Increasing the Robustness of Drone Operations with Galileo Open Service Navigation Message Authentication (OSNMA)

Sophie Damy
Joint Research Centre
European Commission
Ispra, Italy
sophie.damy@ec.europa.eu

Luca Cucchi
Joint Research Centre
European Commission
Ispra, Italy
luca.cucchi@ec.europa.eu

Alberto Mennella
TopView S.r.l
San Nicola La Strada, Italy
alberto.mennella@topview.it

Gianluca Luisi
TopView S.r.l
San Nicola La Strada, Italy
gianluca.luisi@topview.it

Matteo Paonni
Joint Research Centre
European Commission
Ispra, Italy
matteo.paonni@ec.europa.eu

Ignacio Fernandez-Hernandez
DG DEFIS
European Commission
Brussels, Belgium
ignacio.fernandez-hernandez@ec.europa.eu

***Abstract*— As drones are being increasingly used in liability and safety related applications, the trust that can be put in the information they are reporting, in particular regarding their position, is becoming crucial. This paper demonstrates, using real data collected on-board a drone, how Galileo navigation data authentication service can contribute to increase the robustness of the position reported.**

Keywords—drone, authentication, Galileo OSNMA, spoofing

I. Introduction

The rising number of drones accessing the airspace and the increased complexity of their operations in BVLOS (Beyond Visual Line Of Sight) conditions, led to the introduction of additional specific rules and procedures for their use (i.e., EU regulatory package 2021/664 U-space [1]). In this scenario, a solution that ensures the authenticity of the position information is needed for all the U-space stakeholders, especially for safety-related and commercially valuable applications. Moreover, different standardization groups as ISO, EUROCAE, ASTM are working worldwide on the standardization of Unmanned aircraft system Traffic Management (UTM)/U-space services related to strategic, tactical, and post-flight phases of flight for drones' operations. For instance, the UTM services described in ISO 23629-12 [2] have already standardized in the Annex C, a list of operation support services such as Digital LogBook (DLB), Accident and Incident Reporting (ARS) and Legal Recording Service (LRS). In this context, key enabling European GNSS (EGNSS)/U-spaces services are needed to support safe and efficient navigation of Unmanned Aircraft Systems (UASs) especially in BVLOS conditions, where most of the business of UAS operations is expected. In fact, UAS applications in Urban Air Mobility (UAM) ecosystem as medical biological samples transportation, package delivery, taxi UAS service or industrial inspections require the consolidation of the abovementioned services and the creation of new ones, to fully unlock UAS operations thus intercepting a latent business opportunity.

For such UTM/U-space standardized services, the Galileo Open Service Navigation Message Authentication (OSNMA), in combination with other technologies such as the blockchain, may represent the perfect combination for a robust implementation of such services. With OSNMA, Galileo provides the means to authenticate the navigation data transmitted by its satellites. It enables the receiver to verify that the data received was indeed generated by the system and was not modified. Galileo OSNMA is the first contribution of a GNSS system to provide authentication on its open service. In fact, OSNMA may be used to guarantee authenticity of positioning and time data at the very origin, while blockchain will ensure over time that such data is not counterfeited or altered in the future, thus putting the bases for Legal Recording Services or other services related to business applications. These specific challenges are addressed in the Horizon Europe project CERTIFLIGHT, co-financed by EUSPA under Grant Agreement n. 101082484 and Coordinated by TopView s.r.l [3].

In this paper, we demonstrate how the use of OSNMA can increase the robustness of a receiver on-board a drone to spoofing attacks. The paper is structured as follows: first, the benefits of authentication for drone operations are presented in section II, then in section III, Galileo OSNMA is explained in detail. Section IV describes the test carried out and laboratory set-up used to collect the data and analysed the performance of the OSNMA while the results of this experimentation are presented in section V. Conclusions are provided in section VI.

II. Benefits of Authentication for Drone Operations

The benefits of authentication of position and time for drone operations spread from legal protection services (for pilots and UAS Operators during their mission) to data traceability in auditable form.

For applications of advanced air mobility, the possibility to have UAS's payload data synchronized with authenticated Position, Velocity and Timing (PVT) solution is a strong enabler for business applications where traceability is needed (i.e. Proof of Location or Proof of delivery for package transportation). In industrial applications, authentication of PVT merged with payload data can be useful to certify time and position of anomalies/faults detected, for example over a powerline or over a large photovoltaic plant. In 3D reconstruction models used in the construction domain, such data can also be used

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

as genuine "seeds" for the calculation of volumes and surfaces, or for the generation of "certified" digital twin models.

On the other hand, in the world of autonomous drones, liability in case of accident/incident and the impacts on insurance companies require to address new challenges related to technical, legal and ethics aspects. In this domain, assessing the liability chain for UAS operations is very important. The full traceability of the PVT solution with the telemetry data of UAS, including the logs of the decision undertaken by the UAS autopilot and the effect of the autopilot engagement on flight trajectory, is an important added value for insurance companies. This data is also key in the case of investigataion carried by authorities and institutional agencies, to attribute the respective responsibility in case of disputed events.

Finally, the OSNMA service, coupled with the blockchain structure, represents a key element for enabling killer applications such as UAS flight tracks reports with a legal certainty. This solution paves the way for new disruptive services like smart contracts' activations, i.e., contracts based on the effective flight time of operations or flight positions, or automatically enabled by conditions met during the flight or before take-off. These new applications open up a world of new possibilities not only for UAS operators, but also for U-space service providers and other actors involved in U-space airspace operations.

III. Galileo Open Service Navigation Message Authentication

This section describes the OSNMA protocol at a high level and then explained how OSNMA can be used to increase the robustness of the receiver against certain attacks.

A. OSNMA Principle

In November 2021, Galileo launched the public test phase of OSNMA [4], enabling users worldwide to test their implementation of the OSNMA protocol specified in [5] and [6]. From that day, a subset of Galileo satellites have been transmitting OSNMA data over a 40-bit field in E1-B I/NAV message. OSNMA exploits a light-weight protocol developed for broadcast authentication: the Time-Efficient Stream Loss-Tolerant Authentication (TESLA), defined in [7] and standardized in [8].

The protocol is adapted to GNSS [9] and enables, in particular, the verification of the navigation data through a symmetric function (based on Message Authentication Codes, MAC), secured by the delayed released of the key. Thus, a user receives a truncated MAC or tag, and needs to wait for the corresponding key to be transmitted in order to verify the authenticated data. For this, the receiver is required to be synchronized to the Galileo System Time (GST) through an external time source. In practice, the protocol supports users that are synchronized from within 30 seconds of the GST, up to 5 minutes.

The keys used for the tag verification are part of a one-way chain transmitted in a reverse order to its generation. It implies that each key can be verified against a previously broadcast key. The first key of the chain, referred to as the root key, can be verified through its digital signature, which is transmitted at a low rate across the satellites (120 bits per satellite every 30 seconds). A public key, required for the digital signature verification, can be loaded from the OSNMA server to the receiver. Over the air rekeying processes for both the public key and the TESLA chain are also defined. Fig. 1 represents the OSNMA processing logic

The tags can be used to authenticate different part of the navigation data message and may also be used to authenticate the data from different satellites. In fact, a satellite can transmit a tag authenticating its own data (self-authentication) or the data of a nearby satellite (cross-authentication). This means that even if not all satellites are transmitting OSNMA data, it is still possible for a user to authenticate the navigation data of all satellite in view.

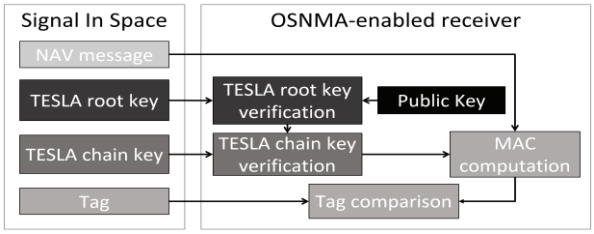

Fig. 1. OSNMA processing overview.

OSNMA is still in a testing phase, to which any interested users can participate. It is expected that the service will be declared operational by the end of 2023. The reference documents, describing the service baseline [10] as well as the guidelines for the implementation of the protocol [11], were published in December 2022.

B. Increasing Receiver Robustness with OSNMA

The unpredictability in the OSNMA bits of the Galileo I/NAV stream derives from the cryptographic nature of the protocol: this represents a game-changer in the receiver resilience and spoofing detection strategies as it makes spoofing attacks harder to succeed. The vast majority of intermediate and simplistic spoofers perform modifications to the navigation data stream, aimed at modifying satellite information. However, as these spoofers do not have the capability to replicate valid OSNMA bits, they will fail to attack Galileo on a receiver correctly implementing the protocol. It is then more likely that an attacker will focus on other constellations not protected by cryptographic-based protocol, also in order to avoid the triggering of possible OSNMA-based detection flags. Such flags can be implemented by the receiver, for example based on the number of observed authentication failures or on the completely and suspicious absence of OSNMA bits. Indeed, once OSNMA enters into service, minimum performance levels are expected to be published, enabling the user to also build a logic around the unavailability of the OSNMA data.

In addition, while OSNMA is currently authenticating only the data from Galileo satellites, it can be leveraged to monitor the PVT solution computed using more constellations, which will be the focus of the next sections. An OSNMA-based solution, exploiting only Galileo satellites, may have a reduced accuracy when compared to a multi-constellation solution, in particular in conditions with limited satellite visibility. While a combined solution, for example using both GPS and Galileo, is expected to yield to better accuracy results, it will be less robust. In particular, as GPS data is not protected, an attacker is likely to decide to only spoof GPS, potentially making the combined solution diverge from the truth.

In order to monitor such behavior, a receiver can compute two PVT solutions:

- An OSNMA-enabled PVT, computed only using satellites which data is authenticated by OSNMA.
- A regular PVT, which can include multiple constellations, expected to provide a more accurate position estimate.

A check can then be performed between these two solutions, in order to detect any inconsistency that could be due to an attack, as proposed in [12] and illustrated in Fig. 2. In particular, the positions are considered consistent when the OSNMA-based position can be found within a sphere centered on the regular, all-in-view position, which radius is a function of the satellite geometry and of the User Equivalent Range Error (UERE). The radius can be computed as:

$$R = K * \sigma_{UERE} * PDOP \quad (1)$$

Where: R is the radius of the sphere around the estimated position (in meters); K is multiplicative factor; σ_{UERE} is the standard deviation for the UERE, which models the measurements errors; and $PDOP$ is the Position Dilution Of Precision, reflecting the geometric diversity of the measurements used.

This sphere is defining an error bound around the estimated position. If the authenticated position falls within this sphere, the positions are considered consistent. If the authenticated position is located outside of it, an inconstancy is detected and an alarm can be raised. For this analysis, a fixed value of σ_{UERE} value is selected, and the $K * \sigma_{UERE}$ value is voluntarily set to 10 m, considered large enough to capture both the signal in space errors as well as local effects and user errors [13]. Further areas of improvements might include the threshold refinement using real data and a more advanced model approach, based on the horizontal and vertical protection levels estimation already used for aviation [14].

Finally, it should also be noted that highly sophisticated spoofing attacks may be capable of estimating the navigation bits in quasi-real time [15], and thus act on the pseudorange and PVT domain without modifying the navigation data, i.e. avoiding OSNMA-based detection. However, such spoofers are sophisticated and complex to implement, making the occurrence of such attack less likely. In addition, advanced techniques exploiting the unpredictability of the OSNMA data have also been developed in order to detect such attacks, as shown in [16] and [17].

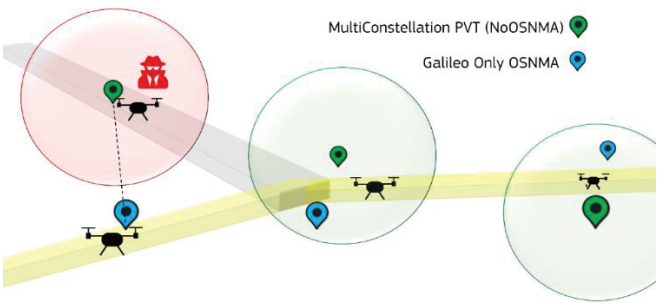

Fig. 2. Spoofing detection principle.

IV. Description of the Tests

A. Flight Trials

In May 2022, some flights activities were performed at the Ispra site of the European Commission Joint Research Centre (JRC) using a multicopter drone to gather Galileo OSNMA data. A commercial professional grade UAS (DJI M300 RTK) equipped with an OSNMA-enabled GNSS Receiver (Septentrio Mosaic X5) was used for the data collection. The drone was also equipped with a reflective prism, tracked by a multi-station (Leica MS60), and used to measure the relative distance to the UAS with electromagnetic waves, independently from the GNSS-based positioning system.

The main objective of the flights was to collect GNSS data on-board the drone in representative and controlled conditions, with the aim to assess the performances of Galileo new features and services.

The flight trials considered 3 typical UAS scenarios:

1. Agriculture/Mapping use case: the Unmanned Aircraft (UA) flies an automatic mission over a parcel of land in open-sky conditions (without trees or building to obstruct the reception of the satellites signal). This test case is representative of mapping and agriculture activities (e.g. spraying of fields).
2. Industrial inspection: the UA is used to inspect a building/specific infrastructure. It flies in parallel to the structure, following a trajectory that enables it to inspect every part of it. In this scenario, the signal reception is blocked on one side by the building.
3. Package delivery: In this scenario, the UA is operated in a simulated urban environment where the presence of tall buildings caused the signals to be blocked and reflected, impacting the performance of the GNSS solution. This scenario is representative of possible conditions encountered in UAM environment.

Fig. 3. Trials of Package delivery applications.

B. Spoofing Scenarios

The simulated scenario is developed from the data collected during the agriculture used case presented above. The trajectory obtained from the multi-station is used to generate the genuine drone trajectory.

In the simulated spoofing scenario, the main objective of the attacker is to spoof the target receiver position by acting only on the GPS constellation while the Galileo constellation remained genuine both in terms of trajectory and of the I/NAV stream including OSNMA data. The target receiver is a drone under a typical agriculture inspection/spraying operation: after some minutes in hovering, the drone starts moving in a typical serpentine trajectory and after some turns, it flies back home and lands vertically. Just before the last turn, a fully synchronized attack on GPS constellation is simulated leading the target receiver to estimate counterfeit straight trajectory from the GPS satellites and genuine trajectory from Galileo satellites.

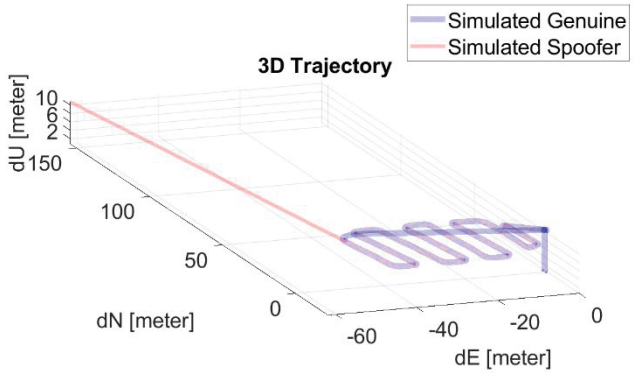

Fig. 4. Genuine and spoofed trajectories.

The objective of the test is to underline the benefit in terms of resilience offered by a target receiver implementing a dedicated PVT solution using only Galileo authenticated satellites compared to a receiver not exploiting the OSNMA protection. Fig. 4 shows the Galileo genuine and the GPS-based counterfeit trajectories.

The same simulated signal, generated with a Radio Frequency Constellation Simulator (RFCS), is then played twice. Firstly, the RFCS is connected to a receiver tracking GPS and Galileo but with OSNMA disabled, in order to assess the impact of the attack on GPS on the multi-constellations PVT solution, without any OSNMA-based spoofing detection capability. Then, to the same receiver but configured with a more stringent logic: only satellites with authenticated navigation data are used to estimate the PVT. It is worth mentioning that a receiver could follow, at least, two different approaches aimed at including authenticated satellites in the PVT solution. The loosest one envisages the exclusion of those satellites not passing the OSNMA verification checks and the most stringent one includes only the authenticated satellites in the PVT solution.

The test is specifically designed to demonstrate the benefits that a strict strategy can offer to a primary multi-constellations PVT approach, as a mean to increase robustness by detecting interferences.

V. Preliminary Results

A. OSNMA Data Availability

The performance of an OSNMA-enabled receiver depends on its capacity to retrieve the different elements of the protocol from the Signal-In-Space (SIS). This capacity is impacted by the satellite visibility but also by the strategy implemented in the receiver to retrieve the elements, as shown in [18] and [19]. In this section, the time required to retrieve the elements in different test conditions are reported, considering that the receiver retrieval strategy is optimised for dynamic conditions, that is: the data is retrieved and combined at the page level, and the repetition of the navigation data is exploited, as described in [18].

In the following table, different key performance indicators are represented:

- The time to retrieve the Digital Signature Message (DSM), which contains the TESLA root key and the elements to verify it;
- The availability of the TESLA chain keys, in particular the duration over which no key is retrieved;
- The time required to authenticate the navigation data from at least 4 satellites, based on the availability of the navigation data and associated tag and key. This estimate does not consider the retrieval of the DSM.

The results in TABLE I. show that the DSM retrieval time is impacted by the environment the mission is carried out in but also by the minimum number of visible Galileo satellites transmitting OSNMA data. The TESLA key, which is repeated across satellites, can be fully retrieved in all cases. The time to authenticate the data from at least 4 satellites is also impacted by the environment, with values varying from 1 minute to up to 3 minutes (95%). It should be noted that while the first authentication introduces a slight delay due to the need to retrieve the different elements, the process can then be performed in a continuous manner. It is also possible for a receiver to store in memory previously verified elements in order to speed up the first time to authentication (OSNMA warm start, as defined in [11]). Finally, as the navigation data set for a given satellite is repeated over several sub-frames, a receiver can also decide to authenticate it once and perform the next verification when new data is transmitted.

TABLE I. OSNMA DATA RETRIEVAL PERFORMANCE

Mission	*Spraying*	*Building inspection*	*Urban air mobility 1*	*Urban air mobility 2*
No. of OSNMA sat. (med./min.)	4/3	4/0	4/2	4/2
DSM time retrieval (95^{th})	146 s	236 s	166 s	182 s
Duration without TESLA chain key (95^{th})	0 s	0 s	0 s	0 s
Time to authenticate 4 satellites (95^{th})	93 s	120 s	60 s	181.5 s

It should also be noted that as the OSNMA protocol authenticates data, it does not impact the measurements themselves but only the availability of these measurements to compute the PVT. As such, OSNMA has a minimal impact on the accuracy obtained with Galileo Open Service, with comparable performances (0.01m difference at 95%) reported both in static and dynamic conditions in [20].

B. Spoofing Detection

Fig. 5 presents the results of the spoofing test. As explained in Section III B., thanks to the cryptographic protection of the navigation layer offered by Galileo system, it is considered more likely that a simplicistic and intermediate attack would focus on the non-protected constellations keeping the Galileo signal genuine. For the sake of simplicity, GPS and Galileo constellations are simulated and the spoofing attack presented in this paper targets the GPS satellites only. As expected, the receiver using GPS and Galileo without OSNMA is fooled by the synchronized attack on the GPS, resulting in a solution that is between the genuine Galileo and the counterfeit GPS trajectories (black dots in the figure). On the other hand, the PVT processing unit based on the OSNMA stringent approach is not affected by the attack on GPS and keeps on providing valid PVT solutions (green dots).

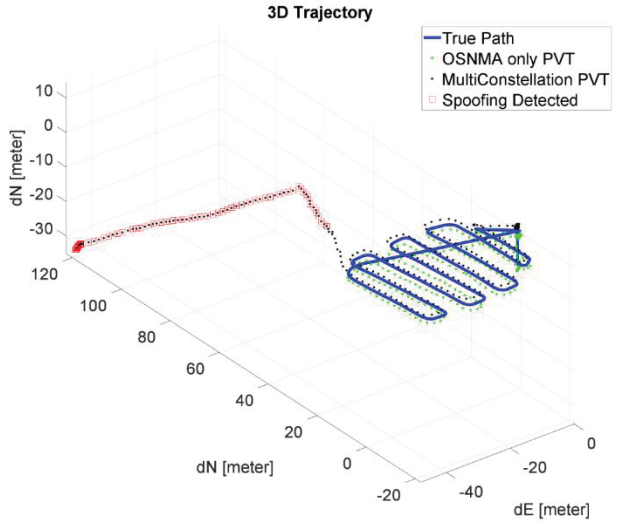

Fig. 5. Standard and OSNMA PVT solutions, with the spoofing detection results indicated in red.

A post-processing elaboration is carried out simulating the approach described in Section III.b., according to which a receiver can assess the reliability of a regular PVT solution by exploiting the consistency check based on the OSNMA PVT and the expected over-bounded sphere centered on the regular PVT solution. For each position record, the receiver evaluates the difference between the OSNMA-enabled and regular PVT solutions and verifies whether this value is larger than the predefined sphere radius. If that is the case, the consistency in the PVT domain is compromised and a potential spoofer attack flag is raised (indicated by a red box). With the specific threshold (1) and the relative genuine and counterfeit trajectories used in this exercise, the spoofer is identified in less than 15 seconds. It should be noted that this detection time may be further reduced by tuning the selected threshold, in particular by characterizing the UERE contributions and potentially by differentiating between the horizontal and the vertical error contributions taking into account speed profiles under different drone flight phases

From the test results, it can be noted that the spoofer is systematically identified once the regular and OSNMA-based PVT solutions start diverging from each other, confirming the feasibility and validity of the detection strategy. It should be noted that the availability of this detection technique depends on the availability of the OSNMA data, and that the impact under different reception conditions will be analysed in future works.

VI. Conclusions

As the number of drones accessing the airspace and the complexity of the operations they are performing are growing, the need for a robust positioning solution is increasing. This is particularly true for safety-related and commercially valuable applications, such as air traffic management or parcel delivery. Authentication also has the potential to support the developments of liability related applications such as insurance investigation or smart contracts.

This paper demonstrates a way to leverage the OSNMA-only PVT solution to increase the robustness of a multi-constellation solution. This solution requires the receiver to run two PVT engines in parallel, so that the additional robustness offered by OSNMA can be exploited while not compromising on the accuracy gain provided by the multi-constellation positioning solution. The feasibility of this technique was demonstrated through a simulation, designed using data collected during an actual drone flight. Future work is expected to further refine the threshold used for the detection of possible interferences, taking into account the OSNMA data availability as well as the probabilities of false alarms and missed detections. The optimisation of the second PVT processing unit in charge of OSNMA-only solution will also be further investigated, in particular regarding a possible reduction of power consumption based on a snapshot approach.

It can be noted that the proposed approach consists in comparing PVT solutions obtained with different satellite sub-sets, which is somehow similar to the approach followed by the Advanced Receiver Autonomous Integrity Monitoring (ARAIM) algorithm [21]. Thus, following a detailed characterization of the spoofing attacks and of the GNSS errors on-board the drone, it may be possible to extend the current scope of integrity monitoring techniques to also cover some spoofing threats benefiting from the assumption that Galileo authenticated satellites are more resilient to attacks

OSNMA is the first contribution of a GNSS to protect its civilian service and has the potential to increase the robustness of receivers against simplistic and more spread spoofing attacks. In complement to OSNMA, Galileo is also planning to provide spreading code authentication with a first implementation based on Assisted Commercial Authentication Service (ACAS) [22]. Other GNSS are also looking to authenticate the signals and data they transmit. GPS is investigating navigation data and spreading code authentication, with the proposed Chips Message Robust Authentication (CHIMERA) scheme [23]. The CHIMERA capability is planned to be demonstrated in 2023 as part of the

GPS NTS3 activities [24]. By combining data and spreading code authentication, it is expected that receivers will be able to protect themselves also against more complex attacks, providing a more robust PVT and thus, enhancing further use of GNSS for drone operations.

REFERENCES

[1] Commission Implementing Regulation (EU) 2021/664 of 22 April 2021 on a regulatory framework for the U-space

[2] International Organization for Standardization, ISO 23629-12:2022, UAS traffic management (UTM) — Part 12: Requirements for UTM service providers

[3] European Union Agency for the Space Programme, "CERTIFLIGHT" Certified E-GNSS Remote TrackIng of Drone and Aircarft FLIGHTs," available at: https://www.euspa.europa.eu/certified-e-gnss-remote-tracking-drone-and-aircraft-flights, accessed on 27/02/2023.

[4] European Union Agency for the Space Programme, "Tests of Galileo OSNMA underway", GSA news item, 11.02.2021, https://www.euspa.europa.eu/newsroom/news/tests-galileo-osnma-underway

[5] European Union, Galileo Open Service Navigation Message Authentication (OSNMA) User ICD for the Test Phase, Issue 1.0, November 2021.

[6] European Union, Galileo Open Service Navigation Message Authentication (OSNMA) Receiver Guidelines for the Test Phase, Issue 1.1, October 2022.

[7] Perrig, A. and Tygar, J. D., "TESLA broadcast authentication." Secure Broadcast Communication: In Wired and Wireless Networks (2003): 29-53.

[8] International Organization for Standardization, ISO/IEC 29192-7:2019 Information security — Lightweight cryptography — Part 7: Broadcast authentication protocols, 2019.

[9] Fernández-Hernández, I., Rijmen, V., Seco-Granados, G., Simon, J., Rodríguez, I., and Calle, J. D. (Spring) A Navigation Message Authentication Proposal for the Galileo Open Service. *J Inst Navig*, 63: 85– 102. doi: 10.1002/navi.125.

[10] European Union, Galileo Open Service Navigation Message Authentication (OSNMA) Signal-In-Space Interface Control Document (SIS ICD), Issue 1.0, December 2022.

[11] European Union, Galileo Open Service Navigation Message Authentication (OSNMA) Receiver Guidelines, Issue 1.0, December 2022

[12] Commission Implementing Regulation (EU) 2021/1228 of 16 July 2021 amending Implementing Regulation (EU) 2016/799 as regards the requirements for the construction, testing, installation, operation and repair of smart tachographs and their components.

[13] F. Ardizzon, G. Caparra, I. Fernandez-Hernandez, C. O'Driscoll, "A Blueprint for Multi-Frequency and Multi-Constellation PVT Assurance", 2022

[14] RTCA DO-229, Minimum Operational Performance Standards (MOPS) for Global Positioning System/Satellite-Based Augmentation System Airborne Equipment, June 2020

[15] T. E. Humphreys, ``Detection strategy for cryptographic GNSS antispoofing," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 49, no. 2, pp. 1073-1090, Apr. 2013, doi: 10.1109/TAES.2013.6494400.

[16] Seco-Granados, G., Gómez-Casco, D., López-Salcedo, J.A. *et al.* Detection of replay attacks to GNSS based on partial correlations and authentication data unpredictability. *GPS Solut* 25, 33 (2021). https://doi.org/10.1007/s10291-020-01049-z

[17] C. O'Driscoll and I. Fernández-Hernández, 'Mapping Bit to Symbol Unpredictability with Application to Galileo Open Service Navigation Message Authentication,' NAVIGATION: Journal of the Institute of Navigation, 2022

[18] S. Damy, L. Cucchi, M. Paonni, "Performance Assessment of Galileo OSNMA Data Retrieval Strategies," *Proceedings of the NAVITEC 2022 conference*, 5-7 April 2022

[19] S. Damy, L. Cucchi, M. Paonni, "Impact of OSNMA Configurations, Operations and User's Strategies on Receiver Performances," *Proceedings of the 35th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2022)*, Denver, Colorado, September 2022, pp. 820-827.

[20] European Union, OSNMA Typical Performance, September 2021, available at: https://www.gsc-europa.eu/sites/default/files/sites/all/files/OSNMA_Typical_Performance.pdf, accessed on 06/04/2023

[21] Working Group C, ARAIM Technical Subgroup, Milestone 3 Report, February 26, 2016.

[22] I. Fernandez-Hernandez *et al*., "Semi-Assisted Signal Authentication for Galileo: Proof of Concept and Results," in *IEEE Transactions on Aerospace and Electronic Systems*, doi: 10.1109/TAES.2023.3243587.

[23] Air Force Research Laboratory Space Vehicles Directorate Advanced GPS Technology, Interface Specification, Chips Message Robust Authentication (Chimera) Enhancement for the L1C Signal: Space Segment/User Segment Interface, IS-AGT-100, 17 April 2019

[24] J. Hinks, J.T. Gillis, P. Loveridge, Shawn, G. Myer, J.J. Rushanan, S. Stoyanov, "Signal and Data Authentication Experiments on NTS-3," *Proceedings of the 34th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2021)*, St. Louis, Missouri, September 2021, pp. 3621-3641.