engineering proceedings

MDPI

Proceeding Paper

Feasibility of Snapshot OSNMA for Spoofing Detection in Urban Scenarios

Husnain Shahid, Sergi Locubiche-Serra*, Luca Canzian§, Carlo Sarto§, Oscar Pozzobon§, Ignacio Fernandez-Hernandez†, Joaquín Reyes-González‡, Gonzalo Seco-Granados*, José A. López-Salcedo***

*Universitat Autònoma de Barcelona (UAB), IEEC-CERES, Bellaterra, Spain
§Qascom SrL, Bassano del Grappa, Italy
†DG DEFIS, European Commission (EC), Brussels, Belgium
‡European Union Agency for the Space Programme (EUSPA), Prague, Czech Republic
* Correspondence: husnain.shahid@uab.cat

Abstract: Spoofing is becoming a critical concern in Global Navigation Satellite Systems (GNSS) as it severely threatens signal integrity and security. To combat it, Galileo E1-B signals implement the Open Service Navigation Message Authentication (OSNMA), a cryptographic protocol aimed at authenticating the navigation data by means of a set of authentication codes that are broadcast with some delay. The user's receiver can collect these codes and verify the authenticity of the associated navigation data, which requires processing several seconds of signal. This becomes difficult in urban environments with severe shadowing, but also in small battery-powered devices, where snapshot-mode operation is implemented for sporadic position fixes. In this context, the present paper takes advantage of the unpredictability of the OSNMA data and explores the feasibility of using snapshots of OSNMA data to reliably detect the presence of spoofers. 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. Simulation results for both open-sky and urban environments reveal that the problem is feasible under certain boundary conditions, as discussed herein.

Keywords: OSNMA, anti-spoofing, snapshot receivers.

Citation: Shahid, H.; Locubiche-Serra, S.; Canzian, L.; Sarto, C ; Pozzobon, O.; Fernandez-Hernandez, I.; Reyes-González, J.; Seco-Granados, G.; A. López-Salcedo, J. Feasibility of Snapshot OSNMA for Spoofing Detection in Urban Scenarios. *Eng. Proc.* **2023**, *1*, 0. https://doi.org/

Published:

1. 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. Thanks to the success in open-sky environments, GNSS is rapidly expanding to applications running in urban scenarios where working conditions are challenging [1]. In parallel, spoofing is becoming an increasing threat whereby an attacker intends to imitate authentic GNSS signals, and ultimately alter the user's navigation solution. This situation poses serious concerns to safety- and liability-critical applications, thus hindering the deployment of GNSS in key emerging sectors.

As a countermeasure, Galileo is providing the Open Service Navigation Message Authentication (OSNMA) service in its E1-B signal, a mechanism employing cryptographic data to verify the authenticity of the navigation message (I/NAV) [2]. Based on the Time Efficient Stream Loss Tolerant (TESLA) protocol, OSNMA authentication data is conveyed in a set of predictable and, most importantly, unpredictable symbols. Nonetheless, despite the unpredictability of some OSNMA data, advanced spoofers 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, which are then broadcast to the victim's receiver. Efforts addressing this problem and more general signal replay attacks can already be found in the literature [3–8]. They are mostly based on monitoring the correlation samples of the received signal, and thus they are not straightforward to implement in existing receivers

unless access to those samples is explicitly granted. For most GNSS receivers it is easier to work instead with the demodulated data symbols provided at their output. Furthermore, SCER attacks are actually very complicated to implement, and in reality, spoofers would have troubles in estimating the unpredictable symbols, thus incurring in a non-negligible probability of error. Such errors would manifest at the victim's receiver, thus becoming an indication of a potential spoofing attack.

The problem aggravates when moving to urban arena with abounding propagation impairments, such as fading and shadowing. In this paper we focus on the latter, whereby the presence of obstacles (*e.g.* buildings, trees) may introduce power attenuations in the received line-of-sight (LOS) signal that easily exceed 30 dB [9]. Although shadowing usually appears combined with periods of good satellite visibility, symbol detection is prone to suffer from severe errors during LOS blockage periods, thus eventually degrading the overall symbol error rate (SER). Consequently, shadowing appears as the main source of symbol errors, thus potentially interfering with the ability to dissociate whether a symbol error is due to a spoofer or to the environment. 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 feasibility of exploiting the OSNMA data unpredictability for implementing a symbol-level spoofing detector for snapshot receivers. To do so, the paper is structured as follows. Section 2 introduces the system architecture for implementing the so-called snapshot OSNMA technique. Section 3 presents the signal model and Section 4 the sources of symbol errors considered herein. The proposed detector is discussed in Section 5 while its feasibility is assessed in Section 6. Finally, conclusions are drawn in Section 7.

2. Snapshot OSNMA System Architecture

The high-level architecture of the snapshot OSNMA service considered in this work is shown in Figure 1. On the left hand side, the user gathers and processes snapshots of the received Galileo E1-B signal in order to estimate the user's position and time by means of assisted GNSS (AGNSS) and coarse-time navigation [10], 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 [11]. 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 determine for 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. Upon reception, the estimated user's position and time are employed by the server to access a trusted repository where unpredictable OSNMA symbols transmitted by Galileo satellites up to that moment are available. When the authentic symbols expected to be received at the user's position and time are retrieved from the trusted repository, they are compared with the symbols actually received by the user. If both coincide, nothing can be said except that the received symbols do coincide with the authentic ones. If too many errors are found (i.e more errors than those expected due to the working conditions), the received signal is declared to be spoofed at symbol level, and consequently, at signal level as well. The affected satellite should therefore be discarded by the user.

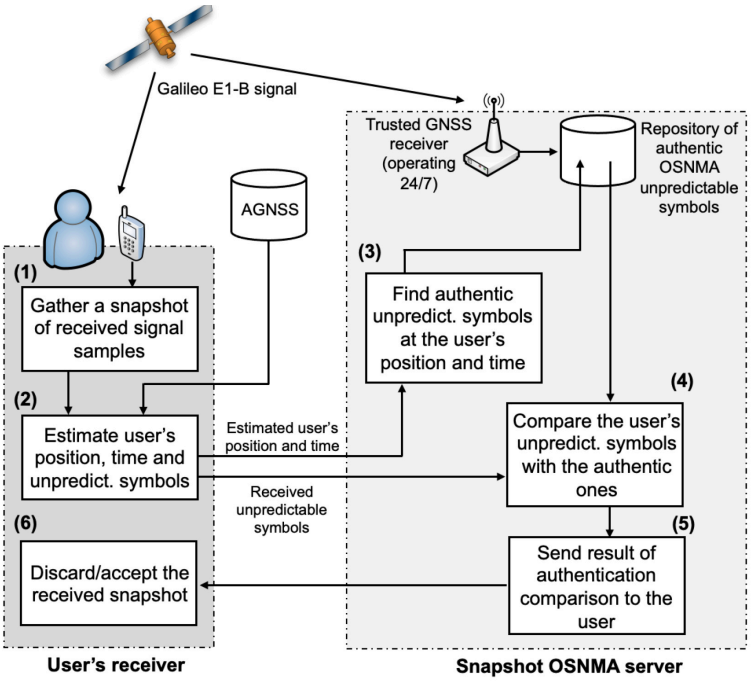

Figure 1. Architecture of the proposed snapshot OSNMA service.

3. Signal Model

3.1. Signal model at the spoofer's side

The OSNMA unpredictable symbols transmitted by a Galileo satellite at a time instant n are denoted herein as $s(n) \in \{\pm 1\}$. While predictable and unpredictable symbols are received altogether, we simplify our model by assuming that the server extracts unpredictable symbols from the symbol stream, as per [5]. If a spoofer was implementing a replay attack, it would struggle to estimate such unpredictable symbols and thus would incur in some probability of error p_s, namely the SER at the spoofer's side. Denoting the symbols transmitted by the spoofer as $\tilde{s}(n)$,

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

where $\bar{s}(n) \doteq -s(n)$ is the sign-reversed version of symbol $s(n)$. A spoofer trying to infer unpredictable symbols in a constrained scenario, potentially subject to propagation impairments, can be regarded as a Binary Symmetric Channel (BSC) where input symbols are sign-reversed at its output with probability p_s. For 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 is the time used by the attacker to estimate the symbol. This time is upper-bounded by the Galileo E1-B symbol period (4 ms), hence reducing T will increase p_s, 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 spoofer's end.

Two different 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,

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

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 symbol error, considering that a maximum of 40 unpredictable symbols are available every odd-page of the I/NAV message (i.e. every 2 seconds).

3.2. 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 also incur in errors due to the presence of thermal noise, propagation effects, etc. at the user's side. This can be modeled as another BSC in series with the one representing the spoofer's symbol decision, and 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 $(C/N_0)_{|\mathrm{a,s}}$ with $(C/N_0)_{|\mathrm{a,u}}$, 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 $(C/N_0)_{|\mathrm{a,s}}$ with $(C/N_0)_{|\mathrm{s,u}}$, which refers to the C/N_0 of the spoofed signal received by the user.

4. Symbol Errors due to Urban Propagation

The SER discussed so far was taking into account that thermal noise was the only source of degradation. While this may be the case in open-sky working conditions, it is not in urban scenarios due to the presence of obstacles that sporadically block the line of sight with the visible satellites, thus introducing severe drops in the received power levels. This situation poses serious concerns to the operation of the proposed spoofing detection method, because symbol errors are likely to appear at the user's side even if no spoofer is present at all. It is for this reason that a dedicated study is needed in order to assess the feasibility of the proposed spoofing detector in urban environments.

In this section we focus on the impact of shadowing effects onto the overall SER. To this end, we resort to the well-known Land Mobile Satellite (LMS) narrowband propagation channel, a statistical model that becomes a self-standing approach for synthesizing large-scale environmental features leading to shadowing events [12]. We will follow the approach in [9], where the signal transmission path is described in two separate states. On the one hand, a *good* state covering light shadowing conditions. On the other hand, a *bad* state covering heavy shadowing and blockage. For each state, fading properties are assumed to follow a stationary Loo distribution whose parameters depend on the environmental conditions such as user's motion, satellite elevation angle, and environment itself, thus leading to multiple possible combinations of such conditions.

We consider a synthetic Galileo E1-B signal with nominal LOS C/N_0 of 45 dB-Hz. Using Montecarlo realizations, we apply different LMS complex time series (*i.e.* in-phase and quadrature components) onto the signal, and repeat the process for the multiple

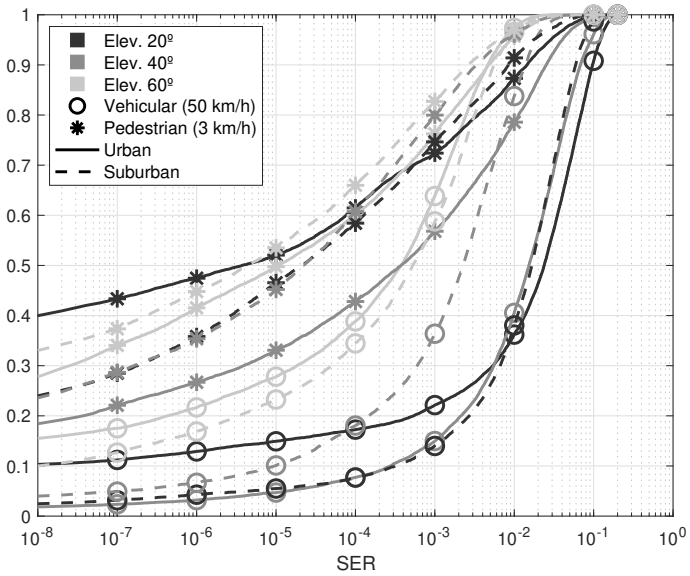

Figure 2. Cumulative distribution function (cdf) of SER in the presence of shadowing and blockage effects in urban and suburban environments at a nominal $C/N_0 = 45$ dBHz.

environmental combinations mentioned above. For user's motion, we consider speeds of 50 and 3 km/h, henceforth termed *vehicular* and *pedestrian* scenarios, respectively. For satellite elevation, the Galileo elevation statistics are considered to select meaningful values. By taking Brussels as a reference location in Center Europe, elevation is below 30º around 50% of the time, whereas 40% is found between 30º and 60º [13]. Therefore, we consider elevation angles of 20º, 40º and 60º. Last, for the environment, we consider *urban* and *suburban* scenarios as representative of strong and mild shadowing conditions, respectively.

Figure 2 depicts the cumulative distribution function (cdf) of the SER experienced in the different combinations above, resulting in a total of 12 plots. In order to draw meaningful conclusions, we focus on the SER values for which the cdf reaches the 0.9 barrier, thus providing some worst-case value that the SER can take. In that sense, for 20º elevation, the SER degrades to $\sim 10^{-1}$ for vehicular motion in both urban and suburban environments, as well as for the vehicular case for 40º elevation in urban. From this point, the SER improves to $\sim 10^{-2}$ for more benevolent scenarios. These include the pedestrian case in urban and suburban, as well as the suburban vehicular, all three referring to 40º elevation. Then, for 60º elevation scenarios, the SER falls between 10^{-3} and 10^{-2}.

The obtained results, particularly those for 20º and 40º satellite elevation angles, are comparable to the values of p_s considered herein, namely $p_s = \{0.1, 0.01\}$ in the optimistic and pessimistic cases, respectively. As a consequence, this is prone to increase the difficulties for a spoofing detector to dissociate whether a symbol error is due to a spoofing attack or it is caused by signal shadowing. Therefore, it is important to take into account the shadowing effect when designing the snapshot-based spoofing detector.

5. Proposed Symbol-Level Spoofer Detection

5.1. Proposed detector

The detector proposed herein has two distinctive features. First, it works on short snapshots of received signal, typically of tens or a few hundreds of ms length. Second, it works at symbol level using the binary OSNMA symbols estimated by the user's receiver for that snapshot. These symbols together with the estimated user's position and time, are sent to a remote server as shown in Fig. 1, where spoofing detection actually takes place. Note that a similar concept but fully implemented at the user's terminal is proposed in [14].

The proposed detector in the present work compares the received OSNMA unpredictable symbols with the expected ones for the user's position and time, available at a remote server. This comparison allows to determine how many of the received symbols

might be altered, which may unveil the presence of a potential spoofer. The comparison is done by computing the Hamming distance $d_{\text{Hamming}}(\hat{\mathbf{s}}_i, \mathbf{s}_i)$ between the received OSNMA unpredictable symbols, $\hat{\mathbf{s}}_i$, and the authentic (i.e. expected) ones, $\mathbf{s}_i$, where $_i$ stands for the i-th snapshot being processed, with $i = 0, \ldots, N-1$. Each snapshot is composed of L symbols and therefore the total number of OSNMA unpredictable symbols used for detection is $Q \doteq LN$. In this way the detector becomes,

$$H(\hat{\mathbf{s}}, \mathbf{s}) \doteq \sum_{i=0}^{N-1} d_{\text{Hamming}}(\hat{\mathbf{s}}_i, \mathbf{s}_i). \tag{7}$$

The above Hamming distance actually provides the number of errors in the received unpredictable symbols with respect to the authentic ones. By monitoring this metric one can determine whether the obtained number of errors is reasonable for a user that should be processing an authentic signal at given working conditions. In that case the SER should be close to $p_{u,0}$, which was shown in Section 3.2 to be the SER in the absence of spoofing.

5.2. 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 (7) can be found to be given by,

$$H(\hat{\mathbf{s}}, \mathbf{s}) \sim \begin{cases} B(Q, p_{u,0}) & : \mathcal{H}_0 \\ B(Q, p_{u,1}) & : \mathcal{H}_1 \end{cases} \tag{8}$$

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

An important remark is that the estimated BPSK symbols from a short snapshot of signal do not have an absolute phase reference and thus may be affected by a 180° phase ambiguity. This means that the estimated symbols 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 (8), thus leading to a mixed Binominal distribution under each of the two hypotheses,

$$H(\hat{\mathbf{s}}, \mathbf{s}) \sim \begin{cases} \frac{1}{2}B(Q, p_{u,0}) + \frac{1}{2}B(Q, 1-p_{u,0}) & : \mathcal{H}_0 \\ \frac{1}{2}B(Q, p_{u,1}) + \frac{1}{2}B(Q, 1-p_{u,1}) & : \mathcal{H}_1 \end{cases} \tag{9}$$

Due to the mixed or bimodal distribution under each hypotheses, two detection thresholds must be set. These are γ on the lower side of the bimodal Binomial distribution and $Q - \gamma$ on the upper side of the bimodal Binomial distribution.

Once the test in (9) is computed, the following decision rule can be implemented,

$$\begin{array}{rcl} H(\hat{\mathbf{s}}, \mathbf{s}) \leq \gamma & \Rightarrow & \text{decide } \mathcal{H}_0 \\ \gamma < H(\hat{\mathbf{s}}, \mathbf{s}) < Q - \gamma & \Rightarrow & \text{decide } \mathcal{H}_1 \\ H(\hat{\mathbf{s}}, \mathbf{s}) \geq Q - \gamma & \Rightarrow & \text{decide } \mathcal{H}_0 \end{array} \tag{10}$$

Note that the threshold γ is in practice determined as [15],

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

with $F^{-1}_{H(\hat{\mathbf{s}}, \mathbf{s}); \mathcal{H}_0}$ the inverse cdf under $\mathcal{H}_0$ and P_{FA} a target probability of false alarm.

For the feasibility study to be conducted herein, the focus will be placed on the receiver operating curve (ROC) and, more particularly, 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 detector performance into a single number and, as it occurs with the ROC curve, no specific threshold γ needs to be set, so that (11) is strictly not needed.

6. Simulation results

The goal of this section is to analyze whether the proposed detector in (10) is feasible or not. That is, whether it can provide meaningful and reliable information whenever a spoofer is present. This is a relevant question because, at first glance, errors due to noise, fading/shadowing, etc. are combined with errors due to spoofing. Thus, it may not be fully clear whether detecting a symbol error is synonym of a spoofer being present or not.

To study this problem, the performance of the proposed detector is analyzed through its AUC curve. Note that the ROC of a random (and thus useless) detector would be a straight line from coordinate $(P_{\mathrm{D}}, P_{\mathrm{FA}}) = (0,0)$ in the bottom left hand corner of the ROC, up to coordinate $(P_{\mathrm{D}}, P_{\mathrm{FA}}) = (1,1)$ in its upper right hand corner [16]. This means that AUC $= 0.5$ for a random detector, while for an ideal detector keeping $P_{\mathrm{D}} = 1$ when $P_{\mathrm{FA}} \to 0$, then AUC $\to 1$. In some special cases the ROC may appear below the straight line of a random detector, thus leading to AUC < 0.5 or even AUC $\to 0$. This happens when hypotheses $\mathcal{H}_0$ and $\mathcal{H}_1$ are reversed in the data being processed. For instance, when BPSK symbols are estimated in the presence of a 180° phase ambiguity, all symbols would incorrectly be estimated sign-reversed. This leads to a mirrored ROC curve to that of the ideal case resulting in AUC$\to 0$, suggesting some underlying structure in the data, which is being interpreted in the opposite way it should be. If the detector was aware, reversing its decisions (i.e. declaring $\mathcal{H}_0$ instead of $\mathcal{H}_1$ and viceversa) would solve the problem.

The experiment conducted herein simulates the unpredictable symbols synchronously 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 since the goal of the spoofer is to prevail over the authentic signal, and have the user's receiver to lock onto it. The AUC of the proposed detector is computed as a function of the snapshot length Q and $(C/N_0)_{\mathrm{a,u}}$. The results are shown in Figs. 3–5 where the plots on the left side assume a spoofer with SER $p_s = 0.1$ whereas the ones on the right side assume $p_s = 0.01$. Results in Fig. 3 assume open-sky conditions whereas Fig. 4 and Fig. 5 assume an LMS urban scenario with 60° and 40° elevation angles, respectively. The SER introduced by the LMS channel was obtained from Fig. 2 as the 90% value of the CDF, thus representing a worst-case assumption and leading to a SER of 10^{-1} and 10^{-2}, for 40° and 60° elevation angles, respectively.

As can be observed in Fig. 3–5, the resulting AUCs can all be divided into three different regions. On the one hand, the region where AUC$\to 0.5$, colored in green, which corresponds to Q and $(C/N_0)_{\mathrm{a,u}}$ values making the detector to behave randomly, thus being unable to distinguish the presence or absence of spoofing. This region is clearly visible in Fig. 4 and 5 ranging from $(C/N_0)_{\mathrm{a,u}} = 0$ to $\sim 20 - 25$ dBHz. Within this region, the proposed detector is not feasible at all.

On the other hand, we have the region where AUC$\to 1$, colored in yellow, clearly distinguished in Fig. 3 for the open-sky scenario and $(C/N_0)_{\mathrm{a,u}} > 25 - 30$ dBHz. Within this region, the detector can always detect the spoofer provided that the latter has a probability of error larger than zero. It is just a matter of time (i.e. having enough symbols) for the spoofer to be detected. It is noted that as the propagation conditions harden, a higher $(C/N_0)_{\mathrm{a,u}}$ is needed for the yellow region to appear. This can be observed when moving from the open-sky scenario in Fig. 3 to the LMS channel with 60° elevation angle in Fig. 4, and then 40° elevation angle in Fig. 5. In general, the detector will continue to be feasible in most urban environments just at the expense of requiring a higher nominal $(C/N_0)_{\mathrm{a,u}}$. It is only for the worst conditions, e.g. with 40° elevation and very sophisticated spoofers having a very low error probability , such as in the right side plot of Fig. 5, the detector becomes unfeasible under reasonable $(C/N_0)_{\mathrm{a,u}}$, being those smaller than 50 dBHz.

Finally, there is a third region in the AUCs shown in the figures below, corresponding to AUC$\to 0$, colored in dark blue. In this region, symbol errors due to noise, fading and

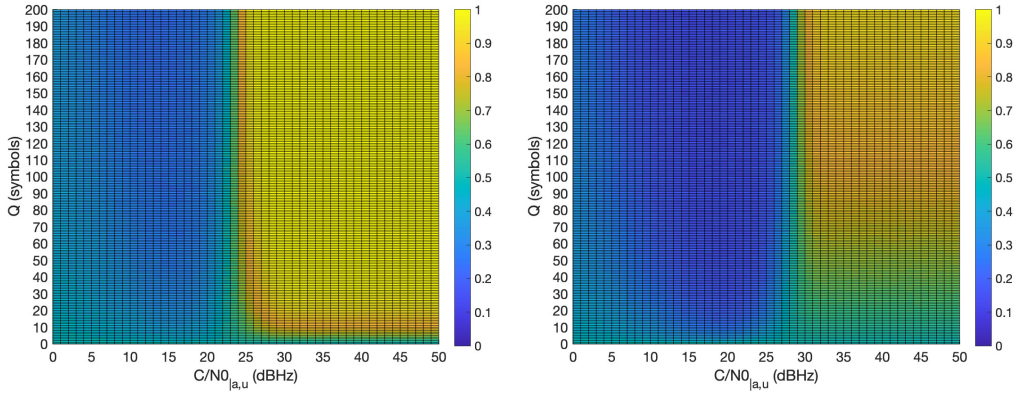

Figure 3. AUC for spoofer at 5dB power advantage in perfect LOS, $p_s = 0.1$ (left), $p_s = 0.01$ (right).

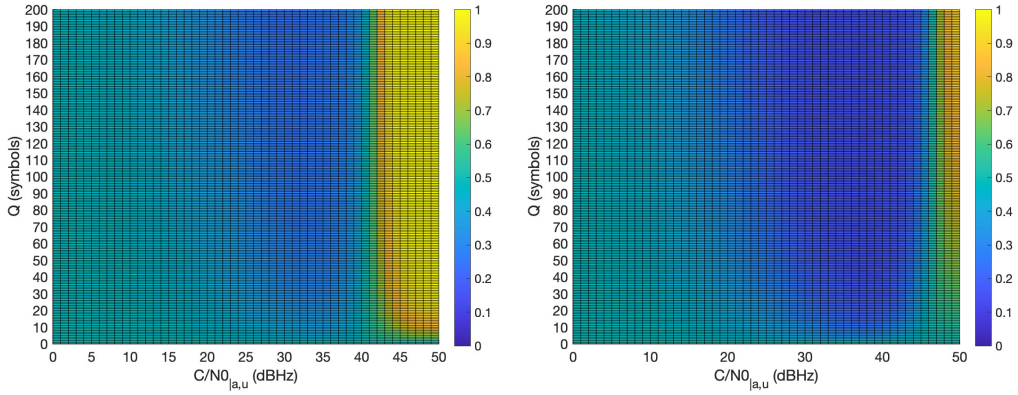

Figure 4. AUC for spoofer at 5dB power advantage in LMS, 60° elev., $p_s = 0.1$ (left), $p_s = 0.01$ (right).

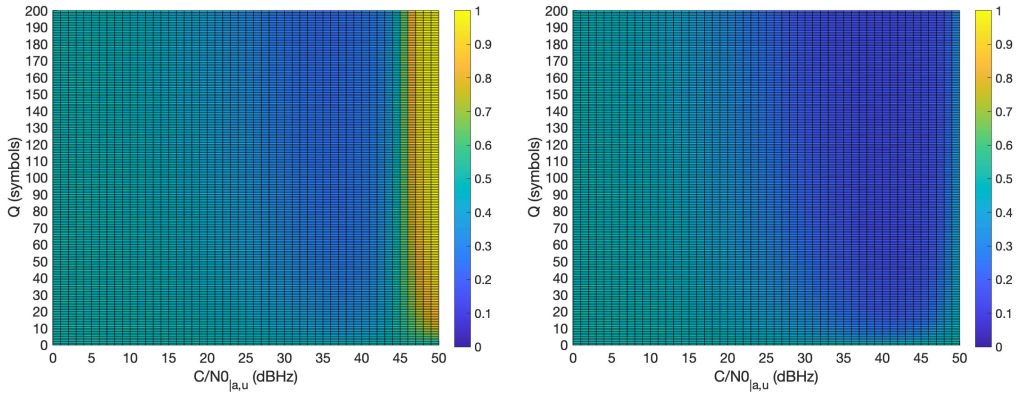

Figure 5.AUC for spoofer at 5dB power advantage in LMS, 40° elev., $p_s = 0.1$ (right), $p_s = 0.01$ (right).

shadowing effects are larger than those due to the spoofer, which remain at $p_s = 0.1$ and $p_s = 0.01$. 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, and $\mathcal{H}_1$ when the spoofed signal is absent, since far more errors are incurred when processing the noisy and degraded authentic signal than the spoofed one. This leads AUC $\rightarrow 0$ and in principle, this dark blue region should be avoided because the detector is not working properly. Actually, it declares the opposite hypothesis to the correct one. However, this problem could be circumvented if a priori information was available, for instance, the knowledge on the current $(C/N_0)_{\mathrm{a,u}}$.

7. Conclusion

This paper has presented the snapshot OSNMA technique for spoofing detection, based on comparing the received OSNMA unpredictable symbols with the authentic ones. Being a symbol-level detection, concerns are raised on whether this approach is feasible considering that symbol errors are already experienced due to noise and propagation conditions. Results show that the proposed detector is feasible and spoofers can reliably be detected under certain working conditions. The boundary condition for such operations are determined and limitations are highlighted, opening the door for further research.

8. Disclaimer

The content of this publication reflects only the authors' 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.

Author Contributions: Conceptualization, Qascom authors; methodology, software, validation, formal analysis, investigation, resources and data curation, UAB authors; writing—original draft preparation, H.S.; writing—review and editing, all authors; visualization, UAB authors; supervision, J.A.L.S.; project administration, C.S.; funding acquisition, Qascom authors. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by EUSPA under the GSA/GRANT/03/2019/02 contract, and in part by the Spanish Agency of Research (AEI) under the Research and Development projects PID2020-118984GB-I00/AEI/10.13039/501100011033 and PDC2021-121362-I00/AEI/10.13039/501100011033.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. European Union Agency for the Space Programme (EUSPA). GNSS Market Report, Issue 6 **2019**.
2. Fernandez-Hernandez, I.; Rijmen, V.; Seco-Granados, G.; Simón, J.; Rodríguez, I.; Calle, J.D. A navigation message authentication proposal for the Galileo Open Service. *Navigation* **2016**, *63*, 85–102.
3. Humphreys, T.E. Detection strategy for cryptographic GNSS anti-spoofing. *IEEE Trans. on Aerosp. and Electron. Syst.* **2013**, *49*, 1073–1090.
4. Fernandez-Hernandez, I.; Seco-Granados, G. Galileo NMA signal unpredictability and anti-replay protection. In Proceedings of the Proc. Intl. Conf. on Localization and GNSS (ICL-GNSS), 2016, pp. 1–5.
5. O'Driscoll, C.; Fernandez-Hernandez, I. Mapping bit to symbol unpredictability in convolutionally encoded messages with checksums, with application to Galileo OSNMA. In Proceedings of the Proc. ION GNSS+, 2020, pp. 3751–3765.
6. Caparra, G.; Laurenti, N.; Ioannides, R.T.; Crisci, M. Improving secure code estimate-replay attacks and their detection on GNSS signals. *Proc. of ESA Workshop on Satellite Navigation User Equipment Technologies (NAVITEC)* **2014**, *2014*.
7. Gallardo, F.; Yuste, A.P. SCER spoofing attacks on the Galileo Open Service and machine learning techniques for end-user protection. *IEEE Access* **2020**, *8*, 85515–85532.
8. Seco-Granados, G.; Gómez-Casco, D.; López-Salcedo, J.A.; Fernandez-Hernandez, I. Detection of replay attacks to GNSS based on partial correlations and authentication data unpredictability. *GPS Solutions* **2021**, *25*, 1–15.
9. Prieto-Cerdeira, R.; Perez-Fontán, F.; Burzigotti, P.; Bolea-Alamañac, A.; Sánchez-Lago, I. Versatile two-state land mobile satellite channel model with first application to DVB-SH analysis. *Intl. Journal of Satellite Commun. and Networking* **2010**, *28*, 291–315.
10. van Diggelen, F. *A-GPS, Assisted GPS, GNSS and SBAS*; Artech House, Boston, London, 2009.
11. European Union. European GNSS (Galileo) Open Service, signal-in-space interface control document, 2021.
12. Arndt, D.; Heyn, T.; König, J.; Ihlow, A.; Heuberger, A.; Prieto-Cerdeira, R.; Eberlein, E. Extended two-state narrowband LMS propagation model for S-Band. In Proceedings of the IEEE Intl. Symp. Broadband Multimedia Syst. and Broadcast., 2012, pp. 1–6.
13. Liang, K.; Chen, Q.; Han, K.; Yang, Z.; Zhang, A.; Ding, C. Time transfer via BDS and Galileo compared to time transfer via GPS. In Proceedings of the Proc. ION Annual Precise Time and Time Interval Syst. and Apps Meeting, 2019, pp. 131–136.
14. O'Driscoll, C.; Winkel, J.; Fernandez-Hernandez, I. Assisted NMA proof of concept on Android smartphones. In Proceedings of the Proc. IEEE/ION Position Location and Navigation Symposium (PLANS), 2023.
15. Kay, S.M. *Fundamentals of statistical signal processing: detection theory*; Vol. II, Prentice-Hall, 1998.
16. Fawcett, T. An introduction to ROC analysis. *Pattern recognition letters* **2006**, *27*, 861–874.