Challenge-Response to Authenticate Drone Communications: A Game Theoretic Approach

Mattia Piana, *Student Member, IEEE*, Francesco Ardizzon, *Member, IEEE*, and Stefano Tomasin, *Senior Member, IEEE*

***Abstract*—As drones are increasingly used in various civilian applications, the security of drone communications is a growing concern. In this context, we propose novel strategies for challenge-response physical layer authentication (CR-PLA) of drone messages. The ground receiver (verifier) requests the drone to move to a defined position (challenge), and authenticity is verified by checking whether the corresponding measured channel gain (response) matches the expected statistic. In particular, the challenge is derived from a mixed strategy obtained by solving a zero-sum game against the intruder, which in turn decides its own positions. In addition, we derive the optimal strategy for multi-round authentication, where the CR-PLA procedure is iterated over several rounds. We also consider the energy minimization problem, where legitimate users want to minimize the energy consumption without compromising the security performance of the protocol. The performance of the proposed scheme is tested in terms of both security and energy consumption through numerical simulations, considering different protocol parameters, different scenarios (urban and rural), different drone altitudes, and also in the context of drone swarms.**

***Index Terms*—Authentication, challenge-response, Drone communications, game theory, and physical layer security.**

I. Introduction

THE use of drones has rapidly increased over the last few years. Starting as a military tool, they are now used in many civil applications such as precision agriculture, environmental monitoring, and disaster management and relief. As drones become integrated into more complex systems, security is a rising concern [1]. Among the major threats, the transmission of jamming or spoofing signals is particularly dangerous as these can disrupt the navigation system [2], [3] and jeopardize the drone mission.

This paper addresses the problem of authenticating messages transmitted by drones. In particular, a drone or ground device (Bob) wants to authenticate messages potentially transmitted by a legitimate drone (Alice) and distinguish them from those transmitted by an *intruder* drone (Trudy) attempting to impersonate Alice. Cryptography-based authentication solutions have several drawbacks: a) they are typically computationally expensive, b) they often provide only computational security, which may be vulnerable to quantum computing-based algorithms, and c) they introduce significant communication overhead. Both communication overhead and computational complexity lead to high energy consumption, which is a limited resource for drones. Therefore, in this paper, we focus on physical layer authentication (PLA) mechanisms that provide security by exploiting the statistical properties of the channels. These techniques typically consume less energy than their crypto-based counterparts while providing information-theoretic security.

PLA has recently been studied in [4], [5], and mechanisms specifically targeting drone communication may rely on fingerprinting [6], or on channel characteristics, eventually supported by a federated learning architecture [7]. Here we focus on a recent evolution of PLA using a challenge-response (CR) approach. In cryptographic CR authentication [8, Sec. 13.5], Alice and Bob share a secret key. Then, Bob sends a message called a *challenge* over a public channel, and Alice computes and sends back to Bob a *response* obtained using a hash function of both the secret key and the challenge. Finally, Bob verifies the authenticity of the sender of the response by comparing the response to a local response obtained using the same secret key and challenge. Instead of relying on crypto-based solutions, we consider CR-PLA, first introduced in [9]. CR-PLA is based on *partially controllable channels*, where the challenge is issued by the verifier Bob by manipulating the propagation environment, while the response is the received signal from Alice, which must be consistent with the expected change. Since the challenge, i.e., the propagation conditions, is randomly chosen by the verifier, it is difficult for Trudy to predict it and transmit a signal that is consistent with it.

In [10] and [11], the authors proposed a first CR-PLA protocol for drone communication. However, a simple channel model was considered, and the challenge distribution was not optimized but chosen as uniform. Additionally, not even the attacker was allowed to optimize their attacks. In this work, we instead consider a more complete channel model and exploit its properties, in particular shadowing, to design the challenge distribution and investigate more sophisticated attacks.

Apart from our previous work [11], while there are studies on the energy consumption of drones, e.g., [12], few studies analyze the link between energy consumption and physical-layer security protocols, as the analyses typically focus on the power consumption of crypto/higher-level solutions, e.g., [13].

Manuscript received –; revised – and – accepted –. Date of publication –; date of current version –.

Corresponding author: M. Piana. This work was partially supported by the European Union under the Italian National Recovery and Resilience Plan (PNRR) of NextGenerationEU, partnerships on "Telecommunications of the Future" (PE0000001 - program "RESTART and PE00000014 - program "SERICS"), and through the Horizon Europe/JU SNS project ROBUST-6G (Grant Agreement no. 101139068). The authors are with the Department of Information Engineering, Università degli Studi di Padova, Padua 35131, Italy. S. Tomasin is also with the National Inter-University Consortium for Telecommunications (CNIT), 43124 Parma, Italy. (email: {mattia.piana@phd., francesco.ardizzon@, stefano.tomasin@}unipd.it).

In this paper, we propose novel strategies for Bob and Trudy when using CR-PLA in drone communication. In particular, in a preliminary phase, Bob measures the channel gain when Alice is at a set of predefined positions. Then, the authenticated transmission protocol requires that Bob first randomly selects a set of positions (with a suitable distribution) and secretly communicates them to Alice. Alice goes to the indicated positions and, for each of them, she transmits a pilot signal together with the message to be authenticated. Next, Bob assesses the authenticity of the received signal by checking that the measured channel gains correspond to the expected ones, estimated during the preliminary phase. In this context, the challenge is represented by the set of positions, and the corresponding response is the set of channel gains estimated by Bob. In turn, for her attack, Trudy randomly selects (with a suitable distribution) a set of positions from which to transmit the pilot signal and her message. The distributions used by Bob and Trudy to select the position sets are optimized to their advantage by finding the Nash equilibria (NEs) of a zero-sum game. In addition, we also consider the problem of minimizing the energy of Alice's movements by proposing both optimal and heuristic strategies to minimize the (average) distance traveled by Alice without sacrificing the security of the protocol.

The contributions of this paper are as follows

- We model the channel between the drone and the receiver, including both the preliminary channel estimation phase and the security protocol.
- We design the statistical distribution of positions generated by Bob and Trudy by modeling the problem as a zero-sum game between legitimate users and Trudy, where the payoff is the missed detection (MD) probability for a target false alarm (FA) probability.
- We consider both optimal and low-complexity solutions for optimizing Bob's position selection statistics.
- We test the proposed technique by numerical simulation, based on a realistic model of both Alice-Bob and Trudy-Bob channels, including shadowing effects in urban and rural scenarios.

Several papers have shown the effectiveness of game theory in authentication. In [14], the authors use game theory to design an authentication protocol for multiple-input and multiple-output (MIMO) channels. In [15], a game-theoretic authentication protocol for zero-trust fifth-generation (5G) Internet of Things (IoT) networks is proposed. The multi-agent scenario where multiple receivers and spoofers play has been analyzed in [16].

A game-theoretic PLA protocol for drone communication was proposed in [17], where Bob chooses the detection thresholds while Trudy plays by choosing the attack probability. However, they consider a more restrictive model where the test is performed by assuming that the previously received signal was authentic, and thus the signal under test should match the previous one.

The rest of the paper is organized as follows. Section II describes the system model in detail. Section III gives an overview of the proposed protocol. The CR-PLA problem is further characterized in Section IV, while Section V details its solution using game theory. Numerical results are given in section VI. Section VII draws the conclusions.

II. System Model

In the considered scenario, Alice is a legitimate drone transmitting messages to Bob, which can be a ground device or, eventually, a second drone. A third drone, Trudy, sends fraudulent messages to Bob. We remark that, although our approach can be applied to multiple drones that collaborate for a joint swarm authentication against multiple coordinated attackers, we mainly focus on a single-drone scenario. Yet, in Section VI, multiple drones are considered. Receiver Bob aims to distinguish messages coming from Alice and Trudy. To this end, we exploit Alice's mobility to design a CR-PLA protocol. In turn, Trudy aims to fool Bob by forging her transmissions so that Bob confuses Trudy's messages as legitimate, i.e., as coming from Alice.

Without loss of generality, we use a Cartesian coordinate system, centered on Bob, to describe any device position. Let $\boldsymbol{x} = (x_1, x_2, x_3)$ be the generic position of Alice and $\boldsymbol{y} = (y_1, y_2, y_3)$ the generic position of Trudy. In particular, we consider the space where Alice and Trudy move to be sampled by a plane grid at altitude h containing M_{A} and M_{T} positions, respectively. Thus, Alice's positions are the set

$$\mathcal{X} = \{\boldsymbol{x}(i) = (x_{i,1}, x_{i,2}, h), \quad i = 1, \ldots, M_{\mathrm{A}}\}. \tag{1}$$

Similarly to Alice, Trudy can move to positions in a plane grid at the same Alice's altitude h, collected into the set

$$\mathcal{Y} = \{\boldsymbol{y}(j) = (y_{j,1}, y_{j,2}, h), \quad j = 1, \ldots, M_{\mathrm{T}}\}. \tag{2}$$

While considering a finite set of positions (e.g., on a grid) makes the design of the authentication protocol easier, i) the results can be straightforwardly extended to a general 3D model ii) the map can be very dense allowing Alice to go everywhere on the grid, up to the accuracy of the drone positioning system.

Exploiting Alice's mobility for authentication purposes also entails an energy cost. As Alice's aim is minimizing such cost, we consider Alice moving from position $\boldsymbol{x}(i)$ to $\boldsymbol{x}(i')$ on a straight line. The cost is then denoted as $E(\boldsymbol{x}(i), \boldsymbol{x}(i'))$. In particular, assuming Alice moves at a constant speed, with magnitude v, on the horizontal plane, the energy consumption (in Joules) is a linear function of the distance [12], namely

$$E(\boldsymbol{x}(i), \boldsymbol{x}(i')) = \alpha_1 \frac{d_{i,i'}}{v} - \alpha_0\,, \tag{3}$$

where α_1 and α_0 are constants parameters and the distance between position $\boldsymbol{x}(i)$ and $\boldsymbol{x}(i')$ is

$$d_{i,i'} = \|\boldsymbol{x}(i') - \boldsymbol{x}(i)\|. \tag{4}$$

Hence, since in (3) the energy is a function of the traveled distance, in the following we will consider the traveled distance instead of the energy as a cost metric[1].

[1]It could also be possible to include the energy spent to reach the maximum velocity. However, we will consider a grid step larger than the distance required to reach such velocity. Thus, the energy consumption due to the initial acceleration is just an additional constant term in (3).

A. Channel Model

Communications among devices occur through narrowband additive white Gaussian noise (AWGN) channels, and their attenuations include path loss, shadowing, and fading. Path loss takes into account the average attenuation caused by the distance traveled by the signal, while shadowing accounts for the presence of objects/obstacles in the environment and is a slow-fading phenomenon, i.e., it changes slowly over time.

Let A_{Tx} and A_{Rx} be the gains of the transmitter and receiver antennas, respectively, in dB. Letting $(f_{\mathrm{c}})_{\mathrm{MHz}}$ be the carrier frequency in MHz and $(d)_{\mathrm{km}} = \|\boldsymbol{q}\|$ the distance (in km) between transmitter in a generic position $\boldsymbol{q}$ and the receiver Bob, we define the path-loss attenuation according to the Friis formula (in dB) as

$$\begin{aligned}(\xi_{\boldsymbol{q}})_{\mathrm{dB}} =& 32.4 + 20\log_{10}(d)_{\mathrm{km}} + 20\log_{10}(f_{\mathrm{c}})_{\mathrm{MHz}} + \\ &- A_{\mathrm{Tx}} - A_{\mathrm{Rx}}.\end{aligned} \tag{5}$$

According to the Gudmundson model [18], the shadowing attenuation in dB $(s)_{\mathrm{dB}}$ follows a zero-mean normal distribution with variance $\sigma^2_{(s)_{\mathrm{dB}}}$, in short $(s)_{\mathrm{dB}} \sim \mathcal{N}(0, \sigma^2_{(s)_{\mathrm{dB}}})$. The shadowing attenuations $(s)_{\mathrm{dB}}$ and $(s)'_{\mathrm{dB}}$, measured at positions $\boldsymbol{q}$ and $\boldsymbol{q}'$, are correlated: defining d_{ref} as the coherence distance [19], the correlation is

$$\mathbb{E}((s)_{\mathrm{dB}}(s)'_{\mathrm{dB}}) = \sigma^2_{(s)_{\mathrm{dB}}} \exp\left(-\frac{\|\boldsymbol{q}-\boldsymbol{q}'\|}{d_{\mathrm{ref}}}\right), \tag{6}$$

where $\mathbb{E}(\cdot)$ denotes the expectation operator. Lastly, when the transmitter is in $\boldsymbol{q}$, the total channel attenuation in dB is [19]

$$(a_{\boldsymbol{q}})_{\mathrm{dB}} = (\xi_{\boldsymbol{q}})_{\mathrm{dB}} + (s)_{\mathrm{dB}}. \tag{7}$$

From (7), the average channel amplitude (in linear scale) can be written as

$$\tilde{g}_{\boldsymbol{q}} = 10^{-\frac{(a_{\boldsymbol{q}})_{\mathrm{dB}}}{20}}. \tag{8}$$

The signal received and sampled by Bob with sampling period T_{s} upon transmission of a symbol b_k at time k is described as [20, Sec. 2.4.2]

$$r_k = \tilde{g}_{\boldsymbol{q}} h_k e^{-j\phi} b_k + w_k, \tag{9}$$

where ϕ is the common phase term due to the signal traveled distance, $h_k \sim \mathcal{CN}(0,1)$ is a complex Gaussian circularly symmetric random variable due to the (fast) fading, and $w_k \sim \mathcal{CN}(0, \sigma^2_w)$ is the thermal noise with variance σ^2_w.

We assume that the symbol period is such that the fading coefficients h_k are i.i.d. random variables. This occurs if $T_{\mathrm{s}} > T_{\mathrm{c}}$, where T_{c} is the coherence time, i.e., the time period over which the fading term h_k in (9) can be considered constant. In turn, T_{c} depends on the velocity of objects in the surrounding environment: the faster the environment changes, the shorter T_{c} is. Given as the maximum speed $v_{\max}$ of object movement with respect to Bob and c as the speed of light in the air, the Doppler frequency shift experienced by Bob is

$$f_{\mathrm{D}} = f_{\mathrm{c}} \frac{v_{\max}}{c}, \tag{10}$$

and following the Clarke's model [21], the coherence time is

$$T_{\mathrm{c}} = \sqrt{\frac{9}{16\pi}} \frac{1}{f_{\mathrm{D}}}. \tag{11}$$

B. Channel Gain Estimation

As detailed in Section III, Bob uses the channel gain as an authentication feature. To this end, Alice transmits K unit-power phase-shift keying (PSK) pilot symbols b_k, $k = 1, \ldots, K$, with $|b_k|^2 = 1$. Since fading and thermal noise are two independent processes, for the transmission of independent unit power symbols, from (9) we have $r_k \sim \mathcal{CN}(0, \tilde{g}^2_{\boldsymbol{q}} + \sigma^2_w)$.

Bob processes the received signal (9) (which depends on the transmitter position $\boldsymbol{q}$) by applying the function $\mu(\cdot)$ and estimates the average channel gain as

$$\hat{m} = \mu(\boldsymbol{q}) = \frac{1}{K}\sum_k |r_k b_k^*|^2 = \frac{1}{K}\sum_k \left|\tilde{g}_{\boldsymbol{q}} h_k e^{-j\phi} + w'_k\right|^2, \tag{12}$$

where w'_k has the same statistics as w_k, since the transmitted symbols have unitary power.

C. Attacker Knowledge

We consider the worst-case scenario for Bob, where Trudy can arbitrarily move close to Alice. Moreover, Trudy knows:

1) the Bob's location,
2) the set $\mathcal{X}$ of possible Alice's positions,
3) the pilot sequence $\{b_k\}$, $k = 1, \ldots, K$, used by Alice to communicate with Bob.
4) Any information acquired by Bob during the training phase (better described in Section III).

III. Challenge-Response Physical Layer Authentication

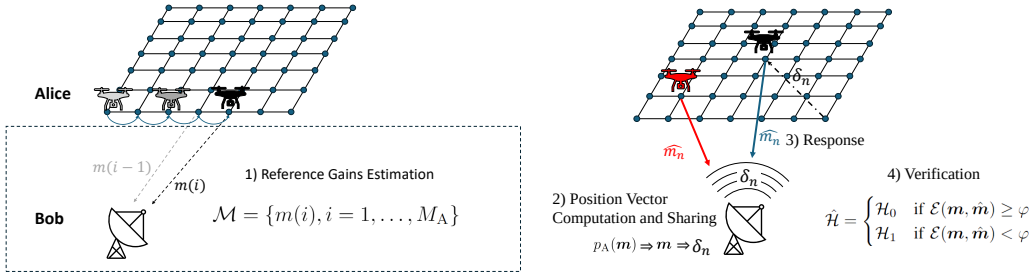
We propose a physical layer authentication mechanism where Bob aims to authenticate received messages by testing the channel gains estimated from the pilot signals. Fig. 1 shows the scheme of the proposed CR-PLA protocol.

The sequence of estimated channel gains is compared against the expected sequence, derived by knowing the positions from which Alice transmitted the signal. Using the channel gains to decide the authenticity of the signal allows Bob to i) avoid using the channel phase, which may lead to errors due to synchronization differences, and ii) average over noise and fading realizations to make a more reliable decision.

We now introduce the proposed CR-PLA protocol. The protocol comprises a setup and an authentication phase.

Set-up phase:

1) *Reference Gains Estimation*: we assume that Alice can transmit authenticated pilot signals, for instance by using a higher-layer authentication protocol. This is a training phase, typical of the PLA schemes (e.g., [10], [14], [22], [23]), aimed at acquiring information used in our authentication protocol. In particular, Alice moves in all the positions in $\mathcal{X}$ and transmits authenticated pilot signals to Bob. Then, Bob estimates the channel gain using $K = K_{\mathrm{est}}$ pilot symbols from each Alice's position using (12). We assume this estimate to be perfect, i.e., considering $K_{\mathrm{est}} \to \infty$ in (12). However, we will investigate in Section VI the behavior of our protocol



(a) Set up: step 1) .

(b) Authentication: steps 2)-4).

Fig. 1. Scheme of the proposed CR-PLA protocol.

with a finite $K_{\rm est}$. Bob then obtains the *channel gain map*

$$\mathcal{M} = \{m(i), i = 1, \ldots, M_{\rm A}\} \ . \tag{13}$$

Authentication phase (to be repeated for each message transmitted by Alice):

2) *Position Vector Computation and Sharing*: Bob randomly draws a vector $\boldsymbol{m} = [m_1, \ldots, m_N]$, $m_n \in \mathcal{M}$ of N gains from the gain map, using the probability mass distribution (PMD) $p_{\rm A}(\boldsymbol{m})$. The design of $p_{\rm A}(\boldsymbol{m})$ is discussed in Sections IV and V. Gains are mapped into corresponding positions $\boldsymbol{x}_{\rm A} = [\boldsymbol{x}_1, \ldots, \boldsymbol{x}_N]$, with $\boldsymbol{x}_n \in \mathcal{X}$, providing the average gains $\boldsymbol{m}$. Next, Bob communicates the set of positions $\boldsymbol{x}_{\rm A}$ to Alice, without disclosing them to Trudy, as better described in the following. This is considered the *challenge* of the CR protocol.
3) *Response*: The transmission of a message by Alice is split into N *rounds*, where at each round n Alice goes to position $\boldsymbol{x}_n$ and transmits K pilot symbols. Bob estimates the channel gain for each transmission and collects the estimates into vector $\hat{\boldsymbol{m}} = [\hat{m}_1, \ldots, \hat{m}_N]$, which is considered to be the *response* of our CR-PLA protocol.
4) *Verification*: Bob must decide whether the estimated vector $\hat{\boldsymbol{m}}$ matches the expected gain vector $\boldsymbol{m}$; thus, whether the received signals were transmitted by Alice or not. This is a binary decision problem. In formulas, let $\mathcal{H}_0$ and $\mathcal{H}_1$ be the legitimate (null) and the under-attack hypothesis, respectively. Let $\mathcal{H}$ the current state ($\mathcal{H} = \mathcal{H}_0$ when Alice transmits and $\mathcal{H} = \mathcal{H}_1$ when Trudy transmits). Given a test function $\mathcal{E}(\boldsymbol{m}, \hat{\boldsymbol{m}})$, the correspondent binary decision $\hat{\mathcal{H}}$ on measurement $\hat{\boldsymbol{m}}$ is

$$\hat{\mathcal{H}} = \begin{cases} \mathcal{H}_0 & \text{if } \mathcal{E}(\boldsymbol{m}, \hat{\boldsymbol{m}}) \geq \varphi \, , \\ \mathcal{H}_1 & \text{if } \mathcal{E}(\boldsymbol{m}, \hat{\boldsymbol{m}}) < \varphi \, , \end{cases} \tag{14}$$

where φ is a user-defined threshold. The choice of the test function is discussed in Section III-B.

Concerning Step 2), several approaches can be adopted to securely communicate the position vector $\boldsymbol{x}_{\rm A}$ to Alice. As a first solution, we may assume that the initial position of Alice is secret, e.g., by having Bob randomly choose that and then secretly communicate it to Alice, for instance, using a key shared before deployment and encoding the message with a one-time pad. Next, Bob only needs to communicate the shifts from the current to the next positions $\boldsymbol{x}_{n+1}$, i.e., $\boldsymbol{\delta}_n = \boldsymbol{x}_{n+1} - \boldsymbol{x}_n$, $n = 1, \ldots, N-1$. This transmission can be public, as the shift alone does not leak information on the final position. Thus, the shift vector $\boldsymbol{\delta}$ constitutes the challenge of the CR protocol to be posed to the device to be authenticated. Note that, however, if Trudy was able to estimate accurately Alice's current location, she may also anticipate her next position by exploiting the public challenge $\boldsymbol{\delta}_n$, thus breaking the authentication protocol. A solution is then to design and secretly share the whole trajectory $\boldsymbol{x}_{\rm A}$ with Alice, either before the protocol starts or, again, using a confidential transmission (e.g., one-time pad or even wiretap coding [24]). While this solution has a higher cost, it has relaxed assumptions on the localization capability of Trudy. Moreover, current state-of-the-art localization techniques assume the tracking device(s) to be fixed on the ground; thus, Trudy should be both fixed and equipped with additional hardware to be a threat (see [25], [26]).

Still about step 2), we assume that for each average gain $m \in \mathcal{M}$, there is a single corresponding position in $\mathcal{X}$, since the shadowing model yields a vanishing probability of having the same gain in multiple map positions.

A. Attack Model

We consider a scenario where Trudy aims at fooling Bob by picking a sequence of N positions $\boldsymbol{y}_{\rm T} = [\boldsymbol{y}_1, \ldots, \boldsymbol{y}_N]$, where $\boldsymbol{y}_n \in \mathcal{Y}$.

Analogously to (13), we define the channel gain set for the Trudy positions as

$$\mathcal{M}_{\rm T} = \{m_{\rm T}(j), j = 1, \ldots, M_{\rm T}\} \, . \tag{15}$$

We consider the worst case wherein the positions chosen by Trudy can be anywhere, also very close to Alice.

The Trudy attack is successful when it passes the test (14). Hence, Trudy attack consists in i) choosing a PMD $p_{\rm T}(\boldsymbol{m}_{\rm T})$ of a vector $\boldsymbol{m}_{\rm T} = \{m_{{\rm T},1}, \ldots, m_{{\rm T},N}\}$, ii) using it to sample a vector $\boldsymbol{m}_{\rm T}$, and iii) mapping it back to a sequence of positions $\boldsymbol{y}_{\rm T}$. In this paper, we assume the attacker can estimate the set in (15), e.g., by intercepting signals coming from Bob when transmitting the challenge.

B. Verification Test

We focus on the verification problem of step 4), and we resort to decision theory to optimize the test function. In the design of the test at Bob, we assume that we do not know the attack statistics, which depend on Trudy's PMD $p_{\mathrm{T}}(\boldsymbol{m}_{\mathrm{T}})$. Indeed, designing a test for specific statistics is, in general, sub-optimal since Trudy may then deviate from it, and choose another one that may be more effective to pass test (14). Before delving into the definition of the test function $\mathcal{E}(\boldsymbol{m}, \hat{\boldsymbol{m}})$, let us introduce the following Lemmas.

Lemma 1: When Alice transmits a large number of pilot symbols ($K \to \infty$), the estimated channel gain $\hat{m}$ with Alice in position $\boldsymbol{x}(i)$ has statistics

$$\hat{m} \sim \mathcal{N}\left(m(i), \frac{m(i)^2}{K}\right), \quad \text{with} \;\; m(i) \triangleq \tilde{g}^2_{\boldsymbol{x}(i)} + \sigma_w^2 \,. \tag{16}$$

Proof: Proof in Appendix A. ∎

Lemma 2: Under the legitimate hypothesis $\mathcal{H}_0$, estimations $\hat{m}_n$ and $\hat{m}_{n'}$ taken at different times n and n' are statistically independent.

Proof: Proof in Appendix B. ∎

Now, to implement (14), we resort to the log-likelihood test (LLT) test. In particular, let us define the log-likelihood for $\mathcal{H} = \mathcal{H}_0$ given $\boldsymbol{m}$ as

$$\mathcal{E}'(\hat{\boldsymbol{m}}, \boldsymbol{m}) = \log p_{\mathcal{H}_0}(\hat{\boldsymbol{m}}|\boldsymbol{m}) \,, \tag{17}$$

where $p_{\mathcal{H}_0}(\hat{\boldsymbol{m}}|\boldsymbol{m})$ is the probability density function (PDF) of $\hat{\boldsymbol{m}}$ given the challenge $\boldsymbol{m}$ when Alice is transmitting. When $\mathcal{H} = \mathcal{H}_0$, the entries of $\hat{\boldsymbol{m}}$ are fully determined by the gains $\boldsymbol{m}$ of step 2). Still, following Lemma 2, estimates relative to different transmitting positions are independent. When Alice is transmitting ($\mathcal{H} = \mathcal{H}_0$), from (16) we have that $\hat{m}_n = m_n + \tilde{w}_n$, where $\tilde{w}_n = \mathcal{N}\left(0, m_n^2/K\right)$. Moreover, (17) becomes

$$\begin{aligned}
\mathcal{E}'(\hat{\boldsymbol{m}}, \boldsymbol{m}) &= \log p_{\mathcal{H}_0}(\hat{\boldsymbol{m}}|\boldsymbol{m}) \\
&= \log \prod_{n=1}^{N} \frac{K}{\sqrt{2\pi} m_n} \exp\left(-\frac{K(\hat{m}_n - m_n)^2}{2m_n^2}\right) \\
&\simeq \sum_{n=1}^{N} \frac{K(\hat{m}_n - m_n)^2}{m_n^2} = \mathcal{E}(\hat{\boldsymbol{m}}, \boldsymbol{m}) \,,
\end{aligned} \tag{18}$$

where in the last approximation we neglected scalar factors that do not alter test (14).

We remark that, differently from the likelihood ratio test, the LLT has no optimality guarantee. Still, the test is effective and is commonly used in many security applications, e.g., [23], [27], [28]. Eventually, it is also possible to implement such a test without knowing the statistical description of $\hat{\boldsymbol{m}}$ under $\mathcal{H}_1$ (see [22] and [29]).

IV. CR-PLA Optimization Problem

The CR-PLA mechanism introduced in the previous section has several tunable parameters, in particular the test threshold φ, and $p_{\mathrm{A}}(\boldsymbol{m})$ and $p_{\mathrm{T}}(\boldsymbol{m}_{\mathrm{T}})$ of Bob and Trudy, respectively. All these parameters have an impact on the security and energy consumed by Alice.

In terms of security, the authentication mechanism can be characterized by the FA and MD probabilities. Let $\mathbb{P}(\cdot)$ denote the probability operator. FA events occur when Alice's messages are considered fake and the corresponding probability is

$$P_{\mathrm{fa}} = \mathbb{P}[\hat{\mathcal{H}} = \mathcal{H}_1 | \mathcal{H} = \mathcal{H}_0]. \tag{19}$$

A MD event occurs when Trudy messages are considered authentic and the corresponding MD probability is

$$P_{\mathrm{md}} = \mathbb{P}[\hat{\mathcal{H}} = \mathcal{H}_0 | \mathcal{H} = \mathcal{H}_1]. \tag{20}$$

In terms of energy consumption by Alice, considering model (3), the performance can be assessed through the average traveled distance over the N rounds, i.e.,

$$\bar{D} = \mathbb{E}\left[\sum_{n=1}^{N-1} d_{i_n, i_{n+1}}\right], \tag{21}$$

where i_n refers to the position $\boldsymbol{x}(i_n)$, i.e., the position of Alice at round n and the expectation depends on $p_{\mathrm{A}}(\boldsymbol{m})$.

Threshold Setting: As a typical approach in hypothesis testing problems, we set a target FA probability and the threshold φ is chosen to meet this requirement. As each term of the summation in (18) is the square of an independent standard Gaussian variable, $\mathcal{E}(\hat{\boldsymbol{m}}, \boldsymbol{m})$ is chi-squared distributed with N degrees of freedom. The FA probability is then

$$P_{\mathrm{fa}} = \mathbb{P}\left(\sum_{n=1}^{N} \frac{K(\hat{m}_n - m_n)^2}{m_n^2} \geq \varphi \,\middle|\, \boldsymbol{m}\right) = 1 - \chi^2_N(\varphi) \,, \tag{22}$$

where $\chi^2_N(\cdot)$ is the cumulative distribution function (CDF) of a chi-squared variable with order N. Thus, we can then compute the threshold φ of the authentication test (14) for a desired P_{fa} as

$$\varphi = \left[\chi^2_N\right]^{-1}(1 - P_{\mathrm{fa}}) \,, \tag{23}$$

where $\left[\chi^2_N\right]^{-1}(\cdot)$ is the inverse CDF of the chi-squared distribution with order N.

For the optimization of the PMDs, we consider both the MD probability and the average traveled distance as targets. However, we assume that the security performance (in terms of MD probability) is more important than the energy performance (in terms of $\bar{D}$).

For the security performance, Bob and Trudy have conflicting targets. Trudy aims at maximizing the MD probability to obtain more effective attacks, i.e.,

$$p^{\star}_{\mathrm{T}}(\boldsymbol{m}_{\mathrm{T}}) = \underset{p_{\mathrm{T}}(\boldsymbol{m}_{\mathrm{T}})}{\arg\max}\, P_{\mathrm{md}} \,. \tag{24}$$

Bob instead aims at choosing $p_{\mathrm{A}}(\boldsymbol{m})$ to minimize the MD probability. Then, for the energy performance, among all the distributions yielding the same MD probability, Bob chooses the one minimizing the average travel distance. Thus, defining the set of distributions minimizing the MD probability as

$$\mathcal{P}_{\min} = \left\{ \hat{p}_{\mathrm{A}}(\boldsymbol{m}) = \underset{p_{\mathrm{A}}(\boldsymbol{m})}{\arg\min}\, P_{\mathrm{md}} \right\}, \tag{25}$$

we look for the PMD minimizing the average distance in this set, i.e.,

$$p^{\star}_{\mathrm{A}}(\boldsymbol{m}) = \underset{p_{\mathrm{A}}(\boldsymbol{m}) \in \mathcal{P}_{\min}}{\arg\min}\; \bar{D} \,. \tag{26}$$

We observe that the optimization problems (24), (25), and (26) are intertwined since the MD probability depends on both PMDs $p_{\mathrm{A}}(\boldsymbol{m})$ and $p_{\mathrm{T}}(\boldsymbol{m}_{\mathrm{T}})$. Now, we observe that the (average) gain estimated by Bob at round n when Trudy is transmitting is

$$\hat{m}_n = z_n = m_{\mathrm{T},n} + \tilde{w}_{\mathrm{T},n}\,, \tag{27}$$

where $m_{\mathrm{T},n} \in \mathcal{M}_{\mathrm{T}}$ is the expected channel gain at round n and $\tilde{w}_{\mathrm{T},n} \sim \mathcal{N}\left(0, m_{\mathrm{T},n}^2/K\right)$ is the estimation error (as for Alice). Thus, combining the test function (18) with (27), the average MD probability can be written as

$$\begin{aligned} P_{\mathrm{md}} =& \mathbb{E}_{\boldsymbol{m},\boldsymbol{m}_{\mathrm{T}}}\left[\mathbb{P}\left(\sum_{n=1}^{N}\frac{K(z_n-m_n)^2}{m_n^2} \le \varphi | \boldsymbol{m}, \boldsymbol{m}_{\mathrm{T}}\right)\right] \\ =& \sum_{\boldsymbol{m}}\sum_{\boldsymbol{m}_{\mathrm{T}}}\mathbb{P}\left(\sum_{n=1}^{N}\frac{K(z_n-m_n)^2}{m_n^2} \le \varphi | \boldsymbol{m}, \boldsymbol{m}_{\mathrm{T}}\right) \times \\ & p_{\mathrm{A}}(\boldsymbol{m}) p_{\mathrm{T}}(\boldsymbol{m}_{\mathrm{T}})\,, \end{aligned} \tag{28}$$

which depends on both Alice's and Trudy's PMDs.

A. Single and Multiple Rounds

We now show that in the considered scenario, both Bob's and Trudy's security-optimal PMD (i.e., problems (24) and (25)) yield independent gain realization at each round, i.e.,

$$p_{\mathrm{A}}^{\star}(\boldsymbol{m}) = \prod_{n=1}^{N} p_{\mathrm{A},n}^{\star}(m_n)\,, \tag{29}$$

$$p_{\mathrm{T}}^{\star}(\boldsymbol{m}_{\mathrm{T}}) = \prod_{n=1}^{N} p_{\mathrm{T},n}^{\star}(m_{\mathrm{T},n})\,. \tag{30}$$

In other words, both Bob and Trudy can extract independent gains across rounds without sacrificing security.

We start noting that Bob is agnostic of Trudy's attack PMD, i.e., he does not know $p_{\mathrm{T}}(\boldsymbol{m}_{\mathrm{T}})$. Hence, there is no relation among different attacks Bob can exploit. Moreover, also following Lemma 2, for a given $\boldsymbol{m}$, the gain estimations in $\hat{\boldsymbol{m}}$ are independent across rounds. Thus, his choice of the position will be independent at each round, and the PMDs constituting the set $\mathcal{P}_{\min}$ in (25) can be written as (29).

Now, we introduce the following theorem on Trudy's optimal strategy.

Theorem 1: For the considered scenario, given Bob's defense PMD $p_{\mathrm{A}}^{\star}(\boldsymbol{m})$ as in (29), Trudy's optimal attack PMD can be factorized as in (30). In other words, Trudy's best attack is to extract independent gains at each round.

Proof: Proof in Appendix C. ∎

From (29) and Theorem 1, both Bob and Trudy choose their gains at each round independently. This implies that the joint optimization of the PMDs can be done at each round. Note, however, that the PMDs can be different at each round. Thus, in the following, we focus on the case $N = 1$, i.e., single round, whose results are applicable also for $N > 1$. In this analysis, we drop the time index n, and so the single-round attack and defense PMDs become $p_{\mathrm{T}}(m_{\mathrm{T}})$ and $p_{\mathrm{A}}(m)$.

V. Game Modeling and Optimization Solution

To address the complexity of the optimization problem defined by (24)-(26), we first frame the security scenario as a game between Trudy and Bob. In the game, the target gains m and m_{T} represent the *actions*. Trudy aims at maximizing the MD probability, while Bob aims at minimizing it. The *mixed strategies* of the game are described by the PMDs $p_{\mathrm{A}}(m)$ and $p_{\mathrm{T}}(m_{\mathrm{T}})$. We then characterize the strategies that constitute a NE of the game, that solve problems (24) and (25) jointly. Among those strategies, we then look for solutions to minimize the average distance traveled by Alice to solve (26).

To describe the CR-PLA mechanism as a game, let us first introduce the probability vector $\boldsymbol{a}$ with length M_{A} and entries

$$a_i = p_{\mathrm{A}}(m(i))\,, \quad i = 1, \ldots, M_{\mathrm{A}}\,, \tag{31}$$

and probability vector $\boldsymbol{e}$ with length M_{T} and entries

$$e_j = p_{\mathrm{T}}(m_{\mathrm{T}}(j))\,, \quad j = 1, \ldots, M_{\mathrm{T}}\,. \tag{32}$$

The game can then be defined as follows:

Players Bob against Trudy.

Sets of actions set $\mathcal{M}$ and $\mathcal{M}_{\mathrm{T}}$ of the gains (and so positions) Bob and Trudy can take.

Payoff for Trudy, the payoff obtained when Bob and Trudy play their actions (choose their positions) is the resulting MD probability P_{md}; correspondingly, for Bob the payoff is $-P_{\mathrm{md}}$. The payoff matrix for Trudy is $\boldsymbol{P} \in [0,1]^{M_{\mathrm{A}} \times M_{\mathrm{T}}}$, with entry (from (18) and (28)) $i = 1, \ldots, M_{\mathrm{A}}$, and $j = 1, \ldots, M_{\mathrm{T}}$

$$\begin{aligned} P_{i,j} &= \mathbb{P}\left[\mathcal{N}\left(\frac{(m_{\mathrm{T}}(j) - m(i))\sqrt{K}}{m_{\mathrm{T}}(j)}, 1\right)^2 \le \varphi \frac{m(i)^2}{m_{\mathrm{T}}(j)^2}\right] \\ &= \chi^2_{\mathrm{NC}}\left(\varphi \frac{m(i)^2}{m_{\mathrm{T}}(j)^2};\ \lambda = \frac{(m_{\mathrm{T}}(j) - m(i))^2 K}{m_{\mathrm{T}}(j)^2}\right), \end{aligned} \tag{33}$$

where $\chi^2_{\mathrm{NC}}(\cdot;\lambda)$ is the non-central chi-squared CDF with parameter λ. Bob's payoff matrix is instead $-\boldsymbol{P}$.

Strategies the PMDs with which actions are taken by two players are $\boldsymbol{a}$ and $\boldsymbol{e}$, for Bob and Trudy, respectively.

Utility function the utility function for Trudy is defined as

$$u_{\mathrm{T}}(\boldsymbol{a}, \boldsymbol{e}) = \sum_{i=1}^{M_{\mathrm{A}}}\sum_{j=1}^{M_{\mathrm{T}}} P_{i,j} a_i e_j\,, \tag{34}$$

i.e., her expected payoff resulting from the strategies of both players. The utility of Bob instead is $u_{\mathrm{A}}(\boldsymbol{a}, \boldsymbol{e}) = -u_{\mathrm{T}}(\boldsymbol{a}, \boldsymbol{e})$. Note that the utility function of Trudy (34) is equivalent to (28) (with $N = 1$).

In game theory, a strategy is pure when the probability distribution is degenerate, e.g., for Bob $a_i = 1$ for some i and 0 otherwise; in all the other cases (including our game) the strategy is *mixed*. Note that Bob and Trudy choose a strategy, not an action: these two concepts are the same only for a pure strategy.

The game can be classified as a static *zero-sum* game of complete information. It is static because there is no time dependency, and single-shot moves fully determine the

outcome of the game. It is a zero-sum game because the two players have opposite objectives, i.e., $u_{\mathrm{A}}(\boldsymbol{a},\boldsymbol{e}) = -u_{\mathrm{T}}(\boldsymbol{a},\boldsymbol{e})$. It has complete information since the sets of actions and the payoffs are common knowledge.

A. Nash Equilibrium Characterization

We recall that strategies $(\boldsymbol{a}^\star,\boldsymbol{e}^\star)$ are a NE (i.e., optimal from a game theory perspective) if there is no unilateral deviation of the players leading to a better utility. In formulae, if $(\boldsymbol{a}^\star,\boldsymbol{e}^\star)$ is a NE, then

$$u_{\mathrm{A}}(\boldsymbol{a}^\star,\boldsymbol{e}^\star) \geq u_{\mathrm{A}}(\boldsymbol{a},\boldsymbol{e}^\star) \quad \forall \boldsymbol{a}\,, \tag{35}$$

and

$$u_{\mathrm{T}}(\boldsymbol{a}^\star,\boldsymbol{e}^\star) \geq u_{\mathrm{T}}(\boldsymbol{a}^\star,\boldsymbol{e}) \quad \forall \boldsymbol{e}\,. \tag{36}$$

We now characterize the set of NE strategies for the considered game. Since the game is zero-sum, let us first define two problems that we will show are strategically equivalent. Let us define the maximin problem, where Bob first optimizes his strategy and then Trudy optimizes her strategy as

$$u^\star_{\mathrm{T,max}} = \max_{\boldsymbol{e}} \min_{\boldsymbol{a}} u_{\mathrm{T}}(\boldsymbol{a},\boldsymbol{e}). \tag{37}$$

Similarly, let us define the minimax problem, where Trudy first optimizes her strategy and then Bob optimizes his strategy as

$$u^\star_{\mathrm{T,min}} = \min_{\boldsymbol{a}} \max_{\boldsymbol{e}} u_{\mathrm{T}}(\boldsymbol{a},\boldsymbol{e}). \tag{38}$$

Let us also define Trudy's strategies $\boldsymbol{e}_{\max}$ and $\boldsymbol{e}_{\min}$ that lead to the $u^\star_{\mathrm{T,max}}$ (37) and $u^\star_{\mathrm{T,min}}$ (38), respectively.

Since the game is zero-sum, the following results hold:

1) As the set of actions is finite, at least one NE exists in mixed strategies [30, Sec. 6.4].
2) From the minimax theorem [31], we have
$$\boldsymbol{e}^\star = \boldsymbol{e}_{\max} = \boldsymbol{e}_{\min}, \quad u^\star = u^\star_{\mathrm{T,min}} = u^\star_{\mathrm{T,max}}\,, \tag{39}$$
thus (37) and (38) are equivalent.
3) *Lemma 3:* All NEs yield the same utility.
Proof: Proof in Appendix D. ∎

B. Game-Based Optimization Problem

From (39), we can compute the utility of any NE by solving the maximin problem (37) via linear programming as shown in [32, Sec. 3.10]. In particular, by letting $\boldsymbol{P}_i^T$ to be the i-th row of $\boldsymbol{P}$, the NE utility is the solution of the following optimization problem

$$\begin{aligned} u^\star = \max_{u} \quad & u \\ \text{s.t.} \quad & u \leq \boldsymbol{P}_i^T \boldsymbol{e}, \qquad \forall i \in 1,\dots,M_{\mathrm{A}}, \\ & \sum_{j=1}^{M_{\mathrm{T}}} e_j = 1, \quad e_j \geq 0, \forall j. \end{aligned} \tag{40}$$

Note that the utility of the game $u^\star$ coincides with the average MD probability of (28) and $\boldsymbol{e}^\star$ (i.e., the solution of (40) achieving $u^\star$) is an optimal solution for Trudy.

As Bob's utility is the opposite of Trudy, we now have a characterization of the set $\mathcal{P}_{\min}$ in (25), as the set of strategies solving (40) with $-\boldsymbol{P}^T$ in place of $\boldsymbol{P}$ (see [32, Sec. 3.10]), thus we have

$$\mathcal{P}_{\min} = \{\boldsymbol{a} : -\boldsymbol{P}^T\boldsymbol{a} \geq u^\star \mathbb{1}\}\,, \tag{41}$$

where $\mathbb{1}$ is the vector with all entries equal to 1. We remark that, thanks to Theorem 1, the NE for the zero-sum game with the utility is the MD over multiple rounds can be derived straight from the NE obtained in (41). We will use this result to find the minimum-distance best response for Bob in the next subsections.

Note that distance minimization has no effect on Bob and Trudy's strategy. In fact, all the approaches presented in the next subsections provide solutions within the NE set of (41). Consequently, distance minimization finds the energy optimal NE among all NEs. According to Lemma 3, since this is a zero-sum game, all NEs yield the same payoff; thus, Trudy cannot use this information to design a better strategy. Finally, we note that we could have included both the safety (MD probability minimization) and the energy objectives in the payoff function for Bob. However, this would have caused two major problems: a) mixing the two goals (security and energy reduction) is problematic because they are associated with incomparable metrics (misdetection probability and energy); b) the resulting game would not be zero-sum, making the analysis of NEs much more complex. Therefore, we decided to prioritize the security objective by considering only NEs that minimize Bob's MD probability, which yields a zero-sum game, and then selecting the NE that minimizes energy.

C. Multi-Round Multiple-NE Solution

We now consider again the optimization problem (24)-(26) with multiple rounds. We denote as $\boldsymbol{a}(i,n)$ the PMD to use when Alice is located in position $\boldsymbol{x}(i)$ at round n. Specifically, each element $a_j(i,n)$ represents the probability of Alice moving to position $\boldsymbol{x}(j)$ at round $(n+1)$ given that she is in position $\boldsymbol{x}(i)$ at round n. We denote as $\boldsymbol{A}(n)$ the $M_{\mathrm{A}} \times M_{\mathrm{A}}$ matrix whose column i is the vector $\boldsymbol{a}(i,n)$, i.e., $\boldsymbol{A}(n)_{\cdot,i} = \boldsymbol{a}(i,n)$. Next, we collect in $\boldsymbol{A} = [\boldsymbol{A}(1),\dots,\boldsymbol{A}(N)]$ the optimal strategies for each position, at each round. The probability of obtaining the sequence of position (indexes) $\mathcal{I} = \{i_1,\dots,i_N\}$ is $p_{\mathcal{I}}(\mathcal{I},\boldsymbol{A}) = \prod_{n=1}^{N-1} a_{i_{n+1}}(i_n,n)$.

Now, since positions and gains have a one-to-one mapping (see (13)), for each sequence of positions $\mathcal{I}$ we have a corresponding vector $\boldsymbol{m}$ and $p_{\mathcal{I}}(\mathcal{I},\boldsymbol{A}) = p_{\mathrm{A}}(\boldsymbol{m})$.

Moreover, the total distance associated with the sequence $\mathcal{I}$ is $\sum_{n=1}^{N-1} d_{i_n,i_{n+1}}$ where $d_{i_n,i_{n+1}}$ is defined in (4). Thus, the average covered distance in (26) can be written as $\bar{D} = \sum_{\mathcal{I}=\{i_1,\dots,i_N\}} \left[\sum_{n=1}^{N-1} d_{i_n,i_{n+1}}\right] p_{\mathcal{I}}(\mathcal{I},\boldsymbol{A})$. About the constraints, we simply force all the probabilities to be Nash Equilibrium.

Given these considerations, the optimization problem to find the optimal multi-round strategy $\boldsymbol{A}^\star$ that corresponds to

$p^{\star}_{\mathrm{A}}(\boldsymbol{m})$ in (26) can be rewritten as

$$\begin{aligned}\boldsymbol{A}^{\star} = \arg\min_{\boldsymbol{A}} & \sum_{\mathcal{I}=\{i_1,\ldots,i_N\}} \left[\sum_{n=1}^{N-1} d_{i_n,i_{n+1}}\right] p_{\mathcal{I}}(\mathcal{I},\boldsymbol{A}) \\ \text{s.t. } & \forall i \in 1,\ldots,M_{\mathrm{A}}, \forall n: \\ & u^{\star}\mathbb{1} \leq -\boldsymbol{P}^T\boldsymbol{a}(i,n) \\ & \sum_{i'=1}^{M_{\mathrm{A}}} a_{i'}(i,n) = 1, \quad \boldsymbol{a}(i,n) \geq \boldsymbol{0}.\end{aligned} \tag{42}$$

We denote the solution of problem (42) as multi-round multiple (MRM)-NE solution. Since the objective function includes $p_{\mathcal{I}}(\mathcal{I},\boldsymbol{A})$, which is obtained as the product of the optimization variables, we have that problem (42) is non-convex.

Concerning the computational complexity of (42), we note the problem is non-convex. We also note that problem (42) has a large number of variables ($M_{\mathrm{A}}^2 N$) and the number of operations required to evaluate the objective function is $(2N+1)M_{\mathrm{A}}^N$, i.e. an exponential number of operations. Finally, the structure of the problem does not suggest any algorithm to solve it efficiently. Thus, in the following, we present a relaxed version of (42) that can be solved with lower complexity.

D. Single-Hop Multiple-NE Solution

As we will see in Section VI, even with a small number of rounds ($N = 2, 3$), we achieve a low MD probability. This suggests that, instead of optimizing over multiple rounds, we could neglect the effect of choosing a position at round n on the distance traveled on subsequent rounds. In other words, we could neglect time in the optimization and apply the same strategy at each round (see [11]). Thus, we simplify (42) by finding a NE that depends solely on Alice's current position, thus, we have $\boldsymbol{a}^{\star}(i,n) = \boldsymbol{a}^{\star}(i)$. For each position $\boldsymbol{x}(i)$, the corresponding NE that minimizes the average distance traveled when the drone is in that position is

$$\begin{aligned}\boldsymbol{a}^{\star}(i) = \arg\min_{\boldsymbol{a}(i)} & \sum_{i'=1}^{M_{\mathrm{A}}} d_{i,i'} a'_i(i) \\ \text{s.t. } & u^{\star}\mathbb{1} \leq -\boldsymbol{P}^T\boldsymbol{a}(i) \\ & \sum_{i'=1}^{M_{\mathrm{A}}} a_{i'}(i) = 1\,, \boldsymbol{a}(i) \geq \boldsymbol{0}\,.\end{aligned} \tag{43}$$

We denote this problem as single-hop multiple (SHM)-NE solution.

Note that to find the optimal strategy $\boldsymbol{A}^{\star}(n) = \boldsymbol{A}^{\star}$ we need to solve (43) M_{A} times (one for each starting position $\boldsymbol{x}(i)$), but each solution is optimal and much easier to compute than (42), since (43) is a simple and fast linear program.

E. Single NE Solution

In this last approach, we find a single NE $\boldsymbol{a}^{\star}$ that minimizes the average traveled distance, without taking into account the current and next positions, thus in a greedy fashion. Consequently we have $\boldsymbol{a}^{\star}(i,n) = \boldsymbol{a}^{\star}$. Let us define the distance matrix $\boldsymbol{D} \in \mathbb{R}^{M_{\mathrm{A}} \times M_{\mathrm{A}}}$, whose entries (from (4)) are

$$\boldsymbol{D}_{i,i'} = d_{i,i'} \quad \text{for } i,i' = 1,\ldots,M_{\mathrm{A}}\,. \tag{44}$$

TABLE I
SIMULATION PARAMETERS

Symbol	Description	Default value
K	Number of pilots symbols	50
N	Number of rounds	1
$\sigma_{(s)_{\mathrm{dB}}}$	Shadowing STD	10 dB
h	Altitude	50 m
M_{A}	Number of Alice positions	15×15
M_{T}	Number of Trudy positions	15×15
f_{c}	Carrier frequency	2.4 GHz

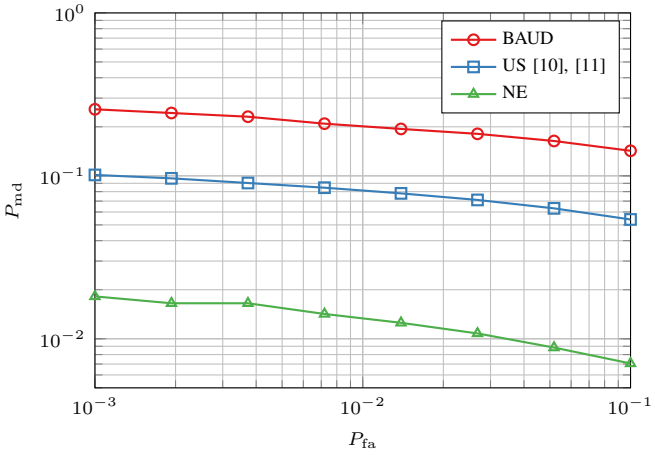


Fig. 2. DET curve of the proposed protocol with different strategies and $N = 2$ rounds.

Given a mixed strategy $\boldsymbol{a}$ for Bob, we compute the average traveled distance as

$$\begin{aligned}\bar{D}(\boldsymbol{D},\boldsymbol{a}) &= \sum_{i=1}^{M_{\mathrm{A}}}\sum_{i'=1}^{M_{\mathrm{A}}} d_{i,i'} a_i a_{i'} \\ &= \boldsymbol{a}^T\boldsymbol{D}\boldsymbol{a}\,.\end{aligned} \tag{45}$$

The optimization problem thus becomes

$$\begin{aligned}\boldsymbol{a}^{\star} = \arg\min_{\boldsymbol{a}} & \quad \boldsymbol{a}^T\boldsymbol{D}\boldsymbol{a} \\ \text{s.t.} & \quad u^{\star}\mathbb{1} \leq -\boldsymbol{P}^T\boldsymbol{a} \\ & \quad \sum_{i'=1}^{M_{\mathrm{A}}} a_{i'} = 1\,, \boldsymbol{a} \geq \boldsymbol{0}\,.\end{aligned} \tag{46}$$

We denote problem (46) as single NE (S-NE) solution.

Since $\boldsymbol{D}$ is not positive semidefinite, (46) is not convex. Still, the structure of (46) is much simpler than (42) as it suggests the usage of sequential least squares programming (SLSQP) [33] that exploits the knowledge of the Hessian matrix, which in (46) is clearly $\boldsymbol{D}$.

VI. NUMERICAL RESULTS

In this section, we report simulation results of the proposed CR-PLA with optimized strategies, and compare them with existing techniques. We consider a scenario wherein both Trudy and Alice move on an horizontal square grid of dimension

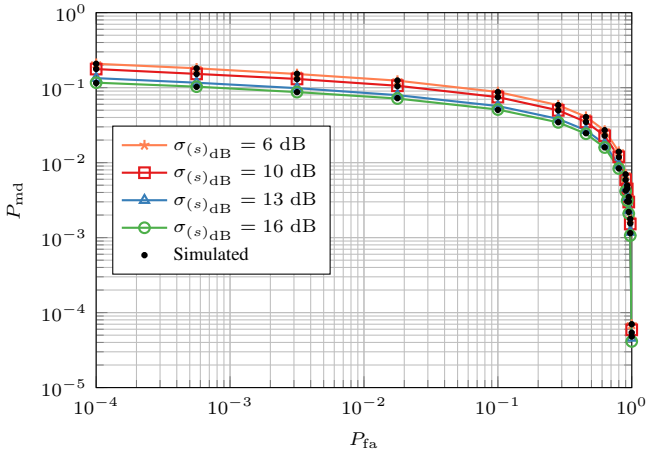


Fig. 3. DET curves for $\sigma_{(s)_{\text{dB}}} = 6$, 10, 13, and 16 dB for simulated and theoretical analysis.

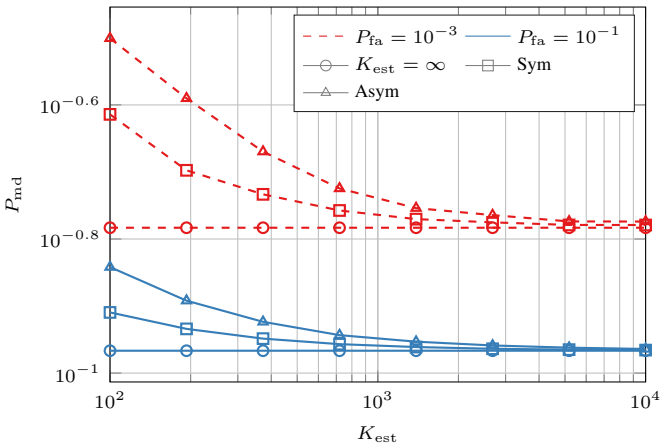


Fig. 4. DET curves for different number of pilot symbols in the set-up phase, K_{est}. Circles for perfect estimation $K_{\text{est}} = \infty$, triangles refer to the Asym scenario, and squares refer to the Sym scenario.

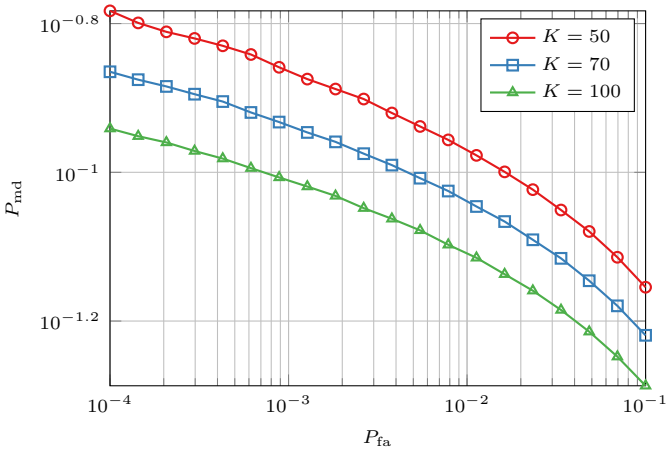


Fig. 5. DET curves for different number of pilot symbols in the authentication phase, K.

$420\,\text{m} \times 420\,\text{m}$ at a fixed height h, with 15 possible values of the position on each (x and y) axis. The values of shadowing STDs $\sigma_{(s)_{\text{dB}}}$ taken from [34] refer to a ray-tracing simulation used to model a channel at 2.4 GHz in different environments. In particular, values $\sigma_{(s)_{\text{dB}}} \simeq 10, 13$, and 16 dB refer to urban and suburban not line-of-sight (NLOS) scenarios, respectively. On the other hand, $\sigma_{(s)_{\text{dB}}} \simeq 6\,\text{dB}$ is taken from [35] where the authors conducted field measurements in rural areas at 2.4 GHz. Table I summarizes the main simulation parameters; if not otherwise stated, the parameters used in the simulations are reported in the column *Default value*.

A. Comparison with Other Approaches

We first compare the security performance of our scheme with other solutions present in the literature. In particular, we consider the uniform strategy (US) proposed in [10] and [11], where Bob and Trudy uniformly pick a gain over the set of possible values of the map. We also consider the case in which Bob still picks the gain uniformly at random, while Trudy uses the strategy that maximizes the MD probability: this is the best attack against the uniform defense strategy proposed in [10], [11]) and we denote it as the best attack against the uniform defense (BAUD) strategy.

Note that the various solutions discussed in Section V achieve all the same security performance since we always consider NEs of the game, and all NEs yield the same MD probability.

Fig. 2 reports the detection error trade-off (DET) curves, i.e., MD probability as a function of the FA probability, considering the proposed game theoretic approach (denoted with NE in the plot) against the US and BAUD strategies. The number of rounds is $N = 2$, while the other parameters are reported in Table I. We confirm that the NE provides the lowest MD probability, as the uniform strategy is not the best for Bob. Moreover, we see that the uniform strategy for Bob is particularly vulnerable to the best attack by Trudy. We also observe that we are able to reduce the MD probability by one order of magnitude with just two rounds.

B. Impact of CR-PLA Parameters

We now investigate the effects of several parameters of the proposed technique on its performance.

Shadowing variance $\sigma_{(s)_{\text{dB}}}$: First, Fig. 3 compares the security performance in environments characterized by different shadowing variances. The figure shows the DET curves, for $N = 1$, $\sigma_{(s)_{\text{dB}}} = 6$, 10, 13, and 16 dB. Lines are obtained with the closed-form formulas of the probability, while black markers show the results obtained with Monte Carlo simulations. We note a perfect agreement between the analytical and numerical results. When comparing the different variances of the shadowing, we note that the MD probability decreases with $\sigma_{(s)_{\text{dB}}}$ (for a fixed FA probability). This is because a high $\sigma_{(s)_{\text{dB}}}$ value increases the map diversity, i.e., positions at the same distance from the receiver have different gains, thus it is harder for Trudy to guess a position leading to the same gain as Alice to fool Bob.

In the next figures, we will keep the shadowing variance fixed to $\sigma_{(s)_{\text{dB}}} = 10\,\text{dB}$.

Number of Pilot Symbols in the Set-up Phase, K_{est}: We now consider the impact of the number of pilot symbols used

for channel estimation in the set-up phase of CR-PLA. When K_{est} is finite, Bob adapts the threshold ϕ to match the desired FA probability. In fact, for a finite number of reference gains estimation pilots K_{est}, the threshold ϕ required to obtain a desired FA probability is computed numerically, as well as the payoff matrix in (33) (containing the MD probabilities) since the test distribution in (18) cannot be computed in closed form. We consider three scenarios: the perfect gain estimation ($K_{\text{est}} = \infty$, our baseline), the Symmetric (Sym) scenario, and the Asymmetric (Asym) scenario. In the Sym case, Bob and Trudy compute the new strategies based on the new threshold and MD probability matrix. Finally, in the Asym case, Bob still keeps the baseline strategy, not taking into account the new setup (i.e., he deviates from the NE), and Trudy, aware of this, designs her strategy to maximize the MD probability.

Fig. 4 shows the obtained performance and we note that, depending on the desired FA probability, the impact of this imperfection soon vanishes by increasing the number of pilots K_{est}. We remark that such a high number of pilots is necessary only in the set-up phase, i.e., once and at the beginning of the protocol. In this simulation, we used a grid of $M_{\text{A}} = M_{\text{T}} = 4 \times 4$ positions.

Number of Pilot Symbols for Channel Estimation K: About the impact of the number of pilot symbols used for channel estimation in the authentication phase of CR-PLA, Fig. 5 shows the DET curves of the proposed solution for $N = 1$ round and $K = 50$, 70, and 100 pilot symbols. We see that a higher K yields better channel estimates and thus lower MD probabilities. However, the benefits are limited, indicating that it may be possible to achieve a good security performance even with low K values, thus potentially saving drone energy and time.

Number of Rounds N: We now consider the impact of the number of rounds N on the security performance. Fig. 6 shows the MD probability as a function of rounds N for FA probabilities 10^{-2}, 10^{-3}, and 10^{-4}. From the results, we see that the MD decreases exponentially with the number of rounds, thus, we can easily reduce the MD probability to desired values by adding a few more rounds. This, however, comes at the cost of increased consumed energy, as discussed below.

Two Drone Authentication: We consider a scenario where Alice and Trudy maneuver two drones each. To avoid any possible collision, Alice set the drones to fly at different altitudes, h_1 and h_2. Additionally, Alice, to avoid introducing any degree of correlation that the attacker may exploit, flies her drones to move independently from one another. In turn, to maximize her chance of success, Trudy sets each of her own drones to fly independently but at the same altitudes of Alice's drones h_1 and h_2. As each Alice-Trudy pair of drones plays independently from the others, each game is solved using (40), and leveraging on the independence, we use test (18) considering $N = 2$, as the shadowing maps and thus reference gains are known. On the other hand, we remark that games played at different rounds are performed on the same shadowing map, while games played at the same time but at different altitudes are played on a different shadowing map. Thus, while in the $N = 2$ round case, the same strategy can be used in both games, for the two drones (single round) scenario, a new strategy has to be computed for each drone pair.

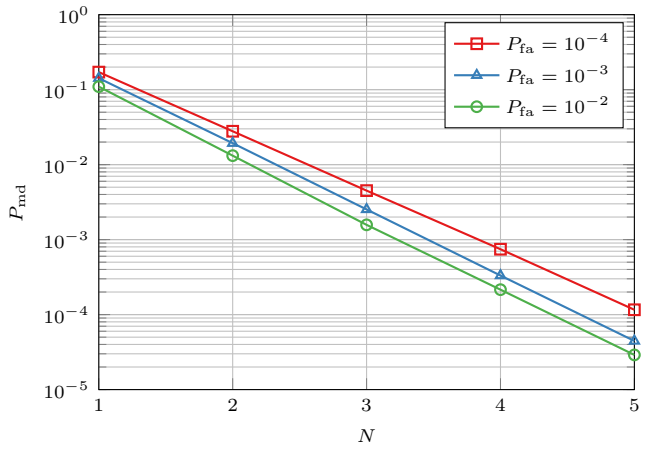


Fig. 6. P_{md} as a function of the number of rounds, N, for $P_{\text{fa}} = 10^{-2}$, 10^{-3}, and 10^{-4}.

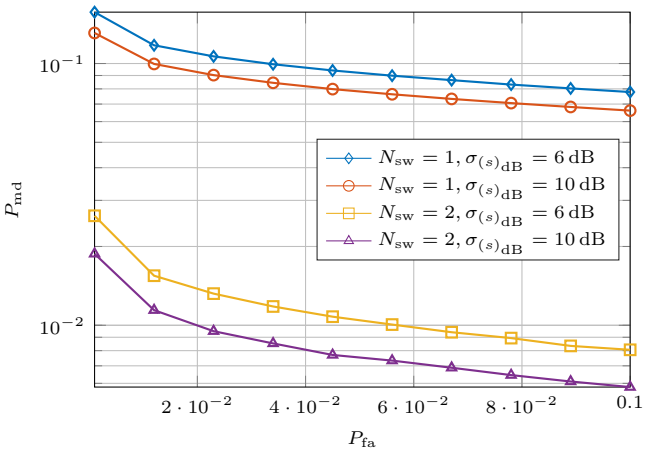


Fig. 7. DET curves with $\sigma_{(s)_{\text{dB}}} = 6\,\text{dB}$ and $10\,\text{dB}$, for the single drones $N_{\text{sw}} = 1$ flying at $h_1 = 30\,\text{m}$, and swarms $N_{\text{sw}} = 2$ scenario where an Alice-Trudy drone pair flies at $h_1 = 30\,\text{m}$ and the other pair flies at $h_2 = 70\,\text{m}$.

Fig. 7 shows the DET curves comparing the scenarios where Alice and Trudy control either one or two drones each, for $\sigma_{(s)_{\text{dB}}} = 6$ and $10\,\text{dB}$. In particular, for the two-drones scenario, the drones are at altitudes $h_1 = 30\,\text{m}$ and $h_2 = 70\,\text{m}$. Indeed, having two drones makes the test more robust, approximately reducing the MD by a factor of 10. Finally, we point out that the proposed approach may be straightforwardly extended to swarm authentication, placing the drones at different altitudes. We also report the results for both the urban and rural areas (in terms of shadowing). Even in this case, we note that a higher shadowing variance improves the security of the authentication mechanism.

C. Impact of The Map Geometry

We now investigate the maps' effects on the proposed solution's performance.

Drone Altitude: First, we investigate the impact of Alice's and Trudy's altitude h. Fig. 8 shows the achieved average

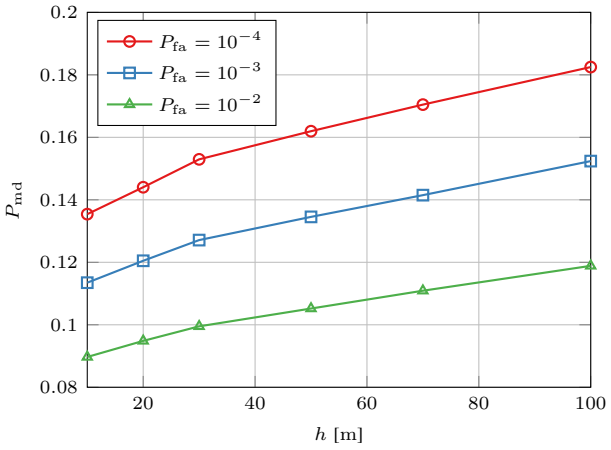


Fig. 8. P_{md} as a function of the drone altitude, h, for $P_{\text{fa}} = 10^{-3}$.

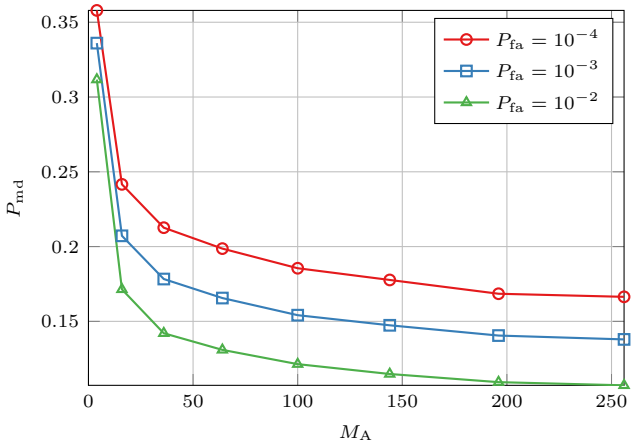


Fig. 9. P_{md} as function of the number of grid positions, for $P_{\text{fa}} = 10^{-2}$, 10^{-3}, and 10^{-4}.

P_{md} as a function of h, for $P_{\text{fa}} = 10^{-2}$, 10^{-3}, and 10^{-4}, with $N = 1$ round. We note that the MD probability slightly increases with h: indeed, increasing the altitude decreases the gain map diversity because the pathloss component becomes approximately constant as the grid area is fixed. In other words, the path loss becomes less relevant as all the grid positions experience the same one as the altitude h increases. This leads to a reduced variance of the gains over the map, and thus more similar challenges/responses, which in turn makes it easier for Trudy to guess the correct response.

Number of Positions on the Map: Then, we consider the impact of the number of positions on the map, with $\mathcal{X} = \mathcal{Y}$. Fig. 9 shows the MD probability as a function of the number of grid positions for $P_{\text{fa}} = 10^{-2}$, 10^{-3}, and 10^{-4}, and $N = 1$ round. We note that by increasing the overall number of positions (thus the number of possible challenges), the MD probability decreases. Still, after a rapid decrease, the MD reaches a plateau. Indeed, as the number of positions increases, the gains of nearby positions become closer, due to the shadowing correlation, thus not providing a significant further diversity for authentication. Still, the results highlight the trade-off between the duration of Step 1) of the protocol (see Section III) and the achievable performance, while showing that i) it is not necessary to sample too finely the space to achieve good performance and ii) a too precise sampling does not necessarily bring benefits for the legitimate party.

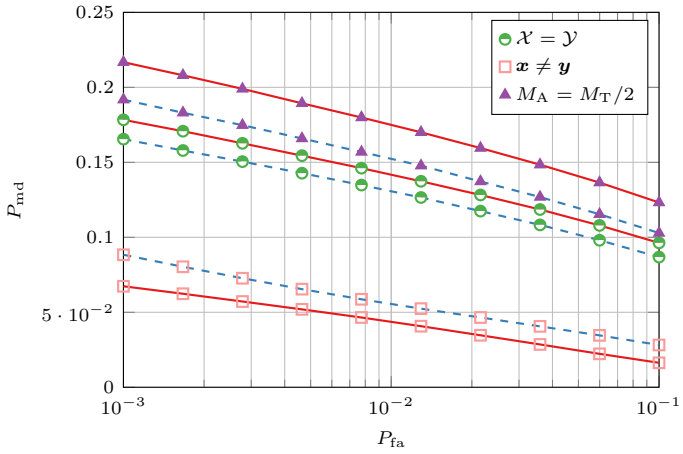


Fig. 10. DET curves with $M_{\text{T}} = 36$ (solid) and $M_{\text{T}} = 64$ (dashed) and various type of Alice-Trudy maps.

Alice-Trudy Map Difference: We study the impact that different sets of positions available to Trudy and Alice have on the DET curves. In particular, we consider the scenario (denoted as $M_{\text{A}} = M_{\text{T}}/2$) wherein the positions in $\mathcal{X}$ are half of those in $\mathcal{Y}$ (thus $M_{\text{A}} = M_{\text{T}}/2$), and Alice's positions are selected uniformly at random from Trudy's map. We compare it with a scenario (denoted as $\mathcal{X} = \mathcal{Y}$) wherein Alice and Trudy have the same map. Lastly, we consider the case in which the maps of Alice and Trudy are the same, but Trudy is not allowed to select the same position as Alice (as this may lead to a clash), and denote this scenario as $\boldsymbol{x} \neq \boldsymbol{y}$. Fig. 10 shows the DET for the three considered cases, comparing the results for $M_{\text{T}} = 36$ and 64, for $N = 1$. We can see that when Alice's map has half of the positions of Trudy, the P_{md} increases, as expected. Still, there are minor differences even though the number of grid positions is halved for Alice: this suggests that as long as there is enough variability in the gains available, Bob can still achieve good security performance. This fact is also confirmed by the scenario where Trudy is deprived of *good* positions (i.e., where she's in the same Alice's location) and the MD decreases. These effects are more visible with fewer grid positions. Indeed, for a denser grid, it is less likely that the deleted positions are relevant.

D. Average Traveled Distance

We now discuss the effectiveness of the distance minimization algorithms. We consider the S-NE, the optimal MRM-NE, and the SHM-NE solutions. For comparison purposes, we also show the average distance for a NE without distance optimization, a random NE is selected at each round (R-NE).

Fig. 11 shows the average distance $\bar{D}$ traveled by Alice over $N = 2$ rounds, as a function of the number of positions of the map M_{A}, positioned on a grid always occupying the same area. As we can see, the distance-optimized solutions

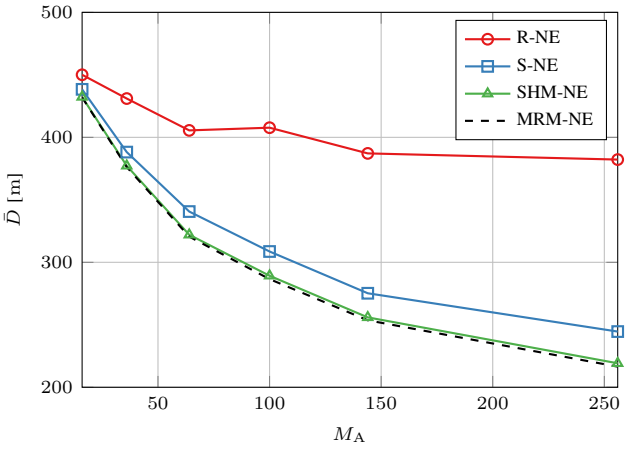


Fig. 11. Average distance traveled by Alice vs the number of grid positions M_{A}, with $N = 2$ rounds, for $P_{\mathrm{fa}} = 10^{-3}$.

outperform the baseline R-NE, and with a larger number of grid positions, the traveled distance decreases. This is because by increasing the positions the more degrees of freedom the optimization algorithms have, thus can find better NEs from the distance perspective. We also notice that the SHM-NE solution outperforms the S-NE solution and achieves close-to-bound performance (represented by the optimal MRM-NE solution) but with much lower computations, confirming our suppositions.

VII. Conclusions

In this paper, we have proposed novel strategies for CR-PLA with drones: we have optimized the PMD used to select the challenge by Bob, and correspondingly, the PMD of the random attack performed by Trudy. We formulated the problem as a zero-sum game with payoff the MD probability, thus characterizing the NEs of the game. To further decrease the MD probability, the protocol can be repeated for multiple rounds/movements.

Among solutions providing the same MD probability, we have then selected the PMD for Bob, yielding the minimum energy consumption due to the movement. Three solutions were proposed: the optimal MRM-NE solution, the S-NE solution where the challenge is chosen drawing always the same NE, and the SHM-NE solution where we associate the best NE to each possible position on the map. SHM-NE performs close to the optimal MRM-NE strategy, but it is much more lightweight in terms of computations.

Simulation results are obtained over realistic urban NLOS and rural scenarios, including path loss, fading, and shadowing phenomena. In particular, the proposed solution achieves MD/FA probabilities of $\sim 10^{-3}$ with only $N = 3$ rounds.

References

[1] M. Adil, M. A. Jan, Y. Liu, H. Abulkasim, A. Farouk, and H. Song, "A systematic survey: Security threats to UAV-aided IoT applications, taxonomy, current challenges and requirements with future research directions," *IEEE Trans. Intell. Transp. Syst*, vol. 24, no. 2, pp. 1437–1455, Feb. 2023.

[2] M. Ceccato, F. Formaggio, and S. Tomasin, "Spatial GNSS spoofing against drone swarms with multiple antennas and Wiener filter," *IEEE Trans. Signal Process.*, vol. 68, pp. 5782–5794, Oct. 2020.

[3] G. Michieletto, F. Formaggio, A. Cenedese, and S. Tomasin, "Robust localization for secure navigation of UAV formations under GNSS spoofing attack," *IEEE Trans. Automat. Sci. and Eng*, pp. 1–14, Sept. 2022.

[4] E. Illi, M. Qaraqe, S. Althunibat, A. Alhasanat, M. Alsafasfeh, M. de Ree, G. Mantas, J. Rodriguez, W. Aman, and S. Al-Kuwari, "Physical layer security for authentication, confidentiality, and malicious node detection: A paradigm shift in securing IoT networks," *IEEE Commun. Surv. & Tut.*, vol. 26, no. 1, pp. 347–388, Firstquarter 2024.

[5] T. M. Hoang, A. Vahid, H. D. Tuan, and L. Hanzo, "Physical layer authentication and security design in the machine learning era," *IEEE Commun. Surv. & Tut.*, vol. 26, no. 3, pp. 1830–1860, Thirdquarter 2024.

[6] S. J. Maeng, Y. Yapıcı, I. Güvenç, H. Dai, and A. Bhuyan, "Power allocation for fingerprint-based PHY-layer authentication with mmWave UAV networks," in *Proc. of the Int. Conf. on Commun. (ICC)*, 2021, pp. 1–6.

[7] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, and H. Karimipour, "Federated learning for drone authentication," *Ad Hoc Netw.*, vol. 120, p. 102574, Sept. 2021.

[8] P. C. Gupta, *Cryptography and network security*. PHI Learning, 2014.

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

[10] F. Mazzo, S. Tomasin, H. Zhang, A. Chorti, and H. V. Poor, "Physical-layer challenge-response authentication for drone networks," in *Proc. of IEEE Global Commun. Conf. (GLOBECOM)*, 2023, pp. 3282–3287.

[11] F. Ardizzon, D. Salvaterra, M. Piana, and S. Tomasin, "Energy-based optimization of physical-layer challenge-response authentication with drones," [Accepted] Proc. of IEEE Global Commun. Conf. (GLOBECOM), 2024. [Online]. Available: https://arxiv.org/abs/2405.03608

[12] H. V. Abeywickrama, B. A. Jayawickrama, Y. He, and E. Dutkiewicz, "Comprehensive energy consumption model for unmanned aerial vehicles, based on empirical studies of battery performance," *IEEE Access*, vol. 6, pp. 58 383–58 394, Oct. 2018.

[13] Y. Zhang, D. He, L. Li, and B. Chen, "A lightweight authentication and key agreement scheme for Internet of Drones," *Comput. Commun.*, vol. 154, pp. 455–464, Mar. 2020.

[14] L. Xiao, T. Chen, G. Han, W. Zhuang, and L. Sun, "Channel-based authentication game in MIMO systems," in *Proc. of IEEE Global Commun. Conf. (GLOBECOM)*, 2016, pp. 1–6.

[15] Y. Ge and Q. Zhu, "GAZETA: Game-theoretic zero-trust authentication for defense against lateral movement in 5G IoT networks," *IEEE Trans. on Inf. Forens. and Secur.*, vol. 19, pp. 540–554, Oct. 2024.

[16] Y. Wu, T. Jing, Q. Gao, Y. Wu, and Y. Huo, "Game-theoretic physical layer authentication for spoofing detection in Internet of Things," *Digit. Commun. and Netw.*, Jan. 2023.

[17] Y. Zhou, P. L. Yeoh, K. J. Kim, Z. Ma, Y. Li, and B. Vucetic, "Game theoretic physical layer authentication for spoofing detection in UAV communications," *IEEE Trans. on Veh. Technol.*, vol. 71, no. 6, pp. 6750–6755, Mar. 2022.

[18] M. Gudmundson, "Correlation model for shadow fading in mobile radio systems," *Electron. Lett.*, vol. 23, no. 27, pp. 2145–2146, Nov. 1991.

[19] N. Benvenuto, G. Cherubini, and S. Tomasin, *Algorithms for Commun. Systems and their Applications*, 2nd ed. Wiley, 2021.

[20] D. Tse and P. Viswanath, *Fundamentals of wireless communication*. Cambridge University Press, 2005.

[21] R. H. Clarke, "A statistical theory of mobile-radio reception," *The Bell Syst. Tech. J.*, vol. 47, no. 6, pp. 957–1000, July-Aug. 1968.

[22] L. Senigagliesi, M. Baldi, and E. Gambi, "Comparison of statistical and machine learning techniques for physical layer authentication," *IEEE Trans. Inf. Forensics Secur.*, vol. 16, pp. 1506–1521, Oct. 2021.

[23] L. Bragagnolo, F. Ardizzon, N. Laurenti, P. Casari, R. Diamant, and S. Tomasin, "Authentication of underwater acoustic transmissions via machine learning techniques," in *Proc. of IEEE Int. Conf. on Microw., Antennas, Commun. and Electron. Syst. (COMCAS)*, 2021, pp. 255–260.

[24] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[25] I. Bisio, C. Garibotto, H. Haleem, F. Lavagetto, and A. Sciarrone, "On the localization of wireless targets: A drone surveillance perspective," *IEEE Network*, vol. 35, no. 5, pp. 249–255, 2021.

[26] S. Srigrarom, N. J. L. Sie, H. Cheng, K. H. Chew, M. Lee, and P. Ratsamee, "Multi-camera multi-drone detection, tracking and localization

with trajectory-based re-identification," in *Proc. 2021 Second International Symposium on Instrumentation, Control, Artificial Intelligence, and Robotics (ICA-SYMP)*, 2021, pp. 1–6.
[27] L. Chiarello, P. Baracca, K. Upadhya, S. R. Khosravirad, and T. Wild, "Jamming detection with subcarrier blanking for 5G and beyond in industry 4.0 scenarios," in *Proc. Annu. Int. Symp. on Pers., Indoor and Mobile Radio Commun. (PIMRC)*, 2021, pp. 758–764.
[28] X. Peng, C. Huang, X. Zhu, Z. Chen, and X. Yuan, "GLRT-based spacetime detection algorithms via joint DoA and Doppler shift method for GNSS spoofing interference," *IEEE Internet Things J.*, pp. 1–1, June 2024.
[29] F. Ardizzon and S. Tomasin, "Learning the likelihood test with one-class classifiers for physical layer authentication," 2024. [Online]. Available: https://arxiv.org/abs/2210.12494
[30] S. Tadelis, *Game theory: an introduction*. Princeton University Press, 2013.
[31] J. V. Neumann, "Zur Theorie der Gesellschaftsspiele," *Math. Ann.*, vol. 100, no. 1, pp. 295–320, Dec. 1928.
[32] A. Washburn, *Two-person zero-sum games*. Springer, 2014.
[33] P. T. Boggs and J. W. Tolle, "Sequential quadratic programming," *Acta Numer.*, vol. 4, p. 1–51, 1995.
[34] N. Sharma, M. Magarini, L. Dossi, L. Reggiani, and R. Nebuloni, "A study of channel model parameters for aerial base stations at 2.4 GHz in different environments," in *Proc. IEEE Annu. Consumer Commun. & Netw. Conf. (CCNC)*, 2018, pp. 1–6.
[35] S. Chandrasekharan, A. Al-Hourani, K. Magowe, L. Reynaud, and S. Kandeepan, "Propagation measurements for D2D in rural areas," in *Proc. of the Int. Conf. on Commun. Workshop (ICCW)*. IEEE, 2015, pp. 639–645.

APPENDIX A
PROOF OF LEMMA 1

From (12) with $\boldsymbol{q} = \boldsymbol{x}(i)$, let

$$\tilde{r}_k = \tilde{g}_{\boldsymbol{x}(i)} h_k e^{-j\phi} + w'_k \,. \tag{47}$$

We note that the real and imaginary parts of $\tilde{r}_k$ are zero-mean Gaussian distributed random variables with variance

$$\tilde{\sigma}^2_{\boldsymbol{x}(i)} = \frac{\tilde{g}^2_{\boldsymbol{x}(i)} + \sigma^2_w}{2} \,, \tag{48}$$

which depends on Alice's position $\boldsymbol{x}(i)$. Consequently, $|\tilde{r}_k|^2$ is exponentially distributed with parameter

$$\lambda_{\boldsymbol{x}(i)} = \frac{1}{2\tilde{\sigma}^2_{\boldsymbol{x}(i)}}. \tag{49}$$

We assume that the samples r_k of the received signal are taken sufficiently far apart in time, i.e., with $T_\mathrm{s} > T_\mathrm{c}$, so the fading coefficients h_k are statistically independent. This implies that

$$\mathbb{E}[\tilde{r}_k \tilde{r}^*_{k'}] = 0 \,, \forall k' \neq k \,, \tag{50}$$

thus samples taken at different times k and k' are independent, since $\tilde{r}_k$ is Gaussian. Hence, we resort to the central limit theorem, thus $\mu(\boldsymbol{x}(i))$, defined in (12), converges, for K sufficiently large, in terms of CDF to a normal distribution

$$\sqrt{K}\left(\mu(\boldsymbol{x}(i)) - \frac{1}{\lambda_{\boldsymbol{x}(i)}}\right) \xrightarrow{d} \mathcal{N}\left(0, \frac{1}{\lambda^2_{\boldsymbol{x}(i)}}\right). \tag{51}$$

Lastly, reordering the terms and defining $m(i) = 1/\lambda_{\boldsymbol{x}(i)}$, we obtain (16).

APPENDIX B
PROOF OF LEMMA 2

From (12) and (47), two gains $\hat{m}_n$ and $\hat{m}_{n'}$ estimated by Bob at different times $n = kT_s$ and $n' = k'T_s$ have correlation

$$\begin{aligned}\mathbb{E}[\hat{m}_n \hat{m}_{n'}] &= \mathbb{E}\left[\frac{1}{K}\sum_k |\tilde{r}_k|^2 \frac{1}{K}\sum_{k'} |\tilde{r}_{k'}|^2\right] \\ &= \frac{1}{K^2}\sum_k \sum_{k'} \mathbb{E}\left[|\tilde{r}_k|^2 |\tilde{r}_{k'}|^2\right].\end{aligned} \tag{52}$$

Next, as discussed in Appendix A, samples $\tilde{r}_k$ and $\tilde{r}_{k'}$ measured at sufficiently far apart instants, and therefore also their squared amplitude, are independent, hence reordering the terms

$$\begin{aligned}\mathbb{E}[\hat{m}_n \hat{m}_{n'}] &= \frac{1}{K^2}\sum_k \sum_{k'} \mathbb{E}\left[|\tilde{r}_k|^2 |\tilde{r}_{k'}|^2\right] \\ &= \frac{1}{K^2}\sum_k \sum_{k'} \mathbb{E}\left[|\tilde{r}_k|^2\right] \mathbb{E}\left[|\tilde{r}_{k'}|^2\right] = \mathbb{E}[\hat{m}_n]\mathbb{E}[\hat{m}_{n'}].\end{aligned} \tag{53}$$

From (53), we have that $\hat{m}_n$ and $\hat{m}_{n'}$ are uncorrelated, thus independent as they are Gaussian.

APPENDIX C
PROOF OF THEOREM 1

As discussed in Section IV-A, Bob draws the gains independently, thus (29) holds. Given that Bob's and Trudy's strategies are independent of each other, the MD probability can be written as

$$\begin{aligned}P_\mathrm{md} = &\sum_{\boldsymbol{m}} \sum_{\boldsymbol{m}_\mathrm{T}} \mathbb{P}\left(\sum_{n=1}^N \frac{K(\hat{m}_n(\boldsymbol{m}_\mathrm{T}) - m_n)^2}{m_n^2} \leq \varphi \Big| \boldsymbol{m}, \boldsymbol{m}_\mathrm{T}\right) \times \\ &p_\mathrm{A}(\boldsymbol{m}) p_\mathrm{T}(\boldsymbol{m}_\mathrm{T}) \,,\end{aligned} \tag{54}$$

where (54) is (28) highlighting the fact that, in general, the measured gain when Trudy is transmitting may be a function of the previous (or next) gains, i.e., $z_n = z_n(\boldsymbol{m}_\mathrm{T}) = \hat{m}_n(\boldsymbol{m}_\mathrm{T})$.

Focusing on the choice of $m_{\mathrm{T},k}$, $k = 1, \ldots, N$, let $\bar{\boldsymbol{m}}_\mathrm{T}$ be the vector $\boldsymbol{m}_\mathrm{T}$ from which we exclude the k-th entry $m_{\mathrm{T},k}$. Next, we define

$$\phi(\bar{\boldsymbol{m}}_\mathrm{T}, \boldsymbol{m}) = \sum_{n=1, n\neq k}^N \frac{K(\hat{m}_n(m_{\mathrm{T},n}) - m_n)^2}{m_n^2} \,, \tag{55}$$

representing the results of all the tests except the k-th test.

To prove the theorem, we focus on the latter term in (54). In particular, we split the k-th test result from the others exploiting (55), as

$$\begin{aligned}&\mathbb{P}\left(\sum_{n=1}^N \frac{K(\hat{m}_n(\boldsymbol{m}_\mathrm{T}) - m_n)^2}{m_n^2} \leq \varphi \Big| \boldsymbol{m}, \boldsymbol{m}_\mathrm{T}\right) = \\ &\mathbb{P}(\phi(\bar{\boldsymbol{m}}_\mathrm{T}, \boldsymbol{m}) = \phi | \bar{\boldsymbol{m}}_\mathrm{T}, \boldsymbol{m}) \times \\ &\mathbb{P}\left(\frac{K(\hat{m}_k(m_{\mathrm{T},k}) - m_k)^2}{m_k^2} \leq \varphi - \phi \Big| m_k, m_{\mathrm{T},k}, \phi\right)\end{aligned} \tag{56}$$

Now, noticed that in (54) it holds

$$p_{\mathrm{T}}(\boldsymbol{m}_{\mathrm{T}}) = \mathbb{P}(m_{\mathrm{T},k}|\bar{\boldsymbol{m}}_{\mathrm{T}})\mathbb{P}(\bar{\boldsymbol{m}}_{\mathrm{T}})\,, \tag{57}$$

by reordering the terms in (54), we can define the probability

$$f(\boldsymbol{m}_{\mathrm{T}}, \boldsymbol{m}) = \mathbb{P}(m_{\mathrm{T},k}|\bar{\boldsymbol{m}}_{\mathrm{T}})\times \\ \mathbb{P}\left(\frac{K(\hat{m}_k(m_{\mathrm{T},k}) - m_k)^2}{m_k^2} \leq \varphi - \phi \Big| m_k, m_{\mathrm{T},k}, \phi\right), \tag{58}$$

which groups together all the terms that are impacted by the choice of the gain $m_{\mathrm{T},k}$ at round k in (54). We note that m_n, $n = 1, \ldots, N$, are independent and that the maximization of this probability depends on neither φ nor ϕ. In other words, this shows that on each round Trudy aims at maximizing (58), regardless of the previous and next choices.

Finally, we can conclude that each round is an independent game that can be solved separately, i.e., the overall attacker PMD can be factorized as in (30).

Appendix D
Proof of Lemma 3

Let $(\boldsymbol{a}_1^\star, \boldsymbol{e}_1^\star)$ and $(\boldsymbol{a}_2^\star, \boldsymbol{e}_2^\star)$ be two NEs. Then, by definition of NE, we have that

$$\begin{aligned} u_{\mathrm{A}}(\boldsymbol{a}_1^\star, \boldsymbol{e}_1^\star) &\geq u_{\mathrm{A}}(\boldsymbol{a}_2^\star, \boldsymbol{e}_1^\star), \\ u_{\mathrm{T}}(\boldsymbol{a}_1^\star, \boldsymbol{e}_1^\star) &\geq u_{\mathrm{T}}(\boldsymbol{a}_1^\star, \boldsymbol{e}_2^\star). \end{aligned} \tag{59}$$

Since the game is zero-sum, we have $u_{\mathrm{T}} = -u_{\mathrm{A}}$, thus $u_{\mathrm{A}}(\boldsymbol{a}_2^\star, \boldsymbol{e}_1^\star) \geq u_{\mathrm{A}}(\boldsymbol{a}_2^\star, \boldsymbol{e}_2^\star)$. Hence

$$u_{\mathrm{A}}(\boldsymbol{a}_1^\star, \boldsymbol{e}_1^\star) \geq u_{\mathrm{A}}(\boldsymbol{a}_2^\star, \boldsymbol{e}_1^\star) \geq u_{\mathrm{A}}(\boldsymbol{a}_2^\star, \boldsymbol{e}_2^\star)\,, \tag{60}$$

and similarly

$$u_{\mathrm{A}}(\boldsymbol{a}_1^\star, \boldsymbol{e}_1^\star) \leq u_{\mathrm{A}}(\boldsymbol{a}_1^\star, \boldsymbol{e}_2^\star) \leq u_{\mathrm{A}}(\boldsymbol{a}_1^\star, \boldsymbol{e}_2^\star)\,. \tag{61}$$

Following the inequalities of (60) and (61) we have that

$$u_{\mathrm{A}}(\boldsymbol{a}_1^\star, \boldsymbol{e}_1^\star) = u_{\mathrm{A}}(\boldsymbol{a}_2^\star, \boldsymbol{e}_2^\star)\,, \tag{62}$$

i.e., the two NEs yield the same utility.