Impact of Residual Hardware Impairments on RIS-aided Authentication

Bilal Çiçek* and Hakan Alakoca*
*Ericsson Research
Istanbul, Turkey
Email: {bilal.cicek, hakan.alakoca}@ericsson.com

***Abstract*—In next-generation communication systems, physical layer security is a key research area with the aim of enhancing authentication mechanisms and providing standalone or complementary support to conventional cryptographic techniques. Since some physical features such as wireless channels and/or hardware impairments of each user equipment are often unique, these can be leveraged in novel authentication methods and models. This study investigates the impact of residual hardware impairments (RHI) on reconfigurable intelligent surface (RIS)-aided communication networks in the presence of spoofing attacks. We find that increasing the number of metasurface elements and the signal-to-noise ratio enhances detection performance with the support of RIS. Furthermore, the integration of RIS significantly improves miss detection and false alarm rate performance thanks to providing richness of channels. We also compare the role of phase-shift matrices in detecting spoofing attacks. Our results show that a higher RHI for Eve facilitates the detection of spoofing attacks with the help of RIS.**

***Index Terms*—authentication, hardware impairments, physical layer security, reconfigurable intelligent surfaces, spoofing attacks**

I. Introduction

Secure communication in 6G networks is crucial for meeting stringent security requirements. The security of reconfigurable intelligent surface (RIS), given its functional operations and unique hardware components, is equally important, as highlighted in [1]. Novel vulnerabilities related to metasurface manipulations, based on signal processing capabilities, are explored in [2]. Additionally, although there are some open research concerns regarding the immaturity level in the communication environment about physical layer security (PLS), it still emerges as a promising approach to enhancing existing security mechanisms. This concept is systematically reviewed in [3], which classifies RIS applications across various system topologies and scenarios. The study in [4] further investigates RIS-aided PLS strategies for 6G internet of things (IoT) networks, addressing threats such as eavesdropping and jamming. It presents design solutions involving resource allocation, beamforming, artificial noise, and cooperative communication, while also identifying research challenges and recent advancements in RIS modeling and optimization.

Physical layer authentication (PLA) is a fundamental concept that leverages physical layer information either independently or in conjunction with other authentication methods. The study in [5] explores the use of angle of arrival in array multiple input multiple output (MIMO) systems to enhance authentication mechanisms in the presence of impersonation attacks. In [6], a RIS-aided IoT scheme is examined for both direct and cascaded channels, using least squares estimation and second-order statistics for statistical analysis. In [7] a challenge-response mechanism is presented in RIS equipment that is used as an electromagnetic challenge generator. The hybrid RIS authentication method presented in [8] enables a detection mechanism for impersonation attacks by jointly analyzing the channel response at both the receiver and the hybrid RIS. A lightweight cross-layer authentication solution for vehicular communication, integrated with a public key-based cryptographic method for RIS-aided scenarios, is discussed in [9]. A tag-based authentication solution to prevent impersonation attacks is presented in [10], which includes a mathematical background covering detection probability and false alarm rates. The study in [11] provides a statistical analysis and mathematical background for PLA-based RIS-aided MIMO networks, leveraging unique channel entropy. Additionally, a RIS-aided channel fingerprinting control approach using microcontrollers is discussed, covering both theoretical and practical aspects. RIS-aided communication links can also be used in wireless secret key generation techniques. A RIS-aided procedure is presented in [12], which improves RIS configuration for physical-layer key generation and simultaneous communication enhancement in static environments. Nevertheless, the studies presented in [5]–[12] do not comprehensively examine the effects of hardware impairments on both the transmitter and receiver sides in the context of PLA-based authentication within RIS-aided communication scenarios.

Realistic models and hardware impairment-based solutions are crucial in the literature to ensure realistic assumptions and feasibility in RIS-aided communication network; however, most related studies do not cover PLA. The study in [13] explores covert communication system which is supported with an active RIS and non-orthogonal multiple access (NOMA) in the presence of hardware impairments, analyzing outage probability, detection error probability, and optimum thresholds for detection. A RIS-aided multi-cluster wireless-powered communication network addressing impairments caused by hardware and providing solutions for average sum rate optimization and energy consumption is investigated in [14]. Another study in [15] focuses on RIS-aided multi-user MIMO networks, aiming to minimize performance degradation due to hardware impairments and imperfect channel state infor-

2024 IEEE Virtual Conference on Communications (VCC) | 979-8-3315-3009-9/24/$31.00 ©2024 IEEE | DOI: 10.1109/VCC63113.2024.10914407

mation (CSI). Power consumption optimization for RIS-aided wireless communication systems under imperfect CSI and hardware impairments is examined using successive convex approximation and block coordinate descent techniques. The impact of residual hardware impairments (RHI) on secrecy outage probability in a RIS-aided NOMA communication environment with eavesdropping attacks is analyzed through closed-form solutions in [16]. Additionally, [17] presents a study on RIS-aided secrecy rate optimization with hardware impairments, aiming that the weighted minimum approximate ergodic secrecy rate is maximized using second-order cone programming and a penalty convex-concave procedure. In [18], the negative effects of hardware impairments on PLA are investigated for MIMO system. However, it does not include RIS component in their model. Lastly, [19] investigates robust transmission design for communication scenarios which is supported with RIS under hardware impairments, focusing on maximizing the secrecy rate in the presence of eavesdropping attacks using successive convex approximation for active beamforming and semidefinite programming.

Our main motivation for this study is showing that how hardware impairments affect the PLA performance. Other motivation is representing impacts of reflecting surfaces number. Also, we aim to show the performance impact of RIS usage in terms of PLA performance by comparing with direct link communication.

Our main contributions in this study are itemized as follows:

- **C1** - We provide a statistical approach validated via simulation analysis of false alarm rate (FAR) and miss detection rate (MDR) in RIS-aided communication in the presence of a spoofing attack. In addition, we provide theoretical analysis of FAR considering autoregressive CSI.
- **C2** - The study shows that how residual hardware impairments (RHI) affect RIS-aided communication networks in the context of spoofing attacks. We contribute to show the performance impact of hardware impairments of legitimate user.
- **C3** - We compare the effectiveness of RIS phase-shift matrices in detecting spoofing attacks, demonstrating their crucial role in detection. By comparing the system scenario with RIS and scenario without RIS, we demonstrate the positive effect of RIS utilization on FAR and MDR.

The structure of this paper is organized as follows: Section II outlines the system model for the RIS-aided spoofing attack scenario with residual hardware impairments. In Section III, we describe the physical authentication method and the corresponding detection mechanism. The numerical results are presented and discussed in Section IV, and the paper is concluded in Section V.

II. System Model

In this paper, we consider a RIS-aided communication networks in the presence of spoofing attacks. Alice sends its data to the Bob over RIS-aided communication link. Here, there is

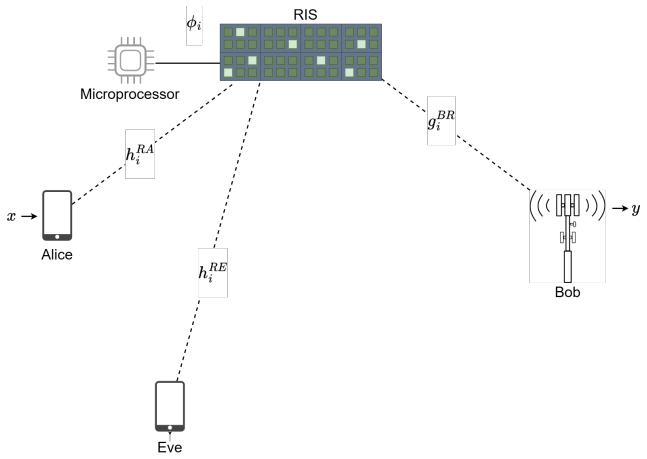

Fig. 1. System model of RIS-aided communication in the presence of spoofing attacker, Eve.

no direct communication link between Alice to Bob and Eve to Bob because it is assumed that the path between transmitters and receiver is blocked due to buildings and obstacles. The system model is represented in Fig. 1 where h_i^{RA} shows the channel coefficients between Alice and i-th reflecting element of RIS, h_i^{RE} is the channel coefficients between Eve and i-th reflecting element of RIS, ϕ_i is phase adjustment value of i-th reflecting element of RIS, g_i^{BR} demonstrates the channel coefficient between i-th reflecting element of RIS and Bob, x shows the sending signal and y shows the received signal at Bob. While Alice and Bob demonstrate the legitimate user in the network, Eve is the attacker trying to send fake messages to Bob. In this system model, the direct link between transmitter and receiver is assumed to be blocked. The receiver Bob receives the signal of transmitters via RIS where the number of RIS reflecting elements is represented as N. In addition, Bob tries to detect whether the received signal comes from Alice or not based on CSI information and authenticate that the signal is sent by Alice. In this authentication mechanism, there are some challenges impacting the authentication performance such as fading, hardware impairments at transceiver and noise at receiver.

The received signal at Bob can be represented as,

$$\begin{aligned} y_t &= \left[\sum_{i=1}^{N} h_i^{Rt} g_i^{BR} e^{j\phi_i}\right](x+\eta_t) + \eta_B + n, \\ &= H_t\,(x+\eta_t) + \eta_B + n, \end{aligned} \tag{1}$$

where h_i^{Rt}, $g_i^{BR} \sim \mathcal{CN}(0,1)$, η_t is transmitter RHI whose distribution is $\eta_t \sim \mathcal{CN}(0,\kappa_t)$, η_B is receiver RHI at Bob whose distribution is $\eta_B \sim \mathcal{CN}(0,\kappa_B)$, n shows the additive White Gaussian noise (AWGN) with σ_n^2 variance, x is the unit power binary phase shift keying (BPSK) signal for both legitimate and attack scenario, i.e. $\mathbf{E}(|x|^2) = 1$, and $t \in \{A, E\}$. $h_i^{Rt}, g_i^{BR}, \eta_t, \eta_B$ and n are independently random variables. $\mathbf{E}(.)$ is given as expectation operator. Furthermore, there are two RIS operation types which are called intelligent and blind transmission in terms of ϕ_i value [20], [21]. In intelligent

transmission, ϕ_i is equal to the negative of channel phases' summation to compensate channel phases to obtain maximum value of signal-to-noise ratio (SNR) which is received at Bob, i.e. $\phi_i = -(\arg\{h_i^{RA}\} + \arg\{g_i^{BR}\})$ where $\arg\{.\}$ shows the argument operator for complex number. This eliminates the complex part of compund channel [20], [21]. Also, ϕ_i is determined according to the only legitimate user, which means that the RIS maximizes the SNR obtained from Alice, not Eve. On the other hand, ϕ_i is equal to the zero and the RIS is responsible for only reflecting signal without any phase adjustment in blind transmission. Then, the channel estimation process is applied at receiver. The estimated channel at Bob can be formulated as

$$\hat{H}_t = y_t x^*, \tag{2}$$

where $(.)^*$ shows the conjugate of argument. As the phase adjustment at RIS eliminates the complex part of individual channels, the distribution of compound channel for Alice-RIS-Bob is given as

$$H_A \sim \mathcal{N}\left(\frac{N\pi}{4}, \frac{N(16-\pi^2)}{16}\right). \tag{3}$$

In addition, the channel characteristic between Eve and RIS follows the Rayleigh fading with unit power. In terms of RIS deployment in attack scenario, the ϕ_i is determined according to the channel information of Alice as it is mentioned before, i.e. $\phi_i = -(\arg\{h_i^{RA}\} + \arg\{g_i^{BR}\})$. Then, Eve-RIS-Bob link is distributed as

$$H_E \sim C\mathcal{N}(0, N). \tag{4}$$

Furthermore, under the assumption of that Alice moves slightly compared to previous position, i.e. current and previous locations are close, the channel of Alice-RIS-Bob path has first order autoregressive model and can be formulated as $H_A(k) = \alpha H_A(k-1) + \sqrt{1-\alpha^2}e(k)$ where $e(k) \sim C\mathcal{N}\left(0, \mathbf{E}(|H_A|^2)\right)$ [18], [22]. The channel estimation error at Bob is calculated as $\epsilon_t = H_t - \hat{H}_t$ and $\epsilon_t \sim C\mathcal{N}(0, \text{Var}(\epsilon_t))$,

$$\begin{aligned}
\text{Var}(\epsilon_t) &= \mathbf{E}(\epsilon_t \epsilon_t^*), \\
&= \mathbf{E}((H_t - y_t x^*)(H_t^* - y_t^* x)), \\
&= \mathbf{E}(|H_t|^2) - 2\mathbf{E}(H_t x y_t^*) + \mathbf{E}(|x|^2)\mathbf{E}(|y_t|^2), \\
&= \mathbf{E}(|H_t|^2) - 2\{\mathbf{E}(|H_t|^2 + |H_t|^2 \eta_t^* x + H_t x \eta_B^*, \\
&+ H_t x n^*)\} + \mathbf{E}(|y_t|^2), \\
&= \mathbf{E}(|H_t|^2) - 2\mathbf{E}(|H_t|^2) + R_{y,t},
\end{aligned} \tag{5}$$

and

$$R_{y,t} = \mathbf{E}(|y_t|^2) = \mathbf{E}(|H_t|^2) + \mathbf{E}(|H_t|^2)\kappa_t + \kappa_B + \sigma_n^2. \tag{6}$$

III. Physical Layer Authentication Method

In this section, we show the decision mechanism for detecting attacker with the aid of CSI. To this end, we introduce the hypothesis testing which is following as

$$\mathcal{H}_0 : \hat{H}(k) = H_A(k), \tag{7a}$$

$$\mathcal{H}_1 : \hat{H}(k) = H_E(k), \tag{7b}$$

where $\mathcal{H}_0$ shows that the received signal comes from legitimate user Alice and $\mathcal{H}_1$ means that the signal obtained at Bob is sent by attacker Eve. To determine that which hypothesis is occured, the likelihood ratio test (LRT) based on the difference between channel coefficient at current time and one at previous time is utilized as

$$\frac{2}{\text{Var}(\epsilon_A) + \text{Var}(\epsilon_t)} ||\hat{H}_t(k) - \alpha \hat{H}_A(k-1)||^2 \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \gamma, \tag{8}$$

where γ is given as predetermined threshold. In this hypothesis testing, the receiver estimates the channel coefficient at each time and it stores the value of estimated channel coefficients. Since the compound channel of legitimate path has first-order autoregressive process, the receiver can apply the LRT based on channel measurement at time interval k and at time interval $k-1$. If the estimated channel at k belongs to the Alice, the difference between the channel coefficients at time k and $k-1$ is small due to autoregressive process. Therefore, the receiver makes a decision based on this approach.

The performance analysis of authentication mechanism can be examined by FAR. The FAR means that the receiver decides the existence of attacker Eve when the signal is sent by Alice. To obtain FAR analysis, the difference between current estimated channel and previous estimated channel is acquired as

$$\begin{aligned}
\beta &= \hat{H_A}(k) - \alpha \hat{H_A}(k-1), \\
&= H_A(k) - \epsilon_A(k) - \alpha H_A(k-1) + \alpha \epsilon_A(k-1), \\
&= \alpha H_A(k-1) + \sqrt{1-\alpha^2} e(k) - \epsilon_A(k) - \alpha H_A(k-1) +, \\
&\alpha \epsilon_A(k-1), \\
&= \sqrt{1-\alpha^2} e(k) - \epsilon_A(k) + \alpha \epsilon_A(k-1).
\end{aligned} \tag{9}$$

The variance of β is formulated as

$$\text{Var}(\beta) = \sigma_\beta^2 = (1-\alpha^2)\mathbf{E}(|H_A|^2) + (1+\alpha^2)\text{Var}(\epsilon_A), \tag{10}$$

and it has complex Gaussian distribution with $\beta \sim C\mathcal{N}(0, \sigma_\beta^2)$. Based on (5), (6) and (10), it can be seen that the variance of β depends on the power of compound channel, noise power at receiver and the RHI of both transmitter and receiver. The distribution of $||\beta||^2$ has Chi-square distribution whose degrees of freedom is 2. Also, the FAR can be explained as

$$\text{FAR} = \mathbf{Pr}(||\beta||^2 > \tilde{\gamma}) = 1 - \text{F}_{||\beta||^2}(\tilde{\gamma}), \tag{11}$$

where $\text{F}_{||\beta||^2}(x) = 1 - \exp(\frac{-x}{\sigma_\beta^2})$ and $\tilde{\gamma} = \gamma \text{Var}(\epsilon_A)$.

When Eve sends the signal, the difference between current estimated channel and previous estimated channel is obtained as

$$\begin{aligned}
\zeta &= \hat{H_E}(k) - \alpha \hat{H_A}(k-1), \\
&= H_E(k) - \epsilon_E(k) - \alpha H_A(k-1) + \alpha \epsilon_A(k-1).
\end{aligned} \tag{12}$$

In this equation, while $H_A(k-1)$ has normal Gaussian distribution, other terms have complex Gaussian distribution. This causes the uncertainty for obtaining theoretical distribution of

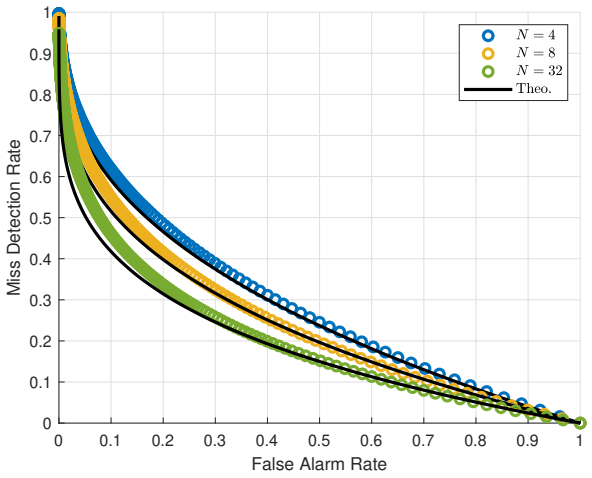

Fig. 2. MDR vs FAR analysis showing the impacts of different number of RIS reflecting elements where $\alpha = 0.9$, SNR=0 dB, $\kappa_A = \kappa_B = 0.1$ and $\kappa_E = 0.4$.

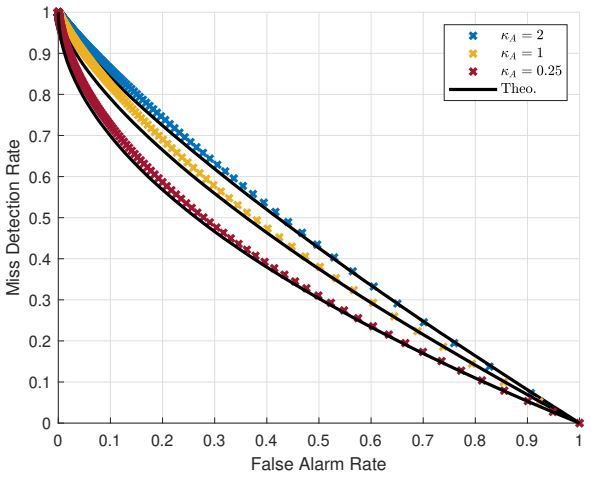

Fig. 3. MDR vs FAR analysis showing the effects of different Alice's hardware impairments where $\alpha = 0.9$, SNR=-10 dB, $\kappa_E = 2$ and $N = 32$.

ζ. Therefore, the theoretical analysis of MDR is not tractable due to the this complexity.

IV. Numerical Results

In this study, RIS-aided communication in the presence of a spoofing attack is investigated through numerical results validating theoretical analysis. The simulations are conducted using an end-to-end approach in a Rayleigh fading channel. Unless otherwise specified, the RIS behavior is configured to maximize the phase alignment for legitimate users. Our FAR-related theoretical findings for the PLA method align closely with the simulation results. In theoretical result curve included figures, we provide FAR theoretical results with MDR simulation results to compare theoretical and simulation results of FAR. Furthermore, the system parameters which are specified in the following paragraphs are selected as those values to obtain readable figures.

Fig. 2 illustrates the impact of the number of surface elements on the MDR and FAR performance under the conditions of $\alpha = 0.9$, $\kappa_A = \kappa_B = 0.1$, $\kappa_E = 0.4$, and an SNR value of 0 dB. It is clearly observed that as N increases, both MDR and FAR performance improve. For instance, increasing the number of surface elements from 4 to 32 can lead to a 52% improvement in the MDR value when the FAR is 0.3. Also, the theoretical results of FAR are very close to simulation results. When the slope of the curve is high such as $N = 32$ case, there are minimal differences with simulation results because the compound channel has real-valued distribution and AR process causes additive complex Gaussian distributed variable. The ϵ_A used in theoretical analysis has complex Gaussian distributed variables as well as compound channel, so the minimal differences are caused by this reason.

The impact of the RHI of the legitimate transmitter node on MDR and FAR is presented in Fig. 3 under the conditions of $\alpha = 0.9$, SNR = -10 dB, $\kappa_E = 2$, and $N = 32$. It is observed that the MDR and FAR improve as the RHI difference between the legitimate transmitter and the spoofing attacker increases. According to the results, in case of presence of attacker whose hardware impairment has larger than legitimate user, PLA is more reliable and provides less error rate of authentication. Also, it can be said that the PLA could be promising technique for detecting malicious IoT user since IoT users have larger hardware impairments. For instance, when the FAR is 0.5, MDR values of 0.42 and 0.3 can be achieved for RHI values of $\kappa = 2$ and $\kappa = 0.25$, respectively.

The impact of SNR on MDR and FAR performance in an RIS-aided communication environment under $\alpha = 0.9$, $N = 32$, $\kappa_A = \kappa_B = 0.1$, and $\kappa_E = 0.4$ is illustrated in Fig. 4. It can be clearly observed that the curve shape changes as the SNR increases. When the value of SNR rises, the decrease rate of MDR is higher than others. Therefore, it can be represented that MDR tends to decrease rapidly in case of increasing SNR. Consequently, the detection probability of the attacker becomes easier under a high SNR regime. For instance, when the MDR is 0.3, altering the SNR from -20 dB to -5 dB results in FAR values of 0.69 and 0.25, respectively.

The behavior of RIS on detection performance is critical for security applications. In this context, intelligent RIS transmissions are based on adjusting phase-shift elements to enhance the SNR of Bob. In the case of blind RIS transmission, the ϕ_i is set to zero for ease of implementation. We examine the impact of RIS behavior on MDR versus FAR in Fig. 5 under the conditions of $\alpha = 0.9$, $N = 32$, $\kappa_A = \kappa_B = 0.1$, and $\kappa_E = 0.4$ under 0 dB SNR. Also, we compare the authentication performance of RIS-aided network with the communication system which has only direct link to represent the impact of RIS on MDR and FAR. In Fig. 5, Ω shows the Rayleigh fading channel power. Unless otherwise stated, the channel power for direct link and individual channels is unit power. The findings indicate that configuring the phase-

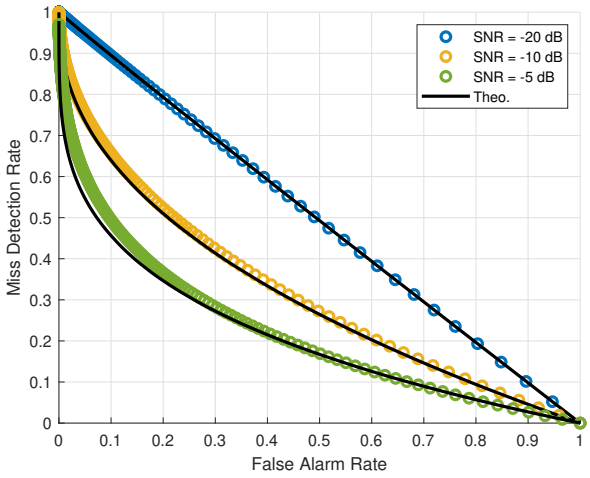

Fig. 4. MDR vs FAR analysis showing the influences of different SNR values where $\alpha = 0.9$, $N = 32$, $\kappa_A = \kappa_B = 0.1$ and $\kappa_E = 0.4$.

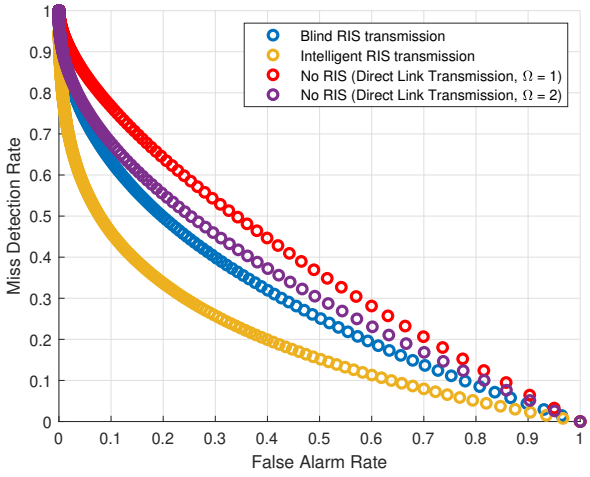

Fig. 5. MDR vs FAR analysis for comparison the performance effects of direct link, intelligent RIS transmission and blind RIS transmission where $\alpha = 0.9$, SNR=0 dB, $N = 32$, $\kappa_A = \kappa_B = 0.1$ and $\kappa_E = 0.4$.

shift matrix to align with legitimate transceiver pairs can improve detection performance. The utilization of intelligent RIS transmission provides significant enhancement compared to blind RIS transmission in terms of MDR and FAR. Furthermore, when we analyze the communication scenario with RIS and without RIS, it can be shown that the use of RIS significantly enhances authentication performance. Especially, it can be seen that RIS utilization provides better performance even compared to direct link scenario having better channel variance, i.e. when channel variance of direct link is 2. This result provides important insights about the positive effects of RIS usage on PLA performance. For instance, achieving a FAR of 0.2 is possible with MDR values of 0.64, 0.5, and 0.33 for scenarios without RIS, with blind RIS, and with intelligent RIS, respectively.

V. Conclusion

In this study, we have examined the impact of RHI on RIS-aided communication scenarios under spoofing attacks. Increasing the number of metasurface elements and SNR has been found to enhance detection performance with the aid of RIS. Additionally, the use of RIS has significantly improved MDR and FAR performance. We have also compared the behavior of phase-shift matrices in detecting spoofing attacks. Our findings have indicated that a higher RHI for Eve helps in detecting spoofing attacks with the assistance of RIS. Furthermore, investigation of different channel fading models' impact on RIS-aided authentication could be a possible research area in future works.

Acknowledgement

This work was supported by The Scientific and Technological Research Council of Turkey (TUBITAK) through the 1515 Frontier Research and Development Laboratories Support Program under Project 5169902, and has been partly funded by the European Commission through the Horizon Europe/JU SNS project ROBUST-6G (Grant Agreement no. 101139068).

References

[1] M. Guo, Z. Lin, R. Ma, *et al.*, "Inspiring physical layer security with RIS: Principles, applications, and challenges," *IEEE Open Journal of the Communications Society*, 2024.

[2] H. Alakoca, M. Namdar, S. Aldirmaz-Colak, *et al.*, "Metasurface manipulation attacks: Potential security threats of RIS-aided 6G communications," *IEEE Communications Magazine*, vol. 61, no. 1, pp. 24–30, 2022.

[3] R. Kaur, B. Bansal, S. Majhi, S. Jain, C. Huang, and C. Yuen, "A survey on reconfigurable intelligent surface for physical layer security of next-generation wireless communications," *IEEE Open Journal of Vehicular Technology*, 2024.

[4] W. Khalid, M. A. U. Rehman, T. Van Chien, Z. Kaleem, H. Lee, and H. Yu, "Reconfigurable intelligent surface for physical layer security in 6G-IoT: Designs, issues, and advances," *IEEE Internet of Things Journal*, vol. 11, no. 2, pp. 3599–3613, 2023.

[5] M. Srinivasan, L. Senigagliesi, H. Chen, A. Chorti, M. Baldi, and H. Wymeersch, "AoA-based physical layer authentication in analog arrays under impersonation attacks," *arXiv preprint arXiv:2407.08282*, 2024.

[6] J. He, M. Niu, P. Zhang, and C. Qin, "Enhancing PHY-layer authentication in RIS-assisted IoT systems with cascaded channel features," *IEEE Internet of Things Journal*, 2024.

[7] S. Tomasin, H. Zhang, A. Chorti, and H. V. Poor, "Challenge-response physical layer authentication over partially controllable channels," *IEEE Communications Magazine*, vol. 60, no. 12, pp. 138–144, 2022.

[8] M. M. Selim and S. Tomasin, "Physical layer authentication with simultaneous reflecting and sensing RIS," in *2023 IEEE 97th Vehicular Technology Conference (VTC2023-Spring)*, IEEE, 2023, pp. 1–5.

[9] M. A. Shawky, S. T. Shah, M. S. Mollel, *et al.*, "Reconfigurable intelligent surface-assisted cross-layer authentication for secure and efficient vehicular communications," *arXiv preprint arXiv:2303.08911*, 2023.

[10] P. Zhang, Y. Teng, Y. Shen, X. Jiang, and F. Xiao, "Tag-based PHY-layer authentication for RIS-assisted communication systems," *IEEE Transactions on Dependable and Secure Computing*, vol. 20, no. 6, pp. 4778–4792, 2023.

[11] A. Bendaimi, A. Abdallah, A. Celik, A. Eltawil, and H. Arslan, "How to leverage double-structured sparsity of RIS channels to boost physical layer authentication," *IEEE Wireless Communications Letters*, 2024.

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

[13] P. Chen, L. Yang, H. Liu, G. Pan, Y. Li, and Z. Yan, "Active RIS-NOMA-aided covert communication with hardware impairments," *IEEE Wireless Communications Letters*, 2023.

[14] L. Zhai, Y. Zou, and J. Zhu, "Robust transmission design for RIS-assisted multi-cluster wireless powered communications with hardware impairments," *IEEE Transactions on Communications*, 2024.

[15] W.-Y. Chen, C.-Y. Wang, R.-H. Hwang, W.-T. Chen, and S.-Y. Huang, "Impact of hardware impairment on the joint reconfigurable intelligent surface and robust transceiver design in MU-MIMO system," *IEEE Transactions on Mobile Computing*, vol. 23, no. 5, pp. 3993–4008, 2023.

[16] Q. Chen, M. Li, X. Yang, R. Alturki, M. D. Alshehri, and F. Khan, "Impact of residual hardware impairment on the IoT secrecy performance of RIS-assisted NOMA networks," *IEEE Access*, vol. 9, pp. 42 583–42 592, 2021.

[17] Z. Peng, R. Weng, C. Pan, G. Zhou, M. Di Renzo, and A. L. Swindlehurst, "Robust transmission design for RIS-assisted secure multiuser communication systems in the presence of hardware impairments," *IEEE Transactions on Wireless Communications*, vol. 22, no. 11, pp. 7506–7521, 2023.

[18] P. Zhang, T. Taleb, X. Jiang, and B. Wu, "Physical layer authentication for massive mimo systems with hardware impairments," *IEEE Transactions on Wireless Communications*, vol. 19, no. 3, pp. 1563–1576, 2020.

[19] G. Zhou, C. Pan, H. Ren, K. Wang, and Z. Peng, "Secure wireless communication in RIS-aided MISO system with hardware impairments," *IEEE Wireless Communications Letters*, vol. 10, no. 6, pp. 1309–1313, 2021.

[20] E. Basar, "Transmission through large intelligent surfaces: A new frontier in wireless communications," in *2019 European Conference on Networks and Communications (EuCNC)*, 2019, pp. 112–117.

[21] E. Basar, M. Di Renzo, J. De Rosny, M. Debbah, M.-S. Alouini, and R. Zhang, "Wireless communications through reconfigurable intelligent surfaces," *IEEE access*, vol. 7, pp. 116 753–116 773, 2019.

[22] L. Xiao, L. J. Greenstein, N. B. Mandayam, and W. Trappe, "Channel-based spoofing detection in frequency-selective rayleigh channels," *IEEE Transactions on Wireless Communications*, vol. 8, no. 12, pp. 5948–5956, 2009.