Physical-Layer Challenge-Response Authentication with IRS and Single-Antenna Devices

Anna V. Guglielmi, Laura Crosara, Stefano Tomasin, and Nicola Laurenti
Dept. of Information Engineering (DEI), University of Padova, Italy
email: {annavaleria.guglielmi@ , laura.crosara.1@phd. , nicola.laurenti@, stefano.tomasin@ }unipd.it

2024 IEEE International Conference on Communications Workshops (ICC Workshops) | 979-8-3503-0405-3/24/$31.00 ©2024 IEEE | DOI: 10.1109/ICCWORKSHOPS59551.2024.10615677

***Abstract*—This paper focuses on a novel challenge-response physical layer authentication (CR-PLA) mechanism for wireless communications. It integrates an intelligent reflecting surface (IRS) under the control of the receiver, which operates as a verifier for the identity of the transmitter. In CR-PLA, the verifier randomly configures the IRS and then checks that the resulting estimated channel is correspondingly modified. We address the trade-off between communication and security performance, in terms of average signal-to-noise ratio (SNR) and missed detection (MD) probability of an impersonation attack, respectively. In particular, we design the probability distribution of the random IRS configuration that maximizes the average receiver SNR under an upper bound constraint on the MD and false alarm (FA) probabilities, for the special case where both the transmitter and the receiver are equipped with a single antenna. Numerical results demonstrate effective balancing of communication metrics and security requirements, suggesting that CR-PLA is a promising solution for future secure wireless communication.**

***Index Terms*—Authentication, Challenge-response, Intelligent Reflecting Surfaces, Physical-Layer Security.**

I. Introduction

Establishing whether a received message truly comes from the legitimate sender or has been forged by an impersonating attacker describes the user authentication problem. If unauthenticated messages are accepted, several risks might occur that go from denial of service to privacy or the loss of control of devices, e.g., in Internet of Things (IoT) contexts.

In the literature, several authentication mechanisms have been proposed, mostly operating at the application layer and using cryptographic approaches. Here, we exploit the propagation characteristics of the physical channel as a signature of the communication link or the transmitting device, in what is known as physical layer authentication (PLA). In [1], the basic approach is introduced: it consists of two phases, i.e., the identification acquisition and the identification verification phases. In the first phase, the receiver Bob (verifier) estimates the channel from signals transmitted by Alice (the authentic source). Higher-layer mechanisms, e.g., based on cryptography, are used to authenticate the signals. In the second phase, whenever Bob receives a new message, he also estimates the channel over which the transmitted signal has propagated and compares this estimate with that in the first phase. If the two are consistently similar (considering that they are both affected by noise), the received message is stated as authentic, otherwise, it is assumed fake. Several technologies, including orthogonal frequency division multiplexing (OFDM), multiple-input multiple-output (MIMO) [2], [3] and underwater acoustic communications [4], employed PLA, using different testing techniques, from Neyman-Pearson tests [5] to machine learning approaches [6]. For an overview on PLA, we refer the reader to [7], [8].

Recently, the controllable nature of wireless channels provided by new communication technologies has been exploited for further improvement of PLA. Specifically, the propagation of wireless signals can be modified using intelligent reflecting surfaces (IRSs), i.e., controllable devices, where the phase shift introduced by each element can be changed. Indeed, when the verifier controls the IRS, he can set a random configuration of the IRS which remains secret to the attacker, and verify that the channel estimated from a received message corresponds to the predicted channel according to the set configuration, [9]. Such an approach provides a *challenge response PLA (CR-PLA)* mechanism, where the random configuration is the challenge and the predicted channel is the expected response. Such an approach can be applied also when other *controllable channels* are available, e.g., when Bob is a drone that changes its position to pose a challenge [10].

In this paper, we aim to design the random IRS configuration of the CR-PLA mechanism. We focus on the simple scenario where both the legitimate transmitter and the verifier are equipped with a single antenna, and the number of elements in the IRS is large. First, we observe that the random IRS configuration affects the data rate of the communication link between the user equipment (UE) and base station (BS). In particular, increasing its randomness yields in general a lower missed detection (MD) probability while also lowering the communication performance. To measure the communication performance we consider the signal-to-noise ratio (SNR) averaged over the random IRS configuration. Then, we consider a generalized likelihood ratio test (GLRT) at the verifier to make the decision about the authenticity of the message and analyze the performance of the CR-PLA scheme in terms of both false alarm (FA) and MD probabilities. Lastly, we design the probability distribution of the randomly selected phase shifts that

This work has been funded in part by the European Commission through the Horizon Europe/JU SNS project ROBUST-6G (Grant Agreement no. 101139068).

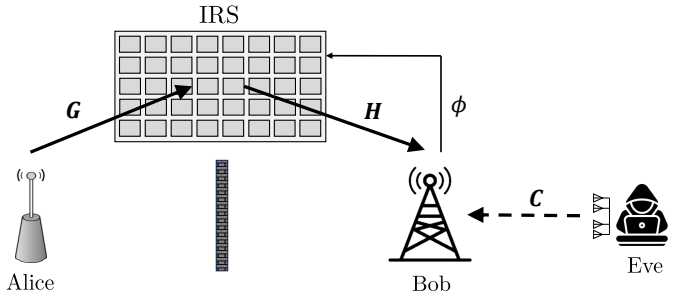

Fig. 1. Communication scenario.

maximize the average SNR under an upper bound constraint on the MD probability for a desired FA probability. In particular, we identify two statistical properties (represented by two real numbers) that capture the effects of the probability density function (pdf) on both the communication and the security metrics, so that the pdf design problem boils down to the optimization of these two parameters, under other constraints. In the design, we consider the worst-case scenario for the defense, by assuming that the attacker has complete channel knowledge, which is a challenging condition in practice.

The rest of the paper is organized as follows. Section II presents the system model and the CR-PLA mechanism. Then, the authentication strategy design is detailed in Section III. In particular, in Section III-A and Sections III-B III-C the communication and the security performance are introduced, respectively; whereas in Section III-D, the design of probability distribution of the randomly selected IRS phase shifts is presented. Numerical results are discussed in Section IV and, finally, conclusions are drawn in Section V.

II. System Model

We analyze the scenario depicted in Fig. 1, where Bob, the receive BS, authenticates messages from the UE Alice, the legitimate transmitter. An attacker Eve aims to impersonate Alice by forging messages and transmitting them to Bob. We assume that all devices (Alice, Bob, and Eve) have a single antenna each.

The communication between Alice and Bob is supported by an IRS with N reflecting elements, each acting as a receive and transmit antenna. In particular, each element has unitary gain and introduces a phase shift $\phi_n = e^{j\theta_n}$, $n = 1, 2, \ldots, N$, on the equivalent baseband signal. We define vector $\boldsymbol{\phi}$ and matrix $\boldsymbol{\Phi}$ as

$$\boldsymbol{\Phi} = \mathrm{diag}\{\boldsymbol{\phi}\} = \mathrm{diag}\{[\phi_1, \phi_2, \ldots, \phi_N]\}. \tag{1}$$

Bob controls the IRS by choosing the phase control matrix $\boldsymbol{\Phi}$ using a secure dedicated channel not accessible to Eve.

We assume that communication between Alice and Bob only happens through the IRS without any additional direct link (for instance, because a direct link is not available). We define $\boldsymbol{G} \in \mathbb{C}^{N\times 1}$ as the vector for the baseband equivalent channel from Alice to IRS, and $\boldsymbol{H} \in \mathbb{C}^{1\times N}$ as the vector of the channel from IRS to Bob. The resulting Alice-IRS-Bob cascade channel random gain is

$$Q_{\mathrm{AIB}} = \boldsymbol{H}\boldsymbol{\Phi}\boldsymbol{G}\,. \tag{2}$$

In the considered scenario, Eve can transmit messages to Bob through a direct channel with gain $C \in \mathbb{C}$.

All channels are assumed to be time-invariant, while the IRS configuration (i.e., the matrix $\boldsymbol{\Phi}$) is under Bob's control and can be changed over time, making the cascade channels controllable. We consider correlated Rayleigh fading channels, thus all entries of the channel vectors $\boldsymbol{H}$ and $\boldsymbol{G}$ are zero-mean complex Gaussian with unitary power and identity correlation matrix. However, most of the obtained derivations could be applied to a more general channel model.

A. CR-PLA Mechanism

The CR-PLA mechanism [9] works as follows. In the *identification association* phase, Alice transmits authenticated pilot signals to Bob who, in turn, estimates the cascade channel Q_{AIB} for several IRS configurations. Such an estimate will then enable Bob to obtain a reference estimate of the cascade channel for *any* IRS configuration $\boldsymbol{\Phi}$

$$\overline{Q}_{\mathrm{AIB}}(\boldsymbol{\Phi}) = Q_{\mathrm{AIB}}(\boldsymbol{\Phi}) + \overline{W}\,, \tag{3}$$

where $\overline{W}$ is the estimation error at Bob, modeled as additive white Gaussian noise (AWGN) with zero mean and power σ^2_{B}.

In the *identification verification* phase, Bob sets a random configuration of the IRS (that constitutes the *challenge*), according to the pdf $p_{\boldsymbol{\Phi}}(\boldsymbol{\Phi})$, and whenever he receives a message, he estimates the cascade channel $\hat{Q}_{\mathrm{AIB}}(\boldsymbol{\Phi})$ and checks if it corresponds to the expected channel $\overline{Q}_{\mathrm{AIB}}(\boldsymbol{\Phi})$.

Under legitimate conditions, when Alice is transmitting Bob estimates the Alice-IRS-Bob cascade channel, i.e.,

$$\hat{Q}_{\mathrm{AIB}} = Q_{\mathrm{AIB}} + W_{\mathrm{B}}\,, \tag{4}$$

where W_{B} is the estimation error at Bob, modeled as AWGN with zero mean and power σ^2_{B}.

B. Attacker Model

We consider a *perfect channel knowledge* scenario in which Eve knows the realizations of $\boldsymbol{H}$, $\boldsymbol{G}$ and C. This assumption, although being generous to Eve, constitutes a worst-case situation for the legitimate receiver. Consequently, it is a conservative approach when investigating authentication mechanisms.

Moreover, we assume that for the attack Eve transmits directly to Bob and she can precode the transmitted pilot to induce any channel estimate to Bob apart from the estimation noise. Thus, when under attack, Bob estimates

$$V = V_0 + W_{\mathrm{B}}\,. \tag{5}$$

where V_0 is the channel forged by Eve. Note that, since gain C is known to Eve, she can pre-compensate it before transmission, thus it becomes irrelevant in our scenario. Moreover, assuming that Eve is equipped with more antennas is also irrelevant, as Bob has a single antenna.

C. Authentication Test

When performing the authentication check, Bob leverages his knowledge of $\overline{Q}_{\mathrm{AIB}}$. Let the channel estimate at Bob be

$$R = \begin{cases} \hat{Q}_{\mathrm{AIB}} & \text{if Alice is transmitting } (b=0)\,, \\ V & \text{if Eve is transmitting } (b=1)\,, \end{cases} \tag{6}$$

with b indicating the legitimate/attack state. The purpose of Bob is to figure out whether the estimated channel R corresponds to the authentic one $\hat{Q}_{\mathrm{AIB}}$, or to a forged channel V, by using his knowledge of $\overline{Q}_{\mathrm{AIB}}$. Thus, Bob performs an authentication test, wherein, given $\overline{Q}_{\mathrm{AIB}}$ and R, he chooses between two hypotheses, i.e., $\mathcal{H}_0$ if the message is from Alice, and $\mathcal{H}_1$ if the message is from Eve. Therefore, the authentication procedure outputs a Boolean value $\hat{b}$, and correct verification is achieved if $\hat{b} = b$.

Since Eve can perform a variety of attacks V_0, we consider that the receiver employs a GLRT, which is appropriate in case of unknown V statistics. Let $f_{\hat{Q}|\mathcal{H}_0}$ be the pdf of $\hat{Q}$ under hypothesis $\mathcal{H}_0$. The generalized log-likelihood function is

$$\Psi = \log f_{\hat{Q}|\mathcal{H}_0}(R). \tag{7}$$

Under hypothesis $\mathcal{H}_0$, and conditioned on the configuration $\boldsymbol{\Phi'}$ chosen by Bob, R has a Gaussian distribution with mean $\overline{Q}_{\mathrm{AIB}}$

$$R = \overline{Q}_{\mathrm{AIB}}(\boldsymbol{\Phi'}) + W_{\mathrm{B}} - \overline{W}. \tag{8}$$

Let $W = W_{\mathrm{B}} - \overline{W}$ represents the overall noise with per-entry variance $\sigma^2 = 2\sigma_{\mathrm{B}}^2$. Thus, (7) becomes

$$\Psi = \frac{2}{\sigma^2}|R - \overline{Q}_{\mathrm{AIB}}(\boldsymbol{\Phi'})|^2, \tag{9}$$

neglecting irrelevant constants. According to GLRT, Ψ is then compared with respect to a threshold τ, and the authentication procedure outputs

$$\hat{b} = \begin{cases} 0 & \Psi < \tau\,, \\ 1 & \Psi \geq \tau\,. \end{cases} \tag{10}$$

III. Authentication Strategy Design

To perform the CR-PLA mechanism, Bob needs to randomly select the IRS configuration to generate the challenge. However, the random IRS configuration selected in the identification phase, while providing authentication capabilities, affects the data rate of the communication link between Alice and Bob. Therefore, we aim to properly design the pdf of the IRS configuration $p_{\boldsymbol{\Phi}}(\boldsymbol{\Phi})$ to get a tradeoff between the security metrics and the resulting achievable rate of the legitimate channel. First, note that under the two hypotheses (7) can be written as

$$\Psi = \frac{2}{\sigma^2}|\delta|^2, \tag{11}$$

with

$$\delta = \begin{cases} W\,, & \text{under hypothesis } \mathcal{H}_0 \\ V_0 - \boldsymbol{H}\boldsymbol{\Phi}\boldsymbol{G} + W\,, & \text{under hypothesis } \mathcal{H}_1. \end{cases} \tag{12}$$

A. Communication Performance

Having assumed a single-antenna transmitter and receiver, the communication-optimal IRS configuration can be expressed in closed form. Indeed, the communication-optimal IRS configuration maximizing the SNR at the receiver is

$$\overline{\theta}_n = \alpha - \angle H_n - \angle G_n, \tag{13}$$

with $n = 0, \ldots, N-1$ and α the angle common to all the IRS elements. To simplify the following computation, we consider $\alpha = 0$ without loss of generality.

For a given IRS configuration $\boldsymbol{\Phi}$, the resulting achievable rate of the Alice-Bob channel is

$$C_{A,B}(\boldsymbol{\Phi}) = \log_2\left(1 + \frac{|\sum_{n=0}^{N-1} H_n G_n e^{j\theta_n}|^2}{\sigma_B^2}\right), \tag{14}$$

which depends on the instantaneous SNR

$$\omega = \frac{|\sum_{n=0}^{N-1} H_n G_n e^{j\theta_n}|^2}{\sigma_B^2}. \tag{15}$$

In the identification phase, we assume that Bob modifies the IRS configuration around the optimal one, obtaining a new phase shift as

$$\theta_n = \overline{\theta}_n + \epsilon_n, \tag{16}$$

with ϵ_n a random variable. Moreover, we assume that ϵ_n are independent and identically distributed for all the IRS elements and that the pdf of ϵ_n is even. This simplifies the design of the defense strategy, so more complex solutions where ϵ_n are correlated and may have different statistics are left for future study. Under these assumptions, the problem of designing $p_{\boldsymbol{\Phi}}(\boldsymbol{\Phi})$ becomes the problem of designing the pdf p_ϵ of ϵ_n.

For communication performance evaluation we consider the average SNR $\Omega = \mathbb{E}[\omega]$, for which we now derive an approximate expression depending on some statistical properties of ϵ_n.

In particular, let us consider the asymptotic case $N \to \infty$. Then, let us define

$$m = \mathbb{E}[e^{j\epsilon_n}] = \mathbb{E}[\cos\epsilon_n] + j\mathbb{E}[\sin\epsilon_n]. \tag{17}$$

Assuming that p_ϵ is even, the second term vanishes and

$$m = \mathbb{E}[\cos\epsilon_n]. \tag{18}$$

Similarly, we define

$$s = s_R + j s_I = \mathbb{E}[\cos^2\epsilon_n] + j\mathbb{E}[\sin^2\epsilon_n] \tag{19}$$

and we have $\mathbb{E}[\cos\epsilon_n \sin\epsilon_n] = 0$ for symmetry reasons.

The mean of each term of the sum in (14) can then be written as

$$\begin{aligned} \mu_{sec} =& \mathbb{E}[H_n G_n e^{j\theta_n}] = \mathbb{E}[|H_n G_n| e^{j\epsilon_n}] \\ =& \mathbb{E}[|H_n|]\mathbb{E}[|G_n|]\mathbb{E}[e^{j\epsilon_n}] = \frac{\pi}{4} m \end{aligned} \tag{20}$$

with variance

$$\begin{aligned}\sigma_{sec}^2 =&\mathbb{E}[|H_n G_n e^{j\theta_n} - \mu_{sec}|^2] \\ =&1 - \mu_{sec}^2 = 1 - \frac{\pi^2}{16} m^2,\end{aligned} \tag{21}$$

since H_n, G_n, and $e^{j\theta_n}$ are independent and $|H_n|$, $|G_n|$ are Rayleigh variables with zero mean and variance $\frac{1}{2}$. By using the central limit theorem, we approximate the sum in (14) as Gaussian distributed, with mean[1] $N\mu_{sec}$ and variance $N\sigma_{sec}^2$.

Therefore, the average SNR depends on m and goes to ∞ as

$$\begin{aligned}\Omega \approx \frac{N\sigma_{\text{sec}}^2}{2\sigma_{\text{B}}^2}\left(2 + \frac{2N^2\mu_{\text{sec}}^2}{N\sigma_{\text{sec}}^2}\right) = \frac{N}{\sigma_{\text{B}}^2}(N\mu_{\text{sec}}^2 + \sigma_{\text{sec}}^2) \\ = \frac{N}{\sigma_B^2}\left((N-1)\frac{\pi^2}{16}m^2 + 1\right) = \Omega(m).\end{aligned} \tag{22}$$

Due to the relation between the achievable rate and the SNR, for ease of computation, we refer to the asymptotic approximate average SNR $\Omega(m)$ as the communication performance.

B. Security Performance

The two possible error events of the authentication mechanism are FAs when Bob discards a message as forged by Eve while it is coming from Alice, and MDs when Bob accepts a message coming from Eve as legitimate. Specifically, an FA occurs when, under hypothesis $b = 0$, $\Psi \geq \tau$, whereas, an MD occurs when, under hypothesis $b = 1$, $\Psi < \tau$. As security metrics of the CR-PLA mechanism, we then consider the probabilities of FA and MD.

In formulas, for a given Alice-IRS-Bob channel and any configuration $\boldsymbol{\Phi'}$, we define then the probability of FA and MD respectively as

$$P_{\text{FA}} = P[\Psi \geq \tau | \hat{b} = 0]\,, \tag{23}$$

$$P_{\text{MD}}(\zeta(V, \boldsymbol{\Phi'})) = P[\Psi < \tau | \hat{b} = 1]\,. \tag{24}$$

Under the legitimate condition $\mathcal{H}_0$, by plugging (8) into (9), we have that Ψ becomes a central chi-square random variable with 2 degrees of freedom and

$$P_{\text{FA}} = 1 - F_{\chi^2,0}(\tau), \tag{25}$$

denoting with $F_{\chi^2,a}(\cdot)$ the cumulative distribution function (CDF) of a non-central chi-square variable with 2 degrees of freedom and non-centrality parameter a.

[1]Note that for a circularly symmetric complex random variable y with non zero complex mean $M = M_r + jM_I$ and real variance S^2, the mean of $|y|^2$ is

$$\begin{aligned}\mathbb{E}[|M+Sw|^2] = \frac{S^2}{2}\mathbb{E}\left[\left(M_R\frac{\sqrt{2}}{S}+\sqrt{2}w_R\right)^2 + \left(M_I\frac{\sqrt{2}}{S}+\sqrt{2}w_I\right)^2\right] \\ = \frac{S^2}{2}(2+\lambda),\end{aligned}$$

with $\lambda = \frac{2|M|^2}{S^2}$ and assuming $w = w_R + jw_I$ circularly symmetric complex Gaussian random variable with zero mean and unitary variance.

Under hypothesis $\mathcal{H}_1$ with attack V_0, using (6) and replacing (5) in (9), Ψ becomes a non-central chi-square random variable with 2 degrees of freedom and non-centrality parameter

$$\zeta(V, \boldsymbol{\Phi'}) = \frac{2}{\sigma^2}||V - \overline{Q}_{\text{AIB}}(\boldsymbol{\Phi'})||^2\,, \tag{26}$$

for a given IRS configuration $\boldsymbol{\Phi'}$. The P_{MD} represents the CDF of this variable evaluated at τ, that is

$$P_{\text{MD}}(\zeta(V, \boldsymbol{\Phi'})) = F_{\chi^2,\zeta(V,\boldsymbol{\Phi'})}(\tau). \tag{27}$$

It is worth noting that the choice of τ is typically set to reach a desired P_{FA}, i.e.,

$$\tau = F_{\chi^2,0}^{-1}(1 - P_{\text{FA}}), \tag{28}$$

and the MD probability becomes

$$P_{\text{MD}}(\zeta(V, \boldsymbol{\Phi'})) = F_{\chi^2,\zeta(V,\boldsymbol{\Phi'})}(F_{\chi^2,0}^{-1}(1 - P_{\text{FA}})). \tag{29}$$

In the following, we consider the average P_{MD}, i.e., $\overline{P}_{\text{MD}} = \mathbb{E}[F_{\chi^2,\zeta(V,\boldsymbol{\Phi'})}(\tau)]$, assuming that V is fixed (i.e., Eve performs a deterministic attack), whereas $\boldsymbol{\Phi'}$ is random. Note that the expectation is done with respect to the distribution of ϕ_n, $n = 0, \ldots, N-1$.

C. Average MD Probability

We now derive the MD probability under a specific attack by Eve and we express it as a function of key statistical parameters for ϵ_n, similarly to what we did for the average SNR.

Attack Strategy: Since Eve does not know the IRS configuration, we assume here that Eve uses as attack the average channel seen by Bob when Alice is transmitting, i.e., she sets the attack channel as $V_0 = \mathbb{E}[Q_{\text{AIB}}]$, where the mean is evaluated with respect to the random IRS configuration. So,

$$V_0 = \boldsymbol{H}\mathbb{E}[\boldsymbol{\Phi}]\boldsymbol{G} = \boldsymbol{H}\overline{\boldsymbol{\Phi}}\mathbb{E}[\text{diag}\{e^{j\epsilon_n}\}]\boldsymbol{G} = m\boldsymbol{H}\overline{\boldsymbol{\Phi}}\boldsymbol{G}. \tag{30}$$

Test Variable: Under attack V_0 (12) becomes

$$\begin{aligned}\delta = m\boldsymbol{H}\overline{\boldsymbol{\Phi}}\boldsymbol{G} - \boldsymbol{H}\boldsymbol{\Phi'}\boldsymbol{G} + W \\ = \sum_{n=0}^{N-1} H_n e^{j\overline{\theta}_n}[m - e^{j\epsilon_n}]G_n + W.\end{aligned} \tag{31}$$

MD Probability: Under attack V_0 the probability $\overline{P}_{\text{MD}}$ can be written as

$$\overline{P}_{\text{MD}} = \mathbb{P}\left[\frac{2}{\sigma^2}|\delta|^2 < \tau\right], \tag{32}$$

and we then investigate the statistics of each term of the sum in (31) to derive an expression for $\overline{P}_{\text{MD}}$.

Specifically, due to the Rayleigh scenario, and from the symmetry of p_ϵ, the terms in the sum of (31) are i.i.d with mean $\mathbb{E}\left[H_n e^{j\overline{\theta}_n}[m - e^{j\epsilon_n}]G_n\right] = 0$, and with real and imaginary parts of the variance defined as

$$\begin{aligned}\sigma_R^2 =&\mathbb{E}\left[\text{Re}\left\{H_n e^{j\overline{\theta}_n}[m - e^{j\epsilon_n}]G_n\right\}^2\right] \\ =&\mathbb{E}\left[(m - \cos\epsilon_n)^2\right] = -m^2 + s_R\end{aligned} \tag{33}$$

$$\sigma_I^2 = \mathbb{E}\left[\text{Im}\left\{H_n e^{j\overline{\theta}_n}[m - e^{j\epsilon_n}]G_n\right\}^2\right] = s_I \tag{34}$$

where $s_R = \mathbb{E}[\cos^2 \epsilon_n]$ and $s_I = \mathbb{E}[\sin^2 \epsilon_n]$. The corresponding cross-correlation is

$$\begin{aligned}\mathbb{E}\Big[\mathrm{Re}\left\{H_n e^{j\bar{\theta}_n}\left[m - e^{j\epsilon_n}\right] G_n\right\} \times \\ \mathrm{Im}\left\{H_n e^{j\bar{\theta}_n}\left[m - e^{j\epsilon_n}\right] G_n\right\}\Big] \\ = \mathbb{E}\left[(m - \cos\epsilon_n)(-\sin\epsilon_n)\right] = \mathbb{E}\left[\cos\epsilon_n \sin\epsilon_n\right] = 0.\end{aligned} \tag{35}$$

By the Central Limit Theorem, for $N \to \infty$, $\delta = \delta_R + j\delta_I$ has a complex zero-mean Gaussian distribution with independent real and imaginary parts with variances $\sigma^2_{\delta,R} = N\sigma^2_R + \frac{\sigma^2}{2}$ and $\sigma^2_{\delta,I} = N\sigma^2_I + \frac{\sigma^2}{2}$, respectively, which are functions of m and s_R through (33) and (34). Finally, from (32) and the results in (33)-(35), we approximate $\overline{P}_{\mathrm{MD}}$ as

$$\begin{aligned}\overline{P}_{\mathrm{MD}} &= \mathbb{P}\left[\delta_R^2 + \delta_I^2 \le \frac{\sigma^2\tau}{2}\right] \\ &\approx \mathbb{P}\left[\sigma^2_{\delta,R} g_1^2 + \sigma^2_{\delta,I} g_2^2 \le \frac{\sigma^2\tau}{2}\right],\end{aligned} \tag{36}$$

where g_1 and g_2 are real Gaussian variables with zero mean and unitary variance. Still $\overline{P}_{\mathrm{MD}}$ depends on m, s_R, and the desired $\overline{P}_{\mathrm{FA}} = P_{\mathrm{FA}}(\tau)$, i.e., $\overline{P}_{\mathrm{MD}}(m, s_{\mathrm{R}}, \tau)$.

To evaluate (36), we need the CDF of a linear combination of two independent central chi-squared random variables with one degree of freedom each. This CDF cannot be expressed in closed form; however, a series can be computed by following [11]. Let us define $\alpha_1 = \sigma^2_{\delta,R}$, $\alpha_2 = \sigma^2_{\delta,I}$, $\beta = \frac{\alpha_1+\alpha_2}{2}$, then we have

$$\begin{aligned}\overline{P}_{\mathrm{MD}}(m, s_{\mathrm{R}}, \tau) = \frac{e^{-\frac{\sigma^2\tau}{4\beta}}}{(2\beta)^2} \frac{\sigma\sqrt{\frac{\tau}{2}}}{\Gamma(2)} \times \\ \sum_{k=0}^{K=\infty} \frac{k! m_k}{(2)_k} L_k^{(1)}\left(\frac{\sigma^2\tau}{2\beta}\right),\end{aligned} \tag{37}$$

where

$$\begin{aligned}m_0 &= 2(2\beta)^2 \prod_{i=1}^{2} (\beta + \alpha_i)^{-1/2} \\ m_k &= \frac{1}{k}\sum_{j=0}^{k-1} m_j d_{k-j}, k \ge 1 \\ d_j &= (-1)^j + \sum_{i=1}^{2} \frac{1}{2}\left(\frac{\beta - \alpha_i}{\beta + \alpha_i}\right)^j, j \ge 1,\end{aligned} \tag{38}$$

and $L_k^{(\alpha)}$ the k-th generalized Laguerre polynomial.

D. Design of the pdf p_ϵ

For a desired $\overline{P}_{\mathrm{FA}}$, we derived that m and s_R are the only parameters on which the communication and security metrics depend, i.e., (22) and (37) , respectively. Our goal is to find the optimal p_ϵ balancing the communication metrics and security requirements. From (16), we aim at finding a feasible p_ϵ such that $\Omega(m)$ is maximized assuring that $\overline{P}_{\mathrm{MD}}(m, s_{\mathrm{R}}, \tau)$ is kept below a certain threshold η.

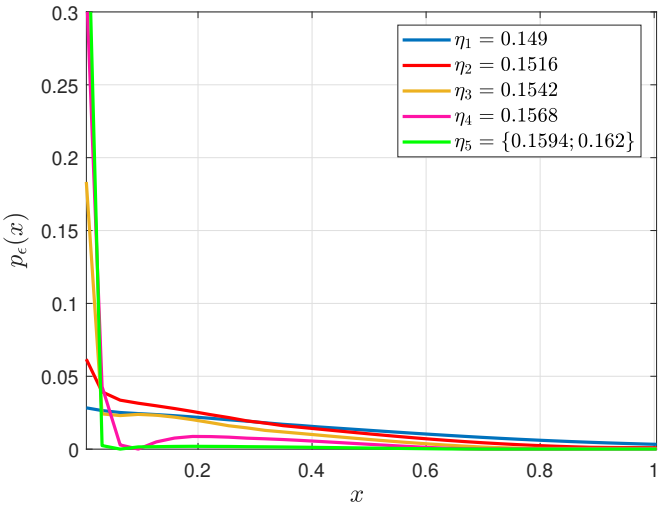

Fig. 2. Probability distribution of ϵ_n considering $\overline{P}_{\mathrm{FA}} = 10^{-3}$, $N = 100$, $\sigma_B = 0.6$, and $\eta \in \mathcal{T} = \{0.149, 0.1516, 0.1542, 0.1568, 0.1594, 0.162\}$.

Thus, we consider the following optimization problem

$$\begin{aligned}\arg\max_{m} \quad & \Omega(m) = \max_{p_\epsilon} \int_{-\infty}^{\infty} \cos(\alpha) p_\epsilon(\alpha) d\alpha \\ \text{s.t.} \quad & \overline{P}_{\mathrm{MD}}(m, s_R, \tau) < \eta \\ & \int_{-\infty}^{\infty} p_\epsilon = 1 \\ & P_{\mathrm{FA}}(\tau) = \overline{P}_{\mathrm{FA}} \\ & p_\epsilon \ge 0.\end{aligned} \tag{39}$$

Note that the problem of designing the pdf of the continuous random variable ϵ_n becomes now the problem of optimizing some of its statistical parameters (namely, m and s_R), which provides a much more tractable optimization problem.

We numerically solve (39) by looking for the $(m^\star, s_R^\star)$ pairs, such that $P_{\mathrm{MD}}(m^\star, s_R^\star) < \eta$, that are feasible solution of the system

$$\begin{cases}\int_{-\infty}^{\infty} \cos(\alpha) p_\epsilon(\alpha) d\alpha = m \\ \int_{-\infty}^{\infty} \cos^2(\alpha) p_\epsilon(\alpha) d\alpha = s_R \\ \int_{-\infty}^{\infty} p_\epsilon(\alpha) d\alpha = 1 \\ p_\epsilon(\alpha) \ge 0 \\ m^2 < s_R \le m\end{cases}. \tag{40}$$

Note that for the sake of computation, we consider ϵ_n as a discrete random variable. Consequently, (40) becomes a linear system with positive solutions. Among the feasible $(m^\star, s_R^\star)$ pairs, we choose then that with the maximum $m^\star$.

IV. Numerical Results

In this Section, we validate the above analysis providing numerical evidence of the balance between communication metrics and security requirements as the result of the optimization problem (39).

Fig. 2 shows the optimal p_ϵ obtained for $\overline{P}_{\mathrm{FA}} = 10^{-3}$, $N = 100$, $\sigma_B = 0.6$, and

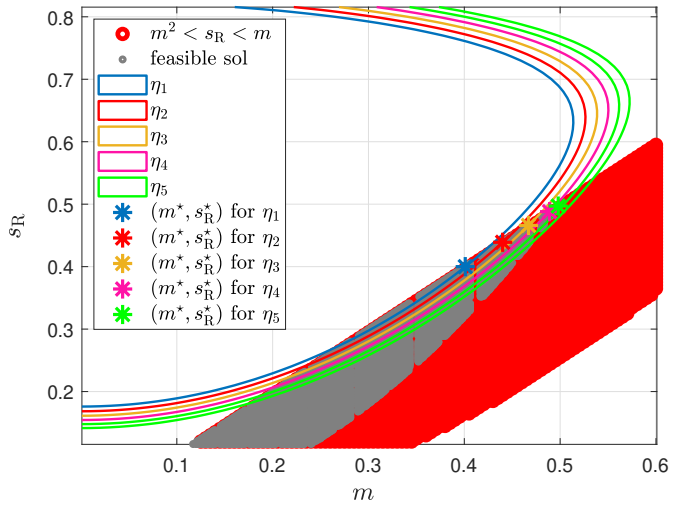

Fig. 3. $\overline{P}_{\mathrm{MD}}(m, s_R, \tau)$ contour plot at levels $\mathcal{T}$, the area defining the pairs (m, s_R) such $m^2 < s_R \leq m$ (in red), the area representing the feasible solutions of (40) (in grey), and the optimal $(m^\star, s_R^\star)$ (stars). The different colors refer to the different considered $\eta \in \mathcal{T}$.

$\eta \in \mathcal{T}=\{0.149, 0.1516, 0.1542, 0.1568, 0.1594, 0.162\}$. It can be seen that for $\eta \geq 0.1594$ the optimal p_ϵ remains the same, whereas for $\eta < 0.149$ any solution solving (39) can be found.

This can be better observed in Fig. 3 where we show the $\overline{P}_{\mathrm{MD}}(m, s_R, \tau)$ contour plot at levels $\mathcal{T}$, the area defined by the pairs (m, s_R) such that $m^2 < s_R \leq m$ (red area), the area representing the feasible solutions of (40) (grey area), and the optimal $(m^\star, s_R^\star)$ pairs (stars) for $\overline{P}_{\mathrm{FA}} = 10^{-3}$. The different colors refer to the different considered η, with $\eta \in \mathcal{T}$. In general, the higher η is, the higher would be $m^\star$, i.e., the more p_ϵ would be defined around zero. This would imply a higher $m^\star$ and then a higher $\Omega(m^\star)$ at the cost of a security degradation due to the reduction in the randomness of $\mathbf{\Phi}$.

To find a tradeoff between Ω and $\overline{P}_{\mathrm{MD}}$, Fig. 4 shows the $\overline{P}_{\mathrm{MD}}(m^\star, s_R^\star, \tau)$ as a function of $\Omega(m^\star)$. In particular, we consider different values of $\overline{P}_{\mathrm{FA}}$ in the set $\{10^{-4}, 10^{-3}, 10^{-2}, 10^{-1}\}$, $N = 100$, and $\sigma_B^2 = 0.6$. It can be seen as for a desired $\overline{P}_{\mathrm{FA}}$, a higher $\Omega(m^\star)$ comes at the expense of a higher $\overline{P}_{\mathrm{MD}}(m^\star, s_R^\star, \tau)$. Furthermore, the smaller the desired $\overline{P}_{\mathrm{FA}}$ is, the smaller the reduction of $\Omega(m^\star)$ in dB would be, if the minimum possible $\overline{P}_{\mathrm{MD}}(m^\star, s_R^\star, \tau)$ is assured. However, the smaller the $\overline{P}_{\mathrm{FA}}$ is, the smaller the minimum $\overline{P}_{\mathrm{MD}}(m^\star, s_R^\star, \tau)$ that can be ensured.

V. Conclusions

In this paper, we have considered a CR-PLA mechanism that leverages the presence of an IRS to perform the challenge-response protocol. We have derived the probability distribution of the randomly selected phase shifts, optimizing the tradeoff between the average SNR of the legitimate channel and the security metrics. We have derived approximate expressions for the FA and MD probabilities, and the average SNR for the special case of single-antenna devices. Numerical results show that a high average SNR would come at the expense of a reduction of MD probability and vice versa.

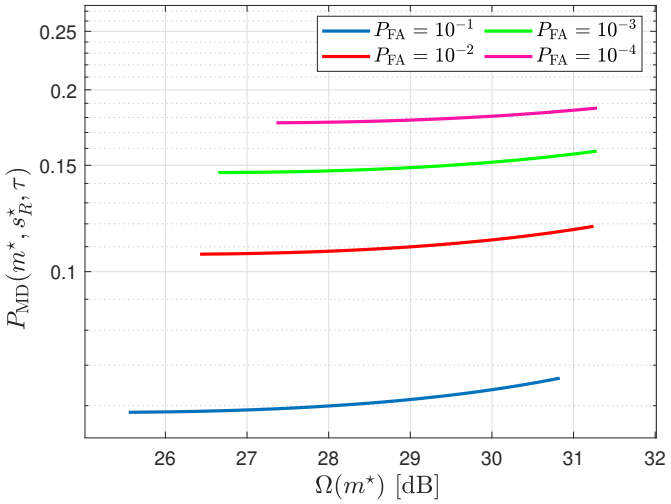

Fig. 4. $\overline{P}_{\mathrm{MD}}(m^\star, s_R^\star, \tau)$ as a function of $\Omega(m^\star)$ for $\overline{P}_{\mathrm{FA}} \in \{10^{-4}, 10^{-3}, 10^{-2}10^{-1}\}$, $N = 100$, and $\sigma_B^2 = 0.6$

References

[1] G. J. Simmons, "Authentication theory/coding theory," in *Advances in Cryptology*, G. R. Blakley and D. Chaum, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 1985, pp. 411–431.

[2] P. Baracca, N. Laurenti, and S. Tomasin, "Physical layer authentication over MIMO fading wiretap channels," *IEEE Trans. Wireless Commun.*, vol. 11, no. 7, pp. 2564–2573, 7 2012.

[3] W. Hou, X. Wang, J.-Y. Chouinard, and A. Refaey, "Physical layer authentication for mobile systems with time-varying carrier frequency offsets," *IEEE Transactions on Communications*, vol. 62, no. 5, pp. 1658–1667, 2014.

[4] R. Diamant, P. Casari, and S. Tomasin, "Cooperative authentication in underwater acoustic sensor networks," *IEEE Trans. Wireless Commun.*, vol. 18, no. 2, pp. 954–968, Feb. 2019.

[5] U. M. Maurer, "Authentication theory and hypothesis testing," *IEEE Transactions on Information Theory*, vol. 46, no. 4, p. 1350–1356, July 2000.

[6] H. Fang, X. Wang, and L. Hanzo, "Learning-aided physical layer authentication as an intelligent process," *IEEE Transactions on Communications*, vol. 67, no. 3, pp. 2260–2273, 2019.

[7] E. Jorswieck, S. Tomasin, and A. Sezgin, "Broadcasting into the uncertainty: Authentication and confidentiality by physical-layer processing," *Proceedings of the IEEE*, vol. 103, no. 10, pp. 1702–1724, 10 2015.

[8] N. Xie, Z. Li, and H. Tan, "A survey of physical-layer authentication in wireless communications," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 1, pp. 282–310, 2021.

[9] 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.

[10] F. Mazzo, S. Tomasin, H. Zhang, A. Chorti, and H. V. Poor, "Physical-layer challenge-response authentication for drone networks," in *Proc. IEEE Global Commun. Conference (GLOBECOM)*, 2023.

[11] A. Castaño-Martínez and F. López-Blázquez, "Distribution of a sum of weighted noncentral chi-square variables," *Test*, vol. 14, pp. 397–415, 2005.