Worst-Case Spoofing Attack and Robust Countermeasure in Satellite Navigation Systems

Laura Crosara, *Graduate Student Member, IEEE*, Francesco Ardizzon, *Member, IEEE*, Stefano Tomasin, *Senior Member, IEEE*, and Nicola Laurenti

***Abstract*— The threat of signal spoofing attacks against global navigation satellite system (GNSS) has grown in recent years and has motivated the study of anti-spoofing techniques. However, defense methods have been designed only against specific attacks. This paper introduces a general model of the spoofing attack framework in GNSS, from which optimal attack and defense strategies are derived. We consider a scenario with a legitimate receiver (Bob) testing if the received signals come from multiple legitimate space vehicles (Alice) or from an attack device (Eve). We first derive the optimal attack strategy against a Gaussian transmission from Alice, by minimizing an outer bound on the achievable error probability region of the spoofing detection test. Then, framing the spoofing and its detection as an adversarial game, we show that the Gaussian transmission and the corresponding optimal attack constitute a Nash equilibrium. Lastly, we consider the case of practical modulation schemes for Alice and derive the generalized likelihood ratio test. Numerical results validate the analytical derivations and show that the bound on the achievable error region is representative of the actual performance.**

***Index Terms*— Spoofing, global navigation satellite systems (GNSSs), signal authentication, physical-layer security.**

I. Introduction

A GROWING number of location-based services rely on GNSSs for positioning and timing, but the widespread adoption of GNSSs has also increased the incentive to mount attacks against them [1]. In particular, the spoofing attack refers to the transmission of counterfeit GNSS-like signals with the intent to produce a wrong position computation at the receiver [1], [2], [3], as represented in Fig. 1.

Recent news has raised concerns about GNSS security since attacks can be performed with inexpensive programmable signal generators and commercial off-the-shelf (COTS) hardware. We thus need to authenticate the GNSS signals, especially when used in contexts where its malfunctioning puts people's safety at risk. Attacks include meaconing, selective delay, distance-decreasing [4], and secure code estimation and replay (SCER) attacks [5], [6]. In particular, the latter can deal with ranging signals protected by cryptography, as it can be used to estimate the message signature and then reconstruct the signal in real time.

In the last decade, the GNSS community has investigated anti-spoofing authentication techniques operating at both data and ranging-code levels. In this paper, we focus on the authentication of the ranging signal at code level, through physical layer-based mechanisms exploiting the channel diversity, regardless of higher layers (e.g., message-level) authentication mechanisms.

Spreading code encryption (SCE) is the most effective option to authenticate the GNSS signals, as it makes the spreading code fully unpredictable for the attacker, thus preventing generation attacks [7]. Moreover, when using SCE, SCER-type attacks have limited success in estimating each spreading code chip from the noisy received signal, as the chip period is typically several orders of magnitude lower than the message symbol period [8]. Some SCE solutions are the P(Y) code for GPS and the commercial authentication service (CAS) for Galileo [9], [10], where the encryption key is derived from the unpredictable signature of Galileo open service navigation message authentication (OS-NMA) [11], [12].

Initially proposed in [13], spreading code authentication (SCA) represents a modification of SCE making use of signal watermarking. A similar SCA technique was presented in [14], where short sequences of spread spectrum security codes (SSSCs) are used to modify the spreading code. This design approach has evolved in [15], and has been applied in [16] and [17], where the scheme called chips-message robust authentication (CHIMERA) is introduced. CHIMERA aims at jointly authenticating both the navigation data and the spreading code of GPS signals for civil usage. Other examples of SCA techniques for open GNSS signals, each employing different methods for generating and placing the watermarked chips, were introduced in [18], [19], [20], and [21]. However, existing anti-spoofing mechanisms are designed as a particular solution without any optimality criterion. Moreover, their performance is evaluated against specific attacks, which may not represent the worst-case scenario for the design mechanism, and do not guarantee system defense against attacks of different types.

A first unified general model for the design, description, evaluation, and comparison of SCA techniques was presented

Manuscript received 10 February 2023; revised 31 July 2023 and 31 October 2023; accepted 26 November 2023. Date of publication 5 December 2023; date of current version 29 December 2023. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. Haijun Zhang. *(Corresponding author: Laura Crosara.)*

Laura Crosara and Francesco Ardizzon are with the Department of Information Engineering, Università degli Studi di Padova, 35131 Padua, Italy (e-mail: crosaralau@dei.unipd.it; ardizzonfr@dei.unipd.it).

Stefano Tomasin and Nicola Laurenti are with the Department of Information Engineering, Università degli Studi di Padova, 35131 Padua, Italy, and also with the National Inter-University Consortium for Telecommunications (CNIT), 43124 Parma, Italy (e-mail: tomasin@dei.unipd.it; nil@dei.unipd.it).

Digital Object Identifier 10.1109/TIFS.2023.3340061

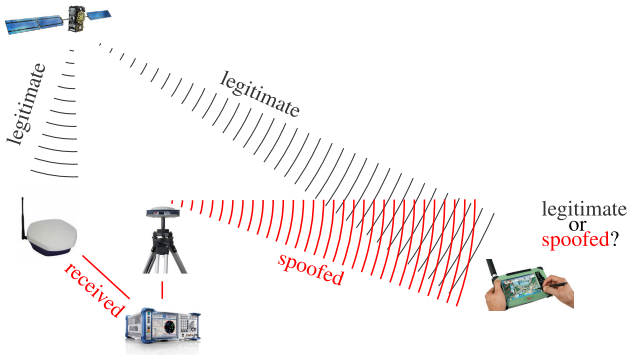

Fig. 1. Spoofing scenario.

in [22], where an optimal compromise is achieved between security and the number of random bits in the watermark. However, the security is only evaluated in terms of conditional guessing probability for the watermarked code given the public one, thereby neglecting the effects of channel transmission, noise, and possible SCER attacks. On the other hand, in [23] a signal authentication method based on physical layer secrecy is presented, in which the navigation signal is transmitted along with a synchronous and orthogonal authentication signal, encoded for secrecy and corrupted by artificial noise (AN). A general security result follows from the impossibility of a spoofer to decode the authentication signal without knowledge of the AN, which is later disclosed for verification. However, a totally general framework for deriving a wide class of solutions, optimizing their parameters, and evaluating their security against a broad set of attacks is still lacking.

This paper makes the following contributions. First, we describe a general model to characterize the spoofing attack in GNSS, considering the presence of multiple space vehicles (SVs), a victim receiver, and an attacker. We describe the optimal attack strategy that minimizes the Kullback-Leibler (K-L) divergence between the received signal distribution in nominal and attack conditions, while still introducing the desired shifts on the satellites' signals. Indeed, the K-L divergence gives an outer bound to the detection error tradeoff (DET) curve (determined by false alarm and missed detection probabilities), which in turn is the appropriate metric to assess the capabilities of the victim receiver in detecting the attack. Therefore, the proposed optimization procedure provides an optimal attack abstracting from the particular detection process, whose efficacy can be assessed beforehand.

For a general class of attack strategies, we derive a closed-form expression for the K-L divergence and a lower bound that only depends on the GNSS scenario and channel physical parameters, regardless of the specific detection strategy adopted by the victim. Then, framing the spoofing and its detection as an adversarial game, we prove that the set of strategies comprised of a Gaussian transmission and the optimal attack is a Nash equilibrium for the game. Moreover, we discuss the K-L divergence obtained at the equilibrium points. Next, we consider the case of practical modulation schemes for Alice and derive the generalized likelihood ratio test. Finally, simulation results for the attack-defense scheme are presented, considering both likelihood ratio test (LRT) and generalized likelihood ratio test (GLRT) attack detection mechanisms. The results validate the analytical derivations and show that the bound on the achievable error region given by the K-L divergence is representative of the actual performance.

The rest of this paper is organized as follows. Section II presents the general GNSS spoofing model in detail, together with performance metrics. In Section III the optimal attack strategy is derived, then analytical results are presented. Defense strategies at both the transmitter and the receiver are discussed in Section IV. Then, numerical results are presented in Section V. Section VI draws the conclusions of the paper.

Notation: Vectors and matrices are denoted by lower and upper case boldface letters, respectively. Symbol $\boldsymbol{A}^{\mathrm{H}}$ denotes the complex conjugate transpose of matrix $\boldsymbol{A}$, while $\boldsymbol{A}^{\dagger}$ denotes the Moore-Penrose pseudo inverse of $\boldsymbol{A}$. Symbol $\boldsymbol{I}_n$, denotes the identity matrix of size $n \times n$, $|\boldsymbol{A}|$ and $\|\boldsymbol{A}\|_F$ stand for the determinant and the Frobenius norm of $\boldsymbol{A}$, respectively. Given two random variables x and y, p_x represents the probability density function (pdf) of x, $p_{x|y}$ represents the conditional pdf of x given y, and p_{xy} represents the joint pdf of x and y. If $\boldsymbol{a} \in \mathbb{C}^n$ and $\boldsymbol{b} \in \mathbb{C}^m$ are random vectors, $\boldsymbol{K}_{ab} = \mathbb{E}[\boldsymbol{a}\boldsymbol{b}^{\mathrm{H}}]$ denotes their $n \times m$ covariance matrix. Finally, log denotes the natural logarithm.

II. System Model

We consider a constellation of m SVs (Alice, block A in Fig. 2) transmitting signals to a receiver (Bob, block B in Fig. 2). By estimating the relative delay among signals received from the m SVs and by knowing the position of the SVs, Bob estimates its position through ranging techniques [24]. A third device (Eve, block E in Fig. 2) receives the signals from the SVs and transmits to Bob. The aim of Bob is to authenticate the received signal, i.e., to determine whether it comes from Alice or Eve. In turn, Eve aims at transmitting signals that can be confused as authentic by Bob but induce a different position estimation. A reliable and asynchronous side communication channel (which cannot be used for position estimation) enables the transmission of authenticated data from Alice to Bob, while Eve cannot access it to build the attack. A possible way to implement this channel is through delayed authentication techniques [25]. In this paper, we investigate how Alice can transmit its signals (on both the main and the side channels) and how Bob can perform the verification step of the authentication procedure. Also, we study possible attack strategies by Eve.

A. Transmission Procedure

The i-th SV, $i \in \{1, 2, \ldots, m\}$, broadcasts a radio signal represented by its discrete-time complex baseband equivalent vector $\bar{\boldsymbol{x}}_i \in \mathbb{C}^n$, with $\bar{\boldsymbol{x}}_i$ independent from $\bar{\boldsymbol{x}}_j$ if $i \neq j$. We define the transmitted word $\boldsymbol{x}$ as the concatenation of the signals transmitted by all SVs: $\boldsymbol{x} = [\bar{\boldsymbol{x}}_1, \bar{\boldsymbol{x}}_2, \ldots, \bar{\boldsymbol{x}}_m] \in \mathbb{C}^{mn}$; word $\boldsymbol{x}$ is also delivered to Bob over the side channel. It is important to note that the side information can also be a compressed lossless version of the transmitted word $\boldsymbol{x}$. Two delays are associated to each signal $\bar{\boldsymbol{x}}_i$, namely $\tau_{\mathrm{B},i}$ and $\tau_{\mathrm{E},i}$, indicating the propagation time of $\bar{\boldsymbol{x}}_i$ from the i-th SV to Bob and to Eve, respectively. Without loss of generality we assume $\min_i\{\tau_{\mathrm{B},i}\} = \min_i\{\tau_{\mathrm{E},i}\} = 0$, so that vectors

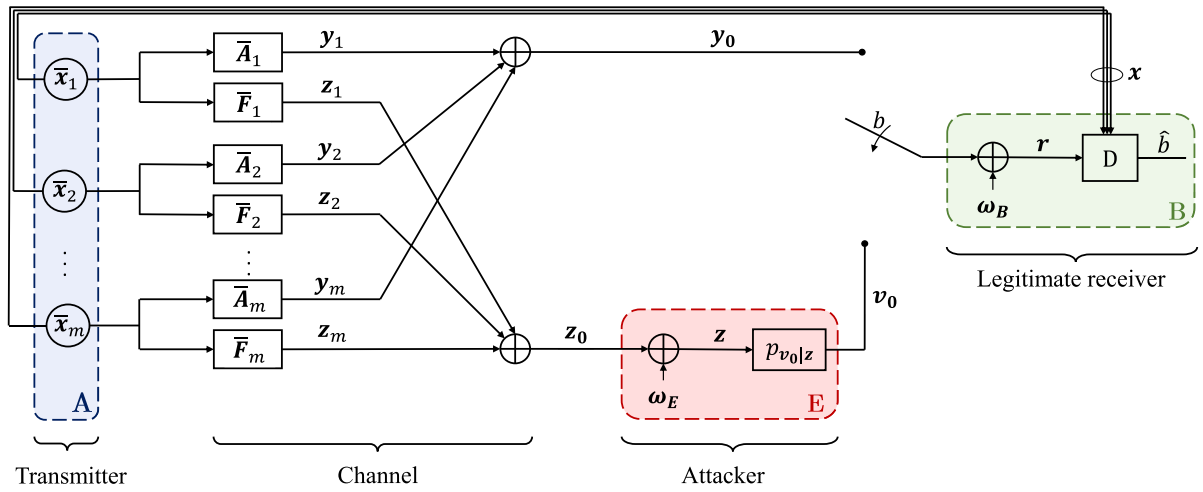

Fig. 2. Anti-spoofing authentication model.

$\boldsymbol{\tau}_{\mathrm{B}} = [\tau_{\mathrm{B},1}, \tau_{\mathrm{B},2}, \ldots, \tau_{\mathrm{B},m}]$ and $\boldsymbol{\tau}_{\mathrm{E}} = [\tau_{\mathrm{E},1}, \tau_{\mathrm{E},2}, \ldots, \tau_{\mathrm{E},m}]$ collect the relative delays between the signals coming from the m satellites. Moreover, we define $\delta_{\mathrm{B}} = \max_i\{\tau_{\mathrm{B},i}\}$ and $\delta_{\mathrm{E}} = \max_i\{\tau_{\mathrm{E},i}\}$.

Signal $\bar{\boldsymbol{x}}_i$, $i \in \{1, 2, \ldots, m\}$, is transmitted through two linear channels $\boldsymbol{y}_i = \bar{\boldsymbol{A}}_i\bar{\boldsymbol{x}}_i$ and $\boldsymbol{z}_i = \bar{\boldsymbol{F}}_i\bar{\boldsymbol{x}}_i$, providing the useful signals received by Bob and Eve, respectively. Matrices $\bar{\boldsymbol{A}}_i$ and $\bar{\boldsymbol{F}}_i$ are determined by relative delays between signals, the fading environment, fluctuations in atmospheric parameters, signal distortion, and channel gains. Moreover, $\bar{\boldsymbol{A}}_i$ and $\bar{\boldsymbol{F}}_i$ include proper padding to guarantee that each channel output vector has the same size. We denote the concatenation of matrices $\bar{\boldsymbol{A}}_i$ and $\bar{\boldsymbol{F}}_i$, for $i = 1, 2, \ldots, m$, as $\boldsymbol{A} = [\bar{\boldsymbol{A}}_1, \bar{\boldsymbol{A}}_2, \ldots, \bar{\boldsymbol{A}}_m] \in \mathbb{C}^{(n+\delta_{\mathrm{B}})\times(mn)}$ and $\boldsymbol{F} = [\bar{\boldsymbol{F}}_1, \bar{\boldsymbol{F}}_2, \ldots, \bar{\boldsymbol{F}}_m] \in \mathbb{C}^{(n+\delta_{\mathrm{E}})\times(mn)}$.

In nominal conditions, Bob and Eve receive the sum of the signals coming from the m satellites, respectively

$$\boldsymbol{y}_0 = \sum_{i=1}^{m} \boldsymbol{y}_i = \boldsymbol{A}\boldsymbol{x}, \quad \boldsymbol{z}_0 = \sum_{i=1}^{m} \boldsymbol{z}_i = \boldsymbol{F}\boldsymbol{x}. \tag{1}$$

Furthermore, $\boldsymbol{y}_0$ and $\boldsymbol{z}_0$ are corrupted by additive Gaussian noise, represented by two circularly symmetric complex Gaussian random vectors $\boldsymbol{\omega}_{\mathrm{B}} \sim \mathcal{CN}(\boldsymbol{0}, \boldsymbol{K}_{\mathrm{B}})$ and $\boldsymbol{\omega}_{\mathbf{E}} \sim \mathcal{CN}(\boldsymbol{0}, \boldsymbol{K}_{\mathrm{E}})$, respectively as

$$\boldsymbol{y} = \boldsymbol{y}_0 + \boldsymbol{\omega}_{\mathbf{B}}, \quad \boldsymbol{z} = \boldsymbol{z}_0 + \boldsymbol{\omega}_{\mathbf{E}}. \tag{2}$$

B. Attack Strategy

The goal of Eve is to falsify the propagation times by introducing the forged delays $\boldsymbol{\tau}_{\mathrm{f}} = [\tau_{\mathrm{f},1}, \tau_{\mathrm{f},2}, \ldots, \tau_{\mathrm{f},m}]$ corresponding the spoofed position, velocity, and time (PVT).

We assume that: (i) Eve does not know $\boldsymbol{x}$ but only knows $\boldsymbol{z}$, which is a noisy and reduced-size version of $\boldsymbol{x}$; (ii) Eve knows the joint distribution of $\boldsymbol{x}$, $\boldsymbol{y}$, and $\boldsymbol{z}$; (iii) Eve knows the forged channel A $\rightarrow$ B, and the actual channels A $\rightarrow$ E, and E $\rightarrow$ B, and the corresponding noise statistics[1]; (iv) Eve is able to cancel the signal $\boldsymbol{y}_0$ at Bob, thus Bob acquires and locks onto the spoofed signal $\boldsymbol{v}$ [27]. Note that assumption (iv) is very favorable to the attacker, thus our results are obtained in a worst case scenario. Thus, when under attack, the signal received by Bob is

$$\boldsymbol{v} = \boldsymbol{v}_0 + \boldsymbol{\omega}_{\mathbf{B}}, \tag{3}$$

where $\boldsymbol{v}$, $\boldsymbol{v}_0 \in \mathbb{C}^{n+\delta_{\mathrm{f}}}$, with $\delta_{\mathrm{f}} = \max \boldsymbol{\tau}_f$.

Assumption (iii) is realistic in a self-spoofing scenario, where the attacker has access to the legitimate receiver channel. Assumptions (iii) and (iv) are favorable to the attacker, thus representing a worst-case scenario that is commonly assumed in the security literature for the design of robust security mechanisms, and establishes an upper bound on the achievable error region. In other terms, in practical conditions, the authentication procedure will perform at least as well as under the considered assumptions. We remark that the attacker cannot process each satellite signal separately: such processing would in fact require the knowledge of each word $\bar{\boldsymbol{x}}_i$, $i = 1, \ldots, m$.

While we consider a single attacker, the multiple attacker's scenario can be cast into our model by considering a block of rows for each attacker in matrix $\mathbf{F}$: with N spoofers, the size of $\mathbf{F}$ will be $(Nn + \delta_N) \times (mn)$, where $\delta_N = \sum_{i=1}^{N} \delta_{\mathrm{E},i}$.

Concerning the attacker strategy, Eve can exploit the information carried by her observations $\boldsymbol{z}$ and, for the sake of generality, we consider that Eve adopts a probabilistic strategy, characterized by the conditional pdf $p_{\boldsymbol{v}_0|\boldsymbol{z}}$. Moreover, since Eve knows the statistics of the noise at Bob, the attack strategy can be described by $p_{\boldsymbol{v}|\boldsymbol{z}}$. The observation $\boldsymbol{z}$ encloses all the information Eve can exploit to deceive Bob, so the forging strategy $\boldsymbol{v}$ is conditionally independent of the transmitted word $\boldsymbol{x}$, given $\boldsymbol{z}$.

Finally, let the received signal by Bob be

$$\boldsymbol{r} = \begin{cases} \boldsymbol{y} & \text{if Bob is locked on the legitimate signal } (b = 0) \\ \boldsymbol{v} & \text{if Bob is locked on the spoofing signal } (b = 1), \end{cases} \tag{4}$$

[1]In [26], we analyzed the system performance when neither Bob nor Eve have perfect channel state information (CSI) and have to rely on noisy estimates of matrices $\boldsymbol{A}$ and $\boldsymbol{F}$.

where b indicates the legitimate/attack state. Therefore, Eve aims at preventing Bob from distinguishing between $\boldsymbol{v}$ and the legitimate $\boldsymbol{y}$ that would be obtained with $\boldsymbol{\tau}_{\mathrm{B}} = \boldsymbol{\tau}_{\mathrm{f}}$.

C. Authentication Procedure

The goal of the legitimate receiver Bob is to figure out whether the received signal $\boldsymbol{r}$ corresponds to the authentic signal $\boldsymbol{y}$, or the spoofed signal $\boldsymbol{v}$, by using his knowledge of $\boldsymbol{x}$, disclosed by Alice through the side channel. To detect the spoofing attack, Bob performs an authentication test, wherein, given $\boldsymbol{x}$ and $\boldsymbol{r}$, Bob chooses between the two hypotheses:

$$\mathcal{H}_0 : \boldsymbol{r} = \boldsymbol{y}, \text{ the message is from Alice,} \tag{5}$$

$$\mathcal{H}_1 : \boldsymbol{r} = \boldsymbol{v}, \text{ the message was forged.} \tag{6}$$

The authentication procedure is summarized in block D, which has the received signal $\boldsymbol{r}$ as input and outputs the Boolean value $\hat{b}$. Correct verification is achieved when $\hat{b}$=b.

It is worth noting that the model of Fig. 2 represents a general GNSS spoofing framework as we make no assumptions about the structure of $\boldsymbol{x}$, apart from a power constraint. Similarly, we do not restrict the attack strategy, which is described by any pdf $p_{\boldsymbol{v_0}|\boldsymbol{z}}$. We assume that $\boldsymbol{x}$ is completely (rather than partially) known to the receiver at the time of verification. Although generous to the defender, this assumption has been considered in all the authentication schemes proposed so far [9], [15], [16], [23].

The parameters of our model can be set to represent other models from the literature. The CHIMERA scheme proposed in [15], [16], and [17] considers only one satellite and part of the spreading code is superimposed with a secret sequence, cryptographically generated from a key. This can be cast into our model by taking $m = 1$ and considering as word $\boldsymbol{x}$ the signal obtained by the superposition of the signed navigation data with the signed version of the spreading code, followed by a binary phase-shift keying (BPSK) modulation. Then, with a delay with respect to $\boldsymbol{x}$, the key to reconstructing the secret sequence is broadcast as side information. A similar approach can be adopted to describe Galileo CAS [9], [10] combined with OS-NMA [11], [12]. The model in [22] can be cast into this frame by restricting $\boldsymbol{x}$ to be a binary watermarking sequence, and the attacker to have complete ignorance on it, thus, removing his observation $\boldsymbol{z}$. In the authentication scheme of [23], $\boldsymbol{x}$ is the superposition of the transmitted authentication message and the AN component. Then, the authentication message and the AN are transmitted to the legitimate receiver through an authenticated channel.

All the parameters presented in this Section are summarized in Table I.

TABLE I
SYSTEM PARAMETERS, $i \in 1, 2, \ldots, m$

Symbol	Definition
m	Number of satellites
n	Length of the discrete time signal $\boldsymbol{x}_i$
$\boldsymbol{x}_i$	Discrete time signal transmitted by the i-th SV
$\boldsymbol{x}$	Transmitted word
$\tau_{\mathrm{B},i}$	Propagation time of $\boldsymbol{x}_i$ from the i-th SV to B
$\tau_{\mathrm{E},i}$	Propagation time of $\boldsymbol{x}_i$ from the i-th SV to E
$\tau_{\mathrm{f},i}$	False propagation time related to $\boldsymbol{x}_i$
$\boldsymbol{\tau}_{\mathrm{B}}$	Vector of propagation times from A to B
$\boldsymbol{\tau}_{\mathrm{E}}$	Vector of propagation times from A to E
$\boldsymbol{\tau}_{\mathrm{f}}$	Vector of false propagation times introduced by E
δ_{B}	Largest propagation time of signals traveling from A to B
δ_{E}	Largest propagation time of signals traveling from A to E
δ_{f}	Largest propagation time of signals traveling from E to B
$\boldsymbol{A}$	A$\rightarrow$ B channel matrix
$\boldsymbol{F}$	A$\rightarrow$ E channel matrix
$\boldsymbol{\omega}_{\mathrm{B}}$	Noise in the channel A$\rightarrow$ B and E$\rightarrow$ B
$\boldsymbol{\omega}_{\mathrm{E}}$	Noise in the channel A$\rightarrow$ E
$\boldsymbol{K}_{\mathrm{B}}$	Covariance matrix of $\boldsymbol{\omega}_{\mathrm{B}}$
$\boldsymbol{K}_{\mathrm{E}}$	Covariance matrix of $\boldsymbol{\omega}_{\mathrm{E}}$
$\boldsymbol{y}$	Received signal through the channel A$\rightarrow$ B
$\boldsymbol{z}$	Received signal through the channel A$\rightarrow$ E
$\boldsymbol{v_0}$	Signal generated by E
$\boldsymbol{v}$	Received signal through the channel E$\rightarrow$ B
$\boldsymbol{r}$	Signal received by B
$\hat{b}$	Decision made by the receiver B
b	Correct value for $\hat{b}$

D. Performance Metric

The performance of an authentication system is assessed by: *a)* the type-I (false alarm) error probability p_{FA}, i.e., the probability that Bob discards a message as forged by Eve while it is coming from Alice; *b)* the type-II (missed detection) error probability p_{MD}, i.e., the probability that Bob accepts a message coming from Eve as legitimate. The LRT is the optimal detection method that minimizes the false alarm probability for a fixed missed detection given $p_{\boldsymbol{x}}$, and $p_{\boldsymbol{v}|\boldsymbol{z}}$ [28]. However, in general, the analytical derivation of these pdf is hardly feasible. Therefore, theoretical bounds on the achievable error probability region, which is the set of achievable points in the $(p_{\mathrm{FA}}, p_{\mathrm{MD}})$ plane, are useful to establish the effectiveness of practical schemes.

A first bound for a given attack strategy is given by the K-L divergence. In fact, from [29] and [30] we have

$$\mathbb{D}(p_{\hat{b}|\mathcal{H}_1} \| p_{\hat{b}|\mathcal{H}_0}) \leq \mathbb{D}(p_{\boldsymbol{rx}|\mathcal{H}_1} \| p_{\boldsymbol{rx}|\mathcal{H}_0}) = \mathbb{D}(p_{\boldsymbol{xv}} \| p_{\boldsymbol{xy}}). \tag{7}$$

In (7) we have considered $p_{\boldsymbol{rx}}$ since we suppose that, at the time of verification, the legitimate receiver knows $\boldsymbol{x}$, and the decision $\hat{b}$ is taken based on both inputs. Therefore, defining the function

$$h(p_{\mathrm{MD}}, p_{\mathrm{FA}}) \triangleq p_{\mathrm{MD}} \log \frac{p_{\mathrm{MD}}}{1 - p_{\mathrm{FA}}} + (1 - p_{\mathrm{MD}}) \log \frac{1 - p_{\mathrm{MD}}}{p_{\mathrm{FA}}}, \tag{8}$$

and observing that $p_{\hat{b}|\mathcal{H}_0}(1) = p_{\mathrm{FA}}$, $p_{\hat{b}|\mathcal{H}_0}(0) = 1 - p_{\mathrm{FA}}$, $p_{\hat{b}|\mathcal{H}_1}(1) = 1 - p_{\mathrm{MD}}$ and $p_{\hat{b}|\mathcal{H}_1}(0) = p_{\mathrm{MD}}$, (7) can be rewritten as

$$h(p_{\mathrm{MD}}, p_{\mathrm{FA}}) \leq \mathbb{D}(p_{\boldsymbol{xv}} \| p_{\boldsymbol{xy}}). \tag{9}$$

This limits the region of achievable $(p_{\mathrm{FA}}, p_{\mathrm{MD}})$ values, depending on $\mathbb{D}(p_{\boldsymbol{xv}} \| p_{\boldsymbol{xy}})$, for any decision mechanism choice.[2]

On one hand, the aim of the attacker Eve is to narrow the achievable region, by making the value of $\mathbb{D}(p_{\boldsymbol{xv}} \| p_{\boldsymbol{xy}})$ as small as possible, operating on the attack strategy $p_{\boldsymbol{v}|\boldsymbol{z}}$.

[2]The bound in (9) is tight when Bob knows Eve's attack strategy and Eve does not know Bob's defense strategy. However, the bound also holds in the case of interest, where Bob does not know what Eve does and Eve knows what Bob does.

On the other hand, Alice aims at enlarging the achievable region, by properly choosing the distribution of the transmitted word $\boldsymbol{x}$ in order to increase $\mathbb{D}(p_{\boldsymbol{xv}}\|p_{\boldsymbol{xy}})$. Therefore, the defense strategy is defined by the pdf $p_{\boldsymbol{x}}$.

The metric $\mathbb{D}(p_{\boldsymbol{xv}}\|p_{\boldsymbol{xy}})$ can be expressed in terms of attack and defense strategies as

$$\begin{aligned}\mathbb{D}(p_{\boldsymbol{xv}}\|p_{\boldsymbol{xy}}) &= \iint p_{\boldsymbol{x}}(a)\,p_{\boldsymbol{v}|\boldsymbol{x}}(b|a)\log\frac{p_{\boldsymbol{v}|\boldsymbol{x}}(b|a)}{p_{\boldsymbol{y}|\boldsymbol{x}}(b|a)}\mathrm{d}a\,\mathrm{d}b\\ &= \iint p_{\boldsymbol{x}}(a)\int p_{\boldsymbol{v}|\boldsymbol{z}}(b|c)\,p_{\boldsymbol{z}|\boldsymbol{x}}(c|a)\,\mathrm{d}c\\ &\quad\cdot\log\frac{\int p_{\boldsymbol{v}|\boldsymbol{z}}(b|c)\,p_{\boldsymbol{z}|\boldsymbol{x}}(c|a)\mathrm{d}c}{p_{\boldsymbol{y}|\boldsymbol{x}}(b|a)}\,\mathrm{d}a\,\mathrm{d}b. \qquad (10)\end{aligned}$$

Highlighting the contribution of attack and defense strategies, let us define

$$f(p_{\boldsymbol{x}},\,p_{\boldsymbol{v}|\boldsymbol{z}}) \triangleq \mathbb{D}(p_{\boldsymbol{xv}}\|p_{\boldsymbol{xy}}), \qquad (11)$$

with fixed channels $p_{\boldsymbol{y}|\boldsymbol{x}}$ and $p_{\boldsymbol{z}|\boldsymbol{x}}$. So, the task that we will address in this paper from the point of view of the defense is defined by the following maximin problem:

$$\max_{p_{\boldsymbol{x}}}\ \min_{p_{\boldsymbol{v}|\boldsymbol{z}}} f(p_{\boldsymbol{x}},\,p_{\boldsymbol{v}|\boldsymbol{z}}). \qquad (12)$$

An important difference that distinguishes attack and defense strategies is that Eve knows the value of $\boldsymbol{\tau}_{\mathbf{E}}$ and the victim position exactly, whereas Alice's defense strategy must be robust and symmetrical with respect to all potential receiver and channel realizations, described by matrices $\boldsymbol{A}$ and $\boldsymbol{F}$.

In Section III we will first address the inner minimization in (12), considering the model presented in Section II and assuming that $\boldsymbol{x}$ is Gaussian distributed. Then, after discussing the achievable K-L divergence values, the maximization task in (12) will be finally investigated in Section IV.

III. Attack Strategy

We now focus on the attack strategy optimization, i.e., from (12), we aim at deriving the conditional pdf $p_{\boldsymbol{v}|\boldsymbol{z}}$ such that

$$p^{\star}_{\boldsymbol{v}|\boldsymbol{z}} = \arg\min_{p_{\boldsymbol{v}|\boldsymbol{z}}}\ f(p_{\boldsymbol{x}},\,p_{\boldsymbol{v}|\boldsymbol{z}}). \qquad (13)$$

We assume that $p_{\boldsymbol{x}} \sim \mathcal{N}(0,\,\boldsymbol{K}_{\boldsymbol{x}})$ and the optimality of this choice will be proven in Section IV-A. Under this assumption, there exists an optimal attack $p^{\star}_{\boldsymbol{v}|\boldsymbol{z}}$ minimizing the divergence in (11) [31].

Theorem 1: Given the zero mean, jointly Gaussian random vectors $\boldsymbol{x}$, $\boldsymbol{y}$, and $\boldsymbol{z}$, the attack solving (13) with fixed channels $p_{\boldsymbol{y}|\boldsymbol{x}}$ and $p_{\boldsymbol{z}|\boldsymbol{x}}$, under the constraint that the random vectors $\boldsymbol{v}$ and $\boldsymbol{x}$ are conditionally independent given $\boldsymbol{z}$, belongs to the class

$$\mathcal{C} = \left\{p_{\boldsymbol{v}|\boldsymbol{z}} \sim \mathcal{N}(\boldsymbol{G}\boldsymbol{z},\,\boldsymbol{C}\boldsymbol{C}^{\mathrm{H}} + \boldsymbol{K}_{\mathbf{B}})\right\}, \qquad (14)$$

therefore the optimal attack can be modeled as

$$\boldsymbol{v} = \boldsymbol{G}\boldsymbol{z} + \boldsymbol{C}\boldsymbol{\omega}_{\mathbf{c}} + \boldsymbol{\omega}_{\mathbf{B}}, \qquad (15)$$

where $\boldsymbol{G} \in \mathbb{C}^{(n+\delta_{\mathrm{f}})\times(n+\delta_{\mathrm{E}})}$ and $\boldsymbol{C} \in \mathbb{C}^{(n+\delta_{\mathrm{f}})\times(n+\delta_{\mathrm{f}})}$.

Proof: See [31, Theorem 2]. ∎

In particular, the pdf $p^{\star}_{\boldsymbol{v}|\boldsymbol{z}}$ is computed by optimizing over $\boldsymbol{G}$ and $\boldsymbol{C}$, so (13) becomes

$$(\boldsymbol{G}^{\star},\,\boldsymbol{C}^{\star}) = \arg\min_{\boldsymbol{G},\boldsymbol{C}}\ f(p_{\boldsymbol{x}},\,p_{\boldsymbol{v}|\boldsymbol{z}}). \qquad (16)$$

We point out that the perfect knowledge of δ_{B} and δ_{E} is not needed. Estimates of these quantities can be derived from geometric considerations, e.g., by measuring the maximum distance between a receiver and a satellite when is on the horizon. Moreover, it is always possible to overestimate this distance, with the only consequence that the channel matrices $\boldsymbol{A}$ and $\boldsymbol{F}$ will be larger than needed, exhibiting a few trailing all-zero rows.

The variance and covariance matrices of the signals defined so far are given by

$$\begin{aligned}\boldsymbol{K}_{\boldsymbol{xy}} &= \boldsymbol{K}_{\boldsymbol{x}}\boldsymbol{A}^{\mathrm{H}}, &(17a)\\ \boldsymbol{K}_{\boldsymbol{y}} &= \boldsymbol{A}\boldsymbol{K}_{\boldsymbol{x}}\boldsymbol{A}^{\mathrm{H}} + \boldsymbol{K}_{\mathbf{B}}, &(17b)\\ \boldsymbol{K}_{\boldsymbol{xz}} &= \boldsymbol{K}_{\boldsymbol{x}}\boldsymbol{F}^{\mathrm{H}}, &(17c)\\ \boldsymbol{K}_{\boldsymbol{z}} &= \boldsymbol{F}\boldsymbol{K}_{\boldsymbol{x}}\boldsymbol{F}^{\mathrm{H}} + \boldsymbol{K}_{\mathbf{E}}, &(17d)\\ \boldsymbol{K}_{\boldsymbol{xv}} &= \boldsymbol{K}_{\boldsymbol{x}}\boldsymbol{F}^{\mathrm{H}}\boldsymbol{G}^{\mathrm{H}}, &(17e)\\ \boldsymbol{K}_{\boldsymbol{v}} &= \boldsymbol{G}\boldsymbol{F}\boldsymbol{K}_{\boldsymbol{x}}\boldsymbol{F}^{\mathrm{H}}\boldsymbol{G}^{\mathrm{H}} + \boldsymbol{G}\boldsymbol{K}_{\mathbf{E}}\boldsymbol{G}^{\mathrm{H}} + \boldsymbol{C}\boldsymbol{C}^{\mathrm{H}} + \boldsymbol{K}_{\mathbf{B}}, &(17f)\end{aligned}$$

Combining (17) with the results of [31], the optimal matrices are

$$\boldsymbol{G}^{\star} = \boldsymbol{A}\boldsymbol{K}_{\boldsymbol{x}}\boldsymbol{F}^{\mathrm{H}}(\boldsymbol{F}\boldsymbol{K}_{\boldsymbol{x}}\boldsymbol{F}^{\mathrm{H}})^{\dagger}, \qquad (18)$$

and $\boldsymbol{C}^{\star} \in \mathbb{C}^{(n+\delta_{\mathrm{f}})\times(n+\delta_{\mathrm{f}})}$ is the square root of the covariance matrix $\boldsymbol{K}_{\boldsymbol{v_0}|\boldsymbol{z}}$ of the signal $\boldsymbol{v}_0$ given $\boldsymbol{z}$. We remark that $\boldsymbol{C}^{\star}$ is obtained either with a closed form expression or through an iterative process.

A. K-L Divergence for Attacks in $\mathcal{C}$

In this Section, we will derive an analytical expression for $f(p_{\boldsymbol{x}},\,p_{\boldsymbol{v}|\boldsymbol{z}})$ when $p_{\boldsymbol{x}}$ is a generic pdf with covariance matrix $\boldsymbol{K}_{\boldsymbol{x}}$. Under the assumption that $p_{\boldsymbol{v}|\boldsymbol{z}} \in \mathcal{C}$, defining $\boldsymbol{B} \triangleq \boldsymbol{G}\boldsymbol{F}$ and $\boldsymbol{\eta} \triangleq \boldsymbol{G}\boldsymbol{\omega}_{\mathbf{E}} + \boldsymbol{C}\boldsymbol{\omega}_{\mathbf{c}} + \boldsymbol{\omega}_{\mathbf{B}}$, (15) can be rewritten as

$$\boldsymbol{v} = \boldsymbol{B}\boldsymbol{x} + \boldsymbol{\eta}, \qquad (19)$$

with

$$\boldsymbol{\eta} \sim \mathcal{N}(\mathbf{0},\,\boldsymbol{K}_{\boldsymbol{\eta}})\ ,\quad \boldsymbol{K}_{\boldsymbol{\eta}} = \boldsymbol{G}\boldsymbol{K}_{\mathbf{E}}\boldsymbol{G}^{\mathrm{H}} + \boldsymbol{C}\boldsymbol{C}^{\mathrm{H}} + \boldsymbol{K}_{\mathbf{B}}. \qquad (20)$$

Following the previous results, metric $f(p_{\boldsymbol{x}},\,p_{\boldsymbol{v}|\boldsymbol{z}})$ can be computed for a generic distribution $p_{\boldsymbol{x}}$ and $p_{\boldsymbol{v}|\boldsymbol{z}} \in \mathcal{C}$ as

$$\begin{aligned}&f(p_{\boldsymbol{x}},\,p_{\boldsymbol{v}|\boldsymbol{z}})\\ &\quad= \mathbb{E}\left[\log\frac{p_{\boldsymbol{xv}}(\boldsymbol{x},\,\boldsymbol{v})}{p_{\boldsymbol{xy}}(\boldsymbol{x},\,\boldsymbol{v})}\right] = \mathbb{E}\left[\log\frac{p_{\boldsymbol{v}|\boldsymbol{x}}(\boldsymbol{v}|\boldsymbol{x})}{p_{\boldsymbol{y}|\boldsymbol{x}}(\boldsymbol{v}|\boldsymbol{x})}\right]\\ &=\mathbb{E}\left[\log\frac{p_{\boldsymbol{\eta}}(\boldsymbol{v}-\boldsymbol{B}\boldsymbol{x})}{p_{\boldsymbol{\omega}_{\mathbf{B}}}(\boldsymbol{v}-\boldsymbol{A}\boldsymbol{x})}\right] = \mathbb{E}\left[\log\frac{p_{\boldsymbol{\eta}}(\boldsymbol{\eta})}{p_{\boldsymbol{\omega}_{\mathbf{B}}}(\boldsymbol{\eta}-(\boldsymbol{A}-\boldsymbol{B})\boldsymbol{x})}\right]\\ &=\mathbb{E}\left[\log\frac{p_{\boldsymbol{\eta}}(\boldsymbol{\eta})}{p_{\boldsymbol{\omega}_{\mathbf{B}}}(\boldsymbol{\eta})}\right] + \mathbb{E}\left[\log\frac{p_{\boldsymbol{\omega}_{\mathbf{B}}}(\boldsymbol{\eta})}{p_{\boldsymbol{\omega}_{\mathbf{B}}}(\boldsymbol{\eta}-(\boldsymbol{A}-\boldsymbol{B})\boldsymbol{x})}\right]\\ &=\mathbb{D}(p_{\boldsymbol{\eta}}\|p_{\boldsymbol{\omega}_{\mathbf{B}}}) + \mathbb{E}\left[((\boldsymbol{A}-\boldsymbol{B})x)^{\mathrm{H}}\boldsymbol{K}_{\mathbf{B}}{}^{-1}(\boldsymbol{A}-\boldsymbol{B})x\right]\\ &=\frac{1}{2}\log\frac{|\boldsymbol{K}_{\mathbf{B}}|}{|\boldsymbol{K}_{\boldsymbol{\eta}}|} + \frac{1}{2}\operatorname{tr}(\boldsymbol{K}_{\boldsymbol{\eta}}\boldsymbol{K}_{\mathbf{B}}{}^{-1}) - \frac{(n+\delta_{\mathrm{f}})}{2}\end{aligned}$$

$$+\frac{1}{2}\left[\operatorname{tr}\left((\boldsymbol{B}-\boldsymbol{A})\boldsymbol{K}_{\boldsymbol{x}}(\boldsymbol{B}-\boldsymbol{A})^{\mathrm{H}}\boldsymbol{K}_{\mathbf{B}}{}^{-1}\right)\right]. \tag{21}$$

Assuming that additive white Gaussian noise (AWGN) is present at the receiver we have $\boldsymbol{K}_{\mathrm{B}} = 2\sigma_{\mathrm{B}}^2\boldsymbol{I}_{n+\delta_{\mathrm{B}}}$, $\boldsymbol{K}_{\mathrm{E}} = 2\sigma_{\mathrm{E}}^2\boldsymbol{I}_{n+\delta_{\mathrm{E}}}$, where σ_{B}^2, σ_{E}^2 are the variances of each component (real or imaginary) of the complex noise at Bob's and Eve's receiver, respectively. Thus, in presence of AWGN (21) is

$$f(p_{\boldsymbol{x}}, p_{\boldsymbol{v}|z}) = \frac{1}{2}\left[\sum_{i=1}^{n+\delta_{\mathrm{f}}}\left(\frac{\lambda_i}{\sigma_{\mathrm{B}}^2} - \log\left(\frac{\lambda_i}{\sigma_{\mathrm{B}}^2}\right)\right) - (n+\delta_{\mathrm{f}})\right] + \frac{1}{2\sigma_{\mathrm{B}}^2}\operatorname{tr}\left((\boldsymbol{B}-\boldsymbol{A})\boldsymbol{K}_{\boldsymbol{x}}(\boldsymbol{B}-\boldsymbol{A})^{\mathrm{H}}\right), \tag{22}$$

where λ_i, $i \in \{1, 2, \ldots, n+\delta_{\mathrm{f}}\}$, are the eigenvalues of $\boldsymbol{K}_{\boldsymbol{\eta}}$. We remark that (21) holds for any distribution $p_{\boldsymbol{x}}$, as long as the attack pdf $p_{\boldsymbol{v}|z}$ is taken from $\mathcal{C}$.

For convenience, we analyze the two terms of (21) separately

$$t_1 \triangleq \frac{1}{2}\left[\sum_{i=1}^{n+\delta_{\mathrm{f}}}\left(\frac{\lambda_i}{\sigma_{\mathrm{B}}^2} - \log\left(\frac{\lambda_i}{\sigma_{\mathrm{B}}^2}\right)\right) - (n+\delta_{\mathrm{f}})\right], \tag{23}$$

$$t_2 \triangleq \frac{1}{2\sigma_{\mathrm{B}}^2}\operatorname{tr}\left((\boldsymbol{B}-\boldsymbol{A})\boldsymbol{K}_{\boldsymbol{x}}(\boldsymbol{B}-\boldsymbol{A})^{\mathrm{H}}\right). \tag{24}$$

Since $c - 1 \geq \log c$, $\forall c \in \mathbb{R}^+$, we can state that each term of the sum in t_1 is greater than or equal to 1. Moreover, $t_1 = 0$ if and only if $\lambda_i/\sigma_{\mathrm{B}}^2 = 1$, $\forall i \in \{1, 2, \ldots, n+\delta_{\mathrm{f}}\}$, i.e., if and only if the attacker manages to construct $\boldsymbol{K}_{\boldsymbol{\eta}} = \boldsymbol{K}_{\mathbf{B}}$. On the other hand, the term t_2 in (21) is independent of the attacker noise $\boldsymbol{\omega}_{\mathbf{E}}$, because it does not depend on $\boldsymbol{K}_{\boldsymbol{\eta}}$. It solely depends on the covariance matrix $\boldsymbol{K}_{\boldsymbol{x}}$, the legitimate receiver noise power σ_{B}^2 in the nominal case, and the difference $\boldsymbol{A}-\boldsymbol{B}$, where $\boldsymbol{A}$ and $\boldsymbol{B}$ are the authentic and the forged channel matrix, respectively. Therefore, the following inequality holds

$$f(p_{\boldsymbol{x}}, p_{\boldsymbol{v}|z}) \geq t_2, \quad \forall p_{\boldsymbol{v}|z} \in \mathcal{C}. \tag{25}$$

B. K-L Divergence Under Optimal Attack

From (21) and (25), we observe that, for a generic $p_{\boldsymbol{x}}$ with covariance matrix $\boldsymbol{K}_{\boldsymbol{x}}$, once the values of $\boldsymbol{A}$, $\boldsymbol{K}_{\boldsymbol{x}}$, and σ_{B}^2 are fixed, the lower bound for the K-L divergence can be expressed as a function of $\boldsymbol{B}$ as

$$\mathbb{D}_{\min}(\boldsymbol{B}) \triangleq \frac{1}{2\sigma_{\mathrm{B}}^2}\operatorname{tr}\left((\boldsymbol{B}-\boldsymbol{A})\boldsymbol{K}_{\boldsymbol{x}}(\boldsymbol{B}-\boldsymbol{A})^{\mathrm{H}}\right). \tag{26}$$

In particular. when the attacker succeeds in constructing $\boldsymbol{K}_{\boldsymbol{\eta}} = \boldsymbol{K}_{\mathbf{B}}$, then $t_1 = 0$, and

$$f(p_{\boldsymbol{x}}, p^{\star}_{\boldsymbol{v}|z}) = \mathbb{D}_{\min}(\boldsymbol{B}^{\star}). \tag{27}$$

A worth noting consideration is that, for a fixed $\boldsymbol{K}_{\boldsymbol{x}}$, $p^{\star}_{\boldsymbol{v}|z}$ achieves the minimum K-L divergence among all the possible attack strategies $p_{\boldsymbol{v}|z} \in \mathcal{C}$, regardless of the shape of $p_{\boldsymbol{x}}$, thus

$$f(p_{\boldsymbol{x}}, p_{\boldsymbol{v}|z}) \geq f(p_{\boldsymbol{x}}, p^{\star}_{\boldsymbol{v}|z}), \quad \forall\, p_{\boldsymbol{v}|z} \in \mathcal{C}. \tag{28}$$

In particular, when $\boldsymbol{K}_{\boldsymbol{x}} = M_x\boldsymbol{I}_{mn}$ (as further discussed in Section IV-A), $\mathbb{D}_{\min}(\boldsymbol{B})$ can be written as

$$\mathbb{D}_{\min}(\boldsymbol{B}) = \frac{M_x}{2\sigma_{\mathrm{B}}^2}\|\boldsymbol{A}-\boldsymbol{B}\|_F^2 = \frac{mn}{2}\,k\,\Lambda_{\mathrm{AB}}, \tag{29}$$

where

$$k = \frac{\|\boldsymbol{A}-\boldsymbol{B}\|_F^2}{\|\boldsymbol{A}\|_F^2} \tag{30}$$

represents a diversity index between $\boldsymbol{A}$ and $\boldsymbol{B}$, and

$$\Lambda_{\mathrm{AB}} = \frac{M_x}{\sigma_{\mathrm{B}}^2}\frac{\|\boldsymbol{A}\|_F^2}{mn}, \tag{31}$$

is the average received signal to noise ratio (SNR) at Bob. Note that the attacker can always choose $\boldsymbol{G}$ such that $k \leq 1$, e.g., by trivially setting $\boldsymbol{G} = 0$, we get $k = 1$. Moreover, term

$$\frac{\|\boldsymbol{A}\|_F^2}{mn} = \frac{1}{m}\sum_{i=1}^{m}\frac{1}{n}\|\boldsymbol{A}\|_F^2 \tag{32}$$

represents the average energy of the m impulsive responses of the legitimate channels. Therefore, (29) describes $\mathbb{D}_{\min}(\boldsymbol{B})$ in terms of the total length of the m transmitted signals (mn), a measure of the difference between the channel matrices (k), where $\boldsymbol{A}$ is the matrix of the legitimate channel and $\boldsymbol{B}$ is the matrix of the forged channel, the SNR of the legitimate channel $A \to B$ (Λ_{AB}).

IV. Defense Strategy Design

The transmission and the attack detection strategies altogether determine the defense strategy. Therefore, in this Section, we investigate how Alice designs the transmitted signal and how Bob performs the verification step of the authentication procedure.

A. Gaussian Transmission

The optimal transmission strategy $p^{\star}_{\boldsymbol{x}}$, is given by the maximin solution of (12). We start by identifying the optimal distribution for a constrained covariance matrix, introducing the following theorem.

Theorem 2: Given a covariance matrix $\boldsymbol{K}_{\boldsymbol{x}}$, let us define $p^{\star}_{\boldsymbol{x}} \sim \mathcal{N}(0, \boldsymbol{K}_{\boldsymbol{x}})$. If the transmission distribution $p_{\boldsymbol{x}}$ is to be chosen among all those with zero mean and covariance $\boldsymbol{K}_{\boldsymbol{x}}$, the pair of strategies $(p^{\star}_{\boldsymbol{x}}, p^{\star}_{\boldsymbol{v}|z})$ constitutes a saddle point of $f(p_{\boldsymbol{x}}, p_{\boldsymbol{v}|z})$.

Proof: For any attack strategy $p_{\boldsymbol{v}|z} \in \mathcal{C}$, we can compute $f(p_{\boldsymbol{x}}, p_{\boldsymbol{v}|z})$ for a generic distribution $p_{\boldsymbol{x}}$ from (21). We note that, when $p_{\boldsymbol{v}|z} \in \mathcal{C}$, the K-L divergence depends on $p_{\boldsymbol{x}}$ only through the covariance matrix $\boldsymbol{K}_{\boldsymbol{x}}$. Consequently, if $p_{\boldsymbol{v}|z} \in \mathcal{C}$, once matrices $\boldsymbol{A}$, $\boldsymbol{B}$, and $\boldsymbol{K}_{\boldsymbol{x}}$ are set, then $f(p_{\boldsymbol{x}}, p_{\boldsymbol{v}|z})$ is constant for each probability distribution $p_{\boldsymbol{x}}$ chosen by Alice. Therefore, we conclude that the set of strategies $(p^{\star}_{\boldsymbol{x}}, p^{\star}_{\boldsymbol{v}|z})$ constitutes a saddle point for $f(p_{\boldsymbol{x}}, p_{\boldsymbol{v}|z})$ since neither the attacker nor the defender can gain by a unilateral change of strategy if the strategy of the other remains unchanged. In particular

$$f(p_{\boldsymbol{x}}, p^{\star}_{\boldsymbol{v}|z}) = f(p^{\star}_{\boldsymbol{x}}, p^{\star}_{\boldsymbol{v}|z}), \quad \forall\, p_{\boldsymbol{x}}, \tag{33}$$

$$f(p^{\star}_{\boldsymbol{x}}, p_{\boldsymbol{v}|z}) > f(p^{\star}_{\boldsymbol{x}}, p^{\star}_{\boldsymbol{v}|z}), \quad \forall\, p_{\boldsymbol{v}|z}, \tag{34}$$

where (33) follows from (21), when the covariance matrix $\boldsymbol{K}_{\boldsymbol{x}}$ is fixed, while (34) holds for the optimality of $p^{\star}_{\boldsymbol{v}|z}$ when the transmission distribution is $p^{\star}_{\boldsymbol{x}}$, as stated in Theorem 1. ■

The maximin problem in (12) can be seen as an adversarial zero-sum game with two players [32], the defense (Alice), and the attacker (Eve). Eve chooses the strategy that maximizes her own payoff, while Alice adopts a maximin strategy, i.e., the one that yields the 'best of the worst' outcomes, so it guarantees an outbound on the performance obtained when Eve plays the best possible attack. In our setup, $p_{\boldsymbol{x}}$ and $p_{\boldsymbol{v}|z}$ are the defender's and attacker's mixed strategies, while $f(p_{\boldsymbol{x}}, p_{\boldsymbol{v}|z})$ and $-f(p_{\boldsymbol{x}}, p_{\boldsymbol{v}|z})$ are their average payoffs,[3] respectively. In this case, the set of strategies $(p^{\star}_{\boldsymbol{x}}, p^{\star}_{\boldsymbol{v}|z})$, constitutes one Nash equilibrium of the game. We remark that there may be many Nash equilibria, however, for the properties of zero-sum games, they all have the same average payoff [33].

From Theorem 2, we conclude that the optimal defense strategy $p^{\star}_{\boldsymbol{x}}$ solving (12) must be a zero mean Gaussian distribution. Furthermore, Alice can choose the covariance matrix $\boldsymbol{K_x}$ of $p^{\star}_{\boldsymbol{x}}$ so that $f(p^{\star}_{\boldsymbol{x}}, p^{\star}_{\boldsymbol{v}|z})$ is maximized while ensuring the constraint on the transmitted power M_x: $\mathrm{tr}(\boldsymbol{K_x}) \leq mn\, M_x$. Given the symmetry of the problem and the transmitter's lack of knowledge of the channel and, consequently, of the matrices $\boldsymbol{A}$ and $\boldsymbol{F}$, a reasonable choice is $\boldsymbol{K_x} = M_x\, \boldsymbol{I}_{mn}$.

From the theory of binary hypothesis testing, we know that if both the statistics of the legitimate and spoofed signal are known (i.e., if the victim is aware of the particular attack strategy adopted by the spoofer) the test yielding the minimum p_{MD} for any given constraint on p_{FA}, is the LRT, also known as Neyman-Pearson criterion [28], [29]. Under the assumption that the attack strategy belongs to class $\mathcal{C}$, the detection problem reduces to the test

$$L' = (\boldsymbol{r} - \boldsymbol{Ax})^{\mathrm{H}} \boldsymbol{K_B}^{-1} (\boldsymbol{r} - \boldsymbol{Ax}) - (\boldsymbol{r} - \boldsymbol{Bx})^{\mathrm{H}} \boldsymbol{K_\eta}^{-1} (\boldsymbol{r} - \boldsymbol{Bx}) \underset{H_0}{\overset{H_1}{\gtrless}} \theta. \tag{35}$$

When both Eve and Alice play the Nash equilibrium strategies derived in Sections III and IV-A, Bob will use the LRT since it is aware of the attack strategy distribution.

B. Transmission Strategies With Practical Modulation Schemes

In Section IV-A we derived that the optimal defense strategy solving (12) must be a zero mean Gaussian distribution. However, in practice, this is not feasible and hence we analyze the case wherein $\boldsymbol{x}$ has symbols from a finite set, e.g., a QAM constellation.

In (21) we showed that, when $p_{\boldsymbol{v}|z} \in \mathcal{C}$, the value of $f(p_{\boldsymbol{x}}, p_{\boldsymbol{v}|z})$ depends on $p_{\boldsymbol{x}}$ only through the covariance matrix $\boldsymbol{K_x}$. This implies that

$$f(p_{\boldsymbol{x}}, p_{\boldsymbol{v}|z}) = f(p^{\star}_{\boldsymbol{x}}, p_{\boldsymbol{v}|z}), \quad \forall\, p_{\boldsymbol{v}|z} \in \mathcal{C}, \tag{36}$$

where $p_{\boldsymbol{x}}$ is a generic distribution of the signal $\boldsymbol{x}$, with the same covariance matrix $\boldsymbol{K_x}$ of $p^{\star}_{\boldsymbol{x}} \sim \mathcal{N}(\boldsymbol{0}, \boldsymbol{K_x})$. Therefore, when the attack belongs to the class $\mathcal{C}$, we may conclude that the performance in terms of divergence is the same with either Gaussian or finite-cardinality modulation. Moreover, from (33) and (34) we have

$$f(p_{\boldsymbol{x}}, p^{\star}_{\boldsymbol{v}|z}) = f(p^{\star}_{\boldsymbol{x}}, p^{\star}_{\boldsymbol{v}|z}) \leq f(p^{\star}_{\boldsymbol{x}}, p_{\boldsymbol{v}|z}), \quad \forall\, p_{\boldsymbol{v}|z}. \tag{37}$$

On the other hand, $p^{\star}_{\boldsymbol{v}|z}$ is the optimal attack strategy only when the transmitted signal $\boldsymbol{x}$ is a Gaussian codeword of length mn. This implies that, for a non Gaussian $p_{\boldsymbol{x}}$, an attack strategy $p^{o}_{\boldsymbol{v}|z} \notin \mathcal{C}$ may exist, that achieves

$$f(p_{\boldsymbol{x}}, p^{o}_{\boldsymbol{v}|z}) \leq f(p_{\boldsymbol{x}}, p^{\star}_{\boldsymbol{v}|z}). \tag{38}$$

Therefore, from (36)–(38) we can derive the following relation

$$\begin{aligned} f(p_{\boldsymbol{x}}, p^{o}_{\boldsymbol{v}|z}) &\leq f(p_{\boldsymbol{x}}, p^{\star}_{\boldsymbol{v}|z}) \\ &= f(p^{\star}_{\boldsymbol{x}}, p^{\star}_{\boldsymbol{v}|z}) \leq f(p^{\star}_{\boldsymbol{x}}, p^{o}_{\boldsymbol{v}|z}). \end{aligned} \tag{39}$$

When the signal $\boldsymbol{x}$ has symbols from a finite set, the transmission strategy differs from $p^{\star}_{\boldsymbol{x}}$, and the optimal attack strategy distribution $p^{o}_{\boldsymbol{v}|z}$ is not known. Hence, the receiver only knows the statistics of the authentic signal, and cannot make assumptions on the attack strategy chosen by E nor has information on the channels A $\rightarrow$ E and E $\rightarrow$ B. In this case, the LRT detection method no longer applies, and a possible solution is to use the GLRT [28], [34], i.e., the detection problem is given by

$$G' = (\boldsymbol{r} - \boldsymbol{Ax})^{\mathrm{H}} \boldsymbol{K_B}^{-1} (\boldsymbol{r} - \boldsymbol{Ax}) \underset{H_0}{\overset{H_1}{\gtrless}} \theta. \tag{40}$$

C. Limiting Scenarios

We now discuss some limiting scenarios, in which the considered spoofing attack achieves complete indistinguishability from the legitimate signal and hence cannot be detected:

- **S1:** $\boldsymbol{A} = \boldsymbol{F}$, wherein Eve performs a meaconing attack, inducing her own position onto Bob;
- **S2:** $m = 1$, so both Eve and Bob receive the signal from only one satellite, and there is not sufficient diversity;
- **S3:** the channel A $\rightarrow$ B is stochastically degraded with respect to the channel A $\rightarrow$ E.

In the following analysis, we assume that the attacker Eve makes use of the optimal attacking strategy $p^{\star}_{\boldsymbol{v}|z}$.

In scenario **S1**, where $\boldsymbol{A} = \boldsymbol{F}$, we have that $\delta_{\mathrm{E}} = \delta_{\mathrm{B}} = \delta_{\mathrm{f}} = \delta$. From (18), Eve gets $\boldsymbol{G^{\star}} = \boldsymbol{I_{n+\delta}}$ so that $\boldsymbol{B^{\star}} = \boldsymbol{G^{\star}F} = \boldsymbol{F}$, and $\boldsymbol{B^{\star}} = \boldsymbol{F} = \boldsymbol{A}$, which implies $\mathbb{D}_{\min}(\boldsymbol{B^{\star}}) = 0$. Thus, the meaconing attack cannot be detected in this model.

In scenario **S2** we are supposing $m = 1$. This implies that $\delta_{\mathrm{E}} = \delta_{\mathrm{B}} = \delta_{\mathrm{f}} = 0$, so $\boldsymbol{A}$ and $\boldsymbol{F}$ are invertible square matrices. Therefore, when $\boldsymbol{G^{\star}}$ is computed as in (18), Eve will get $\boldsymbol{B^{\star}} = \boldsymbol{G^{\star}F} = \boldsymbol{A}$, which implies $\mathbb{D}_{\min}(\boldsymbol{B^{\star}}) = 0$. Therefore, to have $\mathbb{D}_{\min}(\boldsymbol{B^{\star}}) > 0$, Bob has to combine signals from $m > 1$ satellites. However, this is also a necessary condition for the GNSS receiver to estimate the position.[4]

In scenario **S3** we have that the channel A $\rightarrow$ B, represented by the conditional pdf $p_{y|x}$, can be decomposed as the cascade of $p_{z|x}$ and some properly chosen $p_{y|z'}$. Therefore, in this case Eve can choose $p_{v|z} = p_{y|z'}$ to obtain $p_{y|x} = p_{v|x}$. Moreover,

[3] Player's payoffs are averaged over the mixed players' strategies and the noise distribution, $f(p_{\boldsymbol{x}}, p_{\boldsymbol{v}|z}) = \mathbb{E}\left[\log \frac{p_{\boldsymbol{xv}}(\boldsymbol{x},\boldsymbol{v})}{p_{\boldsymbol{x}}p_{\boldsymbol{y}}(\boldsymbol{x},\boldsymbol{v})}\right]$.

[4] We remark that when $m = 1$, the GNSS signal can be used for timing purposes. Still, we consider such timing attacks as out-of-the-scope of the paper, as we focus on position-spoofing attacks.

we have $\boldsymbol{y} = \boldsymbol{G}'\boldsymbol{z}' + \boldsymbol{C}'\boldsymbol{\omega}_{\mathbf{c}}$, and Eve chooses $\boldsymbol{G}^{\star} = \boldsymbol{G}'$ and $\boldsymbol{C}^{\star} = \boldsymbol{C}'$, so that $\boldsymbol{B}^{\star} = \boldsymbol{A}$ and $\mathbb{D}_{\min}(\boldsymbol{B}^{\star}) = 0$. Therefore, in this case, the attack goes undetected.

The more general, and more realistic, spoofing scenario occurs when $m > 1$, $\boldsymbol{A} \neq \boldsymbol{F}$ and $\sigma_{\mathrm{E}}^2 > 0$. Moreover, the hypothesis in scenario **S3** is very pessimistic. Therefore, in a realistic scenario, with the additional assumption that $\ker(A) \nsubseteq \ker(F)$, it is always assured that $\mathbb{D}_{\min}(\boldsymbol{B}) > 0$.

V. Numerical Results

In this Section, we illustrate the performance obtained for LRT and GLRT, when either Gaussian or finite-cardinality signals are used, through a MATLAB simulation, running 5000 channel realizations for each considered scenario.

More in detail, as in our previous work [26] we already tested the case of a realistic channel model, in this Section, matrices $\boldsymbol{A}$ and $\boldsymbol{F}$ account only for the delays. These are the propagation times of each signal $\bar{\boldsymbol{x}}_i$ from the i-th SV to Eve and Bob, and we neglect other possible channel phenomena. Next, we consider an attack strategy $p^{\star}_{\boldsymbol{v}|\boldsymbol{z}}$, described in Section III. We remark that, in a typical GNSS spoofing scenario, the power of the spoofing signal $\boldsymbol{v_0}$ at the receiver can be larger than that of the legitimate signal; thus, the SNR on the attack signal may be larger than with the authentic one. Assuming that an automatic gain control (AGC) at Bob's front-end can scale the received signal to nearly constant amplitude, the receiver noise variance is correspondingly reduced, in the attack case, allowing the spoofer some margin to shape $\boldsymbol{K}_{\boldsymbol{\eta}} = \boldsymbol{K}_{\mathbf{B}}$. This represents the worst case for the defender. However, the defense strategy must be robust regardless of the attack's strength. For this reason, we cannot rely solely on signal power and noise-level monitoring mechanisms. Similarly to (31), we define the received spoofer SNR as

$$\Lambda_{\mathrm{AE}} = \frac{M_x}{\sigma_{\mathrm{E}}^2} \frac{\|\boldsymbol{F}\|_F^2}{mn}. \tag{41}$$

In the analyzed scenarios, we will take into account the delay vector $\boldsymbol{\tau_f}$ associated with the position of our department (DEI) (P1), located in Padua, Italy, and the delay vector $\boldsymbol{\tau_E}$ associated to three different positions, two of which located in Padua, Italy, namely a house in Paolotti street (P2), and the square of Prato della Valle (P3), and the Duomo square (P4), located in Milan, Italy. Fig. 3 illustrates the four positions. Delays' measurements have been collected on the 14th of December 2022, at noon CET. Table II outlines each considered position with their coordinates, while Table III summarizes the distances between the target and Eve's positions.

A. Results With Gaussian Transmission

In this Section performance is evaluated when the transmitted signal $\boldsymbol{x}$ is a Gaussian codeword of length n, as derived in Section IV-A, considering a LRT detection method. Fig. 4 shows the DET curves for the LRT detection method (solid lines) and the performance bounds (dashed lines) derived from the K-L divergence for different values of n, considering the signals coming from $m = 5$ SVs, $M_x = 1$, $\Lambda_{\mathrm{AB}} = -25$ dB, $\Lambda_{\mathrm{AE}} = -10$ dB, when $\boldsymbol{\tau_E}$ and $\boldsymbol{\tau_f}$ collect the delays associated to P1 and P2, respectively. The bound follows the same trend of (29), thus it is representative of the actual performance. The bound is tight for $n = 400$, while the gap between it and the actual performance grows as the value of n rises. Indeed, as n decreases, the DET curves move quickly towards the gray dashed line, which represents the trivial limit case, in which the decision is taken without looking at the signal but tossing a biased coin. Thus, the obtained value of p_{MD} for given values of p_{FA} can be reduced by increasing the value of n, as Fig. 4 shows. When $n = 1200$, the value of p_{MD} decreases by approximately one order of magnitude with respect to the case with $n = 400$. Moreover, we note that the bounds given by the K-L divergence are symmetric, as proven in Appendix A.

Fig. 5 shows the DET curves of the LRT detection method for different values of (a) Λ_{AB} and (b) Λ_{AE}, considering the signals coming from $m = 5$ SVs, $M_x = 1$, in (a) $\Lambda_{\mathrm{AE}} = -10$ dB, in (b) $\Lambda_{\mathrm{AB}} = -20$ dB, when $\boldsymbol{\tau_E}$ and $\boldsymbol{\tau_f}$ collect the delays associated to P1 and P2, respectively. It can be seen that the curves follow the behavior of (29); in fact, the

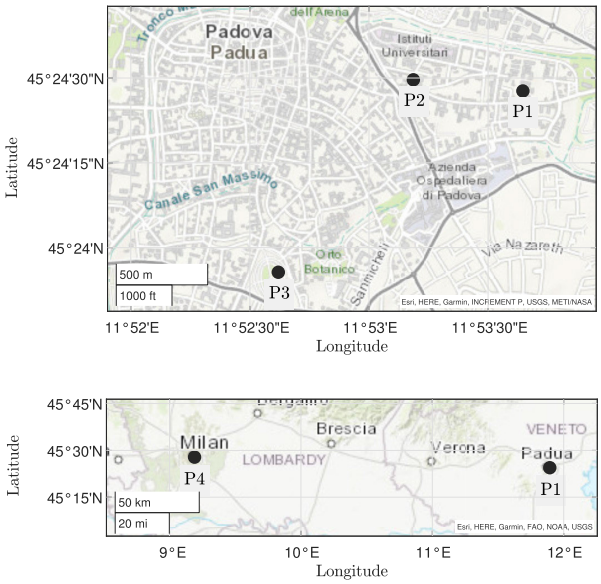

Fig. 3. Map of the considered positions. Three are located in Padua, Italy: DEI (P1), Paolotti Street (P2), and the square of Prato della Valle (P3). One located in Milan, Italy: Duomo Square (P4).

TABLE II
Considered Positions and Their Coordinates

	LLH coordinates	Landmark
P1	45.4077° N, 11.8941° E, 12 m	DEI, Padua, Italy
P2	45.4079° N, 11.8860° E, 12 m	via Paolotti, Padua, Italy
P3	45.3980° N, 11.8766° E, 12 m	Prato della Valle, Padua, Italy
P4	45.4641° N, 9.1903° E, 120 m	Duomo square, Milan, Italy

TABLE III
Distances Between Eve and Target Position

Eve position	Target position	Distance
P1	P2	607 m
P1	P3	1.7 Km
P1	P4	211 Km

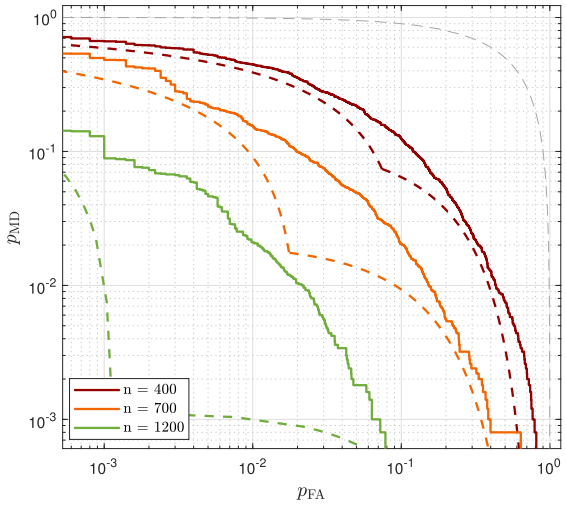

Fig. 4. DET curves for the LRT detection method (solid lines) and K-L divergence bounds (dashed lines) for different values of n, when $p_{\boldsymbol{x}}$ is Gaussian distributed, $M_x = 1$, $m = 5$, $\boldsymbol{\tau_f}$ associated to P1, $\boldsymbol{\tau_E}$ associated to P2, $\Lambda_{\mathrm{AB}} = -25$ dB, and $\Lambda_{\mathrm{AE}} = -10$ dB. The gray dashed line represents the trivial limit case in which the decision is taken by tossing a biased coin.

curves rise when Λ_{AB} decreases, while remaining unchanged for different values of Λ_{AE}. As a result, the performance of the LRT verification mechanism is independent of the attacker's SNR, as long as $\Lambda_{\mathrm{AE}} > \Lambda_{\mathrm{AB}}$.

Fig. 6 shows the DET curves for the LRT detection for different values of n and position pairs, when $M_x = 1$, $m = 5$, $\Lambda_{\mathrm{AB}} = -25$ dB, and $\Lambda_{\mathrm{AE}} = -10$ dB. In each tested scenario, the delays vector $\boldsymbol{\tau_f}$ is associated with P1, while the vector $\boldsymbol{\tau_E}$ is associated with three different positions, i.e., (from the closest to P1 to furthest): P2, P3, and P4. We can see that the curves move away from perfect distinguishability (the lower left corner) when the distance between the position associated with $\boldsymbol{\tau_E}$ and $\boldsymbol{\tau_f}$ decreases. Therefore, the attack performance degrades as the attack's target position moves farther away from the attacker's actual position. Finally, we note that, as for Fig. 4, the defense performance improves (i.e., the curves move towards the bottom left corner) as n increases.

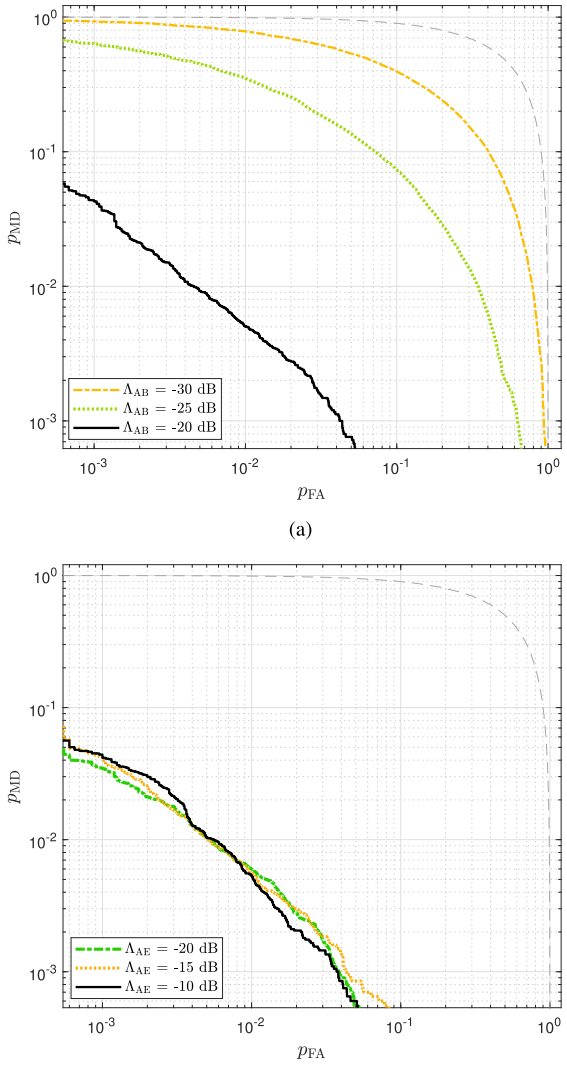

Fig. 5. DET curves for the LRT detection method for different values of (a) Λ_{AB} and (b) Λ_{AE}, when $p_{\boldsymbol{x}}$ is Gaussian distributed, $M_x = 1$, $m = 5$, $n = 500$, $\boldsymbol{\tau_f}$ associated to P1, and $\boldsymbol{\tau_E}$ associated to P2. In (a) $\Lambda_{\mathrm{AE}} = -10$ dB, and (b) $\Lambda_{\mathrm{AB}} = -20$ dB.

B. Results With Practical Modulation Schemes

As discussed in Section IV-B, switching from Gaussian to finite-cardinality signaling does not affect the performance of the verification mechanism, when the attack strategy belongs to $\mathcal{C}$. This behavior will be demonstrated in this paragraph through simulation results. In the following, a BPSK modulation will be considered (i.e., having cardinality $M = 2$).

Fig. 7 shows the DET curves for the GLRT detection method for different values of n, when $p_{\boldsymbol{x}}$ is Gaussian distributed (solid lines) and $p_{\boldsymbol{x}}$ is a Binary distribution (dashed lines), $M_x = 1$, $m = 9$, $\boldsymbol{\tau_f}$ and $\boldsymbol{\tau_E}$ collect the delays associated to P1 and P4, respectively. These results have been obtained for $\Lambda_{\mathrm{AB}} = -20$ dB and $\Lambda_{\mathrm{AE}} = -10$ dB, so we are in the low-SNR regime. As can be seen, the curves obtained with Gaussian and binary signaling are very close, confirming the results of Section IV-B. Moreover, it is seen that GLRT is effective in detecting spoofing, even without any prior knowledge of the spoofer strategy. For practically meaningful values for p_{FA} and p_{MD}, we should consider longer signals, so a higher value of n with respect to the LRT case. Clearly, by observing more samples before making a decision, the decision will be more accurate, but this requires buffering and processing more data. Furthermore, this leads to a longer time to authenticate (TTA). Thus, the observation period must be chosen as a trade-off between the computational resources of the device, the desired TTA, and the desired performance in terms of DET.

Fig. 8 shows the DET curves for the GLRT detection method for different values of n and position pairs, when $p_{\boldsymbol{x}}$ is Gaussian distributed, $M_x = 1$, $m = 9$, $\Lambda_{\mathrm{AB}} = -20$ dB, and $\Lambda_{\mathrm{AE}} = -10$ dB. In each tested scenario, the delay vector $\boldsymbol{\tau_f}$ is associated to P1, while vector $\boldsymbol{\tau_E}$ is associated with P2, P3, and P4. As for the LRT case, the attack performance improves when the distance between the position associated with $\boldsymbol{\tau_E}$ and $\boldsymbol{\tau_f}$ decreases. Therefore, also for the GLRT, the missed detection probability decreases, for a fixed false alarm probability, as the attack's target position moves farther away from the attacker's actual position.

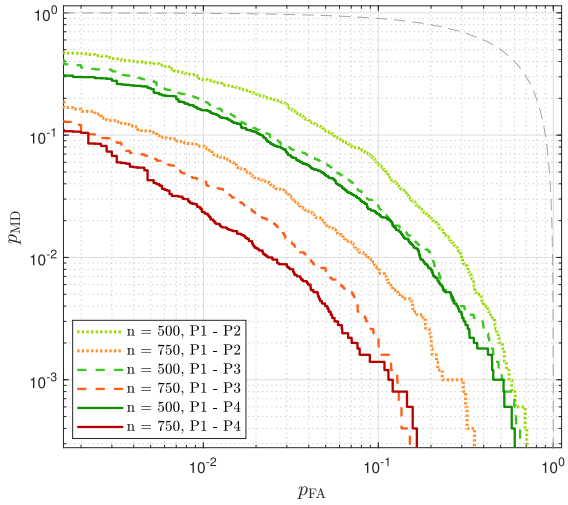

Fig. 6. DET curves for the LRT detection method for different values of n and position pairs, when $p_{\boldsymbol{x}}$ is Gaussian distributed, $M_x = 1$, $m = 5$, $\Lambda_{AB} = -25$ dB, and $\Lambda_{AE} = -10$ dB.

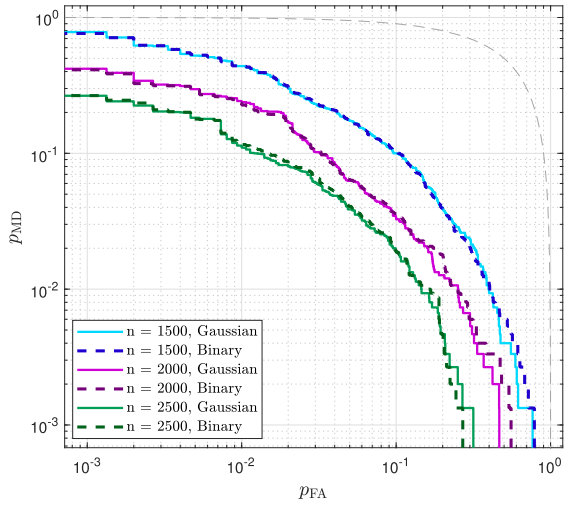

Fig. 7. DET curves for the GLRT detection method for different values of n, when $p_{\boldsymbol{x}}$ is Gaussian distributed (solid lines) and when $p_{\boldsymbol{x}}$ is a Binary distribution (dashed lines), $M_x = 1$, $m = 9$, $\boldsymbol{\tau_f}$ associated to P1, $\boldsymbol{\tau_E}$ associated to P4, $\Lambda_{AB} = -20$ dB, and $\Lambda_{AE} = -10$ dB.

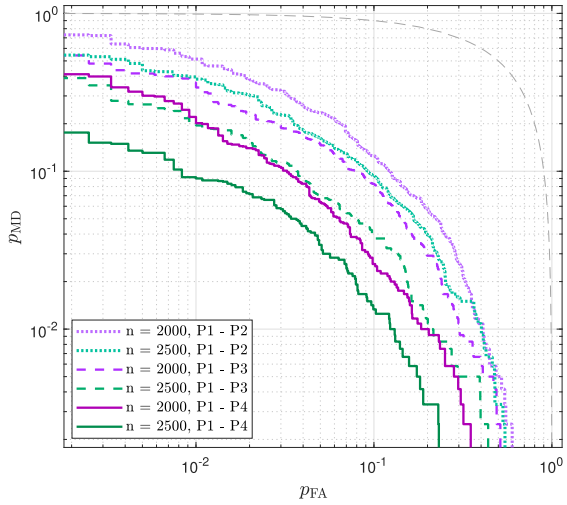

Fig. 8. DET curves for the GLRT detection method for different values of n and position pairs, when $p_{\boldsymbol{x}}$ is Gaussian distributed, $M_x = 1$, $m = 9$, $\Lambda_{AB} = -20$ dB, and $\Lambda_{AE} = -10$ dB.

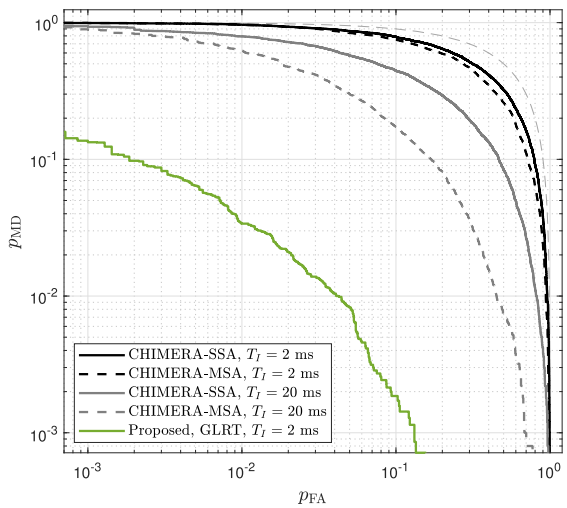

Fig. 9. DET curves for the proposed authentication scheme and optimal attack $p^{\star}_{\boldsymbol{v}|\boldsymbol{z}}$ with GLRT, and the CHIMERA system with forging attack, for $(C/N_0)_B = 45$ dB/Hz, $(C/N_0)_E = 49$ dB/Hz, $m = 5$, and $F_s = 2$ MHz.

C. Performance Comparison With State-of-the-Art Schemes

In this Section, we compare the proposed scheme and the optimal attack derived in Section III with CHIMERA SCA [16], [17]. We focus on a basic attacker forging the spoofing signal using only the public pseudo-random noise (PRN) sequences. The performance is assessed by our GNSS signal simulator and software receiver [35], [36], where we implemented a CHIMERA-like signature as described in [16], with a total marker-insertion duty factor of 10%. We simulated BPSK modulated GPS C/A signals, with spreading code chip rate $F_c = 1.023$ MHz and carrier frequency $f_0 = 1575.42$ MHz. We take into account the delay vector $\boldsymbol{\tau}_f$ associated with P1 and $\boldsymbol{\tau}_E$ associated with P3, with delays' measurements collected on the 14th December 2022, at noon CET.

Concerning the CHIMERA authentication verification at the legitimate receiver, we considered both single- and multiple-signal authentication methods based on the PRN correlation. In the CHIMERA single-signal authentication (CHIMERA-SSA) method, we simulated only one satellite signal and collected the correlation power P both for the authentic and the under-attack scenarios. Then, the signal is authenticated if $P > \theta$, where θ is a suitably chosen threshold. Instead, in the CHIMERA multiple-signal authentication (CHIMERA-MSA), after the acquisition process, we extract the correlation power P_i, $i = 1, \ldots, m$, for each visible satellite, and the received signal is authenticated if $P_i > \theta, \forall\, i \in [1, m]$, or equivalently $\min_i P_i > \theta$. Moreover, notice that a total marker insertion duty factor of 10% yields a correlation loss of 0.9 dB [15]. We denote with $(C/N_0)_{B,i}$ and $(C/N_0)_{E,i}$ the carrier-to-noise ratio of the channel from the i-th SV to Bob and Eve, respectively. For simplicity, we consider $(C/N_0)_{B,i} = (C/N_0)_B$, and $(C/N_0)_{E,i} = (C/N_0)_E$, $\forall i \in [1, m]$. In particular, we considered for both GLRT and CHIMERA-based checks, $(C/N_0)_B = 45$ dB/Hz, sampling frequency $F_s = 2F_c$, and the number of visible satellites is $m = 5$. To simulate the proposed attack we considered $(C/N_0)_E = 49$ dB/Hz with Eve using the public PRN to forge a spoofing signal.

Fig. 9 shows the DET curves for the proposed authentication scheme and optimal attack $p^{\star}_{\boldsymbol{v}|z}$, as derived in Section III, with GLRT, and CHIMERA. We considered two scenarios, where in the first we fix the integration time of the signal at the receiver at $T_{\mathrm{I}} = 2$ ms. In the latter, we keep constant the number of authenticated chips and, as we assumed that only 10% of the PRN chips are signed in CHIMERA, we increase the integration time of the latter by 10 times, so the integration times for the two systems are different and equal to 2 ms for the proposed system and 20 ms for CHIMERA. From Fig. 9 we see that the proposed system with GLRT outperforms both the CHIMERA-based defense mechanisms, in each considered scenario, by lowering by at least one order of magnitude p_{FA} for a fixed p_{MD}.

VI. Conclusion

In this paper we have proposed a general model to characterize the spoofing detection problem in GNSSs when the spoofer observes the legitimate signal, abstracting from the specific modulation formats and cryptographic mechanisms. We have shown that effective detection can be achieved by relying only on the combination of signals from multiple SVs and on the diversity between the attacker position and the intended forged position. We have also investigated a class of attack strategies based on the statistics of the transmitted and received signals, which are shown to be optimal for minimizing the K-L divergence metric. The optimal attack strategy turned out to be a proper linear transformation of the signal received at the attacker position, combined with an appropriately tuned independent additive Gaussian noise. We have derived a lower bound on the K-L divergence, which depends only on the total length of the transmitted signals, on the SNR of the legitimate channel, and on the difference between the forged and the legitimate channel matrices. Moreover, we have discussed the results obtained in relation to different modulation schemes; we have shown that when the attack strategy is the optimal one, with Gaussian or finite-cardinality signaling we get the same performance in terms of K-L divergence. Then, we found a Nash equilibrium of the attack-defense scheme deriving the optimal defense strategy against the above-mentioned attack, which, in turn, is described by a Gaussian distribution. Finally, the performance of the detection schemes against the proposed attack has been analyzed through numerical simulations considering two verification mechanisms: LRT and GLRT.

Appendix A
Symmetry of the K-L Divergence

In this Appendix, we provide a proof of the symmetry of the K-L divergence when the attacker uses the optimal attack strategy $p^{\star}_{\boldsymbol{v}|z}$, presented in Section III, and $\boldsymbol{K}_{\boldsymbol{\eta}} = \boldsymbol{K}_{\mathbf{B}}$, that is

$$\mathbb{D}(p_{\boldsymbol{x}\boldsymbol{v}^{\star}} \| p_{\boldsymbol{x}\boldsymbol{y}}) = \mathbb{D}(p_{\boldsymbol{x}\boldsymbol{y}} \| p_{\boldsymbol{x}\boldsymbol{v}^{\star}}). \tag{42}$$

For any $p_{\boldsymbol{v}|z} \in \mathcal{C}$, $\mathbb{D}(p_{\boldsymbol{x}\boldsymbol{y}} \| p_{\boldsymbol{x}\boldsymbol{v}})$ can be computed following the same procedure as in (21), therefore we get

$$\begin{aligned}\mathbb{D}(p_{\boldsymbol{x}\boldsymbol{y}} \| p_{\boldsymbol{x}\boldsymbol{v}}) =& \frac{1}{2}\Bigg[\log\frac{|\boldsymbol{K}_{\boldsymbol{\eta}}|}{|\boldsymbol{K}_{\mathbf{B}}|} + \mathrm{tr}(\boldsymbol{K}_{\mathbf{B}}\boldsymbol{K}_{\boldsymbol{\eta}}{}^{-1}) \\ &+ \mathrm{tr}\left((\boldsymbol{A}-\boldsymbol{B})\boldsymbol{K}_{\boldsymbol{x}}(\boldsymbol{A}-\boldsymbol{B})^{\mathrm{H}}\boldsymbol{K}_{\mathbf{B}}{}^{-1}\right) - (n+\delta_{\mathrm{f}})\Bigg] \\ =& \frac{1}{2}\left[\sum_{i=1}^{n+\delta_{\mathrm{f}}}\left(\frac{\sigma_{\mathrm{B}}^2}{\lambda_i} - \log\left(\frac{\sigma_{\mathrm{B}}^2}{\lambda_i}\right)\right) - (n+\delta_{\mathrm{f}})\right] \\ &+ \frac{1}{2\sigma_{\mathrm{B}}^2}\mathrm{tr}\left((\boldsymbol{A}-\boldsymbol{B})\boldsymbol{K}_{\boldsymbol{x}}(\boldsymbol{A}-\boldsymbol{B})^{\mathrm{H}}\right)\end{aligned} \tag{43}$$

When the attack strategy is $p^{\star}_{\boldsymbol{v}|z}$ and $\boldsymbol{K}_{\boldsymbol{\eta}} = \boldsymbol{K}_{\mathbf{B}}$, we have that $\lambda_i = \sigma_{\mathrm{B}}^2, \forall i \in \{1, 2, \ldots, n+\delta_{\mathrm{f}}\}$. Therefore, we obtain

$$\begin{aligned}\mathbb{D}(p_{\boldsymbol{x}\boldsymbol{y}} \| p_{\boldsymbol{x}\boldsymbol{v}^{\star}}) &= \frac{1}{2\sigma_{\mathrm{B}}^2}\mathrm{tr}\left((\boldsymbol{A}-\boldsymbol{B}^{\star})\boldsymbol{K}_{\boldsymbol{x}}(\boldsymbol{A}-\boldsymbol{B}^{\star})^{\mathrm{H}}\right) \\ &= \mathbb{D}_{\min}(\boldsymbol{B}^{\star}) = \mathbb{D}(p_{\boldsymbol{x}\boldsymbol{v}^{\star}} \| p_{\boldsymbol{x}\boldsymbol{y}}).\end{aligned} \tag{44}$$

References

[1] Z. Wu, Y. Zhang, Y. Yang, C. Liang, and R. Liu, "Spoofing and anti-spoofing technologies of global navigation satellite system: A survey," *IEEE Access*, vol. 8, pp. 165444–165496, 2020.

[2] D. Margaria, B. Motella, M. Anghileri, J.-J. Floch, I. Fernandez-Hernandez, and M. Paonni, "Signal structure-based authentication for civil GNSSs: Recent solutions and perspectives," *IEEE Signal Process. Mag.*, vol. 34, no. 5, pp. 27–37, Sep. 2017.

[3] M. L. Psiaki and T. E. Humphreys, "GNSS spoofing and detection," *Proc. IEEE*, vol. 104, no. 6, pp. 1258–1270, Jun. 2016.

[4] K. Zhang and P. Papadimitratos, "On the effects of distance-decreasing attacks on cryptographically protected GNSS signals," in *Proc. Int. Tech. Meeting The Inst. Navigat.*, Feb. 2019, pp. 363–372.

[5] T. E. Humphreys, "Detection strategy for cryptographic GNSS anti-spoofing," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 49, no. 2, pp. 1073–1090, Apr. 2013.

[6] G. Caparra, N. Laurenti, R. Ioannides, and C. Massimo, "Improving secure code estimate-replay attacks and their detection on GNSS signals," in *Proc. ESA Workshop Satell. Navigat. Technol. Eur. Workshop GNSS Signals Signal Process. (NAVITEC)*, 2014, pp. 1–8.

[7] J. T. Curran and M. Paonni, "Securing GNSS: An end-to-end feasibility analysis for the Galileo open-service," in *Proc. 27th Int. Tech. Meeting Satell. Division Inst. Navigat.*, Tampa, FL, USA, 2014, pp. 2828–2842.

[8] G. Caparra and J. T. Curran, "On the achievable equivalent security of GNSS ranging code encryption," in *Proc. IEEE/ION Position, Location Navigat. Symp. (PLANS)*, Apr. 2018, pp. 956–966.

[9] R. Terris-Gallego, I. Fernandez-Hernandez, J. A. López-Salcedo, and G. Seco-Granados, "Guidelines for Galileo assisted commercial authentication service implementation," in *Proc. Int. Conf. Localization GNSS (ICL-GNSS)*, Jun. 2022, pp. 01–07.

[10] I. Fernandez-Hernandez et al., "Semi-assisted signal authentication based on Galileo ACAS," 2022, *arXiv:2204.14026*.

[11] I. Fernández-Hernández, V. Rijmen, G. Seco-Granados, J. Simon, I. Rodríguez, and J. D. Calle, "A navigation message authentication proposal for the Galileo open service," *Navigation*, vol. 63, no. 1, pp. 85–102, Mar. 2016.

[12] I. F. Hernández, T. Ashur, V. Rijmen, C. Sarto, S. Cancela, and D. Calle, "Toward an operational navigation message authentication service: Proposal and justification of additional OSNMA protocol features," in *Proc. Eur. Navigat. Conf. (ENC)*, Apr. 2019, pp. 1–6.

[13] M. G. Kuhn, "An asymmetric security mechanism for navigation signals," in *Proc. Int. Workshop Inf. Hiding*, 2005, pp. 239–252.

[14] L. Scott, "Anti-spoofing & authenticated signal architectures for civil navigation systems," in *Proc. Inst. Navigat. GPS/GNSS Conf.*, 2003, pp. 1543–1552.

[15] L. Scott, "Proving location using GPS location signatures: Why it is needed and a way to do it," in *Proc. 26th Int. Tech. Meeting Satell. Division Inst. Navigat.*, Nashville, TN, USA, 2013, pp. 2880–2892.

[16] *Space Vehicles Directorate, Chips Message Robust Authentication (CHIMERA) Enhancement for the L1C Signal: Space Segment/User Segment Interface*, Standard IS-AGT-100, Air Force Research Laboratory, Apr. 2019.

[17] J. M. Anderson et al., "Chips-message robust authentication (Chimera) for GPS civilian signals," in *Proc. 30th Int. Tech. Meeting Satell. Division Inst. Navigat.*, Nov. 2017, pp. 2388–2416.

[18] B. Motella, D. Margaria, and M. Paonni, "SNAP: An authentication concept for the Galileo open service," in *Proc. IEEE/ION Position, Location Navigat. Symp. (PLANS)*, Apr. 2018, pp. 967–977.
[19] S. Wang, H. Liu, Z. Tang, and B. Ye, "Binary phase hopping based spreading code authentication technique," *Satell. Navigat.*, vol. 2, no. 1, pp. 1–9, Feb. 2021, Art. no. 4.
[20] O. Pozzobon, L. Canzian, M. Danieletto, and A. D. Chiara, "Anti-spoofing and open GNSS signal authentication with signal authentication sequences," in *Proc. 5th ESA Workshop Satell. Navigat. Technol. Eur. Workshop GNSS Signals Signal Process. (NAVITEC)*, Dec. 2010, pp. 1–6.
[21] O. Pozzobon, G. Gamba, M. Canale, and S. Fantinato, "Supersonic GNSS authentication codes," in *Proc. 27th Int. Tech. Meeting Satell. Division Inst. Navigat.*, Tampa, FL, USA, 2014, pp. 2862–2869.
[22] N. Laurenti and A. Poltronieri, "Optimal compromise among security, availability and resources in the design of sequences for GNSS spreading code authentication," in *Proc. Int. Conf. Localization GNSS (ICL-GNSS)*, Jun. 2020, pp. 1–6.
[23] F. Formaggio and S. Tomasin, "Authentication of satellite navigation signals by wiretap coding and artificial noise," *EURASIP J. Wireless Commun. Netw.*, vol. 2019, no. 1, pp. 1–17, Apr. 2019, Art. no. 98.
[24] E. D. Kaplan and C. J. Hegarty, *Understanding GPS, Principles and Applications*, 2nd ed. Norwood, MA, USA: Artech House, 2005.
[25] I. Fernández-Hernández, T. Ashur, and V. Rijmen, "Analysis and recommendations for MAC and key lengths in delayed disclosure GNSS authentication protocols," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 57, no. 3, pp. 1827–1839, Jun. 2021.
[26] L. Crosara, F. Ardizzon, S. Tomasin, and N. Laurenti, "Performance evaluation of an indistinguishability based attack against spreading code secured GNSS signals," in *Proc. IEEE/ION Position, Location Navigat. Symp. (PLANS)*, Apr. 2023, pp. 542–552.
[27] T. E. Humphreys, B. A. Ledvina, M. L. Psiaki, B. W. O'Hanlon, and P. M. Kitner, "Assessing the spoofing threat," *GPS World*, vol. 20, no. 1, pp. 28–38, 2009.
[28] S. M. Kay, *Fundamentals of Statistical Signal Processing*, vol. 2. Upper Saddle River, NJ, USA: Prentice-Hall, 1993.
[29] U. M. Maurer, "Authentication theory and hypothesis testing," *IEEE Trans. Inf. Theory*, vol. 46, no. 4, pp. 1350–1356, Jul. 2000.
[30] C. Cachin, "An information-theoretic model for steganography," in *Proc. 2nd Int. Workshop Inf. Hiding (IH)*, in Lecture Notes in Computer Science, vol. 1525, 1998, pp. 306–318.
[31] 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.
[32] G. N. Yannakakis and J. Togelius, *Artificial Intelligence and Games*. Cham, Switzerland: Springer, 2018.
[33] J. Von Neumann and O. Morgenstern, *Theory of Games and Economic Behavior*. Princeton, NJ, USA: Princeton Univ. Press, 1947.
[34] O. Zeitouni, J. Ziv, and N. Merhav, "When is the generalized likelihood ratio test optimal?" *IEEE Trans. Inf. Theory*, vol. 38, no. 5, pp. 1597–1602, Sep. 1992.
[35] F. Formaggio, S. Ceccato, F. Basana, N. Laurenti, and S. Tomasin, "GNSS spoofing detection techniques by cellular network cross-check in smartphones," in *Proc. 32nd Int. Tech. Meeting Satell. Division Inst. Navigat.*, Oct. 2019, pp. 3904–3916.
[36] F. Ardizzon, L. Crosara, N. Laurenti, S. Tomasin, and N. Montini, "Authenticated timing protocol based on Galileo ACAS," *Sensors*, vol. 22, no. 16, p. 6298, Aug. 2022.

Laura Crosara (Graduate Student Member, IEEE) received the B.Sc. degree in information engineering and the M.Sc. degree in telecommunications engineering from the University of Padova, Italy, in 2019 and 2021, respectively, where she is currently pursuing the Ph.D. degree in information engineering with the Department of Information Engineering, under the supervision of Prof. N. Laurenti. Her current research interests include authentication techniques for global navigation satellite systems, physical layer security, and wireless communications.

Francesco Ardizzon (Member, IEEE) received the B.Sc., M.Sc., and Ph.D. degrees in information engineering from the University of Padova, Italy, in 2016, 2019, and 2023, respectively. Since 2022, he has been a Visiting Scientist with the ESA European Space Research and Technology Centre. He is currently an Assistant Professor with the University of Padova. His current research interests include authentication for global navigation satellite systems, physical layer security, and underwater acoustic communications.

Stefano Tomasin (Senior Member, IEEE) received the Ph.D. degree from the University of Padova, Italy, in 2003. He was Visiting Faculty with Qualcomm, San Diego, CA, in 2004, the Polytechnic University in Brooklyn, NY, in 2007, and the Mathematical and Algorithmic Sciences Laboratory of Huawei, Paris, France, in 2015. He joined the University of Padova, where he has been a Full Professor, since 2022. His current research interests include physical layer security, security of global navigation satellite systems, signal processing for wireless communications, synchronization, and scheduling of communication resources. He has been a member of EURASIP, since 2011. He has been a Deputy Editor-in-Chief of the IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, since January 2023.

Nicola Laurenti received the Ph.D. degree in electrical and telecommunication engineering from the University of Padua, Italy, in 1999. In 2001, he became an Assistant Professor with the Department of Information Engineering, University of Padua. From 2008 to 2009, he was a Visiting Scholar with the Coordinated Science Laboratory, University of Illinois at Urbana-Champaign. He is currently an Associate Professor with the Department of Information Engineering, University of Padua. He leads the Research Laboratory on GNSS Security there and has been the Principal Investigator in two projects on GNSS Open Service Signal Integrity Protection and Authentication at the Physical Layer, funded by the European Space Agency. He has been the Unit Leader in several research projects, publicly funded by European and Italian institutions. His research interests include wireless security at the physical, data link and network layers, unconditional security, and quantum key distribution systems.

Open Access funding provided by 'Università degli Studi di Padova' within the CRUI CARE Agreement