Analysis of Channel-Based User Authentication by Key-Less and Key-Based Approaches

Stefano Tomasin, *Senior Member, IEEE*

***Abstract*— User authentication (UA) supports the receiver in deciding whether a message comes from either the claimed transmitter or an impersonating attacker. Information-theoretically secure authentication can be implemented by using either a secret (symmetric key) shared between both the legitimate users or the transmission medium over which the message is transmitted [physical-layer authentication (PLA)]. We analyze these solutions when the physical-layer channel is the unique randomness source for either generating the key or performing PLA. For the symmetric-key-based UA approach, we resort to a secret key agreement. Moreover, we also consider an asymmetric-key-based UA based on the public-key (proven to be *semantically secure*), where the channel is used as an entropy source at one device only. We define the *secure authentication rate* at which the probability that the UA attack succeeds goes to zero as the number of independent and identically distributed variables describing how the channel goes to infinity. Both passive and active attacks are considered, and by numerical results, we compare the various UA schemes.**

***Index Terms*— Physical layer authentication, physical layer security, Rayleigh fading, user authentication.**

I. Introduction

USER AUTHENTICATION (UA) methods in communication systems are used to confirm the identity of a message sender [1]. In particular, the receiver must take a decision on who has transmitted the message considering that an attacker aims at impersonating the legitimate transmitter. Typically, UA includes two phases: an *identification association (ID-A)* phase, when the legitimate transmitter is assigned an identifying feature using an authenticated channel, and an *identification verification (ID-V)* phase, when the identifying feature is verified upon message reception.

Focusing on information theoretically secure (ITS) schemes, many commonly-used UA protocols use a key as identifying feature, i.e., a secret known by both the transmitter and the receiver (symmetric key), and encryption techniques are adopted in the ID-V phase: these methods go also under the name of key-based user authentications (UAs) [2], [3]. An alternative key-less approach is the physical layer authentication (PLA) [4], [5], wherein the identifying feature is the physical channel over which the communication occurs. In this case the ID-A phase consists in the identification of the channel features, while the ID-V phase consists in checking if the received message has undergone the same channel of the ID-A phase, including for example wireless channels (see [4], [6]–[8], [9] for a survey) or biometric [10], [11] features. For example, in wireless systems, propagation phenomena (e.g., fading) are associated to the specific device position, thus the attacker should be in the same location of the legitimate transmitter for a successful impersonation. PLA has been studied for discrete memory-less channels in [12]; implementations for multiple-input multiple-output (MIMO) and intersymbol-interference channels have been proposed in [6] and [13], while a game-theoretic study of PLA has appeared in [14]. Recently, a review of key-based and key-less security approaches with a comparison between cryptographic UA and PLA has been proposed in [15]. In [12] the key-less UA was studied in a new noisy scenario, where in addition to discrete memoryless channels among users, an insecure noiseless channel between the legitimate parties is available. The scheme optimality was further proved in [16]. In [17] encryption techniques are mixed with ITS solutions by adding artificial noise on top of a message authentication code. An alternative solution, similar to key-based approaches implemented at the physical layer, provides the transmission of an authentication tag superimposed to the information signal [18].

In both key-based and key-less approaches a source of randomness (secret to Eve) is needed to either generate the keys or identify the channel features. While for PLA the source of randomness is the channel, for key-based approaches various sources can be considered. When the key is extracted from the channel a secret key agreement (SKA) procedure can be used [19]–[21], which has been advocated also for current WiFi and cellular systems [22]. Various channel features have been exploited for the extraction of the secret randomness, including multiple antenna channels [23], [24], orthogonal frequency division multiplexing (OFDM) systems [6], power spectral densities [25], time-varying channel features [26], and channel impulse response [27].

In this paper we aim at comparing the ITS key-based and key-less authentication approaches using as unique common randomness source the physical channel. For a more complete analysis we also consider asymmetric-key UAs, also named public-key systems, which however are *semantically-secure* rather than ITS [19]. In this case a user generates the private/public key couple still exploiting the channel as unique

Manuscript received July 14, 2017; revised January 4, 2018 and April 17, 2018; accepted June 11, 2018. Date of publication June 26, 2018; date of current version September 10, 2018. The associate editor coordinating the review of this paper and approving it for publication was T. Q. Duong.

The author is with the Department of Information Engineering, University of Padova, 35122 Padua, Italy, and also with the Consorzio Nazionale Interuniversitario per le Telecomunicazioni, Padova Research Unit, 43124 Padua, Italy (e-mail: tomasin@dei.unipd.it).

Digital Object Identifier 10.1109/TWC.2018.2848937

source of randomness, which is a pessimistic assumption, as other sources could be readily available to a single user. However, we restrict to this case to have a common basis of comparison. A first analysis of all these schemes has been proposed in [28] but limited to channels described by a finite number of discrete random variables. Here instead we focus on the asymptotic case where each channel is described by an infinite number of independent and identically distributed (i.i.d.) continuous random variables, modeling for example a narrowband massive-MIMO or a wideband OFDM channel. Leveraging the secrecy of the UA protocols as long as the shared key remains secret, we focus here on an attack wherein Eve only attempts to discover the key by observing her own channel to both Alice and Bob. Seeing UA as a hypothesis testing problem, we adopt the type-I and type-II error probabilities as correctness and security metrics, which correspond to the probabilities of rejecting an authentic message and accepting a non-authentic message, respectively. A similar approach for the analysis of UA solutions has been taken for example in [2], [6], [29], and [30]. The contributions of the paper are, for all the considered UA schemes:

- the proof of correctness, i.e., authentic messages are always accepted;
- the derivation of the secure authentication rate (SAR), a security metric that dictates the rate at which the probability of successful attack (type-II error) goes to zero as the number of variables describing the channel goes to infinity;
- the derivation of SAR expressions for time-invariant channels, time-variant channels and Rayleigh fading channels with additive white Gaussian noise (AWGN);
- the analysis of active attacks aiming at disrupting the ID-A phase in order to ease the impersonation attack in the ID-V phase;
- the evaluation of both optimal Eve's attack and a simple approach wherein she first performs a linear combination of all channel estimates to obtain the minimum mean square error (MMSE) linear estimate of the legitimate channel and then uses it for the attack.

By simulations we closely compare the various systems, highlighting their potentials and vulnerabilities. Note that the practical implementation of the various schemes is out of the scope of this work, that considers only an asymptotic scenario. When practical schemes are deployed, other metrics such as the computational complexity may also be considered to complete the picture.

The rest of the paper is organized as follows. Section II introduces the system model, with emphasis on both the channel and the considered schemes. The analysis of the protocols in terms of SAR is performed in Section III, while its derivation for the relevant case of reciprocal Rayleigh fading AWGN channels is discussed in Section IV. Section V proposes a simple attack scheme based on a linear processing of the channel estimates. Active attacks during the ID-A phase are discussed in Section VI. Numerical results comparing the various strategies are presented in Section VII, before the main conclusions are outlined in Section VIII.

Notation: $\mathbb{P}[\mathcal{X}]$ denotes the probability of the event $\mathcal{X}$. $\mathbb{E}[x]$ denotes the expectation of the random variable x, $\mathbb{H}(x)$ denotes the entropy of the discrete random variable x and $\bar{\mathbb{H}}(x)$ denotes the differential entropy of the continuous random variable x. $\mathbb{I}(x;y)$ denotes the mutual information between random variables x and y. $\mathbb{D}(p||q)$ denotes the Kullback-Leibler (KL) divergence between the two probability density functions (PDFs) p and q. Vectors are denoted in boldface, while scalar quantities are denoted in italic. $\log x$ and $\ln x$ denote the base-2 and natural logarithms of x, respectively. $\det \boldsymbol{A}$ and $\mathrm{tr}\boldsymbol{A}$ denote the determinant and trace of matrix $\boldsymbol{A}$, respectively. $\boldsymbol{A}^T$ denotes the transpose of matrix $\boldsymbol{A}$. $p_x(a)$ denotes the PDF of the random variable x.

II. System Model

We consider a communication system with two legitimate users, Alice and Bob, and one attacker Eve. Time is divided into frames, each of the same duration. In order to simplify the analysis we suppose that in even and odd frames Alice and Bob alternate their transmissions. In particular, starting from the first frame and in all odd frames $2t+1$ ($t = 0, \ldots$) Alice transmits to Bob, while starting from the second frame and in all even frames $2t$ ($t = 1, \ldots$) Bob transmits to Alice. Eve can transmit at any frame. All transmissions include pilot symbols known to all users (including Eve) for channel estimation.

Bob must decide if messages received in odd frames are coming from either Alice or Eve. To this end, the two initial frames are used for ID-A purposes, extracting keys from the channel or identifying reference channel features as described in the following. In forthcoming frames Bob receives messages and performs ID-V, i.e., he decides if they are coming from Alice (hypothesis $\mathcal{H}_0$) or not (hypothesis $\mathcal{H}_1$).[1]

We consider block-fading channels, where channels between each users' couple are assumed to be time-invariant within each frame, while may vary among different frames, in particular we focus on a) time-invariant channels, that remain constant even across frames, and b) time-varying channels that change across frames while being correlated. Each channel within one frame is described by n random variables, modeling for example a narrowband MIMO or single-input-single-output wideband OFDM system. We further assume that the n random variables are i.i.d. with frame-dependent PDF. The k-th random variable in the set of the n random variables of the channel estimated by Bob at frame $2t+1$ is denoted as $x_k(2t{+}1)$, while any random variable of the channel estimated by Alice in frame $2t$ is denoted as $y_k(2t)$. The set of n random variables $x_k(2t+1)$ and $y_k(2t)$ for $k = 1, \ldots, n$ form the random vectors $\boldsymbol{x}(2t+1)$ and $\boldsymbol{y}(2t)$, respectively. Similarly, let $v_{\mathrm{A},k}(2t+1)$ and $v_{\mathrm{B},k}(2t)$ be the k-th random variables of the estimated channels by Eve when either Alice or Bob are transmitting, respectively. Eve will exploit these estimates to perform her attacks. We also define the $2t$-size row vector

$$\boldsymbol{z}_k(2t) = [v_{\mathrm{A},k}(1), v_{\mathrm{B},k}(2), \ldots, v_{\mathrm{A},k}(2t-1), v_{\mathrm{B},k}(2t)] \quad (1)$$

[1] Note that we focus on the case wherein the ID-V phase is performed only once, thus not addressing the problem of key re-use or renewal.

and the $n \times 2t$ matrix $\boldsymbol{z}(2t) = [\boldsymbol{z}_1^T(2t), \dots, \boldsymbol{z}_n^T(2t)]^T$. Let $p_{x_k(t)}(a)$, $a \in \mathbb{C}$ be the frame-dependent PDF of $x_k(t)$ and a similar notation is adopted for the other variables.

We consider three UA approaches: asymmetric channel-based cryptographic authentication (A-CBCA), symmetric channel-based cryptographic authentication (S-CBCA) and physical layer authentication (PLA). In order to obtain a fair comparison of the three approaches, we extract the secret needed for both A-CBCA and S-CBCA from the channel, so that all three schemes have the same unique source of randomness. In key-based approaches the keys are used to perform authentication by cryptographic algorithms. While ITS authentication can be achieved for both S-CBCA [2] and PLA [6], the availability of the public key in A-CBCA does not provide an advantage to the legitimate parties, and cannot be used to obtain ITS authentication [31]. Therefore, we resort to *semantically secure* schemes instead, that have the strongest security within the computational security schemes. Moreover, since an ITS scheme is also semantically secure, we will conclude that all considered schemes achieve semantic security. With this clarification in mind, schemes are assumed to be secure (either semantically or information-theoretically), as long as the keys remain secret. Therefore, Eve only attempts to discover the key by observing her own channel to both Alice and Bob.

Moreover, both Alice and Bob must be able to exchange authenticated messages in the ID-A phase, to ensure that they are talking to each other, and not to Eve. This is a common feature to all UA protocols and we take it for granted. The authenticated channel can be obtained for example when devices are in a protected location immune from attacks. Also, the authenticated channel is available when the keys used for authentication must be renewed, but we can still use the old keys in the ID-A phase.

We now detail the UA procedures for the three authentication approaches.

A. ACBCA

The basic structure of the A-CBCA can be summarized as follows.

ID-A Phase: The following operations are performed:

1) Alice uses the n-size channel vector estimate as a source of n random variables according to their distribution (e.g., Gaussian).
2) These variables are mapped into n uniform random variables using either source coding or randomness extraction [32] techniques, followed by privacy amplification (in order to make the resulting variables secret to Eve). The uniform random variables are defined over a finite alphabet with cardinality detailed in the following Section.
3) The secret bit sequence is mapped into the private/public key couple. For example, when using the Rivest-Shamir-Adeleman (RSA) algorithm with optimal asymmetric encryption padding (OAEP), that has been proven to be semantically secure [19], the secret bits can be used to index both two prime numbers (in RSA for the generation of the private/public key couple) and random numbers needed in OAEP.
4) Alice transmits the public key to Bob over an authenticated channel.

ID-V Phase: Alice adds a signature to her message and encrypts the whole packet with her private key. Bob decrypts the received packet with the public key and checks the signature. If the signature is correct the message is accepted as authentic, otherwise is discarded as non-authentic.

Suitable variants of this scheme have been proposed to prevent various attacks (including the replay attack) and are out the scope of this paper. Note that for A-CBCA other secret sources of randomness (rather than the channel) available to Alice can be used for generating the keys, further enhancing the performance. However, for the sake of a fair comparison with the other authentication schemes we assume that only $\boldsymbol{y}(2)$ is used as source of secret (to Eve) randomness by Alice. Point 2 of the ID-A phase can be performed similarly to the source-based SKA procedure [33], where in this case the secret bits are generated at a single terminal (or in other words both SKA parties observe exactly the same source of randomness).

B. SCBCA

The basic structure of the S-CBCA scheme can be summarized as follows.

ID-A Phase: Alice and Bob share a secret key. The key is obtained from the channel through the SKA protocol [33] applied on the physical channel and using an authenticated error-free public channel. In particular, in the first two frames Alice and Bob estimate their channels and perform the key reconciliation and privacy amplification over the public channel.

ID-V Phase: Alice generates a tag from the message and the secret key and sends both the tag and the message to Bob. Bob generates the same tag from the received message and his key, and compares it with the received tag. If the received tag and the locally generated tag coincide, the message is considered authentic.

For the generation of the tag, we can use Wegman-Carter authentication scheme [34] which has been proved to be ITS. In this case for the i-th message m_i, the tag generated by Alice is

$$\mathcal{T}(m_i) = \mathcal{H}(m_i) + \mathcal{F}(i) \bmod \mu, \tag{2}$$

where μ is a positive integer, $\mathcal{H}$ is a hash function from a properly designed hash functions family, and $\mathcal{F}$ produces a random output from each different input. The secret key $(\mathcal{H}, \mathcal{F})$ is shared between Alice and Bob.

By concatenating ITS authentication and SKA by the composition theorem we obtain a ITS scheme.

C. PLA

With PLA the authentication is provided directly by the physical channel over which the communication occurs [6]. The PLA algorithm works as follows.

ID-A Phase: At frame 1, Bob obtains estimate $\boldsymbol{x}(1)$ of his channel to Alice using an authenticated message, so that he is sure that the estimated channel is connecting him to Alice (rather than Eve).

ID-V Phase: At frames $2t+1$ with $t>0$, whenever Bob receives a message, he decides that it comes from Alice if the estimated channel $\boldsymbol{x}(2t+1)$ is similar to $\boldsymbol{x}(1)$, using a hypothesis testing strategy. In particular, as described in more details in [6] and [29], Bob computes the log likelihood ratio (LLR) of the observed channel in the two hypotheses

$$\Lambda(2t+1) = \log \frac{\mathbb{P}[\boldsymbol{x}(2t+1)|\mathcal{H}_0, \boldsymbol{x}(1)]}{\mathbb{P}[\boldsymbol{x}(2t+1)|\mathcal{H}_1, \boldsymbol{x}(1)]} \tag{3}$$

and compares it with a suitable threshold θ: $\mathcal{H}_0$ is decided if $\Lambda(2t+1) > \theta$, otherwise the decision is for the hypothesis $\mathcal{H}_1$.

Note that a variant of this scheme provides that whenever a new message is authenticated, the new channel estimate is used as a reference for the comparison of forthcoming channel estimates (thus replacing $\boldsymbol{x}(1)$). By this approach, that we denote as *differential PLA*, Bob can better track channel variations.

III. Protocols Analysis With ID-V Attacks

In this section we consider the attacks in the ID-V phase, while attacks in the ID-A phase will be considered in Section VI. In general, a UA protocol is a) correct when a message coming from Alice is verified as authentic by Bob and b) secure when a message coming from Eve is dismissed as non-authentic by Bob. We assess the correctness and security (in either information-theoretical or semantic sense) of each UA protocol.

Let $\boldsymbol{K}(n)$ be either the key used for key-based UA or the set of features used for PLA: since we assume that the n channel realizations are i.i.d., the length of $\boldsymbol{K}(n)$ can grow linearly with n. We aim at establishing the protocols' correctness and security asymptotically, as the number of variables per frame describing the channel n goes to infinity.

We observe that UA is a hypothesis testing problem, that does not necessarily always provide correctness and security. In particular, on the one hand a correctness failure occurs when an authentic message is rejected as non-authentic, which is a type-I error in the hypothesis testing framework. On the other hand, a security failure occurs when a non-authentic message is accepted as authentic, which is a type-II error in the hypothesis test. The type-I error corresponds to the event of not having the same key in the S-CBCA or not recognizing the authentic channel in PLA, while it is absent in A-CBCA (as we assume that the public key is correctly known by everyone). The type-II error corresponds to a successful attack by Eve, i.e., her ability of forging an authenticated message inferring the secret between Alice and Bob.

We first show that as $n \to \infty$ the type-I error probability is vanishing with n; moreover, the probability of successful attack (PSA) by Eve (type-II error probability) $P_s(t)$ is exponentially decaying with n. As a metric for the comparison of the various approaches we consider the SAR (in bit/channel resource), defined as the number of *secret bits in $\boldsymbol{K}(n)$ per random variable* at frame t, i.e.,

$$R(t) = \lim_{n\to\infty} -\frac{1}{n}\log P_s(t). \tag{4}$$

In the following we derive the maximum SAR for each UA protocol. We consider attacks at odd frames, starting from frame $t=3$, after Eve has collected an even number of channel observations.

Remark 1: Note that PLA depends on the frame index t since Eve collects channel estimates at each frame, thus being able to progressively refine her knowledge of the Alice-Bob channel.

Remark 2: Note that as $n \to \infty$ we have an infinite number of bits available in the first two frames, even for time-invariant channels.

A. S-CBCA

We establish the correctness and security of the S-CBCA protocol by the following Theorem.

Theorem 1: As $n \to \infty$, the S-CBCA protocol is correct and the SAR for frame $2t+1$, with $t \geq 1$ is

$$R_{\text{S-CBCA}}(2t+1) = C_{\text{SKA}}(2t+1), \tag{5}$$

where $C_{SKA}(2t+1)$ is the *weak secret-key capacity* of the SKA process between Alice and Bob, given the channel knowledge by Eve at frame $2t$.

Proof: S-CBCA is proved to be correct and ITS [1] provided that the key is secret. About correctness, asymptotically SKA ensures that Alice and Bob have the same key, as long as the secret key rate $R_{\text{SKA}}(2t+1)$ satisfies $R_{\text{SKA}}(2t+1) \leq C_{\text{SKA}}(2t+1)$.

About security, the length of the secret key (in bits) grows as $nR_{\text{SKA}}(2t+1)$. Therefore, we have

$$P_s(t) \approx 2^{-nR_{\text{SKA}}(2t+1)}, \tag{6}$$

from (4) the maximum value of $R_{\text{SKA}}(2t+1)$ is $C_{\text{SKA}}(2t+1)$ and we obtain (5). ■

We recall that the secret key capacity for the source-model SKA is not known in closed form, but is bounded as

$$\begin{aligned}\mathbb{I}(x_k(1); y_k(2)) - \min\{\mathbb{I}(x_k(1); \boldsymbol{z}_k(2t)), \mathbb{I}(y_k(2); \boldsymbol{z}_k(2t))\}\\ \leq C_{SKA}(2t+1)\\ \leq \min\{\mathbb{I}(x_k(1); y_k(2)), \mathbb{I}(x_k(1); y_k(2)|\boldsymbol{z}_k(2t))\},\end{aligned} \tag{7}$$

since the two channel estimates used for SKA are $\boldsymbol{x}(1)$ and $\boldsymbol{y}(2)$ and the information on the channel available at Eve at frame $2t+1$ is $\boldsymbol{z}(2t)$.

Note that results reported for S-CBCA hold for channels described by both continuous and discrete random variables, using the respective definitions of mutual information. The SAR obtained for continuous random variables is an upper bound of the SAR obtained for the corresponding quantized channel.

B. A-CBCA

For A-CBCA we first consider the case wherein the channel estimates are discrete random variables. This occurs for example if Alice quantizes $y_k(2)$ into $\langle y_k(2)\rangle \in \mathcal{A}$, where $\mathcal{A} = \{a_0, \dots, a_{M-1}\}$ is an M-size quantization alphabet. The secret random number used for the private/public key generation is then extracted from $\langle y_k(2)\rangle$. Note that as already observed, the extraction of the secret random number can be seen as a special case of SKA, providing a uniformly random number in the $2^{nR_{\text{A-CBCA}}}$ set, irrespective of the channel statistics.

Theorem 2: The A-CBCA scheme with randomness extracted from the channel is correct and for quantized channel estimates $\langle y_k(2)\rangle$, as $n \to \infty$ its SAR at frame $2t+1$, with $t \geq 1$ is

$$R_{\text{A}-\text{CBCA}}(2t+1) = \mathbb{H}(\langle y_k(2)\rangle | \boldsymbol{z}_k(2t)), \tag{8}$$

where $\mathbb{H}(\cdot|\cdot)$ is the conditional entropy.

Proof: The correctness of the A-CBCA scheme follows immediately by the assumption that the public-key broadcast channel is error-free and authenticated.

About security, the A-CBCA protocol extracts randomness from the channel which is secret to Eve, and can be seen as a source-based SKA protocol where both Alice and Bob observe the same source of randomness, thus being ITS, which implies semantic security. The public-key protocol can be made semantically secure, therefore, the global scheme is semantically secure. In this case the SKA capacity upper bound becomes

$$\begin{aligned}&\min\{\mathbb{I}(\langle y_k(2)\rangle; \langle y_k(2)\rangle), \mathbb{I}(\langle y_k(2)\rangle; \langle y_k(2)\rangle | \boldsymbol{z}(2t))\}\\ &\quad = \mathbb{I}(\langle y_k(2)\rangle; \langle y_k(2)\rangle | \boldsymbol{z}_k(2t)) = \mathbb{H}(\langle y_k(2)\rangle | \boldsymbol{z}_k(2t)),\end{aligned} \tag{9}$$

which coincides with the lower bound

$$\begin{aligned}&\mathbb{I}(\langle y_k(2)\rangle; \langle y_k(2)\rangle) - \mathbb{I}(\langle y_k(2)\rangle; \boldsymbol{z}_k(2t))\\ &\quad = \mathbb{H}(\langle y_k(2)\rangle) - \mathbb{H}(\langle y_k(2)\rangle) + \mathbb{H}(\langle y_k(2)\rangle | \boldsymbol{z}_k(2t)),\end{aligned} \tag{10}$$

providing (8). ■

For the channel quantization case a lower bound on SAR is obtained as follows

$$\begin{aligned}&R_{\text{A}-\text{CBCA}}(2t+1)\\ &\quad = \mathbb{H}(\langle y_k(2)\rangle) - \mathbb{I}(\langle y_k(2)\rangle; \boldsymbol{z}_k(2t))\\ &\quad \geq \max\{0, \mathbb{H}(\langle y_k(2)\rangle) - \mathbb{I}(y_k(2); \boldsymbol{z}({}_k 2t))\},\end{aligned} \tag{11}$$

where the first line is obtained by the definition of mutual information and the second line by the data processing inequality, where we upper-bounded the mutual information between $\boldsymbol{z}_k(2t)$ and the quantized variable by the mutual information between $\boldsymbol{z}_k(2t)$ and the continuous random variables describing the channel estimate.

Now, we consider the case wherein the channel is a continuous random variable, for which the SAR is established by the following Lemma.

Lemma 1: For continuous channel estimates at Alice (i.e., $\boldsymbol{y}(2)$ is a continuous random vector), the SAR is

$$R_{\text{A}-\text{CBCA}}(2t+1) = \infty. \tag{12}$$

Proof: We first observe that the conditional entropy in (8) can be written by definition as the $2t$-dimensional integral

$$\mathbb{H}(\langle y_k(2)\rangle | \boldsymbol{z}_k(2t)) = \int \mathbb{H}(\langle y_k(2)\rangle | \boldsymbol{z}_k(2t) = \boldsymbol{b}) p_{\boldsymbol{z}_k(2t)}(\boldsymbol{b}) \mathrm{d}\boldsymbol{b}, \tag{13}$$

where in the argument of the integral we have the entropy of $\langle y_k(2)\rangle$ conditioned to $\boldsymbol{z}_k(2t) = \boldsymbol{b}$, the integration vector. Now, the continuous random variable $y_k(2)$ is the asymptotic case of the quantized variable $\langle y_k(2)\rangle$ with a number of quantization points $M \to \infty$. Asymptotically, the conditional entropy for each value of $\boldsymbol{z}_k(2t)$ is the *limiting density of discrete points* which tends to infinity logarithmically with M under very mild assumptions [35]. Therefore, the average of the logarithm, which corresponds to the conditional entropy tends to infinity, i.e.,

$$\lim_{M\to\infty} \mathbb{H}(\langle y_k(2)\rangle | \boldsymbol{z}_k(2t)) = \infty, \tag{14}$$

providing (12). ■

Note that in practice a continuous channel estimate is not available at Alice, since radio frequency chain has a finite dynamic range and the continuous value is converted into a discrete value through a quantizer with a finite number of bits. Therefore, the continuous channel estimate represents an asymptotic scenario.

C. PLA

We establish the correctness and security of PLA by the following Theorem.

Theorem 3: The PLA protocol is asymptotically correct, and as $n \to \infty$ its SAR at frame $2t+1$, with $t \geq 1$, is

$$R_{\text{PLA}}(2t+1) = \mathbb{D}(p_{x_k(1),x_k(2t+1)|\mathcal{H}_0} || p_{x_k(1),x_k(2t+1)|\mathcal{H}_1}), \tag{15}$$

where $p_{x_k(1),x_k(2t+1)|\mathcal{H}_0}$ and $p_{x_k(1),x_k(2t+1)|\mathcal{H}_1}$ are the joint PDFs of $x_k(1)$ and $x_k(2t+1)$ when Alice and Eve are transmitting, respectively, at frame $2t+1$ of the ID-V phase.

Proof: About correctness, using the Chernoff-Stein Lemma [36, Th. 11.8.3] we have that for $n \to \infty$ the probability of correctly authenticating messages coming from Alice can be made arbitrarily small.

Information-theoretic security is proven in [6] and [29], and still from the Chernoff-Stein Lemma [36, Th. 11.8.3] the PSA goes to zero as

$$P_s \sim 2^{-n\mathbb{D}(p_{x_k(1),x_k(2t+1)|\mathcal{H}_0} || p_{x_k(1),x_k(2t+1)|\mathcal{H}_1})}, \tag{16}$$

which directly provides (15). ■

Note that the SAR depends on the attack that Eve is performing through $p_{x_k(1),x_k(2t+1)|\mathcal{H}_1}$. Therefore, it is interesting to study a specific attack, as in the following Lemma.

Lemma 2: If Eve is able to induce any channel estimate $\boldsymbol{x}(2t+1)$ to Bob when attacking, and assuming that Eve generates the induced estimate randomly distributed according to the PDF of the legitimate channel given Eve's observations, $p_{x_k(2t+1)|\boldsymbol{z}_k(2t),\mathcal{H}_0}$, then the SAR is upper-bounded by

$$R_{\text{PLA}}(2t+1) \leq \mathbb{I}(x_k(1); x_k(2t+1) | \mathcal{H}_0, \boldsymbol{z}_k(2t)). \tag{17}$$

Proof: See Appendix A. ■

From this lemma we observe that if the statistics of the estimated channels at both Alice and Bob are the same ($p_{x_k(2t+1)}(a) = p_{y_k(2t)}(a)$) then $R_{\rm PLA}(2t+1) \leq \mathbb{I}(x_k(1); y_k(2)|\boldsymbol{z}_k(2t))$, i.e., the PLA has the same upper-bound of S-CBCA.

Note again that results reported for PLA hold for channels described by both continuous and discrete random variables. Also in this case, the SAR obtained for continuous random variables is an upper bound of the SAR obtained for the corresponding quantized channel.

Remark 1: The assumption that Eve can induce a channel that depends on her instantaneous channel does not hold for time-varying channels since Eve does not know exactly her channel to Bob. Therefore, our assumption is conservative and the obtained SAR is a lower bound on the effective SAR. Moreover, for PLA the time-varying channel scenario is particularly challenging, since the variations decrease the ability of the receiver to identify the channel in the ID-V phase. In other words, SAR will decrease over time for PLA and in particular, as $t \to \infty$ the KL divergence will tend to zero, thus nulling the SAR. As already noted, a solution to this problem is provided by differential PLA. Let τ be the frame index of the most recent authenticated message, then for differential PLA $x_k(1)$ should be replaced by $x_k(\tau)$ in (15).

Remark 2: We have assessed the performance of the three UA methods, and we conclude that A-CBCA has an unlimited SAR as we increase the number of quantization bits. For PLA we have an explicit expression for SAR, depending however on the attack by Eve. For the SAR of S-CBCA we have only bounds. Moreover, for a particular attack strategy by Eve the SARs of both PLA and S-CBCA are upper-bounded by the same expression.

IV. Rayleigh AWGN Reciprocal Channels

We now consider a scenario wherein channel estimates are corrupted by AWGN, which corresponds for example to a massive MIMO system wherein all users (Alice, Bob and Eve) have $\sqrt{n}$ antennas each, so that the resulting channel matrices have $n \to \infty$ entries[2]. Moreover, channel matrix entries are assumed i.i.d., and zero-mean unitary power complex Gaussian (ZMUPCG) distributed, in accordance with the Rayleigh fading model. By reordering the n entries of each matrix into a vector we obtain the channel model described in Section II, where $\boldsymbol{x}(t)$, $\boldsymbol{y}(t)$ and $\boldsymbol{z}(t)$ are Gaussian distributed.

We assume that the channel between any couple of devices is reciprocal, therefore, indicating with $\boldsymbol{h}(t)$ the n-size row channel vector between Alice and Bob its estimates can be written as

$$\boldsymbol{x}(t) = \boldsymbol{h}(t) + \sigma_{\rm x}\boldsymbol{w}_{\rm x}(t), \quad \boldsymbol{y}(t) = \boldsymbol{h}(t) + \sigma_{\rm y}\boldsymbol{w}_{\rm y}(t), \quad (18)$$

where $\boldsymbol{w}_{\rm x}(t), \boldsymbol{w}_{\rm y}(t)$ are jointly ZMUPCG distributed and both independent among them and with respect to $\boldsymbol{h}(t)$, while $\sigma_{\rm x}^2$ and $\sigma_{\rm y}^2$ are the noise powers at the receivers. We also define the correlation of $h_k(t)$ entries over time as

$$\mathbb{E}[h_k(t)h_k^*(t+\ell)] = \rho(\ell), \quad k = 1, \dots n. \quad (19)$$

The k-th Eve's channels at frame t (without the estimation noise) are correlated, with correlation coefficients (in the absence of noise) $\alpha_{\rm A}$ and $\alpha_{\rm B}$ to $\boldsymbol{h}(t)$, and affected by AWGN with powers $\sigma_{\rm v,A}^2$ and $\sigma_{\rm v,B}^2$ (typically $\sigma_{\rm v,A}^2 = \sigma_{\rm v,B}^2$). Therefore, her estimate of her channel to Alice is

$$\boldsymbol{v}_{\rm A}(t) = \alpha_{\rm A}\boldsymbol{h}(t) + \sqrt{1-\alpha_{\rm A}^2}\boldsymbol{q}_{\rm A}(t) + \sigma_{\rm v,A}\boldsymbol{w}_{\rm v,A}(t), \quad (20)$$

while her estimate of her channel to Bob is

$$\boldsymbol{v}_{\rm B}(t) = \alpha_{\rm B}\boldsymbol{h}(t) + \sqrt{1-\alpha_{\rm B}^2}\boldsymbol{q}_{\rm B}(t) + \sigma_{\rm v,B}\boldsymbol{w}_{\rm v,B}(t), \quad (21)$$

where $\boldsymbol{q}_{\rm A}(t)$, $\boldsymbol{q}_{\rm B}(t)$ are ZMUPCG vectors describing the independent component of the Eve channels with respect to $h_k(t)$, and the noise vectors $\boldsymbol{w}_{\rm v,A}(t)$, $\boldsymbol{w}_{\rm v,B}(t)$ have ZMUPCG entries independent with respect to $\boldsymbol{h}(t)$, $\boldsymbol{q}_{\rm A}(t)$, and $\boldsymbol{q}_{\rm B}(t)$. Note that by these definitions all channel estimates have unitary variance in the absence of noise.

A. A-CBCA

As we have already seen, by using directly the channel estimate, the SAR of A-CBCA is infinite, thus we focus here on the channel quantization case, and in particular on the bound (11).

First recall that for a Gaussian vector $\boldsymbol{v}$ of size $\bar{k}$ with correlation matrix $\boldsymbol{R}_{\boldsymbol{v}}$ the differential entropy is $\bar{\mathbb{H}}(\boldsymbol{v}) = \log\det((\pi e)^{\bar{k}}\boldsymbol{R}_{\rm v})$. Let us define

$$\begin{aligned}\boldsymbol{R}_{[y_k(2),\boldsymbol{z}_k(2t)]} &= \mathbb{E}[[y_k(2), \boldsymbol{z}_k(2t)]^H[y_k(2), \boldsymbol{z}_k(2t)]] \\ &= \begin{bmatrix} 1+\sigma_{\rm y}^2 & \boldsymbol{r}_{\rm y}^H \\ \boldsymbol{r}_{\rm y} & \boldsymbol{R}_{\boldsymbol{z}_k(2t)} \end{bmatrix}, \end{aligned} \quad (22)$$

where $\boldsymbol{r}_{\rm y} = \mathbb{E}[y_k(2)\boldsymbol{z}_k^H(2t)]$ has entry $\ell = 1, \dots, 2t$

$$[\boldsymbol{r}_{\rm y}]_\ell = \begin{cases} \alpha_{\rm A}^*\rho(\ell-2) & \ell \text{ even}, \\ \alpha_{\rm B}^*\rho(\ell-2) & \ell \text{ odd}, \end{cases} \quad (23)$$

and $\boldsymbol{R}_{\boldsymbol{z}_k(2t)} = \mathbb{E}[\boldsymbol{z}_k^H(2t)\boldsymbol{z}_k(2t)]$, with entries

$$[\boldsymbol{R}_{\boldsymbol{z}_k(2t)}]_{m,n} = \begin{cases} \alpha_{\rm A}^*\alpha_{\rm B}\rho(m-n) & n \text{ odd}, m \text{ even} \\ \alpha_{\rm A}\alpha_{\rm B}^*\rho(m-n) & n \text{ even}, m \text{ odd} \\ |\alpha_{\rm B}|^2\rho(m-n) & n \text{ and } m \text{ even}, m \neq n \\ |\alpha_{\rm A}|^2\rho(m-n) & n \text{ and } m \text{ odd}, m \neq n \\ 1+\sigma_{\rm z}^2 & n = m. \end{cases} \quad (24)$$

Then we have

$$\begin{aligned}\mathbb{I}(y_k(2); \boldsymbol{z}_k(2t)) &= \bar{\mathbb{H}}(y_k(2)) + \bar{\mathbb{H}}(\boldsymbol{z}_k(2t)) \\ -\bar{\mathbb{H}}([y_k(2), \boldsymbol{z}_k(2t)]) &= \log\frac{(1+\sigma_{\rm y}^2)\det\boldsymbol{R}_{\boldsymbol{z}_k(2t)}}{\det\boldsymbol{R}_{[y_k(2),\boldsymbol{z}_k(2t)]}} \\ &= -\log\left(1 - \frac{\boldsymbol{r}_{\rm y}^H\boldsymbol{R}_{\boldsymbol{z}_k(2t)}^{-1}\boldsymbol{r}_{\rm y}}{1+\sigma_{\rm y}^2}\right). \end{aligned} \quad (25)$$

Moreover, the entropy of $\langle y_k(2)\rangle$ is

$$\mathbb{H}(\langle y_k(2)\rangle) = -\sum_{a\in\mathcal{A}} p_{\langle y_k(2)\rangle}(a)\log p_{\langle y_k(2)\rangle}(a), \quad (26)$$

where $\mathcal{A}$ is the quantization alphabet.

[2] Other antennas configurations can be considered, leading to similar results and expressions as those derived in this section. Also, OFDM systems can be cast in this model.

B. S-CBCA

For S-CBCA we have the bound (7). In particular, for the Gaussian case we have

$$\begin{aligned}\mathbb{I}(x_k(1); y_k(2)) &= \bar{\mathbb{H}}(x_k(1)) + \bar{\mathbb{H}}(y_k(2)) - \bar{\mathbb{H}}(x_k(1), y_k(2)) \\ &= -\log\left(1 - \frac{|\mathbb{E}[x_k(1)y_k^*(2)]|^2}{(1+\sigma_\mathrm{x}^2)(1+\sigma_\mathrm{y}^2)}\right) \\ &= -\log\left(1 - \frac{\rho(1)}{(1+\sigma_\mathrm{x}^2)(1+\sigma_\mathrm{y}^2)}\right), \qquad (27)\end{aligned}$$

and analogously to (25)

$$\begin{aligned}\mathbb{I}(x_k(1); \boldsymbol{z}_k(2t)) &= \log\frac{(1+\sigma_\mathrm{x}^2)\det \boldsymbol{R}_{\boldsymbol{z}_k(2t)}}{\det \boldsymbol{R}_{[x_k(1), \boldsymbol{z}_k(2t)]}} \\ &= -\log\left(1 - \frac{\boldsymbol{r}_\mathrm{x}^H \boldsymbol{R}_{\boldsymbol{z}_k(2t)}^{-1} \boldsymbol{r}_\mathrm{x}}{1+\sigma_\mathrm{x}^2}\right) \qquad (28)\end{aligned}$$

where

$$\begin{aligned}\boldsymbol{R}_{[x_k(1), \boldsymbol{z}_k(2t)]} &= \mathbb{E}[[x_k(1), \boldsymbol{z}_k(2t)]^H [y_k(2), \boldsymbol{z}_k(2t)]] \\ &= \begin{bmatrix} 1+\sigma_\mathrm{x}^2 & \boldsymbol{r}_\mathrm{x}^H \\ \boldsymbol{r}_\mathrm{x} & \boldsymbol{R}_{\boldsymbol{z}_k(2t)} \end{bmatrix}, \qquad (29)\end{aligned}$$

and entry $\ell = 1, \dots, 2t$ of $\boldsymbol{r}_\mathrm{x}$ is

$$[\boldsymbol{r}_\mathrm{x}]_\ell = [\mathbb{E}[x_k(1)\boldsymbol{z}_k^H(2t)]]_\ell = \begin{cases} \alpha_\mathrm{A}^* \rho(\ell - 1) & \ell \text{ even}, \\ \alpha_\mathrm{B}^* \rho(\ell - 1) & \ell \text{ odd}. \end{cases} \qquad (30)$$

Moreover, we have

$$\begin{aligned}&\mathbb{I}(x_k(1); y_k(2) | \boldsymbol{z}_k(2t)) \\ &\quad = \mathbb{I}(x_k(1); y_k(2), \boldsymbol{z}_k(2t)) - \mathbb{I}(x_k(1); \boldsymbol{z}_k(2t)) \qquad (31) \\ &\mathbb{I}(x_k(1); y_k(2), \boldsymbol{z}_k(2t)) \\ &\quad = \log\frac{(1+\sigma_\mathrm{x}^2)\det \boldsymbol{R}_{[y_k(2), \boldsymbol{z}_k(2t)]}}{\det \boldsymbol{R}_{[x_k(1), y_k(2), \boldsymbol{z}_k(2t)]}} \qquad (32)\end{aligned}$$

and

$$\boldsymbol{R}_{[x_k(1), y_k(2), \boldsymbol{z}_k(2t)]} = \begin{bmatrix} 1+\sigma_\mathrm{x}^2 & \rho(1) \quad \boldsymbol{r}_\mathrm{x}^H \\ \begin{matrix}\rho(-1) \\ \boldsymbol{r}_\mathrm{x}\end{matrix} & \boldsymbol{R}_{[y_k(2), \boldsymbol{z}_k(2t)]} \end{bmatrix}. \qquad (33)$$

C. PLA

We now consider the PLA scheme. Assuming that Eve generates the induced estimate $\boldsymbol{x}(2t+1)$ randomly distributed according to the PDF of the legitimate channel given Eve's observations, i.e., $p_{x_k(2t+1)|\boldsymbol{z}_k(2t), \mathcal{H}_0}$ the SAR has been computed in [6]. In particular, let us define $\boldsymbol{S} = \boldsymbol{R}_{[x_k(1), \boldsymbol{z}_k(2t)]}^{-1}$ and $\boldsymbol{T} = \boldsymbol{R}_{[x_k(2t+1), \boldsymbol{z}_k(2t)]}^{-1}$ where

$$\begin{aligned}&\boldsymbol{R}_{[x_k(2t+1), \boldsymbol{z}_k(2t)]} \\ &\quad = \mathbb{E}[[x_k(2t+1), \boldsymbol{z}_k(2t)]^H [x_k(2t+1), \boldsymbol{z}_k(2t)]] \\ &\quad = \begin{bmatrix} 1+\sigma_\mathrm{x}^2 & \boldsymbol{r}_{\mathrm{x},2}^H \\ \boldsymbol{r}_{\mathrm{x},2} & \boldsymbol{R}_{\boldsymbol{z}_k(2t)} \end{bmatrix}, \qquad (34) \\ &[\boldsymbol{r}_{\mathrm{x},2}]_\ell = [\mathbb{E}[x_k(2t+1)\boldsymbol{z}_{\boldsymbol{k}}^H(2t)]]_\ell \\ &\quad = \begin{cases} \alpha_\mathrm{A}^* \rho(\ell - 2t + 1) & \ell \text{ even}, \\ \alpha_\mathrm{B}^* \rho(\ell - 2t + 1) & \ell \text{ odd}. \end{cases} \qquad (35)\end{aligned}$$

Partitioning the two matrices as

$$\boldsymbol{S} = \begin{bmatrix} S_{1,1} & \boldsymbol{S}_{1,2} \\ \boldsymbol{S}_{2,1} & \boldsymbol{S}_{2,2} \end{bmatrix} \quad \boldsymbol{T} = \begin{bmatrix} T_{1,1} & \boldsymbol{T}_{1,2} \\ \boldsymbol{T}_{2,1} & \boldsymbol{T}_{2,2} \end{bmatrix} \qquad (36)$$

where $T_{1,1}$ and $S_{1,1}$ are scalars, while all other entries are vectors and matrices of suitable dimensions, we define

$$\boldsymbol{E} = \boldsymbol{S}_{2,2} + \boldsymbol{T}_{2,2} - \boldsymbol{R}_{\boldsymbol{z}_k(2t)}^{-1}, \qquad (37)$$

and

$$\boldsymbol{V} = \begin{bmatrix} T_{1,1} - \boldsymbol{T}_{1,2}^H \boldsymbol{E}^{-1} \boldsymbol{T}_{1,2} & -\boldsymbol{T}_{1,2}^H \boldsymbol{E}^{-1} \boldsymbol{S}_{1,2} \\ -\boldsymbol{S}_{1,2}^H \boldsymbol{E}^{-1} \boldsymbol{T}_{1,2} & S_{1,1} - \boldsymbol{S}_{1,2}^H \boldsymbol{E}^{-1} \boldsymbol{S}_{1,2} \end{bmatrix}^{-1}. \qquad (38)$$

Then (15) becomes the KL divergence of two 2-dimensional Gaussian zero-mean vectors, i.e.,

$$\begin{aligned}&R_\mathrm{PLA}(2t+1) \\ &= \frac{-\ln\det(\boldsymbol{R}_{[x_k(2t+1), x_k(1)]}\boldsymbol{V}) + \mathrm{tr}(\boldsymbol{V}\boldsymbol{R}_{[x_k(2t+1), x_k(1)]}) - 2}{\ln 2}, \qquad (39)\end{aligned}$$

where

$$\begin{aligned}\boldsymbol{R}_{[x_k(2t+1), x_k(1)]} &= \mathbb{E}[[x_k(2t+1), x_k(1)]^H [x_k(2t+1), x_k(1)]] \\ &= \begin{bmatrix} 1+\sigma_\mathrm{x}^2 & \rho(2t) \\ \rho(-2t) & 1+\sigma_\mathrm{x}^2 \end{bmatrix}. \qquad (40)\end{aligned}$$

Note that if the differential PLA approach is used, indicating with τ the most recent authenticated channel estimate, then we have $\boldsymbol{S} = \boldsymbol{R}_{[x_k(\tau), \boldsymbol{z}_k(2t)]}^{-1}$ and matrix $\boldsymbol{R}_{[x_k(2t+1), x_k(1)]}$ becomes $\boldsymbol{R}_{[x_k(2t+1), x_k(\tau)]}$ having an expression similar to (40) where $\rho(2t)$ and $\rho(-2t)$ are replaced by $\rho(2t+1-\tau)$ and $\rho(\tau-2t-1)$, respectively.

V. Linear Eve's Processing

With linear Eve's processing (LEP) Eve first performs a linear combination of all channel estimates to obtain the MMSE linear estimate of the legitimate channel $\hat{\boldsymbol{h}}$, which is then used for the attack. In particular, for the A-CBCA scheme Eve estimates $\boldsymbol{h}(2)$, while for PLA she estimates $\boldsymbol{h}(1)$. For S-CBCA, since we have only bounds on the SAR, Eve estimates a channel that minimizes either of the two SAR bounds. For example, for the minimization of the lower bound, Eve selects among the estimates in the two frames the one that maximizes the minimum of the two mutual information, i.e.,

$$\begin{aligned}\hat{\boldsymbol{h}} = \mathrm{argmax}&_{\boldsymbol{h} \in \{\hat{\boldsymbol{h}}(1), \hat{\boldsymbol{h}}(2)\}} \\ &\min\{\mathbb{I}(x_k(1); \boldsymbol{z}_k(2t)), \mathbb{I}(y_k(2); \boldsymbol{z}_k(2t))\}. \qquad (41)\end{aligned}$$

Let τ be the frame index of the desired channel estimate, $\tau = 1, 2$. We first define the correlation vector

$$\boldsymbol{\beta}(\tau) = \mathbb{E}[\boldsymbol{z}_k(2t) h_k^*(\tau)] \qquad (42)$$

with entries

$$\beta_{2\ell+1}(\tau) = \alpha_\mathrm{A} \rho(\tau - 2\ell - 1), \quad \beta_{2\ell}(\tau) = \alpha_\mathrm{B} \rho(\tau - 2\ell). \qquad (43)$$

Then we have

$$\boldsymbol{z}_k(2t) = \boldsymbol{\beta}(\tau) h_k(\tau) + \boldsymbol{w}_0 \boldsymbol{R}_\mathrm{s}^{1/2}(2t), \qquad (44)$$

where $\boldsymbol{w}_0$ is a jointly ZMUPCG $2t$-size vector with i.i.d. entries and the correlation matrix $\boldsymbol{R}_{\rm s}(2t)$ is

$$\boldsymbol{R}_{\rm s}(2t) = \mathbb{E}[(\boldsymbol{z}_k(2t) - \boldsymbol{\beta}(\tau)h_k(\tau))^H(\boldsymbol{z}_k(2t) - \boldsymbol{\beta}(\tau)h_k(\tau))]. \tag{45}$$

Now, the MMSE estimation of $h_k(\tau)$ is obtained as follows

$$\begin{aligned}\hat{z}_k(2t) &= \frac{1}{\mathrm{tr}(\boldsymbol{R}_{\rm s}^{-2}(2t))}\boldsymbol{z}_k(2t)\boldsymbol{R}_{\rm s}^{-1}(2t)\boldsymbol{1}\\ &= h_k(\tau) + \sigma_{\rm z}(2t)\hat{w}_{\rm z}(2t),\end{aligned} \tag{46}$$

where $\boldsymbol{1}$ is a $2t$-long column vector of all ones, $\hat{w}_{\rm z}(2t)$ is ZMUPCG and

$$\sigma_{\rm z}^2(2t) = \mathrm{tr}^2(\boldsymbol{R}_{\rm s}^{-2}(2t)). \tag{47}$$

In general, LEP is a suboptimal procedure (except for time-invariant channels as discussed below) since it does not fully use $\boldsymbol{z}_k(2t)$. However, this procedure has a limited computational complexity. The SAR obtained with LEP is readily computed from the results of the previous section where $\boldsymbol{z}_k(2t)$ is replaced by $\hat{z}_k(2t)$ having unitary correlation with $h_k(\tau)$ and noise power $\sigma_{\rm z}^2(2t)$.

A. LEP With Time-Invariant Channels

We now focus on time invariant channels, since in this case LEP is optimal. Therefore we have $\boldsymbol{h}(t) = \boldsymbol{h}$, $\boldsymbol{q}_{\rm A}(t) = \boldsymbol{q}_{\rm A}$, $\boldsymbol{q}_{\rm B}(t) = \boldsymbol{q}_{\rm B}$ and $\rho(t) = 1\ \forall t$.

For $t = 1$ we have

$$\boldsymbol{\beta}(1) = \boldsymbol{\beta}(2) = [\alpha_{\rm A}, \alpha_{\rm B}]^T, \tag{48}$$

$$\boldsymbol{R}_s(2) = \begin{bmatrix} 1-\alpha_{\rm A}^2+\sigma_{\rm v,A}^2 & 0 \\ 0 & 1-\alpha_{\rm B}^2+\sigma_{\rm v,B}^2\end{bmatrix}, \tag{49}$$

and for the upper bound of S-CBCA SAR we have

$$\boldsymbol{R}_{[x_k(1),y_k(2),\hat{z}_k(2)]} = \begin{bmatrix} 1+\sigma_{\rm x}^2 & 1 & 1 \\ 1 & 1+\sigma_{\rm y}^2 & 1 \\ 1 & 1 & 1+\sigma_{\rm z}^2(2t)\end{bmatrix}, \tag{50}$$

$$\begin{aligned}\det \boldsymbol{R}_{[x_k(1),y_k(2),\hat{h}_k(2)]} &= (1+\sigma_{\rm x}^2)[(1+\sigma_{\rm y}^2)(1+\sigma_{\rm z}^2(2))-1]\\ &\quad -[(1+\sigma_{\rm z}^2(2))-1]+[1-(1+\sigma_{\rm y}^2)]\\ &= \sigma_{\rm x}^2\sigma_{\rm y}^2+\sigma_{\rm x}^2\sigma_{\rm z}^2(2)+(1+\sigma_{\rm x}^2)\sigma_{\rm y}^2\sigma_{\rm z}^2(2).\end{aligned} \tag{51}$$

For $t > 1$ note instead that, since both $\boldsymbol{q}_{\rm A}$ and $\boldsymbol{q}_{\rm B}$ are the same at all frames, LEP boils down to first estimating

$$\begin{aligned}\bar{\boldsymbol{v}}_{\rm A}(2t) &= \frac{1}{t}\sum_{n=0}^{t-1}\boldsymbol{v}_{\rm A}(2n+1)\\ &= \alpha_{\rm A}\boldsymbol{h} + \sqrt{1-\alpha_{\rm A}^2}\boldsymbol{q}_{\rm A} + \sigma_{\bar{v},{\rm A}}(2t)\boldsymbol{w}_{\rm v,A}(2t),\end{aligned} \tag{52}$$

$$\begin{aligned}\bar{\boldsymbol{v}}_{\rm B}(2t) &= \frac{1}{t}\sum_{n=0}^{t-1}\boldsymbol{v}_{\rm B}(2n)\\ &= \alpha_{\rm B}\boldsymbol{h} + \sqrt{1-\alpha_{\rm B}^2}\boldsymbol{q}_{\rm B} + \sigma_{\bar{v},{\rm B}}(2t)\boldsymbol{w}_{\rm v,B}(2t),\end{aligned} \tag{53}$$

where $\boldsymbol{w}_{\rm v,A}(2t)$ and $\boldsymbol{w}_{\rm v,B}(2t)$ are ZMUPCG and

$$\sigma_{\bar{v},{\rm A}}^2(2t) = \frac{\sigma_{\rm v,A}^2}{t}, \quad \sigma_{\bar{v},{\rm B}}^2(2t) = \frac{\sigma_{\rm v,B}^2}{t}, \tag{54}$$

and then applying MMSE combining on $\bar{\boldsymbol{v}}_{\rm A}(2t)$ and $\bar{\boldsymbol{v}}_{\rm B}(2t)$ as for the case $t = 1$.

In particular, for $t \to \infty$, from (54) we have that $\sigma_{\bar{v},{\rm A}}^2(2t) = \sigma_{\bar{v},{\rm B}}^2(2t) = 0$, and

$$\hat{z}_k(2t) = h_k + \frac{\alpha_{\rm A}(1-\alpha_{\rm A})}{(\alpha_{\rm A}^2+\alpha_{\rm B}^2)}q_{{\rm A},k} + \frac{\alpha_{\rm B}(1-\alpha_{\rm B})}{(\alpha_{\rm A}^2+\alpha_{\rm B}^2)}q_{{\rm B},k}, \tag{55}$$

i.e., the Eve's channel estimate is affected only by $\boldsymbol{q}_{\rm A}$ and $\boldsymbol{q}_{\rm B}$.

In Appendix B we derive the SAR with LEP processing of the A-CBCA scheme considering a uniform quantizer.

VI. Attacks in the ID-A Phase

In this section we consider attacks by Eve in the ID-A phase for the various UA strategies. Eve transmits together and synchronously with both Alice and Bob in the ID-A phase. Therefore, she can overlap her signal on the pilots transmitted by Alice. Furthermore, Eve is assumed to be a full-duplex terminal, therefore, she can transmit pilots and at the same time receive signals by both Alice and Bob thus estimating the channel. Channels are time-invariant (thus we drop index t) and, in order to simplify notation, we assume that Eve has perfect estimates of her channels to both Alice and Bob, i.e., $\sigma_{\rm v}^2 = 0$.

A. Attacks Description

Two attacks are considered: the pilot contamination (PC) and the artificial noise (AN) attack. These attacks are very well known in the literature, and we now apply them to the UA procedures.

1) PC Attack: With PC attack, Eve transmits a scaled version of pilots transmitted by Alice, with scaling diagonal matrices $\boldsymbol{P}_{\rm A}$ and $\boldsymbol{P}_{\rm B}$, so that both Alice and Bob estimate the same channel to Eve, i.e.,

$$\boldsymbol{P}_{\rm A}\boldsymbol{v}_{\rm A} = \boldsymbol{P}_{\rm B}\boldsymbol{v}_{\rm B} = \boldsymbol{1}g, \tag{56}$$

where $\boldsymbol{1}$ is the n-size column vector of all ones. The estimated channels by Alice and Bob are

$$\boldsymbol{x}(t) = \boldsymbol{h} + \boldsymbol{1}g + \sigma_{\rm x}\boldsymbol{w}_{\rm x}(t), \quad \boldsymbol{y}(t) = \boldsymbol{h} + \boldsymbol{1}g + \sigma_{\rm y}\boldsymbol{w}_{\rm y}(t). \tag{57}$$

In order to analyze the performance of this attack we note that if we divide both $x_k(t)$ and $y_k(t)$ by $\sqrt{1+|g|^2}$ we obtain again the model (18)-(21) where now $\sigma_{\rm x}^2$ and $\sigma_{\rm y}^2$ become $\sigma_{\rm x}^2/(1+|g|^2)$ and $\sigma_{\rm y}^2/(1+|g|^2)$, respectively. On her side, Eve using LEP obtains the estimate of $(h_k+g)/\sqrt{1+|g|^2}$

$$\hat{z}_{{\rm PC},k}(2t) = (\hat{z}_k(2t)+g)/\sqrt{1+|g|^2} \tag{58}$$

with noise variance $\sigma_{\rm z}^2(2t)/(1+|g|^2)$. Therefore, the effect of this attack is the scaling of all noise variances, and results of previous Section provide the SAR. Note that the PC attack has an impact also on PLA correctness, when Eve does not transmit pilots after the ID-A phase. In this case Bob may not recognize the Alice-Bob channel as correct, since g is missing. Both A-CBCA and S-CBCA are not affected by this issue, since they only use the key extracted in the ID-A phase.

2) AN Attack: With this attack Eve transmits AN during the ID-A phase, i.e., a random ZMUPCG distributed signal aimed at increasing the noise for both Alice and Bob. This scenario can be analyzed using the results of the previous Section, simply modifying the values of σ_{x}^2 and σ_{y}^2. Note that this attack has no impact on the correctness of the UA process.

B. Defense Strategies

We describe now possible defense strategies against the ID-A attacks.

- **Random pilots**: legitimate parties use random pilots, locally generated at the transmitter and shared with the legitimate receiver after the ID-A phase on the public authenticated error-free channel (which as we have seen, must be in any case available in the ID-A phase). In this case Eve cannot add coherently her pilots and induce the desired channel (see also [37]);
- **Channel and noise power estimation**: if reference values of these powers are available at the legitimate receivers, the attack can be detected (see also [38]);
- **Channel agreement**: as outlined in [38] by estimating the channel at both Alice and Bob and comparing the estimates without disclosing them to Eve it is possible to check if the two legitimate users see the same channel, thus preventing Eve from performing an attack wherein she does not know the channels to Alice and Bob.

Moreover, note that the described attacks require the knowledge of both the Alice-Eve and Bob-Eve channels before transmissions, therefore, implementing the ID-A stage at the very beginning of transmission prevents Eve from getting the channel estimates and deploying the attack.

VII. Numerical Results

We provide now some results on the SAR of the various UA systems. We focus in particular on the Rayleigh AWGN reciprocal channels of Section IV, where both Alice and Bob transmit with unitary power and channels are vectors of i.i.d. ZMUPCG variables. We consider both time-invariant and time-variant channels, and the ID-A attacks described in Section VI. For A-CBCA we have already observed that the SAR can be made arbitrarily large in the presence of a passive eavesdropper: here we report the results for a uniform quantizer with 3 bits (corresponding to 8 quantization levels) and saturation probability of 10^{-2}. For the other schemes instead, since the best performance is obtained for an unquantized channel (that provides more randomness) we only focus on continuous-valued channels.

Unless differently specified we consider $\sigma_{\mathrm{x}}^2 = \sigma_{\mathrm{y}}^2 = \sigma_{\mathrm{v,A/B}}^2 = -10$ dB.

A. Time-Invariant Channels

We start from time-invariant channels. Fig. 1 shows the SAR versus (vs) the correlation coefficients $\alpha_{\mathrm{A}} = \alpha_{\mathrm{B}}$, at ID-V frame $t = 3$, i.e., immediately after the two ID-A frames.

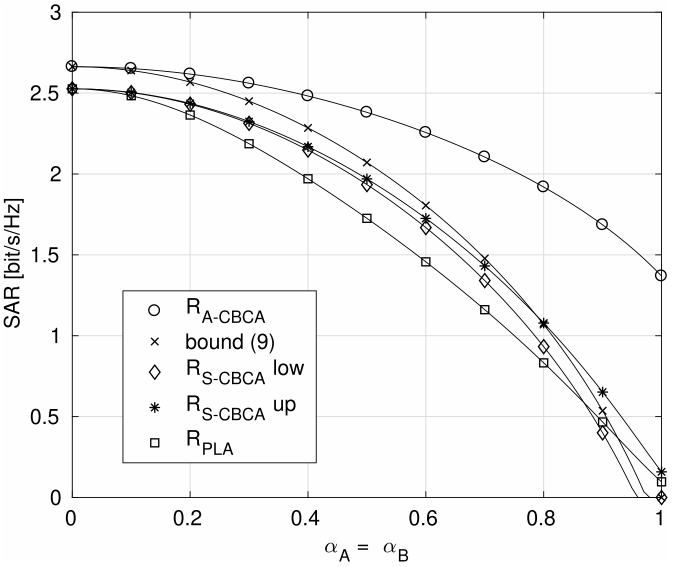

Fig. 1. SAR vs the correlation coefficients $\alpha_{\mathrm{A}} = \alpha_{\mathrm{B}}$ for time-invariant channels at ID-V frame $t = 3$.

The results for the lower and upper bound on the SAR of S-CBCA are shown as $R_{\mathrm{S-CBCA}}$ low and up, respectively. Moreover, we report the bound (11) of A-CBCA. We remark that the reported performance is obtained using only a quantized version of the channel estimate as source of randomness; indeed A-CBCA could use other sources of randomness further improving its performance. As expected, the SAR decreases with an increasing correlation among the legitimate and eavesdropper's channels. Note that even when $\alpha_{\mathrm{A}} = \alpha_{\mathrm{B}} = 1$ we still may have a non-zero SAR. In particular, A-CBCA benefits from the randomness of the noise which is assumed independent with respect to that of Eve. Similarly, in PLA Eve generates a random attack channel having as mean her channel estimate rather than the estimate obtained by the legitimate user in the ID-A steps, and the two estimates differ due to the noise. The lower bound for S-CBCA is indeed zero in this case.

Fig. 2 shows the SAR as a function of the ID-V frame for three values of channel correlations: $\alpha_{\mathrm{A}} = \alpha_{\mathrm{B}} = 0.1$ (solid lines), $\alpha_{\mathrm{A}} = \alpha_{\mathrm{B}} = 0.4$ (dashed lines), and $\alpha_{\mathrm{A}} = \alpha_{\mathrm{B}} = 0.8$ (dotted lines). We observe that the SAR decreases for all schemes as the ID-V frame t increases, because in the meantime Eve has obtained a better channel estimate. The performance degradation is more remarkable for a higher channel correlation factor, since in this case having a more accurate knowledge of her channels to Alice and Bob truly provides Eve a better knowledge of the Alice-Bob channel.

B. Time-Varying Channels

We consider now frame-time-variant channels with Jakes fading. In particular, the channel is time-invariant in each frame while the evolution over frames is

$$h_k(t) = \rho(t) h_k(1) + \sqrt{1 - |\rho(t)|^2}\,\phi_k(t), \tag{59}$$

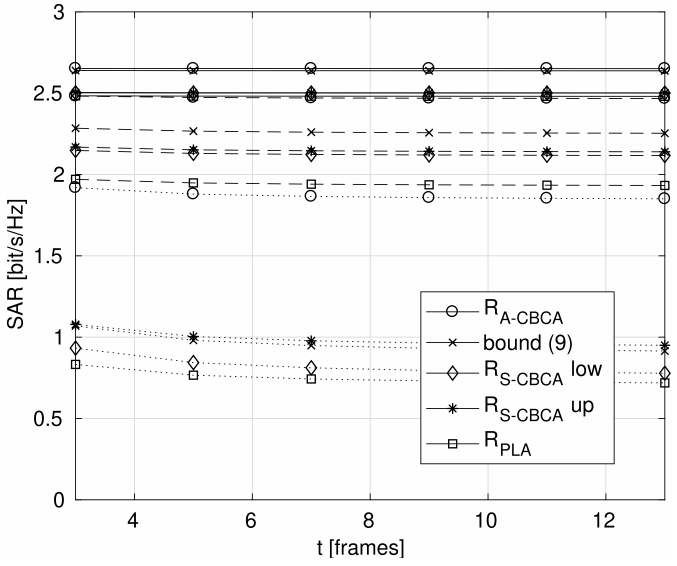

Fig. 2. SAR vs ID-V frame index, for three values of channel correlations: $\alpha_{\rm A} = \alpha_{\rm B} = 0.1$ (solid lines), $\alpha_{\rm A} = \alpha_{\rm B} = 0.4$ (dashed lines), and $\alpha_{\rm A} = \alpha_{\rm B} = 0.8$ (dotted lines).

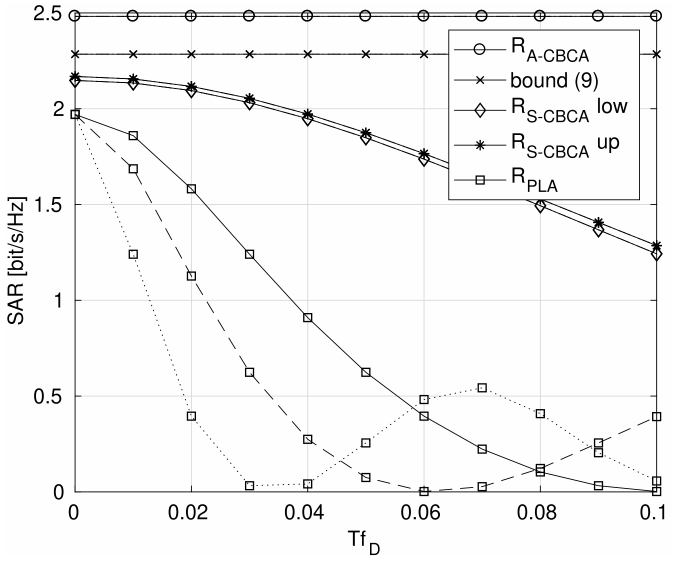

Fig. 4. SAR vs the normalized Doppler frequency for three ID-V frames $t = 3$ (solid lines), $t = 5$ (dashed lines) and $t = 9$ (dotted lines). $\alpha_{\rm A} = \alpha_{\rm B} = 0.4$.

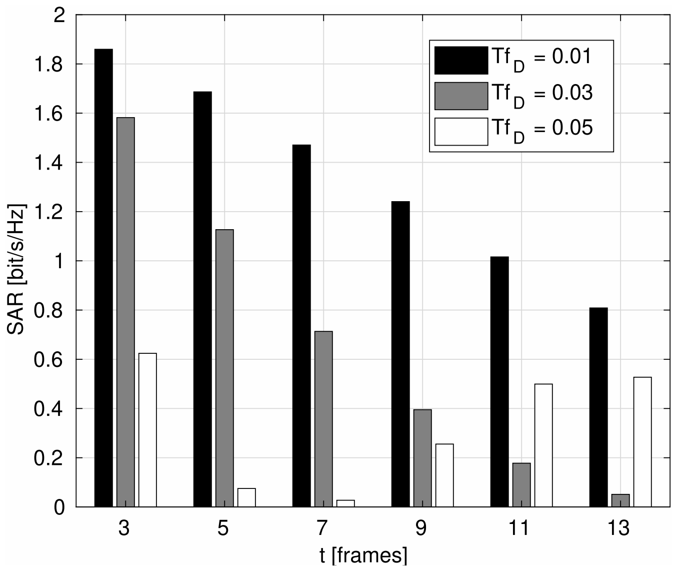

Fig. 3. SAR vs the ID-V frame index, for three values of the normalized Doppler frequency $Tf_{\rm D}$ for the PLA scheme. $\alpha_{\rm A} = \alpha_{\rm B} = 0.4$.

with $\phi_k(t)$ ZMUPCG and

$$\rho(t) = J_0(2\pi f_d t T), \tag{60}$$

with T being the frame duration, f_d the Doppler frequency and $J_0(\cdot)$ the zero-order Bessel function of the first kind.

As we have observed, channel variations have an impact on the ability of PLA to effectively authenticate a legitimate transmission, since the channel (which is used as user signature) changes. Therefore, Fig. 3 shows the SAR vs the ID-V frame index, for three values of the normalized Doppler frequency $Tf_{\rm D}$ for the PLA scheme when $\alpha_{\rm A} = \alpha_{\rm B} = 0.4$. We assume that Eve estimates the channel only in the first two frames (e.g., because in the next frames neither Alice not Bob are transmitting). We observe that the SAR decreases as the normalized Doppler frequency increases. Moreover, as the ID-V frame index increases the SAR is reduced as well. In both cases the channel variations prevent an effective authentication. Lastly, note that for the highest value of the normalized Doppler frequency the SAR increases for a higher number of frames: this is due to the Jakes model, and in particular to the behavior of the correlation (60) as f_d first decreases and then increases.

We now consider the effect of time-variations on all the schemes. Fig. 4 shows the SAR as a function of the normalized Doppler frequency for three ID-V frames $t = 3$ (solid lines), $t = 5$ (dashed lines) and $t = 9$ (dotted lines). Also in this case $\alpha_{\rm A} = \alpha_{\rm B} = 0.4$. We observe that the A-CBCA scheme (again only using quantized channel estimates) is not affected by the time-variation of the channel across frames, as it only uses one frame. Moreover, for S-CBCA the SAR decreases for increasing normalized Doppler frequency but it is insensitive to the frame wherein authentication is performed: in fact, for this scheme the channel is used only in the ID-A phase to establish the secret key and channel variations in next frames are not relevant. On the other hand, S-CBCA and PLA are more heavily affected by channel variations since they impact both ID-A and ID-V phases. Also in this case we observe the effect of increasing channel correlation for high Doppler frequency, as already discussed for Fig. 2.

Lastly, note that results reported for the PLA scheme hold also for differential PLA where however the time reference t now indicates the difference in frames between the last authenticated message and the message to be checked.

C. Active Attacks

We now consider the active attacks described in Section VI, namely both the PC and AN attacks. Fig. 5 shows the SAR as a function of σ_G^2 for both PC (solid lines) and AN attack (dashed lines). Also in this case $\alpha_{\rm A} = \alpha_{\rm B} = 0.4$ and channels

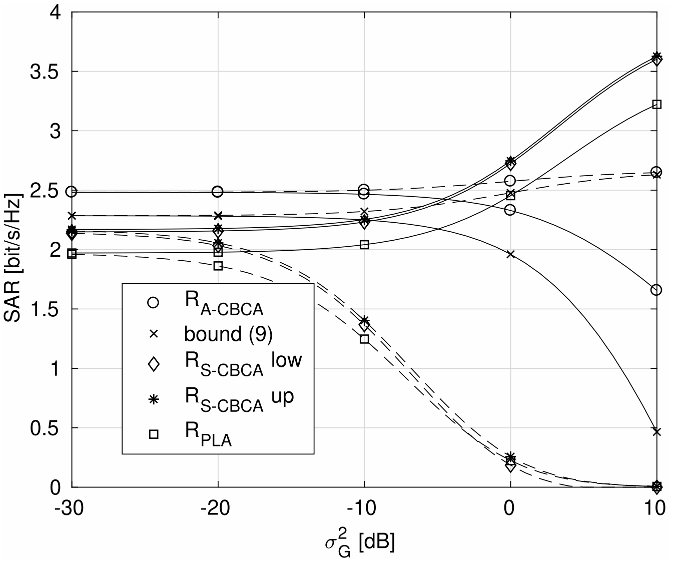

Fig. 5. SAR as a function of σ_G^2 for ID-A-phase attacks, for both the PC attack (solid lines) and the AN attack (dashed lines).

are time-invariant. We recall that for the PC attack σ_G^2 is the power of the random channel superimposed to the effective channel that is estimated by the legitimate users in the ID-A phase. From the figure we observe that this attack is not effective for S-CBCA and PLA schemes, as on the contrary the SAR is increased. Indeed, this attack is equivalent to a reduction of the estimate noise for both Alice and Bob thus resulting in a situation globally favorable to the legitimate users. For A-CBCA this attack is instead effective, since the reduction of the uncertainty on the channel estimated by Bob helps Eve. Note again that other sources of randomness could be used for A-CBCA thus preventing the attack. When we consider the AN attack instead we observe that it is effective against both the S-CBCA and PLA schemes, while it yields a higher SAR (thus not being effective) for A-CBCA. In fact, since the AN is not used by Eve in its estimation phase, this attack provides additional randomness to Alice, that is unknown to Eve, thus supporting the extraction of random bits from the channel in A-CBCA. Instead, the additional noise damages either the extraction a secret key from the channel in the S-CBCA scheme, or the detection of channel variations in PLA scheme. Therefore, the AN attack is effective against these two schemes. As we mentioned, randomizing pilots and channel agreement can be effective in preventing these attacks.

VIII. Conclusion

In this paper we have compared three UA strategies, based on either symmetric/asymmetric keys or on physical layer authentication, where in all cases the authentication features are extracted from the communication channel. The comparison has been performed in terms of SAR, i.e., the rate at which the probability that UA security is broken goes to zero as the number of random variables describing the channel goes to infinity. From both the analysis and the numerical results we conclude that the A-CBCA scheme provides potentially the highest SAR and is immune to channel changes even when limited to using the channel estimation as a source of randomness. Then, the S-CBCA scheme, which uses the source-based SKA, is slightly more sensitive to the channel variations but has a lower bound on SAR that typically is higher than the SAR achieved with PLA. Moreover, PLA is the most sensitive solution to channel variations, which however can be mitigated by using a differential approach.

Appendix A
Proof of Lemma 2

We first observe that by the chain rule

$$\begin{aligned}&\mathbb{D}(p_{x_k(1),x_k(2t+1)|\mathcal{H}_0}||p_{x_k(1),x_k(2t+1)|\mathcal{H}_1})\\&\quad\le \mathbb{D}(p_{x_k(1),x_k(2t+1),\boldsymbol{z}_k(2t)|\mathcal{H}_0}||p_{x_k(1),x_k(2t+1),\boldsymbol{z}_k(2t)|\mathcal{H}_1}).\end{aligned} \tag{61}$$

Moreover, the KL divergence of the joint PDFs can be written as the expectation of KL divergence of conditioned PDFs, i.e., (62), as shown at the bottom of this page, where expectation is taken with respect to $\boldsymbol{z}_k(2t)$. Recalling that conditionally on $\boldsymbol{z}_k(2t)$, $x_k(1)$ and $x_k(2t+1)$ (as generated by Eve) are independent [29], we have

$$p_{x_k(1),x_k(2t+1)|\mathcal{H}_1,\boldsymbol{z}_k(2t)} = p_{x_k(1)|\mathcal{H}_1,\boldsymbol{z}_k(2t)}p_{x_k(2t+1)|\mathcal{H}_1,\boldsymbol{z}_k(2t)}. \tag{63}$$

Now, assuming that Eve does not attack in the ID-A frames, we have $p_{x_k(1)|\mathcal{H}_1,\boldsymbol{z}_k(2t)} = p_{x_k(1)|\mathcal{H}_0,\boldsymbol{z}_k(2t)}$. Moreover, if the attack has PDF $p_{x_k(2t+1)|\mathcal{H}_0,\boldsymbol{z}_k(2t)}$, we have

$$p_{x_k(2t+1)|\mathcal{H}_1,\boldsymbol{z}_k(2t)} = p_{x_k(2t+1)|\mathcal{H}_0,\boldsymbol{z}_k(2t)} \tag{64}$$

and therefore,

$$p_{x_k(1),x_k(2t+1)|\mathcal{H}_1,\boldsymbol{z}_k(2t)} = p_{x_k(1)|\mathcal{H}_0,\boldsymbol{z}_k(2t)}p_{x_k(2t+1)|\mathcal{H}_0,\boldsymbol{z}_k(2t)}, \tag{65}$$

and

$$\begin{aligned}&\mathbb{E}_{\boldsymbol{z}_k(2t)}[\mathbb{D}(p_{x_k(1),x_k(2t+1)|\mathcal{H}_0,\boldsymbol{z}_k(2t)}||\\&\qquad p_{x_k(1),x_k(2t+1)|\mathcal{H}_1,\boldsymbol{z}_k(2t)})]\\&\quad= \mathbb{E}_{\boldsymbol{z}_k(2t)}[\mathbb{D}(p_{x_k(1),x_k(2t+1)|\mathcal{H}_0,\boldsymbol{z}_k(2t)}||\\&\qquad p_{x_k(1)|\mathcal{H}_0,\boldsymbol{z}_k(2t)}p_{x_k(2t+1)|\mathcal{H}_0,\boldsymbol{z}_k(2t)})].\end{aligned} \tag{66}$$

Now, we also have the general relation between mutual information and KL divergence for any three random variables a, b and c, i.e.,

$$\mathbb{I}(a;b|c) = \mathbb{E}_c[\mathbb{D}(p_{a,b|c}||p_{a|c}p_{b|c})], \tag{67}$$

$$\mathbb{D}(p_{x_k(1),x_k(2t+1),\boldsymbol{z}_k(2t)|\mathcal{H}_0}||p_{x_k(1),x_k(2t+1),\boldsymbol{z}_k(2t)|\mathcal{H}_1}) = \mathbb{E}_{\boldsymbol{z}_k(2t)}[\mathbb{D}(p_{x_k(1),x_k(2t+1)|\mathcal{H}_0,\boldsymbol{z}_k(2t)}||p_{x_k(1),x_k(2t+1)|\mathcal{H}_1,\boldsymbol{z}_k(2t)})], \tag{62}$$

therefore, from (61) and (67) we obtain

$$\begin{aligned}&\mathbb{D}(p_{x_k(1),x_k(2t+1)|\mathcal{H}_0}||p_{x_k(1),x_k(2t+1)|\mathcal{H}_1})\\&\qquad\le \mathbb{I}(x_k(1);x_k(2t+1)|\mathcal{H}_0,\boldsymbol{z}_k(2t)),\end{aligned} \tag{68}$$

which by using (16) provides (17).

Appendix B
SAR for A-CBCA With Rayleigh Fading and LEP

We consider a uniform quantizer with saturation interval $[-v_{\rm sat}, v_{\rm sat}]$ and quantization step Δ. We first observe that the Rayleigh channel coefficient h_k has i.i.d. real and imaginary parts, therefore, the SAR will be twice the rate obtained considering the quantization of the real part, i.e.,

$$\begin{aligned}R_{\rm A-CBCA}(2t+1) = -2\sum_{i=0}^{M-1}\int p_{\langle y_k(2)\rangle|\hat{z}_k(2t)}(a_i|b)p_{\hat{z}_k(2t)}(b)\\ \times \log p_{\langle y_k(2)\rangle|\hat{z}_k(2t)}(a_i|b)\mathrm{d}b,\end{aligned} \tag{69}$$

For time-invariant channels and considering (T_{i-1}, T_i) as quantization interval for a_i we have

$$\begin{aligned}&p_{\langle y_k(2)\rangle|\hat{z}_k(2t)}(a_i|b)\\&\quad=\frac{1}{p_{\hat{z}_k(2t)}(b)}\\&\quad\quad\times\int_{-\infty}^{\infty}\mathbb{P}\left(h+\frac{\sigma_{\rm y}}{\sqrt{2}}w_{{\rm y},k}(2)\in(T_{i-1},T_i]\right)\\&\quad\quad\times p_{\hat{w}_{{\rm z},k}(2t)}\left(\frac{\sqrt{2}(b-h)}{\sigma_{\rm z}(2t)}\right)p_{h_k}(h)dh,\end{aligned} \tag{70}$$

where we used half of all noise variances since we are considering only the real part of the channel estimates. Now considering $v_{\rm sat}$ as the (positive) saturation value and $T_i = -v_{\rm sat} + \Delta i$, $T_{-1} = -\infty$, $T_M = \infty$, we have that the first function in (70) is

$$\begin{aligned}&\mathbb{P}\left(h+\frac{\sigma_{\rm y}}{\sqrt{2}}w_{{\rm y},k}(2)\in(T_{i-1},T_i]\right)\\&=\begin{cases}1-\mathrm{Q}\left(\frac{\sqrt{2}(-v_{\rm sat}+\Delta-h)}{\sigma_{\rm y}}\right) & i=0\\ \mathrm{Q}\left(\frac{\sqrt{2}(-v_{\rm sat}+\Delta i-h)}{\sigma_{\rm y}}\right) & i\in[1,M-2]\\ \quad-\mathrm{Q}\left(\frac{\sqrt{2}(-v_{\rm sat}+\Delta(i+1-h)}{\sigma_{\rm y}}\right) & \\ \mathrm{Q}\left(\frac{\sqrt{2}(-v_{\rm sat}+\Delta(M-1)-h)}{\sigma_{\rm y}}\right) & i=M-1,\end{cases}\end{aligned} \tag{71}$$

where i is the quantization index of $y_k(2)$. Moreover, for second and third functions in (70) we have

$$p_{h_k}(h) = \frac{1}{\sqrt{2\pi}}e^{-\frac{h^2}{2}}, \tag{72}$$

$$p_{\hat{w}_{{\rm z},k}(2t)}\left(\frac{\sqrt{2}(b-h)}{\sigma_{\rm z}(2t)}\right) = \frac{1}{\sigma_{\rm z}(2t)\sqrt{2\pi}}e^{-\frac{(h-b)^2}{2\sigma_{\rm z}^2(2t)}}. \tag{73}$$

Both integrals in (70) and in (69) must be solved by numerical methods.

Acknowledgment

The author would like to thank Nicola Laurenti for interesting discussions on the topics of this paper and the anonymous reviewers for their insightful suggestions that have improved the quality of this work.

References

[1] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 5th ed. Upper Saddle River, NJ, USA: Prentice Hall, 2010.

[2] G. J. Simmons, “Authentication theory/coding theory,” in *Proc. Adv. Cryptol.* Berlin, Germany: Springer-Verlag, 1985, pp. 411–431.

[3] G. J. Simmons, “A survey of information authentication,” *Proc. IEEE*, vol. 76, no. 5, pp. 603–620, May 1988.

[4] E. Jorswieck, S. Tomasin, and A. Sezgin, “Broadcasting into the uncertainty: Authentication and confidentiality by physical-layer processing,” *Proc. IEEE*, vol. 103, no. 10, pp. 1702–1724, Oct. 2015.

[5] L. Lai, H. El Gamal, and H. V. Poor, *Message Authentication: Information Theoretic Bounds*. Boston, MA, USA: Springer, 2010, pp. 335–353. [Online]. Available: https://doi.org/10.1007/978-1-4419-1385-2_14

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

[7] T. Daniels, M. Mina, and S. F. Russell, “Short paper: A signal fingerprinting paradigm for general physical layer and sensor network security and assurance,” in *Proc. 1st Int. Conf. Secur. Privacy Emerg. Areas Commun. Netw. (SECURECOMM)*, Sep. 2005, pp. 219–221.

[8] L. Xiao, L. J. Greenstein, N. B. Mandayam, and W. Trappe, “Channel-based spoofing detection in frequency-selective Rayleigh channels,” *IEEE Trans. Wireless Commun.*, vol. 8, no. 12, pp. 5948–5956, Dec. 2009.

[9] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, “Principles of physical layer security in multiuser wireless networks: A survey,” *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1550–1573, 3rd Quart., 2014.

[10] Y. Wang, S. Rane, S. C. Draper, and P. Ishwar, “A theoretical analysis of authentication, privacy, and reusability across secure biometric systems,” *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 6, pp. 1825–1840, Dec. 2012.

[11] T. Ignatenko and F. M. J. Willems, “Fundamental limits for privacy-preserving biometric identification systems that support authentication,” *IEEE Trans. Inf. Theory*, vol. 61, no. 10, pp. 5583–5594, Oct. 2015.

[12] S. Jiang, “Keyless authentication in a noisy model,” *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 6, pp. 1024–1033, Jun. 2014.

[13] J. Liu and X. Wang, “Physical layer authentication enhancement using two-dimensional channel quantization,” *IEEE Trans. Wireless Commun.*, vol. 15, no. 6, pp. 4171–4182, Jun. 2016.

[14] L. Xiao, T. Chen, G. Han, W. Zhuang, and L. Sun, “Game theoretic study on channel-based authentication in MIMO systems,” *IEEE Trans. Veh. Technol.*, vol. 66, no. 8, pp. 7474–7484, Aug. 2017.

[15] J. Zhang, T. Q. Duong, A. Marshall, and R. Woods, “Key generation from wireless channels: A review,” *IEEE Access*, vol. 4, pp. 614–626, 2016.

[16] S. Jiang, “On the optimality of keyless authentication in a noisy model,” *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 6, pp. 1250–1261, Jun. 2015.

[17] X. Wu, Z. Yang, C. Ling, and X. G. Xia, “Artificial-noise-aided message authentication codes with information-theoretic security,” *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 6, pp. 1278–1290, Jun. 2016.

[18] P. L. Yu, J. S. Baras, and B. M. Sadler, “Physical-layer authentication,” *IEEE Trans. Inf. Forensics Security*, vol. 3, no. 1, pp. 38–51, Mar. 2008.

[19] V. Boyko, “On the security properties of OAEP as an all-or-nothing transform,” in *Advances in Cryptology—CRYPTO*, M. Wiener, Ed. Berlin, Germany: Springer, 1999, pp. 503–518.

[20] R. Ahlswede and I. Csiszár, “Common randomness in information theory and cryptography. I. Secret sharing,” *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1121–1132, Jul. 1993.

[21] U. M. Maurer, “Secret key agreement by public discussion from common information,” *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, May 1993.

[22] C. L. K. Ngassa, R. Molière, F. Delaveau, A. Sibille, and N. Shapira, “Secret key generation scheme from WiFi and LTE reference signals,” *Analog Integr. Circuits Signal Process.*, vol. 91, no. 2, pp. 277–292, 2017. [Online]. Available: https://doi.org/10.1007/s10470-017-0941-3

[23] J. W. Wallace and R. K. Sharma, "Automatic secret keys from reciprocal MIMO wireless channels: Measurement and analysis," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 3, pp. 381–392, Sep. 2010.

[24] H. Taha and E. Alsusa, "Secret key exchange and authentication via randomized spatial modulation and phase shifting," *IEEE Trans. Veh. Technol.*, vol. 67, no. 3, pp. 2165–2177, Mar. 2018.

[25] J. K. Tugnait, "Wireless user authentication via comparison of power spectral densities," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1791–1802, Sep. 2013.

[26] L. Xiao, L. J. Greenstein, N. B. Mandayam, and W. Trappe, "Using the physical layer for wireless authentication in time-variant channels," *IEEE Trans. Wireless Commun.*, vol. 7, no. 7, pp. 2571–2579, Jul. 2008.

[27] F. J. Liu, X. Wang, and S. L. Primak, "A two dimensional quantization algorithm for CIR-based physical layer authentication," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2013, pp. 4724–4728.

[28] S. Tomasin, "Comparison between asymmetric and symmetric channel-based authentication for MIMO systems," in *Proc. 21st Int. ITG Workshop Smart Antennas*, Mar. 2017, pp. 1–5.

[29] A. Ferrante, N. Laurenti, C. Masiero, M. Pavon, and S. Tomasin, "On the error region for channel estimation-based physical layer authentication over Rayleigh fading," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 5, pp. 941–952, May 2015.

[30] U. M. Maurer, "Authentication theory and hypothesis testing," *IEEE Trans. Inf. Theory*, vol. 46, no. 4, pp. 1350–1356, Jul. 2000.

[31] U. Maurer, "Information-theoretic cryptography," in *Advances in Cryptology—CRYPTO*, M. Wiener, Ed. Berlin, Germany: Springer, 1999, pp. 47–65.

[32] L. Trevisan and S. Vadhan, "Extracting randomness from samplable distributions," in *Proc. 41st Annu. Symp. Found. Comput. Sci.*, 2000, pp. 32–42.

[33] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge, U.K.: Cambridge Univ. Press, 2011.

[34] J. L. Carter and M. N. Wegman, "Universal classes of hash functions," *J. Comput. Syst. Sci.*, vol. 18, no. 2, pp. 143–154, Apr. 1979. [Online]. Available: http://www.sciencedirect.com/science/article/pii/0022000079900448

[35] E. T. Jaynes, "Information theory and statistical mechanics," *Phys. Rev.*, vol. 106, no. 4, pp. 620–630, May 1957.

[36] T. M. Cover and J. A. Thomas, *Elements of Information Theory* (Telecommunications and Signal Processing). Hoboken, NJ, USA: Wiley, 2006.

[37] D. Kapetanović, G. Zheng, K.-K. Wong, and B. Ottersten, "Detection of pilot contamination attack using random training and massive MIMO," in *Proc. IEEE 24th Annu. Int. Symp. Pers., Indoor, Mobile Radio Commun. (PIMRC)*, Sep. 2013, pp. 13–18.

[38] S. Tomasin, I. Land, and F. Gabry, "Pilot contamination attack detection by key-confirmation in secure MIMO systems," in *Proc. IEEE Global Conf. Commun. (GLOBECOM)*, Dec. 2016, pp. 1–7.

Stefano Tomasin (SM'11) received the Ph.D. degree in telecommunications engineering from the University of Padova, Italy, in 2003. In 2002, he joined the University of Padova, where he is currently an Associate Professor. He has been on leave at Philips Research, Eindhoven, The Netherlands, in 2002, Qualcomm Research Laboratories, San Diego, CA, USA, in 2004, Polytechnic University, Brooklyn, NY, USA, in 2007, and the Huawei Mathematical and Algorithmic Sciences Laboratory, Boulogne-Billancourt, France, in 2014. His current research interests include physical layer security and signal processing for wireless communications, with application to 5th generation cellular systems. From 2011 to 2017, he was an Editor of the IEEE TRANSACTIONS OF VEHICULAR TECHNOLOGIES. He has been an Editor of the *EURASIP Journal of Wireless Communications and Networking* since 2011 and the IEEE TRANSACTIONS ON SIGNAL PROCESSING since 2016.