This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3107871, IEEE Access

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.Doi Number

Enhanced GNSS authentication based on the Joint CHIMERA/OSNMA scheme

Beatrice Motella[1], Mario Nicola[1], and Sophie Damy[2]

[1]LINKS Foundation, Torino, Italy

[2] European Commission, Joint Research Centre, Ispra, Italy

Corresponding author: Beatrice Motella (e-mail: beatrice.motella@linksfoundation.com).

The work has been performed within the FUNTIMES-2 (Future Navigation and TIMing Evolved Signals-2) project, funded by the European Commission under the Horizon 2020 Framework Program (Funding Reference No. 630/PPGRO/RCH/17/9877), and led by Airbus Defence and Space GmbH.

ABSTRACT The authentication of the navigation signals can be considered as the contribution of the system to the robustness against spoofing attacks and it is becoming an important requirement for a growing number of user communities. GPS and Galileo systems are proposing evolutions of their civil signals to embed features of authentication. For Galileo, the Open Service Navigation Message Authentication (OSNMA) is integrated in the Galileo E1 OS signal. For the GPS, the Chips-Message Robust Authentication (Chimera) solution, designed for the GPS L1C signal, is foreseen to be tested soon.

On the other hand, suitable signal processing techniques can be implemented inside the receiver to monitor the quality of the received signals and protect against spoofing attacks. Such techniques shall work as a complement to the authentication strategies, to further increase the signals' robustness. Within this context, the paper presents the *Joint Chimera/OSNMA scheme*, designed to be adopted by a multi-constellation receiver that already exploits both OSNMA and Chimera enhancements. The idea is to further strengthen the robustness with respect to the individual use of the two solutions, to tackle sophisticated spoofing attacks, which are able to avoid detection from navigation message authentication (NMA) techniques. The manuscript proves the high performance of the joint scheme, presenting the results of a wide bench of tests, under different scenarios of spoofing, and user conditions.

INDEX TERMS OSNMA, Chimera, authentication, Galileo, GPS, Navigation Message Authentication, Spreading Code Authentication, dual-constellation receiver

I. INTRODUCTION

The signal structure of civil Global Navigation Satellite System (GNSS) signals is open to the public domain, as for example for the E1 Open Service Galileo signal [1] and the GPS L1 C/A code [2]. As a consequence, signals can be perfectly reconstructed and replicated, thus mimicking the genuine ones, transmitted by the constellation's satellites. In the case such a characteristic is taken as an advantage from a malicious user, with the goal of gaining the control of a victim receiver, the transmission of false signals is referred to as *spoofing*, and might have tremendous consequences [3]-[6].

As these attacks represent an increasing threat to GNSS users, several anti-spoofing techniques have been proposed over the past years to be embedded into the receiver [7]-[14]. These countermeasures include, among others, spatial signal processing using multiple antennas, signal power monitoring, correlator output monitoring and consistency checks. As detailed in [7][10], combinations of these countermeasures can be used to tackle different threats. For example, a receiver can implement power monitoring and consistency checks (e.g. using a RAIM/ARAIM approach [14]). Such combination enables to detect relatively simple spoofing attacks, which are characterized by an increase in power as well as inconsistencies among the measurements, as only some of them are spoofed. However, as attacks are becoming more sophisticated [15], additional anti-spoofing techniques are needed. Subtler attacks can attempt, for instance, to achieve believable consistency between the measurements with a low increased power, while introducing incorrect data in the navigation message. Such attacks can be detected using

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3107871, IEEE Access

authentication techniques, which are being introduced at the *system level*. The introduction of some cryptographic elements in the GNSS signals structure makes the signals not a-priori predictable and provide the user with a mean to verify the authenticity of the received signals [16].

The term *authentication*, in fact, refers to the verification of the authenticity of the received information and that of the transmitting entity [17]. For what concerns GNSS signals, the authentication techniques are often classified as navigation message authentication (NMA) and spreading code authentication (SCA) solutions, without preventing that the two methods can be jointly implemented. NMA denotes the protection of the full frame of navigation message bits or a portion of it. NMA is usually performed by digitally signing the navigation data, thus keeping the navigation message unencrypted. SCA methods work at the chips level and are accomplished with the insertion of unpredictable chips within the nominal spreading code, verifiable by the receiver through proper cryptographic functions.

Both GPS and Galileo are proposing evolutions of their civil signals to embed features of authentication. For Galileo, the Open Service Navigation Message Authentication (OSNMA) is integrated in the Galileo E1 OS signal [18]. For the GPS, the Chips-Message Robust Authentication (Chimera) solution [19], suitable for the GPS L1C signal, is foreseen to be transmitted in 2022 [20].

This paper presents a technique to be implemented inside the receiver, and able to take advantage of the two system authentication enhancements. It is called *Joint CHIMERA/OSNMA scheme*, and has been designed for dual-constellation receivers, able to process and verify Galileo and GPS signals, that embed OSNMA and Chimera features, respectively. The Joint scheme exploits the fact that the two systems will broadcast authenticated signals over the same band and has the goal of further strengthening the separate use of each authentication strategy. NMA guarantees the source of the data and enables the detection of subtler spoofing attacks modifying the navigation message. If the solution is further completed by an SCA, as in the proposed joint Chimera and OSNMA scheme, resilience is further increased, enabling signal replay detection [10].

After this introduction, the paper is organized as follows: section II recaps the main working principles of Chimera and OSNMA services, while section III presents the Joint scheme, along with the details on the procedure for the calibration phase. Section IV is dedicated to the impact of the front-end. The performance of the joint scheme is presented in section V for a wide bench of tests, under different scenarios of spoofing, and user conditions. Section VI draws the conclusions of the work.

II. GNSS AUTHENTICATION

To ease the readability of the paper, before entering the details of the joint scheme, the Chimera and OSNMA solutions are presented hereafter, in sections *A* and *B,* respectively. Section *C* deals with the joint strategies to cross authenticate signals at the system level.

A. CHIMERA IN BRIEF

This section briefly recalls the main working principle of Chimera, based on the information retrieved from references [19] to [22]. Chimera implements both NMA and SCA. Navigation message data are protected by digitally signing most or all the data, while authentication markers replace a fraction of the code chips and are used to authenticate the spreading code. Such markers, considered as the core of the Chimera concept, replace the nominal spreading code symbols at a specified duty factor.

In addition, Chimera foresees the use of two channels: a slow channel for standalone users and a fast channel for more rapid authentication when out-of-band information is available. Fast channel period, in fact, is either 1.5 seconds or 6 seconds and determines the scope of the fast channel keys.

In the case of the slow channel, the markers are cryptographically generated using a key derived from the digitally signed navigation message. In this way, the navigation message and the spreading code cannot be independently generated nor independently spoofed. In the case of the fast channel, the time binding is carried out by the delayed revealing of the keys from an external source.

The proposed Chimera implementation is tailored to GPS L1C signal with Time Multiplexed Binary Offset Carrier (TMBOC) modulation. Markers are inserted into the L1C pilot spreading code as single puncture of L1C BOC(1,1)-modulated markers that replace the corresponding L1C pilot spreading code symbols. As shown in FIGURE 1, markers are placed in dedicated marker segments, which are 33 L1C chips long. The marker chips in a selected marker segment replace the 29 BOC(1,1) chips, that can alternatively belong to the slow (blue chips) or fast channel (yellow chips). The four BOC(6,1) chips, in black, are never modified. A 1-ms portion of the spreading code comprises 31 segments, reserved for slow or fast channel markers, as defined by a deterministic sector pattern that depends on the pseudo-random noise (PRN) code. There are separate duty factors for slow and fast channels, and the total duty factor is given by the sum of the two.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3107871, IEEE Access

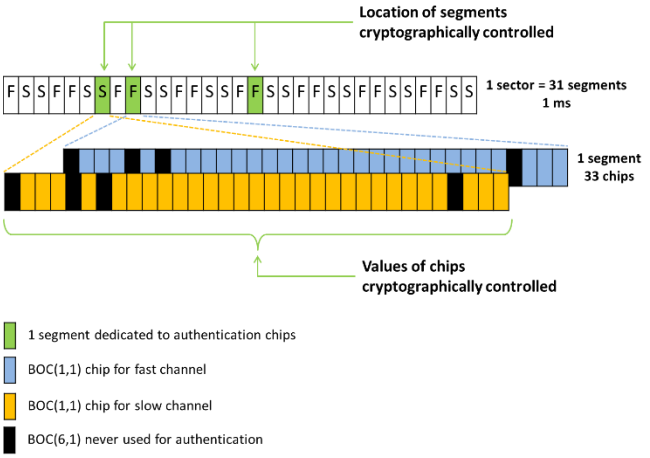

FIGURE 1°. Markers puncturing in the Chimera segments and sectors.

B. OSNMA IN BRIEF

Galileo OSNMA protocol enables users to verify the authenticity of the navigation data they received. A successful verification ensures that the navigation data was sent by the system and was not modified. The Galileo OSNMA protocol only authenticates the navigation data and does not directly protect the range measurement domain, which is addressed by the Commercial Authentication Service (CAS) [23].

This section summarizes the OSNMA protocol described in [18]. OSNMA data is sent on L1-BC I/NAV message, in place of the current Reserved 1 bits, providing 40 bits every page. Among these 40 bits, the first 8 bits are used to send digital signature message (DSM) and the remaining 32 to send truncated message authentication codes (MAC) and associated keys and information. These elements are used for the data authentication in a protocol, which is described below.

The navigation data is authenticated by mean of truncated MACs, named tags, which are verified through a symmetric scheme using a key that is disclosed with some delay, as per the TESLA protocol [24]. This key is part of a TESLA chain, which enables the user to compute previous keys from the current one. This property is exploited to verify the key, either against the root key of the TESLA chain, transmitted in the DSM part of the OSNMA field, or against a previously verified key. The root key itself is verified through an asymmetric scheme based on a digital signature verification, sent in the DSM-KROOT part of the OSNMA field. This asymmetric scheme relies on the use of a public key, known to the user. Renewal and revocations procedures are also in place for the public key and the TESLA chain elements.

The protocol enables the authentication of different elements of the navigation message, which are uniquely identified through the MAC information field.

C.° JOINT STRATEGIES AT THE SYSTEM LEVEL

As described in [18], Galileo OSNMA protocol includes the capability to authenticate GPS navigation data through cross-authentication. This refers to the possibility to authenticate the navigation data of satellites which do not transmit OSNMA data with data retrieved from transmitting satellites. This principle is exploited by the Galileo satellites, as OSNMA data is foreseen to be transmitted only by a subset of satellites. In practice, a satellite transmitting OSNMA data will provide tags relative to its own navigation data and tags relative to the navigation data of the neighboring satellites. Likewise, the protocol can be configured to include tags to authenticate the navigation data of neighboring GPS satellites.

The tags transmitted by a satellite are unambiguously identified by three parameters:

- The Authentication Data & Key Delay (ADKD) field, which identifies the navigation bits being verified;
- The PRN of the satellites whose navigation data is being verified (which can be offset to identify a different constellation);
- The Issue Of Data (IOD) relative to the navigation data.

Regardless of the constellation they are related to, the tags are verified in the same way (described in section *B*), using the same key chain. Thus, navigation data from both Galileo and GPS can be authenticated through one protocol, reducing the number of cryptographic elements to be retrieved and the number of verifications to be performed.

While described here for Galileo, NMA schemes in general have the flexibility to transmit authentication messages for different inputs, if this input can be unambiguously identified. NMA methods are currently under investigation for other systems such as QZSS [25] and SBAS [26][27].

III. THE JOINT CHIMERA/OSNMA SCHEME

This section presents the Joint scheme and details the procedure for the calibration of the threshold: section *A* presents the concept; section *B* describes the steps needed for the calibration phase.

A. THE SCHEME

The proposed algorithm enhances the Galileo ranging level protection, by leveraging on the current version of Chimera and OSNMA single concepts. As sketched in FIGURE 2, the OSNMA by itself is not able to authenticate the ranging signal [28], but suitable strategies, based on the joint use with Chimera, might go in this direction.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3107871, IEEE Access

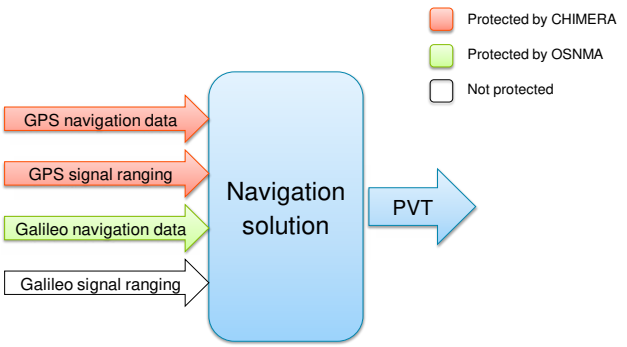

FIGURE 2°. OSNMA and Chimera protect GNSS navigation data and signal ranging.

The Joint scheme exploits specific characteristics of the two authentication techniques. In details: *i)* as for the Chimera, thanks to the spreading code markers, it is able to assure ranging level authentication; *ii)* as for the OSNMA, Galileo signals broadcast the GPS to Galileo Timing Offset (GGTO), defined as the time offset between GPS and Galileo system times. In addition, the OSNMA scheme authenticates the GGTO datum through the Authentication Data & Key Delay (ADKD) number 2 and 4 [18]. ADKD 2 authenticates all the data in the subframe (GGTO included), and ADKD 4 authenticates the word 6 (Galileo-UTC) and the word 10 (GGTO). The GGTO has been introduced as a system contribution to achieve tighter interoperability among GPS and Galileo, but it can be used here in the context of authentication. It is worth mentioning that the GGTO is also transmitted by the GPS L1C signal (subframe 3, page 2).

The joint scheme is based on a verification of compliance within the receiver and can be described by the following assumptions:

1. Chimera can assure ranging level authentication;
2. The GGTO, transmitted and authenticated by the OSNMA signal, bounds the GPS to Galileo time offset;
3. The PVT computation allows the estimation of both the Galileo and GPS times, respectively t_{Galileo} and t_{GPS}.

At the receiver, the verification of the compliance between the difference $(t_{\mathrm{GPS}} - t_{\mathrm{Galileo}})$ and the GGTO shall assure a certain protection of the Galileo signals at the ranging level. Such a verification can be expressed as

$$|(\hat{t}_{\mathrm{Galileo}} - \hat{t}_{\mathrm{GPS}}) - \mathrm{GGTO}| < T \qquad (1)$$

where the hat indicates the estimate obtained by the Position Velocity and Time (PVT) computation and T is a threshold that depends on the receiver and signal conditions. To carry out the verification of compliance, the user must have previously set the threshold T. This step is called *algorithm calibration* and is described in the following section. The actual application of the scheme is presented in section V, under different kinds of spoofing attacks.

It is worth stressing that, as clear from equation (1), the method is based on the monitoring of the GGTO. For this, the implementation of the scheme might be also feasible when the signals are not authenticated. The added value we have when at least one constellation enables both navigation message and spreading code authentication, resides in the fact that the spoofing attack can then also be mitigated.

B. ALGORITHM CALIBRATION

As well described in [29], the difference between the broadcast GGTO and $(\hat{t}_{\mathrm{GPS}} - \hat{t}_{\mathrm{Galileo}})$ shall take into account that the transmitted parameter only corrects for timing differences originated at the satellite, while the estimate $(\hat{t}_{\mathrm{GPS}} - \hat{t}_{\mathrm{Galileo}})$ can include other intersystem biases introduced by the receiver, like group delay differences or delays generated during the signal processing. For this reason, it is necessary to calibrate the threshold in (1), also on the basis of the specific receiver and front-end (FE) in use.

As an example, FIGURE 3 shows the trend of the estimated GGTO, obtained by using the SiGe GN3S Sampler front-end [30], over a data collection of 1 hour (blue line), and compared with the GGTO from the navigation message, set to 0 in the configuration of the signal generator (orange line).

Data collections considered here last 1 hour and are used as examples to show the calibration process. The discussion on the GGTO statistics over time is included in section IV.B, along with some recommendations for an actual implementation inside the receiver.

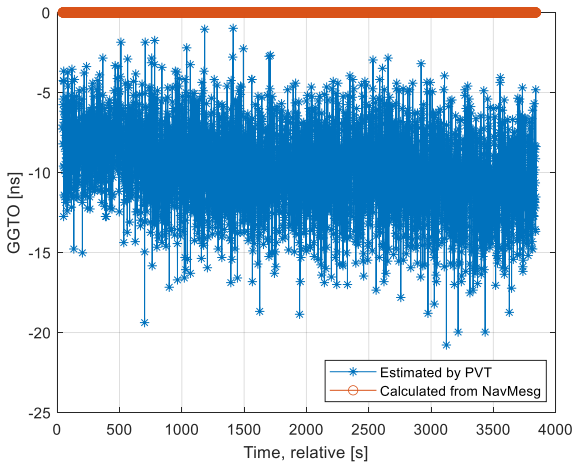

FIGURE 3°. Estimated GGTO, obtained by using the SiGe GN3S Sampler front-end, and compared with the GGTO from the navigation message.

The estimated GGTO presents a constant bias, which needs to be considered for the threshold setting. Equation (1), in fact, shall be rewritten as

$$|(\hat{t}_{\mathrm{Galileo}} - \hat{t}_{\mathrm{GPS}}) - b_{\mathrm{G}} - \mathrm{GGTO}| < T \qquad (2)$$

where b_{G} represents the bias respect to the broadcast GGTO.

As an example, the steps to be followed for the calibration with the SiGe GN3S are summarized hereafter. The same

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3107871, IEEE Access

procedure can be repeated for any specific combination of receiver/front-end in use:

1. Evaluate the estimates $t_G[n] = (\hat{t}_{\mathrm{GPS}}[n] - \hat{t}_{\mathrm{Galileo}}[n]) - \mathrm{GGTO}[n]$ in nominal conditions (i.e.: in the absence of spoofing) for a long-time interval. In the example, we considered 1 hour of data, with output rate of 1 Hz (i.e.: $n = 1, \ldots, 3600$);
2. Verify that $t_G[n]$ follows a normal distribution (see FIGURE 4), and evaluate the mean b_{G} and the standard deviation σ_{G}. In the case of the SiGe GN3S front-end used with the NGene receiver [31], $b_{\mathrm{G}} = 19.3$ ns and $\sigma_{\mathrm{G}} = 2.2$ ns;
3. Fix the desired probability of false alarm P_{fa};
4. Evaluate the threshold in equation (2)

$$T = \sqrt{2}\sigma_{\mathrm{G}} \cdot \mathrm{erfc}^{-1}(P_{\mathrm{fa}}) \qquad (3)$$

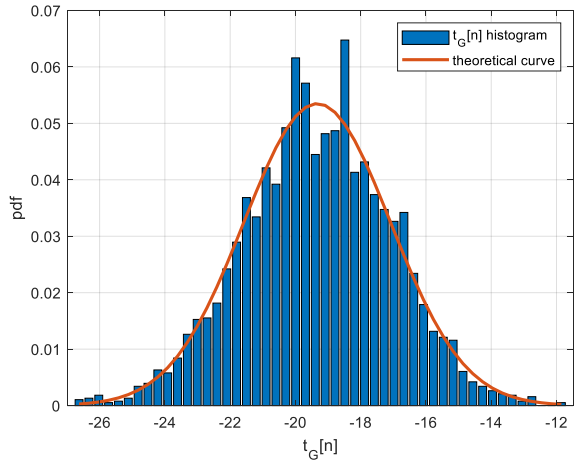

FIGURE 4°. Histogram of $t_G[n]$ and comparison with the theoretical normal distribution.

TABLE I summarizes the values of T, evaluated by varying the probability of false alarm.

TABLE I
THRESHOLD T, EVALUATED FOR DIFFERENT VALUES OF P_{FA}

P_{FA}	T (ns)
10^{-2}	5.8
10^{-3}	7.4
10^{-4}	8.7
10^{-5}	9.9
10^{-6}	11.0

FIGURE 5 shows the verification of compliance on the dataset of FIGURE 3, with T evaluated as in equation (3), for P_{fa} set to 10^{-5}. Of course, the calibration is done on a clean dataset and the threshold is never crossed.

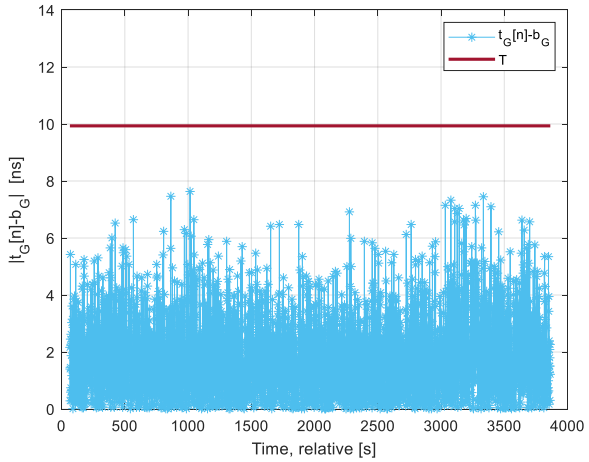

FIGURE 5°. Verification of compliance against the threshold T, for the dataset used for calibration.

Before concluding, it is worth mentioning that the calibration shown in the example has been performed in good satellite geometry conditions, as presented in FIGURE 6. The figure plots, together with the estimated GGTO, the number of GPS and Galileo satellites and the trend of the Time Dilution of Precision (TDOP), which is always between 1 and 2.5, representative of a good satellite geometry. Section V.B will further discuss the possible choices for the calibration in real scenarios.

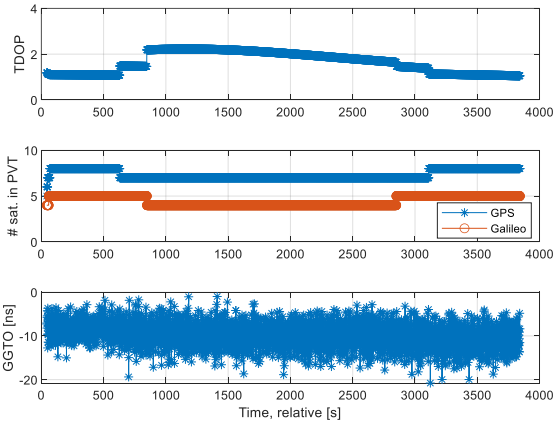

FIGURE 6°. Time Dilution of Precision (TDOP), number of GPS and Galileo satellites used in PVT, and estimated GGTO.

IV. THE ROLE OF THE FRONT-END

As highlighted, the front-end plays a fundamental role in the setting of the threshold since it affects the bias b_{G} between the estimated and the transmitted GGTO. For this, two specific analyses related to the front-end have been conducted: section *A* compares the GGTO estimates obtained with different front-ends, and section *B* deals with the investigation on possible effects due to the external temperature.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3107871, IEEE Access

A IMPACT ON THE ESTIMATED GGTO

A comparison has been done among the estimates of the GGTO obtained with three front-ends: two versions of the SiGe GN3S [30], and one Amungo NUT4NT [32] front-ends.

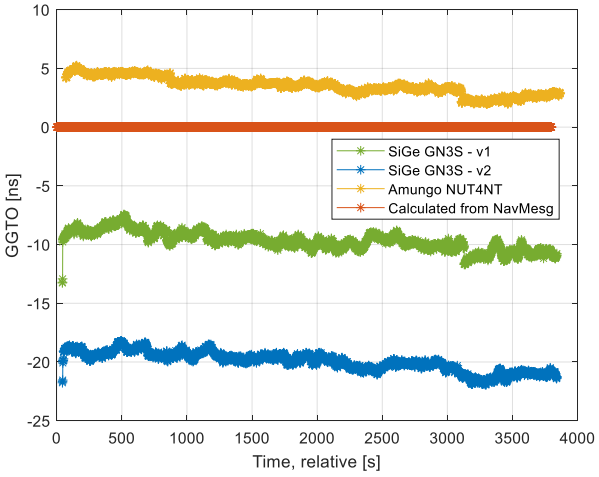

FIGURE 7°. Comparison among the estimates of the GGTO obtained with three front-ends: SiGe GN3S - v1, SiGe GN3S - v2, and Amungo NUT4NT.

The different bias respect to the GGTO extracted from the navigation message (depicted in FIGURE 7) confirms what written in [29], i.e., the difference between the broadcast and the estimated GGTO shall consider that the latter can include biases introduced by the receiver itself.

TABLE II summarizes the characteristics of the three front-ends in terms of sampling frequency f_s, intermediate frequency f_{IF}, and bandwidth (BW), along with their biases evaluated with respect to the broadcast GGTO. For completeness, it also reports the values of σ_G, showing that the GGTO standard deviation does not depend on the front-end in use.

TABLE II
FRONT-END CHARACTERISTICS AND GGTO STATISTIC

Front-end	f_s (MHz)	f_{IF} (MHz)	BW (MHz)	b_G (ns)	σ_G (ns)
SiGe GN3S - v1	16.3676	4.1304	2	-9.9	0.8
SiGe GN3S - v2	16.3676	4.1304	5	-19.3	0.8
Amungo NUT4NT	31.700	9.58	15.12	3.5	0.7

B ANALYIS ON THE IMPACT OF THE TEMPERATURE

The calibration is needed to set the threshold used in the verification of compliance. For this, it is fundamental that the statistic of the GGTO does not change over time, for example due to the variation of the temperature.

Specific tests have been carried out collecting data over several hours, with the scope of investigating the correlation between the temperature and the GGTO estimates. FIGURE 8 and FIGURE 9 show the results of the processing of two datasets, collected in November 2020 and June 2021, respectively, from real signals, in open sky scenario. In both figures the trend of the GGTO is plotted along with that of the recorded temperature over one day (blue lines). Black dots and green dots represent the mean of the GGTO and the mean of the temperature, evaluated over blocks of 4 hours-data. The tests are similar, but performed in different temperature range conditions, i.e.: 3 ÷19 °C (November 19-21, 2020), and 18 ÷ 29 °C (June 9-11, 2021).

By comparing the black and the green curves of the two plots (the four-hours block average of the GGTO and temperature respectively), we can observe that, for the November 2020 data collection, the trend of the two curves seems slightly correlated, though the black curve does not present a maximum in correspondence of a minimum of the green curve. On the other hand, the same conclusion cannot be drawn by observing the results concerning the June 2021 data collection. In this last case, in fact, the trends of the two curves do not present similarities.

As a final remark, FIGURE 10 shows the comparison between the GGTO statistic evaluated on blocks of 4 hours and the GGTO mean evaluated on the whole data collection of 24 hours (November 2020 data collection). The vertical lines represent the intervals $m_{GGTO} \pm 2\sigma_{GGTO}$, where m_{GGTO} and σ_{GGTO} are the mean the standard deviation of the GGTO evaluated on blocks of 4 hours-data. M_{GGTO} is the GGTO mean calculated by using the whole 24 hours' dataset.

M_{GGTO} is always included in the intervals $m_{GGTO} \pm 2\sigma_{GGTO}$, thus proving that the GGTO does not significantly vary over time.

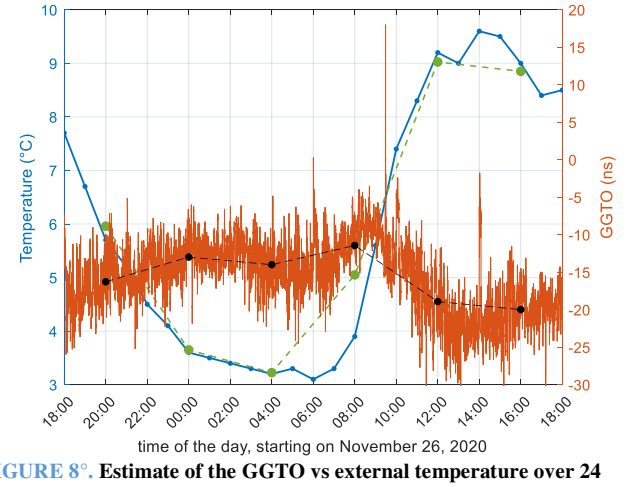

FIGURE 8°. Estimate of the GGTO vs external temperature over 24 hours of data collection (November 2020).

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3107871, IEEE Access

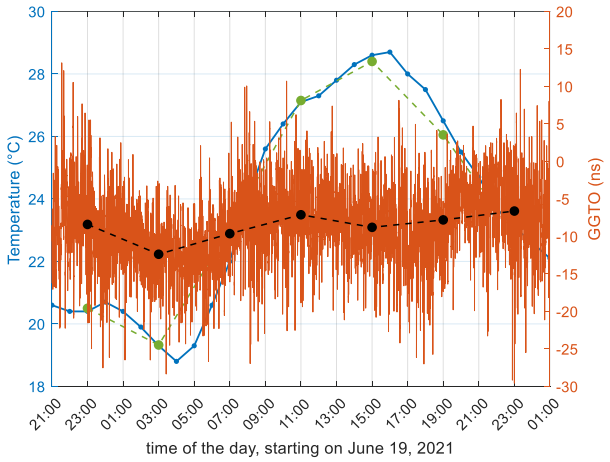

FIGURE 9°. Estimate of the GGTO vs external temperature over 28 hours of data collection (June 2021).

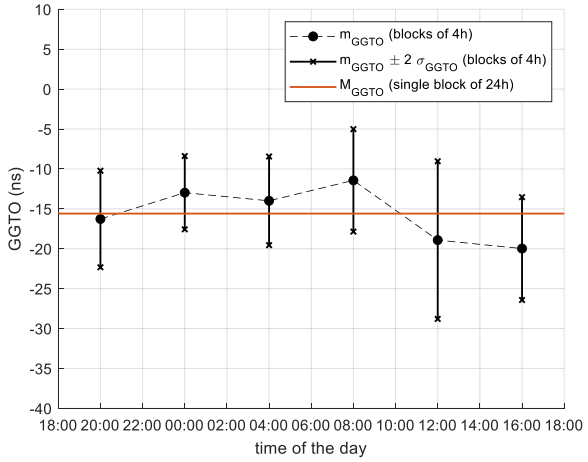

FIGURE 10°. Comparison between the GGTO statistic evaluated on blocks of 4 hours and the GGTO mean evaluated on the whole data collection of 24 hours.

Summing up, from the tests performed we can conclude that a clear dependency between the GGTO and the temperature is not evident. Nevertheless, the paper presents an algorithm for spoofing detection, and it would need specific adaptations for a final implementation inside the receiver.

Of course, the calibration implies certain choices that depend on the specific implementation: for example, one might foresee a single calibration over a long data collection, or successive shorter calibration phases that continuously adapt the threshold, in the absence of spoofing. This last choice would assure higher performance in the detection phase, slightly increasing the computational cost of the overall algorithm.

V. VALIDATION TESTS

As said, the joint Chimera/OSNMA scheme is thought to be adopted by multi-constellation receivers that already exploit both Chimera and OSNMA enhancements. For this reason, the algorithm needs to be tested under sophisticated spoofing attacks, able to avoid detection from NMA algorithms. The hypotheses considered effective for the validation tests can be summarized as follows:

1. The spoofer can transmit the navigation message of all the in-view satellites, for example by reading on-the-fly the bits' values;
2. It is assumed that, thanks to the SCA-part of the algorithm, Chimera would be able to detect ranging level attacks, thus excluding spoofed GPS signals, and the receiver would perform a spoofing mitigation strategy. As a consequence, the received GPS signals are from the authentic constellation, while for the Galileo it is considered that the spoofer is able to counterfeit the whole constellation or a portion of it and the receiver acquires and tracks them.

In other words, for the generation of the attacks, we impose a certain error (in terms of position, velocity or time offset) with respect to the true PVT of the victim receiver. The spoofer in fact is able to generate false signals belonging to both constellations. Of course, a receiver processing only false signals would estimate a GGTO coherent with that obtained by processing only true signals. We consider a spoofer able to produce perfect Galileo OSNMA and GPS Chimera-NMA navigation messages. On the other hand, thanks to the Chimera-SCA part of the algorithm, the receiver can exclude the false GPS signals, and track the authentic GPS signals only. The Galileo signals are then further protected by the joint scheme, that detects inconsistency between constellations.

After the description of the methodology adopted in simulation (section *A*), the performance of the Joint scheme is presented hereafter under different types of attacks: section *B* deals with static and dynamic scenarios, section *C* presents the results concerning spoofing attacks that produce small position errors. Section *D* concerns timing spoofing attacks and section *E* concludes with attacks in which the spoofed satellites belong to both constellations. Each section describes the specific simulation scenario and present the Joint scheme performance in terms of false alarm and detection probabilities.

A. SIMULATION METHODOLOGY

As for the execution of the tests, the signal has been generated with the NAVX-NCS Professional GNSS radio frequency (RF) signal generator [33] and processed by the OSNMA ready NGene software receiver [34]-[36]. The employed dual-constellation RF signal generator has been driven by ad hoc software setups to generate scenarios of signal spoofing attacks. The RF generator is connected via an RF cable to the front-end and then, through the USB bus, to the real-time software receiver. This experimental setup is depicted in FIGURE 11.

It is worth noticing here that the lab simulation of a spoofing attack is easier with respect to the execution of a real attack for

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3107871, IEEE Access

several reasons. First, in the lab, the position of the victim receiver is perfectly known. Second, the signal-in-space injected by the generator as *authentic* signal, is totally known and under control. Third, the *counterfeit* signal, produced by the same generator, can be set as a perfectly superimposed copy of the authentic signal, with perfect alignment in frequency and phase at the receiver's antenna and perfect control of the relative power level. Though achieving analogous working conditions in non-assisting situations might be difficult, testing GNSS receivers in such conditions is anyway relevant, because they represent *ideal cases* of attack and *worst cases* for the receivers.

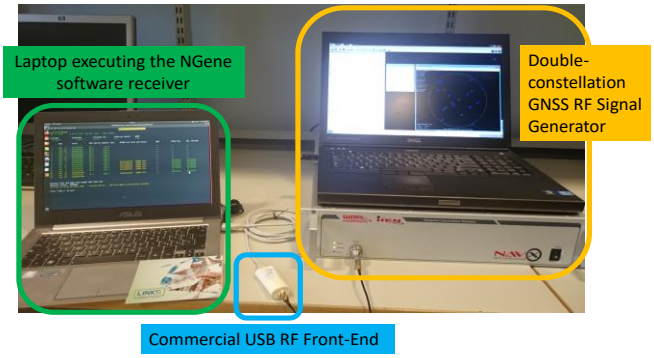

FIGURE 11°. Experimental setup used for the test of the joint Chimera/OSNMA strategy.

B. STATIC AND DYNAMIC SCENARIOS

This section presents the results of the tests both in static and dynamic conditions.

In the first bench of tests, the simulated spoofing scenario foresees that the victim receiver is static, located at the LINKS Foundation premises roof antenna, while the spoofing trajectory is static for the first 5 minutes of data collection and then dynamic with a straight trajectory moving toward West (initial acceleration of 1 m/s^2, constant velocity of 10 m/s, final acceleration of -1 m/s^2). In the last part of the test the spoofer is again static at about 1 km from the true position. The test lasts 24 minutes, and there are 5 Galileo and 8 GPS satellites in view. According to the hypotheses listed at the beginning of the section, all the in-view GPS satellites are authentic, as the receiver is able to reject the forged GPS signals through the use of Chimera. On the other hand, depending on the specific test, all or a subset of the in view Galileo satellites are counterfeit. More specifically 5 tests have been performed, in which the number of the counterfeit Galileo satellites grows from 1 to 5.

The position obtained with the authentic signals and the spoofing trajectory are depicted on the map of FIGURE 12, with green and red dots respectively.

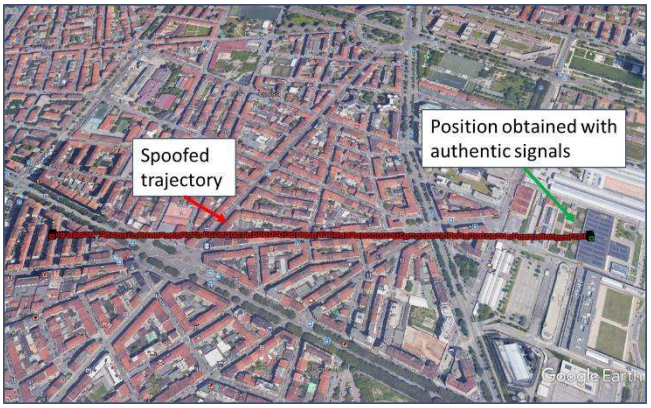

FIGURE 12°. Position obtained with the authentic signals (LINKS Foundation premises roof antenna) and spoofed trajectory: green and red dots respectively.

As an example, the top plot of FIGURE 13 shows the verification of compliance given by equation (2) for the dataset with 4 spoofed Galileo satellites, while the bottom plot is a zoom around the time at which the attack starts (i.e., after 300 seconds of data collection). It is easy to observe how the joint scheme is able to easily detect the attack, with values of $|t_G[n] - b_G|$ well above the threshold for about the whole duration of the dataset. In this case P_{fa} has been set to 10^{-6}, thus resulting in a threshold of 11 ns.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3107871, IEEE Access

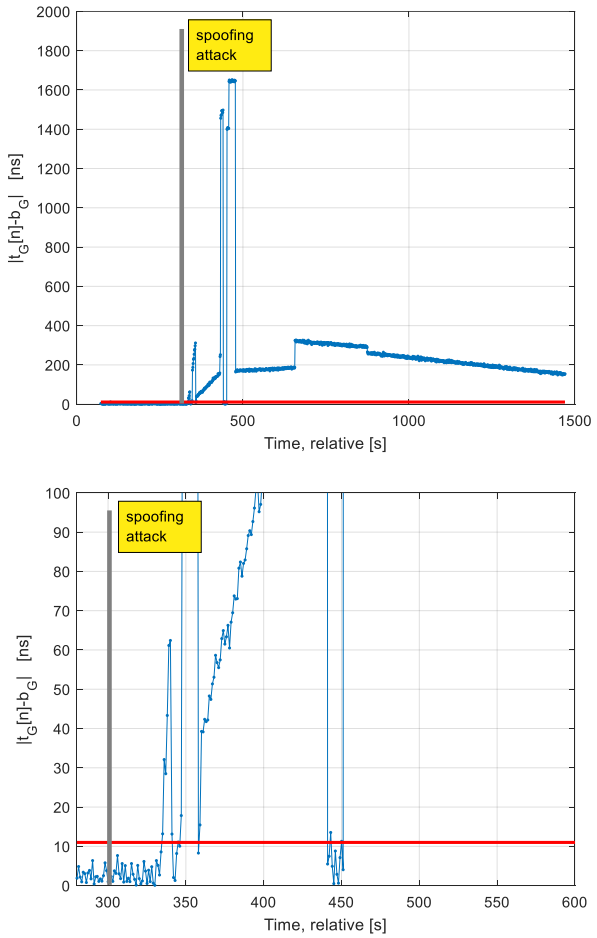

FIGURE 13°. Verification of compliance for the dataset with 4 spoofed satellites (top plot) and zoom around the time instant in which the attack starts (bottom plot).

TABLE III reports the probability of detection P_D for the 5 datasets with 1 to 5 spoofed Galileo satellites, considering the threshold fixed at 11 ns, with $P_{FA} = 10^{-6}$.

P_D is evaluated as N_D/N_T, where N_D is the number of times the metric $|t_G[n] - b_G|$ overcomes the threshold in the time interval after the starting of the attack (i.e.: after second 300 in FIGURE 13), and N_T is the total number of times the metric is evaluated in the same time interval.

TABLE III
P_D, EVALUATED FOR THE 5 DATASETS, GIVEN $P_{FA} = 10^{-6}$. STATIC SCENARIO

# OF SPOOFED GALILEO SATELLITES	P_D
1	0.93
2	0.95
3	0.94
4	0.96
5	0.99

Values of P_D in the table highlight the good performance of the joint scheme, in terms of false alarm and detection probabilities, even with a very limited number of spoofed satellites.

To conclude, FIGURE 14 shows the mitigation of the attack performed by the joint scheme. The green and red lines are in fact the true and the spoofed position respectively, while the blue line is the position error obtained after mitigation through the joint scheme, i.e.: evaluated with only the GPS satellites.

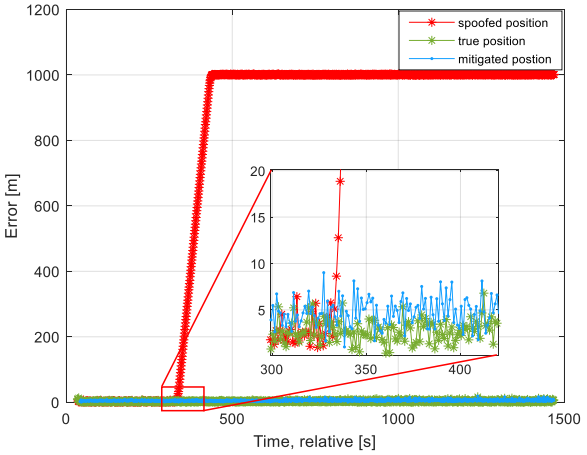

FIGURE 14°. Position error obtained with the authentic signals (green line), with the spoofed signals (red line), and after mitigation (blue line).

Analogously, a similar bench of tests has been carried out in dynamic conditions. In this case, the simulated spoofing scenario foresees that the victim receiver trajectory is static for 3 minutes, and then dynamic following a straight trajectory moving toward North (initial acceleration of 1 m/s^2, constant velocity of 10 m/s). As for the spoofing trajectory, it was superimposed to that of the victim receiver for the first 5 minutes, and dynamic with a straight trajectory moving toward North West (initial acceleration of 1 m/s^2, then constant velocity of 10 m/s North- 10 m/s West). The test lasted 20 minutes, with 5 Galileo and 8 GPS satellites in view, with all the GPS satellites authentic, and all or a subset of the in-view Galileo satellites counterfeit. The position obtained with the authentic signals and the spoofing trajectory is shown on the map of FIGURE 15, with green and red dots respectively.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3107871, IEEE Access

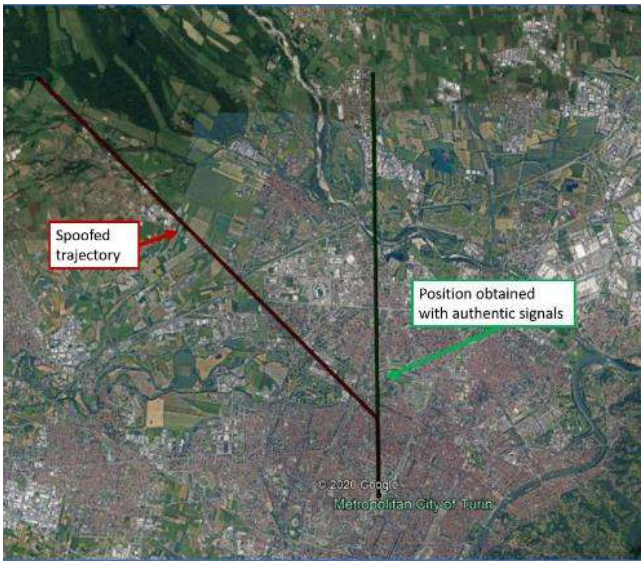

FIGURE 15°. Position obtained with the authentic signals (straight trajectory toward North starting from the LINKS Foundation premises roof antenna) and spoofed trajectory (moving toward North-West after the starting of the attack): green and red dots respectively.

Also in this case, the joint scheme presents very good performance, as reported in TABLE IV that lists the probability of detection for the 5 datasets (in which the number of spoofed Galileo satellites grows from 1 to 5), considering a threshold fixed at 11 ns, with $P_{FA} = 10^{-6}$.

TABLE IV
P_D, EVALUATED FOR THE 5 DATASETS, GIVEN $P_{FA} = 10^{-6}$. DYNAMIC SCENARIO.

# OF SPOOFED GALILEO SATELLITES	P_D
1	0.97
2	0.97
3	0.98
4	0.98
5	0.99

The effects of the mitigation have been evaluated in terms of position error, as shown in FIGURE 16: green and red lines represent the true and the spoofed position respectively, while the blue line is the position error obtained after mitigation through the joint scheme, i.e.: evaluated with only the GPS satellites.

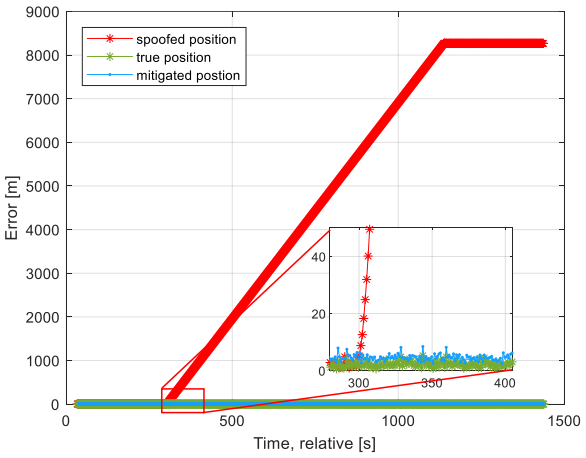

FIGURE 16°. Position error obtained with the authentic signals (green line), with the spoofed signals (red line), and after mitigation (blue line).

C. SPOOFING PRODUCING SMALL POSITION ERRORS

This section presents the tests under a spoofing attack able to produce small position errors, i.e.: up to tens of meters.

The simulated spoofing scenario foresees that the victim receiver is static, while the spoofing trajectory is superimposed to that of the victim receiver for the first 5 minutes, and then alternatively dynamic with a straight trajectory moving toward East (initial acceleration of 1 m/s^2, constant velocity of 1 m/s East) and static for 5 minutes at 10, 20, 50, and 100 meters from the victim receiver true position. The positions obtained with the authentic signals and the spoofing ones are shown on the map of FIGURE 17, with green and red dots, respectively.

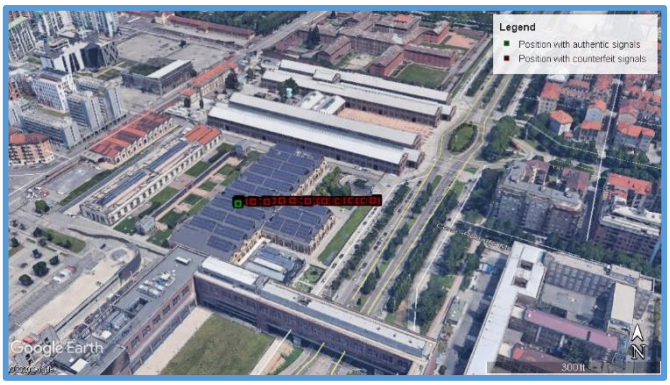

FIGURE 17°. Position obtained with authentic signals, static position at the LINKS Foundation premises roof antenna (green dots), and spoofed trajectory, moving toward East after the starting of the attack (red dots).

More in details, TABLE V summarizes the probabilities of detection corresponding to certain maximum imposed position errors (i.e., 10, 20, 50 and 100 meters). The joint scheme can detect attacks that impose position errors on the victim receiver exceeding 10 meters. On the contrary, for very small position errors (< 10 m), P_D is close to zero.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3107871, IEEE Access

TABLE V
P_D FOR CERTAIN MAXIMUM IMPOSED POSITION ERRORS.

MAXIMUM IMPOSED POSITION ERROR (M)	P_D
10	0.08
20	0.98
50	1
100	1

D. TIMING SPOOFING ATTACK

This section presents the results of the tests under a timing spoofing attack. In details, the simulated spoofing scenario, that lasts 30 minutes, foresees that all the Galileo signals are counterfeit, while all the GPS ones are authentic. The effect produced on receiver clock bias and receiver clock drift are those depicted in FIGURE 18, i.e.: at the 4th, 11th, and 16th minute from the start of the data collection, a drift of up to 20 ns/s is imposed on the victim receiver for 2, 1, and 1 seconds respectively, corresponding to additional 10, 5, and 5 meters imposed on the clock bias.

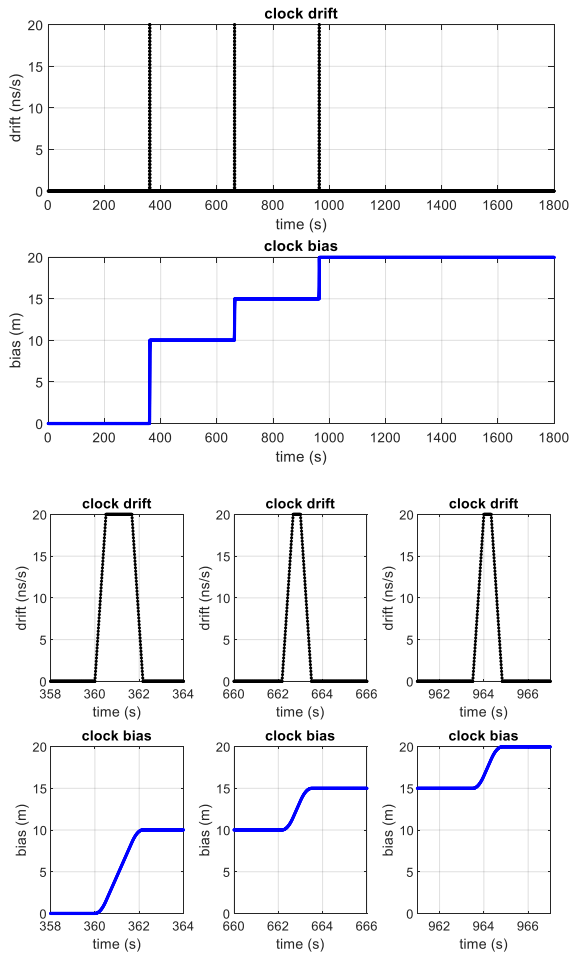

FIGURE 18°. Clock drift and clock bias imposed on the victim receiver (upper plot) and zooms (lower plot) around the time instants of clock bias variations.

This type of attack distorts the time information at the output of the victim receiver. It might be dangerous because the position solution does not result affected, as highlighted by the comparison in FIGURE 19.

Indeed, the imposed bias is directly flipped on the estimated GGTO. This is clear from FIGURE 20, that compares the estimated GGTO in nominal conditions and under spoofing attack. Roughly speaking, the three 'steps' in the bias trend are of around 34, 50, and 68 ns (from the -10 ns in the absence of attack), correspondent to the 10, 15, 20 meters of imposed error.

Consequently, the joint scheme is able to easily detect the attack for the whole data collection, providing a probability of detection of 1, even for very low value of P_{FA}, i.e.: 10^{-6}, as shown in FIGURE 21.

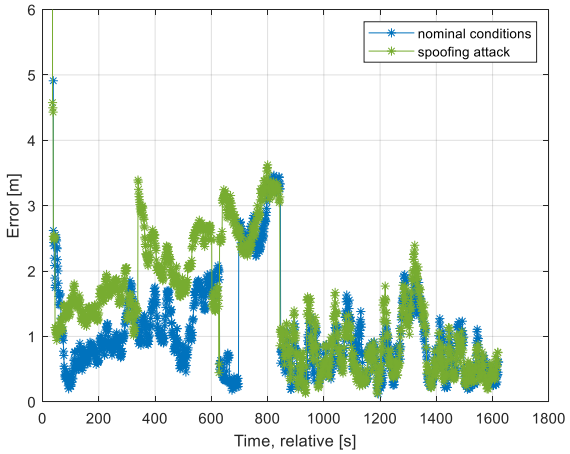

FIGURE 19°. Comparison between the position error in nominal conditions and under the timing spoofing attack.

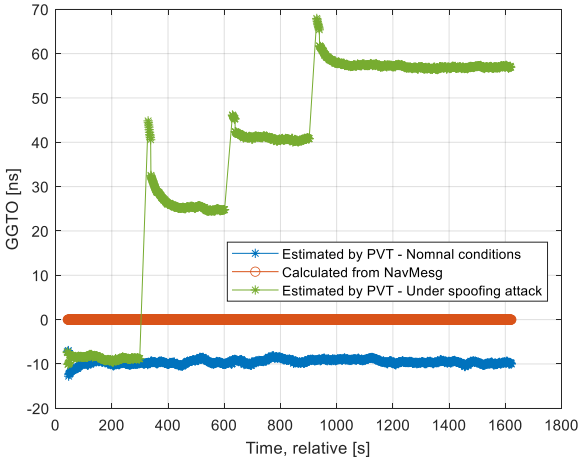

FIGURE 20°. Comparison between the estimated GGTO in nominal conditions and under the timing spoofing attack.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3107871, IEEE Access

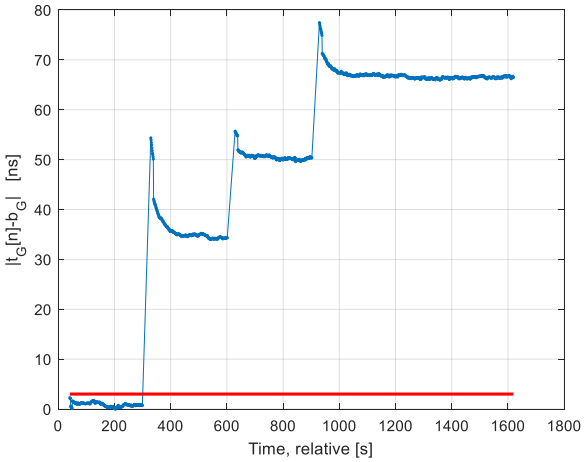

FIGURE 21°. Verification of compliance for the spoofed dataset.

E. SPOOFED SATELLITES BELONGING TO BOTH CONSTELLATIONS

This section presents the tests under a spoofing attack able to produce small position errors, i.e.: up to tens of meters. The main difference respect to previously presented tests (section *C*) is that in this new bench of tests, the attacker is able to falsify not only Galileo, but also GPS signals, thus producing an attack with spoofing signals that belong to both constellations.

In other words, for this specific test, the Chimera protocol is considered not exploited by the receiver. In fact, the joint Chimera/OSNMA scheme has been designed with the scope of detecting anomalies between constellations. This specific test wants to further investigate the performance of the joint scheme, by relaxing the assumption of fully protection of the GPS signals.

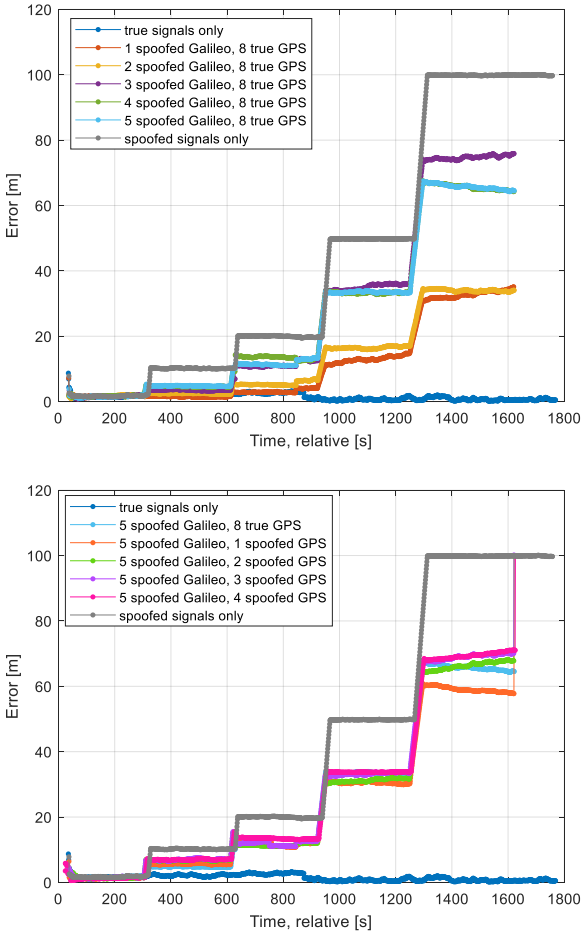

FIGURE 22°. 3D error of the position obtained with authentic signals only (blue line), counterfeit signals only (grey line), and both types of signals (colored lines). Upper plot: GPS constellation: entirely authentic, Galileo constellation: 1 to 5 spoofed satellites (Tests #1 to #5). Lower plot: Galileo constellation: entirely spoofed, GPS constellation: 1 to 4 spoofed satellites (Tests #6 to #9).

As for the victim receiver and spoofing trajectories we can refer to that described in section *C*, FIGURE 17. Here, we performed 9 tests: all of them last 30 minutes, and in all data collections there are 5 Galileo and 8 GPS satellites in view. For the tests #1 to #5 the number of spoofed Galileo satellites grows from 1 to 5, while, in the tests #6 to #9 all the Galileo satellites are spoofed, and the number of GPS satellites grows from 1 to 4.

FIGURE 22 shows the 3D error of the position obtained with authentic signals only (blue line), counterfeit signals only (grey line), and both types of signals (colored lines). The top plot of FIGURE 22 depicts the errors for the cases in which all the GPS constellation is authentic and the number of spoofed Galileo satellites grows from 1 to 5 (i.e.: whole constellation). The bottom plot is related to the cases in which the all the Galileo constellation is counterfeit and the number of spoofed GPS satellites grows from 1 to 4 (i.e.: half constellation).

It is easy to observe how the grey line follows the spoofed trajectory described above, while in the other cases the error is

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3107871, IEEE Access

attenuated due to the presence of authentic signals in the PVT computation.

By following the procedure described in section III, it is possible to apply the verification of compliance to all the described datasets. FIGURE 23 shows the verification of compliance applied to a subset of configurations. The threshold has been set for a probability of false alarm of 10^{-6}.

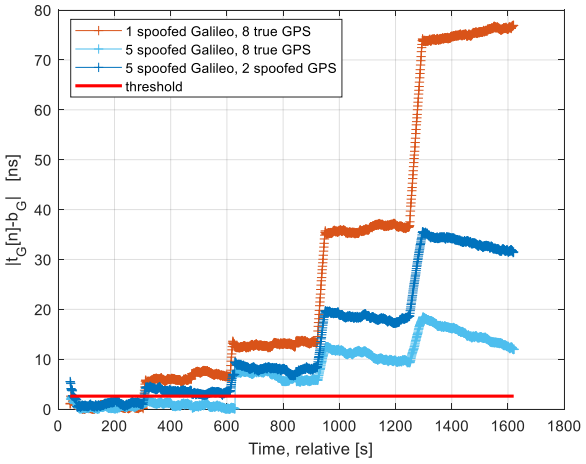

FIGURE 23°. Examples of verification of compliance for the spoofed datasets, for different numbers of spoofed Galileo and GPS satellites.

The complete results are summarized in TABLE VI, that shows the probability of detection obtained in all the analyzed configurations.

For the datasets in which the whole GPS constellation is authentic, the joint scheme easily detects the attack, with a probability of detection always greater than 75%, with peaks of 99%. On the other hand, when the whole Galileo constellation is counterfeit, and there is a subset of false GPS satellites, the joint scheme is able to detect the attack only when the number of fake GPS signals is less than the half of the total number of in view satellites. In fact, when we have 4 or more spoofed GPS satellites the probability of false alarm drops to less than 20%. This is in line with the expectation because the joint scheme is designed to detect anomalies between the two constellations and does not work if the attack affects the two systems in a consistent way. Nevertheless, good results have been obtained also in the cases in which some of the GPS satellites are also counterfeit.

Finally, the variation of detection probability in the different scenarios is worth being commented. Indeed, in the first 5 tests, Galileo is the only attacked constellation and one would expect P_D to grow with the number of spoofed satellites, while it actually decreases. This is due to the fact that the first part of the attack produces small position errors, i.e.: around 10 meters, which is the limit for the joint scheme to work properly, as shown in the experiment of section V.C (see TABLE V). In such conditions, the metric used for the detection is close to the threshold and specific user receiver conditions (e.g.: geometry of the satellites in view, tracking loops performance) might strongly affect P_D. For the sake of completeness, TABLE VI also includes the values of P_D, evaluated on the time interval in which the attack produces errors exceeding 10 m, i.e., after 600 seconds from the start of the data collection: P_D results equal to 1 in all the tests #1 to #5. Similarly, the same time interval is considered for the evaluation of P_D, also for the tests #6 to #9. For the first three tests P_D is close to 1, and drops to 0.22 in the test #9, highlighting the relationship between number of GPS spoofed satellite and detection performance.

TABLE VI
PROBABILITY OF DETECTION VS NUMBER OF SPOOFED GALILEO AND GPS SATELLITES. $P_{FA} = 10^{-6}$.

Tests number	# of spoofed Galileo satellites	# of spoofed GPS satellites	P_D	P_D (for position error exceeding 10 m)
1	1	0	0.99	1
2	2	0	0.99	1
3	3	0	0.99	1
4	4	0	0.86	1
5	5	0	0.75	1
6	5	1	0.77	0.98
7	5	2	0.99	1
8	5	3	0.99	1
9	5	4	0.17	0.22

VI. CONCLUSIONS

The joint Chimera/OSNMA scheme has been designed to be implemented inside multi-constellation receivers, able to exploit both the Chimera and OSNMA enhancements on the GPS and Galileo satellites signals, respectively. The joint scheme in fact leverages the current version of Chimera and OSNMA single concepts, exploiting specific characteristics of the single techniques: as for Chimera, the fact that it is able to assure ranging level authentication, while, for the OSNMA, the fact that it authenticates the GGTO, broadcast by Galileo signals.

The paper presents the scheme, along with the details on the algorithm calibration and the results of a wide bench of tests that prove the high performance of the solution under different types of spoofing attack and user conditions. Indeed, the joint scheme can detect several spoofing attacks, achieving very good performance in terms of false alarm and detection probabilities, also in the case there is only one or few spoofed satellites.

As a final remark, from the analyses carried out, it is clear how the joint scheme brings important benefits in the case one of the two constellations enhances navigation message authentication strategies and the other both navigation message and spreading code authentication. Nevertheless, the implementation of the scheme is also feasible when the signals are not authenticated or when both constellations have

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

NMA+SCA strategies. Of course, in these cases the benefits might be somehow limited.

This paper illustrates the benefits brought by authentication schemes to the monitoring of the position domain solutions, with the example of the timing solutions monitoring through the GGTO. The same principles can also benefit other techniques, such as ARAIM, where sub-set testing could be done against a reference solution computed with authenticated data and ranges.

REFERENCES

[1] European GNSS (Galileo) Open Service Signal-In-Space Interface Control Document. OS SIS ICD, Issue 1.3, December 2016. Available at: https://www.gsc-europa.eu/electronic-library/programme-reference-documents#open

[2] GPS Enterprise Space & Missile Systems Center (SMC) – LAAFB, "NAVSTAR GPS Space Segment/Navigation User Segment Interfaces," IS-GPS-200, 3 August 2020. Available at https://www.gps.gov/technical/icwg/#current

[3] K. McCaney, "Yacht hijacking shows the potential power of GPS spoofing," *GCN*, Aug 01, 2013

[4] Inside GNSS, "Sinister Spoofing in Shanghai," Inside GNSS website, December 10, 2019

[5] D. Goward, "New GPS 'circle spoofing' moves ship locations thousands of miles," *GPS World*, May 26, 2020

[6] E. Falletti, D. Margaria, G. Marucco, B. Motella, M. Nicola and M. Pini, "Synchronization of Critical Infrastructures Dependent Upon GNSS: Current Vulnerabilities and Protection Provided by New Signals," in *IEEE Systems Journal*, vol. 13, no. 3, pp. 2118-2129, Sept. 2019, doi: 10.1109/JSYST.2018.2883752.

[7] M. L. Psiaki and T. E. Humphreys, "GNSS Spoofing and Detection," *in Proceedings of the IEEE*, vol. 104, no. 6, pp. 1258-1270, June 2016, doi: 10.1109/JPROC.2016.2526658

[8] F. Dovis, *GNSS Interference Threats and Countermeasures*. Norwood, MA: Artech House, 2015

[9] C. Günther, "A Survey of Spoofing and Counter-Measures," NAVIGATION, Journal of the Institute of Navigation, Volume 61, Number 3, pages 159 – 177

[10] I. Fernández-Hernández, T. Walter, K. Alexander, B. Clark, E. Châtre, C. Hegarty, M. Appel, M. Meurer, 'Increasing International Civil Aviation Resilience: A Proposal for Nomenclature, Categorization and Treatment of New Interference Threats', Jan. 2019, pp. 389–407, doi: 10.33012/2019.16699.

[11] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle, 'GPS Vulnerability to Spoofing Threats and a Review of Antispoofing Techniques', *International Journal of Navigation and Observation*, vol. 2012, p. e127072, Jul. 2012, doi: 10.1155/2012/127072.

[12] T. E. Humphreys, 'Detection Strategy for Cryptographic GNSS Anti-Spoofing', *IEEE Transactions on Aerospace and Electronic Systems*, vol. 49, no. 2, pp. 1073–1090, Apr. 2013, doi: 10.1109/TAES.2013.6494400.

[13] E. Falletti, G. Falco, V. H. Nguyen and M. Nicola, "Performance Analysis of the Dispersion of Double Differences Algorithm to Detect Single-Source GNSS Spoofing," in *IEEE Transactions on Aerospace and Electronic Systems*, doi: 10.1109/TAES.2021.3061822.

[14] H. Kuusniemi, J. Blanch, Y.-H. Chen, S. Lo, A. Innac, G. Ferrara, S. Honkala, M.Z.H. Bhuiyan, S. Thombre, S. Söderholm, T. Walter, R.E. Phelts, P. Enge, "Feasibility of Fault Exclusion Related to Advanced RAIM for GNSS spoofing detection," *Proceedings of the 30th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2017)*, Portland, Oregon, September 2017, pp. 2359-2370.

[15] T. Humphreys, B. Ledvina, M. Psiaki, B. O'Hanlon, P. Kintner, 'Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer', *Proceedings of the 21st International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2008)*, Savannah, GA, September 2008, pp. 2314-2325.

[16] Wesson, K., Rothlisberger, M. and Humphreys, T. (2012), "Practical Cryptographic Civil GPS Signal Authentication," *Journal of the Institute of Navigation*, 59: 177-193

[17] 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 Processing Magazine*, vol. 34, no. 5, pp. 27-37, Sept. 2017. doi: 10.1109/MSP.2017.2715898

[18] European Commission, Galileo Navigation Message Authentication Specification for Signal-In-Space Testing – v1.1. grow.ddg3.j.1(2018)1670062. October 2018

[19] 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

[20] Alan Cameron, "AFRL tests Chimera to battle spoofers and hackers," *GPS World website*, July 24, 2019. Available here: https://www.gpsworld.com/afrl-tests-chimera-to-battle-spoofers-and-hackers/

[21] J. M. Anderson et al., "Chips-Message Robust Authentication (Chimera) for GPS Civilian Signals," *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.

[22] Scott, L., "Anti-Spoofing & Authenticated Signal Architectures for Civil Navigation Systems," Proceedings of the 16th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GPS/GNSS 2003), Portland, OR, September 2003, pp. 1543-1552.

[23] I. Fernandez-Hernandez, G. Vecchione, F. Diaz-Pulido, "Galileo Authentication: A Programme and Policy Perspective," *69th International Astronautical Congress (IAC2018)*, Bremen, Germany, 1–5 October 2018

[24] ISO/IEC 29192-7:2019, "Information security - Lightweight cryptography - Part 7: Broadcast authentication protocols," July 2019

[25] K. Chino, D. Manandhar and R. Shibasaki, "Authentication technology using QZSS," *2014 IEEE/ION Position, Location and Navigation Symposium - PLANS 2014*, Monterey, CA, 2014, pp. 367-372

[26] L. Tosato, A.D. Chiara, C. Wullems, G.F. Serrano, A. Calabrese, A. Perrig, M. Mabilleau, G. Vecchione, "Broadcast Data Authentication Concepts for Future SBAS Services," *Proceedings of the 33rd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2020)*, September 2020, pp. 1-26.

[27] A. Neish, T. Walter, J.D. Powell, "SBAS Data Authentication: A Concept of Operations," *Proceedings of the 32nd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2019)*, Miami, Florida, September 2019, pp. 1812-1823.

[28] Motella, B., Margaria, D., Paonni, M., "SNAP: An authentication concept for the Galileo open service," *018 IEEE/ION Position, Location and Navigation Symposium*

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3107871, IEEE Access

(PLANS), Monterey, CA, 2018, pp. 967-977, doi: 10.1109/PLANS.2018.8373475.

[29] C. Gioia, J. Fortuny-Guasch and F. Pisoni, "Estimation of the GPS to Galileo time offset and its validation on a mass market receiver," *2014 7th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC)*, Noordwijk, 2014, pp. 1-6, doi: 10.1109/NAVITEC.2014.7045145

[30] http://gnss-sdr.org/node/51

[31] M. Fantino, A. Molino, and M. Nicola. "NGene: A complete GPS and Galileo software suite for precise navigation", Institute of Navigation - International Technical Meeting 2010 (ITM 2010), San Diego, CA, USA, January 2010; pp. 1245-1251

[32] NUT4NT—Amungo Navigation. Available online: https://www.crowdsupply.com/amungo-navigation/nut4nt

[33] IFEN - GNSS Simulator and Receiver Products and Services. Available online: https://www.ifen.com/products/ (accessed on 10 July 2020)

[34] M. Troglia Gamba, M. Nicola and B. Motella, "Galileo OSNMA: an implementation for ARM-based embedded platforms," *2020 International Conference on Localization and GNSS (ICL-GNSS)*, Tampere, Finland, 2020, pp. 1-6

[35] B. Motella, M. Troglia Gamba, M. Nicola, "A real-time OSNMA-ready software receiver," *Proceedings of the 2020 International Technical Meeting of The Institute of Navigation*, San Diego, California, January 2020, pp. 979-991

[36] M. Troglia Gamba, M. Nicola, B. Motella, "GPS Chimera: A Software Profiling Analysis," *Proceedings of the 33rd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2020)*, Sept. 2020, pp. 3781-3793

Dr. BEATRICE MOTELLA received the M. Sc. and Ph. D. degrees from Politecnico di Torino, respectively in 2003 and 2008. During the Ph. D program, she spent one year at the satellite navigation and positioning laboratory, at the University of New South Wales, Sydney, Australia.

Currently, she is a senior researcher at the LINKS Foundation in Turin, Italy. Her activities cover different aspects of the signal processing for radio navigation receivers, with a major focus on GNSS interference monitoring. Recently, 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.

Dr. MARIO NICOLA received the M.S. in Computer Science Engineering from the Politecnico di Torino in 2002. In 2005 he obtained his Ph.D. degree in Electronics and Communications Engineering working on reconfigurable architectures for wireless communication systems.

He is a researcher in the staff of the Space and Navigation Technologies research area at LINKS Foundation, Italy. His main activity is the implementation of algorithms for software radio GPS/Galileo receivers.

Dr. SOPHIE DAMY received an M.Sc in Aeronautical Telecommunications from ENAC (French National School of Civil Aviation), Toulouse, France in 2011 and a Ph.D. degree from the Centre for Transport Studies of Imperial College London, UK, in 2017.

She is currently a scientific project officer at the Joint Research Centre of the European Commission in Ispra, Italy, in the field of satellite based navigation.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/