Physical-Layer Challenge-Response Authentication for Drone Networks

Francesco Mazzo, Stefano Tomasin, Hongliang Zhang, Arsenia Chorti, H. Vincent Poor

Physical-Layer Challenge-Response Authentication for Drone Networks

Francesco Mazzo[1], Stefano Tomasin[2], Hongliang Zhang[3], Arsenia Chorti[4], and H. Vincent Poor[4]
[1] Dept. of Information Engineering, University of Padova (I)
[2] Dept. of Information Engineering and Dept of Mathematics, University of Padova and CNIT (I), corresponding author: stefano.tomasin@unipd.it [3] Peking University (China) – [4]ETIS UMR 8051, CYU, ENSEA, CNRS (FR), and Barkhausen Institut gGmbH (DE) [5] Princeton University (USA)

***Abstract*—Authenticating the communications among drones operating as a network (or a swarm) is crucial for the control of the network. When drones are in turn supporting communications with other ground devices (e.g., in non-terrestrial networks), all nodes in the network need to be authenticated for end-to-end security. The absence of a reliable fixed network architecture among drones, which are only connected by wireless links, calls for new authentication mechanisms that can complement or be used as alternatives to those offered by cryptography. We propose a challenge-response (CR) physical-layer authentication (PLA) mechanism, where, upon a transmission request from a transmitting drone, referred to as Alice, Bob either asks Alice to move in a specific (randomly chosen) position or moves to a (randomly chosen) position: in both cases, changes in the propagation environment are controlled by Bob. Then, the message is transmitted and Bob estimates the channel from the received signal and verifies that it is compatible with the positions assumed by Alice and Bob. Note that Bob may represent a group of drones that cooperate for authentication. We discuss several security challenges to this CR PLA mechanism and compare them with existing approaches. Preliminary results on the performance of the proposed authentication scheme are presented, showing the advantage of the CR PLA approach.**

I. Introduction

The use of drones for communication purposes is a subject of research and investigation by standardization bodies, notably in the contexts of *non-terrestrial networks* (NTNs), [1], flying ad-hoc networks (FANETs) [2], and Internets of drones (IoDs) [3]. Multiple drones can be organized in a network, or *swarm*, to jointly perform coordinated tasks, such as obtaining multiple views of the same scene or increasing the robustness of the connectivity in NTNs [4]. While providing a flexible and agile communication infrastructure, drones are exposed to several security threats, including attacks against global positioning systems to disrupt their navigation [5], [6], denial of service, jamming, and de-authentication attacks (see [7] for a survey).

In this paper, we consider the problem of authenticating drones in a swarm, which is a key issue, especially when the exchanged signals impact the navigation of the drones, and injecting fake control messages into the network may significantly disrupt its operation. Several authentication mechanisms have been proposed in the literature to improve drone security. In [8], a low-latency solution for drone swarms in fifth-generation (5G) networks is proposed, operating with shared keys among the drones; a group authentication technique has been proposed in [9]; the work in [10] proposes a distributed delegation-based authentication mechanism to reduce the traffic overhead toward the 5G core network; a solution leveraging blockchain technology has been proposed in [11]. All these approaches are based on cryptography.

However, cryptographic solutions require the frequent update of secret keys, which in turn requires many resources. As a lightweight alternative security solution, recently, physically unclonable functions (PUFs) have also been investigated: PUFs can be described as sets of hardware fingerprints that can be used in challenge-response authentication schemes. In [12], PUFs and a chaotic system support mutual authentication and establish a secure session key in a swarm. A related solution has been proposed in [13], which resorts to eCRPs (extended challenge-response pairs) to make the system resilient to information disclosure and malicious insider attacks. In [14] a protocol tolerant of minor PUF errors caused by ambient circumstances outside the user's control is proposed, while in [15] a full physical layer authentication protocol is presented leveraging PUFs and node mobility.

In an effort to explore further alternatives, in this paper, we focus on solutions based on signals exchanged at the physical layer, to obtain physical-layer authentication (PLA) mechanisms. Such solutions do not require additional dedicated hardware and exploit most of the signal processing already existing in the devices for communication purposes to also achieve a security target. In particular, in PLA the propagation characteristics of the communication channel between two drones are used as a fingerprint for the exchanged messages since devices in different positions experience different channels (see [16] for more details).

Based on this approach, a cooperative PLA mechanism using multiple drones has been proposed in [17]. Instead of using physical-layer attributes, the information obtained at the medium access control layer or average physical-layer measurements is used for authentication in [18]. However, such an approach is vulnerable to multiple attacks, where the attacker forges different signals to let the victim estimate

This work was supported by the European Union's NextGenerationEU instrument, under the Italian National Recovery and Resilience Plan (NRRP), Mission 4 Component 2 Investment 1.3, enlarged partnership "Telecommunications of the Future" (PE0000001), program "RESTART".

different channels until authentication is broken [19]. Hence, recently the authors proposed a challenge-response (CR) PLA mechanism, based on the *partial control* of the propagation environment by the verifier, [20]: the idea is that the verifier alters the signal propagation environment and checks if this modification is appropriately reflected in the estimated channel obtained from the received signal. Note that this solution is different from the challenge-response authentication mechanism (CRAM) proposed in [21], where the channel is used to hide both the challenge and the response from Eve using a PLS confidentiality mechanism. In CR PLA instead, the channel is *physically changed*.

In this paper, we introduce a CR PLA protocol for a drone swarm and analyze its security properties. In this context, the propagation environment is controlled by moving the drones, i.e., either the verifier (Bob) or the device under verification (Alice). In particular, in the proposed PLA mechanism, upon a transmission request from (presumably) Alice, Bob either asks Alice to move to a specific (randomly chosen) position, or Bob moves to a (randomly chosen) position: in both cases, the propagation environment is altered in a way that is under the control of Bob. Then, the message is transmitted, Bob estimates the channel from the received signal, and he verifies that it is compatible with the positions of both Alice and Bob. Note that Bob may also be a set of drones that jointly cooperate for authentication. We discuss several security challenges to this CR PLA mechanism and compare it with cryptographic-CR techniques. Preliminary results on the performance of the proposed authentication scheme are discussed.

II. System Model

We consider a swarm of N drones organized in a communication network to exchange data. Each drone is equipped with a wireless transmitter and a wireless receiver, and all are operating at the same frequency.

A subset (Bob) of K drones is in charge of verifying if the messages transmitted by the other $N-K$ drones are authentic, i.e., they truly come from the swarm of an attacking device. The attacking device (Eve) is aiming at impersonating one drone of the swarm (Alice), i.e., Eve transmits messages claiming to be Alice. Bob uses PLA to detect the attack.

A. Physical Layer Authentication

A general authentication mechanism is composed of the *identification association (ID-A)* phase, during which the legitimate transmitter is assigned an identifying feature using an authenticated channel, and an *identification verification (ID-V)* phase, where the identifying feature is verified with the message reception.

In PLA, the ID-A phase consists of the identification of the channel features, while the ID-V phase consists in checking if the received message has the same channel features as the ID-A phase. Such channel features, can be, as suggested in [18], the received signal strength indication (RSSI), the carrier frequency offset (CFO), the channel impulse response (CIR), etc. All these features depend on the position of the device and the propagation environment where the swarm is flying, while still having some correlation for a couple of devices in different positions.

Here we denote with a matrix the set of channel parameters used for PLA. In particular, $\boldsymbol{H}^{(AB)}(t)$, $\boldsymbol{H}^{(AE)}(t)$, and $\boldsymbol{H}^{(EB)}(t)$ denote the Alice-Bob, Alice-Eve, and Eve-Bob channels at time t. All these sets of parameters are correlated since they all depend on the common propagation environment shared by the drones. Still, they are different because of the different positions of the devices. We also assume channel reciprocity, thus for example $\boldsymbol{H}^{(AB)}(t) = \boldsymbol{H}^{(BA)}(t)$, the latter being the Bob-Alice channel. The set of parameters $\boldsymbol{H}^{(AB)}(t)$ represents the tag used by Bob to authenticate messages from Alice. All estimates of channel parameters are affected by estimation errors, due for example to the noise.

Attack Model: We assume that Eve obtains estimates of the parameters of her channel to both Alice and Bob ($\boldsymbol{H}^{(AE)}(t)$ and $\boldsymbol{H}^{(EB)}(t)$) when the two drones are transmitting. We also assume that Eve is able to transmit any signal: she does not have power limitation and is equipped with a large number of antennas, thus she can let Bob estimate any set of channel parameters $\boldsymbol{G}(t)$.

III. Challenge-Response Authentication

In a challenge-response (CR) authentication mechanism, Bob asks a question, to which only Alice is able to give the right answer. At any time authentication is needed, the question (and correspondingly the answer) is always different: thus in this case we do not have a tag that is always compared with a reference, fixed tag (as in tag-based authentication,e.g., using digital certificates or passwords), but the check is performed on a time-varying answer. In [22], the terminology for the CRAM is presented:

- *Challenge:* is a question sent by a verifying entity to the entity under verification to establish its identity. The challenge can be *static* or *dynamic*. In the first case, the verifying entity chooses the challenge from a set of predefined challenges while in the second case the challenge changes depending on the system conditions.
- *Response:* it represents the answer sent back by the requesting entity towards the verifying one. The answer is computed with the help of a secret owned only by the two entities.
- *Authentication:* process in which the verifying entity ensures the authenticity of the requesting entity.

A. Proposed CR PLA Mechanism

In [20] a CR mechanism has been proposed for PLA, where the challenge is a modification of the propagation environment desired by the verifier (Bob), while the answer is the resulting channel between Alice and Bob. Here we apply the approach to the considered scenario of a drone swarm. We consider two cases, the stationary and mobile swarm scenarios.

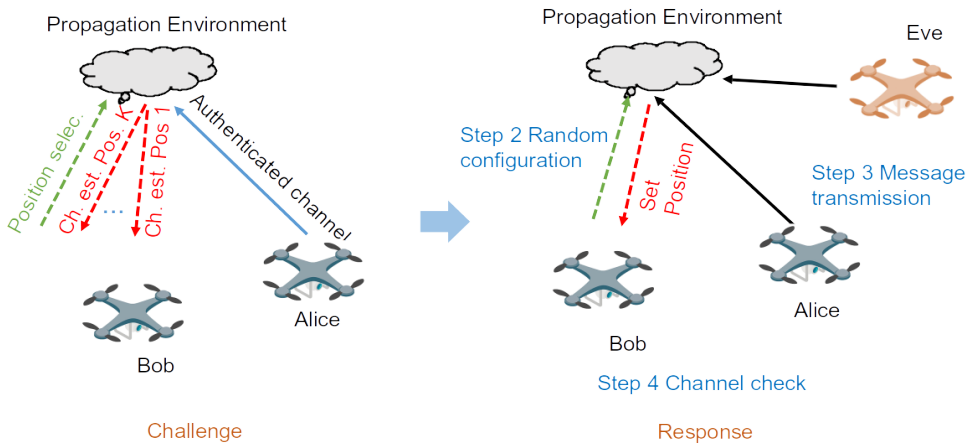

Fig. 1. Proposed CR PLA mechanism.

Stationary Swarm: Bob tells Alice to move in position $\boldsymbol{P}$ while the verifier UAVs do not move, as shown in Fig. 2.a. [1] Given the position $\boldsymbol{P}$, each UAV of the swarm measures a specific channel, which is the answer to the challenge.

Fig. 2 shows the considered scenario, for the case of $K = 1$ (single drone acting as Bob).

Mobile Swarm: given Alice's position, the verifier drones move a pre-determined position (unknown to Eve) to experience a specific channel. This case is shown in Fig. 2.b.

Note that in both cases Bob controls the channel by selecting the position of Alice or Bob: this is the scenario of partially controllable channels of [20]. Moreover, in this preliminary work, we assume that Alice and Bob are able to perfectly control their position in the CR PLA mechanism, while the effects of errors in the positioning on authentication are left for future study.

B. CR Authentication With Stationary Swarm

In this Section, we describe the CR PLA protocol for the stationary swarm. We define $\mathbf{H}_{\boldsymbol{P}}^{(AB)}(t)$ the channel impulse response (CIR) between Alice and Bob at the time t in which Alice is in position $\boldsymbol{P}$ and $\mathbf{H}_{\boldsymbol{P}}^{(AE)}(t)$ and $\mathbf{H}^{(EB)}(t)$ the CIR between Alice and Eve and the CIR between Eve and Bob at the time t, respectively. Let $\mathbf{W}^{(AB)}(t)$ be the estimation error matrix of the channel $\mathbf{H}_{\boldsymbol{P}}^{(AB)}(t)$, $\mathbf{W}^{(EB)}(t)$ the estimation error matrix of the channel $\mathbf{H}^{(EB)}(t)$, and $\mathbf{W}^{(AE)}(t)$ the estimation error matrix of the channel $\mathbf{H}_{\boldsymbol{P}}^{(AE)}(t)$. The CR PLA mechanism comprises the following four steps:

Step 1 (*reference channel acquisition*): In this step Alice moves in several positions known to Bob. For each position, Bob stores the corresponding estimated parameters of his channel to Alice. In this step, we use another authentication mechanism (a key-based cryptography mechanism) to ensure that the estimated channel is truly that relative to Alice (rather than Eve). In general, we assume that after this step Bob can interpolate (or in general predict) the Alice-Bob channel for any position of Alice, even if this position has not been explored in this step. Moreover, such estimates can also be updated as time passes by time-prediction techniques.

Step 2 (*random positioning*): At time t_1, Alice transmits an authentication request to Bob. Bob transmits to Alice the position $\boldsymbol{P}$, at which she has to move. Let $\hat{\boldsymbol{R}}_{\boldsymbol{P}}^{(AB)}(t)$ be these reference estimates of the Alice-Bob channel relative to time t for Alice position $P_{\boldsymbol{P}} \in \mathcal{P}$, where $\mathcal{P}$. This step corresponds to the challenge in cryptography,

Step 3 (*message transmission*): At the time $t_3 = t_2 + t_{shift}$, Alice is in the position $\boldsymbol{P}$, where t_{shift} is the time implied by Alice to move from her initial position to the position $\boldsymbol{P}$. Alice transmits the message, from which Bob estimates, two channels, depending if Alice or Eve is transmitting:

- $\mathcal{H}_0$: packet is from Alice, $\hat{\mathbf{H}}_{\boldsymbol{P}}(t_3) = \mathbf{H}_{\boldsymbol{P}}^{(AB)}(t_3) + \mathbf{W}_2(t_3)$
- $\mathcal{H}_1$: packet is not from Alice, i.e., $\hat{\mathbf{H}}_{\boldsymbol{P}}(t_3) = \mathbf{G}_{\boldsymbol{P}}(t_3) + \mathbf{W}_2(t_3)$,

where $\mathbf{W}_2(t_3) \sim \mathcal{CN}(\mathbf{0}_{N\times N}, \sigma_{t_3,2}^2 \mathbf{I}_{N^2})$ is the noise at the time t_3. The two conditions correspond to the two hypotheses on the received signal, to be checked by Bob.

Step 4 (*channel check*): Bob, helped by other UAVs belonging to the swarm, takes the detection on the authenticity of the message. This is based on the verification that the estimated channel in Step 3 is similar to the reference (predicted) channel $\hat{\boldsymbol{R}}_{\boldsymbol{P}}^{(AB)}(t_3)$. Now, since Bob does not know how Eve will forge the channel (i.e., the value of $\boldsymbol{G}$) he will apply the generalized likelihood ratio test (GLRT) on the received signal. In particular, Bob will compute the log-likelihood

$$\Lambda = \log ||\hat{\boldsymbol{H}}_{\boldsymbol{P}}(t_3) - \boldsymbol{R}_{\boldsymbol{P}}^{(AB)}(t_3)||^2, \tag{1}$$

and decide for $\mathcal{H}_0$ (the message is authentic) if $\Lambda < \tau$, where τ is a suitable threshold.

The overall CR PLA scheme is shown in Fig. 1.

[1] Note that this transmission from Bob to Alice is not authenticated, as we are concerned with the authentication of packets coming from Alice. If Eve transmits a fake packet impersonating Bob, Alice will go to the wrong position and the authentication process does not work, provoking a denial of service, but not an authentication breach.

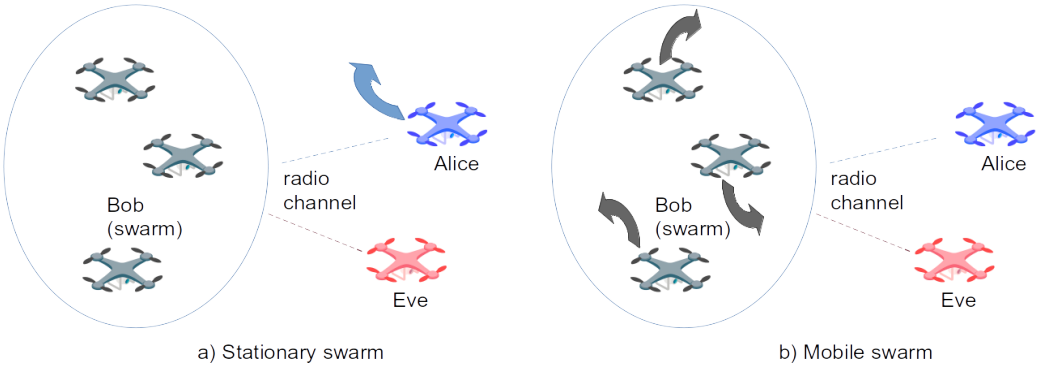

Fig. 2. Scenarios for CR PLA.

Due to the presence of noise, scatters, and interference, no test is immune from errors. The two errors that can occur are the *False Alarm* (FA) when Bob refuses a message coming from Alice and the *Missed Detection* (MD) when Bob accepts a message coming from Eve. The authentication mechanism is said to be *correct* when a message coming from Alice is verified as authentic by Bob and *secure* when a message coming from Eve is deemed non-authentic by Bob. Therefore, a correctness failure happens when we have a FA and a security failure occurs when we have an MD.

On her side, Eve will use the channels $\boldsymbol{H}^{(AE)}(t)$ and $\boldsymbol{H}^{(EB)}(t)$ to infer the Alice-Bob channel $\boldsymbol{R}^{(AB)}(t_3)$ exploiting the spatial correlation of these observations.

C. CR Authentication With Mobile Swarm

In this Section, we describe the CR PLA protocol for the mobile swarm wherein, during the authentication procedure, Alice remains stationary while Bob and other swarm drones move. Also in this case we have the steps of the CR PLA mechanism in the static swarm case, apart from the fact that now in steps 1 and 3 Bob is moving while Alice remains fixed. Moreover, in step 2 now the position of Bob is not communicated to Alice.

The advantage of the mobile swarm case is that Eve does not know the challenge (i.e., the position of Bob) from Bob directly, thus the forge of the channel to break the authentication becomes more challenging. Note however that Eve may know the position of Bob by other means, e.g., using video cameras.

IV. Security Analysis

A. (ϵ, Q)-Security

We now first recall the definition of (ϵ, Q)-secure authentication in cryptography, which will be used to define the security of the new CR PLA mechanism.

In cryptography, CR authentication is performed by letting Bob transmit a challenge x to Alice, who applies on it a message authentication code (MAC) $MAC_{\mathcal{K}}(x)$, generated using a key $\mathcal{K}$ secretly known only by Alice and Bob. Then, Alice transmits the MAC to Bob, who authenticates Alice. Eve intercepts the messages exchanged between Alice and Bob and, upon a new challenge by Bob she forges a fake message (aiming to be the correct response to the challenge) and sends it to Bob to break the authentication procedure.

TABLE I
(ϵ, Q)-Secure Authentication With Cryptographic Authentication and PLA.

	ϵ	Q	Information Avail.
Crypto Auth.	Prob. that Eve succeeds in correctly computing $MAC_{\mathcal{K}}(x)$	Number of other tags that Eve has received.	Both the challenge and the response and exchanged on a public channel.
PLA	Prob. that channel $\boldsymbol{G_P}(t_3)$ is accepted as authentic by Bob.	Number of channel observations $\boldsymbol{H_P}^{(AE)}(t)$ and $\boldsymbol{H}^{(BE)}(t)$.	$\boldsymbol{R_P}^{(AB)}(t_3)$ is only partially predictable by Eve even after authentication.

Definition 1. The cryptographic CR authentication scheme is (ϵ, Q)-secure if, for any attack strategy, the MD probability (i.e., the probability that Eve succeeds in the attack) is ϵ, after Q observed tags by Eve, [23, Sec. 10.2].

The PLA technique proposed in this paper does not completely fit this model. First of all, CR PLA is a keyless approach. Then, the response is not shared on a public channel. In fact, the tag is to the channel between Alice and Bob, $\mathbf{H}^{(AB)}(t)$ and Eve does not see the same channel, as it depends on the drone locations, and Eve's position is different from that of Bob. Therefore, Eve can see a correlated version of $\mathbf{H}^{(AB)}(t)$ with the help of estimates of $\mathbf{H}^{(AE)}(t)$ and $\mathbf{H}^{(EB)}(t)$. In CR PLA, ϵ is still the MD probability while Q is the number of channel measurements that Eve is able to perform. In other words, Q is the number of correlated versions of $\mathbf{H}^{(AB)}(t)$ that Eve owns thanks to the estimates of $\mathbf{H}^{(AE)}(t)$ and $\mathbf{H}^{(EB)}(t)$. The main differences are summarized in Table I.

We are now ready to provide the definition of (ϵ, Q)-security in the PLA context.

Definition 2. A PLA scheme is defined to be unconditionally (ϵ, Q)-secure if the MD probability cannot be larger than ϵ, given that Eve owns at most Q correlated versions of the channel between Alice and Bob, $\mathbf{H}^{(AB)}(t)$.

V. Performance Results

We consider two scenarios: one wherein the positions are taken from a finite discrete set, and the other wherein the challenge channels can be chosen from a continuous set.

A. Discrete Set of Positions

First, consider the case wherein the position $\boldsymbol{P}$ (of either Alice or Bob, in the two scenarios) is taken uniformly at random from a discrete set $\mathcal{P}$ of M positions. Moreover, suppose that Eve knows $\boldsymbol{R}^{(AB)}_{\boldsymbol{P}^*}(t)$ for the single position $\boldsymbol{P}^*$, thus when this position is selected, the MD probability is 1. Eve's information on the Alice-Bob channel is not perfect (and does not improve over time) for any of the other $M-1$ positions: let α be the average MD probability when any other position $\boldsymbol{P}' \in \mathcal{P}$. Now, Bob does not know the position $\boldsymbol{P}^*$ and he selects the position uniformly at random in $\mathcal{P}$ for each message. Then, the MD probability for the CR PLA scheme is

$$\epsilon = \frac{1}{M} + \alpha \frac{M-1}{M}. \tag{2}$$

In this scenario, the CR PLA scheme is, therefore, (ϵ, Q) secure for any Q. Instead, if no CR PLA scheme is used (this is the scenario of [19]) and Alice is in the fixed position $\boldsymbol{P}^*$, the PLA mechanism is totally insecure, since $\epsilon = 1$. Since each movement consumes the energy of its battery, we have to balance the power consumption and small values for ϵ and Q.

Fig. 3 shows ϵ as a function of M for $\alpha = 10^{-1}$, 10^{-2}, and 10^{-3}. As expected from (2), asymptotically (for $M \to \infty$), $\epsilon \to \alpha$, which then establishes a floor in probability. Also, we note that a fairly large number of positions ($M > 10$ or 50) is needed to get close to the asymptotic value.

B. Continuous Set of Positions

In the previous scenario, the MD probability has been set at a fixed value, while in general, it depends also on the number of available positions M: in fact, assuming that a limited space of movements of the drones is available, for a larger M, positions will be closer, yielding a higher MD probability.

For a more realistic analysis, we consider here that each drone is equipped with a single antenna, thus $\boldsymbol{H}^{(AB)}_{\boldsymbol{P}}$ is a vector of K complex numbers. The channel only depends on the distance between the transmitter and the receiver (we ignore shadowing and fading effects), with path-loss exponent 2. We assume that the distance between Alice and Bob can vary (on a horizontal plane) between 1 and 250 m, which (assuming a path-loss with exponent 2) yields a dynamic of 24 dB for each entry of the Alice-Bob channel vector. Thus, Bob can obtain any channel in this range for any of its drones.

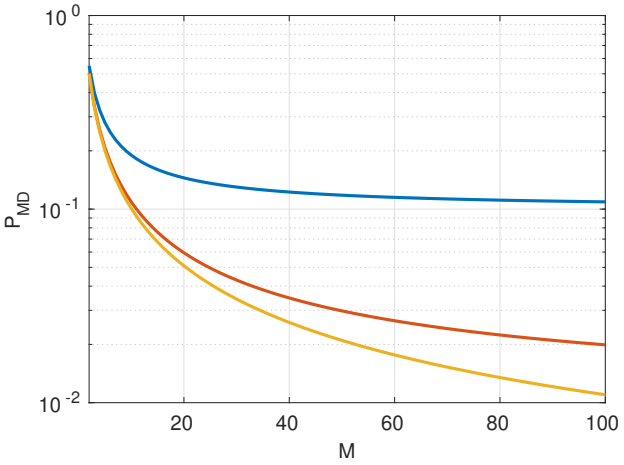

Fig. 3. ϵ as a function of M for $\alpha = 10^{-1}$, 10^{-2}, and 10^{-3}. Note that for a conventional PLA in the same setting, $\epsilon = 1$.

In the considered scenario, using the results of [19], the GLRT (1) becomes

$$2||\hat{\boldsymbol{H}}_{\boldsymbol{P}}(t_3) - \boldsymbol{R}^{(AB)}_{\boldsymbol{P}}(t_3)||^2 < \theta, \tag{3}$$

where we have assumed a noise power of 0 dB. To obtain an FA probability P_{FA}, the value of τ is [19] $\theta = F^{-1}_{\chi^2,2N}(1 - P_{\text{FA}})$, where $F^{-1}_{\chi^2,0}(\cdot)$ is the inverse cumulative distribution function (CDF) of a central chi-square random variable with $2K$ degrees of freedom.

We assume that Eve is able to induce any channel $\hat{\boldsymbol{H}}_{\boldsymbol{P}}(t_3)$ to Bob when performing the attack. Thus, from (3), an MD occurs when the attack channel $\hat{\boldsymbol{H}}_{\boldsymbol{P}}(t_3)$ is inside a $2K$-dimensional hypersphere centered at $\boldsymbol{R}^{(AB)}_{\boldsymbol{P}}(t_3)$ and with radius θ. On the other hand, Bob can choose the entries of $\boldsymbol{R}^{(AB)}_{\boldsymbol{P}}(t_3)$ in a range $[L_{\min}, L_{\max}] = [10^{G_{\min}/20}, 10^{G_{\max}/20}]$, where $G_{\min}$ and $G_{\max}$ are the minimum and maximum channel gains (per entry), respectively. Thus, in a *reference hyper-polyhedron* inside of a hypercube of side $L_{\max}$ but outside of a hypercube of side $L_{\min}$.

Assuming that the positions are chosen such that all the values of the channel entries are selected uniformly in the reference hyper-polyhedron, and that Eve does not know the current challenge, the MD probability at any attack is the ratio between the volumes of the hypersphere and the hyper-polyhedron, i.e., the probability that the attack falls inside a hypersphere positioned at random inside the hyper-polyhedron. In formulas we have the CR PLA is (ϵ, Q)-secure for any Q with

$$\epsilon = \frac{\pi^K \theta^K}{K!} \frac{1}{(L^{2K}_{\max} - L^{2K}_{\min})}, \tag{4}$$

where the first fraction is the volume of the hypersphere and the second fraction is the inverse of the volume of the reference hyper-polyhedron. Note that in this case even if Eve knows which channel should be induced for each position of Alice, as long as Eve does not know the current position, she still

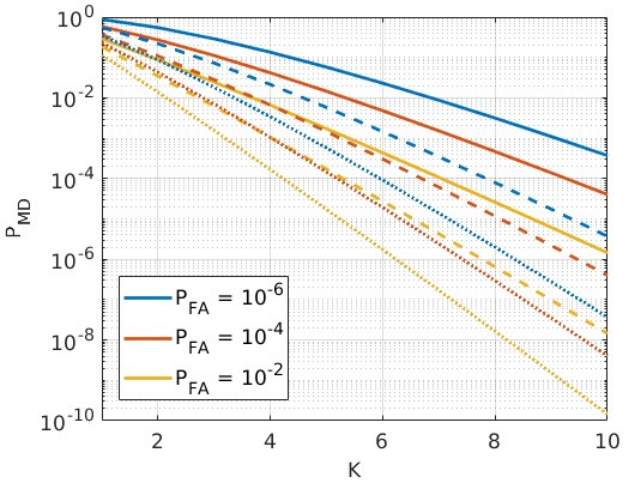

Fig. 4. MD probability (4) as a function of K for $P_{\rm FA} = 10^{-2}$, 10^{-4}, and 10^{-6}, $G_{\rm min} = 0$ dB, and $G_{\rm max} = 20$ (solid lines), 22 (dashed lines), and 24 dB (dotted lines). Note that for a conventional PLA in the same setting, $\epsilon = 1$.

has the uncertainty about where the hypersphere is, and the MD probability will always (irrespective of the attack number) be (4). Fig. 4 shows that MD probability (4) as a function of K for $P_{\rm FA} = 10^{-2}$, 10^{-4}, and 10^{-6}, $G_{\rm min} = 0$ dB, and $G_{\rm max} = 20$, 22, and 24 dB, which correspond to a maximum distance between Alice and Bob of 100, 160, and 250 m. We note a sharp decrease of the MD probability with K, and that a higher target FA probability yields a lower MD probability.

Also, note that if Eve knows the challenge position at each attack and she also knows when an attack is successful, she can store the list of positions and corresponding attacks, as in a cryptographic-based CR system where both the challenge and the response are public. The MD probability of Fig. 3 can then be red as the reciprocal of the number of challenges made available by the CR PLA procedure, and we see that the range is between 10^2 to 10^{10}, which provides a fairly large amount of challenges.

VI. Conclusion

We have introduced an authentication mechanism for communications among drones in a swarm, based on the characteristics of the physical communication channel and on the position of the drones. This mechanism implements a CR authentication mechanism at the physical layer, exploiting the partial controllability of the communication channel. Two cases are considered (where either Alice or Bob moves in the challenge step) and an analysis of the (ϵ, Q)-security is proposed. Preliminary numerical results show that the proposed approach makes the authentication process more accurate than the state-of-the-art PLA mechanism.

References

[1] X. Lin, S. Rommer, S. Euler, E. A. Yavuz, and R. S. Karlsson, "5G from space: An overview of 3GPP non-terrestrial networks," *IEEE Communications Standards Magazine*, vol. 5, no. 4, pp. 147–153, 2021.

[2] W. Zafar and B. Muhammad Khan, "Flying ad-hoc networks: Technological and social implications," *IEEE Technology and Society Magazine*, vol. 35, no. 2, pp. 67–74, 2016.

[3] M. Alam, N. Ahmed, R. Matam, and F. A. Barbhuiya, "IEEE 802.11ah-enabled Internet of drone architecture," *IEEE Internet of Things Magazine*, vol. 5, no. 1, pp. 174–178, 2022.

[4] Y. Zou, J. Zhu, T. Wu, H. Guo, and H. Wei, "Cooperative drone communications for space-air-ground integrated networks," *IEEE Network*, vol. 35, no. 5, pp. 100–106, 2021.

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

[6] G. Michieletto, F. Formaggio, A. Cenedese, and S. Tomasin, "Robust localization for secure navigation of UAV formations under GNSS spoofing attack," *IEEE Transactions on Automation Science and Engineering*, pp. 1–14, 2022.

[7] V. Hassija, V. Chamola, A. Agrawal, A. Goyal, N. C. Luong, D. Niyato, F. R. Yu, and M. Guizani, "Fast, reliable, and secure drone communication: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 4, pp. 2802–2832, 2021.

[8] Y. Aydin, G. K. Kurt, E. Ozdemir, and H. Yanikomeroglu, "Authentication and handover challenges and methods for drone swarms," *IEEE Journal of Radio Frequency Identification*, vol. 6, pp. 220–228, 2022.

[9] ——, "Group authentication for drone swarms," in *Proc. IEEE International Conference on Wireless for Space and Extreme Environments (WiSEE)*, 2021, pp. 72–77.

[10] M. A. Abdel-Malek, K. Akkaya, A. Bhuyan, and A. S. Ibrahim, "A proxy signature-based swarm drone authentication with leader selection in 5G networks," *IEEE Access*, vol. 10, pp. 57 485–57 498, 2022.

[11] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, H. Karimipour, G. Srivastava, and M. Aledhari, "Enabling drones in the Internet of Things with decentralized blockchain-based security," *IEEE Internet of Things Journal*, vol. 8, no. 8, pp. 6406–6415, 2021.

[12] C. Pu, A. Wall, K.-K. R. Choo, I. Ahmed, and S. Lim, "A lightweight and privacy-preserving mutual authentication and key agreement protocol for internet of drones environment," *IEEE Internet of Things Journal*, vol. 9, no. 12, pp. 9918–9933, 2022.

[13] K. Lounis, S. H. H. Ding, and M. Zulkernine, "D2D-MAP: A drone to drone authentication protocol using physical unclonable functions," *IEEE Transactions on Vehicular Technology*, pp. 1–16, 2022.

[14] G. Bansal and B. Sikdar, "Fault resilient authentication architecture for drone networks," in *Proc. IEEE International Conference on Communications Workshops (ICC Workshops)*, 2022, pp. 866–871.

[15] M. Mitev, M. Shakiba-Herfeh, A. Chorti, M. Reed, and S. Baghaee, "A physical layer, zero-round-trip-time, multifactor authentication protocol," *IEEE Access*, vol. 10, pp. 74 555–74 571, 2022.

[16] 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, 2015.

[17] H. Wang, H. Fang, and X. Wang, "Edge intelligence enabled soft decentralized authentication in UAV swarm," in *Proc. IEEE/CIC International Conference on Communications in China (ICCC)*, 2021, pp. 86–91.

[18] ——, "Safeguarding cluster heads in UAV swarm using edge intelligence: Linear discriminant analysis-based cross-layer authentication," *IEEE Open Journal of the Communications Society*, vol. 2, pp. 1298–1309, 2021.

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

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

[21] D. Shan, K. Zeng, W. Xiang, P. Richardson, and Y. Dong, "PHY-CRAM: Physical layer challenge-response authentication mechanism for wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 1817–1827, 2013.

[22] P. Kushwaha, H. Sonkar, F. Altaf, and S. Maity, "A brief survey of challenge–response authentication mechanisms," in *ICT Analysis and Applications*. Springer, 2021, pp. 573–581.

[23] D. R. Stinson and M. B. Paterson, *Cryptography: theory and practice*, 4th ed. Boca Raton: CRC Press, 2019.