An Experimental Performance Assessment of Galileo OSNMA

Toni Hammarberg, José M. Vallet García, Jarno N. Alanko, and M. Zahidul H. Bhuiyan
Navigation and Positioning Department
Finnish Geospatial Research Institute, National Land Survey of Finland
Espoo, Finland
Email:name.surname@nls.fi

***Abstract*—We present Galileo Open Service Navigation Message Authentication (OSNMA) observed operational information and key performance indicators (KPIs) from the analysis of a four day long dataset collected in static open sky condition in southern Finland and using our in-house developed OSNMA implementation. In particular, we present a timeline with authentication related events such as authentication status and type, dropped navigation pages and failed cyclic redundancy checks. We also report KPIs such as the number of simultaneously authenticated satellites over time, percentage of authenticated fixes and time to first authenticated fix, and study how the satellite visibility affects these figures. Finally, we analyze situations where it was not possible to reach an authenticated fix, and offer our findings on the observed patterns.**

***Index Terms*—Galileo, OSNMA, GNSS, authentication**

I. Introduction

During the last decade, major concerns have arisen within the global navigation satellite system (GNSS) community on how to improve the robustness and resilience against attacks with counterfeit GNSS-like signals, also known as spoofing. One method to prevent spoofing is by ensuring that the information reaching the receiver is authentic and originating from the legitimate claimed source. Galileo's Open Service Navigation Message Authentication (OSNMA) is designed to enable this at the receiver end in a manner that virtually eliminates the need of a chain of trust with dependence on external third party services. This service, the first of its kind in the civilian segment, opens the door to many and diverse new applications that require authenticated position.

At present, OSNMA has been in the public observation (PO) test phase for little over a year. In this phase interested users are invited to implement the service at the receiver level, test it and give feedback to the European Union Space Program Agency (EUSPA). The Navigation and Positioning department of the Finnish Geospatial Research Institute (FGI) has created an implementation following the pertinent interface control document (ICD) [1] and the receiver guidelines for the test phase (version 1.1 at the time of this writing), with the particularity that it is to be executed in a computing platform outside of the receiver. This implementation, henceforth denoted as FGI-OSNMA, has been created within the frame of the Horizon2020 funded ESRIUM project, which aims at creating road wear-maps with accurate information about the position and shape of road damage, and to send prompt and real-time notifications to drivers and autonomous vehicles with instructions to avoid the damaged areas and route recommendations to even the road wear [2]. In the ESRIUM project we rely on Galileo's services for a) increasing the positioning accuracy of both, the sensor vehicle mapping the road and the end-user vehicle receiving the notifications, and b) the authentication of the position estimates using Galileo OSNMA, in order to increase the security and robustness of the whole solution and to detect possible spoofing attacks.

Despite OSNMA being a relatively new and modern technology still in its test phase, there is already relevant literature related to it encompassing both theoretical work [3]–[8] and practical performance assessments [9]–[20]. In addition to this, there are a few open source implementations of the OSNMA protocol [21]–[23], and some companies already support it in some of their products, such as Septentrio [24].

This paper expands on the practical OSNMA performance assessments made in the previously cited papers. Similar to [9] and [15], we present operational information and some key performance indicators (KPIs) of OSNMA, such as a timeline showing relevant authentication events, number of authenticated satellites (that is, number of satellites whose navigation message has been successfully authenticated by OSNMA) over time, and number of satellites transmitting OSNMA data over time. In addition to this, we show the dependency of some of the KPIs on the elevation mask. We also take a closer look at the cases where a satellite fails to reach an authenticated status. More specifically, we take a look at the possible failure of navigation pages' cyclic redundancy checks (CRCs), and analyze the cases in which having a low number of satellites transmitting OSNMA data poses problems. Having made an OSNMA implementation, we are in a position to discuss and suggest some practical strategies to optimally handle these cases.

The content of the paper is organized as follows. In Section II we give an overview on the OSNMA protocol focusing on the details needed to understand the rest of this paper. In Section III we then explain the experimental setup. Section IV presents operational information, KPIs and other related analysis. We then discuss the results and present our observations in Section V, and conclude the paper summarizing our findings in Section VI.

II. OSNMA Overview

The goal of OSNMA is to enable the users to verify that the navigation message received through the signal-in-space (SIS) is both unmodified and authentic. The OSNMA authentication system is based on the TESLA broadcast authentication protocol [25]. In this section we give an overview of the TESLA variant used in the OSNMA protocol. For the sake of clarity, we focus on the main technical details necessary to understand the content of this article. A more comprehensive review of modern TESLA variants can be found in [26], and the full details regarding OSNMA can be found in the official specification documents [1], [27].

The TESLA protocol is a method of transmitting a sequence of authentication keys through a one-way communication channel from a transmitter to a receiver via an untrusted communication channel. In OSNMA each key is then used to generate a truncated message authentication code (MAC), called a tag, which authenticates the navigation message sent by a satellite in a previous subframe. This key sequence is generated by starting from a random seed K_i, where i is very large, and the rest of the keys K_{i-k} are obtained by iterating a cryptographic hash function h such that $K_{i-1} = T(h(K_i||t_i||\alpha))$, where $||$ denotes the concatenation operation of bit-level representations of the operands, T is the truncation operation, t_i is the time at which key K_i was transmitted, and α is a hash salt that is set in the protocol parameters. Then the keys $K_1, K_2, K_3, ...$ are transmitted one by one at regular time intervals and in reverse order with respect to their generation. Due to this construction, the verification that K_{i+1} is part of the correct key chain is a matter of simple hashing, while due to the properties of cryptographic hash functions (pre-image resistance, collision resistance), it is practically impossible to compute or forge the next key.

Since the authenticity of the keys is verified using previously authenticated keys, the protocol requires that the receiver has access to a single trusted key K_j from the past. Usually this is the so-called root key. In OSNMA, the root key is transmitted with the SIS along with an Elliptic Curve Digital Signature Algorithm (ECDSA) signature that proves the authenticity of the key. The signature is verified against the Galileo public key, which is available at the European GNSS Service Centre (GSC) website, though this can also be retrieved or renewed via the SIS. The public key is further verified against a Merkle tree, the root of which is meant to be pre-installed in the receiver hardware. Therefore the OSNMA utilizes a variety of well tested cryptographic methods, yet adapts these to the satellite specific use case.

The nominal navigation pages contain 40 bits of OSNMA related data, which is divided into header and root key (HKROOT) (8 bits) and MAC and key (MACK) (32 bits) sections. This data is accumulated over the course of 15 nominal pages, or one subframe, to form a 120 bit HKROOT and 480 bit MACK messages. The HKROOT contains status updates and the data needed for the initialization, while the tags and keys are contained in the MACK section.

It is important to note that in practice not all Galileo satellites will transmit OSNMA data. Instead, the satellites that do transmit OSNMA data will also transmit tags that allow the authentication of navigation messages from other satellites as well. This process is called cross-authentication. The importance of cross-authentication is that is adds redundancy to the system, and in theory, cross-authentication is not limited to Galileo satellites. In the future it may be used to authenticate satellites from other constellation as well.

The last thing the reader should understand about OSNMA is that the tags and authentications are associated with a so-called authentication data and key delay (ADKD) numbers. The ADKD specifies what data is authenticated by the tag and it informs about a potential key delay. The ADKD=0 specifies that the tag authenticates ephemeris, clock, and the status of the satellite. The ADKD=4 specifies that the tag authenticates Galileo constellation (not satellite) specific timing information. Lastly the ADKD=12, also known as Slow MAC, authenticates the same data as ADKD=0, but with an additional 10 subframes delay for the key transmission. For the sake of simplicity, in the coming sections when we say that a satellite is authenticated, we mean that its ephemeris, clock, and status are authenticated by an ADKD=0 or ADKD=12 tag.

Each satellite transmitting OSNMA data transmits tags in a fixed seqeuence, which spans over two subframes or one minute. This sequence, however, may change over time and the possible sequences are described in the OSNMA ICD [1]. During the experiment the transmitted tag sequence was 00S, 00E, 04S, 00E, 12S, 00E, 00S, 00E, 00E, 12S, 00E, 12E. Here the first two characters of the tag identifier specify the ADKD type and the third character specifies whether the tag is for self or cross-authentication (S=self, E=cross).

III. Experimental Setup

The data used in this study was collected with a Septentrio Mosaic X5 receiver loaded with the 4.12.1 firmware (FW) version and connected to a Septentrio PolaNt Choke Ring antenna. The antenna was statically mounted in the roof of a building in FGI's premises in Espoo in southern Finland and in an open-sky environment. The data used in the present study was collected between 24.10.2022 and 28.10.2022, with a total duration of 95 hours, or approximately four days.

The X5 receiver makes available the raw 234 bits of a Galileo I/NAV navigation page via the GALRawINAV block, which includes the even and odd pages concatenated and after deinterleaving and Viterbi decoding [28, Sec. 4.2.5]. The inputs to our OSNMA implementation are these blocks, which are then parsed to obtain the different pieces of information involved in the authentication protocol. Note that the receiver with the referred FW version already supports OSNMA processing, but we used our implementation in this analysis because it gives us more control over the process and better capabilities for in-depth investigation.

All of the processing in this paper has then been done using our own OSNMA implementation, which we call the FGI-

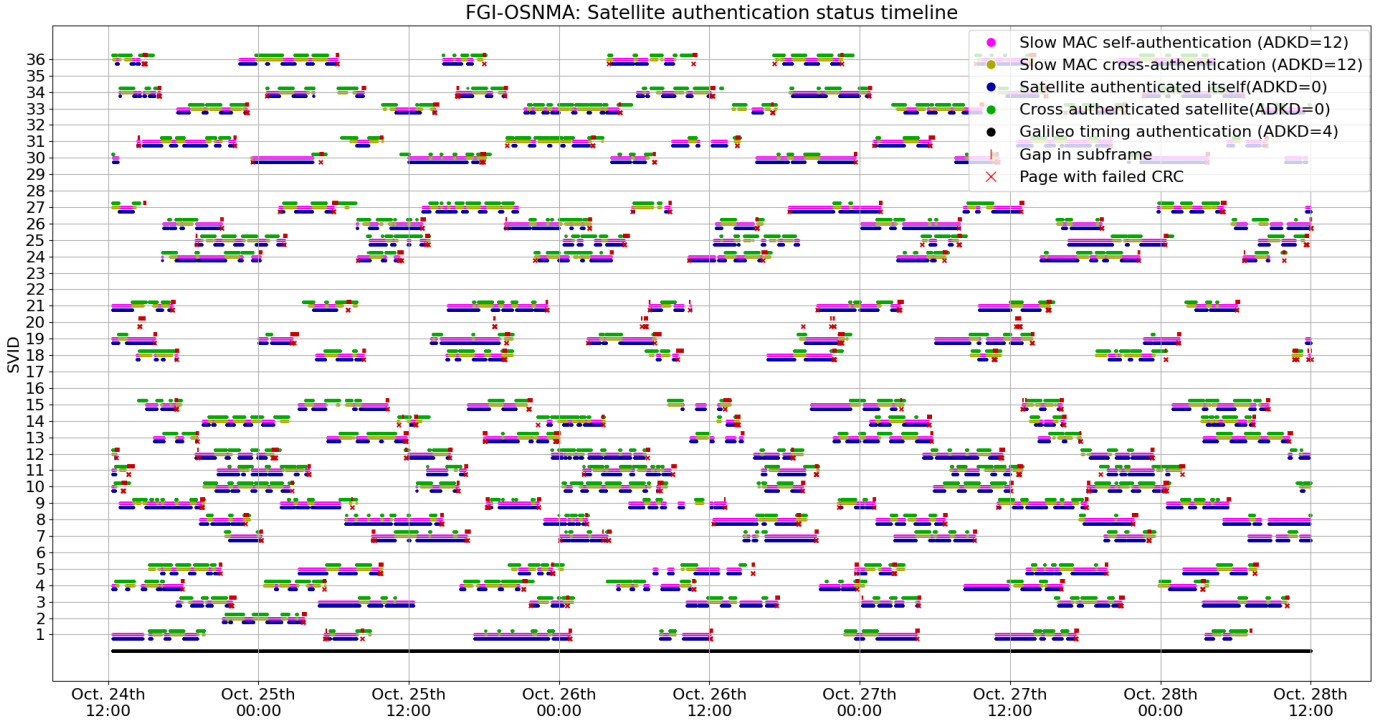

Figure 1: Authentication events over the test period.

OSNMA. The design and implementation of FGI-OSNMA has been made with special emphasis in its modularity, usability in real time and integrability as a library in third party applications. FGI-OSNMA will be made openly available in the near future, and its main characteristics will be explained along its release. The correctness of the implementation has been validated by using the official test vectors published by EUSPA, and by comparing the performance against that obtained with other available OSNMA implementations, such as OSNMAlib [21] or the Septentrio implementation. In particular, the FGI-OSNMA and OSNMAlib give equivalent authentication results on the EUSPA test vectors.

IV. Results and Analysis

We now present OSNMA operational information and KPIs pertaining our tests. Fig. 1 shows what we denote as the *satellite authentication status timeline*. This timeline represents the occurrence of authentication related events as reported by FGI-OSNMA. In addition to the authentication status and type (i.e. ADKD number), the timeline in Fig. 1 shows events where navigation pages were dropped and page CRCs failed. We consider that visualizing the occurrence of these events in the graph gives a valuable and informative view of when and how often they can naturally occur. In addition, their occurrence will be analyzed later in this article. We now proceed to present some observed trends and KPIs associated to Fig. 1 in more detail.

Fig. 2 shows the distribution of the number of simultaneously authenticated satellites (that is, the count of satellites with authenticated status at a given time instant), and Table I

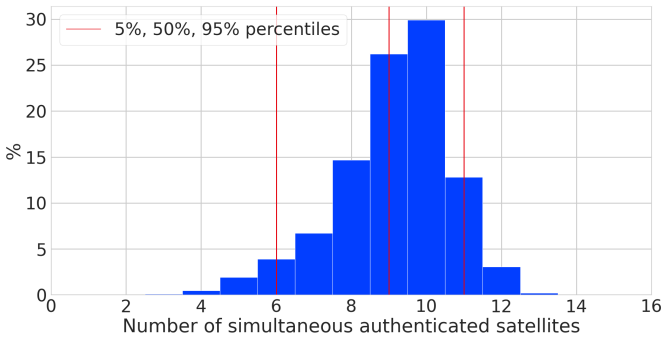

Figure 2: Distribution of the number of simultaneously authenticated satellites available during our tests.

presents some statistics related to these graphs. One important statistic is the percentage of time during which a receiver can compute an authenticated position, velocity and time (PVT). The condition for this to be possible is that there must be at least four authenticated satellites at the same time. We henceforth use the term *authenticated fix* to refer to cases where the before-mentioned condition is met. From the statistics presented in Table I, we observe that there were four or more authenticated satellites visible, and therefore authenticated fixes, 99.74% of the time. Correspondingly, it was not possible to compute authenticated fixes 0.26% of the time.

Table I: Statistics related to the authentication.

Statistic	Value
Simultaneous authenticated satellites: 5% percentile	6
Simultaneous authenticated satellites: average	9.14
Simultaneous authenticated satellites: 95% percentile	11
Percentage of authenticated fixes	99.74%
Self-authentications out of all ADKD=0 authentications	37.91%
Cross-authentications out of all ADKD=0 authentications	62.09%

Other noteworthy patterns in the authentication timeline of Fig.1 include the following.

- While looking fully continuous in the Fig. 1, the Galileo constellation specific timing information (ADKD=4) was authenticated 99.74% of the time. Because the ADKD=4 information is authenticated once every 60 seconds, this means that the timing information was authenticated in all but 15 subframes.
- In the authentication scheme the satellites alternate relatively frequently between self-authentication (which also means that the satellite is transmitting OSNMA data) and cross-authentication following a seemingly random pattern. In relation to this pattern, the specification states that it is indeed unpredictable for the user [1, Sec. 5.2].
- There are numerous cases of failed cyclic redundancy checks (CRCs) or gaps in the subframe (i.e. a subframe missing nominal navigation pages). These are associated with poor signal quality. In the dataset used in this study, these occurred exclusively when the satellites were rising over or disappearing below the horizon, in other words, in cases in which satellites have low elevation and therefore poor signal reception quality. It then comes as no surprise that we observed data reception problems from satellites with low elevation.

Next we investigate how the satellite visibility affects the OSNMA performance. We do this by applying an *elevation mask*. The process is similar to how GNSS receivers discard satellites with low elevation due to high probability of having poor signal quality. We run the OSNMA engine and compute the KPIs using data only from satellites with an elevation higher than the value configured in the mask. The effect of the elevation mask in the OSNMA KPIs computed in this manner can be used as an approximation of what could be the expected performance in environments with limited satellite visibility. For example, in urban environments tall buildings will block the signals coming from satellites with low elevation. The effect of this in the OSNMA performance can be approximated by applying an appropriate elevation mask in the OSNMA processing as explained before.

Fig. 3 shows how the elevation mask affects the average number of authenticated satellites and the percentage of authenticated fixes, and Table II presents some related statistics. From the figure we can observe a gradual and continuous decrease of the percentage of authenticated fixes as the elevation mask increases. The percentage of authenticated fixes decreases slowly at first, but rapidly drops as the elevation mask grows.

Fig. 4 and Table III present the dependency of the TTFAF (that is, how long it would take to a receiver to achieve a first authenticated fix) as a function of the applied elevation mask. The results are computed by running the OSNMA engine over our data one thousand times per elevation mask value, each run starting from a random time point selected from a uniform distribution, and letting the engine run until four satellites become authenticated. Fig. 4 graphically shows the average

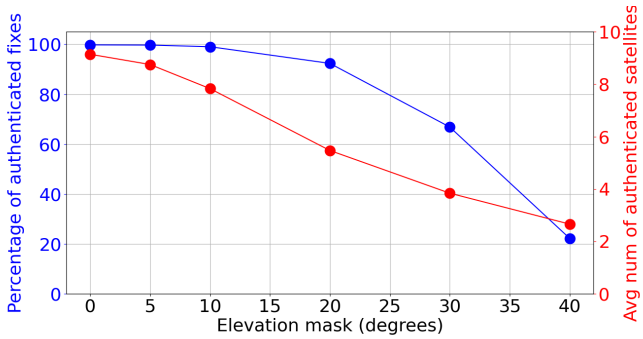

Figure 3: Average number of satellites with authenticated status (red) and percentage of authenticated fixes (blue) as a function of the elevation mask.

Table II: Percentage of authenticated fixes and percentiles of the number of simultaneous authenticated satellites as a function of the elevation mask.

Elevation mask	Number of authenticated fixes	Authenticated sats. count Percentiles: 5%, 50%, 95%
0°	99.74%	6, 9, 11
5°	99.66%	6, 9, 11
10°	99.0%	5, 8, 10
20°	92.33%	3, 6, 8
30°	66.83%	2, 4, 6
40°	22.24%	0, 3, 4

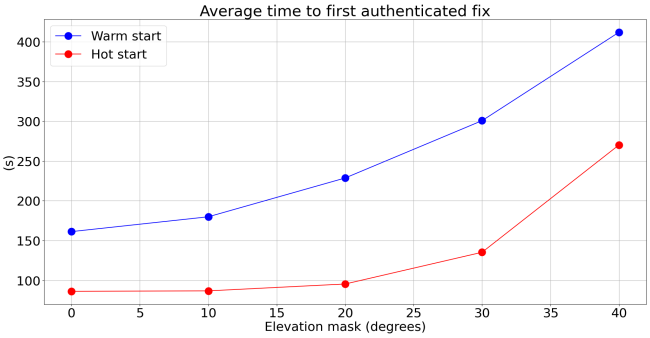

Figure 4: Average time to first authenticated fix (TTFAF) as a function of the elevation mask

values of these realizations, and Table III shows the numerical values of some associated statistics. We present the results for both warm and hot start scenarios. In the OSNMA literature, the warm-start scenario refers to the case where the Galileo public key is available to the receiver beforehand. If in addition to this the TESLA root key is available, the scenario is referred as hot-start. The hot-start case is the most favorable scenario, and is also the most likely in practice when the receiver is in frequent use. As we can observe, and similarly as with other KPIs, the elevation mask can significantly affect the TTFAF. However, the hot-start scenario is visibly less affected until we reach very high levels of elevation mask.

Overall, from Fig. 3 and 4, and their respective statistics from Table II and III, we see that the OSNMA service and usability can be significantly affected by the satellite visibility.

We now proceed to analyze in more detail the cases in which an authenticated fix could not be attained. The following studies are done using a zero elevation mask, that is: including all the information from all the visible satellites.

Some causes of non-authentication are related to the naturally occurring transmission issues: as previously observed, transmission problems can occur during the start or the end of each satellite's visibility period. However, more often the problem seems to be related to the number of satellites transmitting OSNMA data. Fig. 5 and 6 present the number of visible satellites transmitting OSNMA data and the number of authenticated satellites over time, respectively. From Fig. 5 we observe that the number of visible satellites transmitting OSNMA data can drop very low, even down to zero. In Fig. 6 one can see a clear correlation between the drops in the number of authenticated satellites with the times when a low number of visible satellites (e.g. two or less) are transmitting OSNMA data.

While occurring quite rarely, having a low number of visible satellites transmitting OSNMA data can then act as a bottleneck to OSNMA performance. As an example, and as seen in Fig. 6, the situations with the lowest number of authenticated satellites are naturally highly correlated with a low number of satellites transmitting the OSNMA data. In fact, in our dataset all but one failure to reach an authenticated fix were a result of a low number of visible satellites transmitting OSNMA data.

Table III: Percentiles of the TTFAF as a function of the elevation mask in warm- and hot-start scenarios.

Elevation mask	**Warm-start (Percentiles: 10%, 50%, 90%)**	**Hot-start (Percentiles: 10%, 50%, 90%)**
0°	104, 150, 232	74, 86, 98
10°	116, 166, 262	74, 86, 98
20°	136, 208, 338	74, 88, 116
30°	168, 262, 424	78, 102, 152
40°	200, 318, 570	86, 128, 454

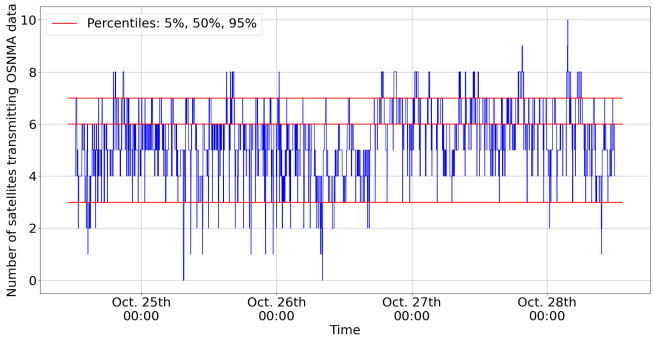

Figure 5: Number of satellites transmitting OSNMA data over time and percentiles of its distribution.

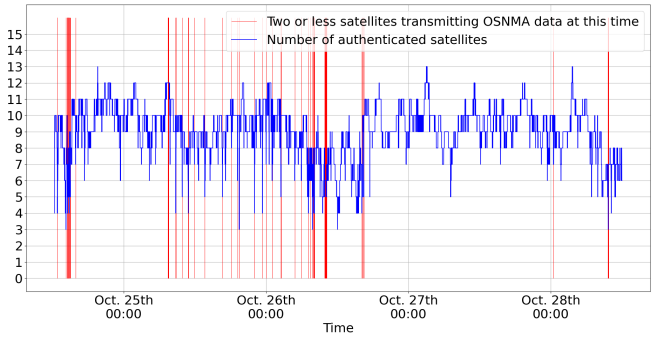

Figure 6: Number of authenticated satellites plotted over time. The times when only two or less satellites are transmitting OSNMA data are marked with a red vertical line.

Table IV: Statistics related to OSNMA data transmission. Most of the time the number of satellites transmitting OSNMA data is adequate to facilitate fully authenticated fixes, but there are occasional drops in this number.

Statistic	**Value**
Number of satellites transmitting OSNMA data: average	5.49
Number of satellites transmitting OSNMA data: 1% percentile	2
Number of satellites transmitting OSNMA data: 5% percentile	3
Number of satellites transmitting OSNMA data: 95% percentile	7
Percentage of time one or less satellites transmit OSNMA data	0.3%

V. Discussion

As can be seen from the results, OSNMA enabled authenticated positioning 99.74% of the time in our experiments in open-sky and high satellite visibility conditions. With respect to the cases in which it was not possible to reach an authenticated fix, we observed that there were mainly two causes.

First of all, when the satellite elevation is low, the signal quality is degraded, which will cause some navigation pages to be corrupted. Consequently, this will cause some subframes to be incomplete. This is of course not related to the OSNMA specification and similar effects can be expected in any satellite-based application. We highlight that for real-world

applications, it is beneficial that the OSNMA implementation extracts any usable data from the subframe, incomplete or not. Even incomplete subframes are likely to contain useful data. Therefore, it is better to process the data on a page level, instead of subframe level.

We now list a few ways in which dropped pages can affect the OSNMA performance.

- The data in the HKROOT message does not require fast reaction, not to mention that the root key (contained in the HKROOT) message transmission uses redundancy: all of the satellites transmitting OSNMA data will transmit the same message, but they transmit the blocks in different order. This makes the root key transmission both fast and robust. Therefore, the impact of receiving an incomplete HKROOT message from one satellite is not very significant. Some information from the HKROOT message is required to start the authentication process. Therefore a delay in parsing the HKROOT due to an incomplete subframe will cause a delay in the first set of authentications. However, in the so-called hot start case (which is the usual one) the receiver has stored a previous HKROOT, and as long as the TESLA key chain does not change, the receiver can start the authentication immediately without the need to wait for the HKROOT messages. Therefore, moderate navigation page drops have little effect on the HKROOT processing.
- If the key (contained in the MACK message) in the subframe is incomplete, it is not possible to authenticate the previous set of tags immediately. However, all of the satellites transmit the same key, not to mention that the receiver may wait for the next key from which it can recover the missing key with hash iteration. Therefore, page drops affecting the key have minimal effect.
- The tags are the critical part of the transmission: they are the most important part of the authentication process and cannot be recovered later. The tags are naturally independent of each other, meaning that even if some of the tags are missing due to dropped pages, the others can still be extracted. Also, multiple satellites may transmit a tag for the same satellite. Therefore, OSNMA offers some redundancy for protecting the data. We consider missing tags due to dropped pages to be the worst case scenario. However, in our experiments we found barely any problem with this.

The second reason for failures found during the analysis of our dataset was that the number of (visible) satellites transmitting OSNMA data occasionally dropped quite low. This behaviour was also noted in [9]. This acts as a bottleneck for OSNMA performance, as each satellite transmitting OSNMA data can only cross-authenticate a limited number of other satellites. In our favorable environmental conditions (open sky), the impact of this was minimal, but it can become critical in applications where the satellite visibility is poor. In particular, our elevation mask studies showed that the elevation mask can have a significant impact on OSNMA performance.

Another important note is that the application of an elevation mask results in valuable authentication information being discarded from some satellites. In that sense, we note that, while receivers commonly apply a 5-15 degree elevation mask in the tracking and/or PVT computation phases, it is better not to apply the same mask to OSNMA processing. While the positioning accuracy is known to get better after applying an appropriate satellite elevation mask, for OSNMA processing having more data available for processing is better. A low elevation satellite might still cross-authenticate other satellites, and as previously noted, the number of satellites transmitting OSNMA data is occasionally very low. In these cases, discarding that information can have a significant impact.

VI. Conclusions

In the analysis of our 4-day long dataset, we observed that 99.74% of the time a receiver would be able to produce authenticated fixes. The cases where an authenticated status could not be attained were mostly due to having a low number of satellites transmitting OSNMA data available to the receiver. While in our open-sky dataset this had little impact on the overall OSNMA performance, we suspect that this can have a great effect in a more challenging environments, such as in urban environments where the satellite visibility might be significantly degraded. This potential performance degradation was further suggested by our studies involving elevation masks. For example, applying a 30°elevation mask resulted in a decrease of the percentage of authenticated fixes from 99.74% to 66.83%. On the receiver side, it would be beneficial not to discard data from satellites with low elevation: while using these satellites in the PVT computation might not be beneficial, using the OSNMA data that they carry increases the chances of cross-authenticating visible satellites, which in turn will makes more authenticated satellites available to the PVT engine. In addition, in the OSNMA service side, increasing the number of satellites that are transmitting OSNMA data will consequently increase the overall probability of attaining authenticated fixes, which would be especially beneficial in obstructed environments.

Acknowledgment

This work was conducted in the scope of the ESRIUM Project, which has received funding from the EUSPA as part of EU-Horizon 2020 research and innovation programme under grant agreement No 101004181.

References

[1] E. Union, "OSNMA user ICD for the test phase, issue 1.0," European Union, Tech. Rep., Nov. 2021.
[2] "ESRIUM project web page," https://esrium.eu/, accessed: 2023-01-31.
[3] I. Fernández-Hernández, T. Ashur, V. Rijmen, C. Sarto, S. Cancela, and D. Calle, "Toward an operational navigation message authentication service: Proposal and justification of additional OSNMA protocol features," apr 2019.
[4] I. Fernández-Hernández, V. Rijmen, G. Seco-Granados, J. Simon, I. Rodríguez, and J. D. Calle, "A navigation message authentication proposal for the galileo open service," *Navigation*, vol. 63, no. 1, pp. 85–102, mar 2016.

[5] D. Margaria, G. Marucco, and M. Nicola, "A first-of-a-kind spoofing detection demonstrator exploiting future galileo E1 OS authentication," apr 2016.

[6] B. Motella, M. Nicola, and S. Damy, "Enhanced GNSS authentication based on the joint CHIMERA/OSNMA scheme," *IEEE Access*, vol. 9, pp. 121 570–121 582, 2021.

[7] M. Motallebighomi, H. Sathaye, M. Singh, and A. Ranganathan, "Cryptography is not enough: Relay attacks on authenticated GNSS signals," *arXiv preprint arXiv:2204.11641*, 2022.

[8] C. O'Driscoll and I. Fernández-Hernández, "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+ 2020)*, 2020, pp. 3751–3765.

[9] M. Nicola, B. Motella, M. Pini, and E. Falletti, "Galileo OSNMA public observation phase: Signal testing and validation," *IEEE Access*, vol. 10, pp. 27 960–27 969, 2022.

[10] M. T. Gamba, M. Nicola, and B. Motella, "Computational load analysis of a galileo OSNMA-ready receiver for ARM-based embedded platforms," *Sensors*, vol. 21, no. 2, p. 467, jan 2021.

[11] B. Motella, M. T. Gamba, and M. Nicola, "A real-time OSNMA-ready software receiver," feb 2020.

[12] M. T. Gamba, M. Nicola, and B. Motella, "Galileo OSNMA: an implementation for ARM-based embedded platforms," jun 2020.

[13] ——, "Computational load analysis of a galileo OSNMA-ready receiver for ARM-based embedded platforms," *Sensors*, vol. 21, no. 2, p. 467, jan 2021.

[14] L. Cucchi, S. Damy, M. Paonni, M. Nicola, M. T. Gamba, B. Motella, and I. Fernandez-Hernandez, "Assessing galileo OSNMA under different user environments by means of a multi-purpose test bench, including a software-defined GNSS receiver," oct 2021.

[15] C. Sarto, O. Pozzobon, S. Fantinato, S. Montagner, I. Fernández-Hernández, J. Simon, J. D. Calle, S. C. Díaz, P. Walker, D. Burkey, G. Seco-Granados, and E. Göhler, "Implementation and testing of OSNMA for galileo," nov 2017.

[16] L. Cucchi, S. Damy, M. Paonni, M. Nicola, and B. Motella, "Receiver testing for the galileo E1 OSNMA and I/NAV improvements," in *Proceedings of the 35th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2022)*, 2022, pp. 808–819.

[17] S. Damy, L. Cucchi, and M. Paonni, "Impact of OSNMA configurations, operations and user's strategies on receiver performances," in *Proceedings of the 35th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2022)*, 2022, pp. 820–827.

[18] S. Cancela, J. D. Calle, and I. Fernández-Hernández, "CPU consumption analysis of TESLA-based navigation message authentication," in *2019 European Navigation Conference (ENC)*. IEEE, 2019, pp. 1–6.

[19] G. Seco-Granados, D. Gómez-Casco, J. A. López-Salcedo, and I. Fernández-Hernández, "Detection of replay attacks to GNSS based on partial correlations and authentication data unpredictability," *Gps Solutions*, vol. 25, no. 2, p. 33, 2021.

[20] S. Cancela, J. Navarro, D. Calle, T. Reithmaier, A. D. Chiara, G. D. Broi, I. Fernández-Hernández, G. Seco-Granados, and J. Simón, "Field testing of GNSS user protection techniques," in *Proceedings of the 32nd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2019)*, 2019, pp. 1824–1840.

[21] A. Galan, I. Fernandez-Hernandez, L. Cucchi, and G. Seco-Granados, "OSNMAlib: An open python library for galileo OSNMA," in *2022 10th Workshop on Satellite Navigation Technology (NAVITEC)*, 2022, pp. 1–12.

[22] D. Estevez, "galileo-osnma," https://github.com/daniestevez/galileo-osnma, 2022.

[23] "osnmaPython," https://github.com/astromarc/osnmaPython, 2023.

[24] Septentrio, "Release notes and installation guide of the mosaic-x5 firmware package v4.12.1," https://www.septentrio.com/system/files/support/mosaic-x5_firmware_v4.12.1_release_notes.pdf, 2023, [Retrieved 1-March-2023].

[25] A. Perrig, J. Tygar, A. Perrig, and J. Tygar, "TESLA broadcast authentication," *Secure Broadcast Communication: In Wired and Wireless Networks*, pp. 29–53, 2003.

[26] K. Eledlebi, C. Y. Yeun, E. Damiani, and Y. Al-Hammadi, "Empirical studies of TESLA protocol: properties, implementations, and replacement of public cryptography using biometric authentication," *IEEE Access*, vol. 10, pp. 21 941–21 954, 2022.

[27] E. Union, "OSNMA receiver guidelines for the test phase, issue 1.0," European Union, Tech. Rep., Nov. 2021.

[28] Septentrio, "mosaic-x5 reference guide," Tech. Rep., Apr. 2022, applicable to version 4.12.1 of the Firmware.