How to Leverage Double-Structured Sparsity of RIS Channels to Boost Physical-Layer Authentication

Amira Bendaimi, Asmaa Abdallah, *Member, IEEE*, Abdulkadir Celik, *Senior Member, IEEE*, Ahmed M. Eltawil, *Senior Member, IEEE*, and Hüseyin Arslan, *Fellow, IEEE*

***Abstract*—Reconfigurable Intelligent Surfaces (RIS)-assisted systems are promising technology in next-generation wireless networks, but are susceptible to spoofing attacks due to their broadcast nature. This letter reveals the unique characteristics of RIS-aided multiple-input multiple-output (MIMO) systems, that improve channel entropy compared to conventional MIMO. By capitalizing on the additional paths introduced by the cascaded channel and the distinctive double-structured sparsity inherent in its virtual representation, we develop a novel channel-based physical layer authentication (PLA) approach. In particular, we construct a robust signature for authentication purposes by extracting the intrinsic RIS features of the virtual angle of arrivals and departures indices. Furthermore, the distribution of the digital signature is analyzed to derive analytical expressions for the false alarm and detection probabilities of the proposed scheme. Simulation results show that the proposed approach surpasses the limitations of previous works, with 14.89% and 72% authentication performance improvements in detection and false alarm rates, respectively.**

***Index Terms*—RIS, physical layer authentication, channel sparsity, spoofing attack, security.**

I. Introduction

WIRELESS communication has undergone remarkable advancements in terms of data rate, reliability, and capacity. These strides have been primarily facilitated by the adoption of MIMO systems, millimeter wave (mmWave) technology, and reconfigurable intelligent surfaces RISs [1]. Among these, RIS emerges as a groundbreaking innovation for future wireless networks thanks to its high array gain, cost-effectiveness, and energy-efficient operation. RIS technology is poised to significantly extend signal coverage, augment system capacity, and enhance the overall efficiency of wireless networks [2]. However, the challenge of security poses a critical concern in wireless systems, primarily due to the open and broadcast nature of the shared medium, which introduces various security vulnerabilities, such as eavesdropping, impersonation and spoofing attacks [3]. RIS has recently emerged as a potential technology in bolstering physical layer security (PLS) against eavesdropping attacks, where various schemes for secret key generation using RIS have been proposed by constructing a time-varying channel environment [4], [5], [6] by introducing artificial randomness to boost secret key rate (SKR) in static environments. Nevertheless, the considerable potential of RIS for PLA has not garnered an equivalent level of research focus. PLA has emerged as an additional security measure to complement conventional cryptography-based techniques, offering cost-effective and lightweight security solutions [7].

A plethora of PLA-related research diverges from traditional cryptographic approaches by leveraging the intrinsic characteristics of the physical layer, which can be broadly classified as active and passive PLA based on the type of feature employed [7]. The active PLA uses an artificial feature such as an authentication tag, e.g., a tag is generated from the RIS-aided channel gain and background noise along with a random signal, which is then embedded into a source message to authenticate the transmitter [8]. Passive PLA on the other hand, utilizes intrinsic features from the channel, such as channel impulse response (CIR) [9], channel sparsity [10], [11] and received signal strength (RSS) [12]. For instance, in [12], RSS is used for spoofing attack detection by controlling the ON-OFF states of the RIS elements. Despite their potential benefits, current PLA methods exhibit certain limitations. Firstly, the active PLA scheme introduces additional computation and signal processing costs, often requiring extra resources, e.g., transmitting dedicated probing signals, which can lead to increased signaling overhead and power consumption and make PLA less suitable for resource-constrained systems such as Internet of Things (IoT) devices [3]. Secondly, channel-based schemes are susceptible to channel variations and experience performance degradation in sparse environments with limited signal propagation paths, where the entropy is minimal and only limited information can be extracted from the channel.

Motivated by the aforementioned concerns, this letter proposes a novel RIS-parameterized PLA scheme, meticulously designed for resilience against spoofing attacks. Our initial analysis uncovers the untapped potential of RIS in bolstering PLA efficiency by demonstrating RIS's ability to significantly enhance the entropy of the communication channel by introducing additional multipaths, thereby effectively countering the challenges posed by low entropy in sparse environments. Consequently, RIS increases the uniqueness of the legitimate channel by providing additional information about the legitimate user. Building upon these insights, we have developed a robust PLA strategy grounded in the double-structured sparsity of cascaded RIS channels. The proposed scheme extracts the RIS-related features in terms of the virtual angle indices to

Manuscript received 5 March 2024; accepted 30 April 2024. Date of publication 7 June 2024; date of current version 9 August 2024. This work was supported in part by the Scientific and Technological Research Council of Turkey (TUBITAK) under Grant 123E226. The associate editor coordinating the review of this article and approving it for publication was Y. Zhu. *(Corresponding author: Amira Bendaimi.)*

Amira Bendaimi and Hüseyin Arslan are with the Department of Electrical and Electronics Engineering, Istanbul Medipol University, 34810 Istanbul, Turkey (e-mail: amira.bendaimi@std.medipol.edu.tr; huseyinarslan@medipol.edu.tr).

Asmaa Abdallah, Abdulkadir Celik, and Ahmed M. Eltawil are with the Computer, Electrical, and Mathematical Sciences and Engineering Division, King Abdullah University of Science and Technology, Thuwal 23955, Saudi Arabia (e-mail: asmaa.abdallah@kaust.edu.sa; abdulkadir.celik@kaust.edu.sa; ahmed.eltawil@kaust.edu.sa).

Digital Object Identifier 10.1109/LWC.2024.3411108

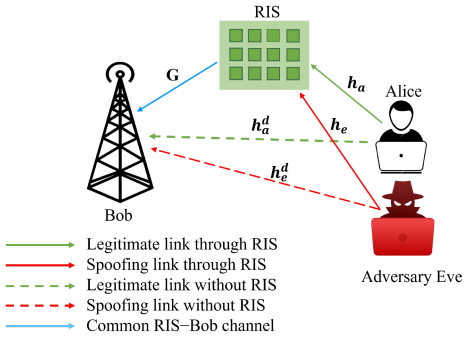

Fig. 1. The RIS-aided mmWave communication system.

forge a distinctive authentication signature. To quantify the efficacy of our proposed method, we have derived closed-form expressions for assessing the probabilities of both false alarm and detection. Finally, simulation results demonstrate the superior authentication performance of the proposed scheme compared to existing approaches with 72% and 14.89% in terms of probability of detection and false alarms.[1]

II. RIS-Assisted mmWave System Model

We consider an uplink RIS-assisted mmWave MIMO communication with three entities: Alice, Bob, and Eve, as depicted in Fig. 1. Alice serves as a legitimate transmitter, Bob is the intended receiver who needs to authenticate Alice's identity, and Eve is the malicious adversary who attempts to deceive Bob. In this particular configuration, both Alice and Eve are equipped with a single antenna and Bob with a N_{B} antenna array, and the RIS is formed by N_{RIS} passive reflecting elements arranged in a uniform linear array (ULA). Without loss of generality, the widely used Saleh-Valenzuela model for mmWave channel characterization is adopted to represent the channels between Alice-Bob and Eve-Bob, in which these channels can be composed of the direct channel $\mathbf{h}_x^d \in \mathbb{C}^{N_{\mathrm{B}}\times 1}$ and RIS-aided cascaded channel $\mathbf{H}_x \in \mathbb{C}^{N_{\mathrm{B}}\times N_{\mathrm{RIS}}}$, where the subscript $x \in \{a, e\}$ represent the nodes Alice and Eve, respectively. First, the direct channel $\mathbf{h}_x^d$ is given as [13]

$$\mathbf{h}_x^d = \sqrt{\frac{N_{\mathrm{B}}}{L_d^x}} \sum_{l_d=1}^{L_d^x} \alpha_{l_d} \mathbf{a}_b\left(\theta_{l_d}^x\right) \tag{1}$$

where L_d^x represents the number of paths between the node x and Bob, α_{ℓ_d} is the complex gain consisting of path loss, and $\theta_{l_d^x}$ denotes the angle of arrival (AoA) at Bob side. Similarly, the RIS−Bob channel denoted by $\mathbf{G} \in \mathbb{C}^{N_{\mathrm{B}}\times N_{\mathrm{RIS}}}$ is given by

$$\mathbf{G} = \sqrt{\frac{N_{\mathrm{B}} N_{\mathrm{RIS}}}{L_g}} \sum_{l_g=1}^{L_g} \alpha_{l_g} \mathbf{a}_b\left(\phi_{l_g}^r\right) \mathbf{a}_r^{\mathsf{H}}\left(\gamma_{l_g}^t\right) \tag{2}$$

and the node x-RIS channel $\mathbf{h}_x^r \in \mathbb{C}^{N_{\mathrm{RIS}}\times 1}$ is expressed as

$$\mathbf{h}_x^r = \sqrt{\frac{N_{\mathrm{RIS}}}{L_r^x}} \sum_{l_r=1}^{L_r^x} \alpha_{l_r} \mathbf{a}_r\left(\gamma_{l_r}^x\right) \tag{3}$$

[1]*Notations:* Bold uppercase $\mathbf{A}$, bold lowercase $\mathbf{a}$, and unbold letters A, a denote matrices, column vectors, and scalar values, respectively. $(\cdot)^{\mathsf{T}}$ and $(\cdot)^{\mathsf{H}}$ denote the transpose and hermitian operators, respectively. $\mathbb{C}^{M\times N}$ denotes the space of $M \times N$ complex-valued matrices. $||\mathbf{a}||$ is 2-norm of vector $\mathbf{a}$. and $|a|$ is the modulus of scalar a.

where L_g, L_r^x denote the number of paths between RIS and Bob, node x and RIS respectively. α_{ℓ_g} and α_{ℓ_r} are the complex gains, and $\mathbf{a}_r(\gamma_{l_g}) \in \mathbb{C}^{N_{\mathrm{RIS}}\times 1}$, $\mathbf{a}_b(\phi_{l_g}) \in \mathbb{C}^{N_{\mathrm{B}}\times 1}$ represent the array steering vectors associated with RIS and Bob, respectively. It is noted that RIS receives the signal from the node x and reflects it to Bob. Hence, AoAs and angle of departure (AoD)s at RIS are represented by $\gamma_{l_r}^x$, γ_{l_g}, while ϕ_{l_g} denotes the AoA at Bob side. Moreover, the array steering vector at Bob can be written as follows

$$\mathbf{a}_b(\phi) = \frac{1}{\sqrt{N_{\mathrm{B}}}}\left[1, \ldots, e^{j2\pi \frac{d}{\lambda}(N_{\mathrm{B}}-1)d\sin(\phi)}\right]^{\mathsf{T}} \tag{4}$$

where λ is the wavelength and d is the distance between adjacent antenna elements, which is usually defined as $d = \lambda/2$. Similarly, the array steering vector at RIS is expressed as follows

$$\mathbf{a}_r(\gamma) = \frac{1}{\sqrt{N_{\mathrm{RIS}}}}\left[1, \ldots, e^{j2\pi \frac{d}{\lambda}(N_{\mathrm{RIS}}-1)d\sin(\gamma)}\right]^{\mathsf{T}}. \tag{5}$$

Finally, The overall cascaded channel of the RIS assisted system $\mathbf{H}_x \in \mathbb{C}^{N_{\mathrm{B}}\times N_{\mathrm{RIS}}}$ from the node x to Bob is $\mathbf{H}_x \triangleq \mathbf{G}\,\mathrm{diag}(\mathbf{h}_x^r)$, which is further explicitly expressed as [14]

$$\mathbf{H}_x = \sqrt{\frac{N_{\mathrm{B}} N_{\mathrm{RIS}}}{L_g L_r^x}} \sum_{l_g=1}^{L_g} \sum_{l_r=1}^{L_r^x} \alpha_{l_g}\alpha_{l_r} \mathbf{a}_b\left(\phi_{l_g}^r\right) \mathbf{a}_r^{\mathsf{H}}\left(\gamma_{\mathrm{RIS}}^t\right) \tag{6}$$

where $\gamma_{\mathrm{RIS}}^t = \gamma_{l_g}^t + \gamma_{l_r}^r$ is the effective AoD at the RIS side and the total number of paths is $L_g L_r^x$. Furthermore, the virtual beam space representation of $\mathbf{H}_x$ is given as

$$\mathbf{H}_x = \mathbf{U}_{N_{\mathrm{B}}} \widetilde{\mathbf{H}}_x \mathbf{U}_{N_{\mathrm{RIS}}}^{\mathsf{T}} \tag{7}$$

where $\mathbf{U}_{N_{\mathrm{RIS}}} \in \mathbb{C}^{N_{\mathrm{RIS}}\times N_{\mathrm{RIS}}}$ and $\mathbf{U}_{N_{\mathrm{B}}} \in \mathbb{C}^{N_{\mathrm{B}}\times N_{\mathrm{B}}}$ represent the unitary discrete Fourier transform (DFT) matrices at the RIS and Bob, respectively, and $\widetilde{\mathbf{H}}_x \in \mathbb{C}^{N_{\mathrm{RIS}}\times N_{\mathrm{B}}}$ is the virtual sparse channel matrix.

III. Exploiting RIS Characteristics to Boost PLA

This section first explains how double-structured sparsity of cascaded RIS channels can improve authentication entropy, then presents the developed signature extraction and authentication mechanism, and finally presents an analysis to evaluate authentication performance.

A. Double-Structured Sparsity for Improved Entropy

Practical millimeter-wave MIMO channels exhibit significant sparsity, presented in a limited number of channel paths between the node x and Bob, typically, $L_d^x \approx 3 \sim 5$ paths [14]. Thereby, the information extracted from a mmWave MIMO channel is limited, resulting in low authentication entropy. Interestingly, the integration of RIS and double-structured sparsity of the resulting cascaded channels inherently introduces supplementary multipath, elevating the total paths in the cascaded channel to $L_g L_r^x > L_d^x$ as demonstrated from equation (6). This enrichment increases the authentication signature entropy and offers extra node-specific information that serves as a unique fingerprint to differentiate legitimate users from attackers, which is further analyzed in Section III-C.

Moreover, the proposed scheme not only leverages the distinct sparsity of the direct channel link but also from the

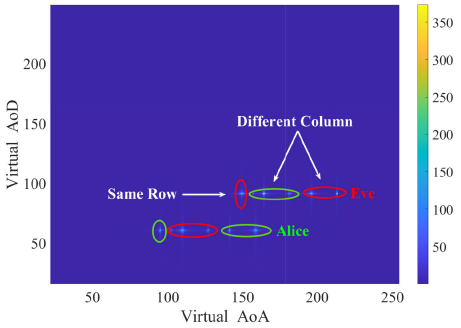

Fig. 2. Beamspace of both Alice (green) and Eve (red) cascaded channels with $L_g = 2$, and $L_r^x = 3$.

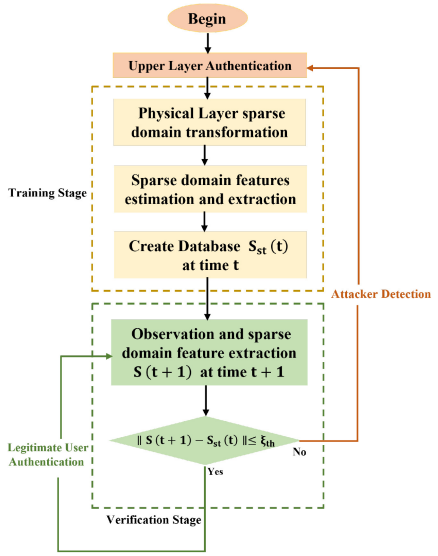

Fig. 3. The proposed PLA flowchart.

unique double-structured sparsity of the beamspace cascaded channel $\widetilde{\mathbf{H}}_x$ [15]. This feature arises from the fact that Bob observes the angular cascaded channels $\widetilde{\mathbf{H}}_x$ of Alice and Eve with entirely identical row supports but different column supports, as illustrated in Fig. 2. This property helps detect spoofing attacks where Eve cannot possess the same row-column-block sparsity structure as Alice. This property can be observed in (6), wherein each complete reflecting path (l_g, l_r) provides a peak element for $\widetilde{\mathbf{H}}_x$, whose row and column indices rely on $\phi_{l_g}^r$ and γ_{RIS}^t, respectively. Therefore, $\widetilde{\mathbf{H}}_x$ has L_g non-zero rows, where each non-zero row has L_r^x non-zero columns containing the peak elements. Thus, the total number of non-zero elements becomes $L_g L_r^x$, which lies on the completely common L_g rows because the channel $\widetilde{\mathbf{G}}$ is common for both Alice and Eve, with the AoAs $\{(\phi_{l_g}^r)\}_{l_g=1}^{L_g}$ being independent of the node index [c.f. Fig. 2]. However, the column support is node-specific, and it is different between Alice and Eve.

B. Signature Extraction and Authentication Decision

The PLA procedure described in this letter comprises two main stages: training and verification, as depicted in Fig. 3. During the training stage, only Alice and Bob nodes are involved, and Alice's identity is authenticated by Bob through higher-layer protocols. Bob captures a unique physical layer signature from the received signal by initially estimating the communication channels from the nodes, employing methods such as those outlined in [15], [16]. These channels offer distinctive fingerprints, encompassing AoAs of the direct and cascaded links at Bob and effective AoD at the RIS, which are respectively estimated as follows

$$\hat{\theta}_{l_d}(t) = \theta_{l_d}(t) + \Delta\theta_{l_d}(t) \tag{8}$$

$$\hat{\phi}_{l_g}(t) = \phi_{l_g}(t) + \Delta\phi_{l_g}(t) \tag{9}$$

$$\hat{\gamma}_r(t) = \gamma_r(t) + \Delta\gamma_{\mathrm{RIS}}(t) \tag{10}$$

where $\Delta\theta \sim \mathcal{N}(0, \sigma_{\Delta\theta}^2)$, $\Delta\phi \sim \mathcal{N}(0, \sigma_{\Delta\phi}^2)$, $\Delta\gamma \sim \mathcal{N}(0, \sigma_{\Delta\gamma}^2)$ are the estimation errors. Furthermore, the identification of support channels becomes crucial to determine the indices corresponding to AoA and AoD pairs for each path within the cascaded channel. Subsequently, a vector is constructed from these indices, serving as a signature for authentication. The indices of the AoAs for both the direct and cascaded links, as well as those of the AoD for the cascaded links, are respectively extracted as

$$n_{\mathrm{D}}^*(t) = \underset{1\le n\le N_B}{\arg\min} \left| \psi_n - \frac{d_c}{\lambda_c}\left(1 + \frac{1}{f_c}\right) \sin\left(\hat{\theta}_{l_d}^x(t)\right) \right| \tag{11}$$

$$n_{\mathrm{B}}^*(t) = \underset{1\le n\le N_B}{\arg\min} \left| \psi_n - \frac{d_c}{\lambda_c}\left(1 + \frac{1}{f_c}\right) \sin\left(\hat{\phi}_{l_g}(t)\right) \right| \tag{12}$$

$$n_{\mathrm{RIS}}^*(t) = \underset{1\le n\le N_{RIS}}{\arg\min} \left| \psi_n - \frac{d_c}{\lambda_c}\left(1 + \frac{1}{f_c}\right) \sin(\hat{\gamma}_r^x(t)) \right| \tag{13}$$

where $\psi_n = \frac{1}{N}(n - \frac{N+1}{2})$ is the spatial direction in the beamspace domain for $n \in \{n_{\mathrm{D}}, n_{\mathrm{RIS}}, n_{\mathrm{B}}\}$. Finally, the resulting signatures of the direct and cascaded links are subsequently stored in the database on Bob's side. The signature of the direct link is expressed as a $1 \times L_d^x$ vector as follows

$$\mathbf{s}_{\mathrm{D}}(t) = \left[n_{\mathrm{D}}^{1*}, \ldots, n_{\mathrm{D}}^{l_d^x *}, \ldots, n_{\mathrm{D}}^{L_d^x *} \right]. \tag{14}$$

The signature of the reflected cascaded link is represented as a $2 \times L_g L_r^x$ matrix as follows[2]

$$\mathbf{S}_{\mathrm{cas}}(t) = \begin{bmatrix} n_{\mathrm{B}}^{1*}, \ldots, n_{\mathrm{B}}^{L_g *}, \ldots, n_{\mathrm{B}}^{1*}, \ldots, n_{\mathrm{B}}^{L_g *} \\ n_{\mathrm{RIS}}^{1*}, \ldots, n_{\mathrm{RIS}}^{L_r *}, , \ldots, n_{\mathrm{RIS}}^{1*}, \ldots, n_{\mathrm{RIS}}^{L_r *} \end{bmatrix}. \tag{15}$$

By considering both the reflected link and the direct link, the resulting signature is formed by concatenating the two signatures of the two links as follows[3]

$$\mathbf{S}_{\mathrm{st}}(t) = \begin{bmatrix} \mathbf{S}_{\mathrm{cas}}(t) & \mathbf{s}_{\mathrm{D}}(t) \\ & \mathbf{0} \end{bmatrix}. \tag{16}$$

[2]In the case of a multi-antenna user with N_x antennas, the signature will be further enriched by incorporating the AoD from the node x denoted as θ_{l_r} with its index n_x^*, resulting in a 3D signature by concatenating the indices n_x^* for the L_r^x paths.

[3]The complexity of the proposed algorithm arises from estimating the indices where the method in [15] is used to achieve minimal pilot overhead for cascaded channel estimation.

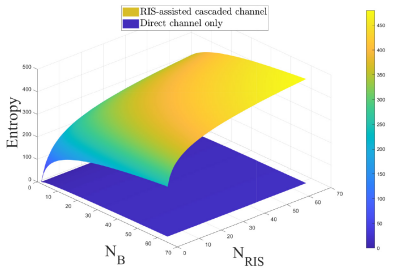

Fig. 4. Authentication entropy of direct and cascaded channels.

For the verification process at $t+1$, the signature $\mathbf{S}(t+1)$ is extracted by following the same process as in the training stage. It is noteworthy that the channels of both Alice and Eve are independent.

In the case of mobility, the cascaded channel denoted by $\mathbf{H}_a$ is assumed to undergo updates at $t+1$ based on a first-order Gauss-Markov model [11]. Subsequently, a binary hypothesis test is conducted to verify the identity of the transmitted signal, expressed as

$$\begin{aligned} \mathcal{K}_0{:}\Delta &= ||\mathbf{S}(t+1) - \mathbf{S}_{\text{st}}(t)|| \leq \zeta_{th} \\ \mathcal{K}_1{:}\Delta &= ||\mathbf{S}(t+1) - \mathbf{S}_{\text{st}}(t)|| > \zeta_{th} \end{aligned} \tag{17}$$

where the hypotheses $\mathcal{K}_0$ and $\mathcal{K}_1$ correspond to signal reception from legitimate (Alice) and illegitimate (Eve) users, respectively; and hypothesis testing parameter ζ_{th} serves as the threshold to distinguish between $\mathcal{K}_0$ and $\mathcal{K}_1$. Bob conducts a comparison between the extracted signature $\mathbf{S}(t+1)$ and the pre-stored reference signature $\mathbf{S}_{\text{st}}(t)$. If the match falls within an acceptable threshold, the transmitter is considered authentic. Otherwise, the transmitter is deemed unauthorized.

C. Authentication Entropy and Performance Analysis

Entropy is defined as the average amount of information contained in a message. For a random variable X, the entropy is given as $H(X) = -\sum_{i=1}^{n} \Pr[x_i] \log_2 \Pr[x_i]$, where $\Pr[x_i]$ is the probability of X's possible value x_i [17]. The authentication entropy of sparse virtual channels can be approximated as the entropy of a uniformly distributed digital signature. Therefore, the authentication entropy of the cascaded channel link can be expressed as $H_{\text{cas}}(X) = L_g L_r^x \log_2(N_{RIS} N_B)$, whereas the entropy of the direct channel link is given by $H_{\text{D}}(X) = L_d^x \log_2(N_B)$. Hence, $H_{\text{cas}}(X) > H_{\text{D}}(X)$ as $L_g L_r^x \log_2(N_{\text{RIS}}) > L_d^x$. Fig. 4 provides a visual representation of the authentication entropy, revealing that the cascaded channel link introduces higher entropy compared to the direct channel link.

In order to model false alarm and detection probabilities, the values of the indices in $\mathbf{S}(t+1)$ and $\mathbf{S}_{\text{st}}(t)$ can be approximated as random variables following a uniform distribution, given that the angles θ_{l_d}, ϕ_{l_g} and γ_r are uniformly distributed $\sim \mathcal{U}(-\pi/2, \pi/2)$. Hence, the hypothesis test statistic is a Gaussian random variable, i.e., $\Delta \sim \mathcal{N}(\mu_a, \sigma_a^2)$. As a result, the corresponding probability distribution function (PDF) is

$$P_{\mathcal{K}_0} = \frac{1}{\sqrt{2\pi\sigma_a^2}} \exp\left(-\frac{(x-\mu_a)^2}{2\sigma_a^2}\right). \tag{18}$$

The probability of a false alarm P_{fa} can be given by

$$\begin{aligned} P_{fa} &= P\{\Delta > \zeta_{th} \mid \mathcal{K}_0\} \\ &= \int_{\zeta_{th}}^{\infty} P_{\mathcal{K}_0}(\Delta)\, dx = Q_a(\zeta_{th}) \end{aligned} \tag{19}$$

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

$$Q(x) = \int_{x}^{+\infty} \frac{1}{\sqrt{2\pi}} \exp\left(-\frac{1}{2}t^2\right) dt. \tag{20}$$

Next, based on the given false alarm rate, P_{fa} we can obtain the corresponding threshold, ζ_{th} as

$$\zeta_{th} = Q_a^{-1}(1 - P_{fa}), \tag{21}$$

where $Q^{-1}(\cdot)$ is the inverse Q-function. Moreover, under hypothesis $\mathcal{K}_1$, the test statistic also follows a Gaussian distribution, i.e., $\Delta \sim \mathcal{N}(\mu_b, \sigma_b^2)$. Thus, the corresponding PDF is

$$P_{\mathcal{K}_1} = \frac{1}{\sqrt{2\pi\sigma_b^2}} \exp\left(-\frac{(x-\mu_b)^2}{2\sigma_b^2}\right). \tag{22}$$

Then, the probability of miss-detection P_{md} is described as

$$\begin{aligned} P_{md} &= P\{\Delta < \zeta_{th} \mid \mathcal{K}_1\} = \int_{-\infty}^{\zeta_{th}} P_{\mathcal{K}_1}(\Delta)\, dx \\ &= 1 - Q_b(\zeta_{th}) \end{aligned} \tag{23}$$

where the probability of detection P_d, which is the probability of correctly detecting a forged signal when Alice did not transmit it, is defined as $P_d = 1 - P_{md}$.

IV. Simulation Results and Analysis

To evaluate the proposed RIS-parameterized PLA scheme, simulations are conducted to assess its performance, which relies on the probability of detection and false alarm. During the simulation, it is considered that both Bob and RIS have the same number of antenna elements $N_{\text{B}} = N_{\text{RIS}} = 128$, operating at a carrier frequency of $f_c = 60$ GHz with an SNR of 0 dB. Additionally, the direct link is modeled with $L_d^x = 5$, while the reflected link is characterized by $(L_g = 3,\ L_r^x = 6)$ path pairs.

To illustrate the impact of incorporating RIS on authentication performance, Fig. 5(a) presents receiver operating characteristic (ROC) curves, which represent the trade-off between the probability of false alarms and the probability of detection for different approaches, comparing cases with and without RIS. The proposed scheme reveals a significant improvement in performance over existing approaches [10], [11] which is about 14.89% compared to [10] and 72% compared to [11]. This improvement is attributed to the fact that the proposed scheme leverages the assistance of RIS and benefits from additional signal paths and diversity offered by RIS to compensate for the sparsity in mmWave channels that is highly presented in the direct link. Additionally, theoretical findings closely align with simulation results, demonstrating the efficiency of our theoretical model in characterizing authentication performance for P_{fa} and P_d. Moreover, the direct channel is used beside the reflected channel with a 2% performance enhancement.

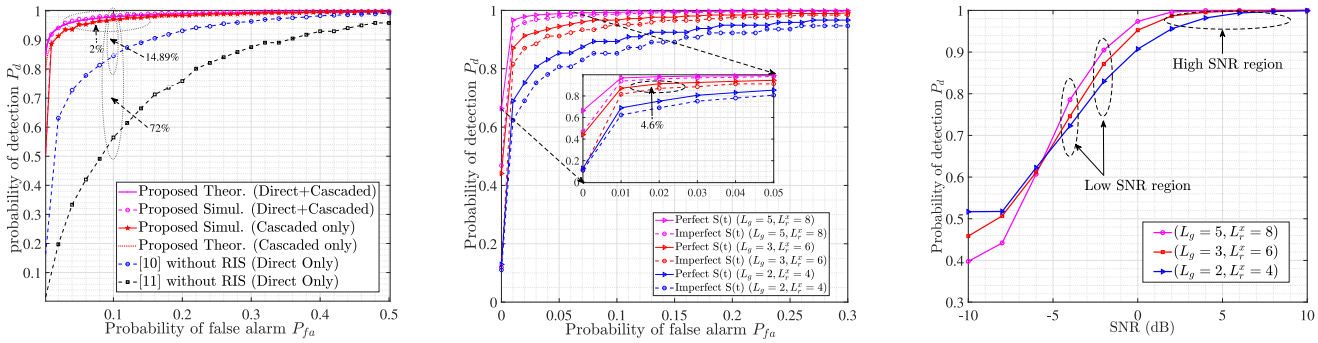

Fig. 5. Comparison of the probability of detection (a) for different schemes, (b) under perfect and imperfect signature estimation with different multipath pairs, (c) under different SNR values.

Fig. 5(b) presents the ROC curves with varied numbers of multipath pairs under different states of signature estimation to demonstrate their influence on the authentication performance. With an increasing number of (L_g, L_r^x) pairs, the probability of a false alarm tends to decrease. It can be seen that the authentication performance is the best when there is $(L_g = 5, L_r^x = 8)$ multipath, outperforming the other cases. Moreover, the proposed signature exhibits a slight performance degradation of around 4.6% in the case of $(L_g = 3, L_r^x = 6)$, attributed to the inaccurate estimation caused by hardware impairments, while still maintaining its superiority under imperfect signature estimation. It's worth noting that in practical authentication systems, meeting security requirements often involves ensuring $P_{fa} < 0.1$ and $P_d > 0.9$ which is always satisfied by our proposed scheme.

Fig. 5(c) illustrates the robustness of the proposed scheme under different SNR values where a higher detection rate is observed even at low SNRs, For instance, at an SNR of -4 dB, the detection probability exceeds $(P_d = 0.75)$. Moreover, the probability of detection gradually increases with the SNR due to the accurate signature estimation at high SNR regions. Henceforth, our proposed scheme highlights its robustness to noise and channel imperfections.

V. Conclusion

This letter proposes a novel scheme for authentication in an RIS-assisted system to achieve robust security against spoofing attacks. The scheme is based on exploiting the RIS channel and its unique sparsity structure. On this basis, we have theoretically analyzed the RIS-related characteristics besides the feasibility of the proposed system. Simulation results demonstrate the superior authentication performance of the proposed scheme compared to the existing approach in the conventional MIMO system, with a 72% performance improvement. Future work involves the analysis of this approach in a wideband system with the integration of hardware impairments to further enhance the authentication performance.

References

[1] M. Alsabah et al., "6G wireless communications networks: A comprehensive survey," *IEEE Access*, vol. 9, pp. 148191–148243, 2021.

[2] S. Hassouna et al., "A survey on reconfigurable intelligent surfaces: Wireless communication perspective," *IET Commun.*, vol. 17, no. 5, pp. 497–537, 2023.

[3] E. Illi et al., "Physical layer security for authentication, confidentiality, and malicious node detection: A paradigm shift in securing IoT networks," *IEEE Commun. Surveys Tuts.*, vol. 26, no. 1, pp. 347–388, 1st Quart., 2024.

[4] J. Yang, Z. Wan, K. Huang, J. Zhao, and X. Ji, "RIS antenna-aided secret key generation for static environment," TechRxiv Preprints, 2023.

[5] T. Lu, L. Chen, J. Zhang, K. Cao, and A. Hu, "Reconfigurable intelligent surface-assisted secret key generation in quasi-static environments," *IEEE Commun. Lett.*, vol. 26, no. 2, pp. 244–248, Feb. 2022.

[6] X. Hu, L. Jin, K. Huang, X. Sun, Y. Zhou, and J. Qu, "Intelligent reflecting surface-assisted secret key generation with discrete phase shifts in static environment," *IEEE Commun. Lett.*, vol. 10, no. 9, pp. 1867–1870, Sep. 2021.

[7] N. Xie, Z. Li, and H. Tan, "A survey of physical-layer authentication in wireless communications," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 1, pp. 282–310, 1st Quart., 2021.

[8] P. Zhang, Y. Teng, Y. Shen X. Jiang, and F. Xiao, "Tag-based PHY-layer authentication for RIS-assisted communication systems," *IEEE Trans. Dependable Secure Comput.*, vol. 20, no. 6, pp. 4778–4792, Nov./Dec. 2023.

[9] N. Xie, J. Chen, and L. Huang, "Physical-layer authentication using multiple channel-based features," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 2356–2366, 2021.

[10] L. Afeef, H. M. Furqan, and H. Arslan, "Physical layer authentication scheme in beamspace MIMO systems," *IEEE Commun. Lett.*, vol. 26, no. 7, pp. 1484–1488, Jul. 2022.

[11] J. Tang, A. Xu, Y. Jiang, Y. Zhang, H. Wen, and T. Zhang, "MmWave MIMO physical layer authentication by using channel sparsity," in *Proc. IEEE Int. Conf. Artif. Intell. Inf. Syst. (ICAIIS)*, Dalian, China, 2020, pp. 221–224.

[12] N. Gao et al., "RIS-assisted physical layer authentication for 6G endogenous security," 2023, *arXiv:2309.07736*.

[13] 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. Top. Signal Process.*, vol. 10, no. 3, pp. 436–453, Apr. 2016.

[14] A. M. Sayeed and N. Behdad, "Continuous aperture phased MIMO: A new architecture for optimum line-of-sight links," in *Proc. IEEE Int. Symp. Antennas Propag. (APSURSI)*, 2011, pp. 293–296.

[15] A. Abdallah, A. Celik, M. M. Mansour, and A. M. Eltawil, "RIS-aided mmWave MIMO channel estimation using deep learning and compressive sensing," *IEEE Trans. Commun.*, vol. 22, no. 5, pp. 3503–3521, May 2023.

[16] X. Wei, D. Shen, and L. Dai, "Channel estimation for RIS assisted wireless communications—Part II: An improved solution based on double-structured sparsity," *IEEE Commun. Lett.*, vol. 25, no. 5, pp. 1403–1407, May 2021.

[17] B. Chen, Y. Zhu, J. Hu, J. C. Pri'ncipe, "δ-entropy: Definition, properties and applications in system identification with quantized data," *Inf. Sci.*, vol. 181, no. 7, pp. 1384–1402, 2011.