IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received March 23, 2021, accepted April 9, 2021, date of publication April 14, 2021, date of current version April 27, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3073115

Physical Layer Spoofing Attack Detection in MmWave Massive MIMO 5G Networks

WEIWEI LI[1], NING WANG[2], (Member, IEEE),
LONG JIAO[3], (Graduate Student Member, IEEE), AND KAI ZENG[3], (Member, IEEE)
[1]School of Information and Electrical Engineering, Hebei University of Engineering, Handan 056001, China
[2]College of Computer Science, Chongqing University, Chongqing 400044, China
[3]Department of Electrical and Computer Engineering, George Mason University, Fairfax, VA 22030, USA

Corresponding author: Ning Wang (nwang5@cqu.edu.cn)

This work was supported in part by the Science and Technology Research Project of Hebei, China, under Grant QN2019059, in part by the Natural Science Foundation of Hebei Province under Grant F2019402206, in part by the Research Program for Top-notch Young Talents in Higher Education Institutions of Hebei Province, China, under Grant BJ2017037, and in part by the Commonwealth Cyber Initiative (CCI) and its Northern Virginia (NOVA) Node, an investment in the advancement of cyber research and development, innovation and workforce development.

ABSTRACT Identity spoofing attacks pose one of the most serious threats to wireless networks, where the attacker can masquerade as legitimate users by modifying its own identity. Channel-based physical-layer security is a promising technology to counter identity spoofing attacks. Although various channel-based security technologies have been proposed, the study of channel-based spoofing attack detection in 5G networks is largely open. This paper introduces a new channel-based spoofing attack detection scheme based on channel virtual (or called beamspace) representation in millimeter wave (mmWave) massive multiple-input and multiple-output (MIMO) 5G networks. The principal components of channel virtual representation (PC-CVR) are extracted as a new channel feature. Compared with traditional channel features, the proposed features can be more sensitive to the location of transmitters and more suitable to mmWave 5G networks. Based on PC-CVR, we offer two detection strategies to achieve the spoofing attack detection tackling static and dynamic radio environments, respectively. For the static radio environment where the channel correlation is stable, Neyman-Pearson (NP) testing-based spoofing attack detection is provided depending on the ℓ_2-norm of PC-CVR. For the dynamic radio environment where the channel correlation is changing, the problem of spoofing attack detection is transformed into a one-class classification problem. To efficiently handle this problem, an online detection framework based on a feedforward neural network with a single hidden layer is presented. Simulation results evaluate and confirm the effectiveness of the proposed detection schemes. For the static radio environment, the detection rate can be improved around 25% with the help of PC-CVR under the NP testing-based detection, and the detection accuracy can reach 99% with the machine learning-based scheme under the dynamic radio environment.

INDEX TERMS Physical layer security, spoofing attack detection, mmWave communication, virtual channel.

I. INTRODUCTION

Due to its extensive applications, the fifth-generation (5G) wireless networks will have a significant impact on people's modern lives. Smart city, autonomous driving, and mobile payment, etc., which are supported by 5G wireless networks, are changing peoples' lifestyles [1]. In the meantime, the security and privacy of 5G wireless networks are of the utmost importance. In these applications, the privacy information and key control commands would be transmitted by 5G wireless techniques, such as millimeter Wave (mmWave) communications and massive multiple-input and multiple-output (MIMO). However, owing to the broadcast characteristics of wireless communications, 5G wireless networks are vulnerable to physical layer security threats, such as identity spoofing attacks [2], [3]. In this attack, the attacker can pretend to be a legitimate user using a faked identity, such as media access control (MAC) address and internet protocol (IP) address, then it may gain illegal benefits to further perform advanced attacks, like man-in-the-middle attacks and denial-of-service attacks [4].

For this security threat, channel-based physical-layer security techniques can provide a countermeasure to identity spoofing attacks [2], [4]–[6]. Resorting to the inherent

The associate editor coordinating the review of this manuscript and approving it for publication was Moussa Ayyash.

features of wireless channels, the channel-based spoofing attack detection can detect different transmitters with different locations [7]–[11]. Most existing channel-based physical-layer security schemes exploit traditional channel features to achieve detection, e.g., received signal strength (RSS) and channel state information (CSI) [4], [11]. When the detection mechanism indicates that there are some signals with the same identity but from different transmitters, the spoofing attack can be flagged. Then, the spoofing attack alarm is raised and follow-up countermeasures could be applied by legitimate users, such as restarting communication and updating the key.

However, these existing channel-based spoofing attack detection methods struggle to be desirable solutions in 5G wireless networks. Taking the unique characteristics of 5G communications into account, the conventional channel features used on existing detection schemes are difficult to support high detection performance. Take mmWave massive MIMO communications as an example. MmWave massive MIMO channels possess high directionality, which is highly sensitive to transceivers' positions. This unique characteristic can be seen as a blessing for prompting the channel-based detection performance in 5G networks. Nevertheless, traditional channel features, e.g., RSS and CSI, are hard to reflect this unique property of 5G channels. Besides, most existing channel-based spoofing attack detection schemes use Neyman-Pearson (NP) testing as the detection strategy, which is based on the analysis of sample distribution and requires a reasonable threshold [7]–[11]. However, when the sample distribution is hard to obtain and the channel correlation parameter is changing due to the dynamic radio environment, to gain a desirable detection performance based on NP testing is struggling.

To fill this gap, in this paper, we propose to introduce a channel virtual/beamspace representation in mmWave Massive MIMO to achieve the spoofing attack detection in 5G wireless networks. The principal components of channel virtual representation (PC-CVR) are extracted as the employed channel feature. In particular, to achieve a desirable spoofing attack detection based on PC-CVR, two detection strategies are proposed to tackle static and dynamic radio environments, respectively. For the static radio environment where the channel correlation is stable, an NP testing-based spoofing attack detection is presented based on the observation of PC-CVR. For the dynamic radio environment where the channel correlation is dynamically changing, the problem of spoofing attack detection is formulated as a one-class classification machine learning problem. Furthermore, to address this dynamic learning problem, an online updating detection framework based on a *s*ingle-hidden *l*ayer *f*eedforward neural *n*etwork (SLFN) is presented, named SLFN-framework. Simulation results validate the effectiveness of the proposed detection schemes based on NP testing and SLFN-framework, respectively. The detection rate can approach 97% with 10^{-2} false alarm rate under the NP testing-based scheme in the static radio environment, while the detection rate of the traditional scheme is around 70% under the same conditions. The detection accuracy under the proposed machine learning-based scheme can reach 99% in the dynamic radio environment.

The main contributions of this work lie in four aspects:

- We propose to introduce a new channel feature, i.e., channel virtual representation, to counter spoofing attacks in mmWave massive MIMO 5G communications.
- We provide an NP testing-based spoofing attack detection based on the ℓ_2-norm of PC-CVR under the static radio environment.
- For the dynamic radio environment, the problem of spoofing attack detection is formulated as a one-class classification machine learning problem, which is free from the requirements of sample distribution and threshold choice.
- An SLFN-framework with the capacity of online updating is proposed to address machine learning-based spoofing attack detection based on PC-CVR.

It is worth noting that this paper is the extended version of our conference paper [12], which developed a basic solution to counter the spoofing attacks under a static radio environment based on channel virtual representation. Compared with our earlier work, the extension of this paper contains these four aspects: 1) A detailed analysis of channel virtual representation is given; 2) The virtual channel-based spoofing attack detection for dynamic radio environment is considered, and the problem of the spoofing attack detection is transformed into a one-class classification problem; 3) A new SLFN-framework is proposed to address the problem of the one-class classification machine learning based on PC-CVR; 4) More simulation results are provided.

The rest of this paper is organized as follows. Section II introduces related works. Section III describes the system model, its motivation and challenges, and Section IV shows the analysis of channel virtual representation. In Section V, the NP testing based on PC-CVR is provided. Machine learning-based spoofing attack detection based on PC-CVR is proposed in Section VI. Section VII provides the simulation and evaluation results, and Section VIII concludes this paper.

II. RELATED WORK

In this section, we will introduce the related work involving identity spoofing attack detection and channel virtual representation.

A. SPOOFING ATTACK DETECTION

Identity spoofing attacks have recently been gaining significant attention from researchers. The authors in [9] provided a survey study on this physical layer threat. For identity spoofing attacks, the attacker can transmit a deceiving signal with a fake identity to the receiver so that the receiver would accept the spoofer as a legitimate user. Channel-based physical layer security techniques can be used to counter this physical layer threat. It is worth noting that physical layer authentication schemes are not to replace the cryptography-based security mechanism. Instead, they are a supplement and enhancement approach for current cryptography mechanisms. In contrast to traditional cryptography-based authentication, physical layer authentication can fill the gap of the security mechanism in the physical layer. Furthermore, since the secure fundamental is based on physical properties, the physical layer authentication is free from key distribution and management, which is more suitable for heterogeneous networks, dense networks, low-complex IoT devices and other 5G networks [7], [13]–[16].

Resorting to channel features, such as RSS [4], [11], power spectral densities (PSD) [10], channel frequency response (CFR) [4], and channel impulse response (CIR) [17], channel-based spoofing attack detection methods can detect the locations of transmitters. In most existing channel-based security technologies, NP testing is the most commonly used detection strategy, in which it requires the analysis of signal distribution and a reasonable threshold. Once the detection mechanism detects that received packets with the same identity information are from different transmitters with different locations, the spoofing attack alarm will be raised. Then the legitimate users in the wireless network will take follow-up countermeasures to this security threat. The most relevant work to this paper is [4], where the authors consider the channel-based spoofing attack detection in a dynamic ratio environment, and a dynamic threshold selection scheme that uses reinforcement learning techniques and game theory was presented to obtain the optimal threshold for NP testing.

However, the unique characteristics of 5G communications have not been noticed in these existing works. Compared with these existing works, there are two main differences between them and our work: (i) we introduce a new channel feature, i.e., PC-CVR, to achieve channel-based spoofing attack detection, rather than traditional channel features; (ii) we propose a new machine learning-based spoofing attack detection strategy to tackle the dynamic radio environment, instead of NP testing that requires sample distribution and a reasonable threshold.

In addition, deep learning approaches have been used in cyber security intrusion detection [18]. For examples, a federated deep learning scheme was proposed to detect the date intrusion in the industrial cyber-physical system [19], the authors in [20] proposed a feed-forward deep neural network using a Wrapper based feature extraction unit, and a cloud-based cyber-physical intrusion detection scheme using deep learning was presented in [21]. However, it is worth noting that intrusion detection and physical layer spoofing attack detection are two different problems. The differences can be reflected in two aspects: (1) Intrusion detection mainly focuses on the high layer data characteristics of the software and network, such as data package and Netflow data; while spoofing attack detection mainly focuses on the physical layer features of wireless channels. (2) Most intrusion detection schemes can employ intrusion datasets as the training samples to establish detection models, such as UNSW-NB15 and AWID intrusion detection datasets [20]. For spoofing attack detection, it is hard to build a spoofing attack dataset since the wireless channel is random and the wireless channel of the attacker is unpredictable. Therefore, the detection approaches used in cyber security intrusion detection are struggling to be directly applied to the physical layer spoofing attack detection.

B. CHANNEL VIRTUAL REPRESENTATION

Channel virtual (or beamspace) representation was first discussed in [22] and has been applied in mmWave and MIMO communication systems [23]. Virtual channels are composed of virtual angle-of-arrival (AoA), virtual angle-of-departure (AoD), and channel gains. It can be seen as a mapping of the real channel in a special space. The authors in [24] have given a fast estimation method to obtain the related parameters. Channel virtual representation has been used to detect pilot contamination attacks in NOMA communications [25]–[27].

Generally speaking, when the number of antennas is sufficient, such as the massive MIMO scenario, different channel paths can be represented by several concentrated path gains with different virtual angles [22]. In practice terms, supported by mmWave and massive MIMO 5G communication, the tiny wavelengths allow for dozens to hundreds of antenna elements to be placed in an array on a relatively small physical platform [28]. Under this case, the virtual channel matrix will become a sparse matrix in mmWave massive MIMO 5G communications. Thus, compared to traditional channel features, the characteristics of the virtual channel are more sparse and concentrated, and the channel differences caused by different locations are easier to distinguish. Therefore, the feature of the virtual channel could beat the traditional channel features in the channel-based spoofing detection under mmWave massive MIMO 5G communications.

III. SYSTEM MODEL, MOTIVATION AND CHALLENGES

This section will introduce the system model, motivation and challenges of this study.

A. SYSTEM MODEL

1) SYSTEM SETUP

We consider a 5G wireless network that consists of a base station (BS) and users including N legitimate users (LU) and potential spoofing attackers (SA) that impersonate another node with a fake identity. Fig. 1 illustrates a typical application scenario. Once the BS has received a packet, it can estimate the channel states associated with the packet. The pilots or the preambles of this packet can be used to estimate the channel of the corresponding transmitter. Transmitters and receivers would equip with mmWave and massive MIMO. The communications between BS and LUs obey normal 5G communication standards, where the beamforming technique can be used to benefit communication. Moreover, the locations of all LUs are fixed in the network, and the location of SA is arbitrary but cannot be the same as LUs.

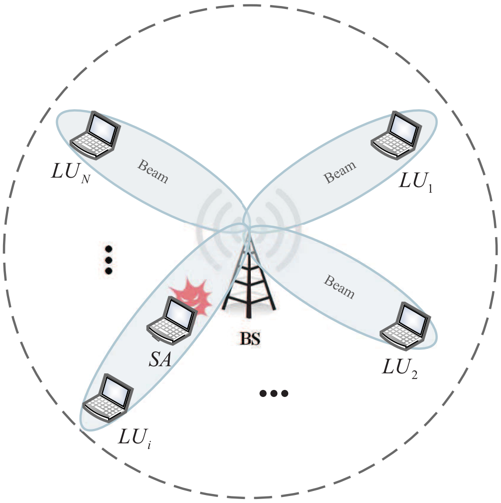


FIGURE 1. A typical mmWave massive MIMO application scenario.

2) THREAT MODEL

We assume that SA is a powerful spoofing attacker who can masquerade the legitimate user by modifying its own identity. The SA can manipulate arbitrary fields in a frame, such as the source and destination IP/MAC addresses, sequence number, frame check, and so on. It may even compromise the authentication key after sniffing the communication between the BS and legitimate users for enough time. The SA could enjoy the same mmWave massive MIMO beam as the victim, as shown in Fig. 1, but cannot replace the victim. During the communication period, the attacker could launch the attack at any time with a fake identity and send a fake packet in any time slot.

3) DETECTION MODEL

In general, for the channel-based spoofing detection study, the hypothesis testing is performed to determine whether the packet with the identity information is indeed sent by the transmitter which the identity information relates [4], [29]. Let $\zeta(H)$ denote the real transmitter that sends a packet with the channel information H, and ξ be the identification information related to the legitimate transmitter which the packet declares. Thus, according to the detection of H, the channel-based spoofing attack detection can be formulated as follow,

$$\begin{aligned} &1)T_0 : \zeta(H) = \xi; \\ &2)T_1 : \zeta(H) \neq \xi. \end{aligned} \tag{1}$$

where the null hypothesis T_0 represents that the real transmitter of this packet is indeed ξ. The alternative hypothesis T_1 indicates that the packet is not sent by the transmitter ξ.

The detection of H is based on the uniqueness of channel states. According to the propagation theory, the channel decorrelation will occur rapidly as the transmitter's location changes by the order of a wavelength [30]. Thus, theoretically, as long as the distance between the transmitters exceeds the wavelength, which is 5mm for systems working at 60GHz, their channel states will be significantly different. As a result, if the receiver can record the channel state of last communication and the channel information of the received packets and the channel record are similar, the transmitter of these received packets is considered unchanged. Otherwise, the received packets could come from different transmitters, and the spoofing attack can be flagged. When the spoofing attack detection works, the spoofing attack alarm is raised and follow-up countermeasures could be applied by legitimate users, such as restarting communication and updating the key.

It is worth noting that even the channel record might be the spoofing attacker's channel, the detection strategy still works because the received packets and the channel record would have significantly difference when the legitimate user sends packets. BS can establish a machine learning-based detection model to detect the received signal, and the machine learning algorithm can be executed in the application layer protocol while the training samples and the target signals are from the physical layer. Moreover, we will consider a static radio environment and a dynamic radio environment, respectively. Under the static radio environment, the channel correlation between the received packet and the recorded packet is stable, and it will be constantly changing under the dynamic radio environment.

B. MOTIVATION

Inspired by the emerging signal processing technology in mmWave communication, i.e., channel virtual representation, we propose to introduce PC-CVR to achieve the channel-based spoofing attack detection in 5G communications. Compared to traditional channel features in existing channel-based detection schemes, the unique characteristics of PC-CVR lie in two aspects:

- *PC-CVR is more sensitive to the location of transmitter.* Channel virtual representation consists of virtual AoA, virtual AoD, and the corresponding path gain. The virtual channel can be seen as a projection of real AoA/AoD on the space of virtual AoA/AoD. The occupied positions by PC-CVR on the virtual AoA/AoD vector can be regarded as the result of sampling the real AoA/AoD. Thus, PC-CVR can represent the characteristics of the real AoA/AoD, which can outperform traditional channel features on localization [31].
- *PC-CVR is more suitable for 5G communication systems.* For channel virtual representation, the resolution of virtual AoA/AoD depends on the number of antennas at the transceiver. Specifically, more antennas can help channel virtual representation to accurately recognize transmitters. Also, channel virtual representation can indicate the high directionality of mmWave, which can be used to promote beamforming in 5G communications [32]. With the development of 5G networks, there would be more antennas and higher frequency, which can benefit PC-CVR in giving it the ability to detect the different transmitters at different locations. As a result, PC-CVR is better applied to the development of 5G networks compared with traditional channel features.

The detailed analysis of the channel virtual representation will be provided in Section IV.

C. CHALLENGES

To achieve a desirable spoofing attack detection based on PC-CVR for 5G wireless networks, we have to tackle the following two issues:

1) *Achieving NP testing-based spoofing attack detection without the probability distribution function of PC-CVR.* In channel-based spoofing attack detection schemes, NP testing is a commonly used detection strategy that depends on the distribution function of samples. For the static radio environment where the channel correlation is stable, the PC-CVR should follow a certain probability distribution function. However, due to the complex signal processing and multiple analog/digital combiners in 5G communications, it is hard to exactly estimate the real probability distribution function of PC-CVR. As a result, it is a challenge to achieve an effective NP testing-based spoofing attack detection without the accurate probability distribution function of PC-CVR.
2) *Effectively tackling dynamic radio environment.* In a dynamic radio environment, the channel correlation is changing due to the randomness and variation of the communication surrounding. However, it is not clear whether this change could impact the probability distribution of PC-CVR. For the NP testing-based detection strategy, it will not work if the probability distribution function is not clear. For this issue, a detection scheme that does not rely on the analysis of the probability distribution function may be a better solution. In this case, machine learning models that achieve classification only depending on training data would be a reasonable alternative way. Based on PC-CVR in the dynamic radio environment, it is an open problem to achieve an effective machine learning-based spoofing attack detection.

For the first issue, Section V will provide a reasonable solution based on the observation of PC-CVR, and Section VI will focus on the second issue and propose a one-class classification machine learning-based solution. To make these solutions easy to follow, we will first review and analyze the channel virtual representation in mmWave massive MIMO communications in the next section.

IV. ANALYSIS OF CHANNEL VIRTUAL REPRESENTATION

Channel virtual representation is developed from a mmWave geometry channel model for mmWave communications. Considering the sparse multipath structure in mmWave, the channel can be represented by a geometry channel model with scatters formed by ray tracing [33], i.e.,

$$H = \sqrt{\frac{N_t N_r}{\rho}} \sum_{l=1}^{L} \alpha_l a_r(\phi_{r,l}) a_t^*(\phi_{t,l}), \tag{2}$$

where N_t and N_r are the antenna number of transmitter and receiver, respectively. ρ indicates the average path-loss. L denotes the number of scatters and α_l is the corresponding fading coefficients with zero mean complex Gaussian distribution. $\phi_{r,l} \in (0, 2\pi]$ and $\phi_{t,l} \in (0, 2\pi]$ denote the physical AoD and AoA angles at the transmission and reception sides. Vectors $a_r(\phi_{r,l}) \in {}^{N_r \times 1}$, and $a_t(\phi_{t,l}) \in {}^{N_t \times 1}$ are the antenna array responses.

Channel virtual representation is applied to represent the mmWave massive MIMO channel by fixed virtual receive and transmit directions [22], [32]. If there is a antenna array consisting of an N_v dimensional uniform linear array, the virtual representation corresponds to system representation with respect to uniformly spaced spatial angles $\vartheta_i = i/N_v$, $i = 0, \ldots, N_v - 1$. The corresponding steering vectors can be defined by $\theta_i = \arcsin(\lambda \vartheta_i / d)$, where d denotes the antenna spacing and λ indicates the wave-length of operation [32]. Thus, a unitary Discrete Fourier Transform (DFT) matrix $N_v \times N_v$ can be obtained,

$$U = \frac{1}{\sqrt{N_v}} \left[a(\theta_0), \ldots, a(\theta_{N_v - 1}) \right]^T, \tag{3}$$

where $U^* U = U U^* = I$, and U^* is the conjugate transpose of U.

Based on this unitary DFT matrix, we have the channel virtual representation,

$$H = U_r H_V U_t^* = \sum_{q=1}^{N_r} \sum_{p=1}^{N_t} H_V(q, p) a_r(\theta_{r,q}) a_t^*(\theta_{t,p}), \tag{4}$$

where $U_r \in \mathbb{C}^{N_r \times N_r}$ and $U_t \in \mathbb{C}^{N_t \times N_t}$ are unitary DFT matrices, which can reflect the fixed virtual receive and transmit angles that uniformly sample the unit angle space. $H_V \in \mathbb{C}^{N_r \times N_t}$ is the virtual channel matrix, in which the entry $H_V(q, p)$ capture the gains of the corresponding paths. $\left\{\theta_{r,q}\right\}$ and $\left\{\theta_{t,p}\right\}$ denote virtual AoAs and AoDs, respectively.

Based on Eq. (2) and Eq. (4), the relationship between channel virtual representation and the physical channel model can be represented by

$$H_V(q, p) = \sum_{l=1}^{L} \alpha_l f(N_r, \phi_{r,l} - \frac{q}{N_r}) f^*(N_t, \phi_{t,l} - \frac{p}{N_t}), \tag{5}$$

where the function $f(\epsilon, \delta)$ is defined as

$$f(\epsilon, \delta) = \frac{1}{\epsilon} \sum_{l=0}^{\epsilon - 1} e^{-j 2\pi \delta l}. \tag{6}$$

From Eq. (5), we can see that the virtual representation $H_V(q, p)$ are samples of a smoothed version of scatters at virtual angles. Thus, the position of the PC-CVR on the virtual angle vectors will indicate the characteristics of the angles of all main scatters.

For a visual description of channel virtual representation, we provide an example of mmWave massive MIMO channels in Fig. 2. A 60GHz mmWave massive MIMO channel with 128 × 128 antennas is considered and the number of main

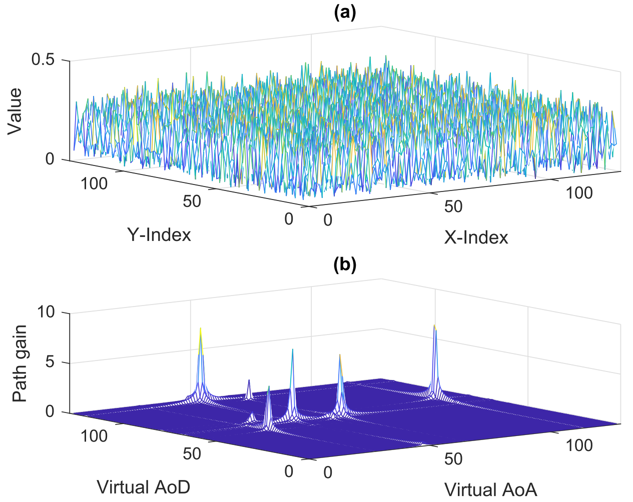


FIGURE 2. An example of mmWave massive MIMO channel with 128 × 128 antennas. (a) The raw channel; (b) The corresponding channel virtual representation.

scatters is 7. Fig. 2(a) shows a traditional channel feature, i.e., RSSI, which is used commonly in existing channel-based spoofing attack detection schemes [4], [4], [11], and Fig. 2(b) gives the corresponding channel virtual representation under the same channel model. We can see that the traditional channel features show a disordered state, which is hard to reflect the directionality and sparsity of mmWave channel. By contrast, the channel virtual representation can indicate the characteristics of scatters, where each scatters with a unique angle can be represented by the PC-CVR with a corresponding group of virtual AoA/AoD bins. All scatters can be distinguishable as long as the antenna space ($N_r \times N_t$) is sufficient. These characteristics would be more beneficial to the recognition of mmWave massive MIMO channels compared with the traditional channel features.

V. NP TESTING-BASED DETECTION UNDER STATIC SCENARIO

In this section, we will address the first issue mentioned in Section III-C. To tackle this problem, we transform the probability statistical problem of PC-CVR into the problem of the ℓ_2-norm of PC-CVR. Furthermore, we found that the ℓ_2-norm of PC-CVR can be fitted by a normal distribution. In this way, NP testing can be achieved even without the exact probability distribution function of PC-CVR. It is worth noting that compared with machine learning-based schemes, the advantages of the NP testing-based detection schemes lie in high execution efficiency without training phases. This method can be applied in scenarios where the statistics distribution of samples is clear.

A. BINARY HYPOTHESIS TESTING

After obtaining channel virtual channel based on Eq. 4, we can use a filter with a threshold τ (e.g., $\tau \in [0.5, 1]$) to extract PC-CVR. Thus, the channel values less than τ will become zero and that higher than τ are retained. Let $\hat{H}_V$ denote the record of the channel and H_V indicate the received channel. Thus, the ℓ_2-norm between the two channels can be given by

$$D(H_V, \hat{H}_V) = \left\| H_V - \hat{H}_V \right\|_2, \tag{7}$$

where $\|\cdot\|_2$ indicates ℓ_2-norm.

Under the normal case, there is a high correlation between H_V and $\hat{H}_V$, since they have the same transmitter with the same propagation path. Hence, the distance between H_V and $\hat{H}_V$ is small. In contrast, under the case of spoofing attacks, the consistency between H_V and $\hat{H}_V$ is broken since they have different propagation paths even during the channel coherence time. Thus, the distance between H_V and $\hat{H}_V$ will be larger than that of the normal case. As a result, the hypothesis testing in Section III-A3 becomes:

$$1)\ \ T_0 : D\left(H_V, \hat{H}_V\right) \leq \eta,$$
$$2)\ \ T_1 : D\left(H_V, \hat{H}_V\right) > \eta.$$

where η denotes a threshold used to separate the distance between T_0 and T_1.

B. DISTRIBUTION AND THRESHOLD

By observing $D(H_V, \hat{H}_V)$, we found that the value of the distance under the normal case and spoofing attack case could approximate a normal distribution. Fig. 3 shows the results of normal distribution fitting for the distances under the normal case and the spoofing case, respectively. In this example, the Monte Carlo simulation count is 10,000, and the channel correlation coefficient is 0.9. We can see that the fitting curves based on normal distributions can fit the data well under both the normal case and the spoofing case.

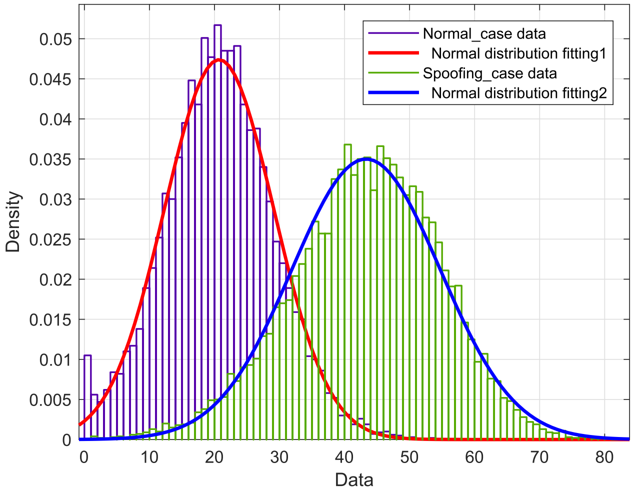


FIGURE 3. The results of normal distribution fitting for the Euclidean distances under the normal case and spoofing case.

Based on this observation, we provide a strategy to obtain the threshold η by using NP testing, where the detection minimizes the miss rate subject to a maximum tolerable constraint on a given false alarm rate.

When obtaining $D(H_V, \hat{H}_V)$, two random normal distributions can be used to fit these values under the spoofing attack case and the normal case, respectively. Let $CN(\mu_a, \sigma_a^2)$ fit the values of $D(H_V, \hat{H}_V)$ under the normal case, and $CN(\mu_b, \sigma_b^2)$ fit the values of $D(H_V, \hat{H}_V)$ under the spoofing attack case.

Here, we use the difference in the mean to distinguish between hypothesis T_0 and T_1. According to NP testing [34], we have

$$\frac{P(D;T_1)}{P(D;T_0)} > \eta, \tag{8}$$

where D denotes the distance between two channels, and η is the threshold we want.

The threshold η can be represented by the given false alarm rate,

$$P_{FA} = P\{D > \eta; T_0\}. \tag{9}$$

Then, we have

$$P_{FA} = \int_{\eta}^{\infty} P_{T_0}(D)dT_n = Q\left(\frac{\eta - \mu_a}{\sigma_a}\right), \tag{10}$$

where $Q(*)$ is the tail distribution function of the standard normal distribution, i.e.,

$$Q(x) = \int_{x}^{+\infty} \frac{1}{\sqrt{2\pi}} \exp(-\frac{1}{2}t^2)dt. \tag{11}$$

Thus, we have

$$\eta = Q^{-1}(P_{FA}) \cdot \sigma_a + \mu_a, \tag{12}$$

where $Q^{-1}(*)$ indicates the inverse function of $Q(*)$.

In this way, according to a given false alarm rate, we can obtain the corresponding threshold to separate hypothesis T_0 and hypothesis T_1.

VI. MACHINE LEARNING-BASED DETECTION FOR A DYNAMIC RADIO ENVIRONMENT

This section focuses on the second issue mentioned in Section III-C, where the probability distribution function of PC-CVR is not clear. For machine learning-based algorithms, with sufficient positive and negative training samples, machine learning models can train a discriminator to achieve classification. Nevertheless, for the spoofing attack detection based on PC-CVR under a dynamic radio environment, we must handle two issues: (i) how to obtain the negative training sample. In practical applications, legitimate users struggle to gain the sample of spoofing attackers since it is difficult to predict the action and location of spoofing attackers; (ii) how to efficiently update the classification mode to adapt to the dynamic radio environment where the channel correlation parameters are changing. To overcome these issues, we propose to transform the problem of spoofing attack detection into a one-class classification problem and present a novel online SLFN-framework to address this problem.

A. ONE-CLASS CLASSIFICATION DETECTION MODEL

One-class classification recognizes the target signals based on a machine learning model which is trained by the positive training samples only. In other words, the machine learning model has only one type of training data. For the spoofing attack detection, the training samples would be from the normal case only.

Formally, let $D_{TR} = [x_i, y_i]$ be a set of training vectors, $x_i \in \mathbb{R}^n$ where $i = 1, \ldots, M$ and M is the number of the training samples. The corresponding state only has the target label, i.e., $y = [y_i] = [1, \ldots, 1]_{1\times M}$. Thus, the one-class classifier aims to use the discriminant function $f : \chi \subseteq \mathbb{R}^n \rightarrow \mathbb{R}$ to train a corresponding machine learning model. For a set of testing data $D_{TE,x} = [\widehat{x}_1, \ldots, \widehat{x}_k]$, the one-class classifier can give the corresponding predictive values, i.e., $\widehat{y} = [\widehat{y}_1, .., \widehat{y}_k]$, where $\widehat{y}_k \in \{0, 1\}$.

Let $\widehat{y}_k = 0$ indicate the normal case and $\widehat{y}_k = 1$ denote the spoofing attack case. The problem of spoofing attack detection shown in Eq. (1) can be represented as

$$f(\widehat{x}_k) = \begin{cases} \widehat{y}_k = 0 & \textit{for Normal} \\ \widehat{y}_k = 1 & \textit{for Spoofing Attack}. \end{cases} \tag{13}$$

Next, we will introduce a feedforward neural network based framework to achieve this machine learning-based spoofing attack detection.

B. SLFN-FRAMEWORK

The presented SLFN-framework consists of three steps: data preprocessing, training process and online update. Fig. 4 shows an overview of this framework. In the data preprocessing, the raw data is normalized and measured. Then, these samples are used to build the generator and discriminator in the training step. In the detection process, the discriminator can be updated according to the changes in the

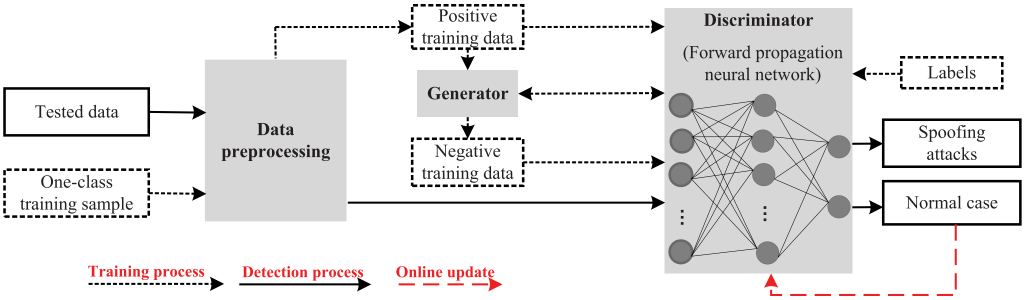


FIGURE 4. One-class detection framework overview.

communication environment. In the following, we will introduce these steps in detail.

1) DATA PREPROCESSING

There are two main data preprocessing processes: normalization and measurement.

- The normalization is to transform the channel matrix of virtual channels into a vector and map the relevant data into a fixed data range. Similar to Section V, a filter with the threshold τ is exploited to extract PC-CVR. The matrix of the channel can be transformed into a vector and mapped into a fixed data range, i.e., $H_V \in \mathbb{C}^{N_r \times N_t} \to h \in \mathbb{R}^{N_{rt} \times 1}$, where $N_{rt} = N_r \times N_t$.
- Two different metrics are utilized to measure the distance between the received channel and channel record, respectively.

  The Euclidean distance (ED) is employed as the first metric:

$$M^{(ED)}(h, h_\Delta) = \|h - h_\Delta\|^2, \tag{14}$$

  where $\|\cdot\|^2$ is the Frobenius norm, h denotes received channel and h_Δ is the channel record.

  The Pearson correlation coefficient (PCC) is as the second metric, given by

$$M^{(PCC)}(h, h_\Delta) = \frac{\sum_{i=1}^{N_{rt}} (h_i - \overline{h})(h_{\Delta i} - \overline{h_\Delta})}{\sqrt{\sum_{i=1}^{N_{rt}} (h_i - \overline{h})^2} \sqrt{\sum_{i=1}^{N_{rt}} (h_{\Delta i} - \overline{h_\Delta})^2}}, \tag{15}$$

  where h_i and $h_{\Delta i}$ denote the element of the channel vector, and $\overline{h}$ and $\overline{h_\Delta}$ indicate the mean values, respectively.

2) TRAINING PROCESS

The training process includes generator training and discriminator training. The generator is to generate the negative training data resorting to the target data (i.e., positive training samples), and the discriminator is to distinguish the spoofing attack case from the normal case.

- The generator training is based on the characteristics of the positive training data. According to the analysis in Section III-A3, the channel correlation under the spoofing attack case is smaller than that of the normal case. That means that the PCC between the record data and the negative training data (spoofing attack case) should be lower than that between the record data and the positive training data (normal case). Moreover, the ED under the normal case should be higher than that of the spoofing attack case. Based on this observation, we can establish a model to generate the negative training data according to the characteristics of positive training data.

  Formally, let D_G denote the negative training data and Ω indicate a irregular region where can randomly select the negative training data. $D_G = [M_{G,i}^{(ED)}, M_{G,i}^{(PCC)}]_{2\times n_G}$, where $i = 1, \ldots, n_G$ and n_G is the number of the negative samples. Thus, the generation of the negative training data can be represented by

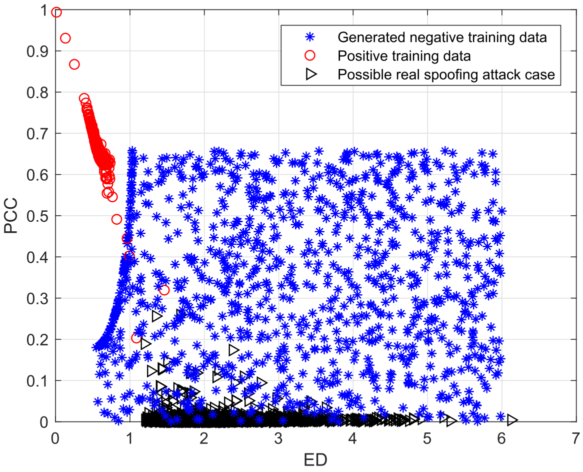


FIGURE 5. **An example of the training positive data and the generated negative training data. The channel correlation coefficient *a* for positive training data is 0.7, and *a* = 0 for the data under spoofing attack case.**

$$D_G = [M_{G,i}^{(PCC)}, M_{G,i}^{(ED)}]_{2\times n_G} \in \Omega$$

$$\Omega \; subject\ to \begin{cases} 0 \leq M_{G,i}^{(PCC)} < M_C^{(PCC)} \\ \chi \geq M_{G,i}^{(ED)} > M_C^{(PCC)} \\ \|D_G - D_C\|^2 \leq R_G \\ R_G = R_C + \psi, \end{cases} \tag{16}$$

  where $[M_C^{(ED)}, M_C^{(PCC)}]_{1\times 2}$ is the center of the positive training data, D_C denotes the center of the sample of the positive data and R_C denotes the area radius of the positive training data. R_G indicates the margin area between the positive training data and the negative training data. χ is the possible upper bound of the generated negative training data and can be simply designed as an empirical value, e.g., $\chi = 10 \times M_C^{(PCC)}$. ψ is a soft margin slack variable and can be optimized in the discriminator training process. Fig. 5 illustrates an example of the negative training data where the positive training data is from the channel correlation condition $a = 0.7$, and such parameter in spoofing attack case is $a = 0$ (The define of the channel correlation condition a will be given in Eq. 22 and Eq. 23 in Section VII.).
- The discriminator is based on a fast forward propagation neural network with single hidden layer. Training a neural network with single hidden layer for classification can be seen as a minimization problem, which is to obtain input weights W, output weights Z, and bias b, i.e.,

$$\min_{W,b,Z} E_{loss} = \sum_{i=1}^{N} (\sum_{j=1}^{K} Z_j g(W_j \cdot x_i + b_j) - y_i), \tag{17}$$

  where x denotes the training samples, $j = 1, .., K$, $i = 1, .., N$, and K and $N = n_P + n_G$ denote the number of neurons in the hidden layer and the number of training samples, respectively. In addition, $y \in \{0, 1\}$ is the label of the training data.

If the active function in the neural network is $g(*)$, the output matrix Θ of the hidden layer can be represented as

$$\Theta = \begin{bmatrix} g(W_1, b_1, x_1) & \dots & g(W_K, b_K, x_1) \\ \vdots & \ddots & \vdots \\ g(W_1, b_1, x_N) & \cdots & g(W_K, b_K, x_N) \end{bmatrix}. \quad (18)$$

Thus, training the single hidden layer neural network can be transformed into the problem to solve a linear system,

$$\Theta Z = Y,$$

where $Y = [y_1, y_2, .., y_N]$ is the label of the training data.

Then, according to [35], if the matrix Θ is determined by initialization and training data, the output weights of the neural network can be solved by

$$Z = \Theta^{+} Y,$$

where Θ^{+} is the Moore-Penrose generalize inverse of Θ. Thus, if the prediction label is $\hat{Y}$ under the training samples, the training accuracy Φ can be represented as

$$\Phi = \frac{\left\| Y - \hat{Y} \right\|_0}{N},$$

where $\|\cdot\|_0$ indicates ℓ_0-norm that counts the number of non-zero values.

Furthermore, to optimize the discriminator and generator, there is a trade-off between Φ and R_G,

$$\min_{\psi} 1 - \Phi + R_G \quad (19)$$

$$\textit{subject to} \begin{cases} 1-\Phi \geq 0.99 \\ R_G = R_C + \psi \\ \psi \in [0, \infty). \end{cases}$$

This optimization problem can be solved by a simple linear programming.

3) DETECTION PROCESS

In the detection process, the proposed detection scheme can achieve discriminator update according to the changes in environment.

Let $\tilde{x}$ indicate the new positive training samples that have been authenticated, $\tilde{N}$ be the size of the training samples, $Z_{(0)}$ denote the original hidden layer output weights, and $Z_{(1)}$ denote the new ones. $\Theta_{(0)}$ is the original output matrix, then the new one $\Theta_{(1)}$ can be obtained from the new samples,

$$\Theta_{(1)} = \begin{bmatrix} g(W_1, b_1, \tilde{x}_1) & \dots & g(W_L, b_K, \tilde{x}_1) \\ \vdots & \ddots & \vdots \\ g(W_1, b_1, \tilde{x}_{\tilde{N}}) & \cdots & g(W_L, b_K, \tilde{x}_{\tilde{N}}) \end{bmatrix} \quad (20)$$

Thus, according to [35], the new output weights $Z_{(1)}$ can be solved by

$$Z_{(1)} = Z_{(0)} + \gamma^{-1} \Theta_{(1)}^{T} (Y_{(1)} - \Theta_{(1)} Z_{(0)}), \quad (21)$$

where $\gamma = \Theta_{(0)}^{T} \Theta_{(0)} + \Theta_{(1)}^{T} \Theta_{(1)}$.

The pseudo-code of the proposed SLNF-framework is provided in Algorithm 1.

Algorithm 1 SLFN-Framework

```
Require: Training sample $H_V$.
  Repeat (for each episode)
  Preprocessing:
    1) Normalization;
    2) Calculate the positive training data according to Eq. (14) and Eq. (15);
  Training process:
    1) Obtain the negative training data according to Eq. (16);
    2) Train discriminator based on Eq. (17);
    3) Optimization based on Eq. (20);
  Detection process:
    1) Calculate the predictive value based on the discriminator.
    2)   If $\hat{y} = 0$
    3)     Accept this message $\tilde{x}$.
    4)   Else
    5)     Raise alarm.
    6)   End If
    7) Update the discriminator according to Eq. (21).
  End Repeat
```

VII. SIMULATION RESULTS

In this section, we provide numerical results to verify the proposed channel-based spoofing attack detection schemes.

A. SIMULATION METHOD

We used MATLAB to evaluate the Monte Carlo experiment data on a general computer, which operates on a 64-bit system with a 16G memory and an i7-7700 CPU. Without loss of generality, according to [32], the physical AoD/AoA, i.e., $\phi_{t,l}$ and $\phi_{r,l}$ are randomly generated with uniform distribution in $(0, 2\pi)$. The number of scatters is set as L and each scatter is assumed to contribute to a single propagation path [36]. Furthermore, according to Section III-A3, under the spoofing attack case, the channel of the legitimate channel and that of the attacker are independent. For the normal case, based on Jakes model [30], the channel correlation can be represented by

$$H_A(k+1) = aH_A(k) + \omega(k), \quad (22)$$

where $H_A(k+1)$ and $H_A(k)$ denote the channel information extracted from two successive packets with the same transmitter. a is the channel correlation parameter, and $\omega(k)$ indicates an i.i.d. zero-mean complex Gaussian process, which is independent of $H_A(k)$. The variance of $\omega(k)$ is defined as

$$\sigma_{\omega}^2 = (1 - a^2)\sigma_A^2. \quad (23)$$

In practical terms, the channel correlation coefficient a can be identified as the term $J_0(2\pi vT / \lambda)$, where λ is the RF wavelength, v is the moving speed of the node and J_0 represents the Bessel function of the first kind and zero-th order [30].

B. NP TESTING-BASED SPOOFING ATTACK DETECTION SCHEMES

Here, we mainly consider three key factors which may influence the performance of detection scheme: (1) The number of multipaths $L = \{5, 10, 15, 20\}$, (2) the number of antennas, i.e., $N_t = N_r = \{16 \times 16, 32 \times 32, 64 \times 64, 128 \times 128\}$, and (3) the signal to noise ratios $SNRs = \{-5, 0, 5, 10\}$. For the proposed virtual channel-based detection scheme, the detection scheme is based on Section V. Meanwhile, the competition detection scheme is commonly used in existing spoofing attack detection schemes, where the channel model (i.e., Eq. (2)) is directly used to achieve NP testing-based spoofing attack detection [4].

In Fig. 6, the detection performance of the proposed scheme is represented by the receiver operating characteristic (ROC) curve, where P_D denotes the detection rate and P_{FA} is the false alarm rate. In this example, the proposed spoofing detection shows a better performance than that of the traditional detection scheme. For instance, when the false alarm rate is $P_{FA} = 0.03$, all of the detection rates P_D on the channel virtual representation based curves can surpass 90%. Under the same conditions, the P_D of the traditional detection scheme is less than 70%. Moreover, Fig. 6 shows that more antennas result in a better detection performance under both the proposed and traditional schemes.

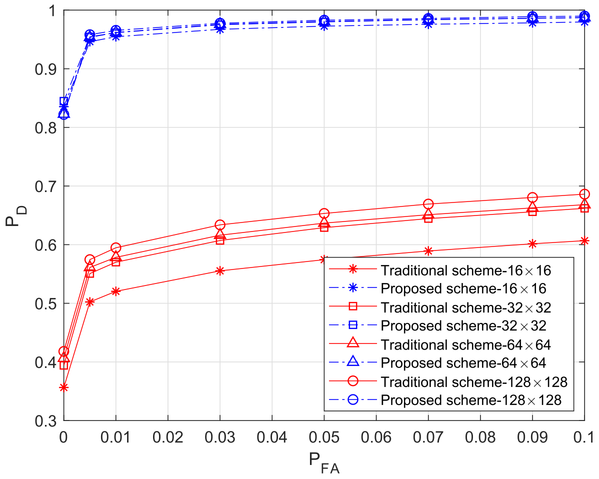


FIGURE 6. Simulated false alarm rate P_{FA} vs. P_D under different antenna numbers $N_t = N_r = \{16 \times 16, 32 \times 32, 64 \times 64, 128 \times 128\}$. In this example, the signal to noise ratio is SNR=10dB; carrier frequency is 28GHz; the multipaths condition $L = 10$, and the number of Monte Carto simulations is 10,000.

Fig. 7 shows the detection performance under different multipath conditions. We notice that all of the curves of the proposed detection schemes are higher than those of traditional schemes. Moreover, even in a complex environment that leads to a great number of multipaths, the detection based on the channel virtual representation based scheme can show better detection performance. For example, as the multipath number $L = 20$, the detection rate P_D of the proposed detection can reach 95% with a false alarm rate $P_{FA} = 0.05$. Whereas, under the same conditions, the detection rate P_D of the traditional detection scheme is around 60%.

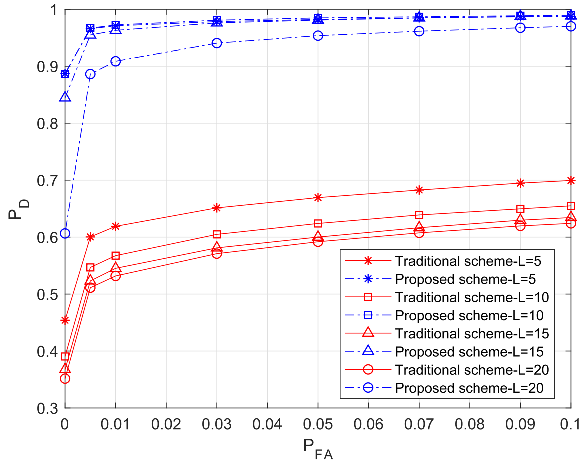


FIGURE 7. Simulated false alarm rate P_{FA} vs. P_D with different multipath conditions $L = \{5, 10, 15, 20\}$. In this example, the signal to noise ratio is SNR = 10dB; carrier frequency is 28GHz; the antenna number of transmitter and receiver is $N_t = N_r = 32$, and the number of Monte Carto simulations is 10,000.

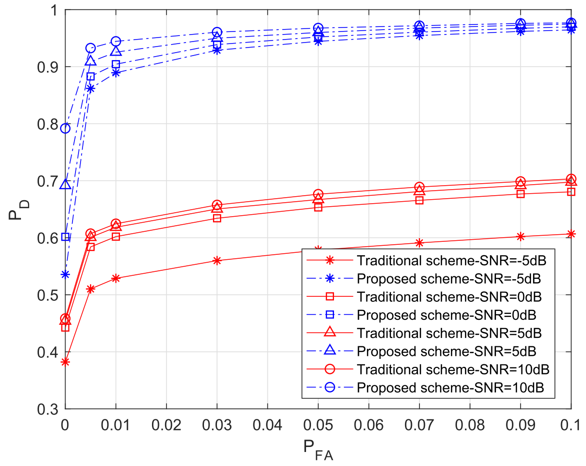


FIGURE 8. Simulated false alarm rate P_{FA} vs. P_D under different SNRs $\{-5, 0, 5, 10\}$dB. In this example, the carrier frequency is 28GHz; the multipaths condition $L = 5$; the antenna number of transmitter and receiver is $N_t = N_r = 32 \times 32$, and the number of Monte Carto simulations is 10,000.

The detection performances under different SNRs are illustrated in Fig. 8. We can see that higher SNR will result in better detection performance. Furthermore, the detection performance of the proposed scheme can achieve a good detection performance even under a lower SNR. For instance, when $SNR = -5dB$, the detection rate under the proposed scheme is higher than 90% as the false alarm rate is $P_{FA} = 0.04$, while it is lower than 60% under the traditional detection scheme. These simulation results show that the spoofing detection scheme based on PC-CVR can receive a significant boost with the help of channel virtual representation under a static radio environment.

C. MACHINE LEARNING-BASED SPOOFING ATTACK DETECTION SCHEMES

To evaluate the effectiveness of the proposed machine learning-based scheme, we consider various environment and communication conditions that may impact the detection performance, including channel correlations, SNRs, the numbers of antennas and training sample sizes. Here, the proposed one-classification detection framework is based on Section VI, i.e., SLFN-framework. While, the competition detection schemes are various popular one-class classifiers, including support vector data description (SVDD) with RBF kernel, Parzen density estimator (Parzen), linear programming data description (LPDD), k-nearest neighbor data description (KNNDD).[1]

Besides, for consistency, we consider the detection accuracy P_{DA} as a performance criterion, given by

$$P_{DA} = 1 - (P_{MD} + P_{FA}), \tag{24}$$

where $P_{MD} = 1 - P_D$ denotes the miss detection rate and P_{FA} is the false alarm rate.

1) STATIC SCENARIOS

In static scenarios, since the communication environment changes slowly, the channel correlation parameters are set to a constant when training and testing the machine learning model.

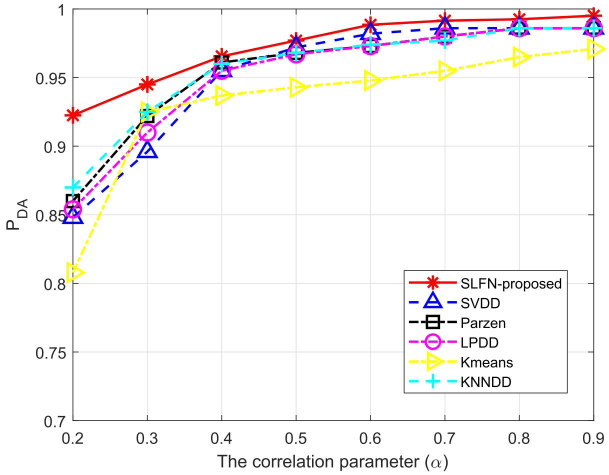


FIGURE 9. Simulated detection accuracy P_{DA} vs. channel correlation parameter α under different classifiers. In this example, the antenna numbers is $N_t = N_r = \{32 \times 32\}$ the signal to noise ratio is SNR=0dB; carrier frequency is 28GHz; the multipaths condition $L = 10$, and the number of Monte Carto simulations is 10,000.

Fig. 9 illustrates the detection performances with different channel correlation parameters α under different classifiers. We can see that the proposed scheme, i.e., SLFN-framework, shows a better performance under different channel correlation parameters than that of other classifiers. For example, when the channel correlation parameter is $\alpha = 0.2$, the detection accuracy of the SLFN-framework can reach above 90%. Under the same conditions, the detection performance of other detection classifiers is around 85%. For the higher channel correlation parameter such as $\alpha = 0.8$, the detection accuracy of all detection schemes can approximate 97%. From Fig. 9, we notice that for different channel correlations, the proposed detection scheme outperforms the other detection methods under the same training samples.

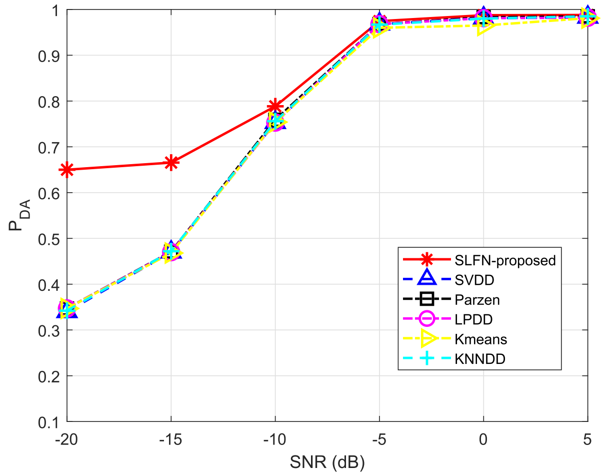


FIGURE 10. Simulated detection accuracy P_{DA} vs. SNR under different classifiers. In this example, the antenna numbers is $N_t = N_r = \{32 \times 32\}$ the channel correlation coefficient is $\alpha = 0.5$; carrier frequency is 28GHz; the multipaths condition $L = 10$, and the number of Monte Carto simulations is 10,000.

In Fig. 10, the fluctuation of detection performance under different SNRs is presented. The proposed detection scheme has a better detection performance than other schemes at a lower SNR. For instance, when SNR $=-15$dB, the detection accuracy of the SLFN-framework approximates 67%, while for other classifiers, the detection accuracy is below 50%. Meanwhile, as the SNR becomes higher such as SNR $= 0$dB, all detection schemes can have similar detection performance (the detection accuracy is around 97%). This implies that the proposed detection scheme has a better anti-noise performance.

Fig. 11 shows the training efficiency under different machine learning schemes with different training sizes of the samples. We notice that the training time of the proposed

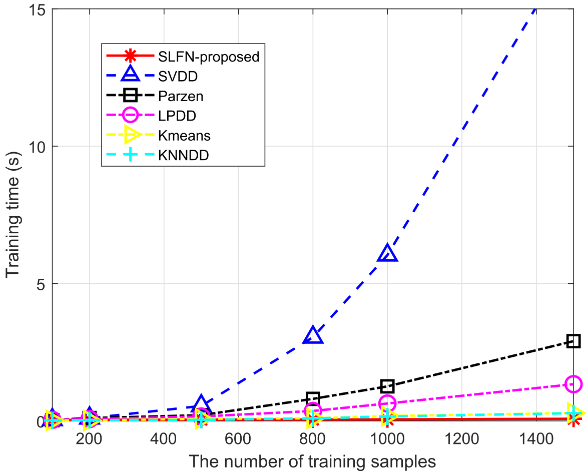


FIGURE 11. Simulated training time vs. the number of training sample under different classifiers. In this example, the antenna numbers is $N_t = N_r = \{32 \times 32\}$ the channel correlation coefficient is $\alpha = 0.5$; the carrier frequency is 28GHz; the multipaths condition $L = 7$, and the number of Monte Carto simulations is 10,000.

[1] Supported by: http://www.prtools.org

scheme does not increase significantly as the training sample size gets larger. The training time of the proposed scheme is less than 0.1s when the size of the training samples is 1500. In other words, the training time required in the presented SLFN-framework in the detection process is very short. By contrast, the other one-class classification schemes are significantly impacted by the size of the training samples, especially SVDD whose kernel is SVM.

The effect of the number of antennas on the detection performance with different classifiers is described in Fig. 12. In this simulation, we take the different numbers of antennas into account, i.e., $N_t = N_r = \{8, 16, 32, 64, 128, 256\}$. From Fig. 12, we can see that the detection performance of the proposed detection scheme with SLFN-framework is very close to that of most other detection schemes (SVDD, Parzen, LPDD, KNNDD). Meanwhile, we also notice that the presented detection scheme beats other detection schemes when the number of antennas is low. For example, when $N_t = N_r = \{8\}$, the detection accuracy of the SLFN-framework is 80%, while it is below 75% under the other detection schemes.

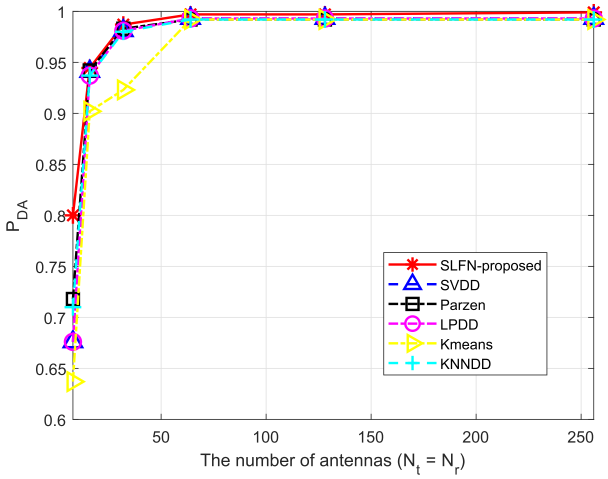


FIGURE 12. **Simulated detection accuracy P_{DA} vs. the number of antennas. In this example, SNR= 0dB; the channel correlation coefficient is $\alpha = 0.5$; the carrier frequency is 28GHz; the multipaths condition $L = 7$, and the number of Monte Carto simulations is 10,000.**

2) DYNAMIC SCENARIOS

In the dynamic scenarios, due to the changing communication environment, the training sample and the detection data in the machine learning model may come from different communication environments. For this case, we consider that the channel correlation parameters in the testing phase of the machine learning model are changing. For example, the training channel correlation coefficient is $\alpha = 0.4$, while the testing channel correlation coefficient is from $\alpha = 0.2$ to $\alpha = 0.9$.

Fig. 13 provides the detection performances with different classifiers under a dynamic radio environment. We can see that the detection accuracy of the proposed detection scheme (i.e., SLFN-framework) is stable and can reach 99% even the channel correlation parameter α is dynamically changing. It implies that the online update mechanism in SLFN-framework can adjust the classifier to adapt to the changes in the communication environment. In contrast, the detection performance of other detection methods shows a significant decrease as the channel correlation changes. Even if the channel correlation is high, for example, when $\alpha = 0.9$, the detection accuracy with these detection schemes (SVDD, Parzen, LPDD, KNNDD) is hard to reach 95%. The reason for this phenomenon is that the testing samples are gradually different from the initial training samples, and these commonly used one-class classification schemes cannot handle this case.

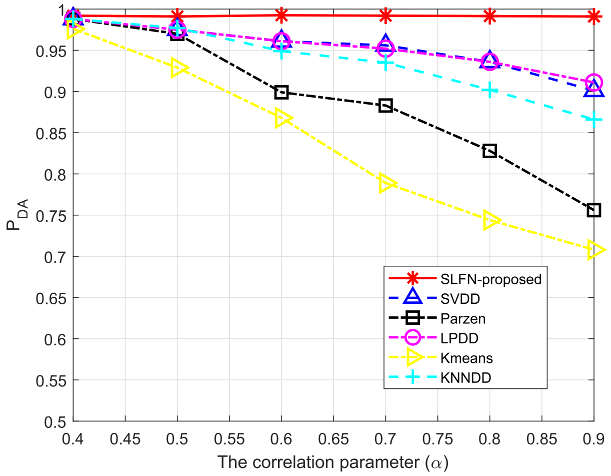


FIGURE 13. **Simulated detection accuracy with different classifiers under changing environment. In this example, the antenna numbers is $N_t = N_r = \{64 \times 64\}$; SNR= 5dB; the training channel correlation coefficient is $\alpha = 0.4$, the testing channel correlation coefficient is from $\alpha = 0.2$ to $\alpha = 0.9$; the carrier frequency is 28GHz; the multipaths condition $L = 5$, and the number of Monte Carto simulations is 10,000.**

Fig. 14 shows the detection performance under different SNRs. To simulate a dynamic radio environment, the initial training sample is based on the channel condition $\alpha = 0.4$,

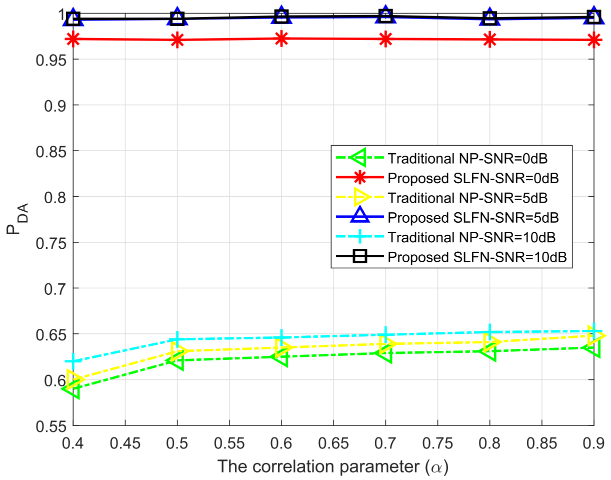


FIGURE 14. **Simulated detection accuracy with different SNRs under changing environment. In this example, the antenna numbers is $N_t = N_r = \{64 \times 64\}$; the training channel correlation coefficient is $\alpha = 0.4$, the testing channel correlation coefficient is from $\alpha = 0.2$ to $\alpha = 0.9$; the carrier frequency is 28GHz; the multipaths condition $L = 5$, and the number of Monte Carto simulations is 10,000.**

while the channel correlation coefficient for the testing samples is gradually changing from $\alpha = 0.4$ to $\alpha = 0.9$ during the detection process. The traditional detection scheme based on the NP testing is considered under this environment, where the channel features are based on Eq. (2) and the optimal threshold is assumed. We notice that higher SNR will result in better detection performance. For instance, when $SNR = 0dB$, the detection accuracy under the proposed scheme is higher than 95%, while it is lower than 70% under the traditional detection scheme.

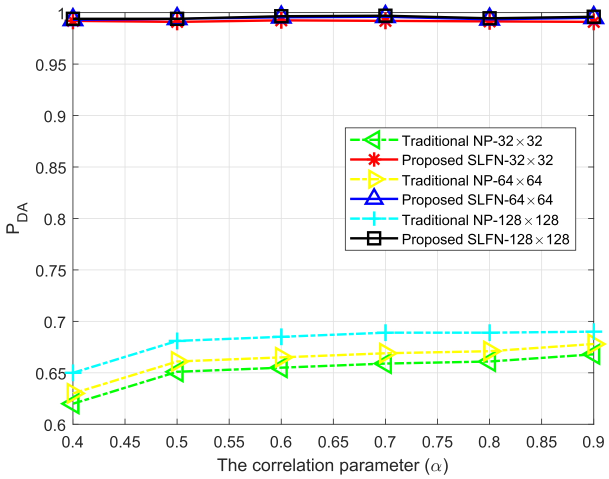


FIGURE 15. Simulated detection accuracy with different antennas under changing environment. In this example, SNR= 5dB; the training channel correlation coefficient is $\alpha = 0.5$, the testing channel correlation coefficient is from $\alpha = 0.2$ to $\alpha = 0.9$; the carrier frequency is 28GHz; the multipaths condition $L = 5$, and the number of Monte Carto simulations is 10,000.

In Fig. 15, the detection performance under the dynamic scenario with different antennas is illustrated. The training samples are based on the channel condition $\alpha = 0.5$, and the channel correlation coefficient for the testing samples is gradually changing from $\alpha = 0.4$ to $\alpha = 0.9$ during the detection process. We can see that the number of antennas can affect the detection performance of traditional schemes based on NP testing. For example, the detection accuracy under the condition of $N_t \times N_r = \{128 \times 128\}$ is higher than that of $N_t \times N_r = \{64 \times 64\}$. For the proposed method, the difference caused by the number of antennas becomes very small, and all three curves under the proposed scheme are very close. These simulation results show that the spoofing detection scheme can receive a significant boost with the help of channel virtual representation and the online SLFN framework.

Remarks: From these simulation results, we can see that: (i) Channel virtual representation can help NP testing to significantly improve the detection performance in the spoofing attack detection; (ii) Compared with these existing popular one-class classifiers, the presented SLFN-framework has remarkable advantages in detection performance, training efficiency, and anti-noise performance. With the online update mechanism, the proposed SLFN-framework scheme can tackle the change of channel correlation parameters in the dynamic radio environment.

VIII. CONCLUSION

In this paper, we provided a new channel-based spoofing attack detection scheme based on channel virtual representation in mmWave massive MIMO communications 5G networks. Resorting to the ℓ_2-norm of PC-CVR, we proposed a spoofing attack detection scheme based on NP testing for the static radio environment where the channel correlation parameter is stable. For the dynamic radio environment where the channel correlation parameter is changing, we presented a machine learning-based spoofing attack detection scheme. The problem of spoofing attack detection was transformed into a one-class classification problem, and a novel online detection scheme, i.e., SLFN-framework was proposed. Simulation results demonstrated that the detection performance of the proposed channel virtual representation based schemes obviously outperforms that of the traditional methods. The detection rate can approach 97% with 10^{-2} false alarm rate under the NP testing-based scheme in the static radio environment, while the detection rate of the traditional scheme is around 70% under the same conditions. The presented SLFN-framework is superior to existing popular one-class classifiers on training efficiency and detection performance, and the detection accuracy can reach 99% in the dynamic radio environment.

REFERENCES

[1] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, "Overview of 5G security challenges and solutions," *IEEE Commun. Standards Mag.*, vol. 2, no. 1, pp. 36–43, Mar. 2018.

[2] K. Zeng, K. Govindan, D. Wu, and P. Mohapatra, "Identity-based attack detection in mobile wireless networks," in *Proc. IEEE INFOCOM*, Apr. 2011, pp. 1880–1888.

[3] N. Wang, P. Wang, A. Alipour-Fanid, L. Jiao, and K. Zeng, "Physical-layer security of 5G wireless networks for IoT: Challenges and opportunities," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8169–8181, Oct. 2019.

[4] L. Xiao, Y. Li, G. Han, G. Liu, and W. Zhuang, "PHY-layer spoofing detection with reinforcement learning in wireless networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 12, pp. 10037–10047, Dec. 2016.

[5] Y. Wu, A. Khisti, C. Xiao, G. Caire, K.-K. Wong, and X. Gao, "A survey of physical layer security techniques for 5G wireless networks and challenges ahead," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 679–695, Apr. 2018.

[6] N. Wang, W. Li, P. Wang, A. Alipour-Fanid, L. Jiao, and K. Zeng, "Physical layer authentication for 5G communications: Opportunities and road ahead," *IEEE Netw.*, vol. 34, no. 6, pp. 198–204, Nov. 2020.

[7] X. Wang, P. Hao, and L. Hanzo, "Physical-layer authentication for wireless security enhancement: Current challenges and future developments," *IEEE Commun. Mag.*, vol. 54, no. 6, pp. 152–158, Jun. 2016.

[8] K. Zeng, K. Govindan, and P. Mohapatra, "Non-cryptographic authentication and identification in wireless networks [security and privacy in emerging wireless networks]," *IEEE Wireless Commun.*, vol. 17, no. 5, pp. 56–62, Oct. 2010.

[9] M. H. Yilmaz and H. Arslan, "A survey: Spoofing attacks in physical layer security," in *Proc. IEEE 40th Local Comput. Netw. Conf. Workshops (LCN Workshops)*, Oct. 2015, pp. 812–817.

[10] J. K. Tugnait, "Wireless user authentication via comparison of power spectral densities," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1791–1802, Sep. 2013.

[11] J. Yang, Y. Chen, W. Trappe, and J. Cheng, "Detection and localization of multiple spoofing attackers in wireless networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 1, pp. 44–58, Jan. 2013.

[12] N. Wang, J. Tang, and K. Zeng, "Spoofing attack detection in mm-wave and massive MIMO 5G communication," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, Jun. 2019, pp. 1–5.

[13] K. Zeng, "Physical layer key generation in wireless networks: Challenges and opportunities," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 33–39, Jun. 2015.

[14] K. Lounis and M. Zulkernine, "Attacks and defenses in short-range wireless technologies for IoT," *IEEE Access*, vol. 8, pp. 88892–88932, 2020.

[15] 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, Oct. 2019.

[16] F. Salahdine and N. Kaabouch, "Security threats, detection, and countermeasures for physical layer in cognitive radio networks: A survey," *Phys. Commun.*, vol. 39, Apr. 2020, Art. no. 101001.

[17] F. J. Liu, X. Wang, and S. L. Primak, "A two dimensional quantization algorithm for CIR-based physical layer authentication," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2013, pp. 4724–4728.

[18] M. A. Ferrag, L. Maglaras, S. Moschoyiannis, and H. Janicke, "Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study," *J. Inf. Secur. Appl.*, vol. 50, Feb. 2020, Art. no. 102419.

[19] B. Li, Y. Wu, J. Song, R. Lu, T. Li, and L. Zhao, "DeepFed: Federated deep learning for intrusion detection in industrial cyber-physical systems," *IEEE Trans. Ind. Informat.*, early access, Sep. 11, 2020, doi: 10.1109/TII.2020.3023430.

[20] S. M. Kasongo and Y. Sun, "A deep learning method with wrapper based feature extraction for wireless intrusion detection system," *Comput. Secur.*, vol. 92, May 2020, Art. no. 101752.

[21] G. Loukas, T. Vuong, R. Heartfield, G. Sakellari, Y. Yoon, and D. Gan, "Cloud-based cyber-physical intrusion detection for vehicles using deep learning," *IEEE Access*, vol. 6, pp. 3491–3508, 2018.

[22] A. M. Sayeed, "Deconstructing multiantenna fading channels," *IEEE Trans. Signal Process.*, vol. 50, no. 10, pp. 2563–2579, Oct. 2002.

[23] T. Kim and D. J. Love, "Virtual AoA and AoD estimation for sparse millimeter wave MIMO channels," in *Proc. IEEE 16th Int. Workshop Signal Process. Adv. Wireless Commun. (SPAWC)*, Jun. 2015, pp. 146–150.

[24] Y. Wang, Z. Tian, S. Feng, and P. Zhang, "A fast channel estimation approach for millimeter-wave massive MIMO systems," in *Proc. IEEE Global Conf. Signal Inf. Process. (GlobalSIP)*, Dec. 2016, pp. 1413–1417.

[25] N. Wang, L. Jiao, A. Alipour-Fanid, M. Dabaghchian, and K. Zeng, "Pilot contamination attack detection for NOMA in 5G mm-wave massive MIMO networks," *IEEE Trans. Inf. Forensics Security*, vol. 15, no. 5, pp. 1363–1378, Sep. 2020.

[26] N. Wang, W. Li, A. Alipour-Fanid, L. Jiao, M. Dabaghchian, and K. Zeng, "Pilot contamination attack detection for 5G mmwave grant-free IoT networks," *IEEE Trans. Inf. Forensics Security*, vol. 16, no. 19, pp. 658–670, Aug. 2021.

[27] N. Wang, L. Jiao, and K. Zeng, "Pilot contamination attack detection for NOMA in mm-wave and massive MIMO 5G communication," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, May 2018, pp. 1–9.

[28] T. S. Rappaport, S. Sun, R. Mayzus, H. Zhao, Y. Azar, K. Wang, G. N. Wong, J. K. Schulz, M. Samimi, and F. Gutierrez, "Millimeter wave mobile communications for 5G cellular: It will work!" *IEEE Access*, vol. 1, pp. 335–349, May 2013.

[29] X. Lu, Y. Zhang, Y. Peng, H. Zhao, and W. Wang, "A real-time two-way authentication method based on instantaneous channel state information for wireless communication systems," *J. Commun.*, vol. 6, no. 6, pp. 471–476, Sep. 2011.

[30] W. C. Jakes and D. C. Cox, *Microwave Mobile Communications*. Hoboken, NJ, USA: Wiley, 1994.

[31] J. A. del Peral-Rosado, R. Raulefs, J. A. Lopez-Salcedo, and G. Seco-Granados, "Survey of cellular mobile radio localization methods: From 1G to 5G," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 2, pp. 1124–1148, 2nd Quart., 2018.

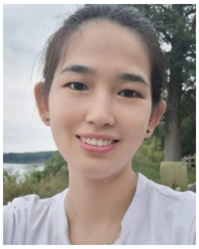
[32] R. W. Heath, N. Gonzalez-Prelcic, S. Rangan, W. Roh, and A. M. Sayeed, "An overview of signal processing techniques for millimeter wave MIMO systems," *IEEE J. Sel. Topics Signal Process.*, vol. 10, no. 3, pp. 436–453, Apr. 2016.

[33] A. M. Sayeed and V. Raghavan, "Maximizing MIMO capacity in sparse multipath with reconfigurable antenna arrays," *IEEE J. Sel. Topics Signal Process.*, vol. 1, no. 1, pp. 156–166, Jun. 2007.

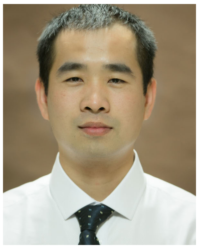
[34] H. L. Van Trees, *Detection, Estimation, Modulation Theory, Part I: Detection, Estimation, Linear Modulation Theory*. Hoboken, NJ, USA: Wiley, 2004.

[35] N.-Y. Liang, G.-B. Huang, P. Saratchandran, and N. Sundararajan, "A fast and accurate online sequential learning algorithm for feedforward networks," *IEEE Trans. Neural Netw.*, vol. 17, no. 6, pp. 1411–1423, Nov. 2006.

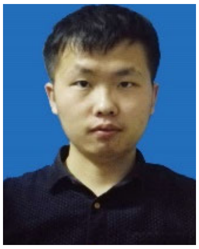
[36] A. Alkhateeb, O. El Ayach, G. Leus, and R. W. Heath, Jr., "Channel estimation and hybrid precoding for millimeter wave cellular systems," *IEEE J. Sel. Topics Signal Process.*, vol. 8, no. 5, pp. 831–846, Oct. 2014.



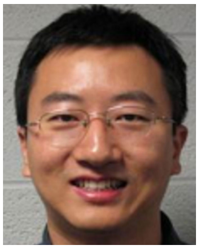
WEIWEI LI received the Ph.D. degree in information and communication engineering from the Beijing University of Post and Telecommunication, in 2015. She is currently an Assistant Professor with the Department of Information and Electrical Engineering, Hebei University of Engineering. Her current research interests include physical layer security, 5G wireless networks, compressed sensing, and privacy of vehicle-to-vehicle communication.



NING WANG (Member, IEEE) received the Ph.D. degree in information and communication engineering from the Beijing University of Post and Telecommunication, in 2017. He was an Engineer with Huaxin Post and Telecommunications Consulting Design Company Ltd., from 2012 to 2013. He was with the Department of Electrical and Computer Engineering, George Mason University, as a Postdoctoral Scholar, from 2017 to 2020. He is currently a Professor with the College of Computer Science, Chongqing University. His current research interests include physical layer security, machine learning, RF fingerprinting, and cyber-physical system security and privacy.



LONG JIAO (Graduate Student Member, IEEE) received the B.Sc. degree in information security from Xidian University (XDU), in 2016. He is currently pursuing the Ph.D. degree with George Mason University. Since 2016, he has been with George Mason University. His current research interests include 5G physical layer security, mmWave communication, mmWave HetNet, and deep learning.



KAI ZENG (Member, IEEE) received the Ph.D. degree in electrical and computer engineering from Worcester Polytechnic Institute (WPI), in 2008. He was a Postdoctoral Scholar with the Department of Computer Science, University of California at Davis (UCD), from 2008 to 2011. He was with the Department of Computer and Information Science, University of Michigan-Dearborn, as an Assistant Professor, from 2011 to 2014. He is currently an Associate Professor with the Department of Electrical and Computer Engineering, Cyber Security Engineering, and the Department of Computer Science, George Mason University. His current research interests include cyber-physical system security and privacy, 5G physical layer security, network forensics, and spectrum sharing networks. He was a recipient of the U.S. National Science Foundation Faculty Early Career Development (CAREER) Award, in 2012, the Excellence in Postdoctoral Research Award from UCD, in 2011, and the Sigma Xi Outstanding Ph.D. Dissertation Award from WPI, in 2008. He is an Editor of the IEEE Transactions on Information Forensics and Security, IEEE Transactions on Wireless Communications, and IEEE Transactions on Cognitive Communications and Networking.