engineering proceedings

MDPI

Proceeding Paper

Sensitivity analysis of Galileo OSNMA cross-authentication sequences†

Aleix Galan [1,*], Cillian O'Driscoll [2], Ignacio Fernandez-Hernandez [3], and Sofie Pollin [1]

[1] KU Leuven, 3000 Leuven, Belgium; aleix.galan@kuleuven.be (A.G.), sofie.pollin@kuleuven.be (S.P.)
[2] Independent Consultant, Cork, Ireland; cillian@codc.ie
[3] DG DEFIS, European Commission, Brussels, Belgium; ignacio.fernandez-hernandez@ec.europa.eu
* Correspondence: aleix.galan@kuleuven.be
† Presented at the European Navigation Conference 2024, Noordwijk, The Netherlands, 22-24 May 2024.

Abstract: Galileo Open Service Navigation Message Authentication (OSNMA) has been transmitted stably over the last years and is expected to be declared operationally in the next months. While the protocol is very flexible, most of the parameters, such as key and tag sizes and cryptographic functions, have been already fixed in view of the operational declaration. However, some degree of flexibility remains in the tag and cross-authentication sequence. The cross-authentication sequence defines the satellites "cross-authenticated" by an authenticating Galileo satellite and is one of the main properties of the OSNMA protocol. It allows authenticating nearby Galileo satellites for higher redundancy against losses, authenticating data from satellites not connected to ground and therefore not transmitting OSNMA, and authenticating GPS or other data in the future. It has a significant impact on OSNMA performance: if the sequence is too long, many cross-authenticated satellites will not be seen by the users, limiting the optimal use of the OSNMA bandwidth, and with major impact in TBA (Time Between Authentications) and Time To First Authenticated Fix (TTFAF). If the sequence is too short, several non-connected but visible satellites may remain unauthenticated, also degrading performance. This paper presents an analysis with real SIS data from different cross-authentication sequences transmitted by Galileo over the last months, involving different tag distribution and number of cross-authenticated satellites including open-sky static, dynamic and urban environments. The work shows the degradation with sub-optimal cross-authentication sequences and identifies current bottlenecks, proposing some recommendations for future sequences.

Keywords: GNSS; Galileo; OSNMA; Spoofing; Authentication

1. Introduction

Galileo OSNMA (Open Service Navigation Message Authentication) [1] is an anti-spoofing technique based on the authentication of the navigation message bits. It has been transmitted in test mode over the past 2 years in the Galileo E1-B signal, allowing to authenticate navigation messages received in both the E1-B and E5b carriers. OSNMA is already working and is expected to be declared operational in the following months, making Galileo the first GNSS constellation to protect its civilian signal.

OSNMA applies the concept of time-binding, where unpredictable bits (message authentication code tags) are transmitted as part of the navigation message and are authenticated at a later time by disclosing a key. A spoofer willing to forge the signal cannot generate these bits in advance because it lacks the knowledge of the key. In OSNMA, the keys are authenticated using consecutive hashes in a variation of the TESLA (Time Efficient Stream Los-Tolerant Authentication) protocol [2]. The tags authenticate parts of the navigation message bits and are a flexible parameter of OSNMA.

Citation: To be added by editorial staff during production.

Academic Editor: Firstname Lastname

Published: date

Similar anti-spoofing schemes are foreseen for other GNSS constellations. GPS is planning to implement Chimera (Chip Message Robust Authentication) in their new generation of civilian signals, GPS L1C [3]. Chimera will authenticate the navigation message, like OSNMA, and the spreading code for integral signal protection. Recently, the Japanese constellation QZSS announced its own signal authentication service [4]. The service aims to authenticate their navigation message and the navigation message of other GNSS constellations but at the expense of a higher latency.

The performance of the cryptographic techniques described above is strongly dependent on the GNSS constellation provider. The selection of appropriate parameters for transmitting the authentication data impacts all users willing to authenticate their position, velocity, and time. In this paper, we explore how a change in the sequence followed by OSNMA when transmitting tags to authenticate other satellites improved the general performance of the protocol. We use live data recorded before and after the sequence change in open sky and urban dynamic environments to analyze the improvement and characterize the wasted transmission bandwidth with the previous sequence.

2. OSNMA Cross-Authentication

2.1 Cross-Authentication Overview

Due to the position of the Galileo ground stations on the Earth's surface, not all constellation satellites can transmit the OSNMA cryptographic data simultaneously. We will refer to a satellite transmitting OSNMA as *connected* and a satellite not transmitting it as *disconnected*. To authenticate the disconnected satellites, the connected satellites send authentication tags for themselves and authentication tags for disconnected satellites, the so-called cross-authentication tags. Although, in theory, the cross-authentication technique could be used to authenticate other constellations or services, they are currently used only for disconnected Galileo satellites. It must be noted that, in the first blueprints, it was possible to cross-authenticate also connected satellites [5].

The tags in OSNMA are organized into 3 categories (or ADKD) depending on the data they authenticate and the key they use. The ADKD 0 authenticates the satellite ephemerides, ionosphere model, and health flag: all the necessary information to authenticate a satellite. The ADKD 12 authenticates the same information but with a key disclosed with a five-minute delay. Lastly, the ADKD 4 authenticates the time parameters common in the constellation.

The transmission of tags in the OSNMA message is defined in a sequence that lasts 2 subframes. Each position of the sequence indicates the ADKD of the tag and if the tag is self-authenticating (*S*) or cross-authenticating (*E*). There are also positions with a flexible tag type (*FLX*), which the receiver must verify using a different method. In this work, we are interested in the cross-authentication ADKD 0 tags, or 00E in the sequence. A complete description of the OSNMA protocol can be found in the interface control document [6].

2.2 Cross-Authentication Algorithm Change

On December 1st, 2023, OSNMA changed the tag sequence and replaced three 00E positions with FLX positions, although they are currently solely used for 00E tags. However, they also changed the algorithm to assign satellites to the 00E positions. In the sequence before the change, Sequence 1, the 00E spots were assigned to disconnected satellites in order of increasing distance from the connected satellite transmitting them. Therefore, the closest disconnected satellite was selected for the first 00E position, the second closest for the second position, and so on until the sixth closest to the sixth position. See the diagram of the Sequence 1 and the cross-authentication tag distribution in Figure 1. The problem with this algorithm was that tags for the last positions were frequently issued for satellites under the horizon. Also, there was a clear imbalance between subframes: the first subframe of Sequence 1 was getting the tags for the closest satellites, while some tags on the second subframe were not used.

With the new sequence, Sequence 2, the six positions are filled with only the four closest disconnected satellites. The first subframe of the sequence does not change and sets the three closest satellites in the three available positions, while in the second subframe the sequence loops and sets the first and second closest satellites again (Figure 1). With this approach, both subframes of the sequence are more balanced, and less tags are issued for satellites under the horizon. During the last months we have seen small variations in the sequences, but all of them have transmitted two tags for the closest cross-authenticated satellites in each subframe.

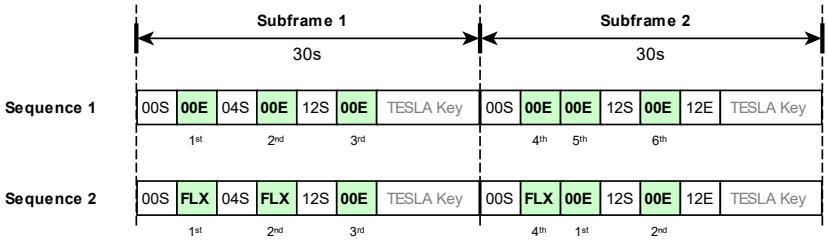


Figure 1. Tag position and distribution of cross-authentication tags for each of the two OSNMA sequences.

To exemplify how both algorithms work we are using real data recorded in November 2023 with Sequence 1 in force and simulating how would the same scenario be with Sequence 2. The results are shown in Figure 2, where the cross-authenticating tags for satellite E07 are displayed as arrows to those satellites. When following the order for Sequence 1, two of the three cross-authentication tags of the second subframe are issued for satellites under the horizon (E34 and E13). However, when using Sequence 2 order, those two positions are used to authenticate the two closest disconnected satellites again. This is a huge improvement since, otherwise, a receiver would have to wait for another 30 seconds (one subframe) to authenticate the closest satellites.

(**a**) (**b**)

Figure 2. Skyplot showing how the satellite E07 is cross-authenticating the disconnected Galileo satellites. The blue box marks those satellites transmitting OSNMA. (**a**) Cross-authentication as recorded in November 2023 with the algorithm of Sequence 1. (**b**) Simulated cross-authentication using the new algorithm of Sequence 2.

3. Open-Sky Static Scenario

To evaluate the impact of the change of sequence for an open-sky scenario we have used recorded data for several hours and days in a static, open-sky location in Cork, Ireland. Table 1 shows a summary of the cross-authentication results, including four captures in August 2023 using Sequence 1 and a single capture in December 2023 using Sequence 2. The table also shows the percentage of cross-authenticated MACs below 0º elevation. As can be seen, the Second Subframe (i.e. that including cross-authenticated satellites 4 to 6) cross authentications refer to satellites below the horizon approximately 70 to 90 % of the time. It is very rare (typically < 1% of the time) that cross-authentications in Subframe 2 provide information that has not already been provided in Subframe 1 (i.e. that including cross-authenticated satellites 1 to 3). Therefore, analyzing over 100 hours of recorded data at a single user location, we observed that over 50 % of the cross-authentication MACs observed by the user were below the horizon, and that 70 to 90 % of the data authenticated in Subframe 2 comes from satellites below the horizon.

Figure 3a and 3b show the CDF of all cross-authentication positions in the sequence, for Sequence 1 and Sequence 2, where Sequence 1 corresponds to the 16 Aug 2023 data capture. While in Sequence 1 about 60% of the cross-authenticated satellites are below 0 degrees of elevation, in Sequence 2 this number is reduced to 30%.

Note also that the impact of the sequencing can be clearly seen in the CDF, where the positions for the "closer" satellites are more frequently at higher elevation. The lines corresponding to the position of the closest satellite in the first and second subframe do not fully overlap because of the variations in the order mentioned in Section 2.2.

Table 1. Summary of cross authentication results from all tests.

Date	Duration	% Cross Auth MACS < 0° Elevation			% Subframe 2 MACs not in Subframe 1
			First Subframes	Second Subframes	
14 Aug 2023	~7.5 hrs	65%	40%	80%	0.12%
16 Aug 2023	~16 hrs	50%	30%	70%	1.03%
18 Aug 2023	~50 hrs	70%	50%	90%	0.02%
21 Aug 2023	~42 hrs	65%	50%	80%	0.19%
21 Dec 2023	~24 hrs	24%	23%	25%	0.06 %

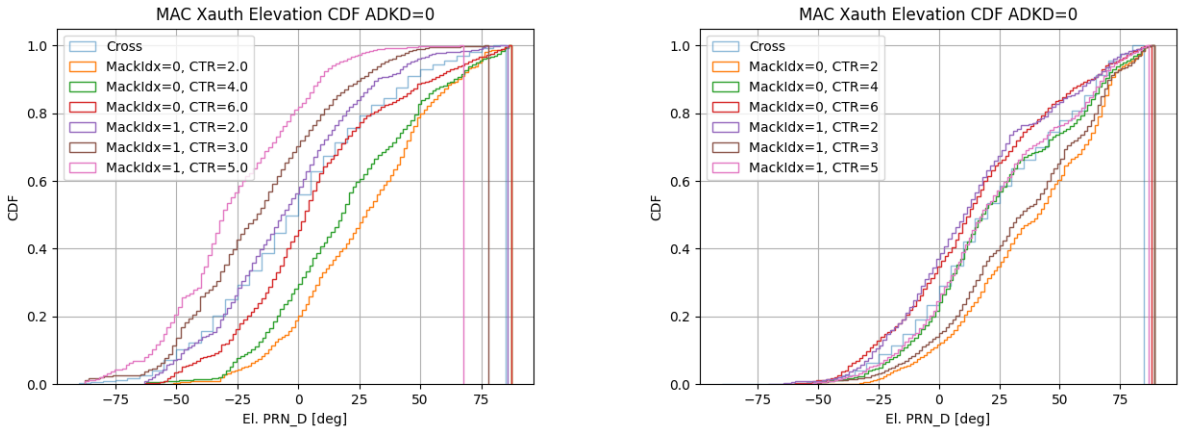


Figure 3. Comparison of two cross-authentication sequences observed at a single point on the Earth's surface. For Sequence 1 (**a**), approximately 60 % of the cross-authenticated satellites seen are below the horizon. For Sequence 2 (**b**), this drops to < 30%.

4. Urban Dynamic Scenarios

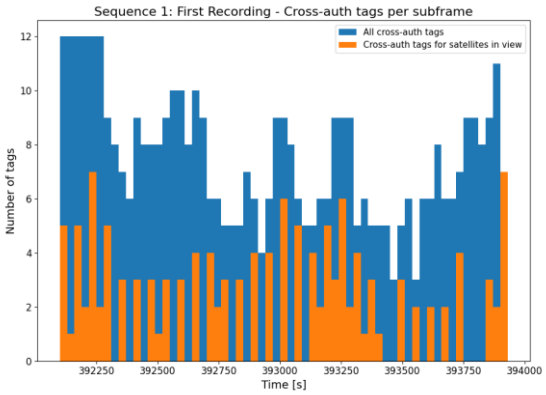
In urban dynamic scenarios, the satellite visibility elevation is not constant at the horizon since physical structures obfuscate the view. Therefore, instead of using the same approach as with the open-sky scenario, we register if a satellite targeted by a cross-authentication tag was in view in the last 30 seconds (one subframe).

To register the live data, we walked in Brussels, Belgium, using a Septentrio mosaic-X5 [7] with firmware version 4.14.0 to log the navigation data bits of Galileo E1-B. The locations chosen were a mix of hard urban, soft urban, and parks. We recorded data in the morning and afternoon for each sequence to have scenarios with different constellation geometry. The log files were then post-processed using the OSNMAlib [8,9] software to extract the OSNMA information.

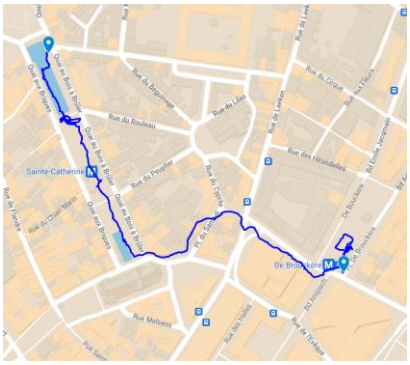
4.1 Live Recordings with Sequence 1

The recordings for Sequence 1 were done on November 30, 2023, exactly one day before the sequence changed. The first recording has a duration of 30 minutes, from 12:54:42 to 13:24:42 UTC. The trajectory followed is shown in Figure 4a and includes a park environment and a narrow street. The second recording has a duration of 30 minutes, from 16:40:37 to 17:10:37 UTC. The trajectory, shown in Figure 4c, comprises narrow streets at the beginning and a more open boulevard at the end of the scenario.

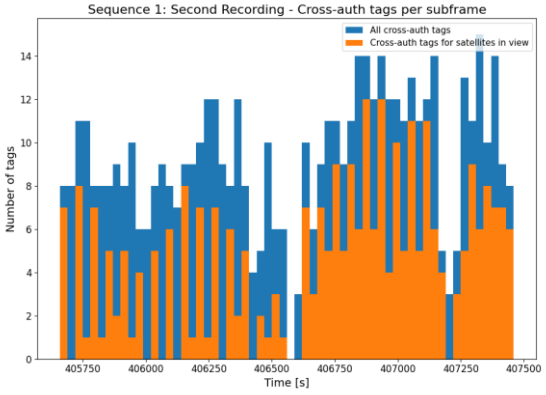
(**a**)



(**b**)



(**c**)



(**d**)

Figure 4. Live recordings for Sequence 1, on November 30, 2023. (**a**)(**c**) Trajectory followed in the recordings. (**b**)(**d**) Total cross-authentication tags and the subset received for a satellite in view in the last 30 seconds. The effect of the good and bad subframes is visible in the alternation of orange bars.

The effect of Sequence 1, with the second subframe having the cross-authentication tags for the further away satellites, is clearly visible in the alternation of orange bars for both recordings (Figure 4b and 4d). Even in the sections of the trajectory with better

visibility some subframes are completed without receiving any cross-authentication tag for a satellite seen in the last 30 seconds.

4.2 Live Recordings with Sequence 2

The recordings to evaluate Sequence 2 were done on December 3, 2023, two days after the sequence change. The routes followed are similar to the recording with sequence 1, but not the same because we collected the data for different purposes before noticing the change in the algorithm. Nonetheless, they include similar situations to the Sequence 1 recordings such as parks and urban canyons. Further analyses of this recording, with focus on OSNMA TTFAF, are presented in [10]. This reference also shows that the cross-authentication sequence may penalize TTFAF due to the imbalance between tags, which favors disconnected satellites, often not visible.

The first recording has a duration of 32 minutes, from 09:49:42 to 10:21:42 UTC. The trajectory is displayed in Figure 5a, and includes the soft urban environment of a park and a long urban canyon with high buildings. The second recording has a duration of 27 minutes, from 13:23:32 to 13:50:32 UTC. The trajectory (Figure 5c) follows some narrow streets in the Brussels old town, briefly entering the Grand-Place. While the visibility was generally low in both recordings, which impacts the total number of tags received, there is no perceived difference between consecutive subframes (Figure 5b and 5d).

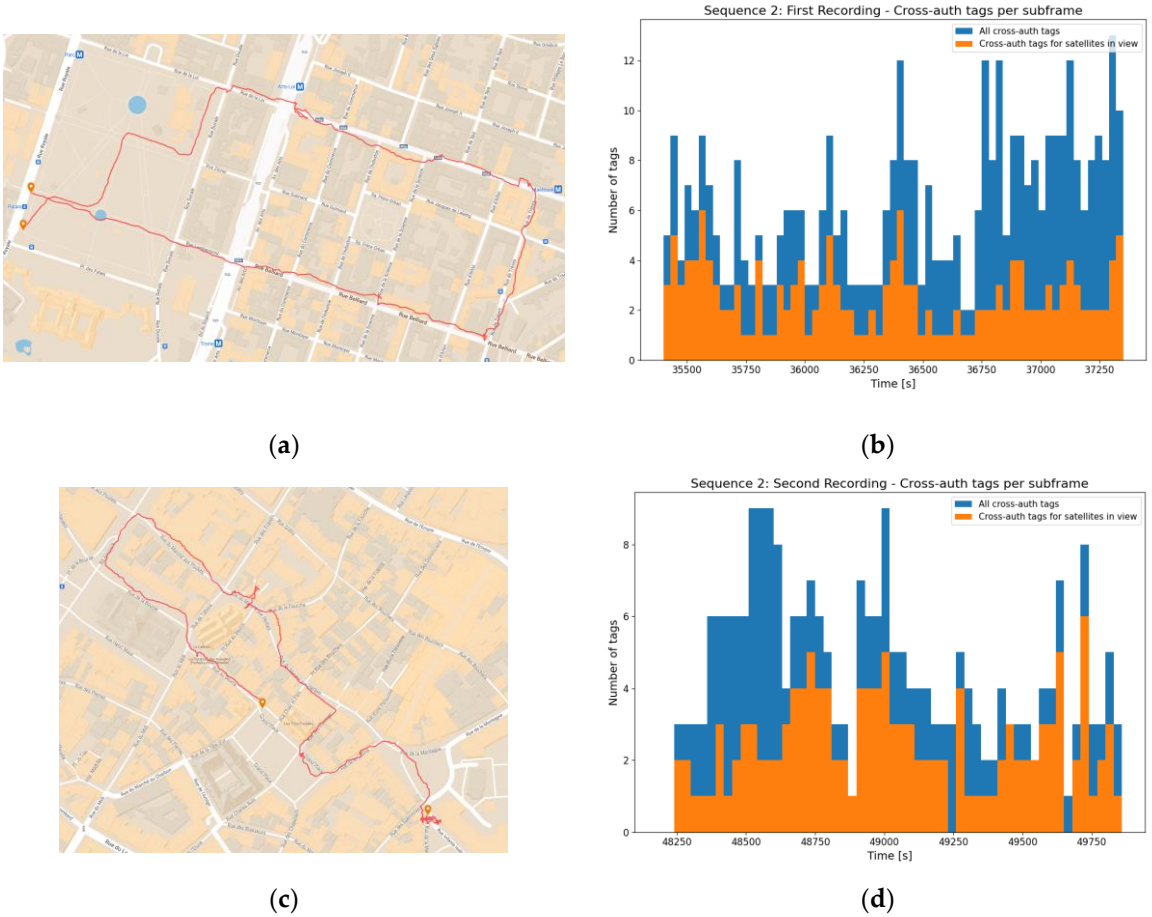


Figure 5. Live recording for Sequence 2, on December 3, 2023. (**a**)(**c**) Trajectory followed in the recordings. (**b**)(**d**) Total cross-authentication tags and the subset received for a satellite in view in the last 30 seconds. There is no clear difference between consecutive subframes.

4.3 Direct Comparison Between Sequences

To empirically compare both sequences, we have calculated the percentage of cross-authentication tags received for satellites in view, and then grouped them into each of the two subframes of a sequence. The data is displayed in Table 2 and visually in Figure 6.

The improvement is clear when comparing Sequence 1 and Sequence 2 recordings. In the first recording of Sequence 1, only 8% of the cross-authentication tags are issued in the second subframe for satellites in view. In the second recording for Sequence 1, where the visibility is a bit better, only 28% of the cross-authentication tags are useful. That means less than 1 tag per subframe, since there are 3 positions for those tags in each subframe.

For Sequence 2, the new algorithm works in balancing both subframes and the difference is minimal between the first and second subframe of the sequence. The results are expected since the only difference between the two subframes is that, in the first subframe, the third cross-authentication tag position transmits a tag for the third closest, and, in the second subframe, for the fourth.

Moreover, the results show no tangible difference between each sequence's morning and afternoon recordings. The difference in geometry and environment of the different recordings affect the percentage values, but there is no difference in the ratio between subframes.

Table 2. Percentage of cross-authentication tags received for satellites in view in the past 30 seconds.

Recording	All Subframes	First Subframes	Second Subframes
Sequence 1 – Recording 1	29%	50%	8%
Sequence 1 – Recording 2	52%	76%	28%
Sequence 2 – Recording 1	41%	42%	41%
Sequence 2 – Recording 2	54%	54%	53%

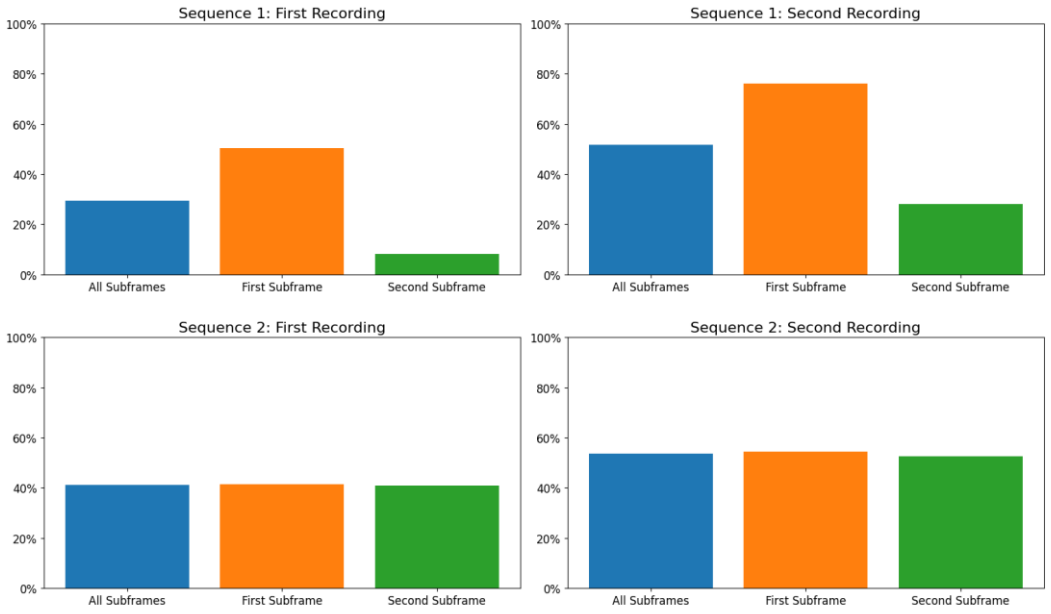


Figure 6. Percentage of cross-authentication tags received for satellites which were in view in the past 30 seconds. Sequence 1 had an imbalance between the first and second subframe of the sequence, while the new algorithm for Sequence 2 fixed the problem.

4.4 Time Between Authentication (TBA)

The direct impact of each sequence for a user willing to use OSNMA can be analyzed using the Time Between Authentication (TBA) for the cross-authenticated satellites seen during the scenario. To do so, we have postprocessed the data using OSNMAlib and

recorded the time when the navigation data for each disconnected satellite was authenticated. By doing it this way we can simulate a real OSNMA execution, as we consider changes of navigation data and the state-of-the-art optimizations included in the library.

The results in Figure 7 show the clear improvement of the new sequence in reducing the mean TBA from 45 to 33 seconds. The reduction is due to the transmission of cross-authentication tags for the two closest satellites on the second subframe of the sequence. With the first sequence, those satellites had to wait for an extra subframe (60 seconds in total) to receive a new tag.

In an open sky scenario, because of the high number of satellites in view, the connected satellites would cover all the disconnected satellites. However, the reduced visibility of the urban scenario demands for a better optimized sequence to not affect the TBA.

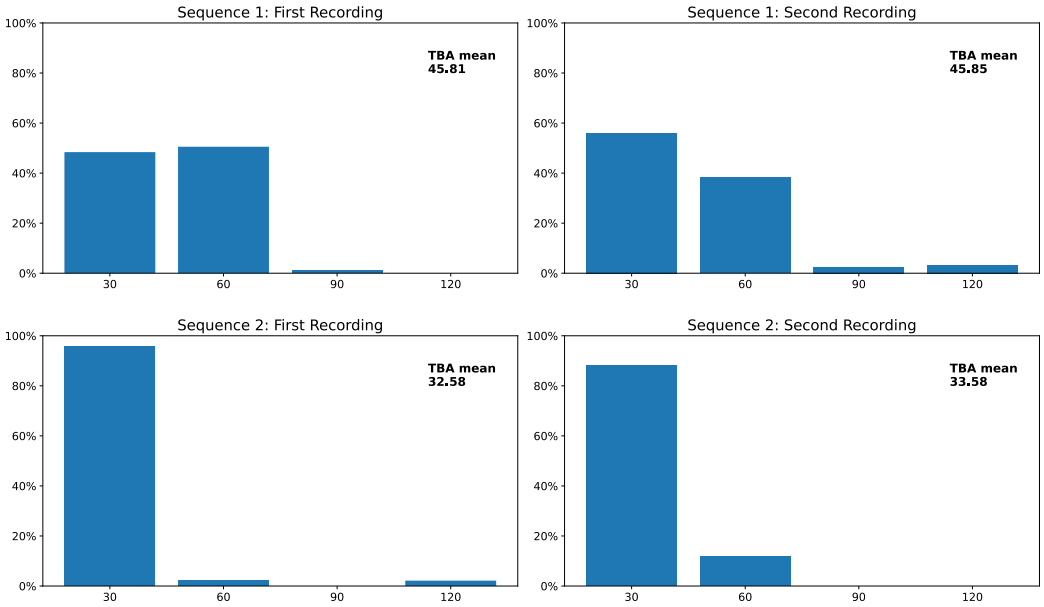


Figure 7. Time between authentications for the disconnected satellites. With the first sequence, several satellites had to wait for 2 subframes (60 seconds) to be authenticated again because no tags were issued for them.

5. Conclusions

The adequate selection of the cross-authentication tag sequence clearly impacts the OSNMA protocol's performance. With the previous Sequence prior to December 2023 including six cross-authenticated satellites, a receiver starting up on the second subframe of the sequence needed to wait for an extra subframe to authenticate the closest disconnected satellites, degrading the authentication metrics. The imbalance between subframes is solved with the new Sequence, where tags for the two closest disconnected satellites are always transmitted regardless of the subframe. With the new Sequence, the cross-authenticated satellites received below zero-degree elevation are reduced from around 50% to 30% at the analyzed location in Cork, Ireland and mean TBA is reduced from around 45 to 33 seconds.

Future work to better characterize OSNMA cross-authentication sequences may include: estimating below-zero-degree cross-authentications in other locations, or globally through a service volume simulator, at different user elevation masks and conditions; metrics the user-received tag frequency for connected and disconnected satellites to avoid tag imbalances; and extend field testing, possibly including ADKD12. Future tag sequence optimizations may consider cross-authenticating tags for connected satellites, or developing sequences based not only on connected nearest neighbors but also on satellite-to-user

geometry, maximizing user performance; or optimizing tag positions in the sequence to reduce TTFAF.

Author Contributions Conceptualization, C.D., A.G., I.F., S.P.; software, A.G, C.D.; writing—original draft preparation, A.G., C.D., I.F.

Funding: This research was partially funded by the Research Foundation Flanders (FWO) Frank de Winne PhD Fellowship, project number 1SH9424N (A.G.).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data presented in this study are available upon request to the corresponding author.

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

References

1. Fernández-Hernández, I., Rijmen, V., ...& Calle, J. D. (2016). A navigation message authentication proposal for the Galileo open service. NAVIGATION: Journal of the Institute of Navigation, 63(1), 85-102.
2. Perrig, A., Tygar, J. D., Perrig, A., & Tygar, J. D. (2003). TESLA broadcast authentication. Secure Broadcast Communication: In Wired and Wireless Networks, 29-53.
3. Anderson, J., Carroll, K., ... & Scott, L. Chips-Message Robust Authentication (Chimera) for GPS Civilian Signals. In Proceedings of the 30th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2017), Portland, Oregon, September 2017, pp. 2388-2416. https://doi.org/10.33012/2017.15206
4. QZSS-SAS. Available online: https://qzss.go.jp/en/overview/services/sv14_sas.html (accessed on 10 May 2024).
5. Walker, P., Rijmen, V., ... & Pozzobon, O. (2015, September). Galileo open service authentication: a complete service design and provision analysis. In Proceedings of the 28th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2015) (pp. 3383-3396).
6. OSNMA Signal-in-Space Interface Control Document (SIS ICD) Issue 1.1. Available online: https://www.gsc-europa.eu/sites/default/files/sites/all/files/Galileo_OSNMA_SIS_ICD_v1.1.pdf (accessed 10 May 2024).
7. Septentrio mosaic-X5 GNSS receiver module. Available online: https://www.septentrio.com/en/products/gps/gnss-receiver-modules/mosaic-x5 (accessed on 10 May 2024).
8. OSNMAlib. Available online: https://github.com/Algafix/OSNMA (accessed on 10 May 2024).
9. A. Galan, I. Fernandez-Hernandez, L. Cucchi and G. Seco-Granados. OSNMAlib: An Open Python Library for Galileo OSNMA. In Proceedings of the 2022 10th Workshop on Satellite Navigation Technology (NAVITEC), Noordwijk, Netherlands, 2022, pp. 1-12, doi: 10.1109/NAVITEC53682.2022.9847548.
10. Galan, A., Fernandez-Hernandez, I., De Wilde, W., Pollin, S., & Seco-Granados, G. (2024). Improving Galileo OSNMA Time To First Authenticated Fix. *arXiv preprint arXiv:2403.14739*.