Challenge-Response PLA with Amplify and Forward Relay: Design and Experimental Validation

Sanaz Baradaran Rowhani[1], Anna V. Guglielmi[1], Davide Scazzoli[2], Maurizio Magarini[2], and Stefano Tomasin[1]
[1] Dept. of Information Engineering, University of Padova, Italy
[2] Dip. di Elettronica, Informazione e Bioingegneria, Politecnico di Milano, Milan, Italy.
email: {sanaz.baradaranrowhani,annavaleria.guglielmi,stefano.tomasin}@unipd.it, {davide.scazzoli,maurizio.magarini}@polimi.it

***Abstract*—Future wireless communication systems will require new security mechanisms to support devices with limited capabilities. We consider a wireless communication link assisted by an amplify-and-forward relay and propose a novel challenge-response physical layer authentication (PLA) mechanism. The authentication-verifying receiver randomly configures the relay and verifies that the measured received power changes accordingly. We design the distribution of the random choice to maximize the average capacity while ensuring an upper bound on misdetection and false alarm probabilities of the authentication test. The performance is assessed by experiments in an indoor scenario with a relay, operating at the 60 GHz Industrial Medical and Scientific frequency band, equipped with 16 antennas organized in a planar array. The trade-off between achieved rate and security is investigated.**

***Index Terms*—Authentication, Challenge-response, AF Relay, Physical-Layer Security.**

I. Introduction

User authentication ensures that a received message originates from the legitimate sender rather than an impersonating attacker. Traditional authentication mechanisms, primarily operating at the application layer, rely on cryptographic techniques. However, an alternative approach, i.e., physical layer authentication (PLA), leverages the propagation characteristics of the physical channel as a unique signature of the communication link from the transmitting device. First introduced in [1], PLA has been applied to various technologies, including orthogonal frequency division multiplexing (OFDM), multiple-input multiple-output (MIMO) [2], [3], and underwater acoustic communications [4]. Authentication techniques range from Neyman-Pearson hypothesis testing [5] to machine learning-based methods [6]. For a comprehensive review of PLA, see [7], [8].

Here, we focus on the recent evolution of PLA exploiting partially controllable wireless channels whose electromagnetic characteristics (*channel configurations*) can be controlled by the receiver. A challenge response PLA (CR-PLA) mechanism has been introduced in [9], where the receiver first estimates the channel from the legitimate transmitter under several channel configurations; then, upon a new transmission, it randomly sets the channel configuration and checks that the estimated channel matches the selected configuration. In [10], a CR-PLA mechanism has been considered that leverages the presence of an intelligent reflecting surface (IRS) with controllable element phases to secure communication among single-antenna devices. The probability distribution of the randomly selected IRS phase shifts has been derived to optimize the tradeoff between the average signal-to-noise ratio (SNR) of the legitimate channel and the security metrics. CR-PLA has also been applied to drone communications [11] and focusing on the design of attack strategies [12].

In this paper, we consider a wireless communication link assisted by an amplify-and-forward (AF) relay equipped with multiple antennas, under the control of the receiver. The end-to-end channels vary based on the combining and beamforming coefficients of the receive and transmit antennas of the relay (named *relay configuration*) and the transmitter's position. Hence, a partially controllable channel is obtained, and the CR-PLA mechanism can be implemented. The relay configurations are taken from a finite set and we optimize the distribution of the random configuration used in CR-PLA. Such optimization takes into account both communication and security performance, as different relay configurations yield different transmission rates, while the distribution has an impact on the missed detection (MD) and false alarm (FA) probabilities of the CR-PLA mechanism. In particular, we aim to find the distribution that maximizes the data rate, with an upper bound on the MD and FA probabilities. In the design, we consider the worst-case scenario for the defense, where the attacker has complete channel knowledge, which is a challenging condition in practice. We then investigate the performance of the proposed solution in an experimental indoor communication scenario, where the AF relay includes two planar arrays of 8×2 antennas, and both transmitter and receiver have each a planar array of 8×2 antennas. Transmissions occur at the 60 GHz Industrial Medical and Scientific (ISM) frequency band with a bandwidth of 1 GHz. Different positions of the legitimate transmitter and different beam directions for both the transmitter and relay are tested, and the corresponding received power is measured.

The paper is organized as follows. Sec. II introduces the system model and CR-PLA mechanism. The authentication strategy is detailed in Sec. III, where the communication and security metrics are defined. In Sec. IV, the design of the probability distribution of the randomly selected relay configuration

This work was supported by the European Union under the Italian National Recovery and Resilience Plan (NRRP) Mission 4, Component 2, Investment 1.3, CUP C93C22005250001, partnership on "Telecommunications of the Future" (PE00000001 - program "RESTART").

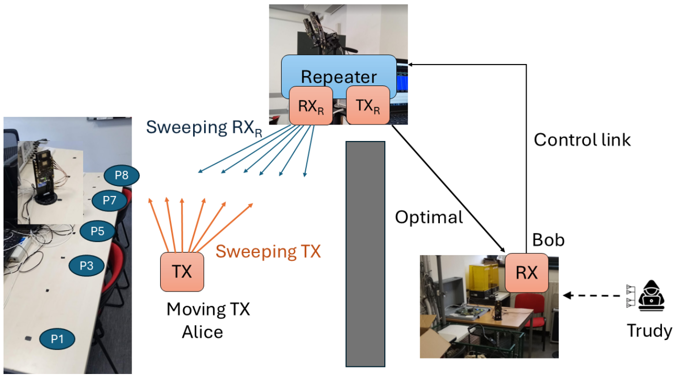

Fig. 1. Communication scenario.

is presented. Sec. V discusses the experimental validation, with Sec. V-A detailing the dataset, and Sec. V-B presenting numerical results. Conclusions are drawn in Sec. VI.

II. System Model

We consider the scenario of Fig. 1, where Bob, the receiver, authenticates messages from Alice, the legitimate transmitter. An attacker Trudy aims to impersonate Alice by forging messages to Bob. Alice, Bob, and Trudy are equipped with N_A, N_B, and N_E antennas, respectively.

The communication between Alice and Bob is supported by an AF relay including two planar antenna arrays, with N_I and N_O antennas, to receive and transmit signals, respectively: once received, baseband-equivalent signals are combined with a combining beamformer providing a scalar complex signal, which is then amplified and transmitted with the array after proper precoding beamforming. The precoding and combining vectors are designed to receive (transmit) signals from azimuth angles θ_I (θ_O) and elevation angles ϕ_I (ϕ_O). The steering vector $\boldsymbol{a}_N(\theta,\phi)$ has entries $[\boldsymbol{a}_N(\theta,\phi)]_n = e^{j\frac{2\pi d}{\lambda}\{(n-1)\sin\theta\cos\phi+(m-1)\sin\phi\}}$, $n = 1,\ldots,N_x$, $m = 1,\ldots,N_z$, where N_x and N_z denote the number of antennas in the x-axis and z-axis, respectively, λ is the wavelength at the carrier frequency, and d the distance between consecutive antennas. The resulting phase control matrix of the AF relay (due to the combiner and the precoder) is

$$\boldsymbol{\Phi} = \mathcal{A}\cdot\boldsymbol{a}_{N_\mathrm{O}}(\theta_O,\phi_O)\cdot\boldsymbol{a}^H_{N_\mathrm{I}}(\theta_I,\phi_I), \tag{1}$$

where $\mathcal{A}$ is a fixed amplification coefficient. Matrix $\boldsymbol{\Phi}$ identifies the current *relay configuration* to be used for authentication and communication purposes. Note that (1) can be equivalently used to describe a fully connected IRS where typically A=1 [13]. However, in our analysis, the relay amplifies the incident signal rather than only reflecting it with the adjustable phase shift as in the case of the passive IRS.

The angles θ and ϕ are taken from a finite alphabet. This is done to replicate the behavior of the hardware used for the experimental captures and the set of possible relay configurations is $\mathcal{F} = \{\boldsymbol{\Phi}_1,\ldots,\boldsymbol{\Phi}_F\}$.

Bob controls the AF relay by choosing the phase control matrix $\boldsymbol{\Phi}$ using a secure dedicated channel inaccessible to Trudy. We assume that communication between Alice and Bob only happens through the AF relay, while the direct link is not available. We define $\boldsymbol{G}\in\mathbb{C}^{N_I\times N_A}$ as the matrix for the baseband equivalent channel from Alice to the AF relay, and $\boldsymbol{H}\in\mathbb{C}^{N_B\times N_O}$ as the matrix of the channel from the AF relay to Bob. We now consider that for any relay configuration, Alice and Bob determine the beamformer used at the transmitter ($\boldsymbol{q}$) and at the receiver ($\boldsymbol{v}$) that maximizes the resulting end-to-end scalar complex channel gain

$$h = \boldsymbol{v}^T\boldsymbol{H}\boldsymbol{\Phi}\boldsymbol{G}\boldsymbol{q}. \tag{2}$$

Note that $\boldsymbol{v}$ and $\boldsymbol{q}$ are a function of $\boldsymbol{H}\boldsymbol{\Phi}\boldsymbol{G}$ although we do not indicate it explicitly for the sake of a simpler notation. For the various relay configurations, we have corresponding complex channel gains in the set

$$\mathcal{H} = \{h_1,\ldots,h_F\}. \tag{3}$$

All channels are assumed to be time-invariant, while the relay configuration (i.e., matrix $\boldsymbol{\Phi}$) is under Bob's control and changes over time, making the cascade channels controllable. In the considered scenario, the link between the relay and Bob remains fixed, meaning that $\boldsymbol{a}_{N_\mathrm{O}}(\theta_O,\phi_O)$ and the Bob's beamformer $\boldsymbol{v}$ are also fixed and optimized to convey most of the signal from the relay to Bob (through $\boldsymbol{H}$).

In the considered scenario, Trudy can transmit messages through a direct channel to Bob, who estimates the channel $g = \boldsymbol{v}^T\boldsymbol{Q}\boldsymbol{b}_T$, where $\boldsymbol{Q}$ is the channel matrix of the Trudy-Bob channel and $\boldsymbol{b}_T$ is the Trudy precoding matrix. We assume that Trudy knows $\boldsymbol{Q}$ and $\boldsymbol{v}$ and that she can choose a precoding that yields any channel g. Such a channel does not change with the chosen relay configuration.

A. CR-PLA Mechanism

The CR-PLA mechanism includes two phases: the *identification association* and *identification verification* phase. The identification association phase is performed every time Alice takes a new position or the surrounding channel changes. The identification verification phase is instead implemented on each received message at Bob. Thus, we assume that there are several message transmissions (thus identification verification phases) between two identification association phases.

Identification Association: Alice transmits authenticated pilot signals to Bob who, in turn, obtains an estimate $\tilde{h}_\ell$ of h_ℓ and measures the resulting received power

$$\overline{P}_\mathrm{B}(\ell) = |\tilde{h}_\ell|^2, \tag{4}$$

for all the relay configurations $\ell = 1,\ldots,F$. We assume that pilot symbols have unitary power. Bob relies on power for authentication instead of complex channel gain, as phase varies over time due to synchronization errors. Given small independent estimation errors (e.g., noise, imperfect channel gain, or small-scale fading), the central limit theorem approximates the received power as Gaussian. Thus, we have

$$\overline{P}_\mathrm{B}(\ell) \approx |h_\ell|^2 + w', \tag{5}$$

where w' is the estimation error at Bob, modeled as a real AWGN variable with zero mean and power σ_B^2.

Identification Verification: Bob sets a random configuration of the relay (that constitutes the *challenge*), according to the probability mass function (PMF)

$$p_{\mathbf{\Phi}}(\ell) = \mathbb{P}[\mathbf{\Phi} = \mathbf{\Phi}_\ell], \tag{6}$$

with $\mathbf{\Phi}_\ell \in \mathcal{F}$, and estimates the received power $\hat{P}_B$ and checks if it matches to the expected received power $\overline{P}_{\rm B}(\ell)$. Under legitimate conditions, when Alice transmits, the received power measured at Bob is again models as

$$\hat{P}_B \approx |h_\ell|^2 + w'' \,, \tag{7}$$

where w'' is the AWGN random variable with power σ_B^2 that describes the estimation error. In particular, since Trudy can perform a variety of attacks, we consider that the receiver employs a generalized likelihood ratio test (GLRT), which is appropriate in case of unknown attack statistics. Let $f_{\mathcal{H}_0}(\cdot)$ be the probability density function (pdf) of $\hat{P}_B$ under hypothesis $\mathcal{H}_0$ that Alice is transmitting. The GLRT function is $\Psi = \log f_{\mathcal{H}_0}(\hat{P}_B)$, i.e.,

$$\Psi = \frac{2}{\sigma^2} |\hat{P}_B - \overline{P}_B(\ell)|^2, \tag{8}$$

neglecting irrelevant constants. According to GLRT, Ψ is then compared with respect to a threshold τ, and the authentication procedure outputs $\hat{b} = 0$ if $\Psi < \tau$ and $\hat{b} = 1$ if $\Psi \geq \tau$.

B. Attack Model

We consider a scenario with *perfect channel knowledge*, where Trudy is assumed to know the exact channel realizations. While this assumption is generous to Trudy, it represents a worst-case scenario for the legitimate receiver. Therefore, it is a conservative approach when investigating authentication mechanisms.

Furthermore, we assume that during the attack Trudy transmits directly to Bob and she can precode the transmitted pilot to induce any channel estimate (thus power measurement) to Bob, apart from the estimation noise. Thus, when under attack (hypothesis $\mathcal{H}_1$), the power of the channel forged by Trudy is P_V and the power measured by Bob is

$$\hat{P}_B = P_V + w''. \tag{9}$$

III. Authentication Strategy Design

To perform the CR-PLA mechanism, Bob randomly selects the relay configuration to generate the challenge in the identification phase. However, this configuration affects also the data rate between Alice and Bob. Therefore, we aim at properly designing $p_{\mathbf{\Phi}}(\ell)$ to get a tradeoff between the security metrics and the resulting achievable rate of the legitimate channel. First, note that under the two hypotheses $\mathcal{H}_0$ and $\mathcal{H}_1$, Ψ can be written as

$$\Psi = \frac{2}{\sigma^2}|\delta|^2, \tag{10}$$

with

$$\delta = \begin{cases} w = -w' + w'' \,, & \text{under hypothesis } \mathcal{H}_0 \\ P_{\rm V} - \overline{P}_B(\ell) + w'' \,, & \text{under hypothesis } \mathcal{H}_1 \end{cases} \tag{11}$$

where w is AWGN with zero mean and power $2\sigma_B^2$.

A. Communication Performance

For a given configuration $\mathbf{\Phi}_\ell \in \mathcal{F}$ ($\ell = 1, \ldots, F$), the resulting achievable rate of the end-to-end channel directly follows from Shannon formula, i.e,

$$C_{A,B}(\ell) = \log_2 \left(1 + \frac{|h_\ell|^2}{\sigma_B^2}\right). \tag{12}$$

B. Security Performance

The two possible error events of the authentication mechanism are FA if Bob rejects a message as forged by Trudy when it comes from Alice, and MD if Bob accepts a message coming from Trudy as legitimate. Notably, an FA occurs when, under the hypothesis that Alice transmits, we have $\Psi \geq \tau$; whereas, an MD occurs when, under the hypothesis that Trudy is transmitting, we have $\Psi < \tau$. As security metrics for the CR-PLA, we consider then the probabilities of FA and MD.

In formulas, for a given power measurement and any relay configuration, we define the probability of FA and MD, respectively, as

$$P_{\rm FA} = \mathbb{P}[\Psi \geq \tau | \mathcal{H}_0] \,, \quad P_{\rm MD} = \mathbb{P}[\Psi < \tau | \mathcal{H}_1] \,. \tag{13}$$

Under the legitimate condition $\mathcal{H}_0$, we have that $\Psi{=}\frac{2}{\sigma^2}|w|^2$ becomes a central chi-square random variable with 1 degree of freedom. Then, the FA probability is defined as $P_{\rm FA} = 1 - F_{\chi_1^2,0}(\tau)$, denoting with $F_{\chi_1^2,0}(\cdot)$ the cumulative distribution function (CDF) of a central chi-square variable with 1 degree of freedom.

Under hypothesis $\mathcal{H}_1$, for a given configuration $\mathbf{\Phi}_\ell \in \mathcal{F}$ we have that

$$\Psi = \frac{2}{\sigma^2}|P_{\rm V} - \overline{P}_B(\ell) + w''|^2 \tag{14}$$

is a non-central chi-square random variable with 1 degrees of freedom and non-centrality parameter $\zeta(P_{\rm V}, \mathbf{\Phi}_\ell) = \frac{2}{\sigma^2}|P_{\rm V} - \overline{P}_{\rm B}(\ell)|^2$. Therefore, the MD probability is the CDF of this variable evaluated at τ, i.e.,

$$P_{\rm MD}(\zeta(P_{\rm V}, \mathbf{\Phi}_\ell)) = F_{\chi^1,\zeta(P_{\rm V},\mathbf{\Phi}_\ell)}(\tau). \tag{15}$$

The choice of τ is usually set to reach a desired $\overline{P}_{\rm FA}$, i.e.,

$$\tau = F^{-1}_{\chi_1^2,0}(1 - \overline{P}_{\rm FA}), \tag{16}$$

and the MD probability becomes

$$P_{\rm MD}(\zeta(P_{\rm V}, \mathbf{\Phi}_\ell)) = F_{\chi_1^2,\zeta(P_{\rm V},\mathbf{\Phi}_\ell)}\left(F^{-1}_{\chi_1^2,0}(1 - \overline{P}_{\rm FA})\right). \tag{17}$$

C. Attack Strategy

Since Trudy does not know the used relay configuration, we consider as attack P_V the average channel power seen by Bob when Alice is transmitting, i.e.,

$$P_{\rm V}(p_{\mathbf{\Phi}}) = \frac{1}{F}\sum_{\ell=1}^{F} p_{\mathbf{\Phi}}(\ell)|h_\ell|^2. \tag{18}$$

It is worth noting that the attack depends on the PMF $p_{\mathbf{\Phi}}$.

Therefore, when under attack, (11) becomes

$$\delta = \frac{1}{F}\sum_{\ell'=1}^{F} p_{\mathbf{\Phi}}(\ell')|h_{\ell'}|^2 - \overline{P}_B(\ell) + w''. \tag{19}$$

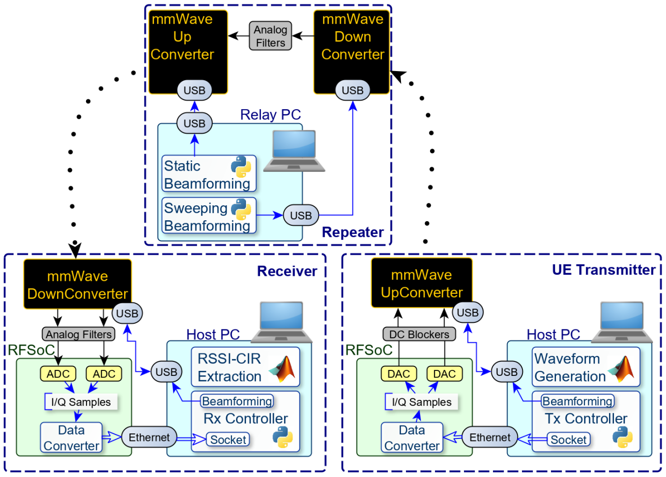

Fig. 2. Hardware and software components used to generate the dataset.

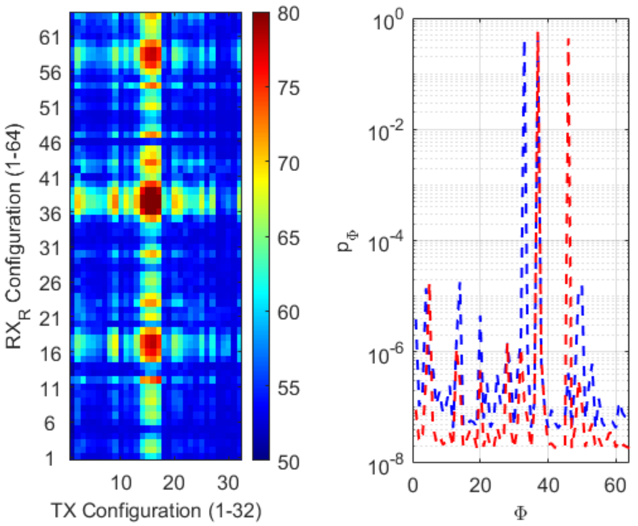

Fig. 3. Heatmap of the received powers [dB] when Alice is in position P_1, varying both Alice beamformer and relay configuration (on the left). Optimal $p_{\mathbf{\Phi}}(\mathbf{\Phi})$ as a function of $\mathbf{\Phi}$ for a desired $\overline{P}_{\rm FA} = 5\cdot 10^{-2}$, where blue dashed curve is for $\eta = 0.15$ and red dashed curve is for $\eta = 0.038$ (on the right).

As a metric to assess the validity of this attack, we consider the average $P_{\rm MD}$, i.e.,

$$\overline{P}_{\rm MD}=\mathbb{E}[F_{\chi^1,\zeta(P_{\rm V},\mathbf{\Phi}_\ell)}(\tau)]=\frac{1}{F}\sum_{\ell=1}^{F} p_{\mathbf{\Phi}}(\ell)P_{\rm MD}(\zeta(P_{\rm V}(p_{\mathbf{\Phi}}),\mathbf{\Phi}_\ell)). \quad (20)$$

Note that Trudy performs a deterministic attack and the expectation in $\overline{P}_{\rm MD}$ is done concerning the PMF of the relay configurations chosen by Bob.

IV. Design of $p_{\mathbf{\Phi}}(\ell)$

Our goal is to find the optimal $p_{\mathbf{\Phi}}(\ell)$ that balances the communication metrics and security requirements. Specifically, for a desired $\overline{P}_{\rm FA}$ we aim at finding $p_{\mathbf{\Phi}}(\ell)$ such that maximizes the average $C_{\rm A,B}$

$$\overline{C}_{\rm A,B} = \frac{1}{F}\sum_{\ell=1}^{F} C_{\rm A,B}(\ell)p_{\mathbf{\Phi}}(\ell), \quad (21)$$

while ensuring that the $\overline{P}_{\rm MD}$ is below a threshold η.

We consider then the following optimization problem

$$\begin{aligned} &\max_{\{p_{\mathbf{\Phi}}(\ell)\}} \overline{C}_{\rm A,B} \\ &\text{s.t.} \quad \overline{P}_{\rm MD} \leq \eta, \quad P_{\rm FA}(\tau) = \overline{P}_{\rm FA}, \\ &\qquad \sum_{\ell=1}^{F} p_{\mathbf{\Phi}}(\ell) = 1, \quad 0 \leq p_{\mathbf{\Phi}}(\ell) \leq 1. \end{aligned} \quad (22)$$

We resort to a numerical approach to solve (22).

V. Experimental Validation

A. Dataset Description

The components used for the experiment are shown in Fig. 2. Signal generation and acquisition are handled by an RFSoC ZCU111 [14], which integrates an UltraScale+ FPGA with ADCs and DACs, both operating at 4096 Msps sampling rate. To optimize data rates while maintaining full analog bandwidth, hardware upsampling and decimation by a factor of 2 are applied. The RFSoC interfaces, with analog up- and down-converters, are implemented using four EVK06003 evaluation kits [15]. These kits perform frequency conversion to the 60 GHz mmWave ISM band and enable analog beamforming. Each module features a half-duplex RF front end with 16 transmit/receive antennas, where the half-duplex constraint arises from the thermal limitations of the evaluation kit. Analog beamforming is implemented using pre-configured phase shifters per antenna, enabling azimuthal steering for θ from -54° to +54° in 5.4° steps. The elevation angles ϕ are fixed at +18°, 0°, and -18°, due to the 2×8 antenna array configuration. This setup results in a codebook of 63 beams plus a single omnidirectional beam, which activates only one antenna. The codebook defines the set of all possible precoding or combining vectors, $\boldsymbol{a}_N(\theta, \phi)$. Six double sweep captures are performed with the transmitter placed in positions P_1, P_3, P_5, P_7, and P_8 (see Fig. 1). The first three positions are spaced 40 cm apart, while the remaining positions have a 20 cm spacing. P_1 to P_5 are oriented normal parallel to the relay, while P_7 and P_8 are rotated by 45° due to the angle between the transmitter and the relay reaching the limit of 54°.

B. Numerical Results

Here, we validate the above analysis providing numerical evidence of the balance between communication metrics and security requirements resulting from optimization problem (22).

The left side of Fig. 3 shows the powers measured by Bob when Alice is placed in P_1, varying her beamformer and relay configuration among all the possible solutions. For the sake of space, we limit the x-axis to the Alice beamformer index of 32. It can be seen that the received power is significantly affected by the choice of Alice beamformer and relay configuration.

Moreover, for fixed Alice beamformer and relay configuration, the received power varies with Alice's position. Therefore, the choice of the communication-optimal relay configuration varies when different positions for Alice are considered. Let us define the optimal beamformer for Alice as the one conveying most of the signal to the relay. Then, the communication-optimal relay configuration is found in the very dark red area in the heatmap. However, other relay configurations are close to the optimum in terms of received power (and thus data rate) and can be used by Bob as the challenge to provide authentication without significantly affecting the data rate. This is further confirmed by the right side of Fig. 3 that shows the optimal $p_{\mathbf{\Phi}}$ as a function of $\mathbf{\Phi}_\ell \in \mathcal{F}$ for Alice in P_1 (with optimal beamformer) and a desired $\overline{P}_{\rm FA} = 5 \cdot 10^{-2}$. The blue dashed curve refers to $\eta = 0.15$, while the red dashed curve to $\eta = 0.038$. It can be seen that Bob does not choose the communication-optimal relay configuration with probability 1 for the challenge generation: approximately the 50% of the time Bob will choose another configuration as a consequence of the tradeoff between the communication and security metrics. Furthermore, the choice of this other configuration varies with the position of Alice as well as η, i.e., the constraint imposed on the $\overline{P}_{\rm MD}$.

The left side of Fig. 4 shows the average rate $\overline{C}_{\rm A,B}$ obtained with the optimal $p_{\mathbf{\Phi}}$ as a solution of (22) and as a function of $\overline{P}_{\rm MD}$. Here we consider the optimal beamformer for Alice but vary her positions and consider $\overline{P}_{\rm FA} = 5 \cdot 10^{-2}$. It can be seen as for a desired $\overline{P}_{\rm FA}$, a higher capacity is obtained at the expense of a higher $\overline{P}_{\rm MD}$ regardless of the considered position. However, for a target $\overline{C}_{\rm A,B}$ some positions are more convenient than others in terms of security: for the defense mechanism, it is better to have Alice in P_1 rather than any other positions since in P_1 a smaller $\overline{P}_{\rm MD}$ is reached. The right side of Fig. 4 shows $\overline{C}_{\rm A,B}$ with the optimal $p_{\mathbf{\Phi}}$ as a function of $\overline{P}_{\rm MD}$ for positions P_1 and P_7 and $\overline{P}_{\rm FA} = 5 \cdot 10^{-2}$ (solid line), $\overline{P}_{\rm FA} = 2.5 \cdot 10^{-2}$ (dashed-dotted line), and $\overline{P}_{\rm FA} = 10^{-2}$ (dashed line). It can be seen that the smaller the desired $\overline{P}_{\rm FA}$ is, the smaller the reduction of the average capacity in dB would be if the minimum possible $\overline{P}_{\rm MD}$ is assured. Moreover, the smaller the $\overline{P}_{\rm FA}$ is, the smaller the minimum $\overline{P}_{\rm MD}$ that can be ensured.

VI. Conclusions

In this paper, we have considered a CR-PLA mechanism that leverages the presence of an AF relay to perform the CR-PLA mechanism. We have derived the probability distribution of the randomly selected relay configurations, optimizing the tradeoff between the average rate of the legitimate channel and the security metrics. The performance is assessed by experiments in an indoor scenario and numerical results show that a high average rate would come at the expense of a reduction of MD probability and vice versa.

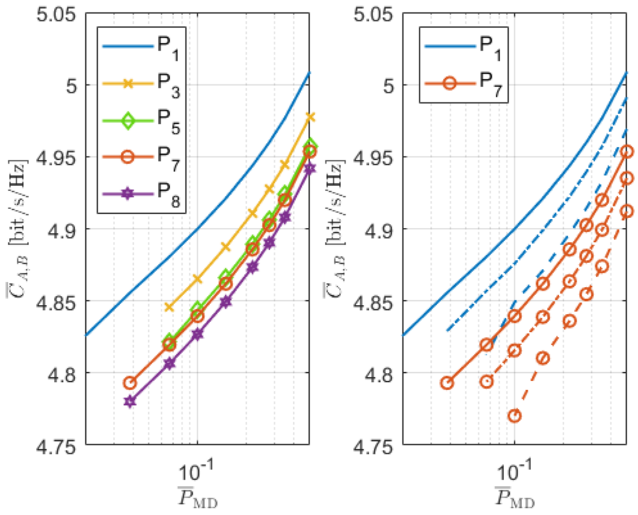

Fig. 4. $\overline{C}_{A,B}$ obtained by considering the optimal $p_{\mathbf{\Phi}}$ as a solution of (22) as a function of $\overline{P}_{\rm MD}$. On the left, we vary Alice's positions and set the desired $\overline{P}_{\rm FA} = 5 \cdot 10^{-2}$. On the right, we consider Alice in positions P_1 and P_7 and $\overline{P}_{\rm FA} = 5 \cdot 10^{-2}$ (solid line), $\overline{P}_{\rm FA} = 2.5 \cdot 10^{-2}$ (dashed-dotted line), and $\overline{P}_{\rm FA} = 1 \cdot 10^{-2}$ (dashed line).

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, Jul. 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 Trans. Commun.*, vol. 62, no. 5, pp. 1658–1667, May 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 Trans. Inf. 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 Trans. Commun.*, vol. 67, no. 3, pp. 2260–2273, Mar. 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 Commun. Surv. Tutor.*, vol. 23, no. 1, pp. 282–310, Jan. 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, Dec. 2022.

[10] A. V. Guglielmi, L. Crosara, S. Tomasin, and N. Laurenti, "Physical-layer challenge-response authentication with IRS and single-antenna devices," in *Proc. of IEEE Int. Conf. Commun. Workshops*, 2024, pp. 560–565.

[11] 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.

[12] L. Crosara, A. V. Guglielmi, N. Laurenti, and S. Tomasin, "Divergence-minimizing attack against challenge-response authentication with IRSs," in *Proc. IEEE Int. Conf. on Comm. Workshops (ICC worksh.)*, 2024.

[13] S. Shen, B. Clerckx, and R. Murch, "Modeling and architecture design of reconfigurable intelligent surfaces using scattering parameter network analysis," *Trans. Wireless. Comm.*, vol. 21, no. 2, p. 1229–1243, Feb. 2022. [Online]. Available: https://doi.org/10.1109/TWC.2021.3103256

[14] AMD. Zynq ultrascale+ rfsoc zcu111 evaluation kit. [Online]. Available: https://www.xilinx.com/products/boards-and-kits/zcu111.html

[15] S. Semiconductors. Evaluation kits and evaluation boards. [Online]. Available: https://www.sivers-semiconductors.com/sivers-wireless/wireless-products/evaluation-kits/