Efficient Identity Spoofing Attack Detection for IoT in MmWave and Massive MIMO 5G Communication

Ning Wang, Long Jiao, Pu Wang, Monireh Dabaghchian, Kai Zeng
Department of Electrical and Computer Engineering
George Mason University, Fairfax, VA, US 22030
E-mail: {nwang5, ljiao, pwang20, mdabaghc, kzeng2}@gmu.edu

***Abstract*—In many IoT (Internet-of-Things) applications, a large number of low-cost IoT devices are connected to the Internet through an access point (AP) or gateway via wireless communication. Due to the resource constraints on IoT devices and broadcast nature of wireless medium, identity spoofing attacks are easy to launch but hard to defend in an IoT wireless access network. In this paper, under the context of 5G communication, we propose an efficient physical layer identity spoofing attack detection scheme for IoT. By harnessing the sparsity of the virtual channel in mmWave and Massive MIMO 5G communication, we propose a two-step detection scheme. In the first step, our scheme detects anomalies by examining the virtual angles of arrival (AoA) and path gains of all the IoT devices simultaneously in a virtual channel space (VCS). In the second step, we introduce a machine learning based detection scheme to detect the actual attack. Simulation results evaluate and confirm the effectiveness of the proposed detection scheme. The minimum Bayes risk of the proposed scheme can be less than 0.5% even in the presence of 100 IoT devices.**

***Index Terms*—Physical layer security, IoT security, Spoofing detection, Virtual channel, mmWave Massive MIMO, 5G**

I. Introduction

With the rapid advancement of embedded systems and wireless communication technologies, a massive amount of small and cheap computing devices with sensing and communication capabilities are being connected to the Internet in support of various IoT (Internet-of-Things) applications, including smart home, smart transportation, healthcare, smart factories, etc [1]. IoT devices usually rely on wireless communication as the first hop to access to the Internet. Due to the open medium nature of the wireless channel and severe resource constraints on many IoT devices, securing wireless IoT systems faces great challenges [2].

Identity spoofing attacks are easy to launch in an IoT access network. By using a faked identity such as the MAC (media access control) or IP (internet protocol) address of the legitimate user, an identity spoofing attacker can claim to be another legitimate IoT device. The attacker can then gain illegal access to the IoT network and launch more advanced attacks, such as man-in-the-middle attacks and denial-of-service attacks [3].

Existing countermeasures to detect identity spoofing attacks include cryptography based schemes and physical layer based mechanisms. Nevertheless, it is challenging to implement strong cryptography based authentication schemes on resource-constrained IoT devices. Even when traditional cryptographic means are feasible, IoT devices are subject to physical compromises in an adversarial environment. Any unprotected keying materials used for authentication stored on the device may be compromised through physical attacks, which will diminish the strength of the cryptography-based mechanisms [3].

Complementing with the cryptography based authentication, physical layer authentication/identification technologies have been proposed [4], [5]. These mechanisms detect identity spoofing attacks by exploiting wireless physical layer characteristics, such as received signal strengths (RSS) [6], channel impulse responses [7], channel frequency responses [8], etc. Most existing physical layer authentication schemes tackle static cases, and a database of trained signal/channel fingerprint is usually required [3]. A channel-assisted authentication scheme in mobile networks authenticates consecutive frames, based on the assumption that the frame interval is within channel coherent time [8]. Furthermore, existing physical-layer spoofing attack detection schemes detect attackers one by one. It is hard to achieve fast and efficient detection when faced with a large number of legitimate users (LUs) in IoT applications.

In this paper, we propose a new identity spoofing attack detection scheme under the context of mmWave and massive MIMO 5G communication, where the simultaneous detection of all the attackers in an IoT access network can be achieved by one detection process. Furthermore, this detection scheme does not require the frame interval to be within the channel coherence time nor a trained database of signal/channel fingerprint. It can tackle both static and dynamic cases. In this study, inspired by the distinguishability and sparsity of the mmWave massive MIMO virtual channel, we present a two-step detection scheme to detect identity spoofing attacks. By extracting the largest path gain in the virtual channel, we first establish a virtual channel space (VCS) to detect whether there is an anomaly among a large number of users. Then, by exploiting the sparsity of the full virtual channel, we use a machine learning based scheme to further decide whether these anomalies are introduced by spoofing attacks. Simulation results show that our proposed detection scheme can reach a remarkable detection performance. The Bayes risk can be less than 0.5% even in the scenario of 100 LUs.

The contributions of this paper lie in three aspects: (1) We propose a novel identity spoofing detection scheme, in which attackers can be detected simultaneously even when there is a large number of users; (2) We introduce the sparsity of virtual channel in mmWave communication to distinguish the large number of LUs; (3) We present a two-step detection scheme to achieve the spoofing attack detection, where a VCS and a machine learning based detection scheme are proposed.

In the remainder of this article, we first introduce the related work in Section II; then the system model is given in Section III; Section **??** presents the proposed two-step detection scheme; Section VI provides the simulation results, and finally Section VII concludes this paper.

II. Related work

A. Physical-layer authentication/identification

Recently, a variety of physical layer authentication/identification schemes have been proposed by exploiting the properties of wireless channels, including received signal strength (RSS) [6], channel state information (CSI) [9], channel impulse responses (CIR) [8], power spectral density (PSD) [10], and channel power-delay profile (PDP) [11]. Most existing physical-layer authentication techniques use hypothesis tests to compare the radio channel information with the record in a trained signal/channel fingerprint database to detect identity spoofing attackers. In contrast to the existing physical-layer authentication schemes, in this paper, we introduce a new physical layer feature, i.e., the sparsity of virtual channel under the mmWave Massive MIMO, to distinguish between legitimate users and identity spoofing attackers.

B. Virtual channel

Virtual channel was first discussed in [12] and has been applied in mmWave and MIMO communication, which have been recognized as two key enabling technologies for fifth-generation mobile networks (5G) [13]. The virtual channel model is based on virtual angle-of-arrival (AoA) and virtual angle-of-departure (AoD). This channel model can be seen as a mapping of the real channel in a special space, and the estimation of virtual channel can be fast obtained [14]. Furthermore, when the number of antennas is large enough, the virtual channel matrix will present sparseness, especially under massive MIMO scenario. Supported by mmWave communication, the tiny wavelengths allow tens to hundreds of antenna elements to be placed in an array on a relatively small physical platform [15]. As a result, the integration of massive MIMO and mmWave presents unique properties, for instance, sparsity and time-varyingness in the virtual channel. We propose to leverage these properties to achieve an efficient identity spoofing detection in this study.

III. System model and motivation

In this section, the communication system model and the threat model are given, besides the motivation of this work is introduced.

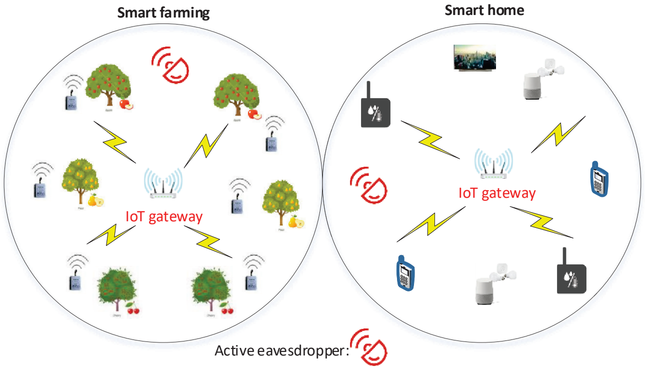

Fig. 1: IoT application scenarios: Smart farm and smart home.

A. IoT communication model

We consider an IoT wireless access network in typical IoT application scenarios, e.g., smart farm and smart home, as illustrated in Fig. 1. In these scenarios, a large number of low-cost IoT devices are connected to a gateway node (i.e., AP) through wireless communication. Under the context of 5G communication, we assume the gateway node is a relatively powerful device equipped with a large number of antennas in support of mmWave and massive MIMO communication. Moreover, the IoT devices are resource-constrained with single antenna and limited computation power. They can be either static or mobile.

B. Attack model

We assume there are one or multiple attackers, who can impersonate one or multiple LU victims by falsifying their identities (e.g, MAC addresses) as the LU victims'. In the case of the transmission phase between transceivers, the spoofing attacker can transmit the deceiving signal with a higher power to the receiver [16]. The attackers may use the same type of devices as the victims, but they cannot be at the same location as the victims. The attackers may already compromise the secret keys of the victims, so cryptography-based authentication may not work. The attackers can be either static or mobile.

C. Motivation

Inspired by the directionality of mmWave, the LUs in an IoT wireless access network can be differentiated by the characteristics of the virtual channel. Furthermore, this virtual channel presents significant sparsity under a certain number of users. Thus, we can count all of the LUs in an IoT communication by examining the characteristics of the virtual channel, simultaneously. In other words, we can count all LUs at the same time. In addition, the virtual channel estimation and the corresponding signal processing are conducted in AP. There is no change or any extra computation/communication required on IoT devices, which makes it suitable for low-cost IoT applications.

IV. Spoofing detection based on virtual channel and challenges

In this section, we present a virtual channel space (VCS) to represented different LUs at AP, and introduce two challenges when using VCS to achieve spoofing detection.

A. VCS

Consider an IoT mmWave system, where an access point (AP) with a multi-antenna array communicates with K users with a single antenna. Based on the geometry channel model with L scatters formed by ray tracing, a sparse multipath structure of mmWave can be represented by a discrete physical model [12]. For the IoT system, the channel between the AP and the k^{th} user can be expressed as the sum of L paths in the form

$$\mathbf{H}^{(k)} = \sqrt{\frac{N_r}{\rho}} \sum_{l=1}^{L} \beta_l \mathbf{a}_r(\theta_l), \tag{1}$$

where ρ is the average path loss, β_l represents the fading coefficient of the $l-$th propagation path, $\theta_l \in [-\pi/2, \pi/2]$ denotes the angles of arrival (AoA). The number of antennas of AP is N_r, and the vector $\mathbf{a}_r(\theta_l)$ indicates the response array for receiving antenna arrays.

The virtual channel can be obtained from the fixed virtual receive directions at AP, that is

$$\mathbf{H}^{(k)} = U_o \mathbf{H}_V^{(k)}, \tag{2}$$

where $\mathbf{U}_o$ is a unitary discrete Fourier transform (DFT) matrix, i.e., $\mathbf{U}_o^H \mathbf{U}_o = \mathbf{U}_o \mathbf{U}_o^H = \mathbf{I}$, and the columns of $\mathbf{U}_o$ are steering vectors corresponding to n fixed spatial angles with uniform spacing $\Delta\theta_o = 1/n$. $\mathbf{H}_V^{(k)}$ is the virtual channel vector whose entries capture the gains of the corresponding paths. Fig.2(a) shows an example of virtual channel for an LU. We can see that there are several large path gains with different virtual AoA.

AP is able to use the virtual channel to represent the channel of different LUs. Here we consider $n = N_r$, and the fixed spatial angles with uniform spacing $\Delta\theta_o = 1/N_r$ can be seen as virtual AoA.

Definition 1: We define a two-dimensional matrix $\mathbf{S}_{VCS}$ as the VCS, which consists of the largest path gain of virtual channel and the corresponding virtual AoA.

Based on Definition 1, different LUs can be mapped into VCS, simultaneously. For instance, Fig. 2(b) gives an example of VCS with 128 antennas, where 21 LUs can be separated in VCS with different virtual AoA and different path gains. VCS can show the number of LUs at the physical layer, in which spoofing attacker is hard to imitate LU. However, we notice that there are some issues to use VCS to achieve a desirable detection, and two main challenges are illustrated as follow.

B. Challenges

Although LUs can be represented by VCS, we found that there are two challenges to use VCS as a desirable spoofing detection at AP.

1) *Multiple LUs are incorrectly represented as one LU in VCS.* Although the VCS can distinguish the different virtual channels corresponding to different LUs, it is possible that two LUs have the closed path gain while the virtual AoA is similar. If the distances between AP and an LU is equal to the distance between other LUs and AP, it is possible the path gains of these LUs are closed in VCS. At the same time, if their virtual AoA are also closed, these LUs may be incorrectly recognized as one LU represented by VCS. Since as the number of antennas at AP is small, VCS is unable to distinguish the difference between these LUs. Thus, there will be ”overlap” for multiple LUs in VCS, and that will mislead AP to count the number of LUs at physical layer.

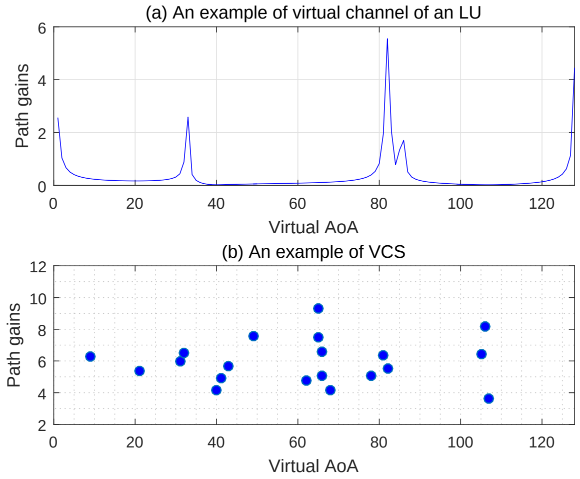

Fig. 2: Virtual channel for an LU and VCS for 21 LUs. (AP with 128 antennas).

2) *An LU is incorrectly represented as Multiple LUs in VCS.* If the transmission paths between AP and LU is line-of-sight (LOS), the LOS path has the largest path gain than other non-line-of-sight (NLOS) path component [17]. However, in the case of NLOS, we found that multiple NLOS paths have the closed path gains with the different virtual AoA, which will be incorrectly represented as multiple LUs in VCS at AP. This phenomenon will confuse AP to count the number of LUs.

Figure 3 shows an example of the probability of integrating these two issues illustrated above. In Fig. 3(a), we can see that the probability of representing multiple LUs as one LU is significantly reduced when the number of antennas is increased. Moreover, it is obvious that the overall probability is lower than 1% even under the condition of 100 LUs with 28 antennas at AP. It implies that the probability of ”overlap” for multiple LUs is very low. Fig. 3(b) illustrates the probability of representing one LU as multiple LUs in VCS. We can see that the probability is approximately 40% under the condition of 100 LUs with 28 antennas. It suggests that the issue that an LU is incorrectly represented as multiple LUs is not a small probability event. Therefore, we need a further step to achieve a desirable spoofing detection based on VCS.

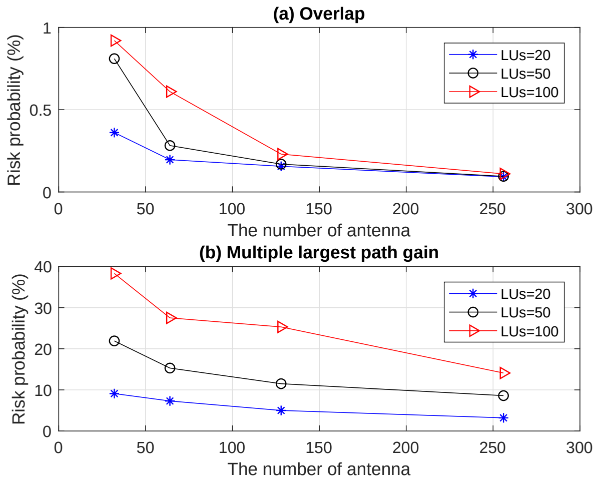

Fig. 3: The probability of the possible issues for VCS. (a) Multiple LUs are represented as one LU in VCS; (b) An LU is represented as Multiple LUs inVCS.

V. Detection strategy

In this section, we present a two-step detection strategy based on the machine learning algorithm to handle the possible issues analyzed above.

A. Two-step detection strategy

Based on VCS, we propose a two-step strategy to achieve the spoofing attacks for IoT. The first step is the anomaly detection of all users, and the second step is to check whether this anomaly is a spoofing attack or not.

Without loss of generality, we assume that the receiver can obtain M signals at each time slot, and the proposed two-step detection scheme is described in Algorithm 1 below.

- **Step 1: Detection based on VCS**.
  By broadcast channel, AP asks all of the users to send their pilot sequence. AP can extract LUs' MAC (or IP) addresses, which present all users who want to connect AP in the MAC layer. Here, the number of different MAC addresses is denoted as N_{MAC}. After channel estimation, all users can be represented by VCS in the physical layer, and the number of LUs in VCS is denoted as N_{PL}. Thus, AP can obtain three possible results: $N_{MAC} > N_{PL}$, $N_{MAC} < N_{PL}$ and $N_{MAC} = N_{PL}$. When $N_{MAC} \geq N_{PL}$, the communication situation can be considered as a normal case. In contrast, as $N_{MAC} < N_{PL}$, the communication situation will be seen as an anomaly. Hence, we have

$$\begin{cases} N_{MAC} \geq N_{PL} & Normal, \\ N_{MAC} < N_{PL} & Anomaly. \end{cases} \tag{3}$$

- **Step 2: Machine learning based detection**.
  If there is an anomaly alarm in step 1, we need to further investigate whether this anomaly is a spoofing attack or not. Based on the observation that virtual channel is distinct between spoofing attack and normal communication, we use the sparsity and the sum of the path gains of the virtual channel as two features to achieve this detection.

Algorithm 1 Two-step spoofing detection algorithm

```
Initialization: Training size $T_{num}$.
Repeat (for each episode)
AP obtains the training data.
Train MLM based on the training data.
    For $t = 1, 2, ...M$(for each signal)
  Step 1:
    AP receives the messages from LUs.
    AP estimates the channel for each LU and map the virtual channel into VCS.
      Compare $N_{MAC}$ with $N_{PL}$.
        If $N_{MAC} \geq N_{PL}$
          Current communication is normal.
          Break
        Else
          Jump to Step 2.
        End If
  Step 2:
      Calculate the features $F_S(H_V)$ and $F_E(H_V)$ via (4) and (5).
      Calculate the predictive value based on MLM.
        If $q(\mathbf{x}) = 1$
          Current communication is normal.
        Else
          Raise alarm.
        End If
    End for
End
```

After normalization, the sparsity of the virtual channel can be illustrated by a sparse metric of a matrix, i.e.,

$$F_S(\mathbf{H}_V) = \| |\mathbf{H}_V| \|_0, \tag{4}$$

where $\| \cdot \|_0$ means ℓ_0-norm, and $| \cdot |$ means module. Then, the sum of the path gains in virtual channel can be given by

$$F_E(\mathbf{H}_V) = \sum_{i=1}^{j} G_i, \tag{5}$$

where G_i is the nonzero path gain in $|H_V|$, and j indicates the number of nonzero path gains.

Thus, we can use a simple machine learning algorithm to identify the attack situation based on F_E and F_S. Let $TR_{XY} = \{(\mathbf{x}_1, y_1), ..., (\mathbf{x}_l, y_l)\}$ be a set of training vectors, $\mathbf{x}_i \in \mathbb{R}^n$, and the corresponding hidden states $y \in \Psi = \{1, 2\}$. The binary classifier uses the discriminant function, i.e., $f : \chi \subseteq \mathbb{R}^n \rightarrow \mathbb{R}$, to train a corresponding machine learning model (MLM). If there is a set of testing vectors, $TE_X = \{\widehat{\mathbf{x}}_1, ..., \widehat{\mathbf{x}}_k\}$, based on the MLM, we can give the predictive value, i.e., $\{\widehat{y}_1, .., \widehat{y}_k\}$. Then the binary classification rule, i.e., $q : \chi \rightarrow \Psi = \{1, 2\}$, can be defined as

$$q(\widehat{\mathbf{x}}_k) = \begin{cases} \widehat{y}_k = 1, & Normal\,case, \\ \widehat{y}_k = 2, & Attack\,case. \end{cases} \tag{6}$$

B. Obtain training data

Most of the traditional spoofing detection schemes are a threshold based segmentation solution, such as Neyman-Pearson testing [8], in which a suitable threshold is selected to distinguish spoofing cases from normal cases. Moreover, it is necessary to analyze the statistical model of features and give a default false alarm rate. In contrast, machine learning based classification scheme is a data-driven solution, where an appropriate set of training data can train a suitable classification model. It does not need the knowledge of the statistical model and a given false alarm rate. Here, considering the low complexity and good performance for the small size of samples, we use the logistic regression algorithm as the machine learning algorithm.

Furthermore, for a spoofing attack detection, how to obtain a set of suitable training data is a problem. In general, the training data for the normal case is relatively easy to be obtained. However, because the attackers are unknown and unpredictable, it is difficult for AP to accurately obtain the training data for the spoofing attack case. Therefore, to solve this problem, we present a pseudo attacker model to help AP to acquire an integrated training data set. The pseudo attacker model is presented by Definition 2, followed by Lemma 1.

Definition 2: (Pseudo attacker model): For a MAC address, if there is one transmitter in normal communication, we define that a pseudo attacker model has two transmitters.

Lemma 1: Let a denote the number of transmitters for one MAC address, and let $\mathbf{H}_{V,N}$ and $\mathbf{H}_{V,A}$ indicate the virtual channels under normal case and spoofing attack case, respectively. Based on definition 2, for the normal case, $a = 1$ and the corresponding feature of virtual channel can be illustrated as $\mathbf{F}_S(\mathbf{H}_{V,N})$ and $\mathbf{F}_E(\mathbf{H}_{V,N})$. While, for training data model, $a = 2$ and the corresponding feature of virtual channel can be illustrated as $\mathbf{F}_S(\mathbf{H}_{V,A})$ and $\mathbf{F}_E(\mathbf{H}_{V,A})$. We have that $\mathbf{F}_S(\mathbf{H}_{V,A})$ can be obtained by $\mathbf{F}_S(\mathbf{H}_{V,N})$, and $\mathbf{F}_E(\mathbf{H}_{V,A})$ can be obtained by $\mathbf{F}_E(\mathbf{H}_{V,N})$.

Proof 1: First, we consider that $\mathbf{F}_S(\mathbf{H}_{V,A})$ can be determined by $\mathbf{H}_{V,N}$. According to Definition 2, $\mathbf{H}_{V,A}$ has more than one transmitter compared with normal case $\mathbf{H}_{V,N}$. Therefore, if we can obtain the training data for $a = 1$ and extract the corresponding features, i.e., $\mathbf{F}_S(\mathbf{H}_{V,N})$ and $\mathbf{F}_E(\mathbf{H}_{V,N})$, it is easy to build a feature for two transmitters. Let $f_N \in \mathbf{F}_S(\mathbf{H}_{V,N})$ and $f_A \in \mathbf{F}_S(\mathbf{H}_{V,A})$. The probability distribution of f_N can approximate a normal distributions, i.e., $\mathbf{f}_N \sim N_t(\mu_1, {\sigma_1}^2)$. We have $f_A = 2f_N$, and $\mathbf{f}_A \sim N_t(2\mu_1, 4{\sigma_1}^2)$. Thus, $\mathbf{F}_E(\mathbf{H}_{V,A})$ can be determined by $\mathbf{H}_{V,N}$. The analysis of $\mathbf{F}_E$ is similar to that of $\mathbf{F}_S$.

Moreover, based on the pseudo attacker model, the MLM can handle the situation of more than two spoofing attackers. When $a > 2$, there will be more multipaths than that of $a = 2$. It is obvious that the corresponding features of virtual channel as $a > 2$, are closer to pseudo attacker model, i.e., $a = 2$, compared with the normal case, i.e., $a = 1$.

VI. Simulation Results

In this section, we present the simulation results to evaluate the validity of the proposed detection scheme.

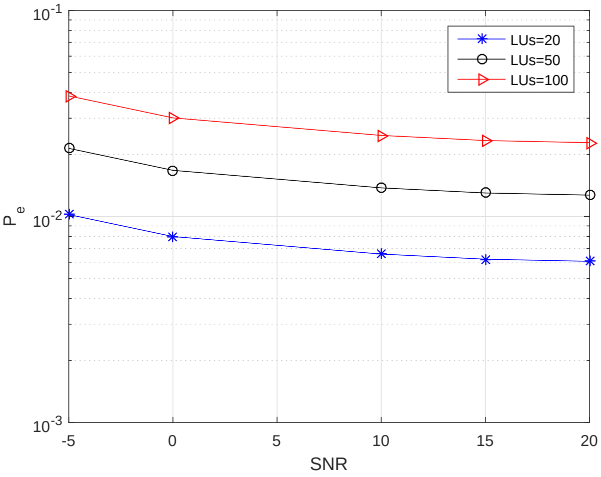

Fig. 4: Minimum Bayes risk VS. SNR under different LUs. In this example, the training and the testing size are 1000; the antenna number is 64; the carrier frequency is 28GHz.

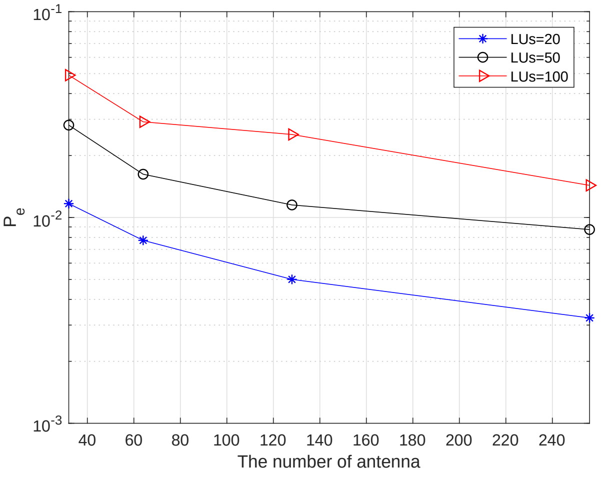

Fig. 5: Minimum Bayes risk VS. the number of antenna under different LUs. In this example, the training size is 1000; the SNR=10dB; the carrier frequency is 28GHz.

Without loss of generality, we consider the physical AoA, i.e., $\phi_{r,l}$ are randomly generated as uniform distribution in $(0, 2\pi)$, and the precision of path gain is about two decimal places. Moreover, we consider different numbers of LUs, i.e., $LUs = \{20\,50\,100\}$, signal to noise ratio $SNRs = \{-5\,0\,5\,10\,15\,20\}$, different number of antennas $N_r = \{28\,56\,128\,256\}$, and different sizes of training data $T_{num} = \{100\,250\,500\,1,000\,1,500\,2,000\}$.

Moreover, for consistency, we consider the minimum Bayes risk P_e as a performance metric, given by

$$P_e = \min(P_{MD} + P_{FA}), \tag{7}$$

where P_{MD} denotes the miss detection rate and P_{FA} is the false alarm rate.

Figure 4 illustrates the impact of SNR under different

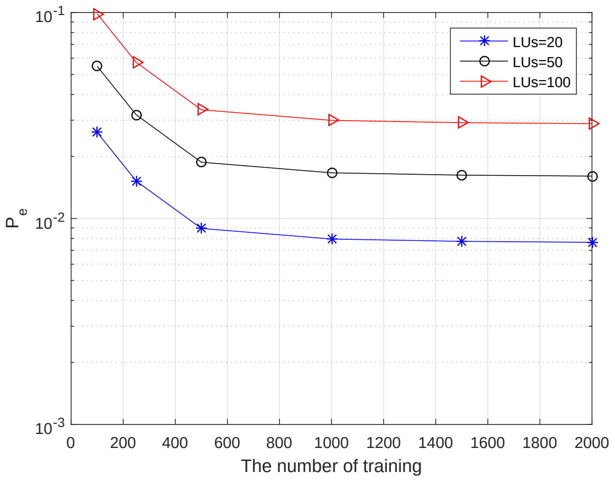

Fig. 6: Minimum Bayes risk VS. the training size under different numbers of LUs. In this example, the SNR=10dB; the antenna number is 64; the carrier frequency is 28GHz.

numbers of IoT users. We can see that as SNR increases, the P_e slowly decreases. Especially, the proposed scheme shows a good detection performance even at a low SNR. For instance, when SNR is -5dB, the P_e is 10^{-2} as the number of LUs is 20. Moreover, the influence of SNR for detection performance will reduce as SNR increase such as all curves become flat when SNR is higher than 10dB.

The detection performance is shown in Fig. 5 under different antenna numbers and different numbers of LUs. We can see that all of the curves are descending as the number of antennas increases. We also notice that when the number of antennas reaches 256, the P_e reaches 10^{-2} when LUs=50. Increasing the number of antennas can improve the detection performance. It suggests that a large number of antennas in AP results in a greater space of VCS, which will enhance the detection performance.

Figure 6 shows the detection performance under different training sizes with different numbers of LUs. We can see that for the training sizes smaller than 600, all the curves are sharply declining. When the training size is increased, the detection performance is improved. While, when the training data size is larger than 1,000, all curves become flat. It implies that increasing training data size can improve the detection performance in a certain range (when the training data size is less than 600). On the other hand, it also indicates that the proposed authentication scheme does not need a large number of training data.

VII. Conclusion

In this paper, we investigated spoofing attack detection in the presence of a large number of low-cost IoT devices. Based on the virtual channel in mmWave massive MIMO 5G communication, a two-step detection scheme was proposed, where a VCS was established and a machine learning based detection strategy was introduced. Simulation results demonstrated the effectiveness of the proposed scheme. The minimum Bayes risk of the proposed spoofing detection can be lower than 0.5% in the condition of 100 IoT devices.

References

[1] M. R. Palattella, M. Dohler, A. Grieco, G. Rizzo, J. Torsner, T. Engel, and L. Ladid, "Internet of things in the 5g era: Enablers, architecture, and business models," *IEEE Journal on Selected Areas in Communications*, vol. 34, no. 3, pp. 510–527, 2016.

[2] A. Costanzo and D. Masotti, "Energizing 5g: Near-and far-field wireless energy and data trantransfer as an enabling technology for the 5g iot," *IEEE Microwave Magazine*, vol. 18, no. 3, pp. 125–136, 2017.

[3] K. Zeng, K. Govindan, and P. Mohapatra, "Non-cryptographic authentication and identification in wireless networks [security and privacy in emerging wireless networks]," *IEEE Wireless Communications*, vol. 17, no. 5, 2010.

[4] L. Xiao, Y. Li, G. Han, G. Liu, and W. Zhuang, "Phy-layer spoofing detection with reinforcement learning in wireless networks," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 12, pp. 10 037–10 047, 2016.

[5] B. Chang, G. Zhao, Z. Chen, and J. Dan, "Detecting phy-layer spoofing attack in wireless networks," in *Globecom Workshops (GC Wkshps), 2017 IEEE*. IEEE, 2017, pp. 1–6.

[6] J. Yang, Y. Chen, W. Trappe, and J. Cheng, "Detection and localization of multiple spoofing attackers in wireless networks," *IEEE Transactions on Parallel and Distributed systems*, vol. 24, no. 1, pp. 44–58, 2013.

[7] F. J. Liu, X. Wang, and H. Tang, "Robust physical layer authentication using inherent properties of channel impulse response," in *Military Communications Conference, 2011-MILCOM 2011*. IEEE, 2011, pp. 538–542.

[8] L. Xiao, A. Reznik, W. Trappe, C. Ye, Y. Shah, L. Greenstein, and N. Mandayam, "Phy-authentication protocol for spoofing detection in wireless networks," in *Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE*. IEEE, 2010, pp. 1–6.

[9] 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," *Journal of communications*, vol. 6, no. 6, pp. 471–476, 2011.

[10] J. K. Tugnait, "Wireless user authentication via comparison of power spectral densities," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 1791–1802, 2013.

[11] W.-L. W. Chin, T. N. Le, and C.-L. Tseng, "Authentication scheme for mobile ofdm based on security information technology of physical layer over time-variant and multipath fading channels," *Information Sciences*, vol. 321, pp. 238–249, 2015.

[12] A. M. Sayeed, "Deconstructing multiantenna fading channels," *IEEE Transactions on Signal Processing*, vol. 50, no. 10, pp. 2563–2579, 2002.

[13] T. Kim and D. J. Love, "Virtual aoa and aod estimation for sparse millimeter wave mimo channels," *2015 IEEE 16th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, pp. 146–150, 2015. [Online]. Available: ¡Go to ISI¿: WOS:000380547100030

[14] Y. Wang, Z. Tian, S. Feng, and P. Zhang, "A fast channel estimation approach for millimeter-wave massive mimo systems," in *Signal and Information Processing (GlobalSIP), 2016 IEEE Global Conference on*. IEEE, 2016, pp. 1413–1417.

[15] 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, 2013.

[16] M. H. Ylmaz and H. Arslan, "A survey: Spoofing attacks in physical layer security," in *Local Computer Networks Conference Workshops (LCN Workshops), 2015 IEEE 40th*. IEEE, Conference Proceedings, pp. 812–817.

[17] A. Sayeed and J. Brady, "Beamspace mimo for high-dimensional multiuser communication at millimeter-wave frequencies," in *Global Communications Conference (GLOBECOM), 2013 IEEE*. IEEE, Conference Proceedings, pp. 3679–3684.