GPS Solutions (2026) 30:27
https://doi.org/10.1007/s10291-025-01968-9

RESEARCH

Boundary conditions for snapshot-based spoofing detection using OSNMA unpredictable symbols

Husnain Shahid[1] · Daniel Egea-Roca[1] · Luca Canzian[2] · Carlo Sarto[2] · Oscar Pozzobon[2] · J. Reyes-González[3] · Gonzalo Seco-Granados[1] · José A. López-Salcedo[1]

Received: 23 February 2024 / Accepted: 18 September 2025

Abstract

Anti-spoofing techniques for Global Navigation Satellite System (GNSS) receivers are garnering growing interest as crucial facilitators for the deployment of GNSS-based applications and services. To this end, Galileo is providing the Galileo Open Service Navigation Message Authentication (OSNMA), which conveys a set of cryptographic data with the purpose of authenticating the content of the Galileo I/NAV message. Some of these data are unpredictable to the users, and therefore cannot be known in advance and used to generate a counterfeit signal, thus introducing an additional protection level against potential spoofers. The purpose of this paper is to discuss the boundary conditions that make possible the use of such unpredictable symbols for spoofing detection. The proposed technique is referred to as *snapshot OSNMA* and it is envisaged as a client–server architecture whereby the user gathers a snapshot of the Galileo E1-B signal, extracts a few unpredictable symbols and sends them to a remote server where their authenticity is analyzed and reported back to the user. The problem is formulated using an equivalent binary symmetric channel (BSC), and results show that spoofing detection is possible provided that certain boundary conditions are fulfilled. The proposed technique thus becomes a valuable candidate for the exploitation of OSNMA in snapshot GNSS receivers where neither continuous processing of the GNSS signal nor OSNMA-enabled capabilities are implemented.

Keywords Galileo · GNSS · Spoofing · OSNMA · Snapshot receiver · Symbol unpredictability

Introduction

Services relying on Global Navigation Satellite Systems (GNSS) are widely present in many market segments ranging from consumer solutions, aviation, maritime, emergency response, agriculture and critical infrastructures, just to mention a few. Despite that GNSS is an essential part of such applications and services, the lack of authentication and the gradual increase of potential spoofing attacks pose a serious threat for its practical use. In response to these attacks, many countermeasures have been developed at all levels, from the user's level to the system level to detect and prevent such attacks. At the user level, these countermeasures include antenna level solutions (Montgomery et al 2009), power-based monitoring to detect anomalous signal strength (Shuli et al 2019), multipeak detection in the presence of spoofer (Wang et al 2013), signal quality monitoring by monitoring the shape of correlation (Sun et al 2018), and consistency checks across GNSS observables (Dingbo et al 2018) etc. At the system level, the recent inclusion of data authentication, namely the Galileo Open Service Navigation Message Authentication (OSNMA) is a remarkable achievement that hinders the implementation of spoofing attacks (Fernández-Hernández et al. 2016). Recent publications described novel sophisticated attack mechanisms that may circumvent the protection provided by the navigation message authentication. That is, by tracking the received signal from the Galileo satellites in view, estimating the unpredictable symbols and retransmitting a replica of the Galileo signal to the victim receiver in order to gradually take over the victim's tracking loops. All these steps would

✉ Husnain Shahid
hshahid@cttc.es; husnain.shahid@uab.cat

[1] IEEC-CERES, Universitat Autònoma de Barcelona (UAB), Barcelona, Spain

[2] Qascom Srl, Bassano del Grappa, Italy

[3] European Union Agency for the Space Programme (EUSPA), Prague, Czech Republic

Published online: 19 November 2025

be carried out by incurring into a negligible or ideally a zero delay, which makes this attack being referred as Security Code Estimation and Replay Attack (SCER) (Humphreys 2013).

In the execution of the attack and specifically, in the process of estimating the unpredictable symbols, the spoofer may incur in some errors at the beginning of unpredictable symbol duration. These errors may last until the spoofer estimate of the unpredictable symbols is reliable enough, and the correct value is determined. This introduces some uncertainty at the beginning of each unpredictable symbol, that can be detected at the user's side for inferring the presence of a potential spoofer. This observation was addressed in (Fernández-Hernández and Seco-Granados 2016) and then in more detail in (Seco-Granados et al. 2021), where five different detectors based on partial correlations of received signal were designed and analyzed to detect SCER attacks. Some other contributions have focused instead on the implementation itself of SCER attacks. For instance, the case in (Caparra et al. 2014), where different ways of determining the unpredictable symbols at the spoofer side were analyzed, in such a way that the spoofed signal could mimic as much as possible the authentic one. A similar problem was addressed in (Gallardo and Yuste 2020) where it was also studied the impact of the spoofed signal onto the user's acquisition search space. In particular, it was shown that the user would observe two GNSS-like signals in the time–frequency search space, and such features were analyzed using machine learning techniques.

One step further was done in (Marucco et al. 2020), where the idea of remote-based authentication was presented. It was based on a client/server approach whereby the client (i.e., the user) sends the received I/NAV pages time-tagged to a remote server, where the content of these pages and the consistency with the timestamp is verified. The problem with this approach is that continuous tracking of the Galileo E1-B signal is needed to retrieve the full set of I/NAV pages. Then, (O'Driscoll et al. 2023) proposed an "Assisted-NMA" concept whereby a smartphone synchronized with an external source can send the received bits including unpredictable ones. Such bits are checked in a server to ensure the signal is not a replay, at least beyond the synchronization level. Finally, (Zhang and Papadimitartos 2019) proposed a method for detecting the Distance-Decreasing (DD) attack on OSNMA signal, a replay attack where unpredictable bits are replayed in advance, before its starting time, to introduce a signal advance at the victim's receiver instead of a delay, as usual.

In this paper we also address a remote-server authentication approach but, contrary to existing contributions, we target snapshot-based applications where the user's position is computed on demand in order to reduce the power consumption. This means that only a small portion of the received signal is available, of just some tens of milliseconds in length. In these circumstances, the receiver cannot have access to the whole OSNMA data and thus cannot implement the full OSNMA functionalities. Furthermore, no pages of the I/NAV message can be retrieved because just a portion of a page is available on the snapshot of received signal. We propose a technique to overcome this limitation and still take advantage of OSNMA to infer the authenticity of the piece of received signal. This will be done by using just a portion of the Galileo I/NAV message, where OSNMA unpredictable symbols are transmitted. This is possible because the position where unpredictable symbols are transmitted onto the I/NAV navigation message is predictable, and thus the user's receiver could be scheduled to wake up at predefined time intervals. Thereby, the proposed technique is referred to as *snapshot* OSNMA. Once the receiver is triggered to wake up, it gathers a snapshot of Galileo E1-B signal, retrieves the unpredictable symbols, computes the position and time, and sends these time-tagged and geo-tagged estimated unpredictable symbols to the remote server. The server then takes these received unpredictable symbols and compares them with the authentic unpredictable symbols that corresponds to the same position and time. Since no OSNMA data is decoded at the user terminal, this approach circumvents the limitations related to the low availability of decoded I/NAV data at the user terminal, which has been reported to be typically less than 10% in most of the existing Android smartphones (O'Driscoll et al. 2023). Since, the proposed snapshot OSNMA spoofing detector strongly depends on the availability of received unpredictable symbols, which are subject to receiver wake up time, this paper also analyzes the impact of clock offset and provides a lower bound on the receiver wake up time. Numerical results are provided on the detection performance of the proposed technique as well as on the time needed for reliable spoofing detection. Results confirm the feasibility of the proposed technique and a faster detection time as compared to other existing techniques, thus supporting the interest of the proposed snapshot-based approach.

This paper is organized as follows; first of all, a short overview of the proposed spoofing detection technique is provided and three different implementations are presented, in order to highlight the differences of the proposed technique with respect to previous contributions in the literature. The next part provides a detailed analysis for determining the boundary conditions and limitations that may hinder the performance of the proposed technique. Then the actual performance of the proposed technique is assessed by incorporating results on the time to detect the spoofer, not addressed either in previous contributions. Finally, the last part of our work discusses some practical aspects that are

relevant from an implementation point of view, and conclusions then drawn.

Proposed snapshot OSNMA paradigm

OSNMA and unpredictable symbols

The Galileo OSNMA incorporates features intended to assist the user's receiver in the verification of the received message authenticity, and thus the mitigation of potential spoofing attacks that may alter the content of the I/NAV message. OSNMA follows an approach based on the Time Efficient Stream Loss Tolerant Authentication (TESLA) protocol, which relies on the transmission of a Message Authentication Code (MAC) to authenticate the message, and a delayed transmission of keys used to compute such MAC (Fernández-Hernández et al. 2016). The delay between the transmission of MAC and the key is made in such a way that the key is unknown to the user until the message and the MAC is received. Therefore, a potential spoofer cannot use the keys to generate the MAC in advance.

The OSNMA data is conveyed in the 40 bits of the "Reserved 1" field available in nominal odd pages of the I/NAV message transmitted on the Galileo E1-B signal component, as shown in Fig. 1(a). Each page, even and odd, has a duration of one second, so one full page spans for a total of two seconds. Then 15 full pages are grouped into one sub-frame, which lasts for 30 s, and 24 of these sub-frames are grouped into one frame, and lasts for 720 s. The OSNMA data are included in odd pages of the I/NAV message, which has a bit rate of 120 bit per second. Since the I/NAV bits are convolutionally encoded with coding rate of ½, this means that each bit is encoded into two symbols with a total of 240 symbols per page. Additionally, 10 synchronization symbols are added at the beginning of each page, which makes a total of 250 symbols per page, transmitted in one second. This means that the symbol period for Galileo E1-B is therefore 4 ms.

Once the bits have been encoded into symbols, the latter are interleaved by writing them column-wise in blocks of 8 symbols and reading them row-wise. This is indicated in Fig. 1(b), where one can see that the cells are filled using a sequential numbering per column, meaning that their content is written column-wise. However, the contents are read row-wise, and this is indicated by the sequential numbering appearing in red in the top of the symbol matrix. The row-wise symbols are what users actually receive, and thus what we actually have to work with. Unpredictable symbols are highlighted in green in Fig. 1(b) (O'Driscoll and Fernández-Hernández 2020). For illustrative purposes, Fig. 1(b) assumes that the 32 bits of the MAC and Key (MACK) section are all unpredictable, which is not the case for all pages. Yet, the principles of our work still hold in other cases.

Since symbols are received row-wise at the receiver, the receiver can collect between 7 and 9 consecutive unpredictable symbols per snapshot. This amount corresponds to the number of green cells in each row of Fig. 1(b) (O'Driscoll and Fernández-Hernández 2022). The analysis presented in this paper will provide answers on how to use such unpredictable symbols for spoofing detection.

Snapshot OSNMA system architecture

The high-level architecture of the snapshot OSNMA spoofing detector presented in this paper is shown in Fig. 2. Three different configurations are possible, composed of two constituent elements, namely the user side and the remote side.

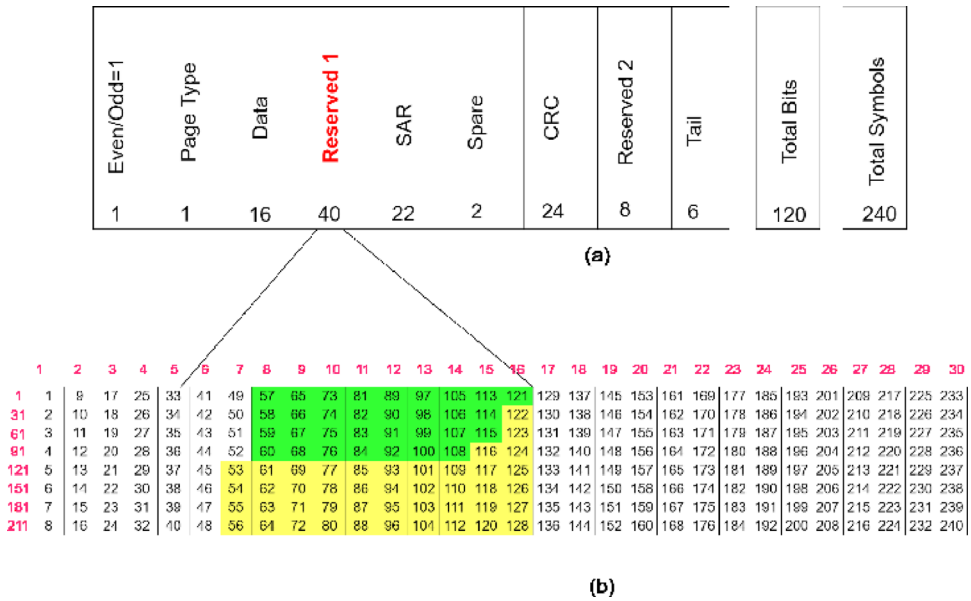

Fig. 1 (**a**) I/NAV nominal odd page for Galileo E1-B, where the "Reserved 1" field containing the OSNMA data is highlighted. (**b**) OSNMA unpredictable symbols position (see green cells) within the I/NAV nominal odd page already encoded and interleaved, that is, as received by the user (O'Driscoll and Fernández-Hernández 2020)

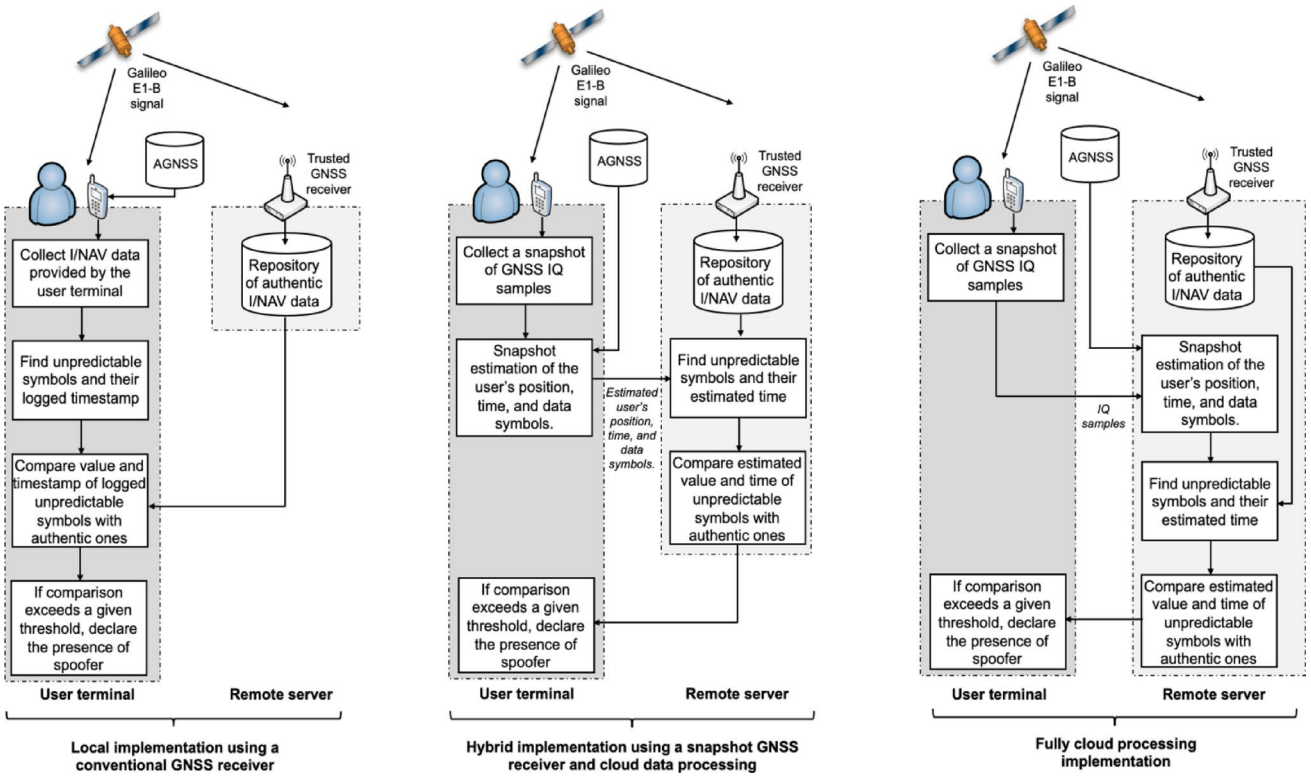

Fig. 2 High-level architecture of the proposed snapshot OSNMA spoofing detector

In the first configuration, all the processing is carried out locally at the user terminal while the remote server just provides the sequence of authentic symbols to be compared against, similarly to what is proposed in (O'Driscoll et al. 2023). The second configuration involves a hybrid implementation whereby the user terminal sends the geotagged and timestamped received symbols to the remote site. The latter is then in charge of comparing with the authentic symbols and deciding on the presence of spoofing. Finally, the third approach is a fully-cloud implementation where the user terminal just gathers the IQ samples of the received Galileo signals and sends these samples to the cloud where all the processing is carried out. This approach would be in line with the general framework of the so-called cloud GNSS signal processing already proposed in (Lucas-Sabola et al., 2018), which is targeting low-power GNSS-enabled IoT devices. The difference though, is that no OSNMA capabilities were considered in (Lucas-Sabola et al. 2018), but just the computation of the plain user's position and time. Our work instead, specifically focuses on using OSNMA capabilities in the cloud.

In this paper we will focus on the second approach, whereby the user is gathering snapshots of just a few tens or hundreds of ms of GNSS received signal in an on-demand basis. These snapshots are processed locally to obtain the user's position and time using coarse-time navigation, in order to circumvent the limitation that the transmission time broadcast by the satellites cannot be retrieved from a ms-length short piece of received signal (Van Diggelen 2009). This is the common approach in many mobile devices that due to computational and power consumption constraints, must resort to an on-demand use of GNSS, and switch off for the rest of the time until the next position fix is requested. It is assumed for the sake of simplicity that the user's receiver is scheduled to gather the snapshots of Galileo E1-B at the time instants where unpredictable OSNMA symbols are expected to be broadcast. This is possible because the transmission of unpredictable symbols is deterministic.

Once the user has obtained its position, time, and the demodulated symbols, these three items are sent to the remote snapshot OSNMA service. When they are received at the remote end, the estimated user's position and time are used to access a repository where the set of all unpredictable OSNMA symbols transmitted by the Galileo satellites up to that moment. This repository would be populated by a trusted Galileo receiver operating 24/7. When the authentic OSNMA symbols that were supposed to be received at the user's position and time are retrieved from the repository, the next step is to compare them with those received by the user, which actually contain both predictable and unpredictable symbols. If the user's received unpredictable symbols coincide with the authentic ones within a given time window, there is no guarantee that the underlying signal has not been spoofed, but at least at symbol level we can declare

that the user's unpredictable symbols are authentic. In contrast, if the user's received unpredictable symbols do contain too many errors with respect to the authentic unpredictable symbols, or the time at which these unpredictable symbols were received exceeds a given time window, then the received snapshot can be declared to be spoofed at symbol level, and consequently, at signal level as well.

Feasibility and boundary conditions of snapshot OSNMA

Before delving into the proposed technique, it is interesting to briefly discuss the feasibility of working at symbol level, and whether the detection of non-coincidences is reliable enough to be used as a spoofing detection metric. To do so, the signal model at spoofer and user side is formulated first.

Signal model at the spoofer's side

The symbols transmitted by a given Galileo satellite will be denoted by $s(n)$ for a given time instant n, with $s(n) \in \{\pm 1\}$. A spoofer willing to implement a SCER attack will try to first track the authentic GNSS signal to estimate the unpredictable symbols contained within $s(n)$, and immediately transmit a replica of such GNSS signal using the estimates. Such transmission should be immediate to minimize the delay incurred by the counterfeit signal, which could easily be detected otherwise as a jump in the observed receiver clock offset. So, the spoofer should minimize the time it takes to infer the value of the current symbol, even if it leads to a non-negligible probability of error p_s on its side. Then, it is these hasty symbol decisions what the proposed technique will actually take advantage of. With this in mind, let us denote the spoofer transmitted symbols by $\widetilde{s}(n)$ so that,

$$\widetilde{s}(n) = \begin{cases} s(n), with\, probability\ 1-p_s \\ \overline{s}(n), with\, probability\ p_s \end{cases} \tag{1}$$

where $\overline{s}(n) \doteq -s(n)$ is the sign-reversed version of symbol $s(n)$. The spoofer can be regarded as a binary symmetric channel (BSC) where input symbols are sign-reversed at its output with probability p_s. We will refer to p_s as the symbol error rate (SER) at the spoofer side and $(\frac{C}{N}_0)|_{a,s}$ as the carrier to noise ratio of the authentic signal when received at the spoofer's terminal.

Signal model at the user's side

The binary symbols provided by most GNSS receivers are the result of taking a hard decision on the output of the prompt correlator, once the receiver is locked to the received signal. These symbols can be expressed as,

$$\widehat{s}(n) = sign(r(n)) \tag{2}$$

where $r(n)$ are the received symbols affected by the thermal noise at the user's receiver. Despite being the optimal rule, taking the sign incurs a non-negligible probability of error due to the presence of noise, which makes it difficult to perfectly ascertain the mapping between the received symbols and the underlying true ones. In particular, the problem can be addressed through hypothesis testing with the following $\mathcal{H}_0$ and $\mathcal{H}_1$ hypotheses:

$$\mathcal{H}_0 : \widehat{s}(n) = \begin{cases} s(n), with\, probability\ 1-p_{u,0} \\ \overline{s}(n), with\, probability\ p_{u,0} \end{cases} \tag{3}$$

$$\mathcal{H}_1 : \widehat{s}(n) = \begin{cases} s(n), with\, probability\ 1-p_{u,1} \\ \overline{s}(n), with\, probability\ p_{u,1} \end{cases} \tag{4}$$

where $p_{u,0}$ is the SER at the user's terminal when no spoofer is present. This is the probability of error when receiving the authentic symbols in additive white gaussian noise (AWGN) at the user's terminal. That is,

$$p_{u,0} = \frac{1}{2}\mathrm{erfc}\left(\sqrt{T_d\left(\frac{C}{N}_0\right)_{|a,u}}\right) \tag{5}$$

where erfc is the error complementary function and $\left(\frac{C}{N}_0\right)_{|a,u}$ is the $\frac{C}{N}_0$ of the authentic signal received at the user's receiver and T_d is symbol period. For the alternate hypothesis $\mathcal{H}_1$ in (4), $p_{u,1}$ is the SER at the user's terminal when the spoofer is present, which is affected by the noise at the user's terminal but also by the error probability incurred by the spoofer. In this case we have the concatenation of two BSC, since errors can occur due to the spoofer or to the user's terminal. Hence, the end-to-end SER at the user's side when the spoofer is present is given by,

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

where p_s is the SER incurred by the spoofer already introduced in (1) and $p_{s,u}$ is the SER of the spoofed symbols when received at the user's terminal, which is given by,

$$p_{s,u} = \frac{1}{2}\mathrm{erfc}(\sqrt{T_d\left(\frac{C}{N}_0\right)_{|s,u}}) \tag{7}$$

with $\left(\frac{C}{N}_0\right)_{|s,u}$ is the $\frac{C}{N}_0$ of the spoofed signal received at the user's receiver. Finally, since there are a total of L symbols in each snapshot, we can stack the hard decided symbols into vector form leading to,

$$\widehat{\boldsymbol{s}}_i = sign\left(r_i\right) = \left[sign\left(r_i\left(0\right)\right), \ldots, sign\left(r_i\left(L-1\right)\right)\right]^T \quad (8)$$

with i the indexation of the snapshot being processed. After formulating the signal model, the feasibility and boundary conditions of snapshot OSNMA are discussed next.

Unpredictable symbol errors induced by spoofer

For many spoofers, particularly those with limited resources, determining the unpredictable OSNMA symbols when implementing a SCER attack is a difficult task. However, randomly guessing the symbols and transmitting them toward the victim's receiver is simple and cost efficient. The SER of such spoofer randomly guessing each unpredictable symbol would be $p_s = \frac{1}{2}$.

Unlike simple spoofers, sophisticated spoofers try to accumulate the authentic signal for a very short period of time in order to collect enough energy to ascertain what the actual value of the current unpredictable symbol is (Fernández-Hernández and Seco-Granados 2016) and (Seco-Granados et al. 2021). Following the same approach as in (Seco-Granados et al. 2021), we will consider two representative spoofing scenarios. The optimistic case considers a SER at the spoofer side of $p_s = 0.1$, which corresponds to the integration of the authentic signal at $(\frac{C}{N_0})|_s = 45$ dB-Hz for just 26μ s. The pessimistic case considers a SER at the spoofer side of $p_s = 0.01$, which corresponds to the integration of the authentic signal at $(\frac{C}{N_0})|_s = 40$ dB-Hz for 271μ s.

To further study this case, we evaluate the probability of having at least one error incurred by the spoofer as a function of the number of unpredictable symbols being guessed.

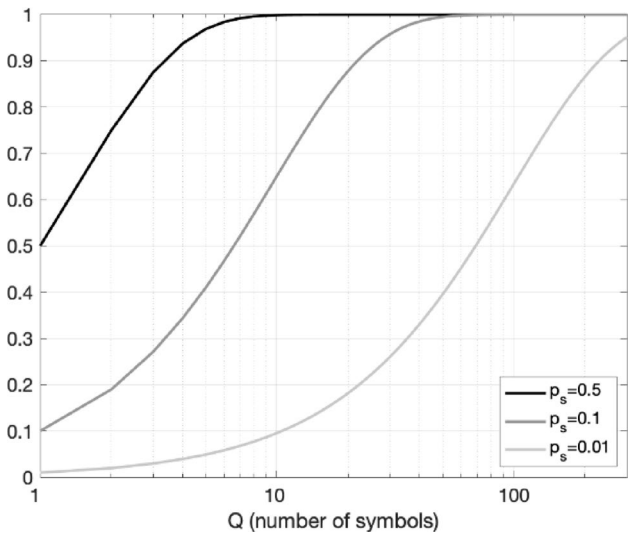

Fig. 3 Probability of having at least one error in a set of Q unpredictable symbols estimated by the spoofer with probability of error p_s

This will provide us with information on how easy it is to have an error (one or more) in a given length of spoofed signal, as observed in Fig. 3. For $p_s = 0.1$, $Q > 22$ symbols are needed to make sure (i.e., $> 90\%$) that at least one of the symbols would be in error due to the spoofer. While the more sophisticated spoofers with $p_s = 0.01$ are much more difficult to detect. This is because $Q > 230$ symbols are needed to make sure (i.e., $> 90\%$) that at least one error is present thus incurring in a latency for spoofing detection of several tens or even hundreds of seconds.

Symbol errors due to user's receiver noise

If the received unpredictable symbols are free from spoofer errors, the user may incur in some errors when trying to infer the actual value of these symbols. This would pose a serious trouble to distinguish between authentic and spoofed symbols. Fortunately, this is not the case as far as thermal noise is considered. The SER purely due to the thermal noise at the user's receiver is actually given by $p_{u,0}$ in (5), and even for a relatively low C/N_0 such as 35 dB-Hz, it results in $p_{u,0} \approx 10^{-7}$. This is several orders of magnitude below the SER caused by spoofer errors and therefore the impact of thermal noise can often be ignored.

Symbol errors due to the overlap of authentic and spoofed signals at the user's receiver

Since both the authentic and the spoofed signals are simultaneously received at the user's terminal, and thus, the overlapped aggregate signal is what the receiver actually processes. We assume that the spoofer managed to align its code replica in both time and frequency to that of the authentic signal. Nevertheless, it is very difficult or even impossible for a spoofer to align its carrier phase offset with that of the authentic signal. Such relative phase offset has a direct impact onto the energy of the aggregated received signal since both individual signals might be added constructively (i.e. having a 0º relative phase offset) or destructively (i.e. having a 180º relative phase offset). The formulation of SER in this case can be found in Appendix. As can be seen Fig. 4, the largest SER due to the phase misalignment, is experienced when both signals have similar power levels and thus signal to spoofer ratio (SSR) is 0 dB. When they overlap destructively, the resulting signal vanishes and thus it is not possible to reliably retrieve the symbols anymore, thus leading to SER$= 0.5$, and clearly unveiling the presence of a spoofer.

The region of SSR values to be avoided by spoofer is indicated by the dashed lines in Fig. 4, since they incur in an

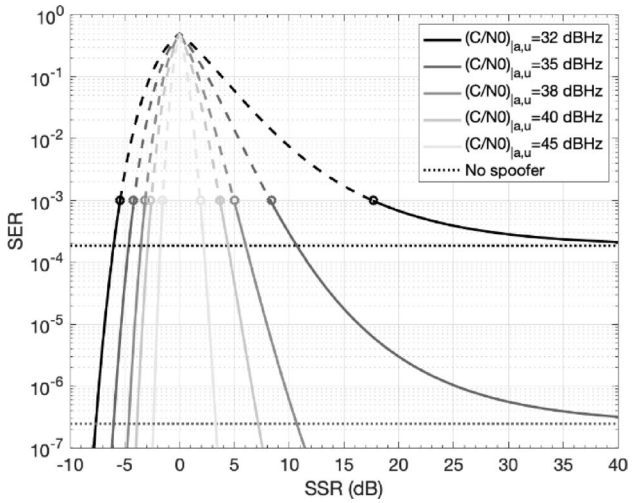

Fig. 4 SER due to the destructive overlapping of the authentic and spoofed signals at the user's receiver as a function of the signal to spoofer ratio (SSR). Dashed lines represent the values of SSR that lead to an excessive SER (i.e.>1E-3), and thus are likely to be avoided by a potential spoofer in order to remain unnoticed

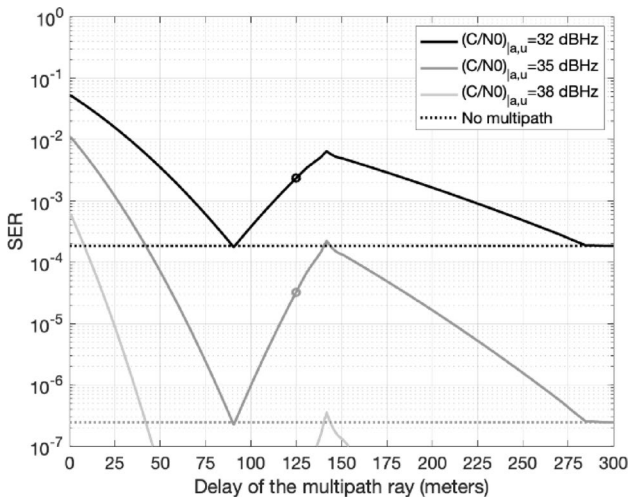

Fig. 5 Worst SER for different $\frac{C}{N_0}$ values of the authentic signal at the user's receiver when a single-ray reflection is present, using SMR=4.5 dB as specified in (ETSI 2020, Appendix A3.3)

easily detectable SER. For instance, $-5 < \text{SSR} < 5$ dB at $\left(\frac{C}{N_0}\right)_{|a,u} = 40$ dB-Hz.

Symbol errors due to multipath

In order to assess the impact of multipath at symbol level, we consider a simple one-ray multipath model following the same approach as in the performance requirements specification in (ETSI 2020, Appendix A3.3).

The SER in the presence of multipath can be computed using the expression in (5) by replacing the nominal energy per symbol, $E_s = T_d C$, with its multipath-affected

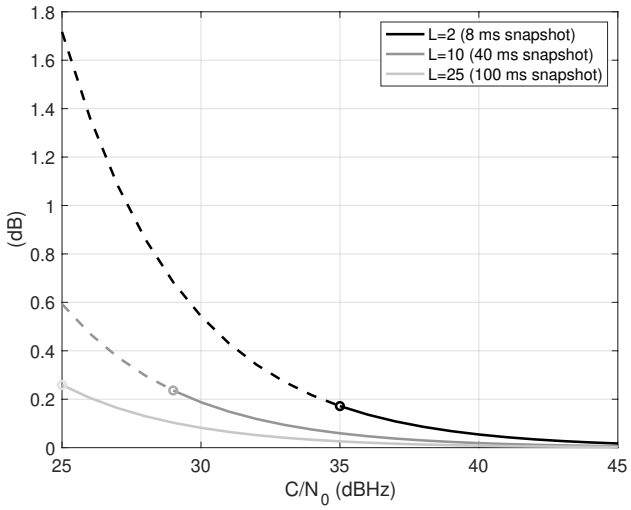

Fig. 6 SER degradation, defined as a loss in $\frac{C}{N_0}$ measured in dB, due to residual carrier phase estimation errors at the user's receiver

counterpart. Two cases are considered, namely when the multipath replica adds constructively or destructively to the line of sight (LOS). The maximum peak of the aggregated correlation function is determined for both cases, and the energy of this peak is retained to compute the effective energy per symbol perceived by the receiver, thus providing the so-called "worst SER".

The results in Fig. 5 have been obtained for a signal to multipath ratio (SMR) of 4.5 dB as specified in (ETSI 2020). For Galileo E1, a relative delay of 125 m is considered as well in (ETSI 2020) for the reflected ray. The value corresponds to the 'o' markers shows a worst SER. Note that despite the very low $\frac{C}{N_0}$ value, multipath is not likely to cause a serious concern for symbol-level spoofing detection.

Symbol errors due to synchronization errors at the user's receiver

Unlike conventional receivers, snapshot receivers operate in acquisition mode only, and thus there is no tracking stage. As a result, residual errors due to the inaccurate estimation of the code and carrier errors parameters may contribute to the symbol error rate degradation. This effect is further aggravated when the user's receiver can only afford to gather a very short snapshot of just a few ms of signal.

The degradation due to phase estimation errors is shown in Fig. 6 as a function of the working $\frac{C}{N_0}$ when processing a snapshot of $L = \{2,10,25\}$ symbols, corresponding to a Galileo E1-B snapshot duration of $\{8,40,100\}$ ms, respectively. The worst losses are of about 0.2 dB, which are only experienced when working at the minimum detectable $\frac{C}{N_0}$ that is needed to detect a satellite with a probability

Table 1 Time delay estimation jitter in a snapshot receiver processing a snapshot of L Galileo E1-B symbols, operating at the minimum detectable C/N_0

Snapshot length	Minimum detectable C/N0 [Pd = 0.9, Pfa = 1E-6]	Time delay estimation jitter at the minimum detectable C/N_0	SER degradation at the minimum detectable C/N_0
(symbols)	(dB-Hz)	(chips)	(dB)
2	34	0.04	0.02
10	29	0.04	0.02
25	26	0.04	0.02

of detection $P_D = 0.9$ and probability of global false alarm $P_{FA} = 10^{-6}$ which is about $\{34,29,26\}\,dB$ for $L = \{2,10,25\}$ symbols, respectively. This is well-above this minimum detectable $\frac{C}{N}_0$ at which user`s receiver typically operate, for instance under the standard values of 40 to 45 dB-Hz experienced outdoors.

Meanwhile, the degradation due to time delay estimation errors $L = \{2,10,25\}$ symbols is 0.02 dB, shown in Table 1. This shows that the impact of time delay estimation errors onto the SER can reasonably be ignored in practice, even when very short snapshots are processed. The degradation relations for both time and carrier phase errors are derived and provided in the Appendix.

Symbol errors due to signal fading

Last but not least, the SER degradation due to the presence of fading and blocking obstacles in urban and suburban scenarios also play a significant role for SER degradation. This effect was thoroughly analyzed by the authors in (Shahid et al. 2023a). The results showed that the SER due to signal fading can rise up to 10^{-1} in vehicular urban scenarios, thus being comparable to a spoofer probability of error. This indicates that fading must be taken into account in the design of the spoofing detector in order to minimize the amount of potential false alarms.

Detection of spoofed unpredictable symbols

This section formulates the proposed symbol-level spoofing detector with two distinctive features. The first one is that it works on a short snapshot of received signal, typically of a few tens or hundreds of ms length. The second feature is that it works at symbol level using the demodulated symbols obtained at the prompt correlator or maximum peak of the correlation function at the user's receiver. Note that no decoding is needed but only to take the sign of the maximum peak of the correlation, as indicated in (2), which is actually the optimal decision rule for deciding equiprobably binary ± 1 symbols in additive white Gaussian noise (Proakis and Salehi 2002).

Proposed detector

Each snapshot of received signal is assumed to provide a set of L unpredictable symbols that are stacked into vector $\widehat{\boldsymbol{s}}_i$ as in (8), for $i = 0,1,\ldots.N-1$ and $Q = LN$ is the total number of snapshots. This implicitly assumes that the snapshot is perfectly synchronized with the time at which unpredictable symbols are received.[1] Based on the set of received symbols, the problem is now how to compare them with the authentic ones in order to determine the presence of a potential spoofer. This can be done by computing the Hamming distance H between $\widehat{\boldsymbol{s}}_i$ and $\boldsymbol{s}_i$, referred herein as $d_H\left(\widehat{\boldsymbol{s}}_i, \boldsymbol{s}_i\right)$, for each received snapshot. In this way the detector becomes,

$$H\left(\widehat{\boldsymbol{s}}, \boldsymbol{s}\right) = \sum_{i=0}^{N-1} d_H\left(\widehat{\boldsymbol{s}}_i, \boldsymbol{s}_i\right) \tag{9}$$

The Hamming distance returns the number of non-coincident elements between the received unpredictable symbols and the authentic ones. By monitoring this metric one can make sure whether the obtained number of errors is 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.

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 (9) is given by,

$$H\left(\widehat{\boldsymbol{s}}, \boldsymbol{s}\right) = \begin{cases} B\left(Q, p_{u,0}\right) : \mathcal{H}_0 \\ B\left(Q, p_{u,1}\right) : \mathcal{H}_1 \end{cases} \tag{10}$$

[1] While this may seem a rather strong assumption, it serves well herein for the purpose of illustrating the feasibility of working with unpredictable symbols. The more general case where both predictable and unpredictable symbols are present can be found in (Shahid et al. 2023b).

where $B(m,p)$ stands for the Binomial distribution for a set of m symbols, Q is the total number of unpredictable symbols, $p_{u,0}$ is the probability of symbol error at the user's side under $\mathcal{H}_0$, i.e., (5) when noise is the dominant degradation, and finally $p_{u,1}$ is the probability of symbol error at the user's side under $\mathcal{H}_1$, which is given by (6). Note that the latter depends on both, errors incurred by the spoofer and errors incurred by the user's receiver itself.

Nevertheless, it must be taken into account that the demodulated symbols from a short snapshot of signal do not have an absolute phase reference and thus can be affected by a phase rotation of 180º. This means that the symbols obtained in (2) and stacked in $\widehat{\boldsymbol{s}}_i$ can either be the correct symbols or the sign-reversed ones. This makes (10) to become a mixed Binominal distribution under each of the two hypotheses,

$$H(\widehat{\boldsymbol{s}},\boldsymbol{s}) \sim \begin{cases} \frac{1}{2}B(Q,p_{u,0}) + \frac{1}{2}B(Q,1-p_{u,0}) : \mathcal{H}_0 \\ \frac{1}{2}B(Q,p_{u,1}) + \frac{1}{2}B(Q,1-p_{u,1}) : \mathcal{H}_1 \end{cases} \tag{11}$$

Due to the mixed or bimodal distribution under each hypothesis, two different detection thresholds need to be implemented. The one on the lower side of the bimodal Binomial distribution will be referred to γ, while the one on the upper side of the bimodal Binomial distribution becomes its complementary, namely $Q-\gamma$.

Once the test statistic in (11) is computed using the symbols in $\widehat{\mathbf{s}}$, the following decision rule can be implemented,

$$H(\widehat{\boldsymbol{s}},\boldsymbol{s}) \leq \gamma \Rightarrow \text{ decide } \mathcal{H}_0 \tag{12}$$

$$\gamma < H(\widehat{\boldsymbol{s}},\boldsymbol{s}) < Q-\gamma \Rightarrow \text{ decide } \mathcal{H}_1 \tag{13}$$

$$H(\widehat{\boldsymbol{s}},\boldsymbol{s}) > Q-\gamma \Rightarrow \text{ decide } \mathcal{H}_0 \tag{14}$$

Threshold settings

The decision of threshold implementation allows to provide insights about the number of errors that can be acceptable in detection process corresponding to the boundary conditions under $\mathcal{H}_0$.

Statistically, the threshold can be obtained from the cumulative distribution function of the detector statistics under $\mathcal{H}_0$ and the target P_{FA} such that,

$$\gamma = \text{cdf}^{-1}_{H(\widehat{\boldsymbol{s}},\boldsymbol{s})}(1-P_{FA}\,|\mathcal{H}_0) = \text{cdf}^{-1}_{B(Q,p_{u,0})}(1-P_{FA}\,|\mathcal{H}_0) \tag{15}$$

where the result on the right hand side of (15) comes from the fact that $H(\widehat{\boldsymbol{s}},\boldsymbol{s})$ in (11) is a bimodal symmetric distribution. The threshold obtained in (15) is found to depend on Q, the number of unpredictable symbols, P_{FA}, the target probability of false alarm, and $p_{u,0}$, the probability of symbol error incurred in the absence of spoofer. Table 2 provides an overview of the representative values that $p_{u,0}$ can take, depending on the different impairments discussed so far, and what their impact is in terms of the detection threshold. An example is shown for $Q=\{32,230\}$ unpredictable symbols and $P_{FA}=\{10^{-4},10^{-6}\}$.

Performance evaluation

Two types of experiments have been carried out herein for preliminary assessment of the proposed detector. The first one is aimed at determining the feasibility of the proposed detector using the Receiver Operating Characteristic (ROC) curve will be considered (Fawcett 2006). Rather than the ROC curve, the analysis will focus on the so-called Area Under the Curve (AUC), as explained next when describing the first experiment. The second experiment is aimed at determining the time that is required to detect a potential spoofer in a snapshot mode to show how feasible detecting a spoofer is from a time domain perspective.

Experiment 1: Area Under the Curve (AUC). The detection performance is assessed here through the AUC, which computes the integral of the ROC curve and thus summarizes into a single number the performance represented in the ROC curve. A key feature of the AUC is that for a detector randomly declaring either $\mathcal{H}_0$ or $\mathcal{H}_1$, the ROC

Table 2 Summary with the contribution of the different impairments affecting the probability of symbol error in the absence of spoofer, $p_{u,0}$, and required detection threshold for $Q=32$ and $Q=230$ unpredictable symbols

dB	Noise	Multipath	Shadowing	Total	Threshold γ(Q = 32)		Threshold γ(Q = 230)	
	$p_{u,0}$	$p_{u,0}$	$p_{u,0}$	$p_{u,0}$	$P_{FA}=10^{-4}$	$P_{FA}=10^{-6}$	$P_{FA}=10^{-4}$	$P_{FA}=10^{-6}$
Open-sky, good $(C/N_0)_{\|a,u}$ (>40 dB-Hz)	$<10^{-18}$ <	0	0	$<10^{-18}$ <	0	0	0	0
Open-sky, moderate $(C/N_0)_{\|a,u}$ (32 dB-Hz)	$2\cdot10^{-4}$	0	0	$2\cdot10^{-4}$	1	2	2	3
One-ray multipath, moderate $(C/N_0)_{\|a,u}$ (32 dB-Hz, SMR = 4.5 dB)	$2\cdot10^{-4}$	$3\cdot10^{-3}$	0	$3\cdot10^{-3}$	3	4	5	7
LMS shadowing, good $(C/N_0)_{\|a,u}$ (45 dB-Hz, urban pedestrian, 95%)	~0	$\sim10^{-2}$		10^{-2}	4	5	10	12
LMS shadowing, good $(C/N_0)_{\|a,u}$ (45 dB-Hz, urban vehicular, 95%)	~0	$\sim10^{-1}$		10^{-1}	11	13	41	47

curve would be a straight line ranging from coordinate $(P_D, P_{FA}) = (0,0)$ to coordinate $(P_D, P_{FA}) = (1,1)$. This means that the AUC would be 0.5 for a random detector. In contrast, for an ideal detector keeping $P_D = 1$ when $P_{FA} \to 0$ the AUC would be equal to 1. So, the AUC values range from 0.5 (worst case) to 1 (best case). 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 situation typically occurs when hypotheses $\mathcal{H}_0$ and $\mathcal{H}_1$ are reversed in the data being processed. Figure 7 shows the AUC in an open-sky scenario as a function of the received $\frac{C}{N}_0$ of the authentic signal, when the spoofer arrives with a 3 dB power advantage over authentic signal and with a random relative phase shift. The plot on the Fig. 7(a) shows the AUC when the spoofer incurs in a probability of symbol error $p_s = 0.1$. In that case, the AUC rapidly raising in the Y-axis when more than 10 symbols are available and the $\frac{C}{N}_0$ is large enough. For spoofer errors to be distinguishable from the receiver own errors, we need $p_{u,0} < p_s$, which starts to happen for $\frac{C}{N}_0 > 25$ dB-Hz, when the detector rapidly scores AUC $\to 1$. In the plot of Fig. 7(b) the same experiment is shown but with a more sophisticated spoofer with $p_s = 0.01$. In that case, more than 200 unpredictable symbols are needed for AUC $\to 1$, in line with the discussion in Fig. 3. Furthermore, the $\frac{C}{N}_0$ working point has now been shifted to the right to account for the fact that $p_{u,0} < p_s$, but that a stricter p_s is now involved. Now, at least $\frac{C}{N}_0 > 30$ dB-Hz is needed to reliably detect the presence of spoofer. While the results in Fig. 7 confirm the feasibility of the proposed detector for open-sky working conditions, similar conclusions are drawn for the stringent LMS channel. In that case, the received $\frac{C}{N}_0$ of the authentic signal is required to be greater than 40 or even 45 dB-Hz for the detector to succeed, even when the spoofer arrives with a power advantage of 5 dB, larger than the 3 dB considered herein. Interested readers can find more details in Shahid et al. (2023a).

Experiment 2: Time to spoofing detection (TTSD). The second experiment intends to assess the time required to reliably detect a spoofer. The results are shown in Fig. 8(a) for $p_s = 0.1$, and Fig. 8(b) for $p_s = 0.01$. According to Fig. 1 (b), $L = 8$ is considered and a moderate $\frac{C}{N}_0$ of 38 dB-Hz is chosen here since it provides interesting insights about the difference in detection performance when either the spoofer or the user has a power advantage relative to this reference $\frac{C}{N}_0$.

For the considered working conditions, the time for detecting 90 % of the time a spoofer incurring in errors with $p_s = 0.1$ is less than 0.5 s, while for a spoofer with $p_s = 0.01$ it requires more than 12 s, as shown in Fig. 8. Such a significant increase is mostly due to the fact that unpredictable symbols are transmitted every 2 s, so if the current symbols are not enough, the receiver must wait 2 s for the next group of unpredictable symbols to be received.

Additionally, Table 3 provides a more detailed overview of the detection time for two practical use cases, namely when the receiver is operating in either low or high duty-cycle. The low duty-cycle refers to the case when the receiver only gathers one out of the four batches of unpredictable symbols that are available per odd page, which are shown in green in Fig. 1. In this case, the receiver will require a higher detection time to compensate for the scarcity of gathered

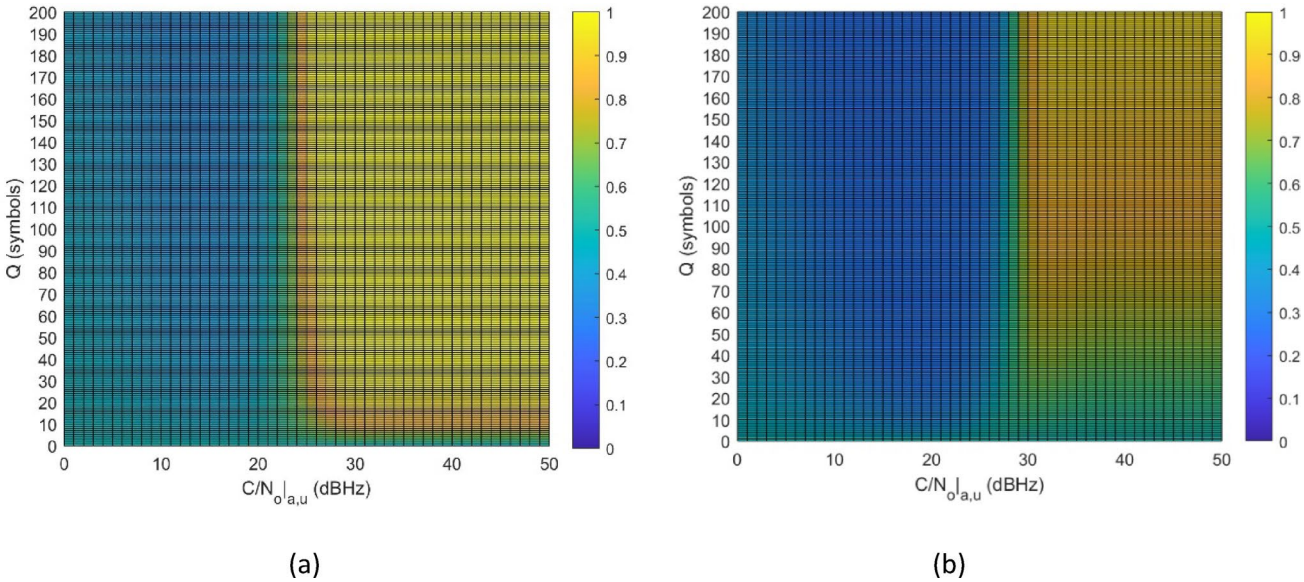

Fig. 7 Area under the ROC curve (AUC) for the proposed spoofing detector in open-sky conditions when the spoofer has a 3 dB power advantage and the probability of error **(a)** $p_s = 0.1$, **(b)** $p_s = 0.01$

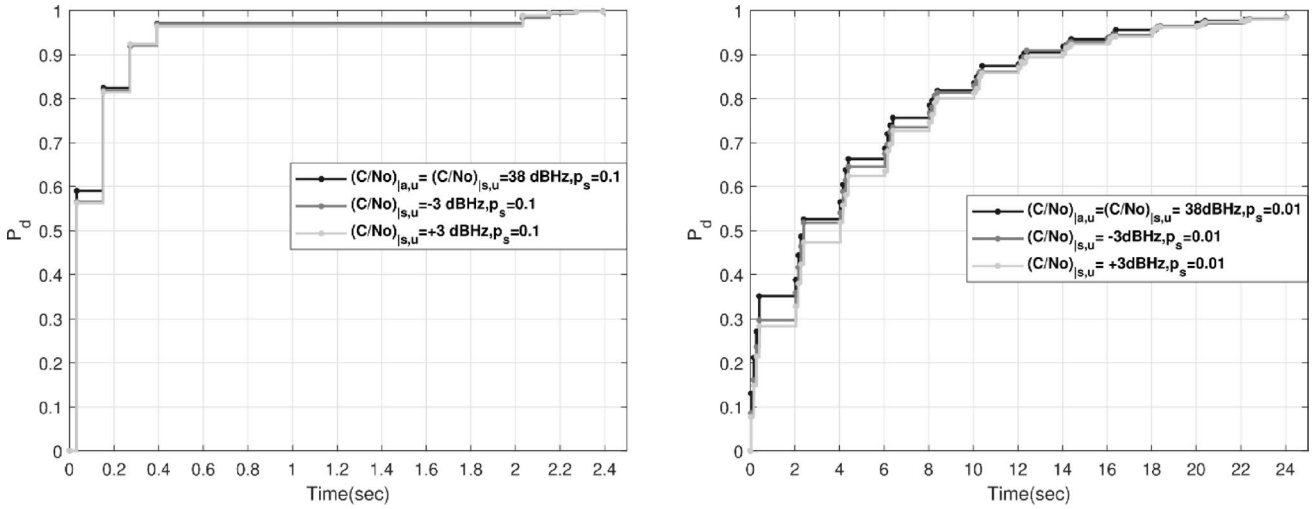

Fig. 8 Probability of detecting the spoofer as a function of time when (**a**) $p_s = 0.1$ and (**b**) $p_s = 0.01$ for $\frac{C}{N}_0 = 38$ dB-Hz at the user's receiver and with the spoofer operating at −3, 0 and +3 dB more of $\frac{C}{N}_0$

Table 3 Required time to detect a spoofer under different duty-cycle conditions of the receiver

		High duty-cycle		Low duty-cycle	
Number of unpredictable symbols per snapshot	Target probability of detection,P_d	Detection time for a spoofer with $p_s = 0.1$ (seconds)	Detection time for a spoofer with $p_s = 0.01$ (seconds)	Detection time for a spoofer with $p_s = 0.1$ (seconds)	Detection time for a spoofer with $p_s = 0.01$ (seconds)
8	0.90	0.27	12.39	4.02	54.03
8	0.95	0.39	18.03	6.03	72.03
8	0.99	2.15	24.15	8.03	98.02
6	0.90	0.38	18.02	6.02	72.02
6	0.95	2.02	22.30	8.02	96.03
6	0.99	2.26	34.14	12.03	143.02

unpredictable symbols per odd page. This effect will be particularly critical for detecting spoofers with low probability of error, such as $p_s = 0.01$. In contrast, by high duty-cycle we refer to the case when all batches of unpredictable symbols per odd page are gathered by the receiver. An overview of the impact of such duty-cycle operation is summarized in Table 3, where it can be seen how the detection time significantly grows in low duty-cycle operations.

In spite of the performance degradation for low duty cycle operation, the resulting detection time can be upper bounded by approximately 10 s, which is smaller than the few tens of seconds that are needed by the partial correlation technique proposed in (Seco-Granados et al. 2021) in similar working conditions. It is worth mentioning, though, that both techniques are actually complementary and should be used jointly. The reason is that for a spoofer not to be detected by the partial correlation technique in (Seco-Granados et al. 2021), it should estimate the unpredictable symbols as soon as possible, thus incurring in the shortest possible delay in the transmitted spoofed signal with respect to the authentic one. However, as the observation time for estimating the unpredictable symbols decreases, the probability of error increases, making it more susceptible to detection by the symbol-level detection technique proposed in the present work.

Practical implementation aspects

The availability of OSNMA data is a general concern in spoofing detection techniques that make use of OSNMA data provided by existing mass-market receivers. This is due to the fact that, as reported in (O'Driscoll et al. 2023), the availability of I/NAV data in those receivers is currently below 10%, in the best case. Therefore, techniques operating in snapshot mode, as the one proposed herein, can make a difference because they directly demodulate a small portion of received data without having to fully decode the whole I/NAV message.

Nevertheless, snapshot receivers must also cope with certain impairments that may impact in terms of spoofing detection performance. The two most relevant impairments are: (1) the visible satellites have different ranges with respect to the user's position, and thus, their signals arrive at the user's receiver with slightly different reception times. This means that not all satellites have the same number of unpredictable symbols. (2) Even if all satellites arrived perfectly time-aligned, the receiver is subject to clock offsets that prevent it from waking up at the exact time when the unpredictable symbols are expected to be received and thus contain less unpredictable symbols than the expected ones. Both impairments will be briefly discussed next.

Relative time delay between visible satellites

The impact of the relative time delays on received signals from different visible satellites is empirically analyzed by employing publicly available data from the online archive of International GNSS Service (IGS) global data centers (IGS 2023). The retrieved data is available for over a period of up to one day and at a sampling rate of 30 s, which is then processed by using the GFZRNX- RINEX GNSS Data Conversion and Manipulation Toolbox (Nischan 2016). After analyzing the real data, the relative time delays between visible satellites are found to exhibit a zero-mean gaussian-like distribution, as can be seen in Fig. 9 (a). The corresponding cumulative density function is shown in Fig. 9 (b), where can be seen that a maximum relative time delay of $\pm$ 10 ms is observed for 90 $\%$ of the time (i.e. ± 2.5 I/NAV data symbols), or up to $\pm$ 20 ms for 99 $\%$ of the time (i.e. ± 5 I/NAV data symbols). This observation must be taken into account when designing both the snapshot length and the wake up strategy to be used by the receiver, since the sequences of unpredictable symbols for different satellites may be offset by 5 symbols one from the other.

Clock offset affecting the wake up time

Another factor is the presence of a receiver clock offset, which translates into an offset on the time at which the receiver wakes up to gather a snapshot of signal. It is worth mentioning that two sources of time are assumed to be available in the proposed technique. The first offset is provided by the local clock of the receiver, is typically on the order of a few tens, and up to a few hundred of ms, when coarse-time navigation is adopted (Peterson et al. 1995). This is the case in snapshot receivers, which implement coarse-time navigation in order to circumvent their lack of knowledge about the transmission time of the received signal, and despite that limitation, be able to solve the user's position and time (Van Diggelen 2009). Apart from the receiver local clock, the snapshot receiver has also access to the external time reference provided by the communication network over which it is connected to the remote server. Such external time reference is often provided through Network Time Protocol (NTP) and can actually be used as an additional countermeasure to combat spoofing replay attacks. In particular, by making sure that the GNSS time estimated by the receiver lies within a certain admissible window. Clock offsets on the order of 10 ms are typically observed in small devices connected wirelessly through 4G/LTE networks (Miškinis et al. 2014), thus often providing a more accurate time reference

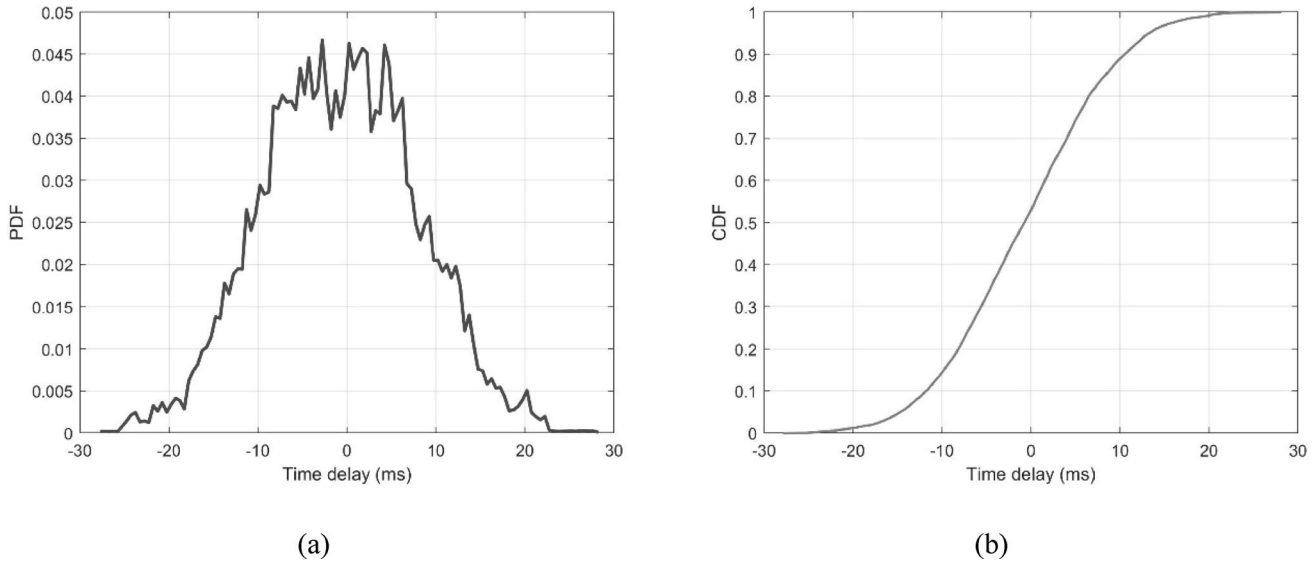

Fig. 9 **(a)** Probability density function (pdf) of the time delay difference between satellites, with respect to a reference one, using real satellite data. **(b)** Cumulative density function (cdf) corresponding to the plot **a**

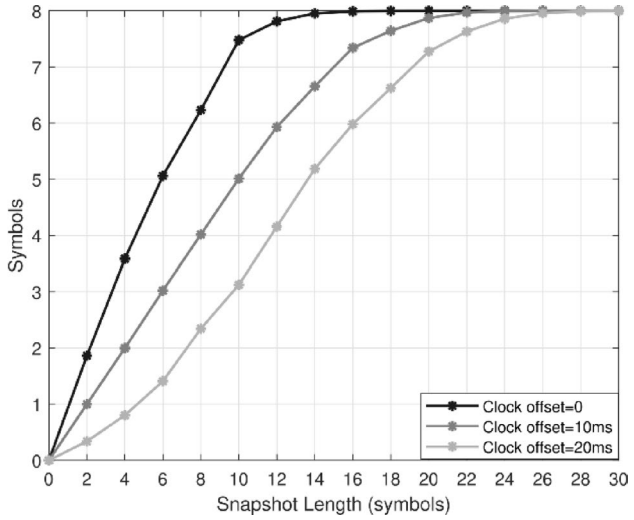

Fig. 10 Mean number of unpredictable symbols for each satellite in view as a function of the minimum snapshot length and the clock offset

than the one provided by the estimated time obtained by the receiver from a short snapshot of GNSS samples.

Figure 10 shows the mean number of unpredictable symbols that are available for each satellite in view as a function of snapshot length and the clock offset on wake-up time. In order to gather on average 8 unpredictable symbols, the minimum snapshot length must be 18 symbols, even if no clock offset is present. As already mentiond, this is due to the fact that visible satellites have different time of arrivals and thus, the snapshot length must be long enough to encompass the sequences of unpredictable symbols from different satellites. This is consistent with the $\pm$ 20 ms relative time delay for 99 % of the time that was discussed in the previous subsection. When a clock offset of 10 ms is present, the average number of unpredictable symbols for this same snapshot decreases to $\sim$7.5 symbols, and it goes down to $\sim$6.5 symbols for a 20 ms clock offset. The results in Fig. 10 can then be used to determine how much the minimum snapshot length should be increased in order to compensate for the clock offset, and thus to preserve the detection performance by avoiding the miss of unpredictable symbols.

Conclusion

This paper has provided a comprehensive analysis of a novel technique for spoofing detection that relies on the use of the unpredictable symbols provided in the I/NAV message of Galileo E1-B signal. The technique is implemented using a snapshot-based approach, opening the door to its deployment via remote or cloud-based platforms. This means that the user receiver can send the received unpredictable symbols, or directly the snapshot of received signal samples, to a remote end where the received OSNMA unpredictable symbols are compared with the authentic ones. The main contribution of this work has been to carefully analyze the feasibility of the proposed technique. Since it operates at the symbol level, several concerns naturally arise regarding its effectiveness, particularly due to potential symbol errors caused by various factors such as thermal noise at the spoofer and at the user's side, the overlap between the authentic and delayed and phase-shifted spoofed replica, the presence of synchronization errors, as well as the degradation introduced by multipath and signal fading. In order to carefully assess the feasibility of the proposed technique, a set of boundary conditions have been derived for such impairments, which reveal that the noise, multipath, synchronization errors are not likely to impact the performance of symbol level snapshot OSNMA spoofing detector under typical GNSS receivers operating conditions. However, some limitations do appear in the presence of signal fading, particularly in vehicular urban scenarios, where the SER severely degrades due to the adverse propagation and seriously hinders the spoofer detection. In addition, practical implementation aspects have also been discussed taking into account whether a sufficient number of unpredictable symbols are provided by the satellites in view, as a function of the snapshot length and the receiver clock offset. Unlike conventional detection techniques, which need to continuously track the received signal, the proposed snapshot OSNMA technique uses only a small portion of the received signal, of just tens of milliseconds in length. Thanks to this feature, the snapshot OSNMA technique does not require the full implementation of all OSNMA functionalities, as only a portion of the navigation message (i.e., specifically the section containing the unpredictable symbols) is needed to detect a spoofing attack. Numerical results confirm that this approach enables faster spoofing detection compared to existing techniques, taking on average less than 10 s for simple spoofers and less than 100 s for sophisticated ones, for 95% detection probability and outdoor clear sky. Overall, the competitive advantage offered by the proposed method makes it highly attractive for emerging applications where power consumption and processing time are constrained, such as in IoT devices, but where fast and reliable spoofing detection is still needed, such as in asset tracking, smart agriculture or drone delivery. This, in turn, facilitates the integration of authentication capabilities into lightweight and cost-sensitive systems.

Appendix

Symbol errors due to the overlap of authentic and spoofed signals at the user's receiver

The SER probability for the overlapped received symbol can be obtained by formulating the following model.

$$r_i(n) = \alpha_0 s_i(n) + \alpha_1 \widetilde{s}_i(n) + \omega_i(n) \tag{16}$$

for $n = 0, \ldots, L-1$ unpredictable symbols and $i = 0, \ldots, N-1$ snapshots, whereas $\alpha_0 = |a_0| e^{j\varnothing_{i,0}}$ and $\alpha_1 = |a_1| e^{j\varnothing_{i,1}}$ are the complex amplitudes of the received authentic and spoofed symbols, respectively.

Under the assumption that $\widetilde{s}_i(n) = s_i(n)$ so that there are no spoofer errors, the overlapped received symbol becomes,

$$r_i(n) = \alpha_0 \left(1 + \frac{\alpha_1}{\alpha_0}\right) s_i(n) + \omega_i(n) \tag{17}$$

where $\widehat{E}_s \doteq \left|\alpha_0 \left(1 + \frac{\alpha_1}{\alpha_0}\right)\right|^2$ now becomes the energy of the overlapped symbol. After simplifying the overlapped symbol energy term and merging it with (5), the SER in the presence of spoofer becomes,

$$p_{u,1} = \frac{1}{2}\mathrm{erfc}\left(\sqrt{T_d\left(\frac{C}{N_0}\right)_{|a,u}\left[1 + \frac{1}{SSR} + 2\frac{cos\Delta\varnothing}{\sqrt{SSR}}\right]}\right) \tag{18}$$

where the snapshot index i has been omitted for the sake of clarity and $SSR \doteq \left|\frac{\alpha_0}{\alpha_1}\right|^2$ whereas $\Delta\varnothing \doteq \varnothing_1 - \varnothing_0$ is the relative phase difference between the authentic and the spoofed signals. Two limit cases can be distinguished depending on whether the two signals overlap constructively, i.e., $\Delta\varnothing = 0$, or destructively, i.e., $\Delta\varnothing = \pi$. The latter leads to the worst SER, which is therefore retained here and given by,

$$p_{u,1} = \frac{1}{2}\mathrm{erfc}\left(\sqrt{T_d\left(\frac{C}{N_0}\right)_{|a,u}\left[1 + \frac{1}{SSR} - \frac{2}{\sqrt{SSR}}\right]}\right) \tag{19}$$

Symbol errors due to synchronization errors at the user's receiver

To determine how much degradation is incurred in terms of SER due to synchronization error, we will make use of the general result in (Bucket and Moeneclaey 1995) for the SER degradation of an M-PSK bandlimited direct-sequence spread spectrum (DS-SS) signal in the presence of estimation errors on the synchronization parameters. Such degradation depends on the working conditions determined by the actual $\frac{C}{N_0}$ and it is given by (measured in dB),

$$D_\xi = -10\log_{10}\left(\frac{E^2[d(\xi)]}{sin^2\left(\frac{\pi}{M}\right)} - \frac{var(d(\xi))}{\frac{2C}{N_o}T}\right)[\mathrm{dB}] \tag{20}$$

where $d(\xi)$ is the distance between the M-PSK decision boundary and a received M-PSK symbol affected by a generic estimation error ξ, and T is the symbol period.

For carrier phase estimation errors, denoted henceforth as $\xi = \epsilon_\theta$, and for the BPSK symbols conveyed by the Galileo E1-B, the result in (20) simplifies to a degradation given by,

$$D_{\epsilon_\theta} \approx \frac{10}{ln10}\mathrm{var}(\epsilon_\theta) \geq \frac{10}{ln10}\frac{2L-1}{L(L+1)}\left(\frac{C}{N_o}T\right)^{-1}[\mathrm{dB}] \tag{21}$$

where the variance of the phase estimation errors, $\mathrm{var}(\epsilon_\theta)$, has been lower bounded in the right hand side of (21) by the corresponding Cramer Rao Lower Bound (CRLB) (Kay 1993, Eq. (15.72)).

For time delay estimation errors, denoted henceforth as $\xi = \epsilon_\tau$, the degradation in (13) particularizes to (Bucket and Moeneclaey 1995),

$$D_{\epsilon_\tau} \approx -\frac{10}{ln10} g''(\mathrm{t})_{|\ \mathrm{t}\ =\ 0}\, \mathrm{T_c^2 var}(\epsilon_\tau) \quad [\mathrm{dB}] \tag{22}$$

where $g''(t)$ is the second derivative of the auto-correlation of the chip pulse used by the DS-SS signal and T_c the chip period.

The time delay estimation jitter has been obtained by numerically evaluating the CRLB for time delay estimation (Kay 1993, Eq. (3.40)), assuming a Galileo BOC(1,1) signal with a user's receiver bandwidth of 5 MHz. The corresponding SER degradation has been obtained by mapping such time delay estimation jitter onto Fig. 4 in (Bucket and Moeneclaey 1995).

Acknowledgements The authors would like to thank Ignacio Fernandez-Hernandez, from DG DEFIS, European Commission, for his insightful comments and suggestions.

Funding Open Access Funding provided by Universitat Autonoma de Barcelona. This work was supported 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 with reference number PID2020-118984 GB-I00/ and PDC2021-121362-I00/AEI/https://doi.org/10.13039/501100011033.

Data availability No specific datasets were needed to obtain the results of this paper.

Declarations

Conflict of interest The authors have no conflict of interests to declare that are relevant to the content of this article. The content of this work reflects only the author's view; and EUSPA is not responsible for any use that may be made of the information it contains.

Ethics approval and consent to participate The approval by the appropriate ethics committee is not applicable for this manuscript. Moreover, this manuscript has not been published (partially or in full) elsewhere and not submitted elsewhere for simultaneous consideration. Results are presented clearly, honestly and without fabrication.

Consent for Publication All authors carefully read and approved to participate in the publication of this manuscript.

References

Bucket K, Moeneclaey M (1995) Effect of random carrier phase and timing errors on the detection of narrowband M-PSK and bandlimited DS/SS M-PSK signals. IEEE Trans Commun 43(2/3/4):1260–1263. https://doi.org/10.1109/26.380164

Caparra G, Laurenti N, Ioannides RT, Crisci M (2014) Improving secure code estimate-replay attacks and their detection on GNSS signals. In: Proceedings of the NAVITEC conference, Noordwijk, The Netherlands, 2014, pp 1–8. https://doi.org/10.13140/RG.2.1.2130.4728

Dingbo Y, Hong L, Fei W, Mingquan L (2018) A GNSS acquisition method with the capability of spoofing detection and mitigation. Chin J Electron 27:213–222. https://doi.org/10.1049/cje.2017.11.001

ETSI TS 103 246–3 (2020) Satellite Earth Stations and Systems (SES); GNSS based location systems; Part 3: Performance.. requirements.https://www.etsi.org/deliver/etsi_ts/103200_103299/10324603/01.03.01_60/ts_10324603v010301p.pdf. Accessed June 2023.

Fawcett T (2006) An introduction to ROC analysis. Pattern Recogn Lett 27(8):861–874. https://doi.org/10.1016/j.patrec.2005.10.010

Fernández-Hernández I, Rijmen V, Seco-Granados G, Simon J, Rodriguez I, Calle JD (2016) A navigation message authentication proposal for the Galileo open service. Navigation 63(1):85–102. https://doi.org/10.1002/navi.125

Fernández-Hernández I, Seco-Granados G (2016) Galileo NMA signal unpredictability and anti-replay protection. In: Proceedings of the International Conference on Localization and GNSS (ICL-GNSS), Barcelona, Spain, 2016, 1–5. https://doi.org/10.1109/ICL-GNSS.2016.7533686

Gallardo F, Yuste AP (2020) SCER spoofing attacks on the Galileo open service and machine learning techniques for end-user protection. IEEE Access 4:85515–85532. https://doi.org/10.1109/ACCESS.2020.2992119

Humphreys TE (2013) Detection strategy for cryptographic GNSS anti-spoofing. IEEE Trans Aerospace Electron Syst 49(2):1073–1090. https://doi.org/10.1109/TAES.2013.6494400

IGS (2023) International GNSS Service. Available at: https://igs.org/data-access/ Accessed December 2022

Kay SM (1993) Fundamentals of statistical signal processing: estimation theory. Prentice-Hall, United States

Lucas-Sabola V, Seco-Granados G, López-Salcedo JA, García-Molina JA (2018) GNSS IoT Positioning. From Conventional Sensors to a Cloud-Based Solution. Inside GNSS, vol. May/June, 53–62, May 2018

Marucco G, Ligios M, Chala SA, Rosengren P (2020) Galileo Open Service Navigation Message Authentication: Exploitation in the Frame of an E-Security Infrastructure. In: Proceedings of the European Navigation Conference (ENC), Dresden, Germany, 2020, 1–10. https://doi.org/10.23919/ENC48637.2020.9317472

Miškinis R, Jokubauskis D, Smirnov D, Urba E, Malyško B, Dzindzelėta B, Svirskas K (2014) Timing over a 4G (LTE) mobile network. In: Proceedings of the European Frequency and Time Forum (EFTF), Neuchatel, Switzerland, 2014, 491–493. https://doi.org/10.1109/EFTF.2014.7331543

Montgomery PY, Humphreys TE, Ledvina BM (2009) Receiver autonomous spoofing detection: Experimental results of a multi-antenna receiver defense against a portable civil GPS spoofer. In: Proceedings of the International Technical Meeting of The Institute of Navigation, 124–130 https://www.ion.org/publications/abstract.cfm?articleID=8295

Nischan, T (2016) GFZRNX-RINEX GNSS data conversion and manipulation toolbox (version 1.05). GFZ Data Services. https://doi.org/10.5880/GFZ.1.1.2016.002

O'Driscoll C, Fernández-Hernández I (2020) Mapping bit to symbol unpredictability in convolutionally encoded messages with checksums, with application to Galileo OSNMA. In: Proceedings of the 33rd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+), virtual, 3751–3765. https://doi.org/10.33012/2020.17715

O'Driscoll C, Winkel J, Fernández-Hernández I (2023) Assisted NMA proof of concept on Android smartphones. In: Proceedings of the IEEE/ION Position Location and Navigation Symposium (PLANS), Monterey, CA, USA, 559–569. https://doi.org/10.1109/PLANS53410.2023.10139953

O'Driscoll C, Fernández-Hernández I (2022) Mapping bit to symbol unpredictability with application to Galileo Open Service Navigation Message Authentication. NAVIGATION: J Inst Navigation. https://doi.org/10.33012/navi.519

Peterson B, Hartnett R, Ottman G (1995) GPS receiver structures for the urban canyon. In: Proceedings of the 8th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GPS), Palm Springs, CA, USA, 1323–1332

Proakis J, Salehi M (2002) Communication systems engineering, 2nd edn. Prentice Hall, United States

Reyes Gonzalez J, Fernandez-Hernandez I, Hubert B, Donatacci M (2021) Using Navigation Message Authentication in Smartphones to Protect against Replay Attacks. In: Proceedings of the RIN Navigation Conference, 2021

Seco-Granados G, Gómez-Casco D, López-Salcedo JA, Fernández-Hernández I (2021) Detection of replay attacks to GNSS based on partial correlations and authentication data unpredictability. GPS Solutions 25(2):1–15. https://doi.org/10.1007/s10291-020-01049-z

Shahid H, Locubiche S, Canzian L, Sarto C, Pozzobon O, Fernandez-Hernandez I, Reyes-Gonzalez J, Seco-Granados G, López-Salcedo JA (2023a) Feasibility of Snapshot OSNMA for Spoofing Detection in Urban Scenarios, In: Proceedings of the European

Navigation Conference (ENC), Noordwijk, The Netherlands, 2023, pp. 1–9. https://doi.org/10.3390/ENC2023-15433

Shahid H, Canzian L, Sarto C, Pozzobon O, Reyes-González J, Seco-Granados G, López-Salcedo JA (2023b) Spoofing Detection Performance of Snapshot OSNMA Under Time and Symbol Errors. In: Proceedings of the Vehicular Technology Conference (VTC2023-Fall), Hong Kong, 2023, pp. 1–7. https://doi.org/10.1109/VTC2023-Fall60731.2023.10333729

Shuli D, Taotao Z, Min L. A (2019) GNSS anti-spoofing technology based on power detection. In; Proceedings of IEEE 8th Joint International Information Technology and Artificial Intelligence Conference (ITAIC), pp. 1134–1137. https://doi.org/10.1109/ITAIC.2019.8785690

Sun C, Cheong JW, Dempster AG, Zhao H, Feng W (2018) GNSS spoofing detection by means of signal quality monitoring (SQM) metric combination. IEEE Access 6:66428–66441. https://doi.org/10.1109/ACCESS.2018.2875948

Van Diggelen F (2009) GPS: Assisted GPS, GNSS, and SBAS. Artech House

Wang J, Li H, Cui X, Lu M (2013) A new method in acquisition to detect GNSS spoofing signal. In: Proceedings of the International Conference on Mechatronic Science, Electric Emerging and Computer (MEC), https://doi.org/10.1109/MEC.2013.6885528

Zhang K, Papadimitartos P (2019) Safeguarding NMA Enhanced Galileo OS Signal from Distance-Decreasing Attacks. In: Proceedings of the International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+), pp. 4041–4052

Husnain Shahid received his MS degree in Electronics and Communication Engineering from Shanghai Jiao Tong University, China 2019. Since 2020, he is with the Department of Electronics and Telecommunication Engineering, Universitat Autonoma de Barcelona. His research interest lies in GNSS signal processing and authentication, and Wireless Communication.

Daniel Egea-Roca received the Ph.D. in Electrical Engineering from Universitat Autònoma de Barcelona (UAB) Spain in 2017. Since 2017, he is with UAB as postdoctoral researcher and involved in several research projects funded by the EC and the European Space Agency (ESA). His research interests include signal processing and its application in threat detection and integrity techniques for GNSS receivers.

Luca Canzian joined Qascom in 2015 and he is currently leading the R&D domain area. He has worked in several projects with ESA, ASI, NASA, the European Commission and Industry. His main expertise involves ground-based and space-based location systems, including systems for detection and location of interference signals, hybridization with inertial measurements, POD techniques, GNSS authentication and anti-spoofing techniques. He holds a PhD in Electrical Engineering from University of Padova (Italy).

Carlo Sarto joined Qascom in 2008 and he is currently Head of Security Engineering. He is responsible for the coordination of engineering activities related to security of navigation and communication satellite systems, at ground, satellite and user segment. He received a degree in computer science at the University of Padua.

Oscar Pozzobon is co-founder, president and CEO in Qascom. He received a Phd in Aerospace and Satellite Applications. He has more than 20 years of experience in space, satellite navigation and cybersecurity, and has been involved in several space programs with the major international space agencies and industries. He is contract professor at the University of Padova.

J. Reyes-González is a Service Engineer at EUSPA. He gained his GNSS technical experience as System Engineer Technical Assistant at ESA/ESTEC, after national and international assignments at innovation projects in GMV and Siemens. Reyes holds a degree in Electronic, Electrical and Mechanical Engineering at ICAI and Master's degree in Space Technology at UPM.

Gonzalo Seco-Granados received the Ph.D. degree in Telecommunications Engineering from the Universitat Politècnica de Catalunya, in 2000, and the MBA degree from IESE Business School, in 2002. Until 2005, he was with the European Space Agency, involved in the design of the Galileo system. Since 2006, he is with Universitat Autònoma de Barcelona and also affiliated with the Institute of Space Studies of Catalonia.

José A. López-Salcedo received his M.Sc. and Ph.D. degrees in Telecommunications Engineering from the Universitat Politècnica de Catalunya, in 2001 and 2007, respectively. Since 2006, he is with Universitat Autònoma de Barcelona, and he also affiliated with the Institute of Space Studies of Catalonia, and he held a visiting appointment at the EC Joint Research Center.