Statistical Characterization of Snapshot OSNMA Spoofing Detection

Husnain Shahid[⋆], Luca Canzian[§], Carlo Sarto[§], Oscar Pozzobon[§]
Joaquín Reyes-González[†], Gonzalo Seco-Granados[⋆], José A. López-Salcedo[⋆]
[⋆]Universitat Autònoma de Barcelona (UAB), IEEC-CERES, Barcelona, Spain
[§]Qascom SrL, Bassano del Grappa, Italy
[†]EUSPA, Prague, Czech Republic

***Abstract*—Spoofing detection in Global Navigation Satellite Systems (GNSS) is gradually becoming need of the hour due to significant increase in sophisticated spoofing attacks that compromise the signal integrity and security. To withstand against these attacks, Galileo is providing the Open Service Navigation Message Authentication (OSNMA) in its E1-B signal component, comprises of a cryptographic protocol that conveys unpredictable data symbols to the user to verify the content of the I/NAV message. In this context, the following paper proposes a reliable spoofer detector by employing the snapshots of received unpredictable symbols and compares them with the authentic ones. The problem is formulated as a Binary Symmetric Channel (BSC), where the feasibility is determined by the probabilities of error at the spoofer's and the user's sides. However, due to the presence of signal impairments, the spoofing detector faces the hypothesis inversion problem (i.e. chooses the wrong hypothesis under certain conditions). The primary focus of this article is to avoid the hypothesis inversion problem by optimizing the statistical characterization of snapshot OSNMA detector and enhance the detection performance by designing appropriate test statistics conditions. Simulation results reveal that utilizing multiple test conditions solves the problem and strengthens the detection performance to a great extent.**

***Index Terms*—OSNMA, anti-spoofing, snapshot receivers.**

I. Introduction

Global Navigation Satellite Systems (GNSS) are experiencing a dramatic growth in the segment of mass-market receivers such as smartphones and Internet-of-Things (IoT) devices. On the other hand, GNSS is covering a myriad of location-based applications including road transportation and automotive, aviation, maritime, agriculture and emergency localization, just to mention a few [1]. In parallel, spoofing is becoming an increasing threat to GNSS signal integrity, whereby an attacker intends to imitate an authentic GNSS signal to ultimately alter the user's navigation solution. In that sense, the lack of signal authentication poses serious concerns to safety- and liability-critical applications, thus hindering the deployment of GNSS in key emerging sectors.

As a countermeasure, Galileo is now implementing the Open Service Navigation Message Authentication (OSNMA) service in its E1-B signal, a mechanism that employs cryptographic data to verify the authenticity of the navigation message (I/NAV) [2]. Based on the Time Efficient Stream Loss Tolerant (TESLA) protocol, the beauty of OSNMA is that the authentication data is conveyed within a set of predictable and, most importantly, unpredictable symbols that, as such, pose difficulties to spoofing attacks. Nonetheless, even implementing such an unpredictability property of the OSNMA data, an advanced spoofer could still succeed by means of the so-called Security Code and Estimation Replay (SCER) attacks [3]. In SCER, the attacker tracks the signals from the satellites and even if they are unpredictable, it performs an estimation of the unpredictable symbols. In this way, the attacker can reconstruct the genuine OSNMA data upon a signal with spoofed I/NAV message and end up forging the victim's position, thus becoming a concerning threat to be addressed in OSNMA.

Efforts addressing the problem of SCER attacks, and more general signal replay attacks, can already be found in the existing literature [3]–[8]. They are mostly based on monitoring the received signal correlation samples and thus they are not straightforward to be implemented in existing receivers unless access to those samples is explicitly granted. This is not the case for most GNSS receivers, which merely provide at their output the observables resulting from processing the received signal and, eventually, the demodulated data symbols. Such symbols are the focus of the present work. The reason is that in the presence of a SCER attack which is actually very complicated to implement, and in reality, spoofers would have troubles in estimating the unpredictable symbols, and thus incurring in a non-negligible probability of error. Such errors will manifest as an increased symbol error rate (SER) at the victim's receiver, thus becoming an indication of a potential spoofing attack.

The problem aggravates, though, when the symbol error probability due to thermal noise (for low C/N_0), the arena of urban environments with abounding propagation impairments, such as multipath and shadowing surpass the error probability due to the spoofer. This situation misleads the proposed detector because it tends to declare *no spoofing* when the spoofed signal is present, while it tends to declare *spoofing* when the spoofed signal is absent, because far more errors

This work was supported in part by the OSNMAplus project funded by the European Union Agency for the Space Programme (EUSPA) under contract GSA/GRANT/03/2019/02, and in part by the Spanish Agency of Research (AEI) under the Research and Development projects PID2020-118984GB-I00/ and PDC2021-121362-I00/AEI/10.13039/501100011033.

979-8-3503-2308-5/23/$31.00 ©2023 IEEE

are being incurred when processing the noisy and severely degraded authentic signal than the spoofed one.

Furthermore, in most handheld receivers, continuous tracking of the GNSS signals is often not possible due to power consumption constraints. Instead, the receiver front-end is periodically switched on, from some tens up to a few hundreds of milliseconds, whereas it remains in sleep mode for the rest of time. This is usually referred to as snapshot processing, and as drawback, it does not allow decoding the navigation messages, thus hampering the implementation of native OSNMA in GNSS receivers with limited computational resources.

In this context, the purpose of this paper is to explore the statistical characterization of symbol-level spoofing detector for snapshot receivers by exploiting the OSNMA data unpredictability. To do so, the paper is structured as follows. Section II introduces the system architecture for implementing the so-called snapshot OSNMA technique. Section III presents the signal model and highlights the sources of symbol errors. The proposed symbol-level spoofer detector is discussed in Section IV while the statistical characteristics of the proposed detector are thoroughly illustrated in Section V. Moreover, simulation performance is assessed in Section VI. Finally conclusions are drawn in Section VII.

II. Snapshot OSNMA System Architecture

The high-level architecture of the so-called snapshot OSNMA service considered in this work is shown in Figure 1. It is composed of two parties that correspond to the user side and the remote server side. On the one hand, the user side is responsible for gathering and processing the snapshots of the received Galileo E1-B signal. The result of such processing is the estimated user's position and time, which are obtained with the help of assisted GNSS (AGNSS) and coarse-time navigation [9], as well as the received OSNMA symbols at each snapshot. It is worth mentioning that the OSNMA bits are transmitted by the Galileo satellites within the 40 bits ”Reserved” field in the odd pages of the I/NAV message [10]. These 40 bits are convolutionally encoded at the transmitter at a rate $1/2$, providing 80 coded bits that are interleaved with the remaining bits of I/NAV odd page and then BPSK modulated. Out of the resulting 250 symbols, only a subset of them are unpredictable, as discussed in [4] and refined in [5]. Most of them are predictable and thus carry no information from a spoofing detection point of view. The interest here is on the unpredictable symbols, which are the ones that potential spoofers need to actively determine while performing a SCER attack and therefore, where errors might be incurred.

Once the symbols of the odd page containing OSNMA have been retrieved from the received signal, they are sent to the remote server where the snapshot OSNMA service is actually running, as shown in Fig. 1. Upon reception at the remote end, the estimated user's position and time are employed to access a repository where the set of all unpredictable OSNMA symbols transmitted by the Galileo satellites up to that moment is available. This repository is populated by a trusted Galileo receiver operating 24/7. When the authentic symbols that were supposed to be received at the estimated user's position and time are retrieved from the trusted repository, the next step is to compare the authentic symbols with those actually received by the user. If both coincide, it is worth to say that the received symbols are identical to the authentic ones and the user's OSNMA data can at least be declared authentic, and the received signal can thus be trusted at symbol level. In contrast, if too many errors are found in the comparison (i.e more errors than those expected due to the working conditions), the received signal can be declared to be spoofed at symbol level, and consequently, at signal level as well. The affected satellite should therefore be discarded by the user.

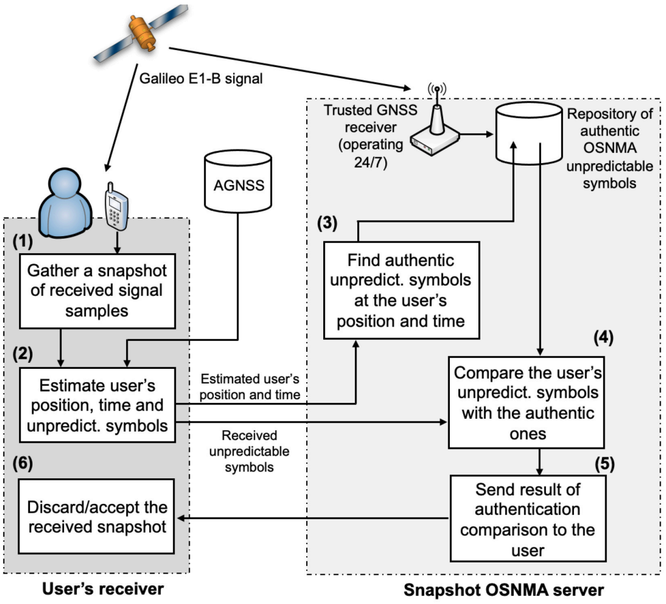
Galileo E1-B signal
Trusted GNSS receiver (operating 24/7)
Repository of authentic OSNMA unpredictable symbols
AGNSS
(1)
Gather a snapshot of received signal samples
(2)
Estimate user's position, time and unpredict. symbols
(3)
Find authentic unpredict. symbols at the user's position and time
(4)
Compare the user's unpredict. symbols with the authentic ones
(5)
Send result of authentication comparison to the user
(6)
Discard/accept the received snapshot
Estimated user's position and time
Received unpredictable symbols
User's receiver
Snapshot OSNMA server

Fig. 1: Architecture of the proposed snapshot OSNMA service.

III. Signal Model

A. Signal model at the spoofer's side

In the sequel, the OSNMA unpredictable symbols transmitted by a given Galileo satellite are denoted as $s(n)$ for a given time instant n, with $s(n) \in \{\pm 1\}$. Note that while predictable and unpredictable symbols are received altogether, we simplify our model by assuming that the server can extract the unpredictable symbols from the symbol stream, as per [5].

In reality, when a spoofer is implementing a replay attack, it would have trouble to estimate such unpredictable symbols and there is some probability p_s that the spoofer may incur in error. This is nothing but the SER at the spoofer's side. Denoting the symbols transmitted by the spoofer as $\tilde{s}(n)$, it follows that

$$\tilde{s}(n) = \begin{cases} s(n) & \text{, with probability } 1-p_s \\ \bar{s}(n) & \text{, with probability } p_s \end{cases} \tag{1}$$

where $\bar{s}(n) \doteq -s(n)$ is the sign-reversed version of symbol $s(n)$. As can be seen, a spoofer trying to infer the unpredictable symbols in a constrained scenario and potentially subject to propagation impairments can be regarded as a

Binary Symmetric Channel (BSC) where the input symbols are sign-reversed at its output with probability p_s. For a BPSK modulation, p_s is given by,

$$p_s = \frac{1}{2}\text{erfc}\left(\sqrt{T(C/N_0)_{|\text{a,s}}}\right) \tag{2}$$

where $T = 4$ ms is the Galileo E1-B symbol period, erfc is the complementary error function and $(C/N_0)_{|\text{a,s}}$ is the carrier-to-noise ratio of the authentic signal received at the spoofer's terminal.

Spoofers considered in this work fall within the category of the so-called *sophisticated* spoofers, because they actively try to estimate the OSNMA unpredictable symbols rather than randomly guess them. To do so, they accumulate the authentic signal for a very short period of time, in order to gather enough energy to ascertain the value of the current unpredictable symbol, while minimizing the delay incurred in the retransmitted signal. This approach was discussed in [4], [8], where it was shown that integrating the authentic signal for just a few chips suffices to obtain a reliable estimate of the unpredictable symbol.

Two different sophisticated spoofers will be considered herein, namely an optimistic spoofer incurring in a relatively high probability of error, $P_e = 0.1$, and a pessimistic spoofer being much more difficult to detect, and incurring in just $P_e = 0.01$. In order to get some insights on the different impact of both spoofers, it is interesting to recall that for a snapshot of Q symbols, the probability that the spoofer incurs in at least one symbol error within such snapshot is,

$$\text{prob(at least one error in } Q \text{ symbols)} = 1 - (1 - p_s)^Q \tag{3}$$

By applying (3), it is found that $Q > 22$ and $Q > 230$ symbols are needed for the optimistic and pessimistic spoofers, respectively, in order to make sure (i.e. 90% of the time) that at least one symbol error due to the spoofer occurs. This provides an idea of how long it takes to observe one single symbol error, taking into account that a maximum of 32 unpredictable symbols are available every odd-page of the I/NAV message (i.e. every 2 seconds).

B. Signal model at the user's side

The symbols estimated by the user's receiver upon processing a snapshot of Galileo E1-B will be denoted by $\hat{s}(n)$. They are the result of taking a hard decision on the output of the prompt correlator, once the receiver is locked to the received signal. As such, the demodulated symbols can incur in error due to the presence of thermal noise, propagation effects, etc. The symbol decision at the user's side can therefore be modeled as another BSC in series with the one representing the spoofer symbol decision. This leads to an equivalent end-to-end binary channel with a total of four possible outputs. Let us first denote by $\mathcal{H}_0$ the situation when no spoofer is present and by $\mathcal{H}_1$ the situation when the signal of interest is being spoofed. The four possible symbol decisions are therefore,

$$\mathcal{H}_0 \quad : \quad \hat{s}(n) = \begin{cases} s(n) & \text{, with probability } 1 - p_{u,0} \\ \bar{s}(n) & \text{, with probability } p_{u,0} \end{cases} \tag{4}$$

$$\mathcal{H}_1 \quad : \quad \hat{s}(n) = \begin{cases} s(n) & \text{, with probability } 1 - p_{u,1} \\ \bar{s}(n) & \text{, with probability } p_{u,1} \end{cases} \tag{5}$$

where $p_{u,0}$ and $p_{u,1}$ stand for the SER at the user's terminal under $\mathcal{H}_0$ and $\mathcal{H}_1$, respectively.

The term $p_{u,0}$ can be readily computed as the SER for a BPSK modulation in (2) by replacing $(C/N_0)_{|\text{a,s}}$ with $(C/N_0)_{|\text{a,u}}$, which refers to the C/N_0 of the authentic signal received by the user. In turn, the term $p_{u,1}$ is given by

$$p_{u,1} = p_s + p_{s,u} - 2p_s p_{s,u} \tag{6}$$

where $p_{s,u}$ is the SER of the spoofed symbols received by the user. It can also be computed as the SER in (2) by replacing $(C/N_0)_{|\text{a,s}}$ with $(C/N_0)_{|\text{s,u}}$, which refers to the C/N_0 of the spoofed signal received by the user.

IV. Proposed Symbol-Level Spoofer Detection

The detector proposed in this work has two distinctive features. First, it works on short snapshots of received signal, typically of tens or a few hundreds of ms length. And second, it works at symbol level using the demodulated symbols provided by the user's receiver to the remote server together with the estimated user's position and time. Note that a similar concept but fully implemented at the user's terminal was addressed in [11]. These refer to the symbols obtained at the maximum peak of the correlation function between the received signal and the local replica, once the code delay, frequency and phase offsets have been estimated and compensated. Note that no decoding is needed but only to take the sign of the maximum peak of the correlation. Each snapshot of received signal is assumed to provide a set of L OSNMA symbols that stacked into vector $\hat{\mathbf{s}}_i$ as,

$$\hat{\mathbf{s}}_i = \text{sign}(\mathbf{r}_i) = [\text{sign}\,(r_i(0))\,, \ldots, \text{sign}\,(r_i(L-1))]^T \tag{7}$$

where $i = 0, 1, \ldots, N-1$ determines the snapshot being processed among a total of N snapshots available. Based on the set of available symbols, the proposed detector compares the unpredictable with the authentic ones to know about if any of them is altered or not by the presence of a potential spoofer. This can be done by computing the Hamming distance between $\hat{\mathbf{s}}_i$ and $\mathbf{s}_i$, referred herein as $d_{\text{Hamming}}\,(\hat{\mathbf{s}}_i, \mathbf{s}_i)$, for each received snapshot. In this way the detector becomes,

$$H(\hat{\mathbf{s}}, \mathbf{s}) = \sum_{i=0}^{N-1} d_{\text{Hamming}}\,(\hat{\mathbf{s}}_i, \mathbf{s}_i) \tag{8}$$

The Hamming distance provides the number of non-coincident elements between two arrays. Hence, the Hamming distance applied to the problem at hand provides the number of errors in the received unpredictable symbols with respect to the authentic ones. By monitoring this metric one can make sure

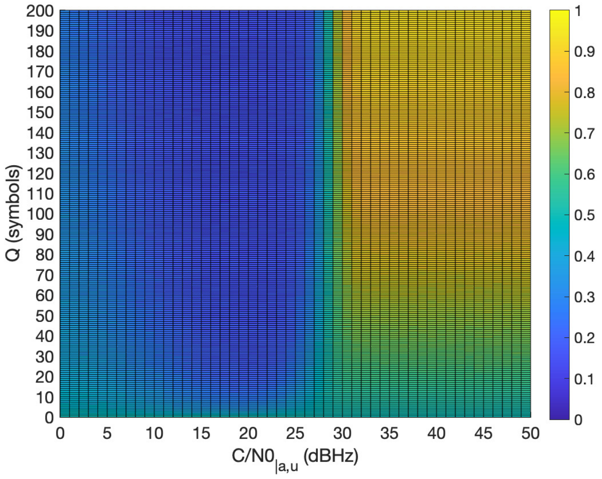

Fig. 2: AUC for a spoofer with 5dB power advantage in perfect LOS conditions with $p_s = 0.01$

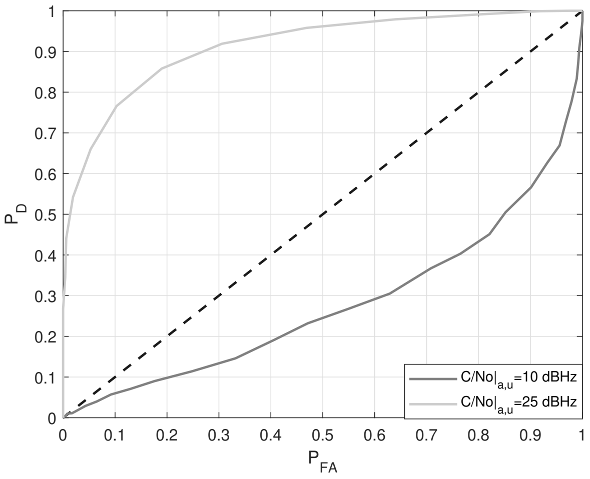

Fig. 3: Empirical ROC curve for a spoofer with 5dB power advantage in perfect LOS with $p_s = 0.1$ and $Q = 100$

whether the obtained number of errors are reasonable for a receiver that should be processing an authentic signal at a given working conditions, and for which the probability of error should be constrained to $p_{u,0}$ in the absence of spoofing.

V. Statistical Characterization

For the two hypotheses under analysis, namely spoofer absent ($\mathcal{H}_0$) or spoofer present ($\mathcal{H}_1$), the statistical distribution of the detector in (8) can be found to be given by,

$$H(\hat{\mathbf{s}}, \mathbf{s}) \sim \begin{cases} B(Q, p_{u,0}) & : \mathcal{H}_0 \\ B(Q, p_{u,1}) & : \mathcal{H}_1 \end{cases} \tag{9}$$

where $B(m, p)$ stands for the Binomial distribution for a set of m symbols and probability of success p. In our case we have $m = Q$ and p is the probability of having a symbol error. That is, either $p_{u,0}$, the aforementioned SER in the absence of spoofer, or $p_{u,1}$, the SER in the presence of spoofer given by (6).

An important remark to be made is that the demodulated symbols from a short snapshot of signal do not have an absolute phase reference and can thus be affected by a rotation of 180°. This means that the symbols retrieved by a snapshot receiver can either be the correct symbols or the sign-reversed ones. This fact must be accounted for in the statistics of the proposed detector in (9), thus leading to a mixed Binominal distribution under each of the two hypotheses,

$$H(\hat{\mathbf{s}}, \mathbf{s}) \sim \begin{cases} \frac{1}{2}B(Q, p_{u,0}) + \frac{1}{2}B(Q, 1 - p_{u,0}) & : \mathcal{H}_0 \\ \frac{1}{2}B(Q, p_{u,1}) + \frac{1}{2}B(Q, 1 - p_{u,1}) & : \mathcal{H}_1 \end{cases} \tag{10}$$

For the feasibility study to be conducted herein, the focus will be placed on the receiver operating curve (ROC) and, the area under the curve (AUC). The former represents the probability of detection as a function of the probability of false alarm, while the latter is the integral of the ROC curve. The advantage of the AUC is that it summarizes the performance represented by the ROC curve into a single number. A key feature of the AUC is that for a detector randomly declaring either $\mathcal{H}_0$ or $\mathcal{H}_1$, the ROC curve would be a straight line ranging from coordinate $(P_{\text{D}}, P_{\text{FA}}) = (0, 0)$ to coordinate $(P_{\text{D}}, P_{\text{FA}}) = (1, 1)$ [12]. This means that the AUC would be equal to 0.5 for a random detector. In contrast, for an ideal detector keeping $P_{\text{D}} = 1$ when $P_{\text{FA}} \to 0$ the AUC would be equal to 1. So typically, the AUC values range from 0.5 (worst case) to 1 (best case). Therefore, a preliminary performance of the proposed detector can be assessed as a function of Q and the C/N_0 at the user's terminal. Note that neither the ROC nor the AUC need a specific threshold γ.

Fig. 2 illustrates the AUC for a spoofer with 5dB power advantage. It is worth noticing that the left side of Fig. 2 approaches to AUC < 0.5 or even AUC $\to 0$, which is colored in dark blue. In this region, the symbol errors due to the noise, fading and shadowing effects are larger than those due to the spoofer, which remains at $p_s = 0.01$. Furthermore, since the spoofer has 5 dB more power than the authentic signal, the spoofed signal provides very little errors as compared to the authentic signal, which is dominated by noise and channel effects. This situation misleads the detector because it tends to declare $\mathcal{H}_0$ when the spoofed signal is present, while it tends to declare $\mathcal{H}_1$ when the spoofed signal is absent, because far more errors are being incurred when processing the noisy and severely degraded authentic signal than the spoofed one. This leads the AUC to be close to zero and in principle, this dark blue region should be avoided because the detector is not working properly.

Fig. 3 is a depiction of hypothesis inversion and further characterizes three different cases of AUC in terms of ROC curve. The central straight line refers to the random detector and can be specified as a lower bound for ROC curve. Similar to the right side or yellow region of Fig. 2 but for $p_s = 0.1$, the curve in the upper side of Fig. 3 is a representation of normal behavior, where the detector works efficiently. In

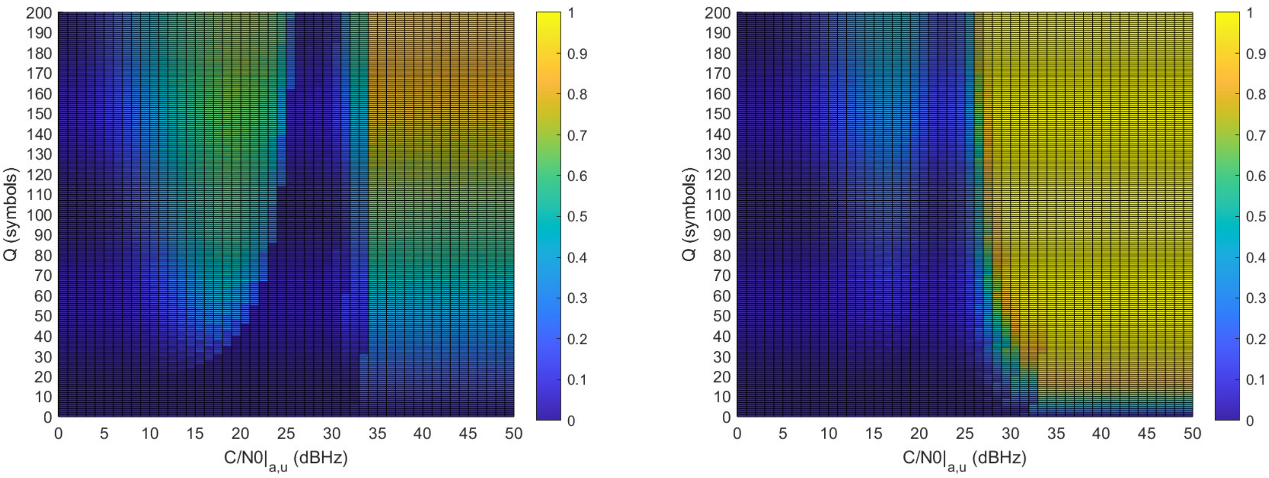

Fig. 4: P_{D} for a spoofer with 5dB power advantage in perfect LOS conditions with $p_s = 0.01$ (Left) and $p_s = 0.1$ (Right)

contrast, the lower side of Fig. 3 is similar to the situation for $p_s = 0.1$ when AUC < 0.5 or AUC $\to 0$, where the detector is consistently declaring the opposite decision to the true one. The reason for displaying the AUC for $p_s = 0.01$ and ROC for $p_s = 0.1$ is to depict the abnormal situations for both error probabilities through concise and different prespectives. Fortunately, this problem could be circumvented by exploiting the detection threshold characteristics. Since, the hypothesis $\mathcal{H}_1$ can exist on either side of the binomial distribution of $\mathcal{H}_0$, two different thresholds γ_1 and γ_2 must be placed for deciding among hypotheses $\mathcal{H}_0$ and $\mathcal{H}_1$, and given by [13],

$$\gamma_1 = F^{-1}_{H(\hat{\mathbf{s}},\mathbf{s});\mathcal{H}_0}(1 - P_{\mathrm{FA}}) \tag{11}$$

and

$$\gamma_2 = F^{-1}_{H(\hat{\mathbf{s}},\mathbf{s});\mathcal{H}_0}(P_{\mathrm{FA}}) \tag{12}$$

where $F^{-1}_{H(\hat{\mathbf{s}},\mathbf{s});\mathcal{H}_0}$ is the inverse cumulative distribution of the detector under $\mathcal{H}_0$ and P_{FA} is desired probability of false alarm. Moreover, it is already remarked that the demodulated symbols can be affected by a rotation of 180°. Therefore, the detection criteria will be based on the following decision rule,

$$\begin{aligned} \gamma_2 \leq H(\hat{\mathbf{s}},\mathbf{s}) \leq \gamma_1 \quad &\Rightarrow \quad \text{decide } \mathcal{H}_0 \\ Q - \gamma_1 \leq H(\hat{\mathbf{s}},\mathbf{s}) \leq Q - \gamma_2 \quad &\Rightarrow \quad \text{decide } \mathcal{H}_0 \end{aligned} \tag{13}$$

and declares the alternative hypothesis $\mathcal{H}_1$ under any of the following test statistics conditions,

$$\begin{aligned} H(\hat{\mathbf{s}},\mathbf{s}) < \gamma_2 \quad &\Rightarrow \quad \text{decide } \mathcal{H}_1 \\ \gamma_1 < H(\hat{\mathbf{s}},\mathbf{s}) < Q - \gamma_1 \quad &\Rightarrow \quad \text{decide } \mathcal{H}_1 \\ H(\hat{\mathbf{s}},\mathbf{s}) > Q - \gamma_2 \quad &\Rightarrow \quad \text{decide } \mathcal{H}_1 \end{aligned} \tag{14}$$

The proposed detector with modified statistical characteristics would be capable to overcome the hypotheses inversion problem and further enhance the detection performance by converting the dark blue region of Fig. 2 and lower symmetrical region of Fig. 3 to the detection region, which is validated in the later section.

VI. Simulation Results

This section imparts the analysis of detection performance given the statistical characterization of snapshot OSNMA. In addition, it provides the insights of, to what extent the formulated detector is feasible to utilize for spoofing detection in an extensive working conditions. To this end, the performance is validated by analyzing the probability of detection P_{D} as a function of Q symbols and $(C/N_0)_{|\mathrm{a,u}}$, while both thresholds γ_1 and γ_2 are calculated as a function of given $P_{\mathrm{FA}} = 10^{-3}$ as in (11) and (12).

The experiment conducted herein simulates the unpredictable symbols being received at the user's terminal from an authentic GNSS satellite at $(C/N_0)_{\mathrm{a,u}}$. When the spoofer is present, it appears simultaneously with the authentic signal and thus both signals overlap at the receiver. As in [8], it is assumed that the spoofer is perfectly aligned in time and frequency with the authentic signal, but with a random and uniformly distributed relative phase. It is also assumed that the spoofer has a 5 dB power advantage with respect to the authentic signal, which is a reasonable assumption taking into account that the goal of the spoofer is to prevail over the authentic signal, and have the user's receiver to lock onto it.

Using the proposed detector with modified statistical properties, it can be observed in Fig. 4, most of the part associated to dark blue region in Fig. 2 is translated into detection region. One could argue that this problem could be solved just by reversing the decision within a specific $(C/N_0)_{|\mathrm{a,u}}$ window. However, it is only possible when BPSK symbols are detected in the presence of a 180° phase ambiguity. In this case it may happen that all symbols are decided incorrectly with a reversed sign and then reversing its decision could solve the problem. Since, one could not know about the exact contribution of error probability p_s by spoofer, which can be even higher and hence, the dark blue area would automatically be included into the detection region due to the significant contribution of symbol errors from the spoofer, which broadens the detection region towards left, but now, just inverting the hypothesis would make it again under $\mathcal{H}_0$. Therefore, it is need of the hour to exploit the statistical properties of the problem and place an appropriate threshold for efficient detection.

The interpretation of Fig. 4 can be performed by dividing into three regions. On the one hand, the prominent region with $(C/N_0)_{\mathrm{a,u}} > 32 - 33$ dBHz can be categorized as normal region, in which the probability density function (PDF) under $\mathcal{H}_1$ lies just next to the PDF under $\mathcal{H}_0$ and the detector can always detect the spoofer provided that the latter has a probability of error different from zero. It is just a matter of time (i.e. having enough symbols) for the spoofer to be detected. On the other hand, there is a region within the range of $24 < (C/N_0)_{\mathrm{a,u}} < 32$ dBHz in Fig. 4 (Left) and $20 < (C/N_0)_{\mathrm{a,u}} < 26$ dBHz in Fig. 4 (Right), where the detector is not feasible at all. It is due to the fact that the symbols error contribution due to impairments under $\mathcal{H}_0$ becomes identical to the total symbol errors under $\mathcal{H}_1$, consequently, two PDFs lie exactly on each other and leave no room to detect on either side of the distribution.

The third region is categorized as critical region for $(C/N_0)_{\mathrm{a,u}} < 25$ dBHz in Fig. 4 (Left) and $(C/N_0)_{\mathrm{a,u}} < 19$ dBHz in Fig.4 (Right), which is a solution to the problem exists in left symmetry of Fig. 2 when AUC < 0.5 or even AUC $\rightarrow 0$. It is worth to observe that the problematic region is converted into detection region in Fig. 4 by identifying the appropriate threshold properties and solved the aforesaid hypotheses inversion problem. Note that, in this region, the detection probability for $p_s = 0.01$ is exceeding as compared to $p_s = 0.1$, which seems to be illogical because $p_s = 0.1$ should bring on with more symbol errors than $p_s = 0.1$ but it is in-fact logical. In this critical region, the distribution under $\mathcal{H}_1$ shall be next to the distribution under $\mathcal{H}_0$. Since the errors incurred by spoofer with $p_s = 0.01$ would be lesser and the corresponding distribution would lie on the extreme next as compared to the distribution associated to $p_s = 0.1$. In other words, AUC for $p_s = 0.01$ in the critical region would have more values closer to zero or less than 0.5 as compared to AUC for $p_s = 0.1$. Since it is implied that more closer the AUC to zero, farther will be the distribution under $\mathcal{H}_1$ from the distribution under $\mathcal{H}_0$. Therefore, it would be easy for a modified detector to detect the attack.

VII. Conclusions

This paper is focused on deriving the statistical characterization of snapshot OSNMA for spoofing detection. The primary idea of snapshot OSNMA technique is based on using the snapshots of OSNMA symbols provided in the I/NAV message of Galileo E1-B signal. In this context, the proposed detector compares the received OSNMA unpredictable symbols with the authentic ones. However, it is perceived that the detector undergoes with the hypothesis inversion problem due to the presence of signal impairments such as thermal noise, multi-path and shadowing etc. In other words, the detector prioritized to nominate the contrary hypothesis when the error contribution from signal impairments dominated over the errors incurred by the spoofer which results in wrong or miss detection. In this essence, this paper provided the solution to this inversion problem by exploiting and modifying the statistical properties of the detector. The profound study of statistical distributions and corresponding simulated results revealed that this problem could be avoided by designing the appropriate decision criteria based on multiple test statistics conditions.

VIII. Disclaimer

This activity has been performed in the scope of the OSNMAplus project, which is funded by the European Union (EUSPA) under grant GSA/GRANT/03/2019 and coordinated by Qascom. The content of this publication reflects only the author's view. EC/EUSPA is not responsible for any use that may be made of the information it contains. Snapshot OSNMA is the subject of the Italian patent application n. 102022000025806 filed on 16/12/2022.

References

[1] E. D. Kaplan and C. Hegarty, *Understanding GPS/GNSS: principles and applications*. Artech house, 2017.

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

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

[4] I. Fernández-Hernández and G. Seco-Granados, "Galileo NMA signal unpredictability and anti-replay protection," in *Proc. International Conference on Localization and GNSS (ICL-GNSS)*. IEEE, 2016, pp. 1–5.

[5] C. O'Driscoll and I. Fernandez-Hernandez, "Mapping bit to symbol unpredictability in convolutionally encoded messages with checksums, with application to Galileo OSNMA," in *Proc. ION GNSS+*, 2020, pp. 3751–3765.

[6] G. Caparra, N. Laurenti, R. T. Ioannides, and M. Crisci, "Improving secure code estimate-replay attacks and their detection on GNSS signals," *Proc. of ESA Workshop on Satellite Navigation User Equipment Technologies (NAVITEC)*, vol. 2014, 2014.

[7] F. Gallardo and A. P. Yuste, "SCER spoofing attacks on the Galileo Open Service and machine learning techniques for end-user protection," *IEEE Access*, vol. 8, pp. 85 515–85 532, 2020.

[8] G. Seco-Granados, D. Gómez-Casco, J. A. López-Salcedo, and I. Fernandez-Hernandez, "Detection of replay attacks to GNSS based on partial correlations and authentication data unpredictability," *GPS Solutions*, vol. 25, no. 2, pp. 1–15, 2021.

[9] F. van Diggelen, *A-GPS, Assisted GPS, GNSS and SBAS*. Artech House, Boston, London, 2009.

[10] European Union, "European GNSS (Galileo) Open Service, signal-in-space interface control document," January 2021.

[11] C. O'Driscoll, J. Winkel, and I. Fernandez-Hernandez, "Assisted NMA proof of concept on Android smartphones," in *Proc. IEEE/ION Position Location and Navigation Symposium (PLANS)*, 2023.

[12] T. Fawcett, "An introduction to ROC analysis," *Pattern recognition letters*, vol. 27, no. 8, pp. 861–874, 2006.

[13] S. M. Kay, *Fundamentals of statistical signal processing: detection theory*, 1998, vol. II.