IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON POSITIONING AND NAVIGATION IN CHALLENGING ENVIRONMENTS

Received February 8, 2022, accepted February 28, 2022, date of publication March 8, 2022, date of current version March 17, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3157337

Galileo OSNMA Public Observation Phase: Signal Testing and Validation

MARIO NICOLA, BEATRICE MOTELLA, MARCO PINI, AND EMANUELA FALLETTI
LINKS Foundation, 10138 Torino, Italy
Corresponding author: Beatrice Motella (beatrice.motella@linksfoundation.com)

ABSTRACT The Public Observation (PO) test phase of the Galileo Open Service Navigation Message Authentication (OSNMA) signal is officially opened since November 15th 2021, by the European Union Agency for the Space Programme (EUSPA). During this phase, any interested users is allowed to access the Signal in Space (SIS) for testing purposes, while the crypto material needed to process the message and verify its authenticity is made available on the European GNSS Service Centre (GSC) web portal. This paper describes the processing of the Galileo E1-B navigation message, as observed during the first days of PO. The purpose is to analyze the crypto and authenticated data carried by the SIS and apply the OSNMA protocol to authenticate the navigation message. The SIS has been processed with the NGene real time software receiver which verifies the authenticity of the navigation data, before evaluating the position fix. The work is completed by an assessment of OSNMA-ready receiver performance, mainly in terms of position accuracy.

INDEX TERMS Authentication, Galileo, GNSS, OSNMA, open service, public observation test phase, spoofing.

I. SPOOFING AND AUTHENTICATION

The well-known Volpe report issued by the Volpe National Transportation Systems Center for the U.S Department of Transportation [1] anticipated in 2001 the assessment of the vulnerabilities of Global Navigation Satellite Systems (GNSSs) in the civil applications. The analysis was not limited to the problem of unstructured interference: indeed, the document already mentioned the *spoofing* as one of the main issues receivers must tackle, thus warning about the importance of implementing anti-spoofing techniques.

The attention of the GNSS community was again drawn to the problem of spoofing about a decade ago, when a group of researchers from the University of Texas at Austin published the results of an experimental investigation, demonstrating the feasibility of carrying out live spoofing attacks against commercial GPS receivers [2], [3]. Following that demonstration, other researchers studied the vulnerability of GPS receivers for various civil applications and the topic of structured interferers begun to attract more and more attention, also driven by new lab demonstrations and some real incidents. This is the ''Black Sea'' case reported in [4], which was probably not an intentional attack, but certainly related to the illegal transmission of false GNSS signals. The scientific literature is constantly updated and the topic is discussed in expert forums [5], as the GNSS-dependency of terrestrial systems keeps growing.

The design of resilient GNSS receivers, capable of detecting and mitigating structured interfering signals, remains a hot research topic. In chronological order, [6]–[13] are some of the most comprehensive technical investigations published on the subject of spoofing and countermeasures. In these works, in addition to a detailed analysis of some spoofing signals and the associated complexity for their generation, the vast panorama of contrast measures is investigated and classified according to different metrics. Although some commercial receivers already implement spoofing detectors, the need for effective algorithms against structured interfering signals remains a priority, especially for security-critical applications. Furthermore, not only the research community has devoted significant effort to develop algorithms to recognize and counteract spoofing attacks at the receiver side, but new authentication services are, or will be, offered at the system level for civilian applications, namely by Galileo on its E1 and E6 bands. As it is well known, the European Galileo program is making an effort to gradually add authentication services to its first and second generation of satellites signals, in order to enable authentication functionalities to future civil

The associate editor coordinating the review of this manuscript and approving it for publication was Ali Broumandan.

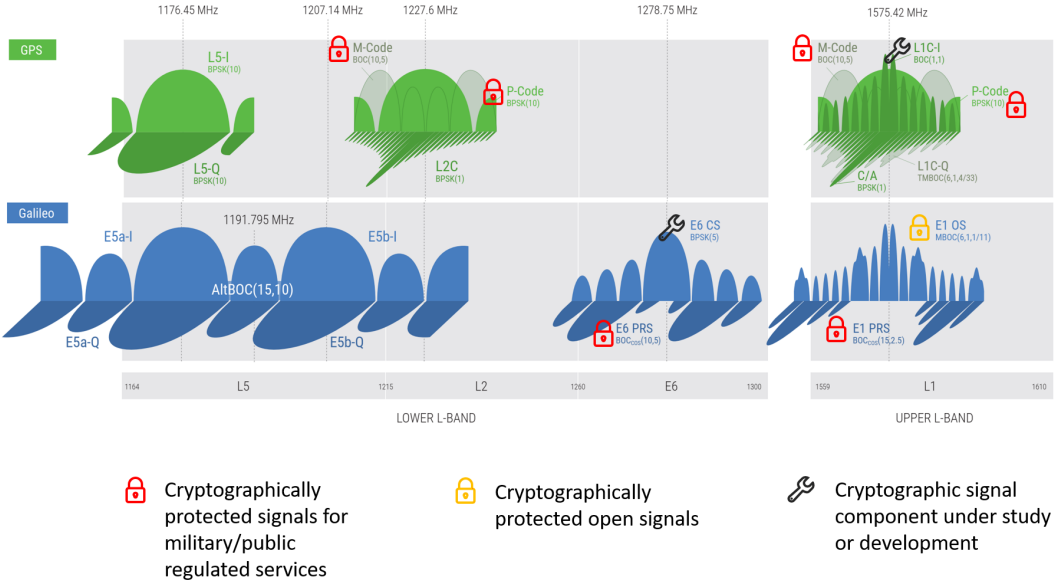

FIGURE 1. Portfolio of criptographically protected signals belonging to GPS and Galileo systems (reworked from [19]).

receivers. The Open Service Navigation Message Authentication (OSNMA) is an integral function of the Galileo Open Service [14], able to provide data authentication to all enabled receivers, through the Navigation Message (I/NAV) broadcast over the E1-B signal component [15], [16].

On November 18th 2020, Galileo satellites started the the first-ever transmission of authentication features in open GNSS signals, by including the OSNMA data in the E1 OS Signal-in-Space (SIS) data message, thus allowing the first-ever OSNMA-protected position fix to be successfully computed [17], [18]. On time with the roadmap in [14], one year later, on November 15th 2021, the Public Observation (PO) test phase of the Galileo OSNMA signal was officially opened by the European Union Agency for the Space Programme (EUSPA), with the goal to reach full service provision by 2023.

Although the OS E1-B is the first signal featuring authenticated components specifically designed for civilian application, it is not the first signal with crypto component in the satellite navigation panorama. As shown by the spectrum of GPS and Galileo signals in figure 1, several signals cryptographically protected are already broadcast by satellites for military or regulated applications, namely the GPS M-code and P-code over L1 and L2, the Galileo Public Regulated Service (PRS) over E1 and E6. The figure also shows new signals under definition, that will embed features of authentication, as the GPS Chips-Message Robust Authentication (Chimera) solution, suitable for the GPS L1C signal and designed for civilian applications [20] or the Galileo Commercial Authentication Service (CAS), which will offer range authentication in the E6 frequency band [21].

Authentication is in all the aspects a new service for the civilian users. The years-long preparatory investigations promoted by the EUSPA have identified a number of application fields which are expected to be the pioneers of the market demand for OS authentication. Among these: logistics, mobile payments, insurance telematics, fleet management and monitoring (terrestrial and maritime), dangerous good transports, road user charging, drones navigation, identification and traffic management, timing. A comprehensive and instructive assessment of such potential market demand and of the technology readiness per target application can be read in [14].

This paper focuses on the Galileo E1-B navigation message, and in particular on the processing of the OSNMA data bits, as observed during the first week of PO. The purpose is to analyze the crypto and authenticated data carried by the SIS and apply the OSNMA protocol to authenticate the navigation message. The signal has been processed with the NGene real time software receiver, able to verify the authenticity of the navigation data, before evaluating the position fix. The work is completed by an assessment of the OSNMA-ready receiver performance, mainly in terms of position accuracy.

After this introduction, the paper describes the OSNMA scheme, along with some details on the requirements the receiver has to satisfy both in terms of internal memory and time synchronization (section II). NGene, the OSNMA-enabled software receiver used for the analysis, is then introduced in section III. Section IV presents the results of the work: after the description of the OSNMA related signal parameters, it analyses the SIS cryptographic and authenticated data and assesses the receiver performance. The conclusions are drawn in section V.

II. THE OSNMA

The OSNMA is the data authentication function for the Galileo Open Service worldwide users, freely accessible to all. It is a technique to authenticate the content of the

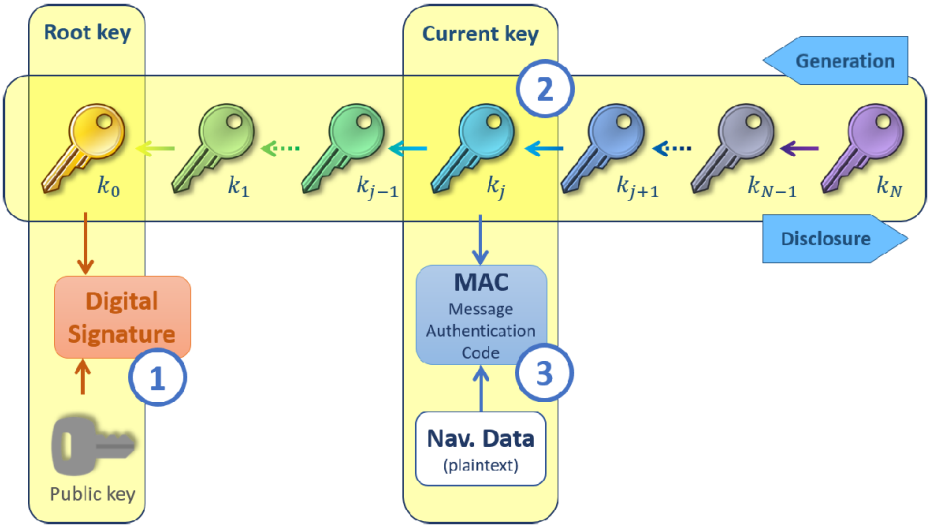

FIGURE 2. Logic for the receiver processing of the OSNMA protocol.

navigation data bits conveyed in the SIS (navigation message authentication technique, NMA), in contrast to other approaches that foresee the jointly implementation of navigation message and spreading code authentication (SCA), as the above-mentioned Chimera [20], [22], [23] or the Spreading Code and Navigation data-based Authentication Proposal (SNAP), suitable for the evolution of the Galileo E1 OS signal [24].

The main processing logic of the OSNMA protocol are summarized in section II-A, referring to [15], [25]–[28] for the detailed description of the service. Section II-B reports the main requirements to be satisfied by the receiver to correctly implement the authentication verification.

A. THE PROTOCOL PROCESSING LOGIC

The OSNMA, whose processing logic is sketched in figure 2, is based on the Timed Efficient Stream Loss-tolerant Authentication (TESLA) protocol [29], in turn structured into two mechanisms, i.e.

- the transmission of a Message Authentication Code (MAC), used to authenticate the plaintext navigation message;
- the delayed transmission of the key used to compute the MAC. The key belongs to a chain of keys, referred to as *TESLA key chain*, in which each key is generated from the previous one with a one-way function. The generation of a chain of length N starts with a random secret key k_N, and ends with a public root key k_0, certified as authentic. The disclosure of the chain occurs in the opposite order.

The delayed release mechanism ensures that the key is not known until after the message and the MAC are received: this prevents the spoofer from generating messages, keys and MACs and broadcasting them compliant to the specifications.

By following the scheme in figure 2, the receiver can perform the verification process by implementing three basic steps, indicated in the scheme by circulated numbers and detailed hereafter:

① The root key is certified as authentic, through an asymmetric scheme based on the verification of the digital signature, transmitted by the SIS, and the public key, available at the receiver;
② The current received TESLA key is authenticated using the root key, by performing the one-way function $\left(k_j \rightarrow k_{j-1}\right)$ the required number of times (j times until 0). Alternatively, if one or more authentication verification have been already successfully occurred (e.g., $k_p \rightarrow k_{p-1} \rightarrow \cdots k_0$, with $p < j$), the current key can also be authenticated with a previous key from the chain, closer than the root key in the keys chain (i.e., the one-way function is computed from k_j to k_p only, for $j - p$ times);
③ The MAC is then generated at the receiver using the current key and the navigation data. If it coincides with the MAC contained in the SIS, the navigation data are authenticated.

B. MAIN RECEIVER REQUIREMENTS

In order to correctly process the OSNMA data and ensure the proper verification of the authentication data, the receiver shall be compliant with specific requirements in terms of both *time synchronization* and *memory* [16]. As for the synchronization with the Galileo System Time (GST), the receiver guidelines issued by the European Union [16] impose a certain synchronization T_L to ensure the user has received the navigation data and associated tag before the corresponding TESLA chain key is disclosed by the system. Under this condition, all tags for all authentication types can be used. Nevertheless, the requirement can be relaxed in the case the

receiver only processes the *slow MACs*, that are MACs whose associated TESLA chain key is transmitted with an extra delay, i.e., 10 sub-frame delay [15].

The receiver also needs to satisfy specific memory requirements. Indeed, all the crypto elements necessary to implement the OSNMA protocol have to be properly stored inside the receiver internal memory [16]. These aspects are deeply analyzed in [30], which also highlights how the amount of memory specifically allocated for the OSNMA can be easily limited by having a little forethought. For example, the storage of the full TESLA chain is not required, but only the last authenticated key has to be available. In addition, the memory required to save the MACK section waiting for the right key, can be dynamically allocated and freed once the verification has been accomplished.

III. THE NGene RECEIVER

The availability of a reconfigurable message processing unit was a fundamental element at the early stage of the signal transmission. This allowed a fast adaptation of the message decoding function to the characteristics of the new message and its possible variations, without impacting on the rest of the receiver functionalities. Fast, modular and safe reconfigurability is the key feature of the software receiver, because it enables quick manipulation and verification of all the receiver functionalities at any stage of the processing chain. For this reason a reconfigurable software receiver has been considered since long time the principal development tool for in-lab analysis, development and prototyping of algorithms and architectures. Our lab has developed, maintained and expanded such software approach in the NGene family of receiver prototypes [31], which fulfilled the needs of several activities and projects. The implementation of the OSNMA receiver algorithm in the message decoding and verification functionalities is one of the most recent branches of the NGene family.

The core NGene processing capability resides in the real-time processing of the GPS, Galileo and EGNOS signal components broadcast on the L1/E1 band, after Intermediate Frequency (IF) downconversion and digitalization of the signal ensemble reaching the antenna. IF donwconversion and digitalization are demanded to an external analog front-end device, which communicates with the NGene supporting platform via USB connection. The Analog-to-Digital (A/D) converter with front-end filtering, along with the antenna and its Low-Noise Amplifier, are the only non-software elements of the receiving chain. The NGene family is configurable to support many such front-ends, USB connected with the software processor, so that it has been used cascaded to several different antenna types and front-ends. Furthermore, being a set of software functions, NGene has been ported on various computing platforms, from Linux-based general purpose personal computers [32]–[36] to ARM-based embedded processors, where it was often indicated as embedded-NGene, or eNGene [37]. The NGene branch adapted to the OSNMA was first developed for execution on a standard PC [30], then it was ported on smaller and portable platforms with ARM processors, namely the ODROID-X2, Raspberry Pi 4 and ODROID-C4 [38], [39].

The first net result of the availability of such a tool has been the opportunity for supporting the OSNMA testing activities in the Testing and Demonstration Hub for EU GNSS at the Joint Research Centre of the European Commission in Ispra, Italy, during the internal testing phase [40]. The same software was then ready for the Public Observation phase, becoming the enabling tool for the generation of the results presented in this paper. In addition, with the final goal of making the NGene receiver ready for Chimera+OSNMA, the complete implementation of the Chimera verification has been recently implemented [23], [41], [42]. In fact, to the best of our knowledge, while some OSNMA-ready commercial receivers are entering the marketplace, none is offering yet the support for Chimera.

IV. AUTHENTICATION FROM LIVE SIGNALS

This section presents the results of the Galileo signals processing, as observed during the first week of PO, namely along six days, starting from November 14th, 2021, approximately at 6:20 p.m. UTC. After summarizing the observed OSNMA parameters transmitted by the SIS (section IV-A), the core results of the OSNMA data processing are reported in section IV-B. The analysis concludes with section IV-C, showing some results on the observed receiver performance.

A. SIS OSNMA PARAMETERS

An OSNMA data message is transmitted within each E1-B I/NAV nominal odd page part, composed by the HKROOT section (8 bit) and the MACK section (32 bit) [15]. Consequently, a complete 120-bit HKROOT message and a complete 480-bit MACK message are transmitted within each 30-seconds sub-frame. Before starting the verification process, the receiver needs to collect the OSNMA parameters contained in the DSM-KROOT message, that provides a digitally signed KROOT for a TESLA chain, the chain cryptographic functions, the key and tag sizes, as well as other parameters that are fixed for each given chain.

Following the notations used in the user Interface Control Document (ICD) [15], table 1 summarizes the OSNMA parameters extracted from the SIS during the observation period. The table reports the description of the parameters, their values as extracted from the DSM-KROOT message, and their corresponding values as for the look-up tables 7 to 11 of [15]. Other important parameters, derived from [15], are summarized in table 2, highlighting their specific setting for the testing phase respect to previous versions of the Interface Control Document (ICD) [25]. It is worth noticing that the values of WN_K and $TOWH_K$ reported in table 1 refer to the first floating root key received during the test: indeed, the system regularly sends floating root keys belonging to the same TESLA chain with a rate of one new key per hour.

TABLE 1. OSNMA parameters in the DSM-KROOT message.

DSM-KROOT parameters	Description	Field value	Corresponding value
NB_{DK}	# of DSM-KROOT blocks	2	8 blocks - 832 bits (l_{DK})
PKID	ID of the Public Key (PK)	2	
CIDKR	ID of the TESLA chain	1	
HF	Hash function	0	SHA-256
MF	MAC function	0	HMAC-SHA-256
KS	Key Size, l_K	4	128 bit
TS	Tag Size, l_t	9	40 bit
MACLT	MAC Look-up table	33	
WN_K	KROOT Week Number	1161	
$TOWH_K$	KROOT Time of Week	80	288000 s
α	Random Pattern	25d3964da3a2 (hex)	

TABLE 2. Other OSNMA parameters.

Other parameters	Description	Value	Specific setting in [15]
NMACK	# of MACK blocks per sub-frame	1	Fixed. NMACK field set to *Reserved1*
NS	max # of satellites with different keys per MACK block	1	Fixed
MACK message offset	offset of one MACK message	enabled	Fixed
MO	MACK Offset	disabled	Fixed. Parameter removed

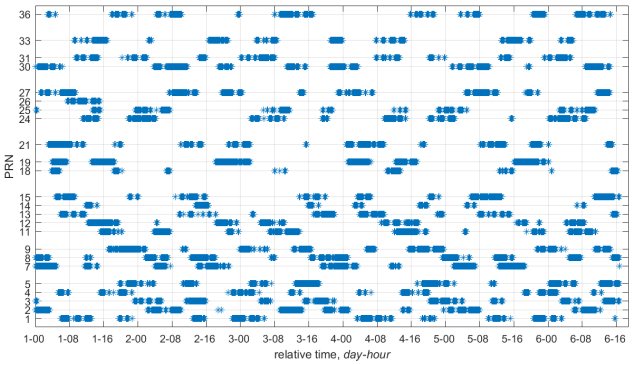

FIGURE 3. Availability of OSNMA data per Galileo PRN.

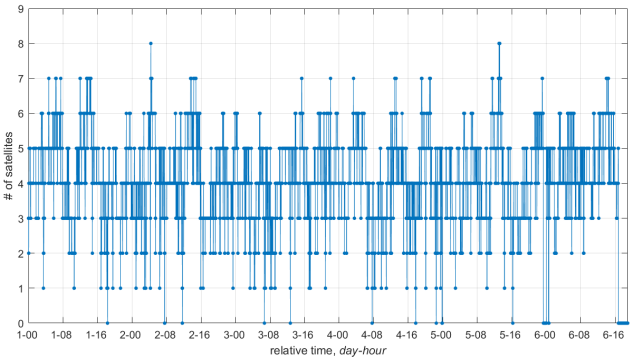

FIGURE 4. Number of Galileo satellites transmitting OSNMA data.

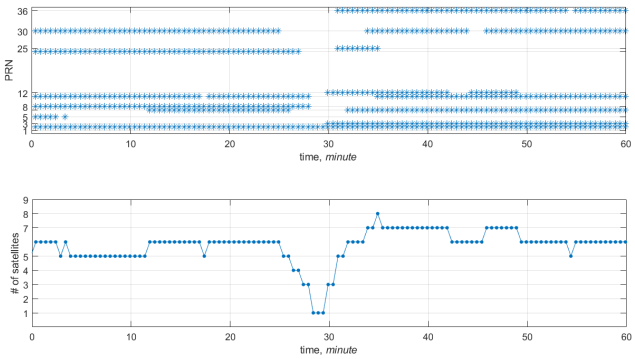

FIGURE 5. Zoomed view of figure 3 (upper plot) and figure 4 (bottom plot).

B. OSNMA SIGNAL TESTING AND VALIDATION

The results summarized hereafter cover two aspects. From one side we present the *signal testing*, i.e.: the analysis of the OSNMA signal observation, as received by the antenna on the roof of the LINKS Foundation premises during the first days of PO. The antenna is located in open sky conditions and the analyzed data collection lasts almost six days. On the other hand, the *signal validation* shows some examples of SIS authentication verification performed by NGene.

The abscissa axis of the figures in this section indicates the relative time from the beginning of data collection (i.e., 14/11/2021 at 6.20 p.m.). Depending on the scale in use, it is expressed either as *day-time* (e.g., "1-08" means "1st day of data - 8 hours after the beginning of the collection") or *seconds*, when only a portion of the plot is depicted.

Figure 3 shows the availability of the OSNMA data per PRN. It reports a marker corresponding to the start of each subframe that contains OSNMA bits. Figure 4 completes the analysis showing the total number of satellites transmitting OSNMA, visible at the LINKS premises antenna, during the six days of data collection. It varies from 0 to 8 and the discussion on its relationship with the receiver accuracy is discussed in section IV-C. From figures 3 and 4, and better from their zoomed view in figure 5, which shows only 60 minutes of data collection at the beginning of the second

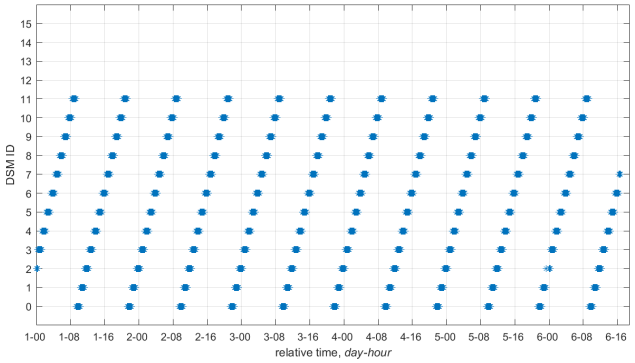

FIGURE 6. Identifier of the DSM.

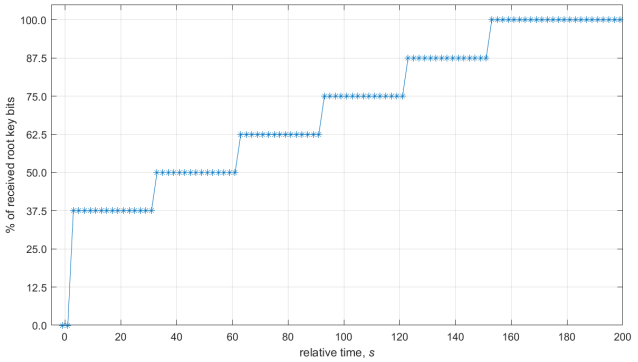

FIGURE 7. Availability of the TESLA root key.

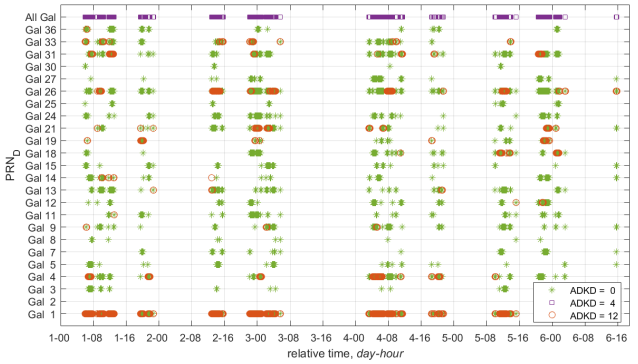

FIGURE 8. Tags received from PRN 1 and corresponding PRN_D for ADKD 0, 4, and 12.

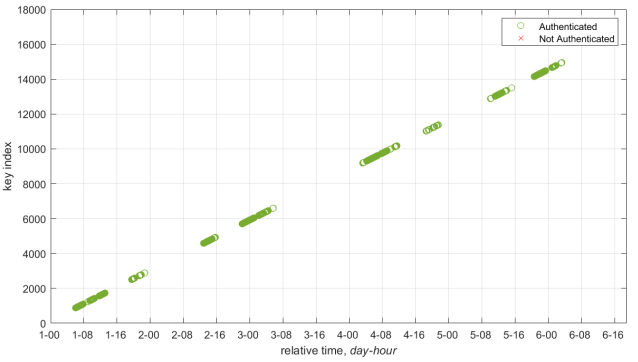

FIGURE 9. Validation of the TESLA keys received from PRN 1.

day, it is evident how the Galileo ground segment sometimes discontinues the transmission of the satellites SISs. As an example, from the upper plot of figure 5 we can see that PRNs 7, 11, 12 and 30 have subframes with empty OSNMA data and there are intervals (bottom plot) in which few of the received satellites are transmitting authentication data. This might be a vulnerability for the receiver. Indeed, a spoofer can easily fool the target device transmitting counterfeit signals with all the OSNMA bits set to zero: since this is a condition that can occur in the authentic signal, the receiver has no mean to detect the attack and might proceed with the processing of the received counterfeit signals.

By proceeding with the signal testing analysis, a further example of datum extracted from the SIS is the DSM ID, the 4-bit identifier of the DSM. Indeed, as a DSM is transmitted in several blocks [15], the DSM ID identifies the DSM associated with the current block. It can take values from 0 to 15: values from 0 to 11 are allocated to DSM-KROOT messages, while values from 12 to 15 are for DSM-PKR messages. Figures 6 shows the DSM ID numbering that follows during the data collection, exclusively allocated to DSM-KROOT messages.

In addition, as clear from section II, to start the verification process, the receiver needs to receive the entire root key. Figure 7 depicts the percentage of received bits composing the root key, showing that the total time needed to complete the reception of the root key is approximately 150 seconds [18].

To conclude the signal testing analysis, figure 8 shows some examples of tags received from PRN 1, when visible to the antenna at the experiment site, with Authentication Data and Key Delay (ADKD) equal to 0 (I/NAV Ephemeris, clock and Status), 4 (I/NAV Timing Parameters), and 12 (same as ADKD 0, but with 10 additional sub-frames of delay) respectively. Figure 8 reports a marker at the start of each sub-frame containing a tag correspondent to a certain PRN_D, which indicates the identifier of the satellite transmitting the data to be authenticated. In the case PRN_D is 255, the tag authenticates some Galileo constellation-related information, not specific for any satellite (ADKD 4) and is reported in the figure with the label *All Gal*. During the observation week, PRN 1 appears to be able to authenticate the data of almost all the other Galileo satellites.

Passing now to the signal validation analysis, figure 9 shows the authentication of the keys belonging to the TESLA chain. Each marker represents a successful validation of a TESLA key received from PRN 1.

By concluding, the authentication of the PRN 1 navigation message through the tags with ADKD 0 and 12 is shown in figure 10: each marker corresponds to the validation of a tag transmitted by PRN_A (i.e.: the identifier of the satellite transmitting the authentication information) to validate the PRN 1 navigation message. All the tags processed along the

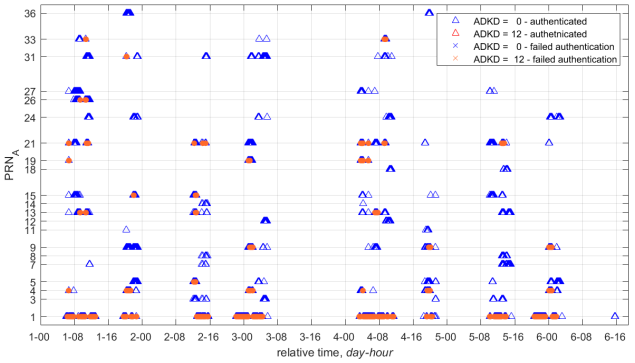

FIGURE 10. Authentication of the PRN 1 navigation message.

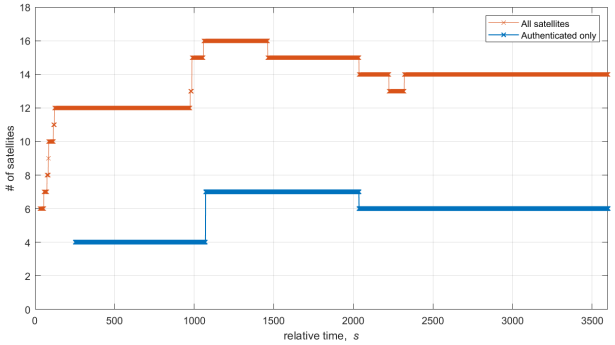

FIGURE 11. Number of GPS + Galileo satellites used by the NGene PVT.

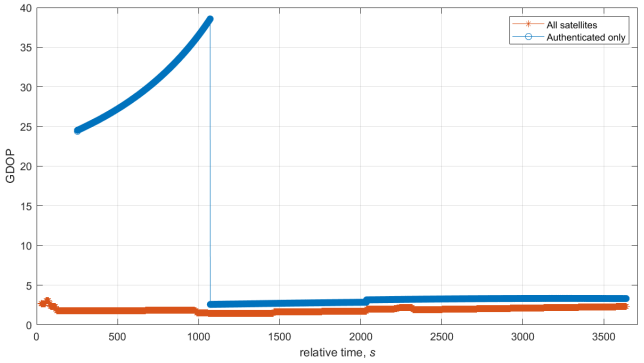

FIGURE 12. Geometrical Dilution of Precision.

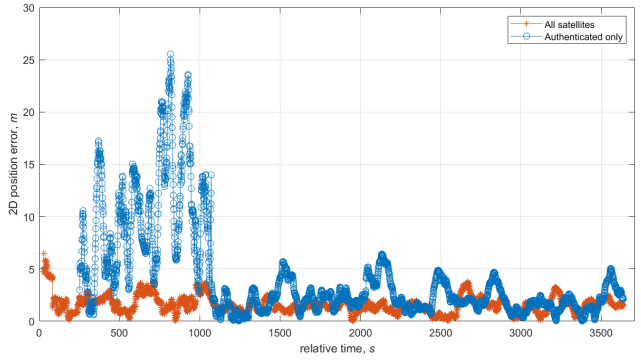

FIGURE 13. 2D position error.

data collection have been successfully verified and none of them failed the verification process.

C. OSNMA-ENABLED RECEIVER PERFORMANCE

Within the receiver, the final output of the authentication verification process is a flag, for each tracked PRN, which indicates whether the carried data are authenticated or not. This flag is updated at with a rate equal to the rate of the MACK blocks, that is 1 MACK block every 30 seconds, during the test phase. Depending on the internal logic of the receiver, the decision on how to use such information within the PVT computation can be different. The receiver can either follow a conservative approach and use exclusively the satellites with a true authentication flag or try to exploit all the measurements and use all the tracked PRNs, independently from the carried authentication information. The following analysis focuses on the comparison of these two strategies and the effects they might have on the receiver performance, mainly in terms of position accuracy. NGene computes the PVT with 1 Hz rate by employing a least squares method and carrier smoothing. The results shown here concern a 1-hour data-set for simplicity of representation, collected on November 25th 2021, and processed with the NGene software receiver. These results are fully representative of the performance obtained during the whole 6-days-long observation session. The data collection set-up included an evaluation kit of a consumer grade GNSS receiver, which run in parallel to NGene and was used as reference.

Figure 11 shows the number of satellites used in PVT, depending on the decision rule implemented in the NGene receiver. It is much lower in the case of using only authenticated satellites and equals the minimum of 4 for about the first 15 minutes of data collection. This is mainly due to the fact that the GPS-cross authentication, foreseen by the OSNMA protocol, is not transmitted by Galileo satellites during this first observation phase, and the entire GPS constellation has to be excluded when the receiver uses only satellites carrying authenticated data. On the other hand, the consumer receiver which has inherently higher sensitivity that the software one, tracks from 11 to 14 satellites for the GPS, and from 7 to 9 satellites for the Galileo; it does not process the authentication data. It can be reasonably expected anyway that a lower number of satellites in tracking is representative of a situation in which a commercial-grade receiver operates in non optimal scenarios, for example in dynamic conditions when some physical obstacles might obstruct part of the satellites signals.

The impact of the satellite selection rule adopted in the PVT computation is clear from the analysis of figures 12 and 13 that respectively present the Geometrical Dilution of Precision (GDOP) and the 2D position error in the two cases. The presence of only 4 authenticated satellites in the first part of the data highly affects the GDOP and consequently the position error.

TABLE 3. 2D- and 3D-position error performance. All satellites vs authenticated satellites only.

	Position error					
	All satellites		Authenticated only		Authenticated only -limited GDOP-	
	2D, m	3D, m	2D, m	3D, m	2D, m	3D, m
Max error	6.5	7.4	25.5	35.1	6.4	7.1
Mean error	1.6	2.4	4.1	5.4	2.1	3.1
1σ error	0.8	1.2	4.5	5.8	1.3	1.4
95th percentile error	**3.1**	**4.7**	**14.4**	**17.1**	**4.8**	**5.7**

This can be also appreciated in the first two columns of table 3 (titled *All satellites* and *Authenticated only*), that reports the maximum, mean, 1σ, and 95th percentile errors, for both the 2D- and 3D- cases, considering the two different receiver rules. As an example, the 95th percentile 2D error passes from 3.1 to 14.4 meters. The 3D one, that was limited to 4.7 meters in the case of using all the visible satellites, reaches 17.1 meters, when only the authenticated ones are used for PVT. In addition, the percentage of time in which the 2D-position error in lower than 5 meter passes from 99.5% to 77.4%, when the PVT is computed with authenticated satellites only. Such a degradation is even worst with the 3D error: it stays under 5 meter for the 95.6% of time if all the satellites contribute to the PVT, and for the 69.1% when only authenticated satellites are used.

For completeness, the last column of table 3 (*Authenticated only -limited GDOP-*) refers to the case in which the receiver enables a control on the GDOP, by forcing the computation of the PVT only when the GDOP is below a certain bound, i.e.: 10. As expected, although the PVT availability results significantly reduced, the position accuracy improves and the errors on the position are comparable with those computed with all the in view satellites. Results are in line with those presented in [18].

These first results highlight the importance of the *GPS cross-authentication*, foreseen by the OSNMA protocol [25]. Once available in fact, it will allow dual-constellation receivers to use both GPS and Galileo satellites, assuring comparable position accuracy performance of that obtained with legacy signals, thus guaranteeing the service continuity.

V. CONCLUSION AND FUTURE ACTIVITIES

On November 18th 2020, Galileo initiated the first ever transmission of authentication capabilities in open GNSS signals, incorporating OSNMA data into the E1-B SIS data message. This paper contains a description of the OSNMA protocol and collects the results of the signal observation carried out in Torino, during the week immediately following the beginning of the public observation phase, in November 2021. A real-time software receiver has proved to be an extremely useful tool for monitoring the parameters transmitted in the navigation messages, analysing all the steps required by the authentication process and evaluating the first performance of a GNSS receiver capable of decoding authenticated messages.

The 6-days observation demonstrates a continuous transmission of OSNMA data from the constellation, although there are intervals of time in which very few, or even none, of the received satellites are transmitting bits of authentication. Such a behaviour, once the system will be fully operational, would lead to the service unavailability, thus opening potential vulnerabilities for the receiver. The final part of the paper reports a first assessment of the receiver performance, in terms of positioning accuracy, assuming the receiver implements a conservative approach and uses measurements only from authenticated PRNs to compute the PVT. Of course, in cases where only a subset of Galileo satellites could be authenticated, the accuracy degrades mainly due to high values of GDOP. This could be representative of scenarios with partial visibility of the sky, but we noticed that once also the GPS cross-authentication will be enabled (i.e.: Galileo satellites authenticate data broadcast by GPS satellites), this situation will be solved. In conclusion, the 6-days observation was invaluable to validate the algorithms implemented in the receiver, according to the last version of the ICD [15] and the receiver guidelines [16], thus proving the transmission of new authenticated data from satellites, through the processing of live signals.

REFERENCES

[1] A. John, "Vulnerability assessment of the transporation infrastructure relying on the global positioning system," U.S. Dept. Transp., Washington, DC, USA, Tech. Rep., Aug. 2001. [Online]. Available: https://www.navcen.uscg.gov/?pageName=pressRelease

[2] University of Texas News. *UT Austin Researchers Successfully Spoof an $80 million Yacht at Sea*. Accessed: Jul. 29, 2013. [Online]. Available:https://news.utexas.edu/2013/07/29/ut-austin-researchers-successfully-spoof-an-80-million-yacht-at-sea/

[3] J. Bhatti and T. E. Humphreys, "Hostile control of ships via false GPS signals: Demonstration and detection," *J. Inst. Navigat.*, vol. 64, p. 467, May 2017. [Online]. Available: https://onlinelibrary.wiley.com/doi/10.1002/navi.183

[4] M. Jones, "Spoofing in the Black Sea: What really happened?" *GPS World*, Oct. 11, 2017. [Online]. Available: https://www.gpsworld.com/spoofing-in-the-black-sea-what-really-happened/

[5] *Thousands of GNSS Jamming and Spoofing Incidents Reported in 2020*. Accessed: Mar. 9, 2022. [Online]. Available: https://www.linkedin.com/pulse/thousands-gnss-jamming-spoofing-incidents-reported-2020-guy-buesnel

[6] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle, "GPS vulnerability to spoofing threats and a review of antispoofing techniques," *Int. J. Navigat. Observ.*, vol. 2012, Jul. 2012, Art. no. 127072, doi: 10.1155/2012/127072.

[7] C. Günther, "A survey of spoofing and counter-measures: A survey of spoofing and counter-measures," *Navigation*, vol. 61, no. 3, pp. 159–177, Sep. 2014.
[8] D. Margaria and M. Pini, *GNSS Interference Threats Countermeasures (GNSS Technology) Applications*, F. Dovis, Ed. Norwood, MA, USA: Artech House, 2015.
[9] D. Borio and C. Gioia, "A sum-of-squares approach to GNSS spoofing detection," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 52, no. 4, pp. 1756–1768, Aug. 2016.
[10] A. Broumandan, A. Jafarnia-Jahromi, S. Daneshmand, and G. Lachapelle, "Overview of spatial processing approaches for GNSS structural interference detection and mitigation," *Proc. IEEE*, vol. 104, no. 6, pp. 1246–1257, Jun. 2016.
[11] M. L. Psiaki and T. E. Humphreys, "GNSS spoofing and detection," *Proc. IEEE*, vol. 104, no. 6, pp. 1258–1270, Jun. 2016.
[12] R. T. Ioannides, T. Pany, and G. Gibbons, "Known vulnerabilities of global navigation satellite systems, status, and potential mitigation techniques," *Proc. IEEE*, vol. 104, no. 6, pp. 1174–1194, Jun. 2016.
[13] D. Margaria, B. Motella, M. Anghileri, J.-J. Floch, I. Fernandez-Hernandez, and M. Paonni, "Signal structure-based authentication for civil GNSSs: Recent solutions and perspectives," *IEEE Signal Process. Mag.*, vol. 34, no. 5, pp. 27–37, Sep. 2017.
[14] *GALILEO Open Service Navigation Message Authentication (OSNMA) Info Note*, European Union Agency for the Space Programme, Prague, Czechia, 2021.
[15] *GALILEO Open Service Navigation Message Authentication (OSNMA) User ICD for the Test Phase, Issue 1.0*, European Union, Maastricht, The Netherlands, Nov. 2021.
[16] *GALILEO Open Service Navigation Message Authentication (OSNMA) Receiver Guidelines for the Test Phase, Issue 1.0*, European Union, Maastricht, The Netherlands, Nov. 2021.
[17] *Tests of Galileo OSNMA Underway*. Accessed: Mar. 9, 2022. [Online]. Available: https://www.euspa.europa.eu/newsroom/news/tests-galileo-osnma-underway
[18] M. Götzelmann, E. Köller, I. V. Semper, D. Oskam, E. Gkougkas, J. Simon, and A. de Latour, "GALILEO open service navigation message authentication: Preparation phase and drivers for future service provision," in *Proc. 34th Int. Tech. Meeting Satell. Division Inst. Navigat.*, Oct. 2021, pp. 385–401, doi: 10.33012/2021.17886.
[19] S. Orolia, *The GNSS Spectrum*. Infographic, 2019. [Online]. Available: https://www.orolia.com/document/the-gnss-spectrum/
[20] *Interface Specification, Chips Message Robust Authentication (Chimera) Enhancement for the L1C Signal: Space Segment/User Segment Interface*, document IS-AGT-100, Air Force Research Laboratory Space Vehicles Directorate Advanced GPS Technology, Apr. 2019.
[21] P. Gutierrez. *GALILEO Authentication and High-Accuracy Service: Coming on Fast*. Accessed: Jul. 8, 2021. [Online]. Available: https://insidegnss.com/galileo-authentication-and-high-accuracy-service-coming-on-fast/
[22] M. Nicola, B. Motella, and M. T. Gamba, "The chimera solution: Performance assessment," in *Proc. Eur. Navigat. Conf. (ENC)*, Nov. 2020, pp. 22–25.
[23] M. Nicola, B. Motella, and M. T. Gamba, "GPS chimera: A software receiver implementation," in *Proc. 34th Int. Tech. Meeting Satell. Division Inst. Navigat.*, Oct. 2021, pp. 4264–4273.
[24] B. Motella, D. Margaria, and M. Paonni, "SNAP: An authentication concept for the Galileo open service," in *Proc. IEEE/ION Position, Location Navigat. Symp. (PLANS)*, Apr. 2018, pp. 967–977, doi: 10.1109/PLANS.2018.8373475.
[25] *GALILEO Navigation Message Authentication Specifications for Signal-In-Space Testing*, European Union, Maastricht, Netherlands, 2016.
[26] 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.
[27] I. F. Hernandez, 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," in *Proc. Eur. Navigat. Conf. (ENC)*, Warsaw, Poland, Apr. 2019, pp. 1–6, doi: 10.1109/EURONAV.2019.8714151.
[28] C. O'Driscoll, "What is navigation message authentication?" GNSS Solutions Column, Inside GNSS, Jan./Feb. 2018, pp. 26–31.
[29] A. Perrig, R. Canetti, J. D. Tygar, and D. Song, "The TESLA broadcast authentication protocol," in *Proc. CryptoBytes*, 2002, pp. 2–13.
[30] B. Motella, M. T. Gamba, and M. Nicola, "A real-time OSNMA-ready software receiver," in *Proc. Int. Tech. Meeting Inst. Navigat.*, San Diego, CA, USA, Feb. 2020, pp. 979–991.
[31] A. Molino, M. Nicola, M. Pini, and M. Fantino, "N-gene GNSS software receiver for acquisition and tracking algorithms validation," in *Proc. Eur. Signal Process. Conf. (EUSIPCO),* Glasgow, U.K., Aug. 2009, pp. 2171–2175.
[32] S. Digenti, M. Nicola, L. Lo Presti, and M. Pini, "Technique for the estimation of PC clock offset in a GNSS-aided network of collaborative users," in *Proc. ESA Workshop Satell. Navigat. Technol. Eur. Workshop GNSS Signals Signal Process. (NAVITEC)*, 2010, pp. 1–8, doi: 10.1109/NAVITEC.2010.5707990.
[33] B. Motella, M. Pini, M. Fantino, P. Mulassano, M. Nicola, J. Fortuny-Guasch, M. Wildemeersch, and D. Symeonidis, "Performance assessment of low cost GPS receivers under civilian spoofing attacks," in *Proc. ESA Workshop Satell. Navigat. Technol. Eur. Workshop GNSS Signals Signal Process. (NAVITEC)*, Dec. 2010, pp. 1–8, doi: 10.1109/NAVITEC.2010.5708018.
[34] D. Margaria, M. Nicola, F. Dovis, N. Linty, and L. Musumeci, "Galileo in-orbit validation E1 and E5 signals: Experimental results and assessment," in *Proc. Workshop Satell. Navigat. Technol.*, 2012, pp. 1–8, doi: 10.1109/NAVITEC.2012.6423065.
[35] D. Margaria, G. Marucco, and M. Nicola, "A first-of-a-kind spoofing detection demonstrator exploiting future Galileo E1 OS authentication," in *Proc. IEEE/ION Position, Location Navigat. Symp. (PLANS)*, Apr. 2016, pp. 442–450, doi: 10.1109/PLANS.2016.7479732.
[36] H. L. Nguyen, G. M. Troglia, E. Falletti, and T. H. Ta, "Situational awareness: Mapping interference sources in real-time using a smartphone app," *Sensors*, vol. 18, p. 4130, Oct. 2018, doi: 10.3390/s18124130.
[37] M. Troglia Gamba, M. Nicola, and E. Falletti, "ENGene: An ARM based embedded real-time software GNSS receiver," in *Proc. Int. Tech. Meeting Satell. Division Inst. Navigat.* Tampa, FL, USA, Sep. 2015, pp. 1–5.
[38] M. T. Gamba, M. Nicola, and B. Motella, "Galileo OSNMA: An implementation for ARM-based embedded platforms," in *Proc. Int. Conf. Localization GNSS (ICL-GNSS)*, Tampere, Finland, Jun. 2020, pp. 1–6.
[39] M. Troglia Gamba, M. Nicola, and B. Motella, "Computational load analysis of a Galileo OSNMA-ready receiver for ARM-based embedded platforms," *Sensors*, vol. 2021, no. 21, p. 467, Jan. 2021, doi: 10.3390/s21020467.
[40] L. Cucchi, S. Damy, M. Paonni, M. Nicola, M. Troglia 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," in *Proc. Int. Tech. Meeting Satell. Division Inst. Navigat.* St. Louis, MI, USA, Sep. 2021, pp. 3653–3667, doi: 10.33012/2021.17966.
[41] M. Troglia Gamba, M. Nicola, and B. Motella, "GPS chimera: A software profiling analysis," in *Proc. Int. Tech. Meeting Satell. Division Inst. Navigat.*, Sep. 2020, pp. 3781–3793.
[42] B. Motella, M. Nicola, and S. Damy, "Enhanced GNSS authentication based on the joint CHIMERA/OSNMA scheme," *IEEE Access*, vol. 9, pp. 121570–121582, 2021.

MARIO NICOLA received the M.S. degree in computer science engineering from Politecnico di Torino, in 2002, and the Ph.D. degree in electronics and communications engineering working on re-configurable architectures for wireless communication systems, in 2005. He is currently a Researcher Staff with the Space and Navigation Technologies Research Area, LINKS Foundation, Italy. His research interest includes the implementation of algorithms for software radio GPS/Galileo receivers.

BEATRICE MOTELLA received the M.Sc. and Ph.D. degrees from the Politecnico di Torino, in 2003 and 2008, respectively. During the Ph.D. program, she spent one year with the Satellite Navigation and Positioning Laboratory, University of New South Wales, Sydney, Australia. She is currently a Researcher with LINKS Foundation, Turin, Italy. She has been involved in projects funded by the European Commission, aimed at the study of authentication features for the second generation of Galileo signals. Her research interests include different aspects of the signal processing for radio navigation receivers, with a major focus on GNSS interference monitoring.

MARCO PINI received the Ph.D. degree in electronics and communications from Politecnico di Torino University. As a result of the experience gained on GNSS receivers, he has been responsible for the Research and Development activities of several projects. He is the Head of the Space and Navigation Technologies Group, LINKS Foundation, Italy. His major research interests include baseband signal processing on new GNSS signals, multi-frequency RF front end design, and software radio receivers.

EMANUELA FALLETTI received the M.Sc. and Ph.D. degrees in telecommunications engineering from Politecnico di Torino, Italy, in 1999 and 2004, respectively. She is the Team Leader of the Space and Navigation Technologies with the AI, Data and Space Division, LINKS Foundation. Currently she has almost 15 years of experience on software radio and digital signal processing techniques and algorithms for advanced GNSS receivers, in particular for interference detection and mitigation, anti-spoofing algorithms, multipath mitigation, and signal simulation. She has authored several scientific papers on journals and international conferences and acts as a peer reviewer for various scientific publications. Her research interests include array signal processing, multi-antenna systems, and wireless propagation channel modeling.