RelativeRFF: Multi-Antenna Device Identification in Multipath Propagation Scenarios

Hongyi Luo*, Guyue Li*, Yuexiu Xing‡, Junqing Zhang§, Aiqun Hu†, and Xianbin Wang¶
*School of Cyber Science and Engineering, Southeast University, Nanjing, 210096, China
†Purple Mountain Laboratories for Network and Communication Security, Nanjing, 210096, China
‡School of Internet of Things, Nanjing University of Posts and Telecommunications, Nanjing, 210003, China
§Department of Electrical Engineering and Electronics, University of Liverpool, Liverpool, L69 3GJ, U.K.
¶Department of Electrical and Computer Engineering, University of Western Ontario, CA
Corresponding author: Guyue Li, Email: guyuelee@seu.edu.cn

***Abstract*—Radio frequency fingerprinting (RFF) is a promising solution for realizing secure and efficient device authentication. The multipath channel overshadows and disrupts the RFF extraction, which causes difficulties in training new models in the presence of fading. Existing approaches attempt to deal with this challenge by traversing channels through simulated channel models. However, this solution requires a large amount of data for training and it is difficult to guarantee that the training covers all possible channels. To mitigate the multipath channel effect on RFF with less training data, we propose a new method in a multi-antenna system, named Relative-RFF (R-RFF), which utilizes channel state information (CSI) feedback to counteract the multipath channel. The RFF imperfection relation between the different antenna chains of the device is proved to be retained after the counteraction of the multipath channel. Numerical results demonstrate that the proposed R-RFF can achieve an identification accuracy of 95.9% for 30 UEs in Tapped Delay Line channel with a signal-to-noise ratio of 20 dB.**

***Index Terms*—Physical layer security, radio frequency fingerprint, device identification, multipath channels.**

I. Introduction

With the unprecedented proliferation of wireless technologies, the number of wireless devices has dramatically increased. While they have become indispensable for both daily life and industrial production [1], wireless communications are vulnerable to malicious attacks due to the broadcast nature of radio signal propagations. Conventional authentication based on digital cryptographic techniques [2] cannot defend against spoofing and impersonating when a digital security scheme is compromised [3]. Moreover, the rapid increase in the number of devices brings tremendous pressure on the generation, distribution, and management of the keys [4, 5]. Consequently, a new and secure method of device authentication is urgently needed, and it should be lightweight and tamper-proof.

Radio Frequency Fingerprint (RFF) is a physical layer solution for secure device authentication [6]. Signal distortion or deformation can occur as a result of manufacturing tolerances and drift tolerances generated in the production of electronic components and printed circuit boards. By taking advantage of these hardware imperfections, the RFF of the device can be extracted for authentication. The identity of the device can be verified by its RFF before data exchange is performed, which enhances the wireless communication system's security. However, multipath channels present a significant obstacle for RFF in practical communications, which interferes RFF and makes it challenging to extract features that can be utilized for authentication from signals [7].

There are three primary categories of existing studies to counteract the impact of multipath channels on RFF, summized as follows.

- **Channel independent feature:** One strategy for combating multipath channels is to find an RFF feature that is resistant to channels. The phase relation between the different antenna chains is considered a feature for device authentication [8]. Nelder-Mead simplex channel estimation for RF-DNA fingerprinting under rayleigh fading conditions was studied, which proved to be superior to waveform-based estimation approaches under increasing fading paths [9]. The work in [10] designed channel independent spectrogram for LoRa RFF.
- **Channel elimination based on feedback:** A pioneering work of DeepRadioID proposed in [11] exploits channel state information (CSI) feedback to address this issue. They designed an FIR filter that dynamically adapts to the multipath channel and enhances fingerprinting from the feedback.
- **Data augmentation:** The data augmentation for channel-resilient RFF relies on a large amount of channel data [12], which results in 75% improvement in the former case with a custom-generated dataset. Theoretically, the more types of channels trained, the better the device classification will be.

However, in the practical multi-antenna system, each antenna has a unique RF imperfection for the transmitting chain and the receiving chain. Multipath channels are cascaded with RF imperfections, which leads to the fact that the upstream and downstream channels are no longer reciprocal. In this case, feedback CSI directly cannot perfectly eliminate the effects of multipath channels. In other words, even if the CSI of the multipath channel is obtained, we are unable to achieve the absolute RFF. The insight of [13] is that although we are unable to obtain the absolute RFF, the relative RFF we can obtain, i.e. we can derive the imperfection relation between

the different antennas of a multi-antenna device. However, obtaining the relative RFF alone is insufficient to successfully authenticate a device, we also need to design a CSI feedback mechanism to perfectly eliminate multipath channels. The feedback mechanism employs relative RFF to perfectly eliminate multipath channels while safely transmitting the relative RFF of the user equipment (UE) to the base station (BS).

To sum up, we propose a new scheme named Relative-RFF (R-RFF), which aims to eliminate multipath channels perfectly and establish RF defect relation between antennas to authenticate devices. Our main contributions are summarized as follows.

- We propose a new R-RFF scheme by exploiting CSI feedback for device authentication in multipath channels. With proper processing of the feedback and relative RFF, the R-RFF scheme is proved to be robust to multipath channels. At the receiving end, we demonstrate that the multipath channel can be perfectly eliminated while the R-RFF of the UE can be perfectly preserved.
- We propose a new relative RFF and give its extraction process. In the authentication phase, we derive a method to neutralize the RF imperfections of the BS and retain the UE imperfections using the relative RFF.
- We simulate three channels with a different number of paths in MATLAB using 5G NR PHY frames for 30 virtual UEs and different signal-to-noise ratio (SNR) levels. Simulation results show that the proposed method can achieve 95.9% recognition accuracy for 30 devices in the Tapped Delay Line (TDL) channel in 3rd Generation Partnership Project (3GPP) Technical Report (TR) 38.901 [14] with SNR of 20 dB.

The rest of the paper is organized as follows. Section II describes the system model and the challenge. Section III elaborates on the details of the proposed method and provides the theoretical analysis of the proposed method. Section IV presents the simulation results. Finally, Section V concludes this paper.

II. System Model

In this section, we present the RF characteristics considered in this paper and give a model of the signal under the influence of these RF imperfections. In addition, we theoretically analyze the challenge faced by traditional RFF extraction: in practical communication systems, the channels are often multipath, which disrupts the RFF. At the same time, multipath channels coupled with RF imperfections result in non-reciprocity of UL and DL channels, which brings the challenge to channel elimination based on feedback.

We consider an orthogonal frequency division multiple access (OFDMA) time division duplexing (TDD) system with multi-antenna UEs. Assume that BS has M antennas, and each of the K UEs has N antennas ($M > N$). The legitimate UE sends a pilot signal $\mathbf{x}_U$ to the BS for authentication. The system operates in the TDD mode and the channels of the uplink and downlink are reciprocal.

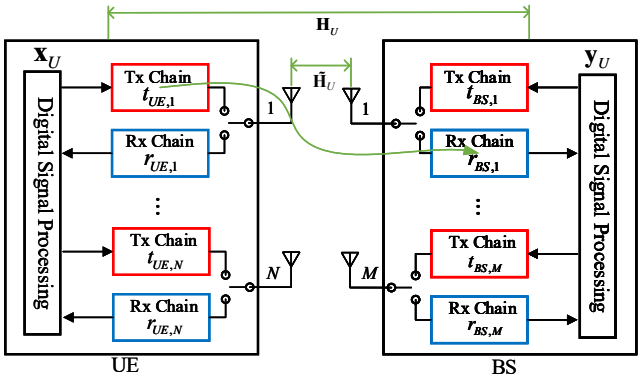

Fig. 1. Internal architecture of the multi-antenna device.

In the RF transmitting and receiving chains considered in this paper, we focus on the analog gains due to hardware imperfections, including DC bias error, Sample Frequency Offset (SFO), IQ imbalance, Carrier Frequency Offset (CFO), Carrier Phase Offset (CPO) and power amplifier (PA) nonlinear. We assume that the RF gains are determined by these factors.

A. Signal Model

Let $\mathbf{H}_U \in \mathbb{C}^{M\times N}$, $\mathbf{H}_D \in \mathbb{C}^{N\times M}$ be the uplink (UL) and downlink (DL) channels between BS and UE, respectively. In the UL, the signal after the receiving chain $\mathbf{y}_U$ from UE to BS is given by

$$\mathbf{y}_U = \mathbf{H}_U\mathbf{x}_U + \mathbf{z}_U, \tag{1}$$

where $\mathbf{x}_U = [x_1, x_2, \ldots, x_N]^T$ is the UL pilot signals sent by the UE, x_n represents the transmission signal of the n-th transmit antenna. The pilot signal received by the BS can be expressed as $\mathbf{y}_U = [y_1, y_2, \ldots, y_M]^T$, and y_m is the signal after the m-th receiving chain of the BS. $\mathbf{z}_U = [z_1, z_2, \ldots, z_M]^T$ is the additive white Gaussian noise (AWGN). As shown in Fig. 1, the equivalent channel from the UE to the BS can be modelled as $\mathbf{H}_U = \mathbf{R}_{BS}\tilde{\mathbf{H}}_U\mathbf{T}_{UE}$, where $\tilde{\mathbf{H}}_U$ is the real uplink wireless channel between UE and BS, $\mathbf{R}_{BS} = \mathrm{diag}(r_{BS,1}, \ldots, r_{BS,m})$ is the receiving chain RF impairment gain of BS, $\mathbf{T}_{UE} = \mathrm{diag}(t_{UE,1}, \ldots, t_{UE,n})$ is the transmitting chain RF impairment gain of UE. Similarly, $\mathbf{H}_D = \mathbf{R}_{UE}\tilde{\mathbf{H}}_D\mathbf{T}_{BS}$. Due to the reciprocity of channels in coherence time, the wireless channel $\tilde{\mathbf{H}}_U = \tilde{\mathbf{H}}_D^T$. This model of RF chain was proposed and verified in [13].

B. The Challenge of Traditional RFF Extraction

In existing MIMO communication systems, the effect of the channel on data transmission is generally eliminated by adding a precoding matrix at the transmitter side. For example, the UE sends a UL pilot signal and the BS can estimate the UL channel. BS utilizes the obtained CSI to generate a precoding matrix to eliminate the effect of the DL channel. However, due to the hardware mismatch, the equivalent channels of the UL and DL are not fully reciprocal. As a result, the CSI produced by the traditional method of channel estimation by delivering the UL pilot signal differs from the practical DL channel. The

disparity between the UL and DL channels increases with the severity of the hardware mismatch.

When using ZF precoding for UL transmissions, the achieved DL channel estimation result is given by $\widehat{\mathbf{H}}_D$, and the precoding matrix is given by

$$\begin{aligned}\mathbf{W}_{ZF} &= (\widehat{\mathbf{H}}_D^T)^H \left[\widehat{\mathbf{H}}_D^T (\widehat{\mathbf{H}}_D^T)^H\right]^{-1} \\ &= \widehat{\mathbf{H}}_D^* \left(\widehat{\mathbf{H}}_D^T \widehat{\mathbf{H}}_D^*\right)^{-1},\end{aligned} \tag{2}$$

and assume that $\mathbf{x}_U = \mathbf{W}_{ZF}\tilde{\mathbf{x}}_U$, where $\tilde{\mathbf{x}}_U$ is the original emitting symbol vector. Substituting $\mathbf{W}_{ZF}\tilde{\mathbf{x}}_U$ into (1) results in

$$\mathbf{y}_U = \mathbf{H}_U \mathbf{W}_{ZF} \tilde{\mathbf{x}}_U + \mathbf{z}_U. \tag{3}$$

Equation (3) can be expanded as

$$\begin{aligned}\mathbf{y}_U &= \mathbf{H}_U \widehat{\mathbf{H}}_D^* \left(\widehat{\mathbf{H}}_D^T \widehat{\mathbf{H}}_D^*\right)^{-1} \tilde{\mathbf{x}}_U + \mathbf{z}_U \\ &= \mathbf{R}_{BS} \tilde{\mathbf{H}}_U \mathbf{T}_{UE} \left[\mathbf{T}_{BS}^T \tilde{\mathbf{H}}_D^T \mathbf{R}_{UE}^T\right]^{-1} \tilde{\mathbf{x}}_U + \mathbf{z}_U.\end{aligned} \tag{4}$$

As can be seen from (4) that the precoding matrix cannot eliminate the effects of the channel because $\mathbf{R}_{BS}\tilde{\mathbf{H}}_U\mathbf{T}_{UE} \neq \mathbf{T}_{BS}^T\tilde{\mathbf{H}}_D^T\mathbf{R}_{UE}^T$. This is because different devices have different RF imperfections, which results in hardware mismatches. The UL and DL channels become non-reciprocal as a result.

Moreover, the RFF is coupled to the channel and is difficult to extract. Hence a partial calibration scheme can be introduced to eliminate redundant RF imperfections while retaining the RF imperfections of the device to be authenticated.

III. Multi-Antenna R-RFF based Device Authentication in Multipath Scenarios

The problem presented in the previous section is that using the traditional method to perfectly eliminate multipath channels is difficult, due to the channel non-reciprocity caused by the different RF chains. Inspired by [13], we propose a Multi-Antenna R-RFF method utilizing the RF imperfection relation between antenna chains to generate channel-robust RFF. As shown in Fig. 2, our approach consists of the training stage and the inference stage.

A. Training Stage

The training stage of the proposed scheme includes the generation of UE's and BS's R-RFF, preprocess of BS, and Support Vector Machine (SVM) training.

1) UE: We use the method in [13], where the reference antenna and the rest of the antennas send pilot signals to each other, to obtain the UE's relation matrix. The process of generating R-RFF from UE is shown in Algorithm 1. The UE selects the first antenna as the reference antenna. The reference antenna sends pilot signals to the remaining antennas, and the remaining antennas send pilot signals to the reference antenna during the coherence time. The UE estimates the channel on the two received signals separately. To determine the RF imperfection relation between the antennas, it divides the results of the channel estimation of the reference antenna and other antennas. The RF imperfection relation coefficient

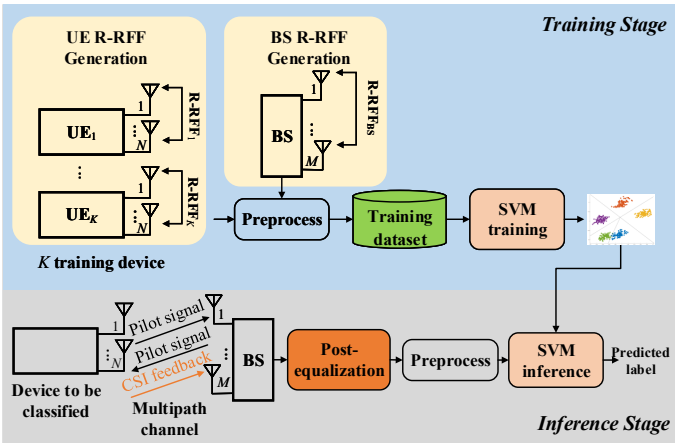

Fig. 2. System overview.

$c_{UE,n\to1}$ between the n-th antenna and the reference antenna is given by

$$c_{UE,n\to1} = \frac{\hat{h}_{UE,n\to1}}{\hat{h}_{UE,1\to n}} = \frac{r_{UE,1}t_{UE,n}}{r_{UE,n}t_{UE,1}} = \frac{c_{UE,n}}{c_{UE,1}}, \tag{5}$$

where, $\hat{h}_{UE,n\to1}$ represents the channel estimation result from the n-st antenna chain of UE to the 1-th antenna chain of UE, $\hat{h}_{UE,1\to n}$ represents the channel estimation result from the 1-th antenna chain of UE to the n-st antenna chain of UE in coherence time. The absolute imperfection of the reference antenna is $c_{UE,1} = \frac{t_{UE,1}}{r_{UE,1}}$ and the absolute imperfection of the n-th antenna is $c_{UE,n} = c_{UE,1}c_{UE,n\to1}$. We normalize the reference value of $c_{UE,1}$ as $c'_{UE,1} = 1$ and $\mathbf{C}_{UE} = \mathrm{diag}\left(c'_{UE,1}, c'_{UE,2}, \ldots, c'_{UE,N}\right)$. As the training stage can be done offline and in a secure environment, it is assumed each UE can send its R-RFF to BS securely.

Algorithm 1 The generation of UE's R-RFF

Input: The pilot signal $\mathbf{s}_{UE,1}, \ldots, \mathbf{s}_{UE,N}$
Output: The R-RFF of UE, $\mathbf{C}_{UE}$

for each $n \in [2, N]$ **do**
  1-st antenna sends pilot signal $\mathbf{s}_{UE,1}$;
  n-th antenna receives $\mathbf{y}_{UE,1\to n}$;
  UE estimates channel $\hat{h}_{UE,1\to n} = \mathbf{y}_{UE,1\to n}\left(\mathbf{s}_{UE,1}\right)^{\dagger}$;
  n-th antenna sends pilot signal $\mathbf{s}_{UE,n}$ in the coherence time;
  1-st antenna receives $\mathbf{y}_{UE,n\to1}$;
  UE estimates channel $\hat{h}_{UE,n\to1} = \mathbf{y}_{UE,n\to1}\left(\mathbf{s}_{UE,n}\right)^{\dagger}$;
  $c_{UE,n\to1} = \frac{\hat{h}_{UE,n\to1}}{\hat{h}_{UE,1\to n}}$;
  $c'_{UE,n} = c_{UE,n\to1}$;
end for
$c'_{UE,1} = 1$;
$\mathbf{C}_{UE} = \mathrm{diag}\left(c'_{UE,1}, c'_{UE,2}, \ldots, c'_{UE,N}\right)$;
return $\mathbf{C}_{UE}$;

2) BS: Similarly, the R-RFF at the BS can be generated and expressed as $\mathbf{C}_{BS} = \mathrm{diag}\left(c'_{BS,1}, c'_{BS,2}, \ldots, c'_{BS,M}\right)$. After

normalizing the R-RFF, we save $\mathbf{C}_{BS}$ into BS. Then we stitch the real and imaginary parts of the main diagonal of $N \times N$ $\mathbf{C}_{UE}$ into an array of $2N \times 1$ length. At this point, we have completed the generation of the R-RFF for the training stage.

We employ SVM for the training of the generated R-RFF. SVM is a kind of generalized linear classifier that can be used for the classification of data. Its decision boundary is the maximum margin hyperplane for learning samples. The core idea of classification learning is to find a partition hyperplane in the sample space based on the training set, and then classify different types of samples. We put the preprocessed array into the One-Against-One multiclass SVM model for training [15].

B. Inference Stage

The UE first sends a pilot signal to the BS, and BS sends a pilot signal to UE during the coherence time. Then the UE performs channel estimation and feeds the channel estimation result back to the BS. Next, BS makes the most of its own R-RFF and the obtained DL channel estimation result to eliminate the multipath channel and extract the R-RFF of the UE. The detailed CSI feedback and post-equalization algorithm is summarized in Algorithm 2.

1) Post-Equalization: Our detailed theoretical derivation of the post-equalization algorithm is as follows. We consider that the BS and the UE have generated their own R-RFF $\mathbf{C}_{BS}$ and $\mathbf{C}_{UE}$ individually. UE first sends the UL pilot signal $\mathbf{S}_U \in \mathbb{C}^{N\times L}$ to BS. BS obtains the UL received signal

$$\mathbf{Y}_U = \mathbf{H}_U \mathbf{S}_U + \mathbf{Z}_U, \tag{6}$$

where $\mathbf{Y}_U \in \mathbb{C}^{M\times L}$, $\mathbf{Z}_U \in \mathbb{C}^{M\times L}$ is AWGN, and L indicates the length of the pilot signal. UE perform channel estimation to obtain $\widehat{\mathbf{H}}_U = \mathbf{Y}_U \left(\mathbf{S}_U\right)^{\dagger}$.

During the coherence time, the BS sends the DL pilot signal $\mathbf{S}_D \in \mathbb{C}^{M\times L}$ to the UE. Similarly, the DL channel estimation can be expressed as $\widehat{\mathbf{H}}_D = \mathbf{Y}_D \left(\mathbf{S}_D\right)^{\dagger}$.

The UE feeds the DL channel estimation result $\widehat{\mathbf{H}}_D$ to the BS. After receiving $\widehat{\mathbf{H}}_D$, the BS transposes it and finds its pseudo-inverse matrix to transform it into the post-equalization matrix

$$\mathbf{W} = \left(\widehat{\mathbf{H}}_D^{*}\widehat{\mathbf{H}}_D^{T}\right)^{-1}\widehat{\mathbf{H}}_D^{*}. \tag{7}$$

The BS multiplies $\widehat{\mathbf{H}}_U$ by its own R-RFF $\mathbf{C}_{BS}$ and finally by the post-equalization matrix $\mathbf{W}$ to obtain

$$\begin{aligned}\mathbf{H}_{RSLT} &= \mathbf{W}\mathbf{C}_{BS}\widehat{\mathbf{H}}_U \\ &= \left(\widehat{\mathbf{H}}_D^{*}\widehat{\mathbf{H}}_D^{T}\right)^{-1}\widehat{\mathbf{H}}_D^{*}\mathbf{C}_{BS}\widehat{\mathbf{H}}_U,\end{aligned} \tag{8}$$

where, $\mathbf{H}_{RSLT}$ represents the Result of the post-equalization. Further expansion of $\widehat{\mathbf{H}}_D$ and $\widehat{\mathbf{H}}_U$ yields

$$\begin{aligned}\mathbf{H}_{RSLT} = &\left(\mathbf{R}_{UE}^{*}\widetilde{\mathbf{H}}_D^{*}\mathbf{T}_{BS}^{*}\left(\mathbf{R}_{UE}\widetilde{\mathbf{H}}_D\mathbf{T}_{BS}\right)^{T}\right)^{-1} \\ &\left(\mathbf{R}_{UE}^{*}\widetilde{\mathbf{H}}_D^{*}\mathbf{T}_{BS}^{*}\right)\mathbf{C}_{BS}\left(\mathbf{R}_{BS}\widetilde{\mathbf{H}}_U\mathbf{T}_{UE}\right) \\ = &\left(\mathbf{T}_{BS}^{T}\widetilde{\mathbf{H}}_D^{T}\mathbf{R}_{UE}^{T}\right)^{-1}\mathbf{C}_{BS}\left(\mathbf{R}_{BS}\widetilde{\mathbf{H}}_U\mathbf{T}_{UE}\right).\end{aligned} \tag{9}$$

Since $\mathbf{T}_{BS}$ and $\mathbf{R}_{BS}$ are diagonal arrays, $\mathbf{C}_{BS}$ can be written in the form of the product of $\mathbf{T}_{BS}$ and $\mathbf{R}_{BS}^{-1}$

$$\begin{aligned}\mathbf{C}_{BS} &= \operatorname{diag}\left(1, c'_{BS,2}, \ldots, c'_{BS,M}\right) \\ &= \frac{1}{c_{BS,1}}\boldsymbol{diag}\left(c_{BS,1}, c_{BS,2}, \ldots, c_{BS,M}\right) \\ &= \frac{1}{c_{BS,1}}\mathbf{T}_{BS}\mathbf{R}_{BS}^{-1}.\end{aligned} \tag{10}$$

Substituting (10) into (9) yields

$$\mathbf{H}_{RSLT} = \frac{1}{c_{BS,1}}\left(\mathbf{T}_{BS}^{T}\widetilde{\mathbf{H}}_D^{T}\mathbf{R}_{UE}^{T}\right)^{-1}\mathbf{T}_{BS}\mathbf{R}_{BS}^{-1}\mathbf{R}_{BS}\widetilde{\mathbf{H}}_U\mathbf{T}_{UE}. \tag{11}$$

Since $\mathbf{T}_{BS}$ is a diagonal array, $\mathbf{T}_{BS}^{T} = \mathbf{T}_{BS}$. Meanwhile, the UL and DL channels are reciprocal in the coherence time, which means $\widetilde{\mathbf{H}}_D^{T} = \widetilde{\mathbf{H}}_U$. Therefore (11) can be written as

$$\begin{aligned}\mathbf{H}_{RSLT} &= \frac{1}{c_{BS,1}}\left(\mathbf{T}_{BS}^{T}\widetilde{\mathbf{H}}_D^{T}\mathbf{R}_{UE}^{T}\right)^{-1}\left(\mathbf{T}_{BS}^{T}\widetilde{\mathbf{H}}_D^{T}\right)\mathbf{T}_{UE} \\ &= \frac{1}{c_{BS,1}}\left(\mathbf{R}_{UE}^{T}\right)^{-1}\mathbf{T}_{UE}.\end{aligned} \tag{12}$$

Since $\mathbf{R}_{UE}$ and $\mathbf{T}_{UE}$ are diagonal arrays,

$$\left(\mathbf{R}_{UE}^{T}\right)^{-1}\mathbf{T}_{UE} = \mathbf{T}_{UE}\mathbf{R}_{UE}^{-1} = c_{UE,1}\mathbf{C}_{UE}. \tag{13}$$

Substituting (13) into (12) yields

$$\mathbf{H}_{RSLT} = \frac{c_{UE,1}}{c_{BS,1}}\mathbf{C}_{UE}. \tag{14}$$

The equation (14) is the feature obtained after reception and post-equalization at the BS. We normalize the first value of $\mathbf{H}_{RSLT}$, the value corresponding to the reference antenna, to obtain the R-RFF $\mathbf{C}_{UE}$ of the UE.

Algorithm 2 CSI Feedback and Post-Equalization

Input: $\mathbf{C}_{BS}$, $\mathbf{S}_D$, $\mathbf{S}_U$
Output: The R-RFF of UE, $\mathbf{C}_{UE}$

UE sends UL pilot signal $\mathbf{S}_U$;
BS receives $\mathbf{Y}_U$;
BS estimates channel $\widehat{\mathbf{H}}_U = \mathbf{Y}_U \left(\mathbf{S}_U\right)^{\dagger}$;
BS sends DL pilot signal $\mathbf{S}_D$ in the coherence time;
UE receives $\mathbf{Y}_D$;
UE estimates channel $\widehat{\mathbf{H}}_D = \mathbf{Y}_D \left(\mathbf{S}_D\right)^{\dagger}$;
UE sends $\widehat{\mathbf{H}}_D$ to BS;
$\mathbf{W} = \left(\widehat{\mathbf{H}}_D^{*}\widehat{\mathbf{H}}_D^{T}\right)^{-1}\widehat{\mathbf{H}}_D^{*}$;
$\mathbf{H}_{RSLT} = \mathbf{W}\mathbf{C}_{BS}\widehat{\mathbf{H}}_U$;
for each $n \in [2, N]$ **do**
    $\mathbf{C}_{UE}(n,n) = \mathbf{H}_{RSLT}(n,n)/\mathbf{H}_{RSLT}(1,1)$;
end for
$\mathbf{C}_{UE}(1,1) = 1$;
return $\mathbf{C}_{UE}$;

According to (14), we have theoretically succeeded in eliminating the effects of the multipath channel. At the same time, we eliminate the effects of the BS imperfections $\mathbf{C}_{BS}$, leaving only the imperfections $\mathbf{C}_{UE}$ of the UE for authentication.

2) SVM Inference: The BS puts the extracted R-RFF into the trained SVM model for inference to determine the UE identity. The predicted label will be compared with the label of the device under test to evaluate the performance of the R-RFF scheme.

IV. Numerical Results

In this section, we evaluate the performance of our proposed R-RFF in terms of classification and multipath channel resistance via Matlab simulations.

A. Simulation Setup

We use MATLAB 5G NR Toolbox to simulate 30 virtual radios, where the UL employs Sounding Reference Signal (SRS) and the DL employs CSI - Reference Signal (CSI-RS) as the pilot signal. For each device, we collected 100 frames for training in the training stage at 30 dB SNR and 900 frames under the SNR from -10 dB to 30 dB in the inference stage. One-Against-One multiclass SVM is used here to train and test the data. In the benchmark, we feed the IQ data received from the UE directly into the same SVM for classification training and inference.

1) Transmitter: The BS is assumed to have 32 antennas and the different UEs are assumed to have 2 or 4 antennas. Both the antennas of BS and UEs are assumed to be fixed antennas similar to [13]. We configure each RF chain of the BS and UEs with different IQ imbalances and wideband PA nonlinearities. The hardware chains of all antennas for the same device have the same CFO and CPO, because different RF front-ends often share the common oscillator in commercial transmitters. We set the ranges of gain and phase imbalances as [-1 1] dB and [-5 5] degrees, respectively [16]. We use the NXP Airfast LDMOS Doherty PA provided in the MATLAB Communications Toolbox named Power Amplifier Characterization. The generalized memory polynomial (GMP) model of PA was used to import PA nonlinearities. We measured PA input and output data to model the PA. The memory length and the polynomial degree are both set to 5. Each parameter in polynomial coefficients of the PA nonlinearity was varied within $\pm 5\%$ of the measured values [17].

2) Channel: AWGN channel, 2-path channel, and Tapped Delay Line (TDL) channel in 3GPP TR 38.901 [14] are adopted for simulation. The 2-path channel has 2 delay paths, whose delays are set to [0 30e-9] s, and the average path gains are set to [-3 -5] dB. TDL-C channel is an NLOS channel with 24 paths, which is specified in the 3GPP protocol. In the simulation of the wideband multipath environment, the delay spread is set to 10e-9 s, and the maximum Doppler shift is set to 10 Hz. The carrier frequency f_c is set to 3.072 GHz, subcarrier spacing is set to 15 kHz, the bandwidth B is set to 15 MHz, and 948 subcarriers are implemented.

B. Simulation Results

As shown in Fig. 3, the recognition accuracy of the R-RFF scheme under the TDL-C channel can reach 97.8% when the number of UEs is less than twenty and the SNR is greater than 15 dB, and it can also maintain above 91.4% at 5 dB. As the number of UEs increases, the recognition accuracy decreases. When the number of UEs is 30, and SNR is above 10 dB, the recognition accuracy of 30 UEs can be more than 93.9%, proving that the proposed R-RFF method works well for the classification of 30 or fewer UEs at four antennas.

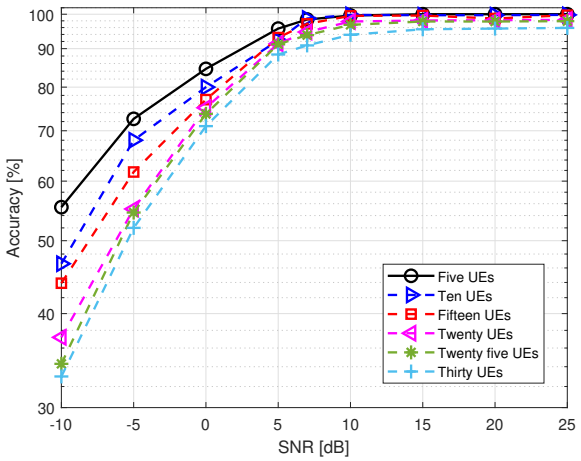

Fig. 3. Recognition accuracy of the different number of UEs when the number of antennas is four.

Fig. 4 presents the recognition accuracy of UEs with different numbers of antennas. It can be seen that the recognition accuracy at four antennas is higher than that at two antennas since the proposed R-RFF scheme relies on the imperfection relation between the antenna chains of the devices. One of the antennas of a two-antenna device is used as the reference antenna, i.e. only the imperfection relation of one antenna can be used as a feature for classification, leading to the poor classification of the two-antenna device. But it also indicates that this scheme which relies on the inter-antenna relation will become more and more effective in the future as the number of antennas of the UEs increases.

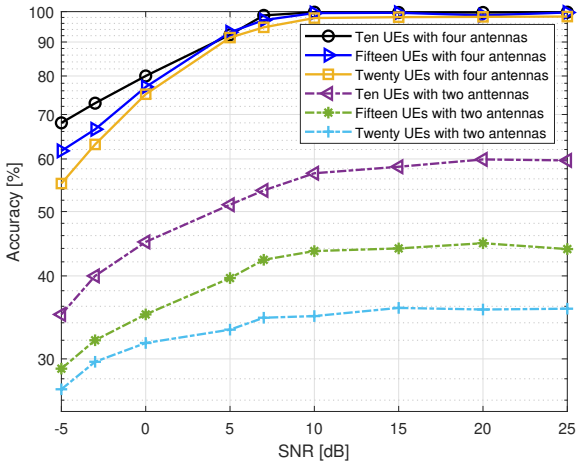

Fig. 4. Recognition accuracy of the different number of antennas.

The recognition accuracy of UEs with different numbers of paths is given in Fig. 5. It can be seen that the accuracy of the benchmark is 87.2% with the AWGN channel, 58.7% with the 2-path channel, and 51.3% with the TDL-C channel when the SNR is 25 dB. It illustrates the lack of robustness of the Benchmark in multipath scenarios. In contrast, despite the number of paths of channels, the proposed R-RFF method yields an accuracy of 97.8% at 10 dB. Hence, the robustness of the R-RFF method in multipath channels is verified in the simulation.

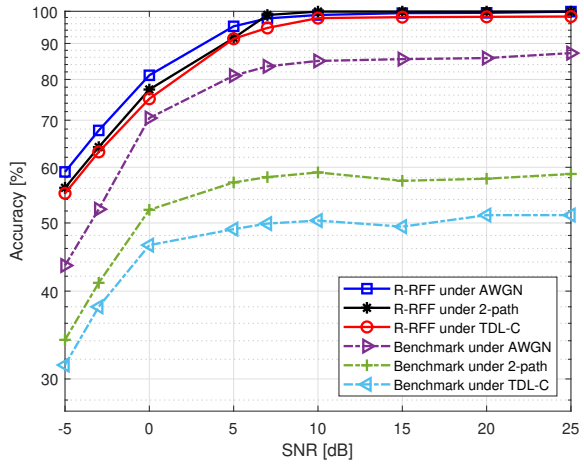

Fig. 5. Classification results on different methods when the number of antennas is four.

V. Conclusion

This paper proposed an antenna relation based RFF approach to address the two bottleneck problems of RFF authentication in the multi-antenna system, i.e., multipath channels and imperfect channel reciprocity. By echoing the channels, precoding can eliminate the ideal multipath channels. However, the imperfect channel reciprocity makes the elimination of multipath channels unfeasible. To overcome this deficiency, we proposed a new R-RFF scheme that utilizes CSI feedback to counteract the multipath channel perfectly. By establishing the RF imperfection relation between the antenna chains of a multi-antenna device, we extracted a stable R-RFF, which could eliminate the non-reciprocal part of the UL and DL channels. Besides, it is derived that post-equalization of the BS's R-RFF could preserve the RFF of the device under test while eliminating the non-reciprocal portion of the channels during UE authentication. The simulation results showed that the proposed R-RFF scheme can authenticate RFF effectively in multipath propagation scenarios in a TDD multi-antenna system.

Acknowledgment

This work was supported in part by the National Key R&D Program of China under Grant 2022YFB2902202, in part by the National Natural Science Foundation of China under Grant 62171121, in part by the Natural Science Foundation of Jiangsu Province under Grant BK20211160 and in part by Jiangsu Provincial Key Laboratory of Network and Information Security under Grant BM2003201. The work of Y. Xing was supported by the Research Foundation for Advanced Talents, Nanjing University of Posts and Telecommunications under Grant XK0160921022. The work of J. Zhang was in part supported by the UK EPSRC under grant ID EP/V027697/1.

References

[1] K. L. Lueth, "State of the IoT 2020: 12 billion IoT connections, surpassing non-IoT for the first time," accessed: Nov. 19, 2020. [Online]. Available: https://iot-analytics.com/state-of-the-iot-2020-12-billion-iot-connections-surpassing-non-iot-for-the-first-time/.

[2] M. Iwamoto, K. Ohta, and J. Shikata, "Security formalizations and their relationships for encryption and key agreement in information-theoretic cryptography," *IEEE Trans. Inf. Theory*, vol. 64, no. 1, pp. 654–685, Jan. 2017.

[3] A. Nooraiepour, W. U. Bajwa, and N. B. Mandayam, "Learning-aided physical layer attacks against multicarrier communications in IoT," *IEEE Trans. Cognit. Commun. Netw.*, vol. 7, no. 1, pp. 239–254, Mar. 2020.

[4] 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.

[5] L. Jiao, N. Wang, P. Wang, A. Alipour-Fanid, J. Tang, and K. Zeng, "Physical layer key generation in 5G wireless networks," *IEEE Wireless Commun.*, vol. 26, no. 5, pp. 48–54, Oct. 2019.

[6] 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, 2019.

[7] 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 INFOCOM*, Toronto, Canada, Jul. 2020, pp. 646–655.

[8] L. N. Kandel, Z. Zhang, and S. Yu, "Exploiting CSI-MIMO for accurate and efficient device identification," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, HI, USA, Dec. 2019, pp. 1–6.

[9] M. Fadul, D. Reising, T. D. Loveless, and A. Ofoli, "Nelder-mead simplex channel estimation for the RF-DNA fingerprinting of OFDM transmitters under rayleigh fading conditions," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 2381–2396, Jan. 2021.

[10] 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.

[11] 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. MOBIHOC*, Catania, Italy, Jul. 2019, pp. 51–60.

[12] 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.

[13] C. Shepard, H. Yu, N. Anand, E. Li, T. Marzetta, R. Yang, and L. Zhong, "Argos: Practical many-antenna base stations," in *Proc. ACM MOBICOM*, Aug. 2012, pp. 53–64.

[14] 3GPP, "Study on channel model for frequencies from 0.5 to 100 GHz," 3rd Generation Partnership Project (3GPP), Technical Report (TR) 38.901, 2019, version 16.0.0.

[15] C.-W. Hsu and C.-J. Lin, "A comparison of methods for multiclass support vector machines," *IEEE Trans. Neural Netw.*, vol. 13, no. 2, pp. 415–425, Mar. 2002.

[16] 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.

[17] D. R. Morgan, Z. Ma, J. Kim, M. G. Zierdt, and J. Pastalan, "A generalized memory polynomial model for digital predistortion of RF power amplifiers," *IEEE Trans. Signal Process.*, vol. 54, no. 10, pp. 3852–3860, Oct. 2006.