EURASIP Journal on Wireless Communications and Networking

RESEARCH Open Access

Authentication of satellite navigation signals by wiretap coding and artificial noise

Francesco Formaggio* and Stefano Tomasin

Abstract

In order to combat the spoofing of global navigation satellite system (GNSS) signals, we propose a novel signal authentication method based on information-theoretic security. In particular, the satellite superimposes to the navigation signal an authentication signal containing a secret authentication message corrupted by artificial noise (AN). We impose the following properties:

a) Authentication and navigation signals are synchronous,
b) Authentication and navigation signals are orthogonal and
c) The secret message is undecodable by the attacker due to the AN.

The legitimate receiver synchronizes with the navigation signal and stores the samples of the authentication signal with the same synchronization. After the transmission of the authentication signal, through a separate public asynchronous ground channel (e.g., a secure Internet connection) additional information is made public allowing the receiver to

a) Decode the authentication message, thus overcoming the effects of AN, and
b) Verify the authentication message.

We assess the performance of the proposed scheme by the analysis of both the secrecy capacity of the authentication message and the attack success probability under various attack scenarios.

Keywords: Artificial noise, Authentication, Global navigation satellite system, Physical layer security, Wiretap coding

1 Introduction

Global navigation satellite systems (GNSS) offer positioning and timing services for an increasing variety of applications (e.g., car and ship navigation, but also synchronization of electrical grid stations). GNSS signals are subject to various security attacks, aiming ultimately at disrupting or altering these applications [1]. In this paper, we focus on the *spoofing* attack, where an attacker (AT) transmits a signal with the purpose of inducing a false specific location estimate to the victim receiver (VR). This attack is *active* as it requires a transmission by the spoofer.

Positioning is typically obtained by measuring the time of arrival of pilot signals known at the receiver. The AT generates and transmits the pilots with proper delays (with respect to other original or spoofed satellite signals) in order to induce the desired position estimation. Moreover, the spoofer can also transmit an additional signal that destructively interferes with the original satellite signal at the VR.

A first defense against spoofing is its detection at the VR. Examples include the detection of either the residual power (on top of the legitimate signal) [2], or pre- [3] or post-correlation [4] power. Other approaches check the consistency of the arrival directions of satellite signals through multiple antennas [5–7]. Another defense strategy is the modification of current GNSS signal to both ease spoofing detection and make the attack more difficult. An interesting opportunity is the transmission of (partially) unpredictable signals, in what is usually denoted as navigation message authentication (NMA). Implementations of NMA include cryptographic schemes

*Correspondence: francesco.formaggio@dei.unipd.it
Department of Information Engineering, University of Padova, via Gradenigo 6/A, Padova, Italy

© The Author(s). 2019 **Open Access** This article is distributed under the terms of the Creative Commons Attribution 4.0 International License (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made.

based on either symmetric-key [8, 9] or asymmetric-key [10, 11] encryption. The partial unpredictability of the signal makes the spoofing attack more difficult as the AT cannot simply transmit a delayed version of the legitimate signal. In a more sophisticated attack, the AT eavesdrops the original satellite signal and then retransmits it (including both pilots and authentication data) in the so-called *meaconing* attack. Variations of this attack include the partial observation of the satellite signal and the reconstruction of the missing part, exploiting the redundancy provided by either forward error correction (FEC) (forward estimation attack, FEA) [12, 13] or spread spectrum techniques typical of GNSS, thus alternating (within the symbol duration) detection and retransmission (security code estimation and replay, SCER) [14].

In this paper, we propose a solution to make the GNSS system more robust to spoofing by operating at the physical layer and exploiting information theory (IT) results (see [15] for a survey on IT authentication solutions). The idea is that the satellite transmits an unpredictable *authentication message* synchronously with the navigation message. In order to prevent meaconing attacks, the satellite also transmits artificial noise (AN) superimposed to the authentication message, to be removed at the receiver before authentication verification. Then, after its transmission over the satellite channel, the authentication message and the AN are separately and securely re-broadcast so that the VR can check the presence and correctness of the authentication message in the earlier received signal. This eases the *detection* of the spoofing attack. The information dissemination can also occur on a separate delay-tolerant but authenticated channel, e.g., over the Internet with cryptographic authentication protocols. In summary, our solution, denoted physical layer authentication (PLA), includes (a) a novel communication architecture to securely share the authentication message and AN with a loose random delay and (b) coding and decoding algorithms for the *authentication message*, together with a technique to decide about its authenticity.

About related literature, in [16] AN is also used on top of an authentication tag, however without synchronization requirements and without an architecture for the dissemination of AN signal and authentication tags. In [17], we proposed to superimpose an AN-corrupted authentication message to the navigation signal, and PLA extends it by including advanced coding and signaling, and analyzing the solution within the framework of wiretap coding.

We show that as the length of the authentication message goes to infinity, we obtain a vanishing probability of success for the spoofing attack. We compute the rate at which the success probability vanishes, under perfect coding and Gaussian signaling. Then, we derive bounds on the success probability when finite-length messages and binary signaling are used. The impact of synchronization errors (due to an ongoing spoofing attack) on the success probability is also considered. For finite-length coding and binary signaling, a predictive attack (similar to meaconing FEA) is analyzed in terms of the probability of passing undetected. By numerical results, we show the effectiveness of the proposed PLA technique against various attacks.

The rest of the paper is organized as follows. Section 2 introduces both the system model and the reference attack strategy. In Section 3, we propose the novel PLA solution, whose correctness and security are analyzed in Section 4. In Section 5, we consider prediction attacks specifically targeting our PLA. The optimization of the transmit power is addressed in Section 6. Numerical results are presented is Section 7 before conclusions are driven in Section 8.

2 System model

Figure 1 shows our reference scenario with a satellite, and two earth devices, i.e., a VR and an AT.

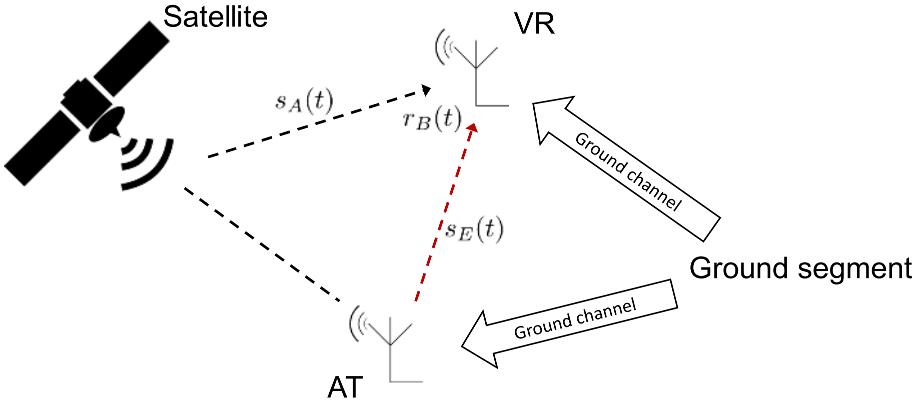

Fig. 1 Reference scenario

Satellite communication channel: In the basic existing configuration, the satellite generates a unitary-power real binary pilot signal d_i with symbol period T_s and spreads it with the real unitary-power spreading pulse

$$s_p(t) \triangleq \sum_{i=0}^{N_c-1} c_i u(t - iT_c)\,, \tag{1}$$

with chip period $T_c = T_s/N_c$, spreading sequence $c_i = \pm\frac{1}{\sqrt{N_c}}$ $i = 0, \ldots, N_c - 1$, and unitary-energy chip pulse $u(t)$. The resulting signal is

$$p(t) = \sum_i d_i s_p(t - iT_s). \tag{2}$$

In the current GNNS, $p(t)$ is also the baseband-equivalent (pilot component) signal transmitted by the satellite, which we will denote as

$$s_{\mathrm{A}}(t) = p(t). \tag{3}$$

In the absence of attacks and considering additive white Gaussian noise (AWGN) channels between all devices, as typically considered in satellite navigation systems, the signal received by the VR is

$$r_B(t) = G_B s_A(t) + w_B(t), \tag{4}$$

where G_{B} is the channel gain, and $w_B(t)$ is the zero-mean AWGN signal with power spectral density $\sigma^2_{w_B}$.

Ground channel: In order to implement our PLA scheme, we need a *ground channel*, i.e., public authenticated channel over which signals are transmitted by the *ground segment*, i.e., the navigation control center on the earth that is controlling GNSS. This channel is not necessarily a satellite link, and it is assumed to be of large bandwidth provided for example through an Internet connection. The authentication is ensured by higher layer authentication protocols [18] (such as https). We assume the AT has no control over the information traveling on the ground channel and, thus, it can not modify it. Moreover, as no fine time synchronization is available on the ground channel, it is not useful for ranging purposes.

2.1 Land satellite model

Channel gain G_{B} can be described by the land mobile satellite link (LMS) according to [19]. A three-state Markov chain (MC) is used to model the slow variations of the line of sight (LOS) due to shadowing and blockage effects while the Loo [20] distribution is used for G_{B} within each state and models shadowing and multipath effects. Therefore, we have

$$G_{\mathrm{B}} e^{j\theta} = l e^{j\phi_0} + g e^{j\phi}, \tag{5}$$

where $G_{\mathrm{B}} \geq 0$, l is log-normally distributed, g is Rayleigh distributed, ϕ_0 and ϕ are uniformly distributed in the interval $[\,0, 2\pi\,]$. In particular,

$$G_{\mathrm{B}} = |e^L e^{j\phi_0} + X + jY|, \tag{6}$$

where

$$L \sim \mathcal{N}(\mu, d_0) \tag{7}$$

$$X, Y \sim \mathcal{N}(0, b_0)\,. \tag{8}$$

The parameters μ, d_0, and b_0 are provided in [19] for different scenarios and for each Markov state. Note that we assume that the channel phase is always compensated at the receiver, thus we obtain the real signal model (4).

2.2 Reference attack

The AT's objective is to forge a navigation signal, send it to the VR, and let it believe it was transmitted by the satellite. We consider in particular here as *reference attack* a strategy wherein AT transmits an amplified (by factor ζ) and delayed (by delay Δ_{E}) version of $p(t)$, i.e.,

$$s_{\mathrm{E}}(t) = \zeta p(t - \Delta_{\mathrm{E}}), \tag{9}$$

where the delay is chosen by AT to induce a desired positioning at the VR. Correspondingly, the signal received by the VR is

$$r_B(t) = G_B s_A(t) + G_{\mathrm{E-A}} s_E(t) + w_B(t), \tag{10}$$

where $G_{\mathrm{E-A}}$ is the gain of the AT-VR channel. The resulting gain $G_{\mathrm{E-A}}\zeta$ of the pilot signal must be big enough to ensure that the received signal from the AT is stronger than that from the satellite, thus forcing the VR to get synchronous to $s_{\mathrm{E}}(t)$. An enhancement of this attack is achieved by transmitting a signal that destructively interferes with $s_{\mathrm{A}}(t)$ at the VR, i.e.,

$$s_{\mathrm{E}}(t) = -\frac{G_{\mathrm{B}}}{G_{\mathrm{E-A}}} s_{\mathrm{A}}(t) + \zeta p(t - \Delta_{\mathrm{E}})\,, \tag{11}$$

where the first term nulls out $G_{\mathrm{B}} s_A(t)$ in (10), while the second term induces the desired delayed signal. Moreover, the AT can receive the signal from the satellite as

$$r_E(t) = G_{\mathrm{E}} s_A(t) + w_E(t), \tag{12}$$

where G_{E} is the channel gain, and $w_E(t)$ is the zero-mean AWGN signal with power $\sigma^2_{w_E}$.

We will assume that the AT knows all channel gains, and we will also assume that in case of attack the VR gets synchronous with the AT signal and perfectly estimates the $G_{\mathrm{E-A}}\zeta$ gain. Therefore, for a simpler notation, we drop the channel gains in the following, assuming $G_{\mathrm{E-A}}\zeta = G_{\mathrm{B}} = G_{\mathrm{E}} = 1$, except when we focus on the LMS channel.

3 Methods

The proposed protocol aims at preventing the reference attack of Section 2.2 and operates in two phases: in the first phase, the satellite broadcasts the pilot, a FEC encoded version of the authentication message and the

AN, while in the second phase the ground segment broadcasts both the uncoded authentication message and the AN over the ground channel. During the first phase, the VR stores the received authentication signal sampled with the timing and synchronism obtained by the pilot signal. In the second phase, the VR removes the AN, decodes the authentication message, and checks if it corresponds to the authentication message broadcast over the ground channel.

We now detail the operations carried out in both phases.

3.1 First phase

In the first phase, the satellite transmits the authentication signal generated as described in Fig. 2. In particular, the satellite encodes the authentication message V in the codeword X^n. The codeword enters the modulator, which outputs real symbols x_k with power σ_x^2 at symbol time T_s. Let R_x be the rate of the message x_k. Then, each symbol is spread with the spreading sequence $c_{A,i} = \pm\frac{1}{\sqrt{N_c}}$, $i = 1, \ldots, N_c$, yielding the T_c-sampled signal

$$y_i = x_{\lfloor i/N_c \rfloor} c_{A,i \bmod N_c}. \tag{13}$$

Finally, the chip pulse $u(t)$ is used to obtain the continuous time real signal

$$x(t) = \sum_i y_i u(t - iT_c). \tag{14}$$

The authentication message V must be undecodable to the AT in the first phase, in order to prevent prediction attacks, as detailed in Section 5. Therefore, the satellite also transmits an AN signal $\omega(t)$ superimposed to $x(t)$. The resulting signal

$$z(t) = x(t) + \omega(t) \tag{15}$$

is superimposed to the ranging signal $p(t)$, and the baseband-equivalent signal transmitted by the satellite becomes

$$s_A(t) = z(t) + p(t), \tag{16}$$

which replaces (3).

We design the superimposed signal (including AN) $z(t)$ to be *orthogonal* to the pilot spreading pulse $s_p(t)$ in each pilot symbol, in order to avoid interference with the synchronization process (operating with $p(t)$), and at the same time guarantee that a legacy receiver is not affected by the new superimposed signals. In order to ensure orthogonality, the spreading code $c_{A,i}$ is orthogonal to c_i, the spreading code of the pilot signal. About the AN, for each symbol of duration T_s, we first generate a stationary Gaussian process $w(t)$, $0 \leq t \leq T_s$, and then project it on $s_p(t)$, i.e.,

$$\omega(t) = w(t) - \rho s_p(t), \tag{17}$$

with

$$\rho = \int_0^{T_s} w(t) s_p(t)\, dt. \tag{18}$$

Note that the Gaussian AN generation may be performed by a physical device providing electrical noise which may be further elaborated numerically. Although generating truly random variables is a challenging task [21–23], we observe that the satellite has typically enough processing power and cannot be physically tampered; therefore, it is reasonable to assume that it can generate random variables with fairly good randomness.

The signals received by both VR and AT on the AWGN channels are still given by (10) and (12), with the new transmitted signal $s_A(t)$ given by (16). The operations at the VR in the first phase are shown in Fig. 3 on the left of the dashed line separating the two phases. In particular, the VR acquires the synchronization on signal $p(t)$, filters the received signal $r_B(t)$ by $u(-t)$, and samples the output before despreading with sequence $c_{A,i}$. In the absence of attack, the resulting discrete-time despread signal can be written as

$$\hat{x}'_k = z_k + w_{B,k}, \tag{19}$$

where $z_k = x_k + \omega_k$ and ω_k is the AN term. The noise samples $w_{B,k}$ and ω_k are still independent and identically distributed (iid) with zero mean and powers $\sigma_{w_B}^2$ and σ_ω^2 respectively.

Note that we have omitted the pilot signal in (19) as its symbols are orthogonal to z_n and ω_k. Similarly, the AT receives in phase 1 the signal

$$\hat{x}'_{E,k} = z_k + w_{E,k}. \tag{20}$$

Since in the first phase AT does not know the AN, the resulting signal to noise ratio (SNR) at the AT is

$$\Gamma_E = \frac{\sigma_x^2}{\sigma_\omega^2 + \sigma_{w_E}^2}. \tag{21}$$

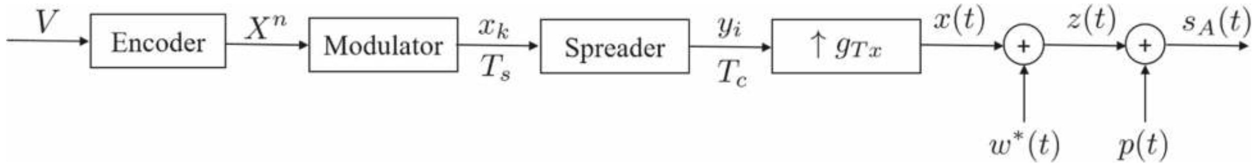

Fig. 2 Satellite transmission scheme in phase 1

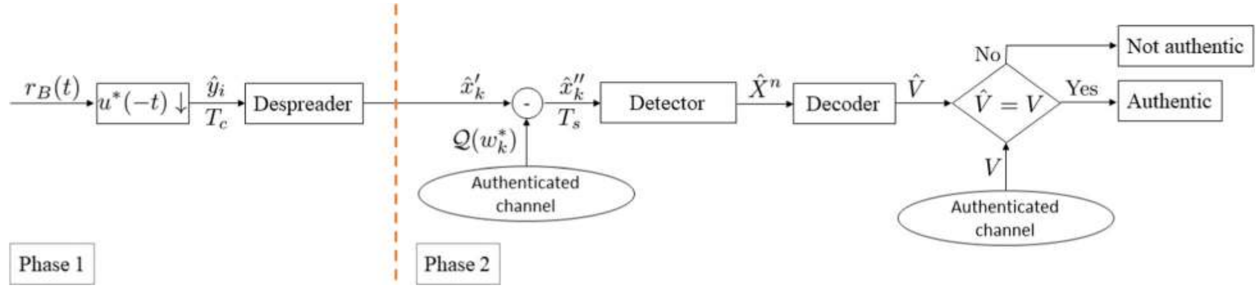

Fig. 3 VR signal processing. Dashed line separates operations occurring in the first phase by those occurring in the second phase

Therefore, we already observe that even with a noiseless receiver, by properly choosing σ^2_ω we can severely degrade the SNR at the AT, thus preventing meaconing attacks. Further details will be provided in Section 4.2.

3.2 Second phase

In the second phase, the ground segment broadcasts both V and a quantized version $\mathcal{Q}(\omega_k)$ of the AN samples ω_k on the ground channel using $\mathtt{b}$ bits per sample[1]. In the absence of attack and perfect synchronization, the quantization error is

$$w_{q,k} \triangleq \omega_k - \mathcal{Q}(\omega_k), \tag{22}$$

with zero mean and power $\sigma^2_{w_q}$. Note that $\mathtt{b}$ is a design parameter which trades off the quantization noise power with the transmission bandwidth of the ground channel.

On its side, the VR receives the signals over the ground channel and elaborates the signal received from the satellite in the first phase according to the scheme of Fig. 3 (at the right of the dashed line). In particular, the VR subtracts from x'_k the quantized AN obtaining

$$\hat{x}''_k = x'_k - \mathcal{Q}(\omega_k) = x_k + w_{B,k} + w_{q,k}. \tag{23}$$

Detection and decoding follow to obtain the decoded message $\hat{V}$. If $\hat{V} = V$, the VR declares that the authentication signal comes from the satellite and the pilot signal is also authentic. Otherwise the VR declares both the authentication message and the pilot as not authentic. Since the synchronization is obtained from $p(t)$, we design the authentication signal such that misalignments between $p(t)$ and $x(t)$ result in an error of the decoded message V, thus revealing the attack. Note also that the AT has no advantage in partially modifying the authentication message, since, once decoded at the VR, it would not match with the message V provided by the ground segment, thus again revealing the attack. In Section 5, we will consider an intermediate situation in which the AT partially observes the signal and attempts to predict the rest of V in the prediction attack.

4 Correctness and security analysis

We now examine the *correctness* and *security* of the proposed PLA solution. The *correctness* of the protocol is its ability to accept as authentic a signal coming from the satellite that corresponds to the condition $\hat{V} = V$. The *security* of the protocol is its ability to detect the *reference attack* described in Section 4.2. We will obtain rules for the design of PLA parameters (such as the rate of the authentication message R_x and the power of the AN) in order to guarantee correctness and security. Since we are dealing with authentication, which is basically a testing problem between the hypotheses of receiving correct or fake messages, its performance is assessed by the probabilities of attack success and authentic message rejection. Therefore, in our framework, the error probability

$$P_e^B \triangleq \mathbb{P}[\,\hat{V} \neq V|\text{no attack}] \approx 0, \tag{24}$$

where $\mathbb{P}[\,\cdot]$ denotes the probability operator, is used as correctness metric, while the success probability of the reference attack is used as security metric, see Section 4.2. In the next section, we will also analyze the security of PLA with respect to prediction (meaconing) attacks on the authentication message.

We consider four communication scenarios, combining finite/infinite codeword lengths with Gaussian/binary signaling. In the following, we will introduce a more efficient feedback where instead of V a smaller-size message can be fed back.

4.1 Correctness analysis

Assuming perfect synchronization, the correctness of the algorithm is then associated with proper coding and signaling that ensure correct decoding of the authentication message. We will now examine PLA correctness under infinite/finite codeword lengths and Gaussian/binary signaling. Indeed, while infinite-length codewords and Gaussian signaling provide optimal theoretic performance, finite length and binary signaling are commonly used in GNSS systems, thus providing insight on practical solutions.

Infinite-length codewords and Gaussian signaling: In this case, it is well known that we can ensure a vanishing decoding error probability as long as the message rate is below the channel capacity, i.e.,

$$R_x \leq C_B, \tag{25}$$

and C_B is the satellite-VR channel capacity after AN removal. Note that with perfect AN cancelation the resulting SNR of the signal at the input of the VR detector in the absence of attack is

$$\Gamma_B = \frac{\sigma_x^2}{\sigma_{w_B}^2 + \sigma_{w_q}^2}, \tag{26}$$

and the capacity is

$$C_B = \frac{1}{2}\log_2\left(1 + \Gamma_B\right). \tag{27}$$

In case of attenuation introduced by the LMS, the VR SNR becomes

$$\Gamma_B = \frac{G_B^2}{\sigma_{w_B}^2 + \sigma_{w_q}^2} \tag{28}$$

and it may occur that the channel is not good enough for the decoding of the authentication message at the VR, generating an outage event with outage probability

$$P_{\text{out}} = \mathbb{P}\left[C_B < R_x\right] = \sum_{i=1}^{3} \mathbb{P}\left[C_B < R_x | S = i\right] \mathbb{P}[S = i], \tag{29}$$

where in the second equation, we conditioned on the LMS state S. For a given state, we also have from (28)

$$P_{\text{out}|S=i} = \mathbb{P}\left[G_B < \sqrt{\left(\sigma_{w_B}^2 + \sigma_{w_q}^2\right)\left(2^{2R_x} - 1\right)} \middle| S = i\right]. \tag{30}$$

Infinite-length codewords and binary signaling: In this case, we can still provide a vanishing error probability, given that the rate is below the constellation-constrained capacity. In particular, the constrained capacity of a binary AWGN channel with SNR Γ is

$$C = \mathbb{H}(y) - \frac{1}{2}\log_2\left(\frac{2\pi e}{\Gamma}\right), \tag{31}$$

where

$$\mathbb{H}(y) = \int_{-\infty}^{+\infty} f_y(a)\log_2\frac{1}{f_y(a)}da \tag{32}$$

is the entropy of the received signal with probability density function (PDF)

$$f_y(a) = \sqrt{\frac{\Gamma}{8\pi}}\sum_{s\in\{-1,1\}} e^{-|s-a|^2\Gamma/2}. \tag{33}$$

In order to compute the capacity, we must resort to the numerical integration of (32).

Finite-length codewords and Gaussian signaling: For codewords of length $\bar{n}$ and Gaussian signaling, we cannot anymore ensure vanishing error probability. In order to compute the (non-zero) probability that the VR does not decode V, denoted $P_e\left(\Gamma_{\text{B}}, R_x, \bar{n}\right)$, we resort to literature results on finite-length codewords regime [24, 25]. In particular, we lower-bound the codeword error probability $P_e\left(\Gamma, R, \bar{n}\right)$ on AWGN channel with SNR Γ, transmission rate R, and codeword length $\bar{n}$ as

$$P_e\left(\Gamma, R, \bar{n}\right) \geq q\left(\Gamma, R, \bar{n}\right), \tag{34}$$

where

$$q(\Gamma, R, \bar{n}) \triangleq Q\left(\sqrt{\frac{\bar{n}}{G}}\left(\frac{F - R}{\log_2 e} + \frac{\ln(\bar{n})}{2\bar{n}}\right)\right), \tag{35}$$

$$F = \frac{1}{2}\log_2\left(1 + \Gamma\right), \tag{36}$$

$$G = \frac{\Gamma(2 + \Gamma)}{2(1 + \Gamma)^2}, \tag{37}$$

and $Q(\cdot)$ is the complementary cumulative distribution function (CDF) of a continuous normal variable.

Finite-length codewords and binary signaling: For this case, (34) and (35) still hold with [24, 25]

$$F = 1 + \frac{H^{(1)}}{\ln(2)}, \tag{38}$$

$$G = H^{(2)} - H^{(1)2}, \tag{39}$$

where

$$H^{(\ell)} = \frac{1}{\sqrt{2\pi\Gamma}}\int_{-\infty}^{\infty} e^{-\frac{1}{2\Gamma}(b-\Gamma)^2}\left(-h(b)\right)^{\ell}db, \tag{40}$$

$$h(b) = \ln\left(1 + e^{-2b}\right). \tag{41}$$

The probability of rejecting an authentic message is still lower-bounded by (34), with the new H and G in the definition of the function $q(\cdot)$ given still by (35).

4.2 Security analysis against the reference attack

Considering now the reference attack, assuming that the VR acquires the synchronization on the spoofed signal, i.e., the attack on the pilot signal is successful, we aim at assessing the probability that the VR also demodulates V from the asynchronous authentication signal, thus failing to reveal the attack.

First note that if Δ_E is larger than T_c, the despreading of the authentication message with an asynchronous spreading signal yields a very low output, thus we can assume that the attack is always detected. Therefore, we focus on the case wherein $0 \leq \Delta_E < T_c$. After despreading and AN removal, $\hat{x}_k''$ in (23) is affected by the previously transmitted symbol x_{k-1}, i.e.,

$$\hat{x}_k'' = \alpha x_k + \beta x_{k-1} + w_{B,k} + w_{k,\Delta_E}^{(q)}, \tag{42}$$

where α and β are non-negative interference coefficients and $w^{(q)}_{k,\Delta_E}$ is the residual quantization error with power $\sigma^2_{w_{q,\Delta}}$ that now depends also on Δ_E. This results in a new VR's SNR

$$\Gamma'_B(\Delta_E) = \frac{\alpha^2\sigma_x^2}{\beta^2\sigma_x^2 + \sigma^2_{w_B} + \sigma^2_{w_{q,\Delta}}}. \tag{43}$$

Note that if there is no delay, i.e., $\Delta_E = 0$, we have $\alpha = 1$, $\beta = 0$, $\sigma^2_{w_{q,\Delta}} = \sigma^2_{w_q}$ and hence $\Gamma'_B = \Gamma_B$. If, on the other hand, $\Delta_E > 0$, then $\alpha < 1$ and $\beta > 0$. This, together with $w^{(q)}_{k,\Delta_E}$, decreases the VR's SNR and mines his capability to decode $\hat{V}$, resulting in the attack being uncovered. Closed-form expressions for α, β, and $\sigma^2_{w_{q,\Delta}}$ are derived in Appendix A.

Now, we examine PLA security, i.e., its ability to detect the attack in various transmission configurations. We indicate with $P_{\text{succ}}(\Delta_E)$ the probability of an attack passing undetected (thus full success of the AT), as a function of the induced positioning signal delay.

Infinite-length codewords and Gaussian signaling: Let

$$C'_B(\Delta_E) = \frac{1}{2}\log_2\left(1 + \Gamma'_B(\Delta_E)\right) \tag{44}$$

be the channel capacity induced to the VR by the reference attack. Given a chosen working point of the authentication message rate R_x, the probability of successful attack, considering infinite codeword length and Gaussian signaling, is

$$P_{\text{succ}}(\Delta_E) = \begin{cases} 1 & \text{if} \quad C'_B(\Delta_E) > R_x \\ 0 & \text{if} \quad C'_B(\Delta_E) < R_x, \end{cases} \tag{45}$$

since, from the converse theorem on capacity, the codeword error probability of the VR tends to 1 as the codeword length tends to infinity. We observe that we can reduce the feedback and provide only the secret bits. As soon as these coincide with the one decoded at the receiver, we can ensure authenticity.

Infinite-length codewords and binary signaling: For binary signaling, (45) still holds, but the capacity is computed through (31) by replacing Γ with $\Gamma'_B(\Delta_E)$.

Finite-length codewords and Gaussian signaling: Given the codeword length $\bar{n}$ and the authentication message rate R_x in this case the reference attack is successful with probability

$$P_{\text{succ}}(\Delta_E) = 1 - P_e\left(\Gamma'_B(\Delta_E), R_x, \bar{n}\right). \tag{46}$$

Using (34) and (35), we obtain the upper bound

$$P_{\text{succ}}(\Delta_E) < 1 - q\left(\Gamma'_B(\Delta_E), R_x, \bar{n}\right). \tag{47}$$

Finite-length codewords and binary signaling: The analysis is the same as for the previous paragraph, but using (38)–(41) instead of (36)–(37).

Remark on the replay attack. In the replay attack, the AT retransmits the received signal to the VR right after reception, with arbitrary power. Therefore, the replayed signal contains also the non-predictable component $z(t)$ and differs from the legitimate signal only by the additional noise introduced by the AT front-end. Clearly, in absence of AT noise, no defense is possible against this attack, whereas the AT operates simply as an ideal amplifier, and the malicious received signal is indistinguishable from the legitimate one. We then do not consider it specifically in this paper, while it has been considered for example in [17]. In [17], we addressed the case wherein the AT introduces noise by assessing the authentication performance under various SNR regimes.

5 Security against prediction attacks

As we have just seen, the proposed protocol is secure against the reference attack; however, we can consider a more general attack wherein AT partially observes the signal transmitted by the satellite in phase 1, predicts the whole signal and transmits it to the VR. This attack is similar to FEA considered in the literature, where however our authentication protocol was not present.

This attack is based on the possibility of predicting $s_{\text{A}}(t)$ (including the authentication part), which is now investigated. While the authentication message is encoded with FEC and therefore the codeword has a specific structure that actually eases prediction, the AN samples are independent and unpredictable. Therefore, the AT will only predict and transmit the authentication message without AN. Under this attack, the VR will then suffer from the cancelation of an AN that is not present, thus actually introducing noise on the signal at the input of the detector.

The best thing the AT can do is to align his prediction of $x(t)$, that we denote $\hat{x}(t)$, with the forged positioning signal. Following (11), the attack signal becomes

$$s_E(t) = -[\hat{x}(t) + p(t)] + \hat{x}(t - \Delta_{\text{E}}) + p(t - \Delta_{\text{E}}), \tag{48}$$

such that, if $\hat{x}(t) = x(t)$ and following (10), the signal received in phase one by the VR is

$$r_B(t) = \hat{x}(t - \Delta_{\text{E}}) + p(t - \Delta_{\text{E}}) + \omega(t) + w_B(t). \tag{49}$$

In phase two, we have

$$\hat{x}''_k = x_k + w_{B,k} + w^{(q)}_{k,\Delta_E}, \tag{50}$$

which is similar to (42) except that now there is no symbol interference in the authentication message. The VR's SNR becomes

$$\Gamma''_B(\Delta_E) = \frac{\sigma_x^2}{\sigma^2_{w_B} + \sigma^2_{w_{q,\Delta}}}. \tag{51}$$

Therefore, even in the presence of un-removed AN, the VR may decode the authentication message transmitted by the AT, thus accepting the signal as authentic. If we condition to the event of correct prediction, which happens with probability

$$P_{\text{pred}} \triangleq \mathbb{P}[\hat{x}(t) = x(t)]\,, \tag{52}$$

then the success probability of the prediction attacks becomes $P_{\text{succ}}(\Delta_{\text{E}})$ of Section 4.2 with $\Gamma''_B(\Delta_{\text{E}})$ in place of $\Gamma'_B(\Delta_{\text{E}})$.

In the following, we will consider two specific prediction attacks, namely, the blind prediction and the codeword prediction attack. For each attack, we evaluate P_{pred}, as a metric of success of the attack in our authentication context.

Blind prediction attack: In this case, the AT does not use the signal received from the satellite but directly attempts to guess the authentication message. For a finite number of possible codewords, there is a non-zero probability that the guess is correct. The AT generates and transmits $s_{\text{A}}(t)$ according to the guessed authentication codeword, with the desired delay Δ_{E}.

Codeword prediction attack: In this case, the AT receives a fraction of the signal transmitted by the satellite (corrupted by AN) and attempts to decode the authentication message. Then, it transmits the decoded codeword as its own authentication message with the desired delay Δ_{E}. This attack exploits the structure of the codeword introduced by FEC and is equivalent to the FEA attack present in the literature (not with our authentication scheme).

We now analyze each of these attacks against PLA.

5.1 Blind prediction attack

With ideal transmission, i.e., when codewords with infinite lengths are used for x_k, the probability that the VR guesses the correct message V is vanishing. For a finite length $\bar{n}$, the prediction probability is instead associated with the probability of correctly guessing the codeword into a codebook of $R_x\bar{n}$ entries; therefore,

$$P_{\text{pred}} = 2^{-R_x\bar{n}}. \tag{53}$$

5.2 Codeword prediction attack

In order to avoid the codeword prediction attack, we must reduce the probability of correct decoding of the codeword by the AT for a partial observation of the received signal in the first phase. This feature is provided by the AN that affects the decoding capabilities of the AT.

Infinite-length codewords and Gaussian signaling: For perfect coding and Gaussian signaling, we can avoid the codeword prediction attack by ensuring that no information is obtained on the secret message by the observation of $r_{\text{E}}(t)$ in the first phase, i.e.,

$$\mathbb{I}(V; r_E(t)) = 0, \tag{54}$$

where $\mathbb{I}(\cdot;\cdot)$ denotes the mutual information function. This condition will also ensure that no information is obtained on V by a partial observation of $r_E(t)$. From results on wiretap-coding, the secrecy condition (54) is satisfied as long as ([26], Chaper 5)

$$R_x \geq C_E = \frac{1}{2}\log_2\left(1 + \Gamma_E\right), \tag{55}$$

where C_E is the capacity of the satellite-AT channel. Note that in our authentication framework, mutual information matters only for prediction attacks, because in the reference attack the AT does not attempt to construct V by eavesdropping $z(t)$. Therefore, assuming as worst case that the AT has a noiseless receiver ($\sigma^2_{w_E} = 0$), from (21) and (55), the noise power σ^2_ω must satisfy

$$\sigma^2_\omega \geq \frac{\sigma^2_x}{2^{2R_x} - 1}. \tag{56}$$

Still by the wiretap coding theory, there exist suitable wiretap codes for the satellite such that the part of the authentication message that remains secret to the AT has a secrecy rate

$$R_A = R_x - C_E, \tag{57}$$

and the probability of guessing the correct codeword is vanishing with the codeword length as

$$P_{\text{pred}} = 2^{-R_A\bar{n}}. \tag{58}$$

Note that with respect to the blind prediction attack, R_x is now replaced by $R_{\text{A}} < R_x$. In turns, R_A is maximized when $R_x = C_B$, and we obtain the secrecy capacity [26]

$$C_A \triangleq C_B - C_E, \tag{59}$$

while the design constraint (56), assuming negligible quantization noise, becomes

$$\sigma^2_\omega > \sigma^2_{w_B}. \tag{60}$$

Note that in our context, the secrecy of message V is only instrumental to the authentication of the navigation message. Therefore, with a small abuse of notation, we will denote as *authentication capacity* the secrecy capacity C_A, as the secret bits are those that prevent the AT from guessing the authentication message. For a practical implementation of this approach, existing wiretap codes can be used (see for example the survey papers [27] and [28]), with a variety of trade-offs between wiretap performance, code length, and decoding complexity. Further investigation is also needed, though outside of the scope of this paper, on specific requirements of the wiretap codes for our scheme. Here, indeed, confidentiality is only instrumental to preventing prediction attack and the security metric is the success probability of the spoofing attack.

Infinite-length codewords and binary signaling: The analysis of the previous paragraph holds with the difference that C_B and C_E must be computed numerically using (31)–(33).

Finite-length codewords and Gaussian signaling: We still first assume Gaussian signaling. Due to the finite-length regime, (54) does not hold anymore. Considering a codeword prediction attack performed by the AT at symbol $n < \bar{n}$, the probability of successful attack is upper-bounded as

$$\begin{aligned} P_{\text{pred}}(n) &\leq \max\left\{1 - P_e\left(\Gamma_E, R_x, n\right), 2^{-R_x n}\right\} \\ &\leq \max\left\{1 - q\left(\Gamma_E, R_x, n\right), 2^{-R_x n}\right\}, \end{aligned} \tag{61}$$

where the second inequality comes from two facts:

a) $q(\Gamma, R_x, n)$ is a lower bound on the codeword error probability and
b) the bound (34) is based on the fact that the code is optimized for length $\bar{n}$, while the AT attempts decoding after receiving n symbols, thus we have a further source of error by this mismatch.

The maximum comes from the fact that the success probability cannot be lower than $2^{-R_x n}$, which corresponds to the complete random choice of the attack codeword.

Finite-length codewords and binary signaling: In this case, (61) still holds using (38)–(41).

6 Power optimization

We now aim at optimizing σ_x^2, given a fixed power budget, i.e.,

$$A = \sigma_x^2 + \sigma_\omega^2. \tag{62}$$

This corresponds to choosing the trade-off between the power assigned to the authentication message and the AN, for a total additional power (with respect to the non-authenticated system) A. We consider two design criteria which lead to different optimization problems, aiming at increasing security against reference and prediction attacks, respectively.

6.1 Optimization against the reference attack

In this case, we want to maximize the protection against the reference attack, while also achieving a desired value for R_x, under power constraint (62). To this end, we choose an operating point $\Delta_E = \epsilon$, corresponding to the maximum tolerable synchronization error in standard operating conditions. Performance is then dictated by how fast $\Gamma_{\text{B}}(\Delta_{\text{E}})$ decreases, when $\Delta_{\text{E}} \geq \epsilon$, due to an ongoing attack that introduces an asynchronism larger than the expected maximum.

First, observe that when $u(t)$ has a rectangular shape $\Gamma_{\text{B}}(\Delta_{\text{E}})$ is a monotonically decreasing function for $0 \leq \Delta_{\text{E}} \leq T_c$, as shown in the Appendix A. Then, we aim at minimizing the derivative of Γ_{B} around ϵ, so that the system is as sensitive as possible to unexpected synchronization errors. With a slight abuse of notation, we define the derivative of $\Gamma_{\text{B}}(\Delta_{\text{E}})$ computed at ϵ as

$$f(\sigma_x^2) \triangleq \left.\frac{\partial \Gamma_{\text{B}}(\Delta_{\text{E}})}{\partial \Delta_{\text{E}}}\right|_{\Delta_E = \epsilon}, \tag{63}$$

where we highlight the derivative dependency on σ_x^2 that we want to optimize. The problem then can be written as

$$\begin{aligned} &\min_{\sigma_x^2 \geq 0} f\left(\sigma_x^2\right) \\ &\text{subject to (62) and } R_x - \frac{1}{2}\log_2(1 + \Gamma_{\text{B}}(\epsilon)) \leq 0, \end{aligned} \tag{64}$$

where the second constraint ensures correctness at $\Delta_E = \epsilon$ (still tolerable delay) for the case with infinite codeword length and Gaussian signaling.

We now solve the optimization problem. For ease of notation, let us rename the optimization variable as $o \triangleq \sigma_x^2$. With algebraic computations, we have

$$f(o) = \frac{N_2 o^2 + N_1 o}{(D_1 o + D_0)^2}, \tag{65}$$

where

$$\begin{aligned} N_2 =& 2A_1A_2B^2\epsilon^2 - 4A_1A_2 + 4A_1^2A_2 + 4A_1A_2^2\epsilon \\ &+ 2A_2^2B^2\epsilon^3 - 4A_2^2\epsilon + 4A_1A_2^2\epsilon + 4A_2^3\epsilon^2 - 2A_1^2B^2\epsilon \\ &- 2B^2A_2^2\epsilon^3 - 4B^2A_1A_2\epsilon^2 \\ &- 2A_2A_1^2 - 2A_2^3\epsilon^2 - 4A_1A_2^2\epsilon, \\ N_1 =& 2A_1A_2\sigma_{w_B}^2 + 4AA_1A_2 - 4AA_1^2A_2 - 4AA_1A_2^2\epsilon \\ &+ 2A_2^2\sigma_{w_B}^2\epsilon + 2AA_2^2\epsilon - 4AA_1A_2^2\epsilon - 4AA_2^3\epsilon^2 \\ &+ 2AA_2A_1^2 + 2AA_2^3\epsilon^2 + 4AA_2^2A_1\epsilon, \\ D_1 =& B^2\epsilon^2 - 2 + 2A_1 + 2A_2\epsilon, \\ D_0 =& \sigma_{w_B}^2 + 2A - 2AA_1 - 2AA_2\epsilon. \end{aligned}$$

By deriving $f(o)$ and setting it to zero, we find the candidate solutions of the optimization problem. We have

$$f'(o) = \frac{(2N_2D_0 - N_1D_1)o + N_1D_0}{(D_1o + D_0)^3} = 0 \tag{66}$$

and the only candidate point is

$$o^* = \frac{N_1D_0}{N_1D_1 - 2N_2D_0}. \tag{67}$$

We now consider the constraints in (64). The power constraint has been eliminated by substituting $\sigma_\omega^2 = A - \sigma_x^2$ in (86), while the correctness constraints yield the upper bound

$$\sigma_x^2 \leq \frac{(1 - 2^{2R_x})(\sigma_{w_B}^2 + 2A - 2A\alpha)}{(1 - 2^{2R_x})(\beta^2 - 2 + 2\alpha) - \alpha^2} = \hat{\sigma}_x^2. \tag{68}$$

The feasible set is then the compact set $\mathcal{E} = \{\sigma_x^2 | 0 \leq \sigma_x^2 \leq \min(\hat{\sigma}_x^2, A)\}$. The solution of the overall optimization problem is the point σ_{opt}^2, among o^* and the extrema of $\mathcal{E}$, providing the minimum value of $f(\cdot)$.

6.2 Authentication capacity maximization

In this case, we want to maximize the protection against prediction attacks, that as we have seen, can be achieved by maximizing the secrecy rate given the power budget (62), i.e.,

$$\max_{\sigma_x^2 \geq 0} C_A\left(\sigma_x^2\right) \quad \text{subject to (62)}, \tag{69}$$

where again with a slight abuse of notation, we have highlighted C_A dependency on σ_x^2. Note that $C_A\left(\sigma_x^2\right) > 0$ only if $\sigma_\omega^2 > \sigma_{w_B}^2$; therefore, we must have $A > \sigma_{w_B}^2$.

For the AWGN channel, consider the case $\sigma_{w_q}^2 = 0$, wherein VR and AT SNRs are

$$\Gamma_B = \frac{\sigma_x^2}{\sigma_{w_B}^2}, \quad \Gamma_E = \frac{\sigma_x^2}{\sigma_\omega^2}. \tag{70}$$

Exploiting the concavity of the logarithm, (69) is equivalent to

$$\max_{\sigma_x^2 > 0} -\frac{1}{A\sigma_{w_B}^2}\left(A - \sigma_x^2\right)^2 + \frac{A + \sigma_{w_B}^2}{A\sigma_{w_B}^2}\left(A - \sigma_x^2\right). \tag{71}$$

The objective function is now a down-facing parable; hence, the solution of (71) is

$$\sigma_{\text{opt}}^2 = \frac{A - \sigma_{w_B}^2}{2}. \tag{72}$$

7 Results and discussion

We consider the transmission scenario of Fig. 1 with a single satellite. The ground channel is assumed error-free and with a large band. As for the Galileo signal, we assume $N_c = 4,092$ and $T_c = 10^{-6}/1.023$ s [29]. The VR's noise power is $\sigma_{w_B}^2 = 0, -5$, or -10 dB, that are typical values for GNSS receivers [30]. For the AT, we assume $\sigma_{w_E}^2 = 0$, i.e., a noiseless receiver, as a worst case for the authentication problem.

About the transmission chip $u(t)$, we consider two options, shown in Fig. 4. In particular, $u_1(t)$ is the chip pulse used in the Galileo E1b system [29], while $u_2(t)$ is a chip pulse characterized by a smaller support designed in order to make the authentication signal more fragile to synchronization errors, as discussed in Section 4.2. The design of $u(t)$ can be further improved for a practical implementation, but this is left for future works.

As an example of various issues that must be addressed in the design of the chip pulse beyond its sensitivity to synchronization errors, we consider here its occupied band, by showing in Fig. 5 the power spectral density (PSD) of $x(t)$ modulated by the two chip pulses. We note that the new pulse has a similar PSD to the standard one, thus making $u_2(t)$ a good candidate (at least about band occupation) for future GNSS systems. In the following, we will show the merits of $u_2(t)$ for authentication purposes.

With reference to Sections 4, 5, and 6, we now provide various performance results.

7.1 Correctness analysis

About correctness, we have shown that it is related to the capability of the VR to correctly decode the authentication message sent by the satellite.

Infinite-length codewords: In this case, correctness is ensured as long as the rate of the authentication message R_x is below the capacity of the satellite-VR channel. Thus, we show the outage probability (29) for three propagation scenarios [19], namely, (1) urban area, vehicle mounted antenna, elevation 30^{circ}; (2) suburban area, vehicle mounted antenna, elevation 60^{circ}; and (3) intermediate tree shadowed area, elevation 80^{circ}.

Figure 6 shows P_{out} for the three scenarios in the case of Gaussian signaling, as a function of R_x. Note that a lower elevation (scenario 1) has more impact on the outage

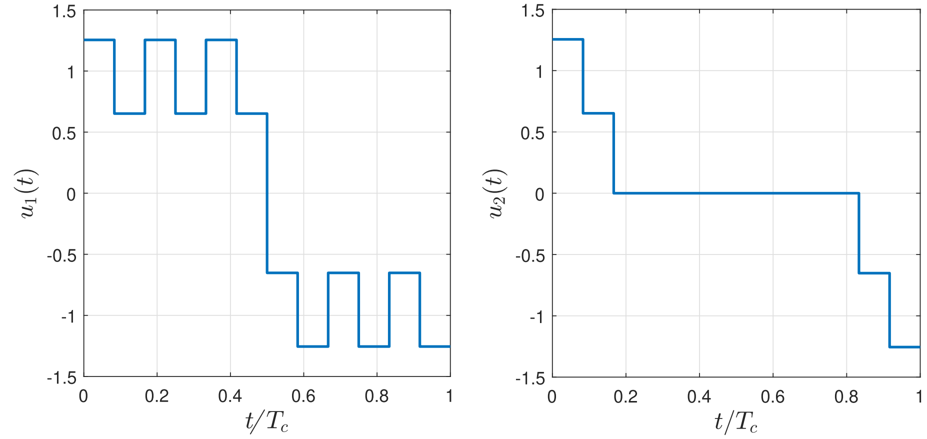

Fig. 4 Two considered chip pulses: $u_1(t)$ and $u_2(t)$

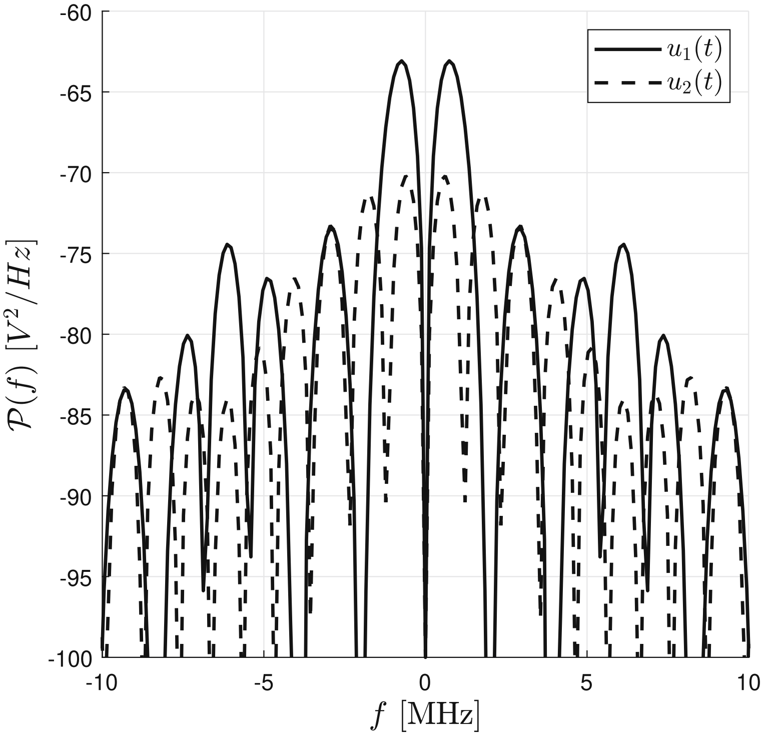

Fig. 5 PSD of $x(t)$ modulated by the chip pulses of Fig. 4

probability rather than differences in user motion settings as the curves of scenarios 2 and 3 are closer to each other.

Similar results (omitted here for the sake of conciseness) are obtained for the case of binary signaling.

Finite-length codewords: For finite-length codewords, we have seen that there is a non-zero probability that the VR does not recognize as authentic the signal coming from the satellite, due to decoding errors in the authentication message.

Figure 7 shows the lower bound to the codeword error probability, $q(\Gamma_B, R_x, \bar{n})$, as a function of $\bar{n}$ for both Gaussian and binary signaling and $\Gamma_B = 1$ dB. We observe that for a higher rate, the error probability increases, e.g., for $\bar{n} = 300$ (for Gaussian signaling) the probability of error goes from $2 \cdot 10^{-3}$ to $2 \cdot 10^{-2}$ by increasing the rate of 0.05 b/s/Hz.

Moreover, we observe that for Gaussian signaling, the codeword error rate decreases faster with $\bar{n}$ rather than with binary signaling. Note however that the functions $q(\cdot)$ are approximations of bounds for codeword error probability [25]; therefore, the distance between the binary and the Gaussian case we read in the plots might not be exact.

7.2 Reference attack

As discussed Section 4.2, the success of the reference attack depends on the delay between the authentication and the navigation message, as well as the operating conditions of the VR. We now consider the various signaling and coding configurations with AN power $\sigma_\omega^2 = 0$ dB and VR's noise power $\sigma_{w_B}^2 = -5$ dB.

Infinite-length codewords: Figures 8 and 9 show C'_B vs the attack delay $\Delta_{\rm E}$ for both Gaussian and binary signaling, and for chip pulse $u_1(t)$ and $u_2(t)$. We observe that with $u_1(t)$ (Galileo system), the capacity drops to zero for $\Delta_{\rm E} > 0.2\ T_c$, while with $u_2(t)$ (proposed pulse) having a more compact support, the capacity drops to zero already for $\Delta_{\rm E} = 0.15\ T_c$. Therefore, with the proposed chip, we can detect a reference attack inducing even smaller delays. Moreover, as observed earlier, binary and Gaussian signaling provides similar performance.

Note that by setting the coding rate R_x below $C_A(\Delta_{\rm E}^*) = 0$, we have that an attack with delay $\Delta_{\rm E} > \Delta_{\rm E}^*$ is detected as, from the converse theorem on capacity, the codeword error probability of the VR tends to 1 as $\bar{n}$ tends to infinity. Note however, that the choice of R_x must also take into account the sensitivity of VR to synchronization errors in normal operation (i.e., when the received signal is coming from the satellite), in order to avoid false alarms.

Finite-length codewords: For finite-length codewords, Gaussian signaling, and $\sigma_{w_B}^2 = -5$ dB, the reference attack is successful with non-zero probability. Figures 10 and 11 show the upper bound to the attack success probability $1 - q(\Gamma'_B(\Delta_{\rm E}), R_x, \bar{n})$ (see (47)). We note the impact

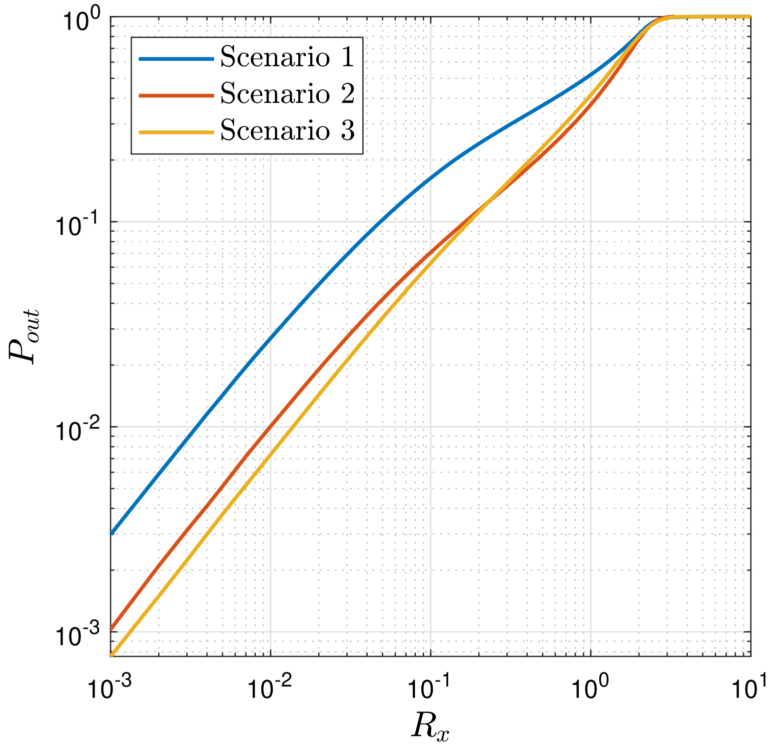

Fig. 6 P_{out} for three different propagation scenarios as a function of R_x

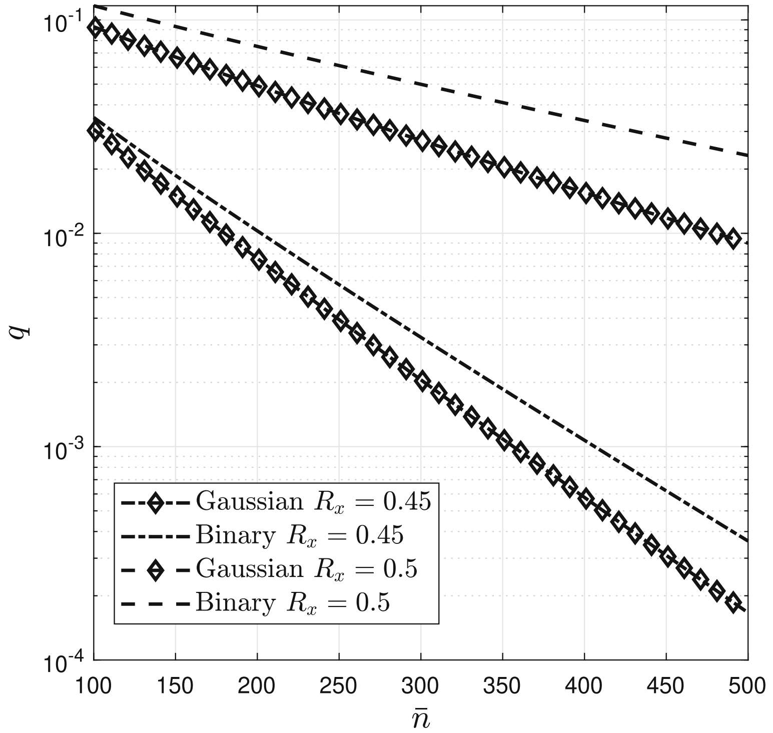

Fig. 7 $q(\Gamma_B, R_x, \bar{n})$ for $\Gamma_B = 1$ dB, Gaussian and binary signaling and two different values of R_x, as a function of the codeword length $\bar{n}$

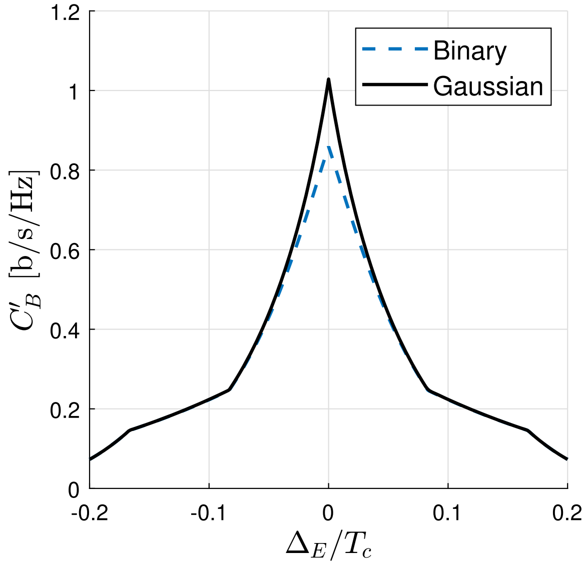

Fig. 8 Degradation of VR's capacity versus the delay Δ_E, using the transmission chip pulse $u_1(t)$, with $\sigma^2_{w_B} = -5$ dB and $\sigma^2_\omega = 0$ dB

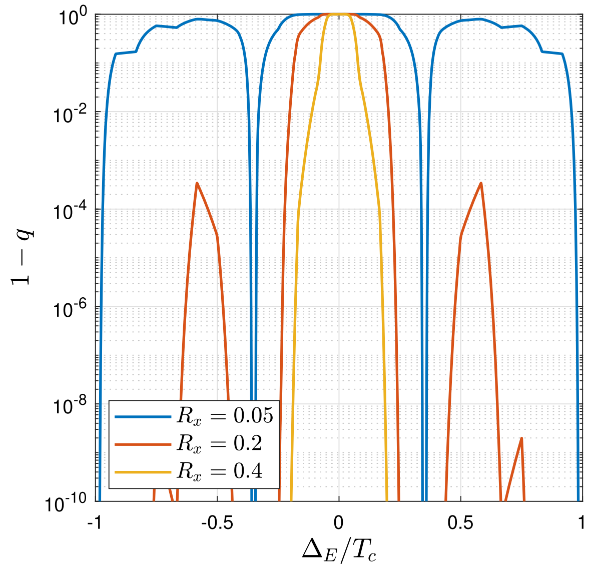

Fig. 10 $1 - q(\Gamma'_B(\Delta_E), R_x, \bar{n})$ (Gaussian case) as a function of the attack delay Δ_E for three values of R_x and using pulse $u_1(t)$ of Fig. 4, $\sigma^2_{w_B} = -5$ dB

of the attack delay Δ_E on the error probability P_e. The two symmetric lobes are due to the particular structure of pulses $u_1(t)$ and $u_2(t)$ that exhibit positive values in the first half chip and negative values in the second half. Also in this case , $u_2(t)$ is more robust than $u_1(t)$ against the reference attack, yielding an attack success probability lower than 10^{-10} for $0.3 < \Delta_E/T_c < 0.8$. Similar considerations hold for the binary signaling case, omitted here for sake of conciseness.

7.3 Prediction attacks

We have seen that the prediction attacks are more powerful than the reference attack, given a successful $x(t)$ prediction. In this section , we evaluate P_{pred}, as defined

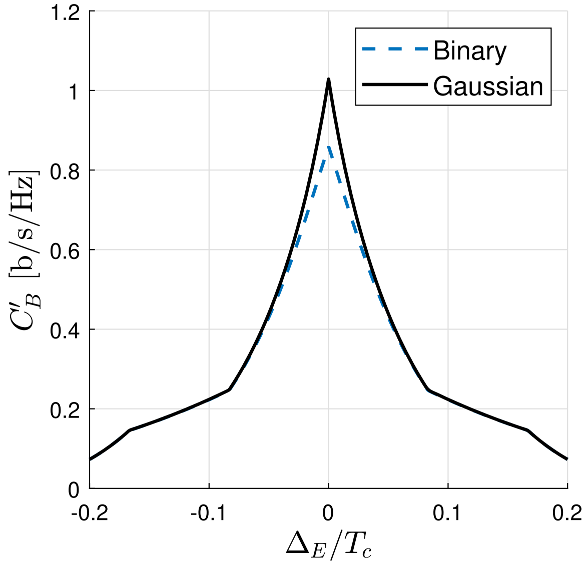

Fig. 9 Degradation of VR's capacity versus the delay Δ_E, using the transmission chip pulse $u_2(t)$, with $\sigma^2_{w_B} = -5$ dB and $\sigma^2_\omega = 0$ dB

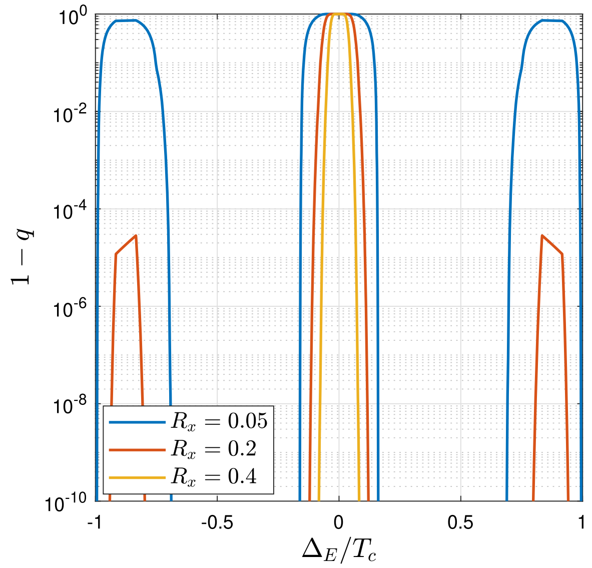

Fig. 11 $1 - q(\Gamma'_B(\Delta_E), R_x, \bar{n})$ (Gaussian case) as a function of the attack delay Δ_E for three values of R_x and using pulse $u_2(t)$ of Fig. 4, $\sigma^2_{w_B} = -5$ dB

in (52), for various system configurations. In particular, for the blind prediction attack, P_{pred} is a simple exponential function of $\bar{n}$ and R_{x}, thus we omit showing it, and we focus on the codeword prediction attack that also depends on the device operating conditions.

Figure 12 shows P_{pred} as function of σ_ω^2 and $\bar{n} = 250$ for the codeword prediction attack. We consider $R_A = C_B - C_E$ with capacities given by Gaussian (marked lines) and binary (without markers) signaling, for three values of $\sigma_{w_B}^2$. In general, we observe that the Gaussian signaling offers more protection against the codeword prediction attack than binary signaling. However, the difference with the binary signaling becomes less relevant as $\sigma_{w_B}^2$ increases.

We now asses the impact of the number of quantization bits b on P_{pred}, see (58), for the PLA scheme with $R_A = C_A$ and C_B given by (27). Figure 13 shows P_{pred} as a function of σ_ω^2 for different values of b, with $\mathrm{b} = \infty$ corresponding to no quantization of the AN. We can see that a lower b requires the system to work with a higher σ_ω^2 in order to keep a desired level of P_{pred}. However, note how performance rapidly approaches $\mathrm{b} = \infty$, as soon as b increases, suggesting that implementations with a reasonably low b are close to optimal.

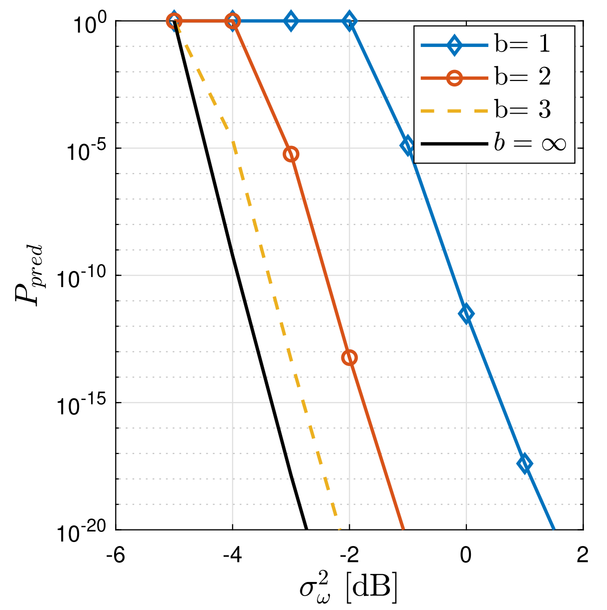

Fig. 13 P_{pred} for the codeword prediction attack as a function of σ_ω^2 for different values of b. Gaussian signaling, with $\sigma_{w_B}^2 = -5$

7.4 Power optimization

In this section, we consider the power optimizations of Section 6.

Reference attack: For the optimization against the reference attack, Fig. 14 shows $f\left(\sigma_{\text{opt}}^2\right)$, (see (63)) as a function of A for three values of $\sigma_{w_B}^2$. We note that for an increasing power budget A, we can make the system more sensitive to synchronization errors, which corresponds to having a smaller $f\left(\sigma_{\text{opt}}^2\right)$.

Figure 15 shows σ_{opt}^2 as a function of A and three values of $\sigma_{w_B}^2$. In general, we need to spend more power on the authentication message rather than on AN. For a small A,

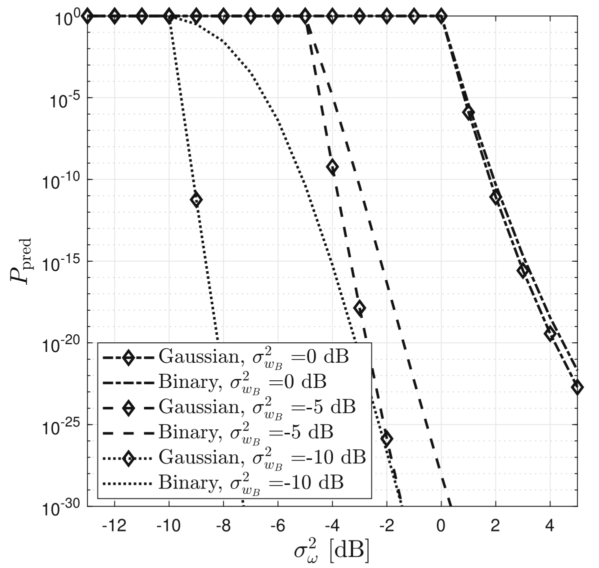

Fig. 12 P_{pred} for the codeword prediction attack as a function of σ_ω^2. Binary (no markers) and Gaussian (markers) signaling, with $\Gamma_B = 5$ dB and three different values of $\sigma_{w_B}^2$

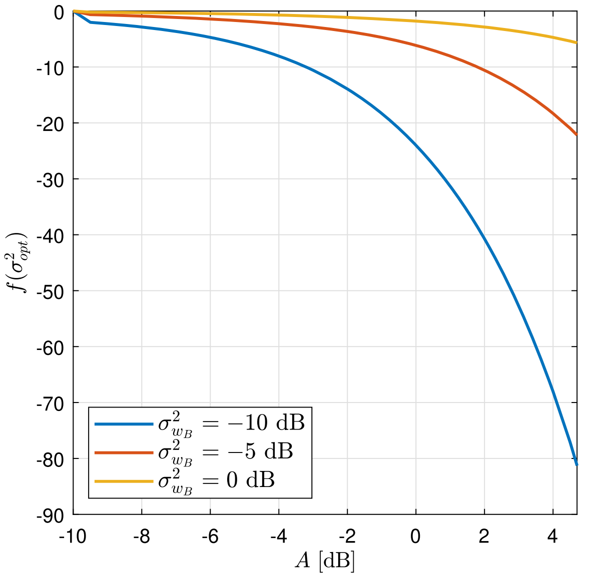

Fig. 14 $f(\sigma_{\text{opt}}^2)$ as a function of A for three values of $\sigma_{w_B}^2$

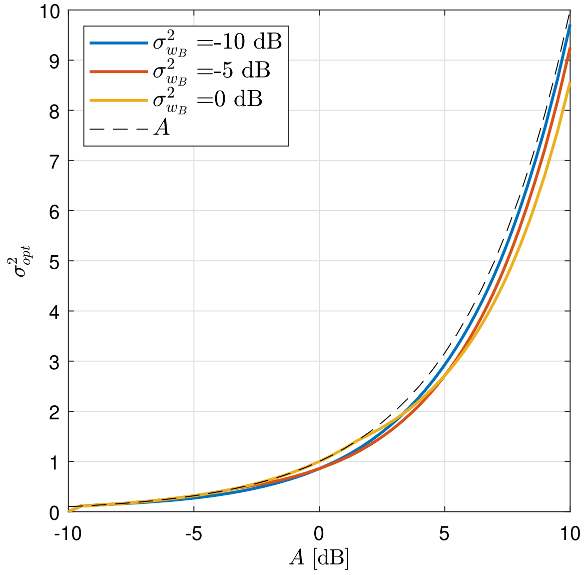

Fig. 15 σ^2_{opt} as function of A for three values of $\sigma^2_{w_B}$

we actually do not need AN (thus $\sigma^2_{\text{opt}} = A$). This corresponds to the candidate point o^* in (67) being outside the feasible set $\mathcal{E}$.

Prediction attacks: Figure 16 shows the authentication capacity (59) as a function of the power constraint A for different values of $\sigma^2_{w_B}$. The power of the AN is chosen according to (72) and Gaussian signaling is assumed (see Section 6.2). We recall that in our model, the navigation signal has unitary power, i.e., $A = 0$ dB implies that we are using the same amount of power for both the navigation and authentication components. Note that a 0 dB thermal noise power yields zero authentication capacity for $A = 0$ dB, and we thus need $A > 2.2$ dB to obtain a positive C_A.

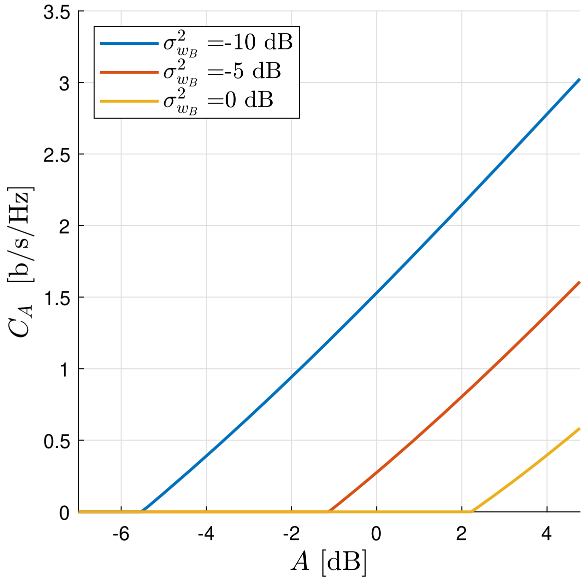

Fig. 16 Authentication capacity under power constraint A for three values of $\sigma^2_{w_B}$

8 Conclusions

In this work, we proposed a novel authentication protocol, and we showed that the proposed solution effectively authenticates a navigation message. We analyzed the protocol performance under various transmission constraints, such as finite-length codewords, binary signaling and power constraints. We conclude that the proposed strategy is effective in providing authentication of the Galileo signal, preventing the reference attack for Gaussian signaling and significantly lowering the success of attacks for finite-length codeword and finite signaling. We also considered prediction attacks specifically targeting the PLA, showing how the unpredictability of the AN further increases its security.

Appendix A: Derivation of interference coefficients for the reference attack

The interference coefficients in (43) are given by

$$\alpha = \int_{\epsilon}^{T_s} s_T(\tau - \epsilon) s_R(\tau) d\tau, \tag{73}$$

$$\beta = \int_{0}^{\epsilon} s_T(\tau + T_s - \epsilon) s_R(\tau) d\tau, \tag{74}$$

$$s_T(t) = \sum_{i=0}^{N_c - 1} c_{A,i} g_{Tx}(t - iT_c). \tag{75}$$

For the residual quantization error $w^{(q)}_{k,\epsilon}$, we have

$$\omega_{k,\epsilon} = \int_{kT_s}^{(k+1)T_s} \omega(\tau - \epsilon) s_R(\tau - kT_s) d\tau, \tag{76}$$

and thus

$$w^{(q)}_{k,\epsilon} = \omega_{k,\epsilon} - \mathcal{Q}(\omega_k). \tag{77}$$

The power of $w^{(q)}_{k,\epsilon}$ is

$$\sigma^2_{w_{q,\Delta}}(\epsilon) = \mathbb{E}\left[|w^{(q)}_{k,\epsilon}|^2\right], \tag{78}$$

where $\mathbb{E}[\cdot]$ is the expectation operator. Considering perfect quantization, i.e., $\omega_k = \mathcal{Q}(\omega_k)$, $\omega_{k,\epsilon}$ and ω_k are two correlated Gaussian random variables. Note that

$$\sigma^2_{w_{q,\Delta}} = \mathbb{E}\left[\left(w^{(q)}_{k,\epsilon}\right)^2\right] + \mathbb{E}\left[(\omega_k)^2\right] - 2\mathbb{E}\left[w^{(q)}_{k,\epsilon}\omega_k\right]. \tag{79}$$

Now we have

$$\begin{aligned}\mathbb{E}\left[\omega_{k,\epsilon}\omega_k\right] &= \\ &= \mathbb{E}\left[\int_0^{T_s}\int_0^{T_s} \omega(\tau)s_T(\tau)\omega(\tau'-\epsilon)s_R(\tau')d\tau' d\tau\right] \\ &= \int_0^{T_s}\int_0^{T_s} \mathbb{E}\left[\omega(\tau)\omega(\tau'-\epsilon)\right] s_T(\tau)s_R(\tau')d\tau' d\tau,\end{aligned} \tag{80}$$

where the second line comes from (77), the third line comes from the linearity of the expectation, and we considered $k = 0$ in the integral limits for the noise stationarity. Since $\omega(t)$ is a white Gaussian process, by definition the inner expected value becomes

$$\mathbb{E}\left[\omega(\tau)\omega(\tau'-\epsilon)\right] = \delta(\tau-\tau'+\epsilon)\sigma_\omega^2, \tag{81}$$

where $\delta(\cdot)$ is the continuous time impulsive function. Due to the integral properties of $\delta(\cdot)$, (80) becomes

$$\mathbb{E}\left[w_k^\epsilon \omega_k\right] = \sigma_\omega^2 \int_0^{T_s-\epsilon} s_T(\tau)s_R(\tau+\epsilon)d\tau = \sigma_\omega^2 \nu_\epsilon, \tag{82}$$

where the result of the integral ν_ϵ only depends on ϵ and the transmitter and receiver pulses. Note that if $\epsilon = 0$, then $\omega_k = \omega_{k,\epsilon}$ and $w_{k,\epsilon}^q = 0$. Moreover, for a high ϵ, the correlation between ω_k and $\omega_{k,\epsilon}$ decreases; if ϵ exceeds T_s, the two variables become uncorrelated ($\nu_\epsilon = 0$), since they insist on disjoint intervals of $\omega(t)$. Under these conditions, $\sigma_{w_{q,\Delta}}^2 = 2\sigma_\omega^2(1-\nu_\epsilon)$.

We now show that Γ_{B} is a monotonically decreasing function for $0 \le \Delta_{\mathrm{E}} \le T_c$, when $u(t)$ has a rectangular shape. From (73), we get

$$\alpha = A_1 + A_2\Delta_E, \tag{83}$$

where

$$A_1 = T_c \sum_{i=1}^{i=N_c} c_i^2, \quad A_2 = \sum_{i=2}^{i=N_c} c_i c_{i-1} - \sum_{i=1}^{i=N_c} c_i^2. \tag{84}$$

Note that $A_2 \le 0$, therefore α decreases with Δ_{E}. By definition of ν_ϵ in (82), we also get $\alpha = \nu$ since the symmetry of the rectangular shape we are considering yields the same expression for the correlation integral. Similarly, from (74) we get

$$\beta = c_1 c_{N_c}\Delta_{\mathrm{E}} = B\Delta_{\mathrm{E}}, \tag{85}$$

where β is an increasing function of Δ_{E}. By definition of Γ_{B}, we have

$$\Gamma'_{\mathrm{B}}(\Delta_{\mathrm{E}}) = \frac{(A_1+A_2\Delta_{\mathrm{E}})^2\sigma_x^2}{(B\Delta_{\mathrm{E}})^2\sigma_x^2 + \sigma_{w_B}^2 + 2\sigma_\omega^2(1-A_1-A_2\Delta_{\mathrm{E}})}, \tag{86}$$

where the numerator is a decreasing function of Δ_{E} and the denominator is an increasing function of Δ_{E}. It follows that $\Gamma_{\mathrm{B}}(\Delta_{\mathrm{E}})$ is a monotonically decreasing function of Δ_{E}.

Endnote

[1] Note that indeed the AN signal $\omega(t)$ can be directly generated at the satellite. Note also that the satellite must transmit the quantized AN samples to the ground segment.

Abbreviations

AN: Artificial noise; AT: Attacker; AWGN: Additive white Gaussian noise; BPSK: Binary phase shift keying; CDF: Cumulative distribution function; FEA: Forward estimation attack; FEC: Forward error correction; iid: Independent and identically distributed; IT: Information theory; LMS: Land mobile satellite link; LOS: Line of sight; NMA: Navigation message authentication; MC: Markov chain; PDF: Probability density function; PLA: Physical layer authentication; PSD: Power spectral density; PSK: Phase shift keying; SCER: Security code estimation and replay; SNR: Signal to noise ratio; VR: Victim receiver

Acknowledgements

No acknowledgements.

Funding

No Specific funding.

Availability of data and materials

No data is available.

Authors' contributions

The contribution of this paper consists in the proposal and analysis of a novel authentication scheme for the authentication of GNSS signals. Both authors contributed significantly in writing the manuscript and they read and approved the final version.

Competing interests

The authors declare that they have no competing interests.

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Received: 21 September 2018 Accepted: 21 March 2019
Published online: 18 April 2019

References

1. D. P. Shepard, T. E. Humphreys, A. A. Fansler, Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks. Int. J. Crit. Infrastruct. Prot. **5**(3-4), 146–153 (2012)
2. K. D. Wesson, D. P. Shepard, J. A. Bhatti, Humphreys T.E., in *Radionavigation Laboratory Conference Proceedings*. An evaluation of the vestigial signal defense for civil GPS anti-spoofing (University of Texas, Austin, 2011)
3. D. M. Akos, Who's afraid of the spoofer? GPS/GNSS spoofing detection via automatic gain control (agc). Navig. J. Inst. Navig. **59**(4), 281–290 (2012)
4. A. Cavaleri, B. Motella, M. Pini, Fantino M., in *Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC) 2010 5th ESA Workshop on*. Detection of spoofed GPS signals at code and carrier tracking level (IEEE, Noordwijk, 2010), pp. 1–6
5. M. Cuntz, A. Konovaltsev, M. Heckler, A. Hornbostel, L. Kurz, G. Kappen, Noll T., in *Proc. ION GNSS, vol 2010*. Lessons learnt: The development of a robust multi-antenna GNSS receiver (Oregon Convention Center, Portland, 2010), pp. 21–24
6. E. Axell, M. Alexandersson, Lindgren T., in *Localization and GNSS (ICL-GNSS), 2015 International Conference on*. Results on GNSS meaconing detection with multiple cots receivers (IEEE, Gothenburg, 2015), pp. 1–6
7. E. Axell, E. G. Larsson, Persson D., in *Acoustics, Speech and Signal Processing (ICASSP), 2015 IEEE International Conference on*. GNSS spoofing detection using multiple mobile cots receivers (IEEE, Brisbane, 2015), pp. 3192–3196
8. P. Levin, D. S. De Lorenzo, P. K. Enge, S. C. Lo, Authenticating a signal based on an unknown component thereof, June 28 2011. US Patent 7,969,354
9. B. W. O'Hanlon, M. L. Psiaki, J. A. Bhatti, D. P. Shepard, T. E. Humphreys, Real-time GPS spoofing detection via correlation of encrypted signals. Navigation. **60**(4), 267–278 (2013)

10. A. J. Kerns, K. D. Wesson, Humphreys T.E., in *Position, Location and Navigation Symposium-PLANS 2014, 2014 IEEE/ION*. A blueprint for civil GPS navigation message authentication (IEEE, Monterey, 2014), pp. 262–269
11. L. Scott, in *Proceedings of the 16th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GPS/GNSS 2003)*. Anti-spoofing & authenticated signal architectures for civil navigation systems (Oregon Convention Center, Portland, 2001), pp. 1543–1552
12. J. T. Curran, C. O'Driscoll, Message authentication as an anti-spoofing mechanism (2017). Technical report, Working Paper. researchgate.net
13. G. Caparra, S. Ceccato, N. Laurenti, J. Cramer, in *Proc. of the 30th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2017), Portland, OR*. Feasibility and limitations of self-spoofing attacks on GNSS signals with message authentication, (2017), pp. 3968–3984
14. T. E. Humphreys, Detection strategy for cryptographic GNSS anti-spoofing. IEEE Trans. Aerosp. Electron. Syst. **49**(2), 1073–1090 (2013)
15. E. Jorswieck, S. Tomasin, A. Sezgin, Broadcasting into the uncertainty: Authentication and confidentiality by physical-layer processing. Proc. IEEE. **103**(10), 1702–1724 (2015)
16. X. Wu, Z. Yang, C. Ling, X. G. Xia, Artificial-noise-aided message authentication codes with information-theoretic security. IEEE Trans. Inf. Forensics Secur. **11**(6), 1278–1290 (2016)
17. F. Formaggio, S. Tomasin, G. Caparra, S. Ceccato, N. Laurenti, in *Proc. IEEE 2018 26th European Signal Processing Conference (EUSIPCO)*. Authentication of Galileo GNSS signal by superimposed signature with artificial noise, (Rome, 2018), pp. 2573–2577
18. W. Stallings, *Cryptography and network security: Principles and practice*. (Pearson, Upper Saddle River, 2017)
19. F. P. Fontan, M. Vázquez-Castro, C. E. Cabado, J. P. Garcia, E. Kubista, Statistical modeling of the LMS channel. IEEE Trans. Veh. Technol. **50**(6), 1549–1567 (2001)
20. C. Loo, A statistical model for a land mobile satellite link. IEEE Trans. Veh. Technol. **34**(3), 122–127 (1985)
21. J. E. Gentle, *Random number generation and Monte Carlo methods*. (Springer Science & Business Media, New York, 2006)
22. H. Niederreiter, *Random number generation and quasi-Monte Carlo methods, vol. 63*. (Society for Industrial & Applied Mathematics, US, 1992)
23. P. L'Ecuyer, *Handbook of Computational Statistics*. (Springer, Berlin, 2012)
24. T. Erseghe, On the evaluation of the Polyanskiy-Poor–Verdú converse bound for finite block-length coding in AWGN. IEEE Trans. Inf. Theory. **61**(12), 6578–6590 (2015)
25. T. Erseghe, Coding in the finite-blocklength regime: Bounds based on Laplace integrals and their asymptotic approximations. IEEE Trans. Inf. Theory. **62**(12), 6854–6883 (2016)
26. M. Bloch, J. Barros, *Physical-layer security: from information theory to security engineering*. (Cambridge University Press, 2011)
27. M. Hayashi, R. Matsumoto, Construction of wiretap codes from ordinary channel codes (2010). arXiv preprint arXiv:1001.1197
28. W. K. Harrison, J. Almeida, M. R. Bloch, S. W. McLaughlin, J. Barros, Coding for secrecy: An overview of error-control coding techniques for physical-layer security. IEEE Signal Proc. Mag. **30**(5), 41–50 (2013)
29. I. Galileo, Galileo open service, signal in space interface control document (OS SIS ICD) (2008). European space agency/European GNSS supervisory authority
30. A. Joseph, GNSS solutions: Measuring signal strength (2010). GNSS insidegnss.com

Submit your manuscript to a SpringerOpen journal and benefit from:

► Convenient online submission
► Rigorous peer review
► Open access: articles freely available online
► High visibility within the field
► Retaining the copyright to your article

Submit your next manuscript at ► springeropen.com