rectified Linear Unit (ReLU) activation function is set within the convolution layers. Moreover, the fully connected layer uses the softmax activation function to perform the classification among the target devices. The filter size in each convolutional layer is set to (3 × 3) in order to capture the details of the proposed RFF in the CCDs, with the corresponding number of filters being set to 32, 64, 128 and 256. In addition, during the training of the proposed CNN network set, we perform a parameter sweep to find its optimal hyperparameters. The hyperparameters include the number and size of filters for each convolutional layer, the initial learning rate, the minimum batch size, and the maximal epoch.

VI. EXPERIMENTAL EVALUATION

In this section, the performance of the proposed RFFI system is evaluated in the cable-connected and OTA measurements.

A. Setup

1) Device Configuration: The configuration of the experiments for the proposed PUF-assisted RFF transmitter is depicted in Fig. 2. For cable-connected measurements, the antenna is replaced with a direct RF coaxial cable connection. In the experiments, the sampling rate is set to 2 Msps, and the roll-off factor β, symbol span D, and symbol duration T of the RRC filter are set to 0.5, 8, and 100 ms, respectively. With deliberately chosen long symbol duration T, the inter-symbol interference (ISI) is dominantly contributed by the non-linear memory effect because of the cascade of the transmitter RRC, the non-linear PA, and the receiver RRC. This reduces the potential ISI effect from the multi-path channels.

2) CNN Configuration: Training dataset: The receiver data are collected for selected $\boldsymbol{\Gamma}_{Lk}$ (k = 1, 2, ..., 6) of each PA under test in high SNR condition, i.e., 40 dB, under both cable-connected and OTA measurements. The additive white Gaussian noise (AWGN) is subsequently applied to these high SNR symbols, artificially producing numerous training samples with varied SNRs. In this work, the SNR range for the training samples is set to 0 dB to 35 dB with a step of 1 dB, 50 data packets per SNR value, or equivalently CCDs, are generated for each of the 6 chosen $\boldsymbol{\Gamma}_L$ for each PA. The training dataset consists of all samples associated with the 8 PAs. The samples in the dataset are randomly divided into 80% and 20% for training and validation. Test dataset: For the test dataset, the receiver data are collected from each targeted PA with the selected $\boldsymbol{\Gamma}_{Lk}$, and they are converted to CCDs.

TABLE V
CNN TRAINING HYPERPARAMETERS.

Training hyperparameters	Range	Optimal value
Optimizer	(Rmsprop, Adam, Sgd)	Sgd
Initial learning	(0.1, 0.001, 0.0001)	0.0001
Mini-batch size	(32, 64, 128, 256)	128
Maximal epochs	(60–150)	150
Filter size	(3, 6, 9)	3
No. filter 1st layer	(16, 32)	32
No. filter 2nd layer	(32, 64, 128)	64
No. filter 3rd layer	(64, 128, 256)	128
No. filter 4th layer	(128, 256, 512)	256

For each target PA under test, the test dataset comprises 200 packets per SNR value.

The minimum batch size, the maximal epoch, and the initial learning rate are set to 128, 150, and 1×10^{-4}, respectively. All the deep learning models were trained and tested on a PC with NVIDIA GeForce GTX 4060 GPU using Matlab deep learning toolbox[1]. The hyperparameters of the proposed CNN architecture are listed in Table V.

B. PA Active Load-Pulling Test

Using the active load-pulling setup in Fig. 5, 6 measured $\boldsymbol{\Gamma}_L$ for each PA are selected, and their AM/AM and AM/PM curves are measured, and Bessel-Fourier fitted, see the example for the PA-1 in Fig. 10. It is worth pointing out that the PA output reflection coefficients $\boldsymbol{\Gamma}_{Lk}$ in Fig. 6 are obtained using a Maury passive load tuner. The PA load-pull results are shown in Fig. 4, from which the selectable PA load impedance (or reflection coefficients $\boldsymbol{\Gamma}_L$) is labelled. Those PA characteristics shown in Fig. 6 are used in the simulations presented in Fig. 9. While in Fig. 10, the 6 selectable $\boldsymbol{\Gamma}_L$ were generated using the active load-pulling effect, instead of using a passive load tuner. This is a more practical method in IoT applications as only minimum hardware add-ons (e.g., circulator and Mag/Phase control devices) are required. However, this, unfortunately, is less accurate than the passive method due to the variation and non-ideal property of the extra hardware employed. Thus, in Fig. 10 the 6 selectable $\boldsymbol{\Gamma}_L$ generated using this active load-pulling method are slightly different from those selected in Fig. 6. There are subsequently used in the experimental validation presented in the following subsections. Despite these differences, all selected $\boldsymbol{\Gamma}_L$ meet RFF requirements, ensuring minimal impact on the link performances.

C. Cable-Connected Evaluation

The cable-connected measurement is first conducted in order to provide a baseline assessment of the proposed RFFI system, removing other factors introduced by the characteristics of the antenna and the wireless multi-path channel. This allows us to better understand the capabilities of the proposed RFFI system.

A photograph of the cable-connected experiment is shown in Fig. 11. The transmitter, consisting of a USRP X310, a PA under test, a circulator, and a tunable attenuator, is directly connected to a receiver (USRP N200) via a well-matched RF coaxial cable. The tunable attenuator here is added to adjust the SNR of the received signals, which can create test datasets with different SNR levels.

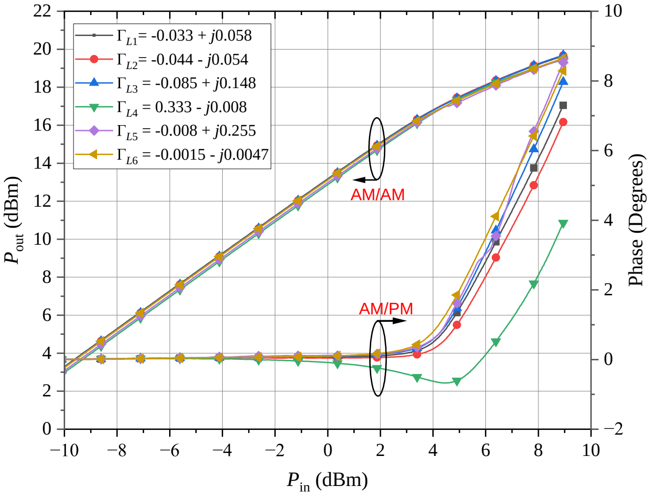


Fig. 10. Bessel-Fourier fitted AM/AM and AM/PM measurement curves with 6 varied $\boldsymbol{\Gamma}_L$ for PA-1.

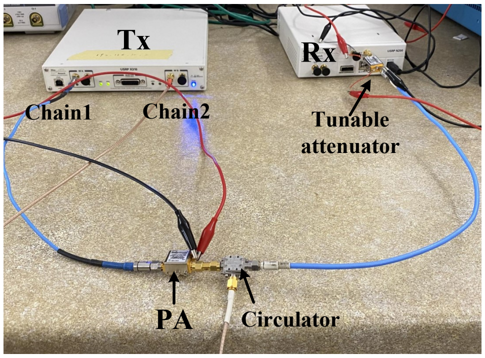


Fig. 11. Photograph of the cable-connected experiment setup.

Our initial measurement focused on the evaluation of the effects of the 6 different $\boldsymbol{\Gamma}_L$ on the non-linear memory RFF features for each PA. Specifically, each PA output reflection coefficient is set to each of the pre-selected $\boldsymbol{\Gamma}_{Lk}$ $(k = 1, 2, ..., 6)$ by leveraging the active load-pulling technique outlined in Section III-C. The measured constellation diagrams for the PA-1 associated with the 6 $\boldsymbol{\Gamma}_L$ are exemplified in Fig. 12, while the converted CCDs are showcased in Fig. 14. These results suggest that the active load-pulling technique can modify the non-linear characteristics of the PA by tuning the coefficient $Ae^{j\theta}$.

In order to demonstrate that the proposed active PA load-pulling does not severely compromise link performance, the link bit error rates (BERs) have been calculated that are based on the measured data in the cable-connected experiment. For the BERs shown in Fig. 13 for the PA-$\{3, 6\}$ with different PA loads, i.e., 50 Ω load and the other 6 selectable active loads, it can be seen that in low to medium SNR up to 10 dB, the system performance is reduced by only about 1 to 2 dB. In the high SNR region, the links with load-pulling PAs appear to have a higher noise floor compared with the fixed 50 Ω system.

[1] https://uk.mathworks.com/help/deeplearning/

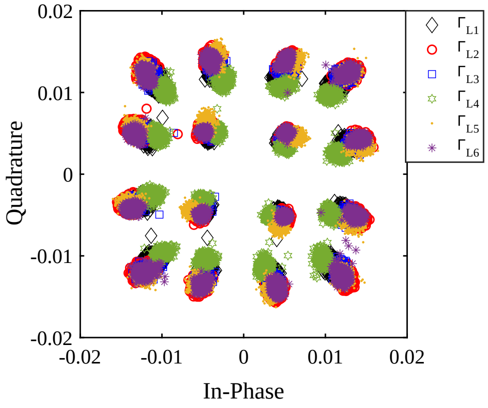


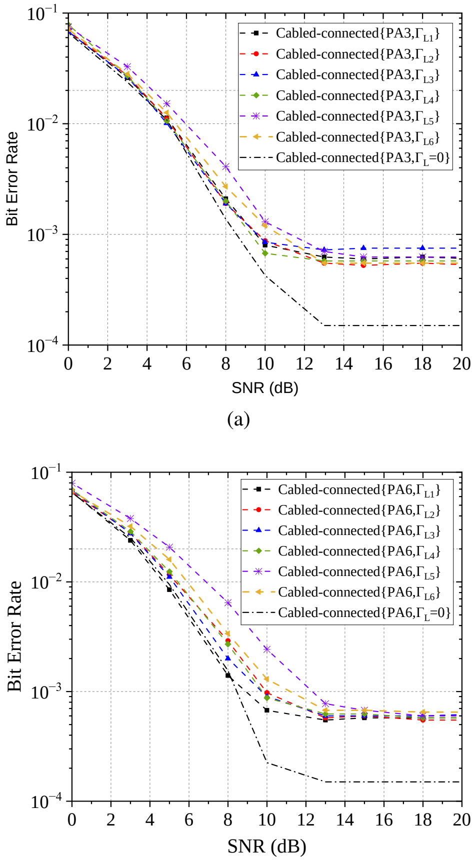
Fig. 12. Measured 16-QAM CDs for the cable-connected link with PA-1. Six $\boldsymbol{\Gamma}_L$ shown in Fig. 10 were studied. PA output power was kept identical to around 16 dBm.

This phenomenon is likely attributed by the extra interference due to the non-ideal isolation of the RF circulator. Overall, it is important to highlight that the utilization of the PUF-assisted RFF approach, facilitated through active load-pulling to adjust PA output impedance does not noticeably compromise the link performance. The observed degradation of 1 to 2 dB can be tolerated by wireless receivers.

Furthermore, we generated sufficient CCD images for training and test. The classification accuracy versus SNR for each PA, which is obtained by averaging among 6 varied $\boldsymbol{\Gamma}_{Lk}$, is shown in Fig. 15. The training dataset for this test comprises 10,800 packets for each PA, structured into 6 $\boldsymbol{\Gamma}_L$, each containing 1,800 packets. The configuration of this training dataset is denoted as the training set#1. From the results, we can see that compared with other PAs, the PA-3 is slightly less sensitive to the load changes, and the average classification accuracy for each of the remaining PAs is higher than 90% when SNR is no lower than 21 dB. Overall, this demonstrates the effectiveness of enlarging RFF feature differences by actively altering the PA output impedance without compromising the link power budget.

We also evaluated the effects of active load-pulling on different PAs. For one experiment, each PA is randomly assigned with a $\boldsymbol{\Gamma}_{Lk}$, which forms eight new PA models, given as $\{PA_i, \boldsymbol{\Gamma}_{Lk}\}$. We then collected training and test dataset and performed classification. Such experiments were repeated for 20 rounds with random selections of $\boldsymbol{\Gamma}_{Lk}$. The training dataset configuration for this test comprises 14,400 packets, structured into 8 PAs with $\boldsymbol{\Gamma}_{Lk}$. The configuration of this training dataset is denoted as the training set#2.

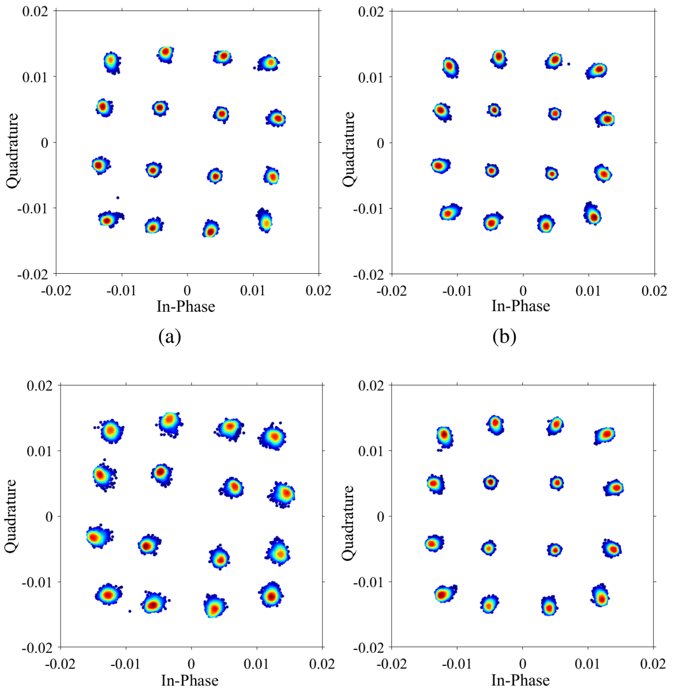
The average classification accuracy over 20 tests is shown in Fig. 16. The proposed PUF-assisted RFF methodology significantly outperforms the conventional 50-Ω load system in the cable-connected experiment, especially in low SNR regions. As examples, about 22%, 17%, and 12% improvements are achieved at SNRs of 0 dB, 5 dB, and 10 dB, respectively. The accuracy is higher than 90% when SNR is no lower than 21 dB.



(a)

(b)

Fig. 13. Calculated BER curves associated with different PA loads, based on the measured data in cable-connected experiment, (a) PA-3; (b) PA-6.



(a)

(b)

(c)

(d)

Fig. 14. Measured CCDs associated with the different $\boldsymbol{\Gamma}_L$ of PA-1. The measured SNR is around 35 dB. (a) $\boldsymbol{\Gamma}_{L1}$. (b) $\boldsymbol{\Gamma}_{L3}$. (c) $\boldsymbol{\Gamma}_{L4}$. (d) $\boldsymbol{\Gamma}_{L6}$.

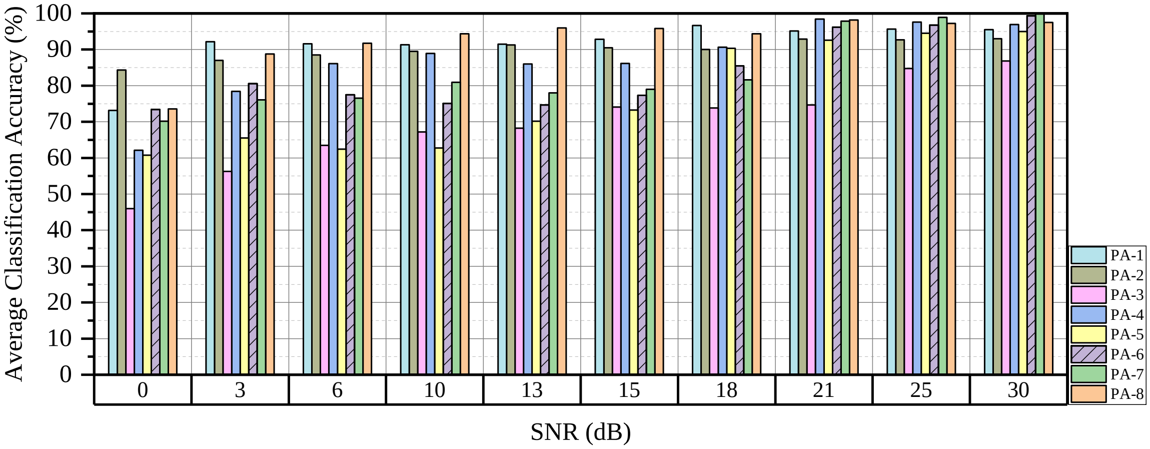


Fig. 15. Average classification accuracies among 6 varied $\boldsymbol{\Gamma}_L$ for each of the 8 PAs in the cable-connected measurements.

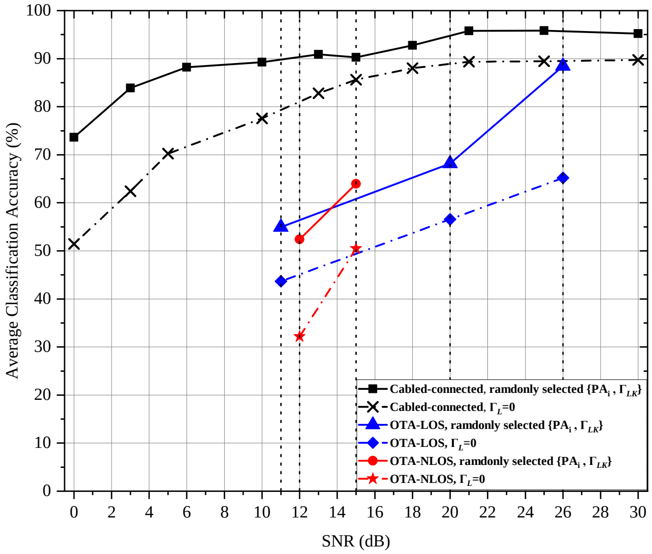


Fig. 16. Average classification accuracy in cable-connected and OTA measurements.

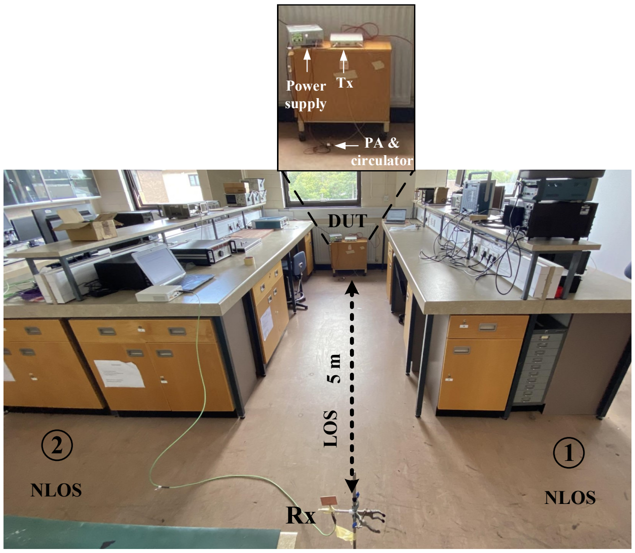


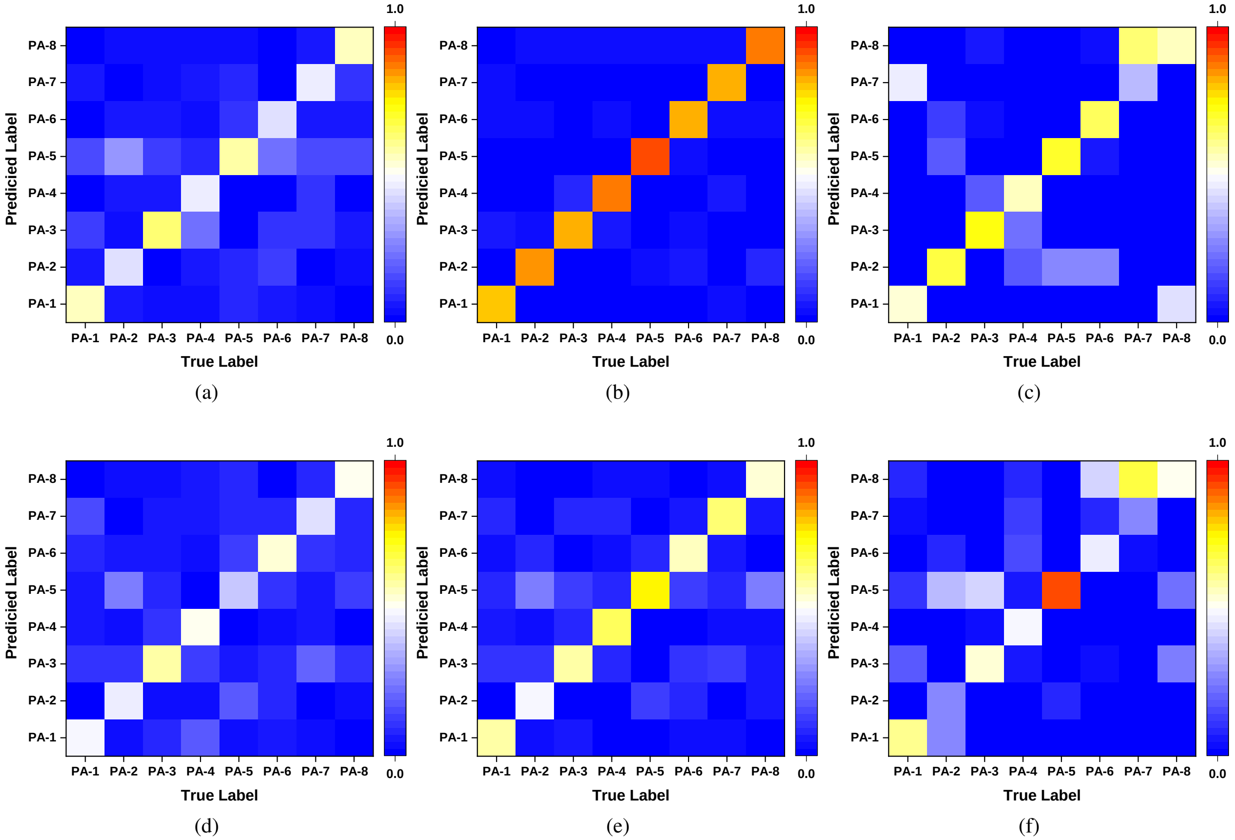
Fig. 17. Photograph of the OTA experiment setup.

D. OTA Experimental Evaluation

To study the RFFI performance in a real wireless link, OTA experiments were conducted, which include all other effects from antennas and wireless channels. During this process, the receiver collects the wirelessly transmitted signals from the target DUTs with varied $\boldsymbol{\Gamma}_L$. The experiment photo is given in Fig. 17. Both LOS and NLOS link environments were investigated. The target DUTs and the receiver were positioned in a lab with common lab furniture and equipment around. At the transmitter and receiver ends, two vertically polarized microstrip patch antennas were deployed, with a realized gain of approximately 4.5 dBi at the operation frequency of 2.4 GHz. For the LOS scenario, transmission distances of 1 meter, 3 meters, and 5 meters were studied, corresponding to measured SNRs of 26, 20, 11 dB, respectively. Regarding the NLOS measurements, the receiver was located at two labeled locations, as indicated in Fig. 17. The measured SNRs of the two NLOS scenarios were found to be around 15 dB and 12 dB for locations 1 and 2. During the OTA measurement, the $\boldsymbol{\Gamma}_L$ of the DUTs were adjusted by the active load-pulling technique in a similar way as in the cable-connected experiment. In the training stage, an LOS link enjoying higher than 40 dB SNR was used. The classification errors are randomly distributed among devices, which indicates their hardware RFF feature differences are enlarged.

Same as the cable-connected measurements, in the OTA measurements, each of the eight PA models was paired with a selectable $\boldsymbol{\Gamma}_L$, and 20 tests were performed. The average classification accuracy is also shown in Fig. 16. In the LOS scenario, the accuracy is 88.43% at SNR of 26 dB, and 64% at SNR of about 15 dB for the NLOS scenario. The OTA experiment demonstrated about 11% to 24% improvement in average classification accuracy with the proposed PUF-assisted RFFI system under both LOS and NLOS OTA scenarios, compared to PAs under test having $\boldsymbol{Z}_L$ of 50 Ω. In contrast, the average classification drops to 60% in the OTA experiment at 15 dB SNR.

The confusion matrix can provide more details on classification performance, e.g., where the most mis-classification



(a) (b) (c)

(d) (e) (f)

Fig. 18. Confusion matrices in OTA measurements averaged among 20 random rounds. (a) The proposed approach, LOS-5m, average accuracy: 55%. (b) The proposed approach, LOS-1m, average accuracy: 88.43%. (c) The conventional apprach ($\boldsymbol{\Gamma}_L = 0$), LOS-1m, average accuracy: 65.2% (d) The proposed approach, NLOS-2, average accuracy: 52.4%. (e) The proposed approach, NLOS-1, average accuracy: 64%. (f) The conventional approach ($\boldsymbol{\Gamma}_L = 0$), NLOS-1, average accuracy: 50.5%

happens. The resulting confusion matrices based on these 20 rounds of random $\boldsymbol{\Gamma}_L$ selections in the OTA measurements are exemplified in Fig. 18, for both our proposed approach and the conventional method ($\boldsymbol{\Gamma}_L = 0$). By comparing Figs. 18(b) and 18(c) (and also Figs. 18(e) and 18(f)), our proposed approach has much better classification performance, in terms of the overall classification accuracy and the distribution of misclassification. For example, in Fig. 18(c), lots of misclassification happened between PA-1 and PA-7 as well as PA-7 and PA-8, which is not acceptable. Our proposed approach does not have dominant misclassification between any two PAs, as observed from Fig. 18(a), (b), (e), and (f), thanks to the enlarged the RFF feature differences among wireless devices of same vendor.

VII. Conclusion

In this paper, a novel approach of utilizing PUF to assist the enlargement of the RFF feature differences among wireless devices of the same vendor was proposed. The PA's characteristic is affected by its output reflection coefficient $\boldsymbol{\Gamma}_L$ (or equivalently the output load impedance $\boldsymbol{Z}_L$), which can be tuned by exploiting the active load-pulling effect. We implemented RO-PUF to configure the PA output reflection coefficient $\boldsymbol{\Gamma}_L$ in a secure and unique way. The resulting enlarged PA RFF feature differences with varied PA output $\boldsymbol{\Gamma}_L$ was used for RFFI . We converted received signals to CCD and designed a CNN-based deep learning model for classification. The proposed RFFI approach was validated through the cable-connected and OTA experiments to classify eight PA models from the same vendor. In the cable-connected experiment, the proposed scheme achieved over 90% classification accuracy for SNRs of greater than 13 dB. In the OTA experiments, the average classification accuracy for the LOS scenario was 89% at SNR of 26 dB, and 64% at SNR of 15 dB for the NLOS scenario. This classification accuracy drop in the OTA experiment may be attributed to factors such as antenna impedance mismatch, multipath channels, and interference from ambient wireless systems operating at 2.4 GHz. Further investigations are needed to address these challenges and develop mitigation strategies. Compared to the conventional systems without enlarging RFF features, our proposed approach achieved 11% to 24% average classification accuracy improvement in the OTA tests.

References

[1] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani, "Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and a first empirical look on internet-scale IoT exploitations," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2702–2733, 2019.

[2] J. Zhang, G. Li, A. Marshall, A. Hu, and L. Hanzo, "A new frontier for IoT security emerging from three decades of key generation relying on wireless channels," *IEEE Access*, vol. 8, pp. 138 406–138 446, 2020.

[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, 2015.

[4] L. Xie, L. Peng, J. Zhang, and A. Hu, “Radio frequency fingerprint identification for Internet of Things: A survey,” *Security and Safety*, vol. 3, p. 2023022, 2024.

[5] 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, 2016.

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

[7] J. Zhang, G. Shen, W. Saad, and K. Chowdhury, “Radio frequency fingerprint identification for device authentication in the internet of things,” *IEEE Commun. Mag.*, vol. 61, no. 10, pp. 110 – 115, 2023.

[8] 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, 2020.

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

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

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

[12] S. Rajendran and Z. Sun, “RF impairment model-based IoT physical-layer identification for enhanced domain generalization,” *IEEE Trans. Inf. Forensics Security*, vol. 17, pp. 1285–1299, 2022.

[13] J. Xu and D. Wei, “Polarization fingerprint-based LoRaWAN physical layer authentication,” *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 4593–4608, 2023.

[14] H. Givehchian, N. Bhaskar, E. R. Herrera, H. R. L. Soto, C. Dameff, D. Bharadia, and A. Schulman, “Evaluating physical-layer BLE location tracking attacks on mobile devices,” in *Proc. IEEE Symposium on Security and Privacy (SP)*, 2022, pp. 1690–1704.

[15] 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.

[16] 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.

[17] S. S. Hanna and D. Cabric, “Deep learning based transmitter identification using power amplifier nonlinearity,” in *Proc. Int. Conf. Computing, Networking and Communi. (ICNC)*, 2019, pp. 674–680.

[18] J. Xu, Y. Shen, E. Chen, and V. Chen, “Bayesian neural networks for identification and classification of radio frequency transmitters using power amplifiers’ nonlinearity signatures,” *IEEE Open J. Circuits & Syst*, vol. 2, pp. 457–471, 2021.

[19] Y. Li, Y. Ding, J. Zhang, G. Goussetis, and S. K. Podilchak, “Radio frequency fingerprinting exploiting non-linear memory effect,” *IEEE Trans. on Cogn. Commun. Netw.*, vol. 8, no. 4, pp. 1618–1631, 2022.

[20] V. Chen, J. Xu, Y. Shen, and E. Chen, “RF fingerprint classification with combinatorial-randomness-based power amplifiers and convolutional neural networks: Secure analog/RF electronics and electromagnetics,” *IEEE Solid-State Circuits Mag.*, vol. 14, no. 4, pp. 28–36, 2022.

[21] Y. Ma and Y. Hao, “Antenna classification using Gaussian mixture models (GMM) and machine learning,” *IEEE Open J. Antennas Propag.*, vol. 1, pp. 320–328, 2020.

[22] S. Balakrishnan, S. Gupta, A. Bhuyan, P. Wang, D. Koutsonikolas, and Z. Sun, “Physical layer identification based on spatial–temporal beam features for millimeter-wave wireless networks,” *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 1831–1845, 2020.

[23] Q. Zhou, Y. He, K. Yang, and T. Chi, “Physical-layer identification of wireless IoT nodes through PUF-controlled transmitter spectral regrowth,” *IEEE Trans. Microw. Theory Techn.*, 2023.

[24] C.-H. Chang, Y. Zheng, and L. Zhang, “A retrospective and a look forward: Fifteen years of physical unclonable function advancement,” *IEEE Circuits Syst. Mag.*, vol. 17, no. 3, pp. 32–62, 2017.

[25] B. Chatterjee, D. Das, S. Maity, and S. Sen, “RF-PUF: Enhancing IoT security through authentication of wireless nodes using in-situ machine learning,” *IEEE Internet Things J.*, vol. 6, no. 1, pp. 388–398, Feb. 2019.

[26] A. Ashtari, A. Shabani, and B. Alizadeh, “A new RF-PUF based authentication of internet of things using random forest classification,” in *Proc. 16th Int. ISC Iranian Soc. Cryptol. Conf. Inf. Secur.Cryptol. (ISCISC)*, 2019, pp. 21–26.

[27] M. F. Bari, B. Chatterjee, K. Sivanesan, L. L. Yang, and S. Sen, “High accuracy RF-PUF for EM security through physical feature assistance using public Wi-Fi dataset,” in *Proc. IEEE Int. Microw. Symp. (IMS)*, 2021, pp. 108–111.

[28] S. Yoon, S. Han, and E. Hwang, “Joint heterogeneous PUF-based security-enhanced IoT authentication,” *IEEE Internet Things J.*, pp. 18 082–18 096, 2023.

[29] X. Qi, A. Hu, and T. Chen, “Lightweight radio frequency fingerprint identification scheme for V2X based on temporal correlation,” *IEEE Trans. Inf. Forensics Security*, 2023.

[30] A. Ghorbani and M. Sheikhan, “The effect of solid state power amplifiers (SSPAs) nonlinearities on MPSK and M-QAM signal transmission,” in *Proc. 6th Int. Conf. Digit. Process. Signals Communi.*, 1991, pp. 193–197.

[31] A. Saleh, “Frequency-independent and frequency-dependent nonlinear models of TWT amplifiers,” *IEEE Trans. Commun.*, vol. 29, no. 11, pp. 1715–1720, 1981.

[32] C. Rapp, “Effects of HPA-nonlinearity on 4-DPSK/OFDM-signal for a digital sound broadcasting system,” in *Proc. 2nd Eur. Conf. Satellite Communi.*, Oct. 1991, pp. 179–184.

[33] J. C. Fuenzalida, O. Shimbo, and W. L. Cook, “Time domain analysis of intermodulation effects caused by non-linear amplifiers,” *COM-SAT Tech.Rev.*, vol. 2, no. 1, pp. 89–143, 1973.

[34] M. J. C. Sanchez, A. Segneri, A. T. Georgiadis, S. A. Kosmopoulos, G. Goussetis, and Y. Ding, “System performance evaluation of power amplifier behavioural models,” in *Proc. IET Active Passive RF Devices Seminar*, London, U.K., Apr. 30, 2018, pp. 1–6.

[35] V. Teppati, A. Ferrero, and G. L. Madonna, *Modern RF and Microwave Measurement Techniques*. Cambridge University Press, 2013, ch. Load- and source-pull techniques, pp. 345–383.

[36] M. Microwave, “High-gamma automated tuners (HGT™) and high power automated tuners,” load tuner datasheet [Online], Aug. 28. 2023. Available: https://www.maurymw.com/pdf/datasheets/4T-050G06.pdf.

[37] Mini-Circuits. Ultra flat gain, low noise, monolithic amplifier, PGA-105+ datasheet. Accessed on Aug. 28. 2023. [Online]. Available: https://www.minicircuits.com/pdfs/PGA-105+.pdf

[38] T. Bauer and J. Hamlet, “Physical unclonable functions: A primer,” *IEEE Security Privacy*, vol. 12, no. 6, pp. 97–101, 2014.