Location-Invariant Radio Frequency Fingerprint for Base Station Recognition

Yilun Sun, Guyue Li, *Member, IEEE*, Hongyi Luo, Yuexiu Xing, Shuping Dang, *Member, IEEE* and Aiqun Hu, *Senior Member, IEEE*

***Abstract*—Pseudo base station (BS) is an illegal radio device that exploits the security vulnerabilities of fifth generation (5G) communications and then implements corresponding network attacks, such as spoofing attack. These malicious actions cause security and privacy threats and hinder the wide deployment of wireless access networks. To address these problems, efficient BS identification mechanisms are necessary. Radio frequency fingerprinting (RFF) and channel fingerprinting are potential solutions. Unfortunately, existing solutions are limited to be applicable to scenarios where the locations of pseudo BSs are fixed, while the emerging challenges brought by movable pseudo BSs can hardly be addressed by mature wireless security mechanisms. In this letter, we propose a signal echoing protocol (SEP) to reduce the influence on wireless channels and construct the location-invariant RFF. When BS and user equipment (UE) communicate using SEP, UE can accurately estimate the channel to recognize different BSs. Numerical results demonstrate that the proposed scheme can reach a high classification accuracy for ten BSs, by 95.2% at the signal-noise ratio (SNR) of 25 dB.**

***Index Terms*—MIMO system, hardware mismatch, RF fingerprint, location-invariant identification, physical-layer security.**

I. Introduction

In the era of fifth generation (5G) communications and beyond, wireless technology plays a key role in our everyday life [1]. However, the broadcast nature of wireless transmission makes device authentication challenging [2]. In particular, the spoofing attack caused by pseudo base station (BS) seriously disrupts the management of legitimate wireless application systems and threatens the security of users' digital properties, e.g., personal data [3], [4]. This phenomenon is becoming increasingly serious with the rapid growth of the Internet of Things (IoT) devices, which are of relative simple structures and less computational capability.

Accordingly, efficient device authentication mechanisms are required for enhancing the security of wireless networks, especially those lightweight networks, radio frequency fingerprint identification (RFFI) is a promising technique to classify the identities of wireless devices [5]. The hardware part of the transmitting equipment and the receiving equipment has unique defects which can be used to identify the equipment on account of the uniqueness and robustness of radio frequency fingerprint (RFF) [6]. In addition, RFF of each device is also hard to tamper with [7]. So far, the research scope of the RFFI technology mainly covers ZigBee, LoRa, and Bluetooth. Applications of RFFI in the area of pseudo BS recognition are in progress.

Existing algorithms rely on received signal strength indicator (RSSI) and dynamic RFF to recognize pseudo BS [8]. These existing algorithms can provide the visual interface of a signal map with good user interaction. Nevertheless, the effectiveness of these algorithms depends on the location of the mobile terminal, and these algorithms are also sensitive to channel interference in practical application scenarios. In terms of overcoming the effect of location, researchers have conducted extensive research in recent years, and two main schemes are proposed. One of both is to collect the measured data in different locations as the training data and design a classifier with the help of the multi-channel convolutional neural network (MCCNN) [2]. The other is to extract a differential constellation trace figure (DCTF) from the collected samples in different locations, and the DCTF is analyzed by image recognition algorithms [9]. However, the above methods have some limitations. For example, it is impossible to collect data in an extensive and ubiquitous manner. Therefore, it is not suitable for wireless applications with the requirement of high precision.

In this regard, we utilize the relative hardware mismatch (HM) relation of different antennas in multiple-input multiple-output (MIMO) communication systems as key the feature of each BS. As MIMO becoming a promising paradigm in 5G networks, a typical BS usually has 64 or more antennas and can thus provide more dimensions of features for RFF. The increase of the number of antennas opens up new possibilities for further research. Making the most of an increasing number of antennas, this letter proposes a novel signal echoing protocol

This work was supported in part by the National Key R&D Program of China (No. 2022YFB2902202); in part by the National Natural Science Foundation of China (No. U22A2001, 62171121); in part by the National Natural Science Foundation of Jiangsu Province, China (No. BK20211160); in part by the Research Foundation for Advanced Talents, Nanjing University of Posts and Telecommunications (No. XK0160921022).

Yilun Sun and Hongyi Luo are with the School of Cyber Science and Engineering, Southeast University, Nanjing 210096, China (e-mail: sunyilun@seu.edu.cn; hongyiluo@seu.edu.cn).

Guyue Li (*corresponding author*) is with the School of Cyber Science and Engineering, Southeast University, Nanjing 210096, China, also with Purple Mountain Laboratories for Network and Communication Security, Nanjing 211111, China, and also with the Jiangsu Provincial Key Laboratory of Computer Network Technology, Nanjing 210096, China (e-mail: guyuelee@seu.edu.cn).

Yuexiu Xing is with the School of Internet of Things, Nanjing University of Posts and Telecommunications, Nanjing 210003, China. (e-mail: yxxing@njupt.edu.cn).

Shuping Dang is with the Department of Electrical and Electronic Engineering, University of Bristol, Bristol BS8 1UB, U.K. (e-mail: shuping.dang@bristol.ac.uk).

Aiqun Hu is with the School of Information Science and Engineering, Southeast University, Nanjing 210096, China, also with Purple Mountain Laboratories for Network and Communication Security, Nanjing 211111, China, and also with the Jiangsu Provincial Key Laboratory of Computer Network Technology, Nanjing 210096, China (e-mail: aqhu@seu.edu.cn).

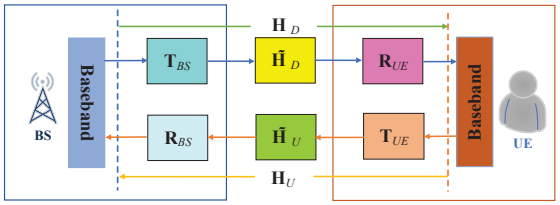


Fig. 1. System model considered in this letter.

(SEP) to eliminate the interference of wireless channels and constructs a location-invariant RFF. The main contributions of this letter are summarized as follows:

- We utilize the correlation among antennas of each BS and establish the RFF using the defective relation among multiple antennas.
- We propose a protocol called SEP to recognize a particular BS. It can eliminate the effect of wireless channels on the identification problem and realize a location-invariant RFF.
- We establish a simulation model jointly considering both transmitter and receiver HM. Numerical results show that the recognition accuracy of ten BSs is up to 95.2% at the SNR of 25 dB.

II. System Model

In this letter, we consider a MIMO communication system that consists of a BS with M antennas and a user equipment (UE) with N antennas, assuming $M > N$ that is in line with most realistic wireless applications. Both the channel and signal models are detailed in the sequel.

A. Channel Model

As shown in Fig. 1, denoting the wireless transmission channel matrices of uplink (UL) and downlink (DL) as $\tilde{\mathbf{H}}_U$ and $\tilde{\mathbf{H}}_D$, the overall channel matrices of UL and DL are $\mathbf{H}_U$ and $\mathbf{H}_D$, which signify the HM of the transmitter, wireless channel, and the HM of the receiver. According to [10], in time division duplexing (TDD) pattern, $\tilde{\mathbf{H}}_U = \tilde{\mathbf{H}}_D^T = \mathbf{H}$ and $\mathbf{H} \in \mathbb{C}^{M\times N}$, the elements in matrix $\mathbf{H}$ are Rayleigh distributed. The overall channels in the considered MIMO communication system can be expressed in the matrix form as

$$\mathbf{H}_U = \mathbf{R}_{BS}\mathbf{H}\mathbf{T}_{UE}, \tag{1}$$

and

$$\mathbf{H}_D = \mathbf{R}_{UE}\mathbf{H}^T\mathbf{T}_{BS}, \tag{2}$$

where $\mathbf{R}_{BS}$ and $\mathbf{R}_{UE}$ represent the receive hardware gain matrices of BS and UE, respectively; $\mathbf{T}_{BS}$ and $\mathbf{T}_{UE}$ represent the transmit hardware gain matrices of BS and UE, respectively. In reality, the environment factors, such as temperature and random phase variations of phase-locked loop (PLL), have little influence on RFF in steady state [11], [12]. The model in our letter applies for the steady-state environments, in which, the robustness of RFF suffers little from environment factors. For simplicity, all the effects of hardware impairments are thus considered to be linear [13]:

$$\begin{aligned}
\mathbf{R}_{BS} &= \mathrm{diag}(r_{BS,1},...,r_{BS,M}),\\
\mathbf{R}_{UE} &= \mathrm{diag}(r_{UE,1},...,r_{UE,N}),\\
\mathbf{T}_{BS} &= \mathrm{diag}(t_{BS,1},...,t_{BS,M}),\\
\mathbf{T}_{UE} &= \mathrm{diag}(t_{UE,1},...,t_{UE,N}).
\end{aligned} \tag{3}$$

UL and DL channels between the mth antenna of the BS and the nth antenna of the UE can be expressed as

$$\begin{aligned}
h_{U,n\to m} &= r_{BS,m}h_u t_{UE,n},\\
h_{D,m\to n} &= r_{UE,n}h_d t_{BS,m},
\end{aligned} \tag{4}$$

where h_u and h_d represent the wireless channel gains between the mth antenna and the nth antenna in the UL and DL, respectively; assuming the channel reciprocity, we have $h_u = h_d$. Different antennas usually have different levels of HM, and therefore, $t_{BS,m}$, $r_{BS,m}$, $t_{UE,n}$, and $r_{UE,n}$ are unequal to each other.

B. Signal Model

In the SEP proposed in this letter, we need to echo the received signal by establishing the signal transmission model between the UL and DL. Let UE send the UL signal vector $\mathbf{S}_U = [s_{U1},...,s_{UN}]^T$ and BS send the DL signal vector $\mathbf{S}_D = [s_{D1},...,s_{DM}]^T$. The UL and DL signal models can thus be expressed as:

$$\begin{aligned}
\mathbf{Y}_U &= \mathbf{H}_U\mathbf{S}_U + \mathbf{Z}_U,\\
\mathbf{Y}_D &= \mathbf{H}_D\mathbf{S}_D + \mathbf{Z}_D,
\end{aligned} \tag{5}$$

where $\mathbf{Y}_D = [y_{D1},...,y_{DN}]^T$ is the received signal vector of UE, and $\mathbf{Y}_U = [y_{U1},...,y_{UM}]^T$ is the received signal vector of BS; $\mathbf{Z}_D = [z_{D1},...,z_{DN}]^T$ and $\mathbf{Z}_U = [z_{U1},...,z_{UM}]^T$ are the additive Gaussian noise vectors, z_{Um} and $z_{Dn} \sim \mathcal{CN}(0,\sigma_n^2)$, where σ_n^2 is the average noise power at the nth antenna.

C. Classifier

We use K-nearest neighbor (KNN) as a classifier, that determines which category the data belongs to based on the category of its nearest K points. The classification decision rule by KNN is majority voting, which is equivalent to the empirical risk minimization. KNN also enables high precision and excellent classification capability, making it suitable for RFFI.

III. Design of Signal Echoing Protocol

In this section, we propose a method to obtain the relative feature among antennas and review the scheme proposed in [13], through which, we finally construct a location-invariant RFF.

A. Relative Defects among Multiple Antennas

The absolute RFF is not always possible to obtain. Therefore, by design, an accurate RFF should not become the prerequisite for accurate BS identification. To this end, we propose an algorithm to obtain the relative RFF, which is also sufficient to characterize the identity of BS, and the model is shown in Fig. 2. This kind of self transmission and reception

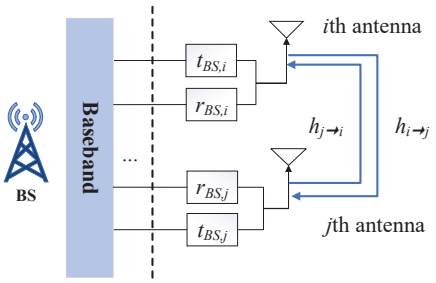


Fig. 2. Self transmission and reception model.

model was first proposed in [14], and the author also built up a hardware system based on this. We were inspired by it and then proposed our algorithm to obtain the relative RFF. The bidirectional channels between the ith antenna of BS and the jth antenna of BS are given by

$$\begin{aligned}\tilde{h}_{j\to i} &= r_{BS,i}h_{i\to j}t_{BS,j},\\ \tilde{h}_{i\to j} &= r_{BS,j}h_{j\to i}t_{BS,i},\end{aligned} \tag{6}$$

where $h_{i\to j} = h_{j\to i}$ because of channel reciprocity. The first antenna is chosen to be the reference antenna. Here, we introduce defect matrix

$$\mathbf{C}_{BS} = \mathbf{T}_{BS}\mathbf{R}_{BS}^{-1}, \tag{7}$$

where

$$\mathbf{C}_{BS} = \mathrm{diag}(c_{BS,1}, ..., c_{BS,M}), \tag{8}$$

$$c_{BS,m} = \frac{t_{BS,m}}{r_{BS,m}}, \tag{9}$$

and $c_{BS,m}$ represents the unique defect of the mth antenna.

According to (6), the bidirectional channels between the first antenna and the mth antenna ($m \neq 1$) can be represented as

$$\begin{aligned}\tilde{h}_{1\to m} &= r_{BS,m}h_{1\to m}t_{BS,1},\\ \tilde{h}_{m\to 1} &= r_{BS,1}h_{m\to 1}t_{BS,m}.\end{aligned} \tag{10}$$

Channel estimation is performed for the signal received by each antenna to obtain $\hat{h}_{1\to m}$ and $\hat{h}_{m\to 1}$. We define

$$c_{BS,m\to 1} = \frac{\hat{h}_{m\to 1}}{\hat{h}_{1\to m}} = \frac{t_{BS,m}r_{BS,1}}{r_{BS,m}t_{BS,1}} = \frac{c_{BS,m}}{c_{BS,1}}, \tag{11}$$

and normalize the defect of the first antenna to be 1, i.e., $c_{BS,1} = 1$; Then, the relative defect of the mth antenna is $c'_{BS,m} = c_{BS,m\to 1}$, leading to

$$\mathbf{C}'_{BS} = \mathrm{diag}(1, c'_{BS,2}, ..., c'_{BS,M}) = \frac{1}{c_{BS,1}}\mathbf{C}_{BS} \tag{12}$$

that consists of $c'_{BS,m}$ and can also be seen as a relative defect feature of this BS. Similarly, the relative defect feature of UE $\mathbf{C}'_{UE}$ can be obtained and written as:

$$\mathbf{C}_{UE} = \mathbf{T}_{UE}\mathbf{R}_{UE}^{-1}, \tag{13}$$

and

$$\mathbf{C}'_{UE} = \mathrm{diag}(1, c'_{UE,2}, ..., c'_{UE,N}) = \frac{1}{c_{UE,1}}\mathbf{C}_{UE}. \tag{14}$$

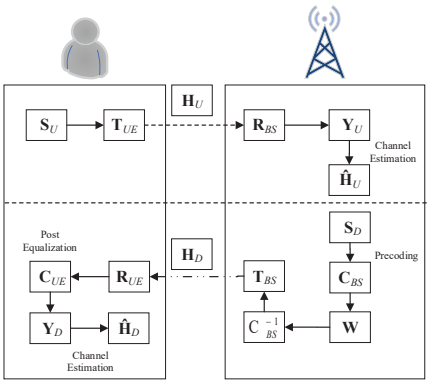


Fig. 3. Process of SEP proposed in this letter.

B. Design of SEP

According to the scheme introduced above, the defect matrix of BS $\mathbf{C}'_{BS}$ can be obtained, which can be utilized before and after the precoding process. The zero-forcing (ZF) precoding scheme is helpful to eliminate the effect of wireless channel matrix $\mathbf{H}$. ZF precoding method uses the transpose of UL channel estimation $\hat{\mathbf{H}}_U^T$, which can be expressed as

$$\mathbf{W} = (\hat{\mathbf{H}}_U^T)^H[\hat{\mathbf{H}}_U^T(\hat{\mathbf{H}}_U^T)^H]^{-1} = \hat{\mathbf{H}}_U^*(\hat{\mathbf{H}}_U^T\hat{\mathbf{H}}_U^*)^{-1}. \tag{15}$$

Substituting (15) into (5):

$$\begin{aligned}\mathbf{Y}_D =& \mathbf{H}_D\hat{\mathbf{H}}_U^*(\hat{\mathbf{H}}_U^T\hat{\mathbf{H}}_U^*)^{-1}\mathbf{S}_D + \mathbf{Z}_D\\ =& (\mathbf{R}_{UE}\mathbf{H}^T\mathbf{T}_{BS})(\mathbf{R}_{BS}^*\mathbf{H}^*\mathbf{T}_{UE}^*)\\ & [(\mathbf{T}_{UE}^T\mathbf{H}^T\mathbf{R}_{BS}^T)(\mathbf{R}_{BS}^*\mathbf{H}^*\mathbf{T}_{UE}^*)]^{-1}\mathbf{S}_D + \mathbf{Z}_D.\end{aligned} \tag{16}$$

where $\mathbf{T}_{UE}$ and $\mathbf{R}_{BS}^T$ can be extracted from $[(\mathbf{T}_{UE}^T\mathbf{H}^T\mathbf{R}_{BS}^T)(\mathbf{R}_{BS}^*\mathbf{H}^*\mathbf{T}_{UE}^*)]^{-1}$ because they are diagonal matrices. In this way, (16) can be further simplified as:

$$\begin{aligned}\mathbf{Y}_D =& (\mathbf{R}_{UE}\mathbf{H}^T\mathbf{T}_{BS})(\mathbf{R}_{BS}^*\mathbf{H}^*)\\ & [(\mathbf{H}^T\mathbf{R}_{BS})(\mathbf{R}_{BS}^*\mathbf{H}^*)]^{-1}\mathbf{T}_{UE}^{-1}\mathbf{S}_D + \mathbf{Z}_D.\end{aligned} \tag{17}$$

From the above, we find that the wireless channel matrix $\mathbf{H}$ still exists, which degrades the robustness of RFF. To address this problem, an equalization method called the full equalization proposed in [13] can be used to process the received signal. The following proposition is proposed and proven to justify the use of full equalization:

Proposition: Given $\mathbf{C}_{UE}$ and $\mathbf{C}_{BS}$, the ZF precoding can be tailored and performed to eliminate the effects of wireless channels and HM feature, by which the signals transmitted from the BS can be received at the UE with a higher level of fidelity.

Proof: Please refer to Appendix.

However, while eliminating the BS feature together with the wireless channel, the ZF precoding also brings difficulty in device recognition and can hardly be directly applied to the communication system considered in the letter. We propose SEP whose process can be summarized in Fig. 3. The normal precoding process can hardly eliminate the effect of wireless channels and leave the RFF of BS because of the HM. Therefore, in SEP, the precoding process is designed as

$$\mathbf{W}_{cal} = \mathbf{C}_{BS}'^{-1}\mathbf{W}\mathbf{A}'_{BS}, \tag{18}$$

where $\mathbf{A}'_{BS} \in \mathbb{C}^{N\times(M/N)}$ and $\mathbf{A}'_{BS}$ consist of elements in $\mathbf{C}'_{BS}$, $\mathbf{A}'_{BS} = \frac{1}{c_{BS,1}}\mathbf{A}_{BS}$. The signal received by UE is thus given by

$$\begin{aligned}\mathbf{Y}_D =&\mathbf{H}_D\mathbf{W}_{cal}\mathbf{S}_D + \mathbf{Z}_D\\ =&\frac{c_{BS,1}}{c_{BS,1}}(\mathbf{R}_{UE}\mathbf{H}^T\mathbf{T}_{BS})(\mathbf{R}_{BS}\mathbf{T}_{BS}^{-1})(\mathbf{R}_{BS}^*\mathbf{H}^*\mathbf{T}_{UE}^*)\\ &[(\mathbf{T}_{UE}\mathbf{H}^T\mathbf{R}_{BS})(\mathbf{R}_{BS}^*\mathbf{H}^*\mathbf{T}_{UE}^*)]^{-1}\mathbf{A}_{BS}\mathbf{S}_D + \mathbf{Z}_D\\ =&\mathbf{R}_{UE}(\mathbf{H}^T\mathbf{R}_{BS}\mathbf{R}_{BS}^*\mathbf{H}^*)(\mathbf{H}^T\mathbf{R}_{BS}\mathbf{R}_{BS}^*\mathbf{H}^*)^{-1}\\ &\mathbf{T}_{UE}^{-1}\mathbf{A}_{BS}\mathbf{S}_D + \mathbf{Z}_D\\ =&\mathbf{R}_{UE}\mathbf{T}_{UE}^{-1}\mathbf{A}_{BS}\mathbf{S}_D + \mathbf{Z}_D.\end{aligned} \tag{19}$$

After receiving the signal, UE conducts the post equalization process with the defect matrix of UE obtained by $\mathbf{C}'_{UE} = \frac{1}{c_{UE,1}}\mathbf{T}_{UE}\mathbf{R}_{UE}^{-1}$, by which the equalization scheme is carried out as:

$$\begin{aligned}\mathbf{Y}_D =&\mathbf{C}'_{UE}\mathbf{R}_{UE}\mathbf{T}_{UE}^{-1}\mathbf{A}'_{BS}\mathbf{S}_D + \mathbf{C}'_{UE}\mathbf{Z}_D\\ =&\frac{1}{c_{UE,1}}\mathbf{A}'_{BS}\mathbf{S}_D + \mathbf{C}'_{UE}\mathbf{Z}_D.\end{aligned} \tag{20}$$

In this way, channel estimation is performed by UE to obtain the feature matrix of the BS, which can be utilized to identify different BSs.

IV. Numerical Results and Discussion

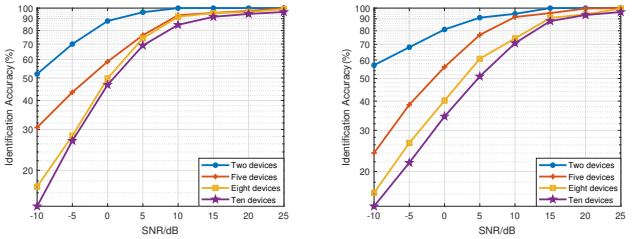
In this section, the simulations are performed to evaluate the performance of the proposed SEP. The simulation parameters are set as follows: the system consists of one UE and ten BSs, among which the UE is configured with 4 antennas, and each BS is configured with 32 antennas.

The configurations of simulation are given as follows: Each BS/UE device is simulated by adding a set of different RFF features where the frequency offset of each antenna ranges from 2 kHz to 4 kHz; the phase noise level distributes over the range of -80 dB $\sim$ -100 dB randomly; the I/Q gain imbalance and I/Q phase mismatch are randomly over the range of 0.9 $\sim$ 1 and 0.01 $\sim$ 0.06, respectively. For simplicity, it is assumed that the channels between antennas and the channels between UE and BS are Rayleigh channels which have only a single path.

A. Identification Performance

In the training phase, we simulate 1,000 groups of relative feature of BS, where $\mathbf{C}'_{BS}$ is denoted as the training set. After that, 500 groups of DL channel estimation are simulated by UE using SEP as the test set. The simulation results of identification accuracy are expressed as the probability of correctly identifying the BS within the target class and the KNN model is employed in the simulation as a classifier.

In addition, aiming at evaluating the performance and robustness of SEP at different SNR levels, we vary the SNR level from -10 dB to 25 dB with an increment of 5 dB, under different channels. The identification accuracy corresponding to different numbers of BSs at different SNR levels under the Rayleigh channel and time delay line (TDL) channel with 24 paths is shown in Fig. 4. It can be seen from this figure that the identification accuracy improves as the SNR increases. SEP can achieve the classification accuracy of more than 80% when the SNR level is higher than 10 dB. In addition, the simulation performance under the TDL channel is slightly lower than that under the Rayleigh channel, which verifies that the proposed SEP method has better robustness with different wireless channel paths.



(a) Rayleigh channel (single-path) (b) TDL channel (multi-path)

Fig. 4. Recognition accuracy versus SNR under different numbers of BSs with different types of channels

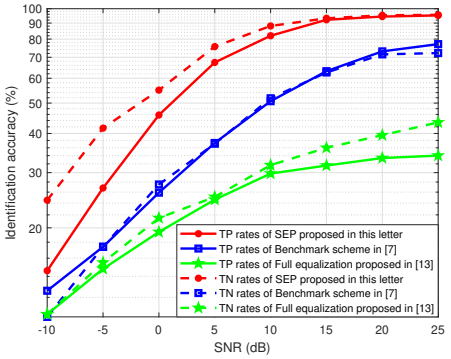


Fig. 5. Recognition accuracy versus SNR under different schemes.

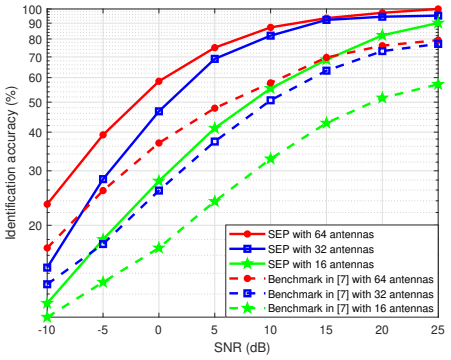


Fig. 6. Comparison of recognition accuracy between SEP and benchmark with different numbers of antennas.

B. Comparison with Other Schemes

The recognition performance of the proposed SEP is assessed in terms of both true positive (TP) and true negative (TN) rates. As shown in Fig. 5, it is clear that both rates vary. According to [13], the proposed full equalization has

the shortcoming of eliminating the BS feature together with wireless channels. Consequently, the UE receives the pure DL signal without any feature, leading to a lack of features. Channel state information (CSI) is exploited in [7] for device identification using the training set and the test set with a ratio of 8.5:1.5. Inspired by this work, the benchmark scheme in the letter simulates 1,000 samples of CSI collected from different sources, from which these samples are first divided randomly into two parts: 80% of the training set and 20% of the test set. By comparison, we find that the performance of SEP is better than that of the benchmark scheme. The benchmark scheme achieves the identification accuracy of 77.1% at the SNR level of 25 dB, while SEP can reach 95.2%. These results and the performance advantage of SEP can be interpreted by the fact that it is impossible to collect measured signals in an extensive and ubiquitous manner, which causes the loss of recognition accuracy. Fortunately, SEP can eliminate the interference caused by wireless channels, hence leading to the achieved improvement in identification performance.

Fig. 6 illustrates and compares the recognition accuracy of SEP and the benchmark with different numbers of antennas. SEP has better performance than the benchmark when the numbers of antennas are the same. Fig. 6 also shows that the accuracy increases with the number of antennas. As shown in this figure, SEP can reach the accuracy of almost 100% with 64 antennas at the SNR level of 25 dB, which is better than 95.2% with 32 antennas. This is aligned with our expectation since more antennas can provide more dimensions of features for RFF of BS, which improves the accuracy of recognition.

V. Conclusion

This letter constructed a location-invariant RFF to recognize BS. Firstly, we found that the idiosyncrasy of wireless channels affects the robustness of RFF. Most existing schemes can hardly eliminate this effect and retain the RFF of BS at the same time. To overcome this shortcoming, we proposed a new scheme called SEP. We obtain the defect matrices in way of transmitting and receiving pilot signals by the BS itself, which are also used as training samples of BS feature. By echoing the signal received by the BS, the UE can obtain the channel estimation and identify whether it is a pseudo BS. Simulation results showed that the proposed SEP algorithm is the state of art, reaching the identification accuracy of 95.2% at the SNR level of 25 dB. It has also been verified that SEP provides an effective way to recognize BS in MIMO systems.

Appendix

Defining signal model $\mathbf{H}_U = \mathbf{R}_{BS}\mathbf{H}\mathbf{T}_{UE}$ and $\mathbf{H}_D = \mathbf{T}_{BS}\mathbf{H}\mathbf{R}_{UE}$, defect matrices $\mathbf{C}_{BS} = \mathbf{R}_{BS}\mathbf{T}_{BS}^{-1}$, $\mathbf{C}_{UE} = \mathbf{R}_{UE}^{-1}\mathbf{T}_{UE}$, the ZF precoding scheme can be utilized, that pseudo inverses the UL channel estimation result by

$$\mathbf{W} = (\mathbf{H}_U^H\mathbf{H}_U)^{-1}\mathbf{H}_U^H. \tag{21}$$

The received signal $\mathbf{Y}_D$ can thus be written as

$$\begin{aligned}\mathbf{Y}_D =& \mathbf{S}_D\mathbf{W}\mathbf{H}_D + \mathbf{Z}_D\\ =& \mathbf{S}_D(\mathbf{H}_U^H\mathbf{H}_U)^{-1}\mathbf{H}_U^H\mathbf{H}_D + \mathbf{Z}_D\\ =& \mathbf{S}_D\mathbf{T}_{UE}^{-1}[\mathbf{H}^H\mathbf{R}_{BS}^H\mathbf{R}_{BS}\mathbf{H}]^{-1}\\ & (\mathbf{H}^H\mathbf{R}_{BS}^H)\mathbf{T}_{BS}\mathbf{H}\mathbf{R}_{UE} + \mathbf{Z}_D.\end{aligned} \tag{22}$$

It can be observed from above that $\mathbf{T}_{UE}^{-1}[\mathbf{H}^H\mathbf{R}_{BS}^H\mathbf{R}_{BS}\mathbf{H}]^{-1}(\mathbf{H}^H\mathbf{R}_{BS}^H)\mathbf{T}_{BS}\mathbf{H}\mathbf{R}_{UE}$ is not a diagonal matrix, because of which the full equalization modifies the precoding method. Finally, the following matrix can be resulted from the precoding process:

$$\mathbf{W}_{F-post} = \mathbf{C}_{UE}(\mathbf{H}_U^H\mathbf{H}_U)^{-1}\mathbf{H}_U^H\mathbf{C}_{BS}. \tag{23}$$

By substituting (2) and (23) into (22), $\mathbf{Y}_D$ is given.

$$\begin{aligned}\mathbf{Y}_D =& \mathbf{S}_D\mathbf{W}_{F-post}\mathbf{H}_D + \mathbf{Z}_D\\ =& \mathbf{S}_D\mathbf{R}_{UE}^{-1}[\mathbf{H}^H\mathbf{R}_{BS}^H\mathbf{R}_{BS}\mathbf{H}]^{-1}\\ & (\mathbf{H}^H\mathbf{R}_{BS}^H\mathbf{R}_{BS}\mathbf{H})\mathbf{R}_{UE} + \mathbf{Z}_D\\ =& \mathbf{S}_D + \mathbf{Z}_D.\end{aligned} \tag{24}$$

This completes the proof of the proposition.

References

[1] Z. Zhang, A. Hu, and X. Wei, "An artificial radio frequency fingerprint embedding scheme for device identification," *IEEE Commun. Lett.*, vol. 26, no. 5, pp. 974–978, May. 2022.

[2] P. Yin, L. Peng, J. Zhang, M. Liu, H. Fu, and A. Hu, "LTE device identification based on RF fingerprint with multi-channel convolutional neural network," in *Proc. IEEE GLOBECOM*, Madrid, Spain, Dec. 2021, pp. 1–6.

[3] S. Hussain, O. Chowdhury, S. Mehnaz, and B. E., "LTEInspector: A systematic approach for adversarial testing of 4G LTE," in *Proc. Symp. Netw. Distrib. Syst. Secur., NDSS*, San Diego, CA, Feb. 2018, pp. 1–15.

[4] A. Shaik and R. Borgaonkar, "New vulnerabilities in 4G and 5G cellular access network protocols: Exposing device capabilities," in *WiSec - Proc. Conf. Secur. Priv. Wirel. Mob. Networks*, Miami Florida, USA, May. 2019.

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

[6] Y. Chen, L. Yin, J. Sun, and S. F. Li, "Research on channel reciprocity of massive MIMO time division duplex system," *Journal of Beijing University of Posts and Telecommun.*, vol. 41, no. 3, pp. 56–62, June. 2018.

[7] L. Kandel, Z. Zhang, and S. Yu, "Exploiting CSI-MIMO for accurate and efficient device identification," in *Proc. IEEE GLOBECOM*, Waikoloa, HI, USA, Dec. 2019, pp. 1–6.

[8] W. Zhong, H. Wang, and C. Liu, "Journal of data acquisition and processing," *Journal of Data Acquisition and Processing*, vol. 35, no. 6, pp. 1125–1133, Nov. 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, Feb. 2019.

[10] Y. Hara, Y. Yano, and H. Kubo, "Antenna array calibration based on frequency selection in OFDMA/TDD systems," *IEICE Trans. Commun.*, vol. E92-B, no. 10, pp. 3195–3205, Oct. 2009.

[11] A. Arslan and F. Georg, "Symbol based statistical RF fingerprinting for fake base station identification," in *Proc. 29th Int. Conf. Radioelektron., (RADIOELEKTRONIKA)*, Pardubice, Czech Republic, Apr. 2019.

[12] M. Azarmehr, A. Mehta, and R. Rashidzadeh, "Wireless device identification using oscillator control voltage as RF fingerprint," in *Proc. IEEE 30th Can Conf. on Electr. and Comput. Eng., CCECE*, Windsor, ON, Canada, May. 2017.

[13] W. Zhang, Nat., H. Ren, C. Pan, and M. Chen, "Large-scale antenna systems with UL/DL hardware mismatch: Achievable rates analysis and calibration," *IEEE Trans. Commun.*, vol. 63, no. 4, pp. 1216–1229, Apr. 2015.

[14] C. Shepard, H. Yu, and N. Anand, "Argos: Practical many-antenna base stations," in *Proc. Annu. Int. Conf. Mobile Comput. Networking*, Istanbul, Turkey, Aug. 2012.