On Mixing Authenticated and Non-Authenticated Signals Against GNSS Spoofing

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

***Abstract*— Anti-spoofing techniques for current global navigation satellite systems (GNSS) authenticate signals on a single band and from a single system. However, nowadays commercial GNSS receivers commonly calculate the position, velocity, and time (PVT) solution by simultaneously utilizing signals from multiple constellations and bands, with a substantial enhancement in both accuracy and availability. Therefore, anti-spoofing techniques have recently been proposed that mix authenticated and on-authenticated signals to increase performance without sacrificing security. In this paper, we formalize the models of such signal mixture-based authentication checks. We propose a spoofing attack generating a fake signal that leads the victim to a target PVT solution, undetected. We analytically relate the degrees of freedom of the attacker in manipulating the victim's solution to both the employed security checks and the number of open non-authenticated signals that can be tampered with by the attacker. The performance of the considered attack strategies are tested on an experimental dataset. Finally, we assess the limits of PVT-based GNSS authentication checks where both authenticated and non-authenticated signals are used.**

***Index Terms*— PVT assurance, signal authentication, spoofing, GNSS.**

I. Introduction

GLOBAL navigation satellite systems (GNSS) provide positioning and timing for various civil and military applications. However, GNSS signals are susceptible to both accidental and intentional interference due to their observable weak received signal power. Therefore, an attacker can compromise location and timing-aware applications using *spoofing attacks* i.e., by sending fake GNSS signals, leading the receiver into the calculation of a forged location or time [1], [2], [3]. Furthermore, civilian GNSS signals and modulation formats are open to the public [4], [5]. This means that it is indeed possible for the attacker to ignore the legitimate signals and use a so-called *signal generation attacks*, generating new GNSS signals with correct modulation formats and spreading code but fake phase and frequency. Additionally, several works have reported successful attacks even using off-the-shelf hardware [6], [7].

To counter spoofing attacks, several techniques have been proposed, to be implemented either at the receiver side or in a more system-wide manner. Receiver-side techniques are, typically, consistency checks [8], [9], [10], [11], [12], [13], [14], [15]. A relevant example is *signal quality monitoring* (SQM), where the user monitors a set of metrics evaluating the quality of the correlation peaks [10], or the received signal strength, and checks that the received signal power or the carrier-to-noise-ratio matches a predefined statistic [11]. Alternatively, a receiver may use an inertial measurement unit (IMU) [13] to confirm the acceleration and movement direction, or antenna arrays to detect the angle-of-arrival of the received GNSS signals and reject signals coming from anomalous directions [12]. Other techniques involve consistency check with the position, velocity, and time (PVT) solution obtained from a cellular network [15]. Although effective in many practical applications, these techniques exhibit two main drawbacks. First, they rely on additional hardware (antenna arrays, IMU) or additional sources of information (SQM, cellular network). Second, they assume the attacker is not capable of replicating the legitimate signals exactly.

System-wide authentication mechanisms instead incorporate unpredictable features as a signature into the broadcast GNSS signals so that a verification-enabled receiver can then elaborate on these characteristics to distinguish authentic signals from forgeries. The features can be inserted at data and ranging levels. Navigation message authentication (NMA) [16], [17], adds a signature on the navigation data. Ranging-level authentication works at the spreading code level, which can be either signed (as in spreading code authentication (SCA)), or fully encrypted (as in spreading code encryption (SCE)). In both cases, the correct spreading code is not public and is distributed only to the intended legitimate users (often a posteriori). Ranging-level techniques can effectively complement data-level ones since they are less vulnerable to secure code estimation and replay (SCER) type attacks [18], [19]. Examples of authentication in existing systems include assisted commercial authentication service (ACAS) and chips-message robust authentication (CHIMERA). ACAS is a SCE solution proposed for Galileo that complements open service (OS)-NMA by offering ranging-level authentication in the E6 band [20], [21]. For GPS, CHIMERA [22], [23] aims at jointly authenticating the navigation data and the spreading code of GPS signals for civil usage, implementing both NMA and SCA.

Manuscript received 30 March 2023; revised 28 August 2023, 27 October 2023, 10 February 2024, and 19 March 2024; accepted 19 March 2024. Date of publication 25 March 2024; date of current version 6 May 2024. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Hossein Pishro-Nik. *(Corresponding author: Francesco Ardizzon.)*

Francesco Ardizzon and Laura Crosara are with the Department of Information Engineering, Università degli Studi di Padova, 35131 Padua, Italy (e-mail: ardizzonfr@dei.unipd.it; crosaralau@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.2024.3381473

An issue with all the system-wide spoofing detection techniques is that they only authenticate signals for a single constellation and most often, for a single component. Thus a receiver aiming to compute an authenticated PVT solution, has to discard all the other signals. On the other hand, GNSS receivers typically exploit signals of all available components and constellations, to increase the ranging measurements and improve the availability and the accuracy of the PVT solution. So, a receiver may use both authenticated and non-authenticated signals thereby trading off security against accuracy. Alternatively, receivers may also authenticate non-protected signals by performing consistency checks with authenticated signals, i.e., trusted anchors. The non-protected signals passing the check will be included in the PVT, while the others will not be considered as trusted and thus discarded. We call such a strategy an authentication cross-check. Thus, by choosing the selectivity of the authentication cross-checks it is possible to find the trade-off between security and navigation performance. Still, an in-depth security analysis of these techniques is not available in the literature and their weakness against more sophisticated attacks has not been formally studied.

With the aim of improving the trustfulness of the PVT, [24] discusses a stepwise approach wherein the receiver exploits the authenticated signals as trust anchors for the complete PVT solution. One of the checks from [24] has been included in [21] to verify the consistency between the encrypted E6C and the open E1B Galileo measurements. Still, the effectiveness of that approach degrades when including signals from different systems, especially in urban scenarios.

In [25], an authentication cross-check is proposed to enhance the Galileo ranging level protection by leveraging on the combination of CHIMERA and open service navigation message authentication (OS-NMA) single system authentication. Knowing that the GPS and the Galileo reference times are related by the GPS-to-Galileo time offset (GGTO) [26], a consistency check is made between the measured local clock biases and the GGTO retrieved from the navigation messages. However, in [25] the security of the scheme is only shown against an attack with naively forged signals.

In this paper, we investigate the security vulnerabilities of authentication cross-checks to advanced spoofing attack strategies, and establish how secure these checks can effectively be depending on system parameters and mechanisms features. To do so we derive advanced spoofing attack strategies targeting authentication cross-checks, and probing their vulnerabilities. In particular, we assume that the protected signals are authenticated by a ranging level mechanism and no other check is used by the receiver,[1] which has to solely rely on system-wide security mechanisms and authentication cross-checks.

More in detail, the main contributions of the paper are the following.

1) A novel general framework for the PVT authentication cross-checks is introduced that i) abstracts from the specific implementation details; ii) includes the existing or proposed cross-check techniques as particular cases; iii) allows to find new attacks (see next point); and iv) can be applied to evaluate the performance and limitations of any (existing or future proposal) cross-authentication technique. To the best of the authors' knowledge, such a general framework is not available in the literature.
2) Previously unknown attack strategies that break the authentication cross-checks proposed in [25] and other approaches based on the same principle, and a novel generation time spoofing attack of the signal generation type.
3) The limits of the novel attacks are analytically investigated, for instance, by relating the degrees of the freedom of the attacker in manipulating the victim's solution to the parameters of the transmission/propagation scenario.
4) The attack effectiveness is evaluated by simulation considering both a noiseless and a realistic noisy scenario.
5) The feasibility and real-world effectiveness of the attacks are assessed by using an experimental dataset collected by a Septentrio PolarRx5 receiver.

This paper shows significant vulnerabilities of the emerging approach of mixing authenticated and non-authenticated signals and calls for a revision of solutions such as [25] before their possible adoption in future standards.

The rest of this paper is organized as follows. Section II introduces the system model. Section III provides a general model for the PVT-based authentication checks. Then, Section IV describes the proposed attack strategies. Section VI presents the numerical results, obtained from the experimental dataset. Finally, Section VII provides the conclusions.

List of Abbreviations

ACAS	assisted commercial authentication service
AWGN	additive white Gaussian noise
CHIMERA	chips-message robust authentication
DET	detection error trade-off
GDOP	geometric dilution of precision
GGTO	GPS-to-Galileo time offset
GNSS	global navigation satellite systems
ICTO	inter-constellation time offset
NMA	navigation message authentication
OS	open service
OS-NMA	open service navigation message authentication
PDOP	position dilution of precision
PVT	position, velocity, and time
SCA	spreading code authentication
SCE	spreading code encryption
SCER	secure code estimation and replay

II. System Model

We consider a multi-constellation receiver acquiring signals from $M > 1$ constellations. A subset of the received signals is authenticated ranging level, i.e., protected by a SCE (or SCA) mechanism. It is assumed that no fault can happen in the authentication assessment of these signals; thus, the attacker cannot generate new signals to replace the authenticated ones.

In general, the victim receiver obtains signals from N visible satellites: N_{A} are authenticated while the remaining $N_{\mathrm{O}} = N - N_{\mathrm{A}}$ are open (i.e., non-authenticated). For ease of notation,

[1] Or that the spoofer is a sophisticated attacker able to fool these consistency checks.

the authenticated satellites are indexed by $j = 1, \ldots, N_{\mathrm{A}}$, while non-authenticated satellites are indexed by $j = N_{\mathrm{A}} + 1, \ldots, N$. After acquisition and tracking (see, e.g., [27, Ch. 5]), the receiver obtains a vector of pseudorange measurements $\boldsymbol{r} = [r_1, \ldots, r_{\mathrm{N}}]^{\mathrm{T}}$.

We define as PVT solution in legitimate conditions[2]

$$\boldsymbol{p}_{\mathrm{M}} = [x,\ y,\ z,\ t_1,\ \ldots,\ t_M]^{\mathrm{T}}\,, \tag{1}$$

denoting the receiver's three-dimensional position in Earth-centered Earth-fixed (ECEF) coordinates, and the clock biases, one per each time reference. The actual derivation is described in Appendix A. Alternatively, the receiver may consider only a single time reference, e.g., one among the GNSS time references or the coordinated universal time (UTC), and relate the others to the first, correcting them by using the respective inter-constellation time offset (ICTO) [28, Ch. 21]. In this case, as outlined in Appendix B, the solution is

$$\boldsymbol{p}_{\mathrm{S}} = [x,\ y,\ z,\ t]^{\mathrm{T}}\,. \tag{2}$$

We remark that in both (1) or (2) the position and timing computation procedure is analogous. Thus for ease of reading, both will be denoted as $\boldsymbol{p}$, distinguishing between the two when necessary.

For instance, as the time corrections can be obtained from a trusted source, e.g., from the navigation data authenticated by OS-NMA in Galileo E1 BC, such information is considered to be authenticated and exploited for security purposes. In these cases, the receiver must estimate each clock bias separately from the others, as in (1), before the actual check. On the other hand, when the assessment is based, for instance, on the receiver position, formulation (2) will be considered.

A. PVT Solution

This Section provides a high-level description of how GNSS receivers typically compute the PVT solution, which later will be used as input for the authentication cross-checks.

At each epoch, position and time are computed following an iterative approach, starting from the initial solution $\hat{\boldsymbol{p}} = [\hat{x}, \hat{y}, \hat{z}, \hat{t}_1, \ldots, \hat{t}_M]^{\mathrm{T}}$, or $\hat{\boldsymbol{p}} = [\hat{x}, \hat{y}, \hat{z}, \hat{t}]^{\mathrm{T}}$, depending on whether the receiver aims to get (1) or (2), respectively. In particular, $\hat{\boldsymbol{p}}$ is the PVT solution computed at the previous epoch or a predefined starting point (*cold start*). The approach follows a linearization procedure, where the PVT solution is related to the range by the geometry matrix $\boldsymbol{G}$. Thus, given the range measurement of the jth signal r_j and its estimate $\hat{r}_j$, the *range residual* is

$$\Delta r_j = r_j - \hat{r}_j\,. \tag{3}$$

Next, observe that the pseudorange displacement $\Delta\boldsymbol{r}$ is related to the position displacement $\Delta\boldsymbol{p}$ as

$$\Delta\boldsymbol{r} = \boldsymbol{G}\Delta\boldsymbol{p} = \begin{bmatrix}\boldsymbol{G}_{\mathrm{A}}\\ \boldsymbol{G}_{\mathrm{O}}\end{bmatrix}\Delta\boldsymbol{p}\,, \tag{4}$$

where the geometry matrix $\boldsymbol{G}$ is row-wise divided into $\boldsymbol{G}_{\mathrm{A}}$ and $\boldsymbol{G}_{\mathrm{O}}$, corresponding to the authenticated and the open signals, respectively. From the previous relation, it follows that $\Delta\boldsymbol{p}$ can be computed from $\Delta\boldsymbol{r}$ as

$$\Delta\boldsymbol{p} = (\boldsymbol{G}^{\mathrm{T}}\boldsymbol{G})^{-1}\boldsymbol{G}^{\mathrm{T}}\Delta\boldsymbol{r} \triangleq \boldsymbol{H}\Delta\boldsymbol{r}\,, \tag{5}$$

[2]Note that we neglect the computation of the velocity, focusing instead on position and timing.

where $\boldsymbol{H}$ is the Moore-Penrose pseudoinverse of $\boldsymbol{G}$, often called also *least-squares solution* matrix. We remark that the components of matrix $\boldsymbol{H}$ depend only on the relative geometry between the user and the N satellites participating in the least-squares computation. Finally the position is updated as $\hat{\boldsymbol{p}}' = \hat{\boldsymbol{p}} + \Delta\boldsymbol{p}$, where $\hat{\boldsymbol{p}}'$ is the starting point for the next iteration.

The iterative procedure continues until either i) the maximum number of iterations is reached or ii) the solution update is smaller than a user-defined step, i.e., $\|\Delta\boldsymbol{p}\| < \xi$. More details about the procedure and the derivation of each term are reported in the Appendix A and B.

B. Attacker Model

In this Section, we detail the attacker's capabilities and operations. It is assumed that the message data (e.g., atmospheric corrections and ephemeris) are retrieved from a publicly available authenticated side channel and that the actual victim receiver position is known by the attacker. We take into consideration two distinct attacks:

Generation attack: This attack consists of the generation and transmission of fake GNSS signals, corresponding possibly different PVT solutions than the one computed using the legitimate signals.

Relay attack: This attack, sometimes referred to as *meaconing*, consists of sampling, recording, and relaying the entire modulated signal with unchanged code and data.

The attacker can generate, relay, or selectively delay the open signals, since, in this case, both the spreading code and the message content are entirely public. On the other hand, the attacker can only use a relay attack on authentication signals. Generation attacks cannot instead be performed as these are protected at ranging-level, and the attacker has no knowledge of the actual signed spreading code

We assume that the victim under attack acquires and locks onto the forged signals transmitted by the attacker. This is achieved, for instance, by increasing the transmitting power of the forged signals or canceling the legitimate open ones.

The attacker aims at inducing the victim receiver to obtain as PVT solution a target $\boldsymbol{p}^\star$ solution instead of the authentic solution $\boldsymbol{p}$. However, there exist targets $\boldsymbol{p}^\star$ that are not reachable, as will be discussed in Section IV. The attacker will choose the target as the closest solution to $\boldsymbol{p}^\star$ looking among those that do not raise an alarm at the victim receiver. To achieve this goal, they tamper the signals propagation times, altering the range residuals $\Delta\boldsymbol{r}$ by a term $\Delta\boldsymbol{r}_{\mathrm{T}}$, such that, when under attack, (4) and (5) become respectively

$$\Delta\boldsymbol{r}^\star \triangleq \Delta\boldsymbol{r} + \Delta\boldsymbol{r}_{\mathrm{T}} = \boldsymbol{G}(\Delta\boldsymbol{p} + \Delta\boldsymbol{p}_{\mathrm{T}})\,, \tag{6}$$

$$\Delta\boldsymbol{p}^\star \triangleq \Delta\boldsymbol{p} + \Delta\boldsymbol{p}_{\mathrm{T}} = \boldsymbol{H}\Delta\boldsymbol{r}^\star\,. \tag{7}$$

This means that the range tampering $\Delta\boldsymbol{r}_{\mathrm{T}}$ causes a displacement $\Delta\boldsymbol{p}_{\mathrm{T}}$. So, the PVT solution update induced by the attacker is

$$\boldsymbol{p}^\star = \hat{\boldsymbol{p}} + \Delta\boldsymbol{p}^\star = \hat{\boldsymbol{p}} + \Delta\boldsymbol{p} + \Delta\boldsymbol{p}_{\mathrm{T}}\,. \tag{8}$$

We remark that the linear approximation (7) holds when the pseudorange displacement $\Delta\boldsymbol{r}_{\mathrm{T}}$ introduced by the attacker is

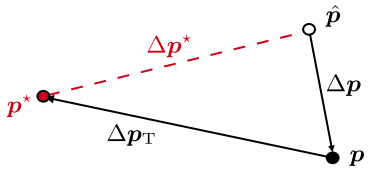


Fig. 1. Example of the scenario under attack: $\hat{p}$ is the solution at the iteration start, p is the legitimate solution, $p^\star$ is the attacker target solution obtained by mixing open and tampered signals.

small with respect to r [27, Ch. 7]. In Section VI,the effectiveness of this linearization-based attack is assessed by evaluating the attack performance as a function of the magnitude of the pseudorange displacements to be induced, i.e., the distance between the target $p^\star$ and the real position p.

Fig. 1 shows the displacement of the attacker PVT solution due to the attacker tampering: in legitimate conditions, starting from $\hat{p}$, the receiver would compute Δp to obtain the legitimate solution p (in blue). In turn, the attacker wants to lead the receiver to the target $p^\star$ (in red), thus they tamper the signals, causing the alteration Δp_{T}. Notice that Fig. 1 may represent the actual 3D position or the whole PVT solution space, i.e., considering points in the $3+M$ space.

For the sake of clarity, we will distinguish between authenticated and non-authenticated ranges residuals, $\Delta r_{\mathrm{T,A}}$ and $\Delta r_{\mathrm{T,O}}$, that the attacker introduces to the authenticated and non authenticated signals, respectively

$$\Delta r_{\mathrm{T}} = \begin{bmatrix} \Delta r_{\mathrm{T,A}} \\ \Delta r_{\mathrm{T,O}} \end{bmatrix}. \tag{9}$$

Finally, it is natural to partition the least square matrix as $H = [H_{\mathrm{A}}\, H_{\mathrm{O}}]$, where H_{A} and H_{O} represent the matrix associated to the authenticated and the open signals, respectively. In particular, since the attacker can only perform a relay attack on the authenticated signals, the attacker modification on the authenticated signal ranges is modeled as $\Delta r_{\mathrm{T,A}} = k\mathbf{1}$, where $\mathbf{1}$ is the column vector filled with all ones. Indeed, when performing a generation attack, the attacker sets $k = 0$, i.e., only the open signals are actually fake.

III. Models for PVT-Based Authentication Cross-Checks

The receiver computes the PVT solution using both authenticated and non-authenticated ranges. Next, to assess its authenticity, it performs one or more consistency checks on the PVT result (or in part of it). We use decision theory to describe the problem and consider the two hypotheses

$\mathcal{H}_0$: PVT is legitimate, signals are legitimate,

$\mathcal{H}_1$: PVT is fake, signals have been tampered with.

The consistency check provides one of the two decision

$\hat{\mathcal{H}}_0$: Check passed, PVT solution is legitimate

$\hat{\mathcal{H}}_1$: Check failed, PVT solution is not legitimate.

This allows us to define the *false alarm* and *missed detection* probabilities as

$$p_{\mathrm{FA}} = P(\hat{\mathcal{H}}_1|\mathcal{H}_0)\,, \quad p_{\mathrm{MD}} = P(\hat{\mathcal{H}}_0|\mathcal{H}_1)\,. \tag{10}$$

The next Sections describe the classes of consistency checks to authenticate the PVT, also related to the required service.

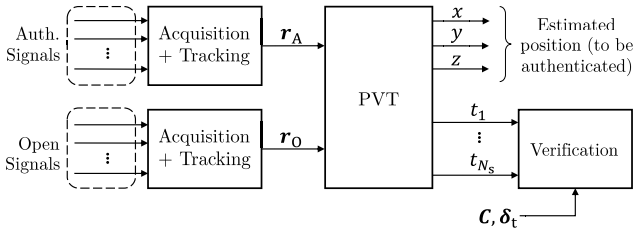


Fig. 2. Block scheme of the time-based check.

A. Time-Based Checks for Navigation Services

The receiver collects signals from M different GNSS and computes p as in (1). More in detail, p contains the position coordinates and M clock biases, one per GNSS time reference, obtained as in Appendix A. The time references are related by the ICTO, thus the receiver considers the solution to be authentic if

$$\theta_{\mathrm{t}} \triangleq Cp \leq \delta_{\mathrm{t}}\,, \tag{11}$$

where C is a matrix that selects and relates a pair of clock biases (with the appropriate sign), while δ_{t} contains an upper bound of the expected ICTO, eventually tuned to meet a predefined false alarm. The mechanism for time-based checks is summarized in Fig. 2. Matrix C has $N_{\mathrm{c}} = 2\,(M-1)$ rows, with δ_{t} containing $M-1$ upper-bounds on the measured ICTO and equally as many lower bounds. Therefore, C has only $M-1$ linearly independent rows. The i-th row of C is c_i: this will be associated to the i-th element of δ_{t}, $\delta_{\mathrm{t},i}$, such that the i-th check will be $\theta_{\mathrm{t},i} = c_i H r \leq \delta_{\mathrm{t},i}$. We remark that a meaconing attack operating on all the signals is often not a viable option for the attacker, since even if it goes undetected by (11), in general, it fails as p will be the attacker position rather than an arbitrary target $p^\star$.

For instance, in [25], the authors propose to authenticate the computed PVT solution through a time consistency check. In particular, the signals from the two constellations, one transmitting authenticated signals and the other transmitting open signals, are combined to compute the position and timing (Appendix A). Then, denoting as t_1 and t_2 the clock biases associated with the time reference of each constellation, the PVT solution is verified by checking if the difference between the time correction is consistent with the reference ICTO, as

$$|(t_2 - t_1) - b - \mathrm{ICTO}| < T\,, \tag{12}$$

where T is a threshold that is set by the receiver, and b is a bias set during the calibration phase. More details about the security check and the parameters' derivation are reported in [25]. Check (12) can be framed in (11), by choosing

$$C = \begin{bmatrix} 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & -1 & 1 \end{bmatrix}, \quad \delta_{\mathrm{t}} = \begin{bmatrix} T + b + \mathrm{ICTO} \\ T - b - \mathrm{ICTO} \end{bmatrix}. \tag{13}$$

This means that the attacker must craft a Δr_{T} that changes the estimated time offset by at most $\delta_{\mathbf{t}}$. In the rest of the paper, we will refer to this scheme as *ICTO-based authentication cross-check*.

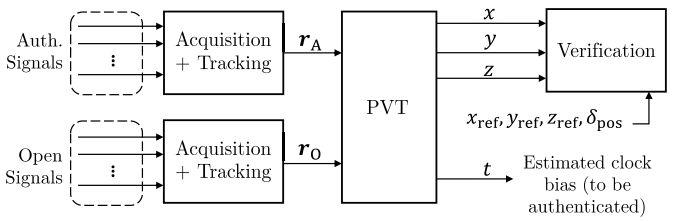


Fig. 3. Block scheme of the position-based check.

B. Position-Based Checks for Timing Services

The goal here is to provide a secure GNSS-based timing source. We assume the receiver knows a priori its position, whose coordinates are denoted by x_{ref}, y_{ref}, and z_{ref}, that may be obtained either by computing the PVT solution using only authenticated ranges, from a secure side channel, or it can be a priori known (e.g., in a static scenario). However, none of these solutions provide a reliable timing correction. Hence, the receiver exploits all the available measurements, both authenticated and open, and obtains the position and time $\boldsymbol{p}$, as outlined in Appendix B. To verify its authenticity, the receiver verifies that the reconstructed position is consistent with its a priori knowledge of the position, verifying that

$$\theta_{\text{pos}} \triangleq \sqrt{\boldsymbol{\xi}^{\text{T}}\boldsymbol{\xi}} \leq \delta_{\text{pos}}\,, \tag{14}$$

where $\boldsymbol{\xi} \triangleq [x_{\text{ref}} - x, y_{\text{ref}} - y, z_{\text{ref}} - z]^{\text{T}}$ is the 3D position displacement with respect to the reference position. If the check passes, i.e., the position computed using all the signals is coherent with the reference one, the solution is considered safe and the receiver uses the timing correction from $\boldsymbol{p}$ to correct the local clock. An example of such a setting is described in [29]. The position-based check is summarized in Fig. 3.

IV. Proposed Attack Strategies

This Section describes the attack strategies that alter the PVT solution without alerting the victim receiver. First, we focus on the ideal noiseless scenario, where the signals received by the attacker and the victim are unaffected by noise. The attack will be generalized for an additive white Gaussian noise (AWGN) channel scenario in Section V.

To be successful, the attacker must alter only the non-protected signals, and choose the $\Delta\boldsymbol{r}_{\text{T}}$ such that $\Delta\boldsymbol{p}^{\star}$ passes the check employed by the victim, and leads the victim to the PVT target $\boldsymbol{p}^{\star}$. In this first phase, we assume that the victim receives the signals as intended by the attacker. Moreover, we consider that the attacker knows the pseudoranges $\boldsymbol{r}$ that the victim would measure in the legtimate scenario. Section V analyzes the scenario wherein the attacker cannot pre-compensate the channel, and the victim receives a noisier copy of the tampered signal.

In the following Sections, we derive the attacking strategies for the timing and the position-based checks. The first is intended for receivers that obtain the ICTOs from a trusted source (e.g., OS-NMA) and want to provide secure positioning. The latter targets timing receivers, where the position is known a priori (e.g., static scenario with calibration with a trusted source), but the receiver has to provide instead secure timing information.

A. Generation Attack Against Time-Based Checks

Consider a legitimate receiver employing the check described in Section III-A, where the PVT solution is considered to be authentic if the clock bias differences are consistent with the ICTOs derived from a side channel.

The first step is to identify the set of *feasible solutions* that do not raise an alarm at the receiver. Next, a solution that leads the receiver's estimated position close to the target position $\boldsymbol{p}^{\star}$, is selected. To identify the set of feasible solutions, the following result can be used.

Theorem 1: Given a constraint vector $\boldsymbol{\delta}'$, the set of feasible solutions for the attacker containing all the range alterations that do not raise an alarm in (11) is the affine space

$$S = \left\{\Delta\boldsymbol{r}_{\text{p}} + s\,,\, s \in \mathcal{N}(\boldsymbol{C}\boldsymbol{H}_{\text{O}})\right\}\,, \tag{15}$$

where $\Delta\boldsymbol{r}_{\text{p}}$ is a solution of $\boldsymbol{\delta}' = \boldsymbol{C}\boldsymbol{H}_{\text{O}}\Delta\boldsymbol{r}_{\text{T,O}}$, and $\mathcal{N}(\boldsymbol{X})$ is the null space of $\boldsymbol{X}$. Moreover, it holds

$$\dim(S) = N_{\text{O}} - M + 1\,. \tag{16}$$

Proof: Condition (11) requires

$$\boldsymbol{C}\boldsymbol{p}^{\star} = \boldsymbol{C}\hat{\boldsymbol{p}} + \boldsymbol{C}\Delta\boldsymbol{p}^{\star} = \boldsymbol{C}\hat{\boldsymbol{p}} + \boldsymbol{C}\Delta\boldsymbol{p} + \boldsymbol{C}\Delta\boldsymbol{p}_{\text{T}} \leq \boldsymbol{\delta}_{\text{t}}\,. \tag{17}$$

We assume that, in the legtimate scenario, the check (11) is passed, thus, $\boldsymbol{C}\hat{\boldsymbol{p}} + \boldsymbol{C}\Delta\boldsymbol{p} = \boldsymbol{\delta}'' \leq \boldsymbol{\delta}_{\text{t}}$: for instance, this models also the case where the defender's measurements are affected by noise. So, to avoid raising an alarm, the attacker can choose any alteration that induces a change smaller than $\boldsymbol{\delta}_{\text{t}} - \boldsymbol{\delta}''$, i.e., from (17) the shift induced by the attacker is

$$\boldsymbol{C}\Delta\boldsymbol{p}_{\text{T}} \triangleq \boldsymbol{\delta}'\,,\quad \boldsymbol{\delta}' \leq \boldsymbol{\delta}_{\text{t}} - \boldsymbol{\delta}''\,. \tag{18}$$

By using (5) and considering that only non-protected signals can be manipulated by the attacker, we have

$$\begin{aligned}\boldsymbol{\delta}' = \boldsymbol{C}\Delta\boldsymbol{p}_{\text{T}} = \boldsymbol{C}\boldsymbol{H}\Delta\boldsymbol{r}_{\text{T}} = \boldsymbol{C}\begin{bmatrix}\boldsymbol{H}_{\text{A}} & \boldsymbol{H}_{\text{O}}\end{bmatrix}\begin{bmatrix}\boldsymbol{0}\\ \Delta\boldsymbol{r}_{\text{T,O}}\end{bmatrix}\\ = \boldsymbol{C}\boldsymbol{H}_{\text{O}}\Delta\boldsymbol{r}_{\text{T,O}}\,.\end{aligned} \tag{19}$$

The attacker controls $\boldsymbol{\delta}'$, thus they can choose it such that $\boldsymbol{\delta}' \in \mathcal{R}(\boldsymbol{C}\boldsymbol{H}_{\text{O}})$, so that (19) has at least one solution. Indeed, $\text{rank}(\boldsymbol{C}\boldsymbol{H}_{\text{O}}) = M - 1$, since $\boldsymbol{C}$ has $M - 1$ linearly independent rows.[3] The matrix resulting from the product $\boldsymbol{C}\boldsymbol{H}_{\text{O}}$ has size $N_{\text{c}} \times N_{\text{O}}$.

Hence, by the Rouché-Capelli's theorem, (19) describes a linear undetermined system that admits infinitely many solutions, belonging to the affine space S as defined in (15), where $\Delta\boldsymbol{r}_{\text{p}}$ is any particular solution of (19), which can be found, for instance, by Gaussian elimination. Moreover, since the dimension of an affine space is the dimension of its associated linear space, it holds

$$\begin{aligned}\dim(S) &= \dim(\mathcal{N}(\boldsymbol{C}\boldsymbol{H}_{\text{O}}))\\ &= N_{\text{O}} - \text{rank}(\boldsymbol{C}\boldsymbol{H}_{\text{O}}) = N_{\text{O}} - M + 1 > 1\,.\end{aligned} \tag{20}$$

[3]We made the tacit assumption that $N_{\text{O}} \geq M$ and that the geometry are such that $\boldsymbol{C}\boldsymbol{H}_{\text{O}}$ is full row rank.

So, each solution of (19) depends on $N_{\mathrm{O}} - M + 1$ parameters. □

Theorem 1 has two main consequences. First, let us consider the worst-case scenario for the attacker, where the legitimate range residuals $\Delta\boldsymbol{r}$ are such it yields $\boldsymbol{C}\Delta\boldsymbol{p} = \boldsymbol{\delta}$. In this case, there is no margin for the attacker that, from (18), has to pick an attack with $\boldsymbol{\delta}' = 0$. Still, (15) shows that it is possible to lead a successful attack, by picking ranges from the null space $\mathcal{N}(\boldsymbol{C}\boldsymbol{H}_{\mathrm{O}})$. Secondly, it shows that the increased number of signals used in the PVT computation by the legitimate receiver potentially leads to an increased degree of freedom given to the attacker to manipulate the fake PVT solution, since the dimension of the null space increases. In general, using more open signals improves the accuracy of the PVT estimation. Therefore, a trade-off between accuracy and security is at stake here. However, there may be scenarios where $N_{\mathrm{A}} < 4$, therefore no fully authenticated PVT solution is available at all. In these cases, the victim receiver has to increase the number of the open signals used for the PVT solution or not compute any solution at all. We remark that the attacker is assumed to know the satellites in view by the victim. Thus, the attacker tampers with the whole set of measurements $\boldsymbol{r}_{\mathrm{T}}$ used by the victim. This means that even using a subset of such measurement will still lead to the target position $\boldsymbol{p}^{\star}$.

Next, we derive the actual range alterations that lead the victim receiver to the target position $\boldsymbol{p}^{\star}$ by considering the worst-case scenario for the attacker, where $\boldsymbol{\delta}' = \boldsymbol{0}$. In this case, (19) describes a linear homogeneous system whose solutions belong to the linear space $S = \mathcal{N}(\boldsymbol{C}\boldsymbol{H}_{\mathrm{O}})$. Indeed, this boils down to the general case by adding in the calculations a range vector related to the particular solution $\Delta\boldsymbol{r}_{\mathrm{p}}$. Thus, any solution belonging to S can be written as

$$\Delta\boldsymbol{r}_{\mathrm{T}} = \begin{bmatrix}\boldsymbol{u}_1 & \dots & \boldsymbol{u}_K\end{bmatrix}\begin{bmatrix}\alpha_1 \\ \dots \\ \alpha_K\end{bmatrix} = \boldsymbol{U}\boldsymbol{\alpha}\,, \tag{21}$$

where $\boldsymbol{u}_1, \dots, \boldsymbol{u}_K$ is an orthonormal basis of S, $\alpha_k \in \mathbb{R}$, $\forall k = 1, \dots, K$, and $K \triangleq \dim(S)$. Notice that $\boldsymbol{U}$ is a matrix with $3 + M$ rows and K columns.

From (6)-(8), it holds

$$\boldsymbol{\Delta p}^{\star} - \boldsymbol{\Delta p} = \boldsymbol{\Delta p}_{\mathrm{T}} = \boldsymbol{H}\boldsymbol{U}\boldsymbol{\alpha}\,, \tag{22}$$

where in the last step we have used the fact that the attacker will only use the range alterations that do not raise an alarm, i.e., belonging to (15) so having the form in (21).

Resorting to the Moore-Penrose pseudoinverse, we obtain

$$\boldsymbol{\alpha}^{\star} = \left(\boldsymbol{U}^{\mathrm{T}}\boldsymbol{H}^{\mathrm{T}}\boldsymbol{H}\boldsymbol{U}\right)^{-1}\boldsymbol{U}^{\mathrm{T}}\boldsymbol{H}^{\mathrm{T}}\left(\Delta\boldsymbol{p}^{\star} - \Delta\boldsymbol{p}\right)\,. \tag{23}$$

Finally, plugging this in (21), we obtain the target range alteration

$$\Delta\boldsymbol{r}_{\mathrm{T}}^{\star} = \alpha_1^{\star}\boldsymbol{u}_1 + \dots + \alpha_K^{\star}\boldsymbol{u}_K\,. \tag{24}$$

Indeed, as required, this attack will not raise any alarm while taking the victim exactly to $\boldsymbol{p}^{\star}$.

Attack Against the GGTO-Based Authentication Cross-Check: We consider the authentication procedure in [25] and exploit the previous analysis to derive the attack. This technique considers only signals from Galileo and GPS, thus $M = 2$. According to (16), we expect to find a space of feasible solutions S with size $\dim(S) = N_{\mathrm{O}} - 1$. We consider the worst-case scenario for the attacker where $\boldsymbol{\delta}' = \boldsymbol{0}$. Combining (13) and (19) and denoting as $\boldsymbol{h}_{\mathrm{O},i}$ the i-th row of $\boldsymbol{H}_{\mathrm{O}}$, we have

$$\boldsymbol{C}\boldsymbol{H}_{\mathrm{O}}\Delta\boldsymbol{r}_{\mathrm{T,O}} = \boldsymbol{0} \Leftrightarrow (\boldsymbol{h}_{\mathrm{O},4} - \boldsymbol{h}_{\mathrm{O},5})\Delta\boldsymbol{r}_{\mathrm{T,O}} = 0\,. \tag{25}$$

Thus, $\Delta\boldsymbol{r}_{\mathrm{T,O}}$ belongs to the null space $\mathcal{N}(\boldsymbol{h}_{\mathrm{O},4} - \boldsymbol{h}_{\mathrm{O},5})$. This corresponds to the orthogonal complement to the space generated by column vector $(\boldsymbol{h}_{\mathrm{O},4} - \boldsymbol{h}_{\mathrm{O},5})^{\mathrm{T}}$, or

$$S = \mathcal{N}(\boldsymbol{h}_{\mathrm{O},4} - \boldsymbol{h}_{\mathrm{O},5}) = \left\langle(\boldsymbol{h}_{\mathrm{O},4} - \boldsymbol{h}_{\mathrm{O},5})^{\mathrm{T}}\right\rangle^{\perp}\,. \tag{26}$$

Considering that $\boldsymbol{h}_{\mathrm{O},4}$ and $\boldsymbol{h}_{\mathrm{O},5}$ are column vectors of length N_{O}, the null space in (26) has clearly size $N_{\mathrm{O}} - 1$ and, as expected, $\dim(S) = N_{\mathrm{O}} - 1$.

B. Attack Against Position-Based Checks

We consider the class of checks described in Section III-B. Here, the victim is using GNSS for timing, while it is monitoring its own position for the security check. Indeed, in such condition the position is well-known, so the attacker can only tamper the timing estimation, and induce a PVT shift of the type

$$\Delta\boldsymbol{p}_{\mathrm{T}} = \boldsymbol{H}\Delta\boldsymbol{r}_{\mathrm{T}} = [\boldsymbol{\xi}\ c\gamma_{\mathrm{T}}]^{\mathrm{T}}\,,\ \text{subj. to}\ \|\boldsymbol{\xi}\| \le \delta_{\mathrm{pos}}\,, \tag{27}$$

where $c\gamma_T$ is the time shift that the attacker aims to induce to the victim clock. The constraint assures that no alarm is raised at the legitimate receiver, since (14) is satisfied.

The next paragraphs will derive a relay and a generation attack against the position-based check. Using either one, the attacker is able to induce the target time shift (27). While a generation attack may be preferable since, for instance, it does not introduce additional noise at the victim due to the attacker receiver noise, we will prove that it can only be performed if $N_{\mathrm{O}} \ge 4$ signals are used by the victim.

1) Relay Attack Against the Position-Based Check: Starting from (27), a first solution for the attack is computed straightly from (4) as

$$\Delta\boldsymbol{r}_{\mathrm{T}} = \boldsymbol{G}\Delta\boldsymbol{p}_{\mathrm{T}} = c\gamma_T\boldsymbol{1} + \boldsymbol{G}\boldsymbol{\xi}\,, \tag{28}$$

where $\boldsymbol{1}$ is a vector of ones with the same size as $\boldsymbol{p}$. In the worst-case scenario for the attacker, $\delta_{\mathrm{pos}} = 0$, i.e., no change in the position is tolerated at the legitimate receiver, it yields $\|\boldsymbol{\xi}\| = 0$ and thus $\Delta\boldsymbol{r}_{\mathrm{T}} = c\gamma_T\boldsymbol{1}$. This means that the attacker has to receive, record, and retransmit both authenticated and open signals with an additional delay, as is typically the case for the meaconing attack. This also shows that when $\boldsymbol{\xi} \neq \boldsymbol{0}$ the chosen solution differs by (at most) $\boldsymbol{G}\boldsymbol{\xi}$ from the meaconing solution.

Finally notice that, as pointed out in Section II-B, this attack can be performed even when the ranges are authenticated by SCE or SCA. So, this attack is only feasible if the attacker is close enough to the victim, as the position computed by the victim is actually the attacker's position. If this does not occur, it will induce a different position calculation, that will alert the victim. However, especially when considering realistic scenarios, relay attacks may introduce additional noise. Thus, if possible, the attacker would rather use a generation attack even for position-based checks.

2) Generation Attack Against Position-Based Checks: In this Section, we derive this attack. Additionally, we show under which conditions it is possible for the attacker to perform such an attack against the position-based check. The attacker aims at finding a $\Delta \boldsymbol{r}_{\mathrm{T}}$ that induces a time shift equal to $c\gamma_{\mathrm{T}}$ on the estimated clock bias, solving (27). For ease of reading, we focus on the worst-case scenario where $\delta_{\mathrm{pos}} = 0$, or equivalently $\|\boldsymbol{\xi}\| = 0$.

Analogously to the procedure outlined in Section IV-A, the set of solutions for (27) is

$$V = \left\{ \Delta \boldsymbol{r}_{\mathrm{p}} + s \, , s \in \mathcal{N}(\boldsymbol{H}) \right\} , \tag{29}$$

where the particular solution is the relay attack $\Delta \boldsymbol{r}_{\mathrm{p}} = c\gamma_{\mathrm{T}} \mathbf{1}$.

Indeed, $\boldsymbol{H}$ is $4 \times N$ and $\mathrm{rank}(\boldsymbol{H}) = 4$, therefore

$$\dim(\mathcal{N}(\boldsymbol{H})) = \mathcal{R}(\boldsymbol{H}) - \mathrm{rank}(\boldsymbol{H}) = N - 4. \tag{30}$$

We remark that to compute the PVT result, it always holds $N \geq 4$, so $\dim(\mathcal{N}(\boldsymbol{H})) \geq 0$. Hence, any range tampering that induces the target time shift, can be written as

$$v = c\gamma_{\mathrm{T}} \mathbf{1} + \sum_{n=1}^{N-4} \beta_n \boldsymbol{u}_n = c\gamma_{\mathrm{T}} \mathbf{1} + \boldsymbol{U}\boldsymbol{\beta} \, , \tag{31}$$

where vectors $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_{N-4}$ form a basis for the null space $\mathcal{N}(\boldsymbol{H})$, collected as the columns of the basis matrix $\boldsymbol{U}$.

Our aim is to find the range tampering that belongs to V and does not require any alteration on the authenticated ranges. This latter requirement is formalized as

$$\boldsymbol{U}_{N_{\mathrm{A}}} \boldsymbol{\beta} + c\gamma_{\mathrm{T}} \mathbf{1}_{N_{\mathrm{A}}} = 0 \, , \tag{32}$$

where $\boldsymbol{U}_{N_{\mathrm{A}}}$ and $\mathbf{1}_{N_{\mathrm{A}}}$ collect the first N_{A} rows of $\boldsymbol{U}$ and $\mathbf{1}$, respectively.

A sufficient condition for (32) to admit at least one solution is that $\boldsymbol{U}_{N_{\mathrm{A}}}$, with size $N_{\mathrm{A}} \times (N-4)$, has to be left invertible. This happens if $N_{\mathrm{A}} < N - 4$ or, equivalently, $N_{\mathrm{O}} > 4$.[4]

Moreover this also assures that $c\gamma_{\mathrm{T}} \mathbf{1}_{N_{\mathrm{A}}} \in \mathcal{R}(\boldsymbol{H})$. Under this condition, the coefficients vector is computed as

$$\boldsymbol{\beta}^{\star} = -c\gamma_{\mathrm{T}} \left(\boldsymbol{U}_{N_{\mathrm{A}}}^{\mathrm{T}} \boldsymbol{U}_{N_{\mathrm{A}}} \right)^{-1} \boldsymbol{U}_{N_{\mathrm{A}}}^{\mathrm{T}} \mathbf{1}_{N_{\mathrm{A}}} \, . \tag{33}$$

Finally, for the generation attack, the attacker has to pick ranges

$$\Delta \boldsymbol{r}_{\mathrm{T}}^{\star} = c\gamma_{\mathrm{T}} \mathbf{1} + \sum_{n=1}^{N-4} \beta_n^{\star} \boldsymbol{u}_n \, . \tag{34}$$

Indeed, by construction of $\boldsymbol{\beta}^{\star}$, $\Delta r_n^{\star} = 0$ for $1 \leq n \leq N_{\mathrm{A}}$, hence only the open signals need be tampered.

In conclusion, this shows that if $N_{\mathrm{O}} \geq 4$, the attacker can exploit the just described procedure to perform a generation-type attack that alters the victim time by a factor γ_{T}, generating only the open signals.

[4]Under the condition $N_{\mathrm{O}} > 4$, $\boldsymbol{U}_{N_{\mathrm{A}}}$ is left invertible only if the basis vectors $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_{N-4}$ of the null space $\mathcal{N}(\boldsymbol{H})$ are chosen in such a way that $\boldsymbol{U}_{N_{\mathrm{A}}}$ has full row rank.

V. Analysis for the Realistic Scenario

This Section analyzes the proposed attacks performance in a realistic scenario that takes into account the noise at the victim and the attacker receivers. We remark that, when the attacker performs a generation attack, the fake signals are only affected by the noise added at the victim receiver. While, when the attacker performs a relay attack, the tampered signals are affected by both the noises produced by the victim's and the attacker's receivers. Let us assume that the channels between the satellites and the receivers, of both the attacker and the victim, are AWGN, as well as the channel between the attacker and the victim. We denote with σ_{L} and σ_{A} the noise standard deviations at the victim and attacker receiver, respectively. Moreover, as typically done for GNSS, we assume each channel to be independent, with equal variance.

The noise affects the pseudorange estimations, thus, the covariance matrices of the legitimate and tampered pseudoranges residuals, respectively, are

$$\boldsymbol{\Sigma}_{\mathrm{L}} = \mathrm{cov}(\Delta \boldsymbol{r}) \triangleq \sigma_{\mathrm{L}}^2 \boldsymbol{I}_N \, , \quad \boldsymbol{\Sigma}_{\mathrm{T}} = \mathrm{cov}(\Delta \boldsymbol{r}^{\star}) \triangleq \sigma_{\mathrm{T}}^2 \boldsymbol{I}_N \, , \tag{35}$$

where $\sigma_{\mathrm{T}}^2 = \sigma_{\mathrm{L}}^2$ when the attacker performs a generation attack, and $\sigma_{\mathrm{T}}^2 = \sigma_{\mathrm{L}}^2 + \sigma_{\mathrm{A}}^2$ when they perform a relay attack. Moreover, the legitimate pseudorange residuals are zero-mean, at the convergence of the PVT iterative computation. Taking into account the additional tampering introduced by the attacker, the tampered pseudoranges mean is

$$\mathbb{E}\left[\Delta \boldsymbol{r}^{\star} | \mathcal{H}_1 \right] = \mathbb{E}\left[\Delta \boldsymbol{r} + \Delta \boldsymbol{r}_{\mathrm{T}} \right] = \Delta \boldsymbol{r}_{\mathrm{T}} \, . \tag{36}$$

The next Sections will separately consider the attacks to the timing and the position-based checks.

A. Attacks to the Time-Based Checks

Our aim is to statistically characterize the vector $\boldsymbol{\theta}_{\mathrm{t}}$, defined in (11), in realistic conditions. Indeed, $\boldsymbol{\theta}_{\mathrm{t}} = \boldsymbol{C}\boldsymbol{H}\Delta \boldsymbol{r}$ is a Gaussian vector since it is derived from the linear combination of the Gaussian vector $\Delta \boldsymbol{r}$. Thus, it is characterized by its mean and covariance, considering both legitimate and under-attack conditions.

In the legitimate scenario, $\mathcal{H}_0$, the mean is

$$\mathbb{E}[\boldsymbol{\theta}_{\mathrm{t}} | \mathcal{H}_0] = \boldsymbol{C}\boldsymbol{H}\mathbb{E}[\Delta \boldsymbol{r} | \mathcal{H}_0] = 0 \, , \tag{37}$$

while the covariance of $\boldsymbol{\theta}_{\mathrm{t}}$ in $\mathcal{H}_0$ is

$$\begin{aligned} \boldsymbol{\Sigma}_{\mathbf{0}} &\triangleq \mathbb{E}\left[\boldsymbol{\theta}_{\mathrm{t}} \boldsymbol{\theta}_{\mathrm{t}}^{\mathrm{T}} | \mathcal{H}_0 \right] = \mathbb{E}\left[\boldsymbol{C}\boldsymbol{H}\Delta \boldsymbol{r} (\boldsymbol{C}\boldsymbol{H}\Delta \boldsymbol{r})^{\mathrm{T}} | \mathcal{H}_0 \right] \\ &= \boldsymbol{C}\boldsymbol{H}\mathbb{E}\left[\Delta \boldsymbol{r} \Delta \boldsymbol{r}^{\mathrm{T}} \right] \boldsymbol{H}^{\mathrm{T}} \boldsymbol{C}^{\mathrm{T}} = \sigma_{\mathrm{L}}^2 \boldsymbol{C}\boldsymbol{H}\boldsymbol{H}^{\mathrm{T}} \boldsymbol{C}^{\mathrm{T}} \, , \end{aligned} \tag{38}$$

where the last step uses the definition of $\boldsymbol{\Sigma}_L$ given in (35).

For the under-attack scenario, $\mathcal{H}_1$, the mean is given by

$$\mathbb{E}[\boldsymbol{\theta}_{\mathrm{t}} | \mathcal{H}_1] = \boldsymbol{C}\boldsymbol{H}\Delta \boldsymbol{r}_{\mathrm{T}} \triangleq \boldsymbol{\mu} \, , \tag{39}$$

while, analogously to (38), the covariance of $\boldsymbol{\theta}_{\mathrm{t}}$ in $\mathcal{H}_1$ is

$$\boldsymbol{\Sigma}_{\mathbf{1}} \triangleq \mathbb{E}\left[\boldsymbol{\theta}_{\mathrm{t}} \boldsymbol{\theta}_{\mathrm{t}}^{\mathrm{T}} | \mathcal{H}_1 \right] = \sigma_{\mathrm{T}}^2 \boldsymbol{C}\boldsymbol{H}\boldsymbol{H}^{\mathrm{T}} \boldsymbol{C}^{\mathrm{T}} \, . \tag{40}$$

where the last equality follows from the definition of $\boldsymbol{\Sigma}_T$ given in (35). Moreover, the attack to the time-based check described in Section IV-A is a generation attack, thus $\sigma_{\mathrm{T}}^2 = \sigma_{\mathrm{L}}^2$.

The false alarm and miss detection probabilities are, respectively,

$$p_{\mathrm{FA}} = \mathcal{P}\left[\bigcup_{i=1}^{N_\sqcup}\{\theta_{\sqcup,i} > \delta_{\sqcup,i}\}\middle|\mathcal{H}_0\right] = 1-\mathrm{P}\left[\bigcap_{i=1}^{N_\mathrm{c}}\{\theta_{\mathrm{t},i} \le \delta_{\mathrm{t},i}\}\middle|\mathcal{H}_0\right], \tag{41}$$

$$p_{\mathrm{MD}} = \mathcal{P}\left[\bigcap_{i=1}^{N_\sqcup}\{\theta_{\sqcup,i} \le \delta_{\sqcup,i}\}\middle|\mathcal{H}_1\right]. \tag{42}$$

We remark that, in general, metrics $\theta_{\mathrm{t},i}$ and $\theta_{\mathrm{t},j}$, with $i \neq j$, are not statistically independent.

Attack Against the ICTO-Based Authentication Cross-Check: Consider now the check of [25], where only Galileo and GPS are considered. First, neglect the bias $b + GGTO$, which can be subtracted in advance from one measurement. So, it yields $\delta_{\mathrm{t},1} = \delta_{\mathrm{t},2} = T$. Moreover, from (13), $\boldsymbol{c}_1 = -\boldsymbol{c}_2$, thus also $\theta_{\mathrm{t},1} = -\theta_{\mathrm{t},2}$, and (41) becomes

$$\begin{aligned} p_{\mathrm{FA}} &= 1 - P(\theta_{\mathrm{t},1} < T \wedge \theta_{\mathrm{t},2} < T|\mathcal{H}_0) \\ &= 1 - P(-\delta_1 < \theta_{\mathrm{t},1} < T|\mathcal{H}_0) = 2Q(T/\sigma_0)\,, \end{aligned} \tag{43}$$

where $\sigma_0 = \sigma_{\mathrm{L}}\sqrt{\boldsymbol{c}_1\boldsymbol{H}\boldsymbol{H}^{\mathrm{T}}\boldsymbol{c}_1^{\mathrm{T}}}$. Next, we can invert the above relation to computing the threshold values as a function of the p_{FA} set by the receiver,

$$T = \sigma_0 \mathrm{Q}^{-1}\left(\frac{1}{2}p_{\mathrm{FA}}\right). \tag{44}$$

Analogously, calling μ_1 and μ_2 the first and second element of $\boldsymbol{\mu}$, respectively, the miss detection probability is

$$\begin{aligned} p_{\mathrm{MD}} &= P(\theta_{\mathrm{t},1} \le \delta_{\mathrm{t},1} \wedge \theta_{\mathrm{t},2} \le \delta_{\mathrm{t},2}|\mathcal{H}_1) \\ &= \mathrm{Q}\left(\frac{-T-\mu_1}{\sigma_1}\right) - \mathrm{Q}\left(\frac{T-\mu_1}{\sigma_1}\right) \\ &= \mathrm{Q}\left(-\frac{\sigma_0}{\sigma_1}\mathrm{Q}^{-1}\left(\frac{1}{2}p_{\mathrm{FA}}\right) - \frac{\mu_1}{\sigma_1}\right) \\ &\quad - \mathrm{Q}\left(\frac{\sigma_0}{\sigma_1}\mathrm{Q}^{-1}\left(\frac{1}{2}p_{\mathrm{FA}}\right) - \frac{\mu_1}{\sigma_1}\right), \end{aligned} \tag{45}$$

where $\mu_1 = -\mu_2 = \boldsymbol{c}_1\boldsymbol{H}\Delta\boldsymbol{r}_{\mathrm{T}}$ and $\sigma_1 = \sigma_{\mathrm{T}}\sqrt{\boldsymbol{c}_1\boldsymbol{H}\boldsymbol{H}^{\mathrm{T}}\boldsymbol{c}_1^{\mathrm{T}}}$. Thus, (45) shows the missed detection probability as a function of the false alarm, legitimate and attacker channel noises, and $\boldsymbol{\mu}$. In particular, $\boldsymbol{\mu}$ is also related to the range alteration induced by the attacker, which is a function of the distance between the true solution $\boldsymbol{p}$ and the target $\boldsymbol{p}^\star$.

In a generation attack scenario, where $\sigma_0 = \sigma_1$, for small values of μ_1, from (45) we get $p_{\mathrm{MD}} = 1 - p_{\mathrm{FA}}$, which means that fake signals are indistinguishable from the legitimate ones. This shows that the success probability depends on μ_1, the amount of displacement induced by the attacker, so that the more the attacker tries to tamper with the signals, the easier it is for the victim to detect the attack. For instance, if we consider a relay attack for position spoofing, as *selective delay*, then $\sigma_1 \gg \sigma_0$, i.e., the noise standard deviation of the tampered pseudoranges is higher than that of the legitimate ones, $p_{\mathrm{MD}} \to 0$ for any chosen p_{FA}, thus the receiver is always able to detect the attack. Section VI-C will provide a numerical evaluation of these observations.

B. Attacks to the Position-Based Checks

This Section aims at statistically characterizing the term θ_{pos} in (14), in a realistic environment, i.e., when the measurements are affected by noise, by relating security performance, i.e., false and miss detection, to the channel noise in the legitimate and under-attack scenarios, σ_{L}^2 and σ_{T}^2. Notice that, in the legitimate case, this problem is equivalent to the general problem of characterizing the position accuracy for GNSS.

From (14), we can write

$$\theta_{\mathrm{pos}}^2 = \boldsymbol{\xi}^{\mathrm{T}}\boldsymbol{\xi}\,, \tag{46}$$

where $\boldsymbol{\xi}$ is the 3D position displacement with respect to the reference position. We remark that the reference position (with coordinates $[x_{\mathrm{ref}}, y_{\mathrm{ref}}, z_{\mathrm{ref}}]$) is assumed to be known without error. Thus, to characterize the performance of the test (14) let us model term $\boldsymbol{\xi}$ first. Indeed, $\boldsymbol{\xi}$ is a Gaussian vector since the position is derived as a linear combination of the Gaussian random vector $\Delta\boldsymbol{r}$, as in (5). In the legitimate case,

$$\mathbb{E}[\boldsymbol{\xi}|\mathcal{H}_0] = 0\,, \tag{47}$$

since the PVT solution is expected to converge to the reference position itself. For the covariance

$$\mathbb{E}[\boldsymbol{\xi}\boldsymbol{\xi}^{\mathrm{T}}|\mathcal{H}_0] = \sigma_{\mathrm{L}}^2\boldsymbol{H}_{1-3}\boldsymbol{H}_{1-3}^{\mathrm{T}}\,, \tag{48}$$

where $\boldsymbol{H}_{1-3}$ denotes the first three rows in $\boldsymbol{H}$.

Under attack, we have

$$\mathbb{E}[\boldsymbol{\xi}|\mathcal{H}_1] = \boldsymbol{H}_{1-3}\Delta\boldsymbol{r}_{\mathrm{T}}\,, \tag{49}$$

and, for the covariance,

$$\mathbb{E}[\boldsymbol{\xi}\boldsymbol{\xi}^{\mathrm{T}}|\mathcal{H}_0] = \sigma_{\mathrm{T}}^2\boldsymbol{H}_{1-3}\boldsymbol{H}_{1-3}^{\mathrm{T}}\,. \tag{50}$$

Note that (46) is a quadratic form, so we can take advantage of the following Theorem.

Theorem 2: The random variable $\theta_{\mathrm{pos}}^2 = \boldsymbol{\xi}^{\mathrm{T}}\boldsymbol{\xi}$, with $\boldsymbol{\xi} \sim \mathcal{N}(\boldsymbol{\mu}, \boldsymbol{\Sigma})$, can be written as

$$\theta_{\mathrm{pos}}^2 = (\boldsymbol{u}+\boldsymbol{b})\,\boldsymbol{\Lambda}\,(\boldsymbol{u}+\boldsymbol{b}) = \sum_i^3 \lambda_i(u_i+b_i)^2\,, \tag{51}$$

where $\boldsymbol{u} \sim \mathcal{N}(\boldsymbol{0}, \boldsymbol{I}_3)$, $\boldsymbol{\Lambda}$ is the diagonal matrix obtained from the decomposition $\boldsymbol{\Sigma} = \boldsymbol{P}\boldsymbol{\Lambda}\boldsymbol{P}^{\mathrm{T}}$ and $\boldsymbol{b}^{\mathrm{T}} = \boldsymbol{P}^{\mathrm{T}}\boldsymbol{\Sigma}^{-\frac{1}{2}}\boldsymbol{\mu}$. Hence, θ_{pos}^2 can be expressed as the linear combination of non-central chi-square random variables of degree 1, with non-centrality parameter b_i^2.

Proof: The proof can be found in [30, Ch. 3], for the quadratic form $Q(\boldsymbol{X}) = \boldsymbol{X}^{\mathrm{T}}\boldsymbol{A}\boldsymbol{X}$, but using $\boldsymbol{A} = \boldsymbol{I}$. □

Indeed, in the legitimate case, $\boldsymbol{\xi}$ has zero mean, thus, θ^2 is actually the linear combination of (central) chi-square random variables of degree 1. Still, it is not possible to derive the closed-form expression for either the false alarm or miss detection probabilities, thus relating the metric value, θ_{pos} to the chosen threshold.

For an application-oriented (but approximate) derivation of such relation, let us exploit the definition of geometric dilution of precision (GDOP) [27, Ch. 7]. First, the reference system is rotated to have the first three coordinates pointing to the east-north-up reference frame. Next, by repeating the steps in (48),

$$\mathbb{E}\left[\Delta\boldsymbol{p}\Delta\boldsymbol{p}^{\mathrm{T}}\right] = \sigma_L^2\boldsymbol{H}\boldsymbol{H}^{\mathrm{T}} = \sigma_L^2\left(\boldsymbol{G}^{\mathrm{T}}\boldsymbol{G}\right)^{-1}. \tag{52}$$

Hence, taking the trace operation, the GDOP is given by

$$\text{GDOP} = \frac{1}{\sigma_L}\sqrt{\sigma_{\text{E}}^2 + \sigma_{\text{N}}^2 + \sigma_{\text{U}}^2 + \sigma_{\text{t}}^2}\,, \tag{53}$$

where σ_{E}^2, σ_{N}^2, and σ_{U}^2 are the variances associated respectively with the error along the East, North, and vertical directions while σ_{t}^2 is the error for the clock bias (measured in meters). To focus on the position error, it is useful to consider the position dilution of precision (PDOP)

$$\text{PDOP} \triangleq \frac{1}{\sigma_L}\sqrt{\sigma_{\text{E}}^2 + \sigma_{\text{N}}^2 + \sigma_{\text{U}}^2}\,, \tag{54}$$

These terms are used to model, and therefore also to predict, the positioning error since the GDOP values are related to the pseudorange noise and the geometry. Thus, low GDOP values are typically associated with high PVT solution accuracy. An additional in-depth discussion of the GDOP and their derivation can be found in [28, Ch. 21].

Hence, it is possible to use this characterization to describe $p(\theta_{\text{pos}}|\mathcal{H}_0)$ and $p(\theta_{\text{pos}}|\mathcal{H}_1)$. Still, these estimates would be based only on an approximate model which is not suited for security analysis. The performance of the position check will be therefore evaluated only numerically, in Section VI-C.

VI. Numerical Results

In this Section, we assess the performance of the proposed attack against the authentication mechanism discussed in Section III. More in detail, first we describe the data collection procedure and the validation phase. Next, we test both the attacks of Section IV, considering both noiseless and noisy scenarios.

A. Data Collection

The dataset was built by collecting signals from a quasi-urban environment with a Septentrio PolarRx5 receiver connected to an A42 Hemisphere antenna. In particular, the measurements were collected from our lab window sill (45.408° N, 11.894° E, altitude 30 m above the sea level).

The receiver output was post-processed obtaining a dataset of measurements from different constellations. We focused on GPS L1 C/A and Galileo E1 BC. The dataset contains 10 min of measurements, collected with a frequency of 1 Hz, for a total of 600 PVT epochs. We consider the GPS signals as authenticated (e.g., by CHIMERA) and the Galileo signals as open, and we collected signals from $N = 8$ different satellites in view, with $N_{\text{A}} = 3$ and $N_{\text{O}} = 5$.

More in detail, for each considered epoch, the dataset contains the pseudorange measurements, the satellite clock biases, the tropospheric and the ionospheric delays (estimated using the Klobuchar model [31]), and the satellite positions. Satellite clock biases, atmospheric delays, and satellite positions were derived from the respective navigation message.

To test the performance of the attacks, we implemented a PVT computation block operating as summarized in the Appendices, following the description of [32, Ch. 8].

To validate our PVT block, we report in Fig. 4 respectively the positions computed by the Septentrio receiver, in red, and those computed by our PVT block, in blue. The positions obtained from the Septentrio receiver are slightly more precise than ours: the error standard deviations were 3.03 m and 3.13 m using, respectively, the Septentrio receiver and our PVT block.

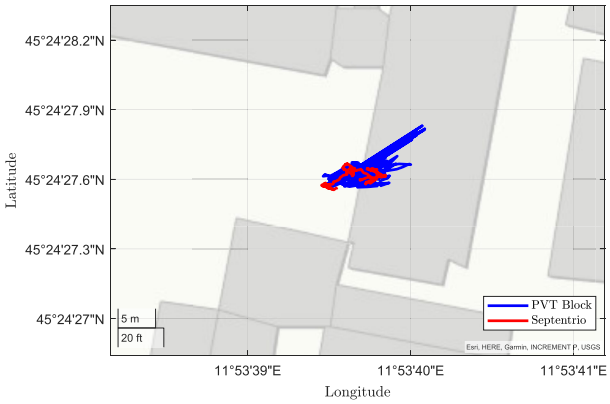
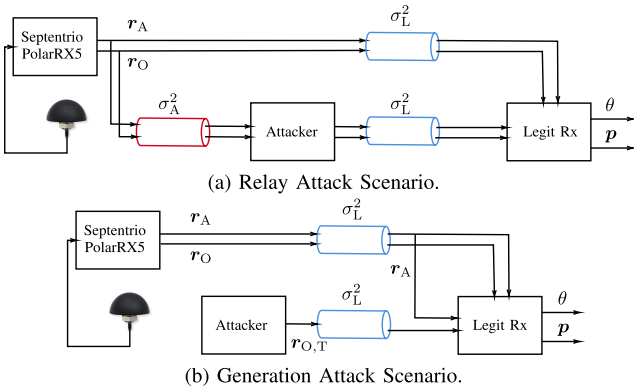


Fig. 4. Validation of our PVT block: position computed using our PVT block (blue) and the Septentrio's software (red).



(a) Relay Attack Scenario.

(b) Generation Attack Scenario.

Fig. 5. Testing model for the relay attack (a) and the generation attack (b).

Fig. 5 shows a scheme summarizing the testing methodology, which also includes the AWGN channels with noise standard deviations σ_{L}, σ_{T}, and σ_{A}, respectively. First, we collect measurements using the Septentrio PolarRx5 receiver. Next, in the relay attack (Fig. 5a) the attacker will receive and retransmit both authenticated and open signals. The victim will either receive the legitimate signal or the forged one, compute the corresponding position and timing solution $\boldsymbol{p}$ and the result of the considered authentication cross-check.

An analogous procedure is repeated for the generation attack, with the difference that the attacker computes the (open) fake signals without processing the legitimate ones. The legitimate receiver obtains either legitimate open and authenticated signals, or, when under attack, legitimate authenticated signals and spoofed open signals.

B. Attacks in Ideal Scenario Conditions

We now present the attack performance in the noiseless scenario, i.e., with $\sigma_{\text{L}} = \sigma_{\text{T}} = \sigma_{\text{A}} = 0$, distinguishing between the attack to the time-based and the position-based checks.

1) Attack Against the Time-Based Check: The attack is simulated as follows, at each epoch we

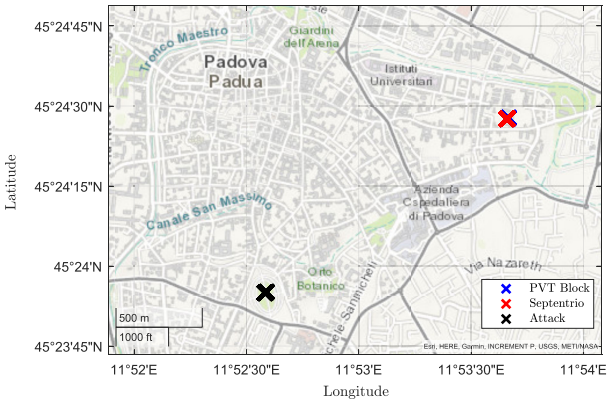


Fig. 6. Positions computed in the legitimate (blue) and under attack scenario (blue), compared to the ground truth (red). The position computed in the under-attack scenario coincides with the target $\boldsymbol{p}^\star$.

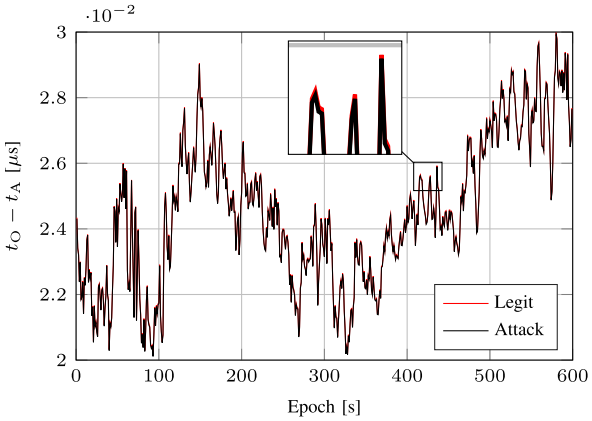


Fig. 7. Metric for the check (12): the metric computed under attack (blue) is superimposed to the one computed in the legitimate case (red).

1) compute the PVT solution by using the legitimate measurements (legitimate case);
2) choose the target position $\boldsymbol{p}_1^\star$;
3) obtain the tampered ranges by using (24);
4) feed the tampered ranges to the PVT block;
5) check the authenticity of the solution using the *ICTO-based authentication cross-check* (12).

In particular, we set the target position $\boldsymbol{p}_1^\star$ at 45.398° N, 11.876° E, with altitude 12 m (Prato della Valle square, Padua, Italy). The distance between the legitimate and the target position is roughly 1.7 km.

Notice that, between steps 3) and 4) we omitted the actual fake signal generation and the processing of the victim on the received signal. This means that we assumed that, under attack, the victim processes the tampered signal as intended by the attacker. Still as experimentally proved, e.g., in [6] and [7], it is indeed feasible to induce to the victim the fake signals, hence we skipped these steps.

Fig. 6 shows the positions computed in the legitimate and under-attack scenarios: the attacker is always able to induce the target position and only negligible errors are observed with respect to the target position. No issue has been observed in terms of availability, i.e., all the fake ranges led to the computation of a PVT solution.

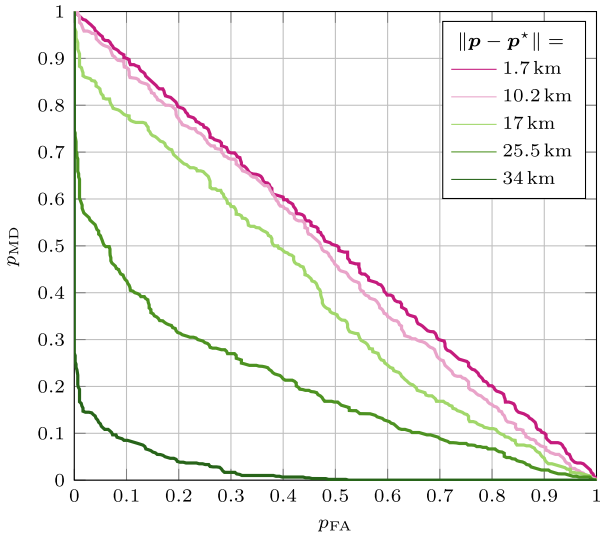


Fig. 8. DET curves for different distances between legit and target positions, for the time-based authentication cross-check against the proposed generation attack.

TABLE I
PARAMETERS OF THE ATTACK TO THE POSITION AUTHENTICATION CROSS-CHECK: ATTACK STARTS AND ADDITIONAL CLOCK BIASES

	Attack 1	Attack 2	Attack 3
t_{start}	60 s	100 s	150 s
$\Delta t - \Delta t_L$	30 μs	10 μs	5 μs

Fig. 7 shows the difference between the clock biases t_O and t_A used in the security check (12), computed respectively in the legitimate and under-attack case. Indeed, the check cannot distinguish the legitimate from the under-attack scenario, since the actual differences between legitimate and fake are well below the standard deviation of the metric itself. Hence, for any threshold T, the check cannot effectively detect the attack. For these reasons, the proposed attack can spoof the victim's position without being detected.

Fig. 8 shows instead the detection error trade-off (DET) curves for different distances between the target and the actual position. Indeed as this distance increases, it becomes easier for the victim to detect the spoofing attack. In particular, the attack success probability rapidly decreases for distances higher than 10 km. This is in line with our observations in Section II-B, confirming that the linearization procedure is not reliable in designing the attack if the target position is too far from the real one. Still, we remark that it may not be reasonable for the attacker to consider the target position too far since other signals of opportunity may be exploited by the victim to check the computed position.

2) Attack Against the Position-Based Check: The relay attack against the position authentication cross-check was discussed in Section IV-B for the noiseless scenario, thus, we are considering a self-spoofing scenario where the attacker and victim receiver are very close. In particular, we carried out three different attacks (Table I), with different induced time shifts and attack start times.

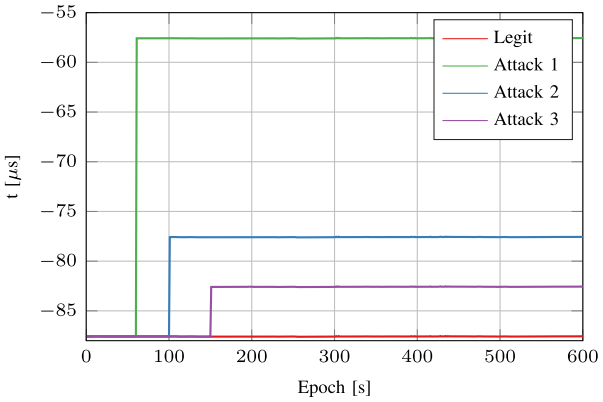


Fig. 9. Effect of the time attack on the clock bias estimated by the victim: Δt for the legitimate case (red), for Attack 1 (green), 2 (blue), and 3 (purple), whose parameters are reported in Table I.

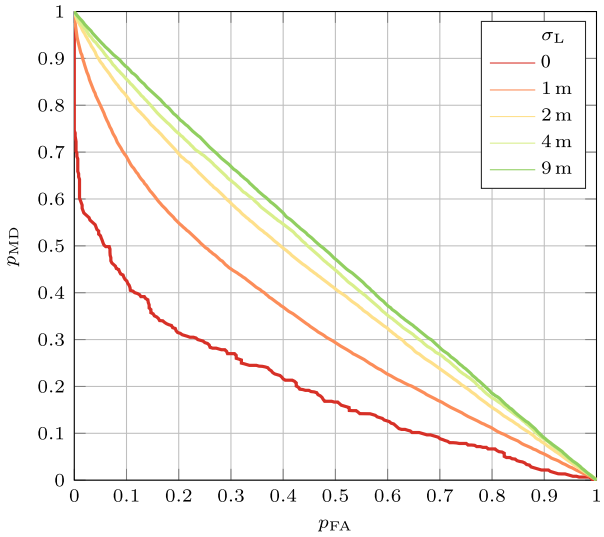


Fig. 10. DET curves with for the generation attack against time-based checks, when the attack target position is 25.5 km away from the victim location, for different values of σ_L.

Fig. 9 shows the results of the step-change on the clock bias estimated by the victim. This represents a best-case scenario for the defender, since, typically, the time shift is induced in a ramp-like manner (e.g., see the classification of [33]). Indeed, if the considered attacks are successful, the more sophisticated attacks will be successful as well. During the tests, all the considered attacks achieve their aim, inducing the target time shifts. On the other hand, consider the actual position check, no significant position deviation is induced by any of the attacks, since the deviation is at the cm-level, well below the actual accuracy of the receiver. Again, none of these attacks would be detected by the victim using the considered authentication cross-check.

C. Results With Noisy Measurements

In this Section, the performance of the proposed attack are evaluated in noisy conditions, distinguishing between time-based and position-based checks.

Starting from the experimental dataset, we run a Montecarlo simulation, repeating each experiment 35 times, therefore obtaining in total 21 000 PVT measurements.

1) Attacks Against the Time-Based Check: As proved in Section IV-A, we show that it is possible for the attacker to lead a successful attack using a generation attack.

We repeat the same attack simulation procedure adopted for the noiseless scenario but, between steps 3) and 4), we add AWGN to both the legitimate and the fake pseudoranges, according to the noise standard deviation at the victim receiver σ_L, with $\sigma_L = 0, 1, 2, 4$, and 9 m. We remark that, in this case, the attacker performs a generation attack, thus pseudoranges are only affected by the noise at the victim receiver. In general, a reasonable value for the noise standard deviation is 7.1 m [27, Ch. 7].[5] To evaluate the attack performance, we consider a target position 25.5 km away from the victim receiver location.

Fig. 10 reports the DET curve for the generation attack against time-based checks, showing the miss detection probability p_{MD} as a function of the false alarm probability p_{FA} and various values of σ_L. We notice that, as the noise at the victim receiver increases, the victim becomes unable to distinguish between legitimate and fake signals. Still, the results confirm that the check is not fully reliable even when the noise is minimal since, even in this condition, to get $p_{MD} < 10^{-2}$ it would yield $p_{FA} \approx 0.88$, thus rejecting most of the legitimate signals.

2) Attacks Against the Position-Based Check: As discussed in Section IV-B, if $N_O < 4$ only a relay attack can induce the desired clock shift while keeping low the probability of being detected. Conversely, when $N_O \geq 4$, also a generation attack can be used to achieve the same goal. It is worth noting that, when both the relay and the generation attack are viable, the latter is always the preferred option, since it involves signal generation instead of retransmission, and, as a result, the attacker does not introduce additional noise to achieve a better performance in terms of p_{FA} and p_{MD}, as will be discussed in this Section.

First, we consider the relay-type attack described in Section IV-B. Indeed, this represents the worst case for the attacker. To show the attack performance, we add noise only to the tampered ranges, so we consider $\sigma_L = 0$. Thus, the fake pseudoranges variance is $\sigma_T^2 = \sigma_A^2$.

We consider the scenarios where the attacker aims to induce a shift in the estimated clock bias $\Delta t - \Delta t_L = 10\,\mu s$. No relevant difference was observed when considering $\Delta t - \Delta t_L =$ 5 and 30 μs. In all the considered scenarios, when receiving the tampered signal, the victim computes the clock bias set by the attacker, with only negligible error. Hence whenever no alarm was raised, the attacks were successful.

Fig. 11 reports the DET curves of the attack for several values of σ_A. Indeed, for $\sigma_A = 0$, thus simulating an attacker able to perform a relay attack without adding any additional noise, tampered and legitimate signals are indistinguishable. On the other hand, as σ_A increases, it is easier for the victim to detect the attack. Still, even when $\sigma_A = 9$ m, the check is only partially effective since to get low values of missed detection the victim experiences high false alarm: for instance to get

[5]For instance, from our measurements, we get slightly more than 3 m.

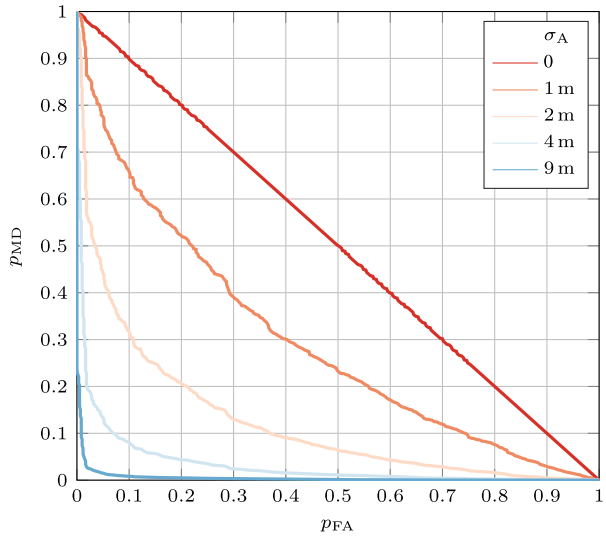


Fig. 11. DET curves for the relay attack against the position authentication cross-check, for $\Delta t - \Delta t_L = 10\,\mu s$, for several values σ_A and σ_L fixed.

$p_{MD} < 10^{-3}$ (not such a low value for a security application) the victim would obtain a $p_{FA} > 0.2$.

Concerning the generation attack against the time-based check, we carried out attack simulations adding the AWGN of the victim receiver to both fake and legitimate ranges, with $\sigma_L = 0, 1, 2, 4$, and 9 m. For all the considered values of noise standard deviation, the fake ranges resulted to be indistinguishable from the legitimate ones, and all the DET curves collapsed to the line $p_{FA} = p_{MD}$.

VII. Conclusion

In this work, a novel general framework for PVT authentication cross-check has been presented. With these checks, the receiver verifies the authenticity of the PVT solution computed using non-protected and authenticated signals, by using the authenticated signals as trusted anchors. The proposed framework abstracts from the specific implementation details of the cross-check, encompassing existing cross-checks as particular cases, and allows for evaluating the performance and limitations of any cross-authentication technique. In particular, we have exploited the framework itself to derive novel attacks, that for instance can break the authentication scheme proposed in [25]. More in detail, we have proposed attacks against both the time-based and the position-based authentication cross-checks. Moreover, we have analytically investigated the limits of the proposed attacks, by relating the degrees of freedom of the attacker in manipulating the victim PVT with the scenario parameters, e.g., the number of available authenticated signals. Numerical results have confirmed the effectiveness of both attacks: in particular, we have considered both simulated noiseless and noisy scenarios, and an experimental dataset, collected using a Septentrio PolarRx5 receiver.

Given the unquestionable usefulness of the authentication cross-checks, e.g., in contexts where the sole use of the authenticated signals does not lead to PVT, our work shows significant vulnerabilities of such emerging checks and calls for a revision of the current solutions before their possible adoption in future standards.

Appendix A
PVT Computation With Separate Time References

We describe the PVT linearization procedure and the derivation of each term needed to update the result during the iterative approach, to compute the terms of 5.

From the received signal, the receiver obtains the pseudorange vector $\boldsymbol{r}$. For ease of reading, we consider only signals from two systems: hence the output will contain entries t_1 and t_2, the clock biases associated with each of the time references, e.g., to the GPS or the Galileo system time. In particular, the receiver collects N_1 signals from the first constellation and $N_2 = N - N_1$ from the latter.

In general, each pseudorange is modeled by

$$r_j = \rho_j + ct_j - ct_1 \mathbb{1}_1(j) - ct_2 \mathbb{1}_2(j) + D_{\text{atm},j} + \eta\,, \qquad (55)$$

where ρ_j is the geometric range, i.e., the Euclidean distance between the (estimated) receiver position and the jth satellite position, with coordinates (x_j, y_j, z_j), defined as

$$\rho_j \triangleq \sqrt{(x_j - x)^2 + (y_j - y)^2 + (z_j - z)^2}\,, \qquad (56)$$

c is the speed of light, t_j is the satellite clock bias, $D_{\text{atm},j}$ models the atmospheric delays, and η models the remaining errors, considered as noise. The indicator functions $\mathbb{1}_1(j)$ and $\mathbb{1}_2(j)$ are introduced to identify the satellite constellations, i.e., $\mathbb{1}_1(j) = 1$ if satellite j belongs to the first constellation and 0 otherwise, while $\mathbb{1}_2(j) = 1$ if satellite j belongs to the second and is 0 otherwise. Notice that (approximations of) the satellites' positions, x_j, y_j, and z_j, t_j, and $D_{\text{atm},j}$, are retrieved directly from the navigation messages.

Next, we introduce the terms

$$a_{x,j} \triangleq \frac{x_j - \hat{x}}{\hat{\rho}_j}, \quad a_{y,j} \triangleq \frac{y_j - \hat{y}}{\hat{\rho}_j}, \quad a_{z,j} \triangleq \frac{z_j - \hat{z}}{\hat{\rho}_j}\,, \qquad (57)$$

which represent the components of the unit vector pointing from the (approximate) receiver to the jth satellite position. This allows us to introduce the geometry matrix

$$\boldsymbol{G} \triangleq \begin{bmatrix} a_{x,1} & a_{y,1} & a_{z,1} & 1 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{x,N_1} & a_{y,N_1} & a_{z,N_1} & 1 & 0 \\ a_{x,N_1+1} & a_{y,N_1+1} & a_{z,N_1+1} & 0 & 1 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{x,N} & a_{y,N} & a_{z,N} & 0 & 1 \end{bmatrix}. \qquad (58)$$

Following the linearization procedure reported, for instance, in [27, Ch. 2], and recalling (3), we obtain

$$\Delta r_j = a_{x,j}\Delta x + a_{y,j}\Delta y + a_{z,j}\Delta z - c\,t_1 \mathbb{1}_1(j) - c\,t_2 \mathbb{1}_2(j)\,, \qquad (59)$$

which can be equivalently written in matrix form as (4). This relates the range residuals to the PVT update vector $\Delta\boldsymbol{p} = [\Delta x, \Delta y, \Delta z, \Delta t_1, \Delta t_2]^{\mathrm{T}}$.

Notice that, the residuals as ordered naturally as

$$\Delta \boldsymbol{r} \triangleq \begin{bmatrix} \Delta r_1 \\ \vdots \\ \Delta r_{N_1} \\ \Delta r_{N_1+1} \\ \vdots \\ \Delta r_N \end{bmatrix} = \begin{bmatrix} \Delta \boldsymbol{r}_1 \\ \Delta \boldsymbol{r}_2 \end{bmatrix}. \tag{60}$$

Lastly, given $\boldsymbol{G}$, we can compute its Moore-Penrose inverse $\boldsymbol{H}$ and solve (5).

More details about the PVT derivation and other aspects related to it, such as the impact of $\boldsymbol{H}$ on the solution accuracy, can be found in [27, Ch. 2,7] and [28, Ch. 21].

Appendix B
PVT Computation With Unique Time Reference

If the ICTO between the system is known it is possible to take into account and solve the PVT linearization considering just one of the M time references. Without loss of generality, we consider the case where measurements are collected from two constellations and the ICTO $= t_2 - t_1$ is known by the receiver. This relates to the case where the signals are received from both GPS and Galileo and the GGTO is obtained from the I/NAV messages. Next, (55) becomes

$$r_j = \rho_j + ct_j - ct_1 - c\,\text{ICTO}\,\mathbb{1}_2(j) + D_{\text{atm},j} + \eta\,, \tag{61}$$

Next, we can consider this as if the satellites were synchronized to the same time reference, thus matrix $\boldsymbol{G}$ becomes

$$\boldsymbol{G} \triangleq \begin{bmatrix} a_{x,1} & a_{y,1} & a_{z,1} & 1 \\ \vdots & \vdots & \vdots & \vdots \\ a_{x,N_1} & a_{y,N_1} & a_{z,N_1} & 1 \\ a_{x,N_1+1} & a_{y,N_1+1} & a_{z,N_1+1} & 1 \\ \vdots & \vdots & \vdots & \vdots \\ a_{x,N} & a_{y,N} & a_{z,N} & 1 \end{bmatrix}. \tag{62}$$

The rest of the procedure is analogous to the one reported in Appendix A.

References

[1] S. Miljanovic et al., "Experimental testing and impact analysis of jamming and spoofing attacks on professional GNSS receivers," in *Proc. Int. Conf. Localization GNSS (ICL-GNSS)*, 2022.

[2] 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.

[3] T. E. Humphreys, B. M. Ledvina, M. Psiaki, B. W. O'Hanlon, and J. P. M. Kintner, "Assessing the spoofing threat: Development of a portable GPS civilian spoofer," in *Proc. 21st Int. Tech. Meeting Satell. Division Inst. Navigat.*, 2008, pp. 1–12.

[4] *Galileo Signal-in-Space Interface Control Document*. Accessed: Mar. 2023. [Online]. Available: https://www.gsc-europa.eu/sites/default/files/sites/all/files/Galileo_OS_SIS_ICD_v2.0.pdf

[5] *NAVSTAR GPS Space Segment/Navigation User Interfaces*, document IS-GPS-200, Mar. 2023. [Online]. Available: https://www.gps.gov/technical/icwg/IS-GPS-200M.pdf

[6] S. Ceccato, F. Formaggio, G. Caparra, N. Laurenti, and S. Tomasin, "Exploiting side-information for resilient GNSS positioning in mobile phones," in *Proc. IEEE/ION Position, Location Navigat. Symp. (PLANS)*, Apr. 2018, pp. 1515–1524.

[7] M. Lenhart, M. Spanghero, and P. Papadimitratos, "Relay/replay attacks on GNSS signals," in *Proc. 14th ACM Conf. Secur. Privacy Wireless Mobile Netw.*, Jun. 2021, pp. 380–382.

[8] A. J. Jahromi, "GNSS signal authenticity verification in the presence of structural interference," Ph.D. dissertation, Dept. Geomatics Eng., Univ. Calgary, Calgary, AB, Canada, 2013.

[9] A. J. Jahromi, A. Broumandan, S. Daneshmand, G. Lachapelle, and R. T. Ioannides, "Galileo signal authenticity verification using signal quality monitoring methods," in *Proc. Int. Conf. Localization GNSS (ICL-GNSS)*, Jun. 2016, pp. 1–8.

[10] C. Sun, J. W. Cheong, A. G. Dempster, H. Zhao, L. Bai, and W. Feng, "Robust spoofing detection for GNSS instrumentation using Q-channel signal quality monitoring metric," *IEEE Trans. Instrum. Meas.*, vol. 70, pp. 1–15, 2021.

[11] N. R. S. Miguel, Y.-H. Chen, S. Lo, T. Walter, and D. Akos, "Calibration of RFI detection levels in a low-cost GNSS monitor," in *Proc. IEEE/ION Position, Location Navigat. Symp. (PLANS)*, Apr. 2023, pp. 520–535.

[12] Z. Chen, H. Li, Y. Wei, Z. Zhou, and M. Lu, "GNSS antispoofing method using the intersection angle between two directions of arrival (IA-DOA) for multiantenna receivers," *GPS Solutions*, vol. 27, no. 1, pp. 1–13, Oct. 2023.

[13] M. Ceccato, F. Formaggio, N. Laurenti, and S. Tomasin, "Generalized likelihood ratio test for GNSS spoofing detection in devices with IMU," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 3496–3509, 2021.

[14] G. Oligeri, S. Sciancalepore, S. Raponi, and R. D. Pietro, "PAST-AI: Physical-layer authentication of satellite transmitters via deep learning," *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 274–289, 2023.

[15] 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.

[16] 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," *Navigat., J. Inst. Navigat.*, vol. 63, no. 1, pp. 85–102, Mar. 2016.

[17] 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.

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

[19] G. Caparra, N. Laurenti, R. Ioannides, and M. Crisci, "Improving secure code estimation-replay attacks and their detection on GNSS signals," in *Proc. 7th ESA Workshop Satell. Navigat. Technol. Eur. Workshop GNSS Signals Signal Process. (NAVITEC)*, 2014, pp. 1–8.

[20] 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.

[21] I. Fernandez-Hernandez et al., "Semi-assisted signal authentication for Galileo: Proof of concept and results," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 59, no. 4, pp. 4393–4404, Aug. 2023.

[22] L. Scott, "Anti-spoofing & authenticated signal architectures for civil navigation systems," in *Proc. 16th Int. Tech. Meeting Satell. Division Inst. Navigat.*, 2003, pp. 1543–1552.

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

[24] F. Ardizzon, G. Caparra, I. Fernandez-Hernandez, and C. O'Driscoll, "A blueprint for multi-frequency and multi-constellation PVT assurance," in *Proc. ESA Workshop Satell. Navigat. Technol. Eur. Workshop GNSS Signals Signal Process.*, 2022, pp. 1–9.

[25] B. Motella, M. Nicola, and S. Damy, "Enhanced GNSS authentication based on the joint CHIMERA/OSNMA scheme," *IEEE Access*, vol. 9, pp. 121570–121582, 2021.

[26] C. Gioia, J. Fortuny-Guasch, and F. Pisoni, "Estimation of the GPS to Galileo time offset and its validation on a mass market receiver," in *Proc. 7th ESA Workshop Satell. Navigat. Technol. Eur. Workshop GNSS Signals Signal Process. (NAVITEC)*, Dec. 2014, pp. 1–6.

[27] E. D. Kaplan and C. J. Hegarty, *Understanding GPS, Principles and Applications*, 2nd ed. Norwood, MA, USA: Artech House, 2005.

[28] P. Teunissen and O. Montenbruck, *Springer Handbook of Global Navigation Satellite Systems*. Cham, Switzerland: Springer, 2017.

[29] 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.
[30] A. Mathai and S. Provost, *Quadratic Forms in Random Variables*. New York, NY, USA: Taylor & Francis, 1992.
[31] J. A. Klobuchar, "Ionospheric time-delay algorithm for single-frequency GPS users," *IEEE Trans. Aerosp. Electron. Syst.*, vol. AES-23, no. 3, pp. 325–331, May 1987.
[32] K. Borre, D. Akos, N. Bertelsen, P. Rinder, and S. Jensen, *A Software-Defined GPS and Galileo Receiver: A Single-Frequency Approach*. Cambridge, MA, USA: Birkhäuser Verlag, Jan. 2007.
[33] E. Schmidt, J. Lee, N. Gatsis, and D. Akopian, "Rejection of smooth GPS time synchronization attacks via sparse techniques," *IEEE Sensors J.*, vol. 21, no. 1, pp. 776–789, Jan. 2021.

Francesco Ardizzon (Member, IEEE) received the B.Sc. degree, the M.Sc. degree, and the Ph.D. degree in information engineering from the University of Padova, Italy, in 2016, 2019, and 2023, respectively. In 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.

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. Nicola Laurenti. Her current research interests include authentication techniques for global navigation satellite systems, physical layer security, and wireless communications.

Stefano Tomasin (Senior Member, IEEE) received the Ph.D. degree from the University of Padova, Italy, in 2003. He joined the University of Padova, where he has been a Full Professor, since 2022. He was a Visiting Faculty Member with Qualcomm, San Diego, CA, USA, in 2004; Polytechnic University, Brooklyn, NY, USA, in 2007; and the Mathematical and Algorithmic Sciences Laboratory, Huawei, Paris, France, in 2015. 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 the Deputy Editor-in-Chief of 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 Padova, Italy, in 1999. In 2001, he became an Assistant Professor with the Department of Information Engineering, University of Padova. From 2008 to 2009, he was a Visiting Scholar with the Coordinated Science Laboratory, University of Illinois Urbana–Champaign. He is currently an Associate Professor with the Department of Information Engineering, University of Padova. He leads the Research Laboratory on GNSS Security, University of Padova, and has been the principal investigator in two projects on GNSS Open Service Signal Integrity Protection and Authentication at the Physical Layer, funded by 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