Receiver Protocol and Pitfalls of NMA and SCA Processing Under Spoofing Conditions for Future GNSS Signals Authentication

Markel Arizabaleta, Thomas Pany, *Universität der Bundeswehr München, Germany*
Tommaso Scuccato, Andrea Dalla Chiara, *Qascom, Italy*
Cillian O'Driscoll, *Cillian O'Driscoll Consulting Limited, Ireland*
Neil Hanley, *Queen's University Belfast, United Kingdom*

BIOGRAPHY (IES)

Markel Arizabaleta is a research associate at the Universität der Bundeswehr München since 2017, where he is involved in GNSS signal processing and signal authentication. He has a M. Sc. in Telecommunication Engineering, and he studied in the University of the Basque Country (UPV-EHU), Spain, and in Tampere University of Technology, Finland, where he has previously been involved on joint 5G communications and positioning systems.

Prof. Thomas Pany is with the Universität der Bundeswehr München at Space Systems Research Center (FZ-Space) where he leads the satellite navigation unit LRT 9.2 of the Institute of Space Technology and Space Applications (ISTA). He teaches navigation focusing on GNSS, sensors fusion and aerospace applications. Within LRT 9.2 a good dozen of full-time researchers investigate GNSS system and signal design, GNSS transceivers and high-integrity multi-sensor navigation (inertial, LiDAR) and is also developing a modular UAV-based GNSS test bed. ISTA also develops the MuSNAT GNSS software receiver and recently focuses on Smartphone positioning and GNSS/5G integration. He has a PhD from the Graz University of Technology (sub auspiciis) and worked in the GNSS industry for seven years. He authored around 200 publications including one monography and received five best presentation awards from the US institute of navigation. Thomas Pany also organizes the Munich Satellite Navigation Summit.

Tommaso Scuccato received a B. Sc. degree in Electronics and Telecommunication Engineering and a M. Sc. In Information and Communication Engineering from University of Trento (Italy). His research activities were focused on remote sensing radars for planetary observation. He joined Qascom in 2018, where he has been involved in the development of GNSS software simulators and receivers, with a particular interest in signal authentication.

Dr. Andrea Dalla Chiara is currently leading the Simulation Tools Division in Qascom; formerly he has been designer and developer of GNSS/SBAS simulators and receivers focusing on authentication techniques at signal and data level. He collaborates with Qascom since 2010, where he actively participated in many projects with ESA, NASA, the European Commission and Industry. Previously he led a SME in the radio frequency identification domain and he worked for Infineon as designer and test engineer of smart power ICs. He holds a MSc degree in Microelectronics from University of Padova (Italy) and a PhD in Information Technology with focus in instrumentation and measurements and RF interference.

Dr. Cillian O'Driscoll received his M.Eng.Sc. and Ph.D. degrees from the Department of Electrical and Electronic Engineering, University College Cork, Ireland. He was a senior research engineer with the Position, Location and Navigation (PLAN) group at the Department of Geomatics Engineering in the University of Calgary from 2007 to 2010.

He was with the European Commission from 2011 to 2013, first as a researcher at the JRC, and later as a policy officer with the European GNSS Programmes Directorate in Brussels. From January 2014 to June 2017, Dr O'Driscoll was a research fellow at University College Cork. He is currently an independent consultant. His research interests are in all areas of GNSS signal processing.

Dr. Neil Hanley is a Principal Engineer at the Centre for Secure Information Technologies (CSIT), at Queen's University Belfast, UK. His research interests include cryptographic engineering, embedded security and FPGA design, with a focus on physical unclonable functions, side-channel analysis and hardware cryptographic accelerators, including for quantum resilient encryption schemes. He holds a PhD in Engineering from University College Cork, Ireland, and a B.Eng in Electrical & Electronic Engineering from the same institution.

ABSTRACT

The scope of the paper is to provide a generic receiver architecture that can cope with future Navigation Message Authentication (NMA) and Spreading Code Authentication (SCA) for the open service (OS) Global Navigation Satellite System (GNSS) signals. The authentication proposals can be divided in those that suggest the encryption of the navigation data, those that suggest encryption of the spreading code, and those that suggest combining both encryptions. However, on the receiver side, the mere implementation of such algorithms is not enough to identify a spoofing attack, and therefore, further receiver capabilities need to be considered when defining a GNSS signal authentication receiver architecture.

The primary goal of the investigation is to define a receiver architecture capable of detecting spoofing attacks and to identify the possible pitfalls that affect the receiver performance. For this purpose, a new signal is defined to provide authentication capabilities to a mass-market receiver. The proposed receiver architecture is then used with the newly defined authentication signal to test the spoofing detection capabilities under different receiver conditions, and attack scenarios. The scope of the verifications is to identify the possible pitfalls that might wrongfully affect to the spoofing detection mechanism.

INTRODUCTION

Authentication is nowadays one of the main topics to be covered for the current and next generation Open Service (OS) Global Navigation Satellite System (GNSS) signals. Among the techniques suggested in literature, two main concepts have already been defined at signal design level: navigation message authentication (NMA) and spreading code authentication (SCA). The first one, NMA, consists on encrypting the navigation message data bits that are transmitted so that the receiver can employ an asymmetric algorithm (based on private-public key concept) to verify that the navigation data has been generated indeed by the space segment. Some examples of the NMA implementation are discussed in literature in [1]-[3] and more specific for the Galileo system in [4]-[5], which uses the ‘reserved1’ field of the E1-B navigation message to deliver the encryption of the navigation message. The Galileo Open Service Navigation Message Authentication (OSNMA) protocol is based on time efficient stream loss-tolerant authentication (TESLA) concept [6]-[7]. The second authentication concept, spreading code authentication, is based on encrypting the spreading code in order to protect the pseudorange measurements.

To protect the navigation data, navigation message encryption (NME) techniques and navigation message authentication techniques can be used. Similarly, to protect the spreading code, spreading code encryption (SCE) techniques and spreading code authentication (SCA) techniques can be used [1]-[3]. For the NME and SCE cases, the encryption requires symmetric keys, which are secret and cannot be extracted from the receiver. Therefore, a tamper resistant receiver is required, which generates internally the encrypted navigation data and the secret spreading code and compares the results with the incoming data and encrypted spreading code. For mass-market receivers, the symmetric encryption techniques cannot be used because there is no available way of protecting the secret keys. Consequently, mass-market receivers must employ NMA and SCA techniques for authentication purposes. The difference with these techniques is that the key employed for encrypting in the transmitter side (space segment in this case), is provided also to the receiver with a certain delay, so that the authentication is done with a certain delay.

Against the encrypted navigation data bits, and spreading code chips, there are two main threats: meaconing [2], [8] and security code estimation and replay (SCER) attacks [2], [8]-[9]. The meaconing attack is based on retransmitting the signal on-the-fly, which can be done by using, for example, a repeater. Therefore, meaconing attacks are considered to be an easy to perform attack. On the other hand, the SCER attacks are considered to be more complex attacks. SCER attacks are based on estimating the encrypted chips (or navigation bits) and retransmitting them. The complexity of such attacks come into the requirement of low processing latency, as the estimation needs to be implemented as soon as possible so that the spoofing signal is transmitted as soon as possible. Additionally, the estimation of encrypted chips is cumbersome due to the transmission of GNSS signals below the noise floor. To perform a good estimation of the encrypted chips, an attacker requires a high gain antenna, which can only be employed to spoof a single satellite, and therefore several of such antennas are required to spoof all the satellites in view of a single GNSS constellation. The issue with such antennas is they are physically large, bulky, and costly. An alternative to use high-gain antennas are antenna arrays, which use

several elements to achieve a high-gain, and a single antenna array would also be valid to acquire and track simultaneously all satellites in view. Anyhow, the higher the desired antenna gain, the higher is the number of elements required for the antenna array to reach the desired antenna gain, which makes the antenna array also bulky.

The objective of this publication is to define the overall receiver protocol and requirements for performing NMA and SCA authentication schemes, and to identify the receiver pitfalls. To achieve this, first, the experimental set-up is introduced, where the software tool-chain employed to test the receiver authentication protocol is introduced, with the definition of a new authentication signal, and the two scenarios, which include the following channel models: a static additive white Gaussian Noise (AWGN) and a dynamic land-mobile-satellite (LMS). Afterwards, the receiver authentication protocol is presented for a generic GNSS receiver and the assumptions considered are introduced. Knowing the test scenarios and the receiver authentication protocol and assumptions, the results obtained from the test under spoofing and SCER attack are discussed. Finally, the observed receiver limitations and pitfalls are identified.

EXPERIMENTAL SET-UP

The experimental set-up selected for testing the receiver architecture proposed in the next section is based on the Galileo E1-B/C signals at a reception power density of 50 dB-Hz. In addition to the Galileo Open Service (OS) signal, a new signal (E1-N) is generated with two components, an in-phase and a quadrature-phase component, both Binary Phase Shift Key (BPSK) modulated at a chip rate of 1.023 Mchip/s and centered in the center frequency of the L1/E1 band (i.e. centered at 1.57542 GHz). The in-phase component is completely dedicated to the authentication data transmission. The authentication data component, from now on E1-N data component, has been designed with the following characteristics:

- Data rate of 241 bps, from which 217 bits are employed for the authentication data and 24 for the cyclic redundancy check (CRC) error detection
- Tail of 4 bits
- Turbo encoded with rate ½
- 10 symbols included before the authentication data for synchronization purposes

Therefore, a total of 500 symbols are transmitted per second. A second of authentication data bits is illustrated in Figure 1.

Payload	CRC	Tail
217 bits	24 bits	4 bits

Figure 1. Structure of the navigation message

On the other hand, the quadrature phase, from now on anti-spoofing protection (ASP) component, is a fully encrypted pilot component, which carries the secret spreading code chips to be SCA authenticated in a delayed manner. Regarding the transmission power of each E1-N signal component, the E1-N data component is transmitted at nominal power (i.e., at the same transmission power than the E1-B or E1-C), while the E1-N ASP component is transmitted 10 dB below the nominal power.

Regarding the E1-N data component, an authentication frame has been selected to be 5 seconds long, as it is the duration of the E1-N ASP component. It means that one authentication frame is made up of 5 messages. The authentication data involved in the designed protocol are:

- Signature of I/NAV message, for NMA purposes
- ASP seed, so that the receiver can generate the secret spreading code
- ASP seed signature, so that the receiver can verify that the extracted ASP seed has been transmitted from the satellite
- Key management used to update the public keys stored in the receivers. This is out of scope for the current study

Figure 2 provides an overview of the data transmitted during an authentication frame. The first 6 bits of each authentication page, or authentication data second, are used to determine the message type, i.e., for synchronization purposes within an authentication message, which is 30 seconds long. As the authentication message and the I/NAV message sub-frame have the same duration (i.e. 30 s), they are transmitted in parallel. The first page within an authentication frame is used to deliver the ASP seed (128 bits long), which is used to generate the secret spreading code transmitted during the previous authentication frame. The secret spreading code is generated at the transmission side by using an AES-CTR-128 stream-cypher, which provides 128-bits of security. In order to verify if the decoded ASP seed is the correct one, the ASP seed signature, which is 512 bits long, is also transmitted through the authentication signal. The ASP seed signature is generated by using EC-Schnorr on 256-bit elliptic curves giving 128-bit security [10]. In order to retrieve the ASP seed signature, the receiver is required to successfully decode the first four pages from an

authentication frame. In order to improve the data availability of the ASP seed and its signature, the use of a common ASP seed has been defined for all satellites, which are then XOR-ed with the satellite pseudo-random-noise (PRN) number and then used to generate the satellite specific secret spreading code. Moreover, the private key used to generate the ASP seed signature is shared among all the satellites, resulting even in the same signature and thus improving the service availability. The third authentication element transmitted in the E1-N data component is the I/NAV signature. In order to retrieve the I/NAV signature, all second to fourth pages need to be successfully decoded from all authentication frames within a 30 s long authentication message. In this case, as the I/NAV and its signature are extracted in parallel, the NMA protocol can be implemented as soon as the whole I/NAV sub-frame is decoded. Similar to the ASP seed signature, the I/NAV signature is generated at the transmission side by using EC-Schnorr [10].

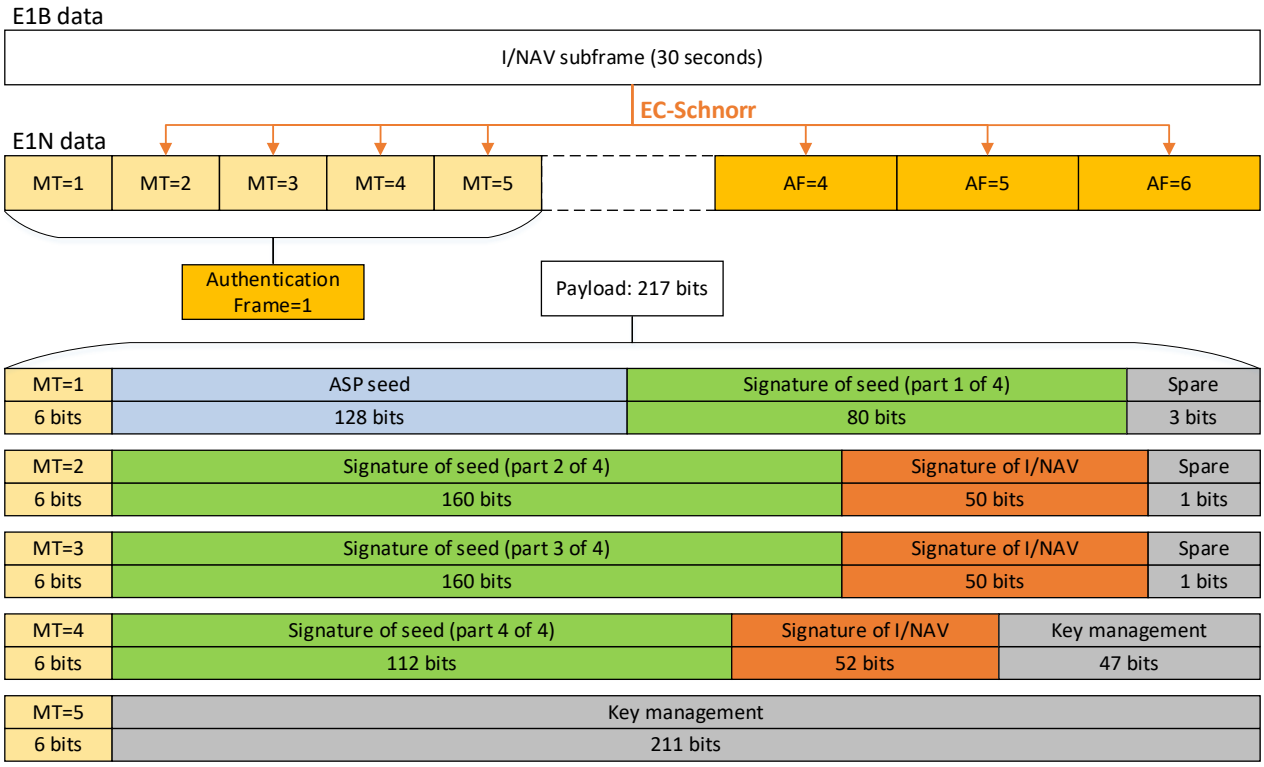

Figure 2. Authentication data transmission structure

Finally, the key management bits are transmitted in the fourth and fifth pages within an authentication frame.

To perform the experimentations, a software-based testbed has been defined as shown in Figure 3. First of all, the signal generation is performed by using Qascom's QA707 signal simulator, where the scenarios are defined, including the channel conditions and the environment type (i.e. a benign environment is simulated, or an scenario where the receiver is under attack). Based on the selected scenario, the QA707 outputs a binary file containing the GNSS signals, the authentication signals, and if selected, the spoofing signals. Additionally, it outputs a QA707 signal configuration file with all the relevant information related to each one of the simulated signals. Based on the later configuration file, the MuSNAT configuration file is generated, making the MuSNAT software receiver [11], able to acquire and track the GNSS signals, and by using slave-tracking, to track the authentication signal. All relevant information (e.g. the tracking output and transmission time), is stored in the MuSNAT database, and additionally, MuSNAT outputs a baseband binary file for each snapshot taken from the E1-N ASP component, which are later used in a post-processing manner for SCA verification. Finally, all the authentication procedures are implemented in the developed Matlab-based Secure Receiver (SECREC) module, which emulates the receiver architecture introduced in the next section.

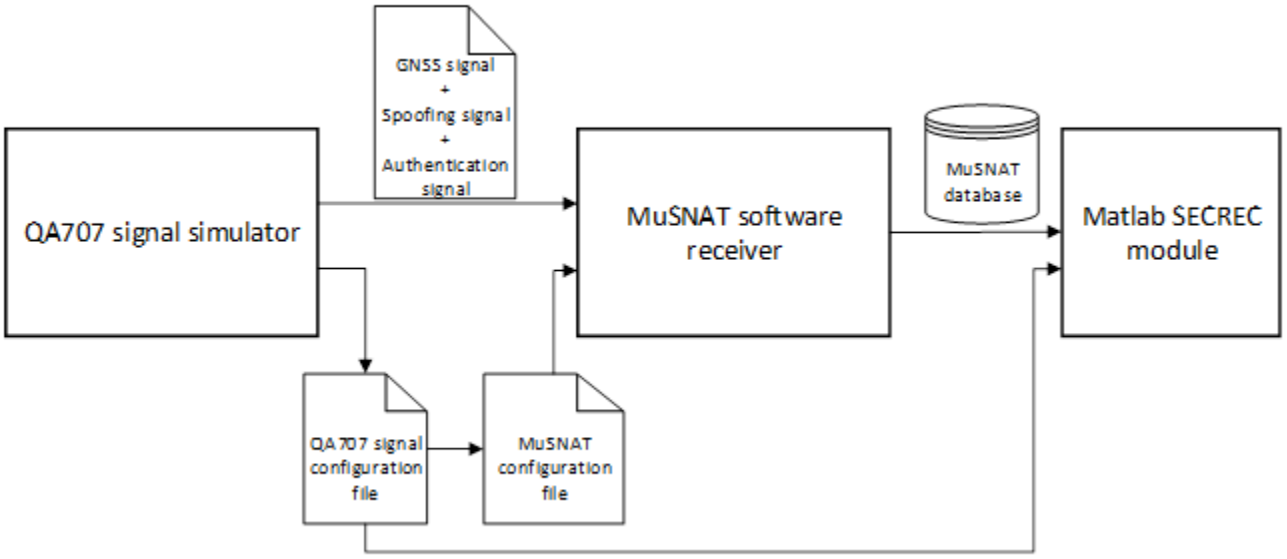

Figure 3. Experimental set-up

The scenarios simulated with the software tool-chain of Figure 3 are mainly a static AWGN and a dynamic LMS channel model. The receiver protocol has been tested under benign channel conditions (i.e., under no attack), and under spoofing and SCER attacks. For the static scenario, the attacker applies an attack that shifts the receiver location towards the east. This is represented on the left-hand of Figure 4 by the QA707 signal simulator, where in red the spoofing trajectory is provided, and on the right-hand of Figure 4 by the MuSNAT software receiver. In the latter, only the trajectory of the spoofing trajectory can be observed, due to the successfully applied attack, and the circles represent the estimated positioning error computed by MuSNAT.

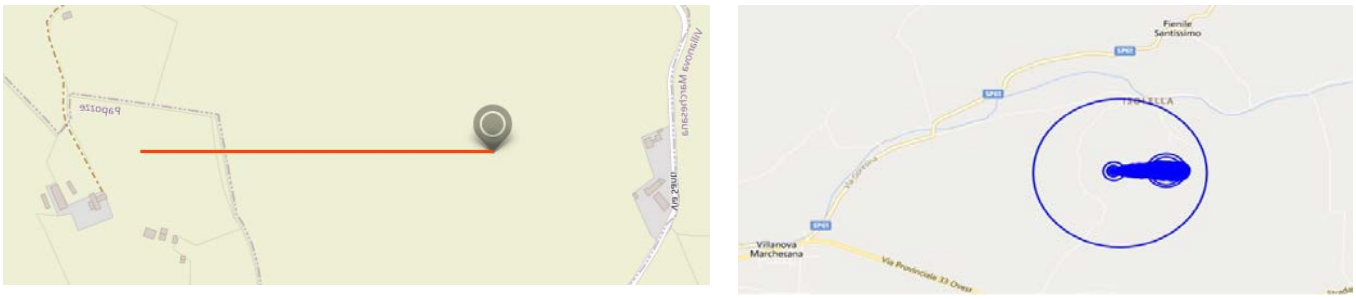

Figure 4. Static AWGN scenario with the trajectory for the spoofed signal retrieved from the QA707 on the left, and the estimated user position extracted from MuSNAT on the right

In the case of the dynamic LMS channel model, the victim receiver is supposed to move linearly towards the East, while the attacker applies a slight deviation to the computed position towards the South. This is represented in the left-hand Figure 5, where in blue the real/victim receiver trajectory is represented and in red the trajectory induced by the attacker. As in the static case, on the right-hand only the deceived receiver's position is observed, provided by MuSNAT.

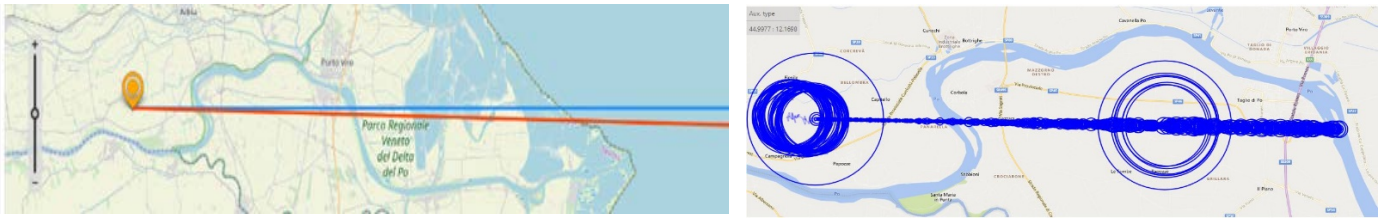

Figure 5. Dynamic LMS scenario with the real (blue) and spoofed (red) signals retrieved from the QA707 on the left, and the estimated user position extracted from MuSNAT on the right

Finally, the satellite position w.r.t. the user position at the beginning of the simulation time must be considered, as it will influence the behaviors of the signals under LMS channel conditions. The implementation of the LMS channel model has been performed following the ITU recommendation P.681 [12]. This is represented in Figure 6, where all the 9 Galileo satellites to acquire and track are observed. Two main observations have been made in the simulations, the first one is that the highest satellite in view, E21, is above 60° of altitude, therefore, the effects of the LMS channel are not noticed in this signal. The second observation is applied to the lower satellite in the skyplot, E6, which is not visible for the whole simulation as after around 700 s of runtime the satellite gets below the 5° elevation mask applied for the simulations. Regarding the rest of the satellites, the influence of the LMS channel is observed to be more severe in those satellites with lower elevation angle.

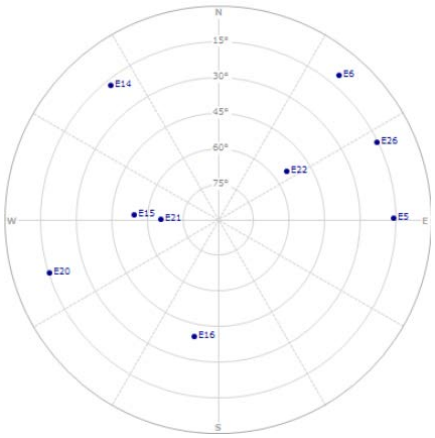

Figure 6. Skyplot of the Galileo satellites at the beginning of the simulation time

RECEIVER ARCHITECTURE AND ASSUMPTIONS

This section describes the receiver architecture for signal authentication for a generic receiver after the signal tracking block. Figure 7 provides the schematic overview of the receiver protocol. It must be noted that the presented schematic is related to a single signal, and that for each signal being authenticated the same procedure must be applied.

The starting point of the authentication functions for a GNSS signal is the correlation output. Currently, mass-market receivers use the correlation output of the navigation data signals to compute the user position, however, when authentication is applied, a reconstruction of the navigation data bits to be authenticated is required and stored until they are authenticated. When authenticating the signals, the correlation output of the authentication signal also needs to be considered. At this point, the authentication signal is considered to be either a new signal containing the authentication information as in the test scenarios presented in the previous section, new pages designed to transmit authentication data such as in GPS L1C Chimera [13]-[14] or certain fields of the navigation message dedicated for the authentication data such as in Galileo OSNMA [4]-[5]. In either of the cases, the navigation and authentication data are demodulated, decoded, and checked for errors. After this process, the receiver will account with the navigation data bits and the authentication data bits separately.

Additionally, the baseband samples containing the encrypted spreading code (fully or partially encrypted) are stored in memory for posteriori spreading code authentication purposes. As the baseband samples need to be code-aligned and carrier wiped-off, for each satellite a different baseband sample file is employed. Furthermore, a different baseband sample file is employed for each ASP snapshot.

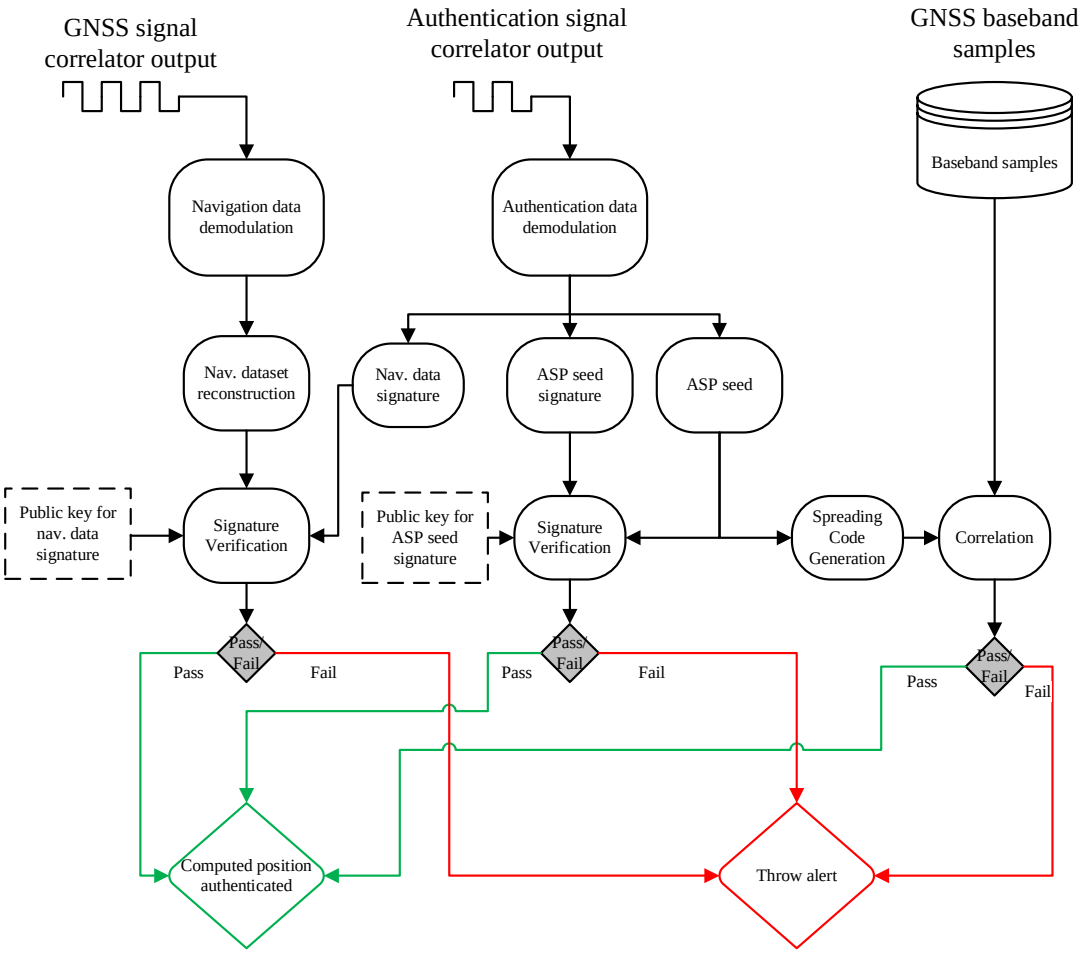

Figure 7. Receiver architecture for GNSS signal authentication

The authentication protocol itself consist on **three** subtasks:

- **Verification of the navigation data**: uses the reconstructed navigation data bits, the I/NAV signature, and a locally (in the receiver) stored public key.
- **Verification of the ASP seed**: it uses the decoded ASP seed, ASP seed signature and the locally (in the receiver) stored public key.
- **Verification of the encrypted spreading code chips**: it uses the ASP seed to generate the fully or partially encrypted spreading codes and the baseband sample files to perform the correlation and verify the presence of the encrypted chips.

The verification of the navigation data requires the selected fields of the navigation data bits which are used to generate the signature in the space segment and the navigation data signature retrieved from the authentication data bits. By using a locally stored public key, the verification routine for the reconstructed navigation data bits can be executed to prove that the navigation data signature extracted from the authentication data bits is correct. If the verification route passes, then the decoded navigation data bits are considered to be authentic, otherwise an alert is thrown.

The verification of the ASP seed requires the bits belonging to two of the authentication data fields: the ASP seed and the ASP seed signature. Similarly, to the navigation data case, the ASP seed is verified by using the ASP seed signature extracted from the authentication data bits, and a locally stored public key (different from the one used for the navigation data verification process). If the verification route passes, then the receiver assumes that the extracted ASP seed has been transmitted from the satellite. In the case of not passing the verification route, the receiver raises an alarm. In order to provide higher authentication data availability, a common ASP seed and signature has been employed in the test scenarios. This allows the receiver to authenticate all signals, even

at low elevation angles (e.g. < 30°), by just extracting the authentication data from any other single satellite, e.g. one at a higher elevation.

The last authentication subtask consists on verifying the encrypted code chips, and for that the extracted ASP seed is used together with the satellite specific PRN number to generate the encrypted code chips by using an AES-CTR-128 stream cypher. The encrypted code chips and the samples stored in the corresponding baseband sample file are correlated in order to determine the presence of the encrypted spreading code. Once the correlation is performed, the receiver must check if the correlation peak is above a given detection threshold, this determines if the encrypted signal is present or not.

Considering that the legacy (E1-B/C) signal has been designed to be acquired and track for a minimum CN0 of 35 dB-Hz [14], and that the encrypted pilot employed in the test scenarios later on is transmitted at 10 dB below the legacy signal, the minimum CN0 for the E1-N ASP component is 25 dB-Hz. Assuming that the received signal is essentially noise, a false alarm of 10^{-6} is achieved at the lower bound of Th_{det} = 24.42 dB-Hz. The chi-squared distribution cumulative function has been used to determine this detection threshold value as indicated in [15].

Furthermore, it has been assumed that a sensitivity of at least 0.9 is desired. As the sensitivity is computed by considering a Rice distribution with its non-centrality parameter set to 25 dB-Hz and considering that every five seconds 2 baseband sample files are stored for later authentication, an integration time of T_{int} = 101 ms is required for the encrypted chips in order to reach the indicated probability of detection P_d = 0.9. This means that every five seconds, two spreading code checks are performed, and that if only one of the correlation peaks surpasses the threshold Th_{det}, then the five seconds to which the encrypted spreading code belongs is assumed to be authenticated. For the testing purposes, a 101 ms snapshot has been performed every 2.5 s.

Moreover, it must be considered that it might not be enough with detecting the encrypted spreading code to determine that the signal is authentic, under a spoofing or an SCER attack, if the attacker does not drive away the victim enough from its true position (projected into the line-of-sight for the respective satellite), the encrypted spreading code might still be detectable with that ASP detection criteria. It might show a degradation in the CN0, but not enough to be below the detection threshold, Th_{det}. On the other hand, a SCER-capable spoofer will overpower its estimate of the E1-N component to ensure some correlation at receiver side. Therefore, a refinement is required in the detection of the encrypted spreading codes. The suggested detection mechanism consists on using the knowledge of the CN0 difference between the legacy and the encrypted pilot component, by defining an upper and a lower threshold, Th_{up} and Th_{low} consecutively, to determine the validity of the detected encrypted spreading code. These two thresholds are computed by defining a so-called margin from the power difference between the legacy and the encrypted spreading code CN0. During the test, a margin of 2 dB have been selected.

$$Th_{up} \geq CN0_{legacy} - CN0_{ASP} \geq Th_{low} \tag{1}$$

$$\begin{aligned} Th_{up} &= CN0_{legacy} - CN0_{ASP,theoretical} + Margin \\ Th_{down} &= CN0_{legacy} - CN0_{ASP,theoretical} - Margin \end{aligned} \tag{2}$$

These three authentication subtasks need to be authenticated in parallel, to validate the whole GNSS (Galileo in the case of the test scenario) signal, if any of them fails, then the signal will not be considered authenticated. In order to consider a computed position authentic, at least four satellites are required to be authenticated.

In summary, the assumptions considered are the following ones:

- All two public keys (for navigation data and for ASP seed verification) are locally stored in the receiver.
- A common ASP seed and ASP seed signature is used by all satellites in a same authentication frame to increase the authentication data available under challenged environments, so that the extraction of the data from a single satellite is enough to authenticate all.
- Encrypted spreading code detection threshold: Th_{det} = 24.14 dB-Hz with $P_{fa} = 10^{-6}$ and an expected $CN0_{min}$ = 25 dB-Hz
- Required integration time of the stored baseband sample file: T_{int} = 101 ms for P_d = 0.9 with 2 E1-N ASP correlation checks every 5 seconds, only one needs to be detected and validated to authenticate that the 5-second-long signal segment.
- A fully encrypted spreading code (E1-N ASP) snapshot has been taken every 2.5 s
- After the detection of the E1-N ASP component, the snapshot needs to be validated by comparing the CN0 difference between the legacy and the E1-N ASP component against a given thresholds as indicated in (1)

- At least four satellite signals need to be authenticated to determine that the user computed position is authentic.

It should be clearly noted that this working assumption can be tailored to the specific use cases where an authentic position and/or time is required. E.g. seeds can for example be retrieved via other secure communications lines (internet) and sample logging might occur at a higher rate (e.g. every 500 ms). The proposed authentication signal is very flexible in its exploitation by the receiver.

RESULTS UNDER SPOOFING AND SCER ATTACK

This section provides the results of the tested receiver protocol in static AWGN and dynamic LMS channel conditions, but first the performed attacks are introduced. The applied attacks are a spoofing attack and a SCER attack. Both attacks transmit synchronously the navigation and authentication data signals.

In the case of the spoofing attack, the secret/encrypted chips of the E1-N ASP component are not estimated, therefore, the attack consist only on estimating the legacy E1-B and authentication E1-N data symbols and retransmitting them. Additionally, the attacks are performed in such a way that at the beginning of the simulation the attacker's signal strength is 30 dB below the one of the real signals, and it gradually increases until it gets 6 dB stronger than the satellite signal, which is achieved after 120 s of the simulation time, and then it starts driving the user position away from its true position while it maintains power advantage of 6 dB.

In the case of the SCER attack, in addition to estimating the data symbols as it is done in the spoofing attack scenario, the spoofer uses an antenna with a 10 dB gain, providing a reception signal power of 60 dB-Hz of the satellite signals. With this antenna the attacker employs the 30% of the chip duration to perform the estimation of the encrypted chips with an assumed chip error rate of 22.16 %. Such systems are described in e.g. [16] and [17]. The SCER attack affects to the detection of the ASP component in the victim's side, and therefore the validation of the detected ASP component explained in the previous section is required.

Considering the properties of the attacks, it can be foreseen that the main difference between the two attacks will be observed on the E1-N ASP detection procedure (the data transmission is equal in both scenarios). By considering the static AWGN scenario first, the validation procedure of the E1-N ASP component is observed in Figure 9 for the spoofing attack, and in Figure 10 for the SCER attack. The power difference between the legacy signal and the ASP component is performed by considering both legacy signals, i.e., the power difference is computed between E1-B/C and E1-N ASP, and this results in 12 dB. By considering a margin of 2 dB and using the expressions in (2), the upper and lower thresholds are computed and employed for the validation of the detected ASP snapshots. For these scenarios, the upper threshold is defined as Th_{up} = 14 dB-Hz, and the lower threshold as Th_{low} = 10 dB. Only if the power difference is located within these two thresholds is considered that an ASP snapshot is authenticated.

In order to provide a reference behavior of the ASP verification procedure, Figure 8 shows the E1-N ASP verification procedure under static AWGN channel conditions at a signal reception of 50 dB-Hz and in benign environment, i.e., under no attack. As it is observed, the estimated E1-N ASP power density is within the expected power density range for all tracked satellites, i.e., between the upper and lower validation thresholds defined as stated in (2). As the plotted ASP components have their ASP seed also authenticated, once the I/NAV message is authenticated once for each satellite, the received satellite signals are continuously authenticated via E1-N ASP component.

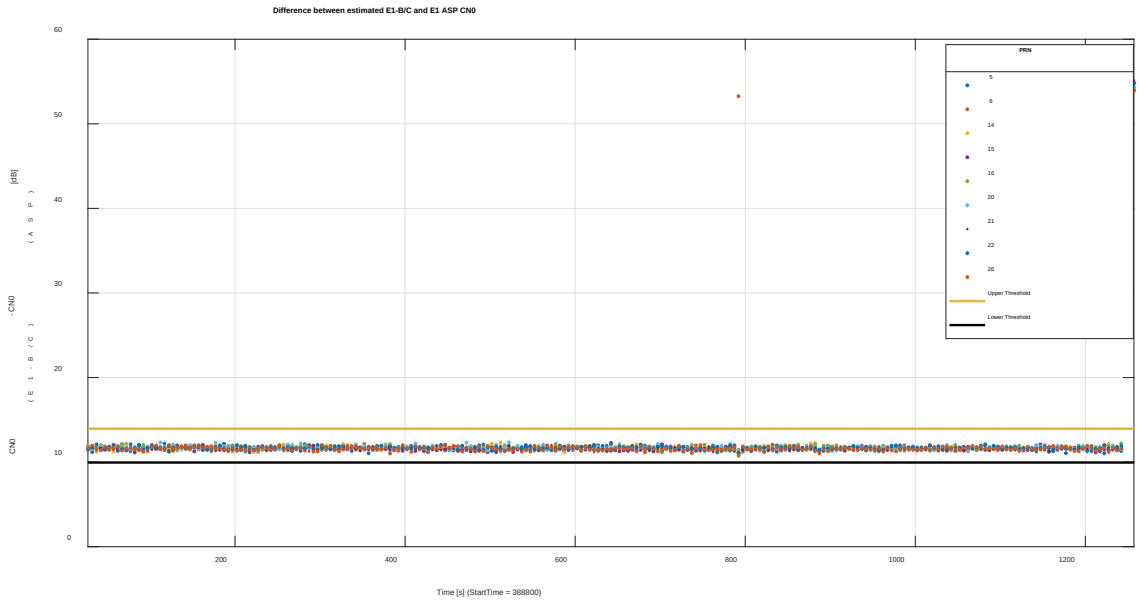

Figure 8. Validation procedure of the detected E1-N ASP component for the static AWGN channel under benign environment and a signal reception of 50 dB-Hz

Figure 9 shows that at the beginning of the simulation, the power difference between the E1-B/C and the E1-N ASP component increases considerably. This happens due to the fact that the attacker is getting over the victim's tracking loops, therefore an increase of the E1B/C power is seen but no increase in the power of the E1-N ASP component happens. After 120 s, the attacker has already the control of the user's tracking loops, and therefore, starts driving away the estimated position from the true position. While it drives away the user from its true position, the power of the ASP components decreases while the power of the E1-B/C remains constant (or only deceases slightly as the overlap between true and spoofing signal diminishes). The power reduction happens because the tracked E1-B/C and the E1-N data components are not anymore code aligned with the E1-N ASP component. This misalignment increases as the estimated user position increases w.r.t. its true position. However, it must be noted that the geometry between the satellite position and the direction of the spoofed position directly affects to the estimated CN0 of the ASP component. This can be observed in the satellite 16 which is located at the South of the victim receiver (see Figure 6), and as the spoofer drives the user towards the East (see Figure 4), the spoofer's direction is nearly orthogonal to the satellite position, and therefore, the detection of the signal is barely affected.

Figure 10 shows a similar scenario for the SCER attack, however, the estimated power difference between the E1-B/C and the E1-N ASP component are closer to Th_{up} (Upper Threshold). This happens due to the estimation performed by the attacker, which tries to correctly estimate the encrypted chips before retransmitting them. As the estimation process at 60 dB-Hz does not provide a high enough rate of successfully estimated chips, the power difference remains still out of the validation range of 10 to 14 dB. Furthermore, as the number of correctly estimated chips varies for consecutive ASP snapshots, the power difference looks noisier than in the case of the spoofing attack.

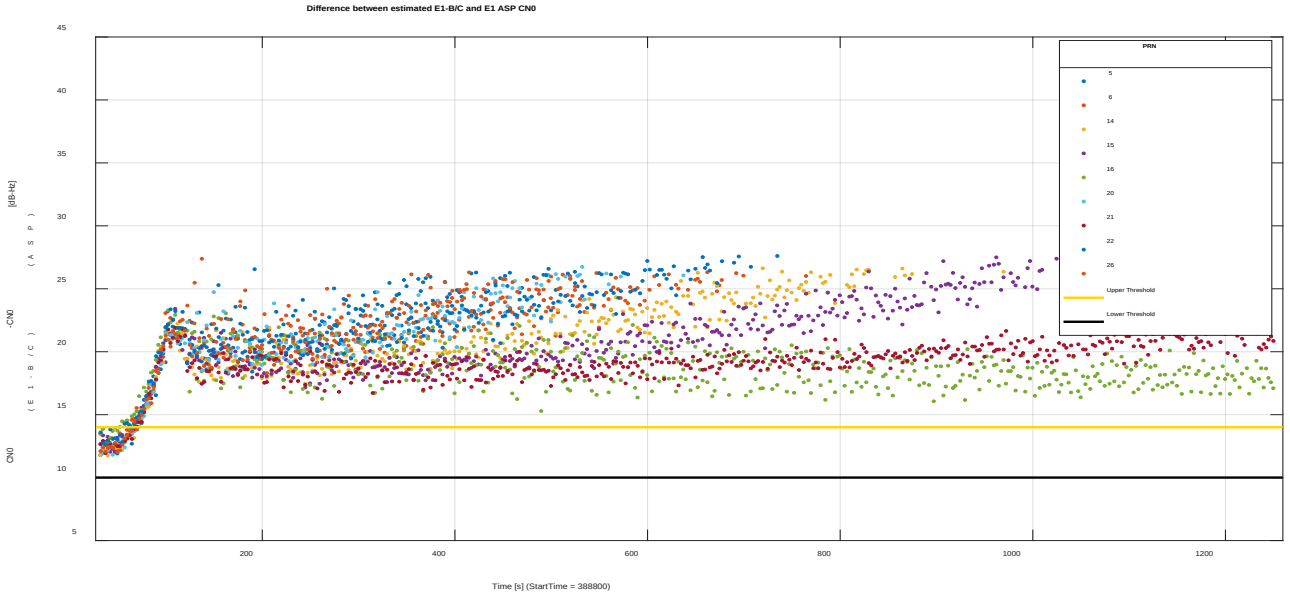

Figure 9. Validation procedure of the detected E1-N ASP component for the static AWGN channel under spoofing attack and a signal reception of 50 dB-Hz

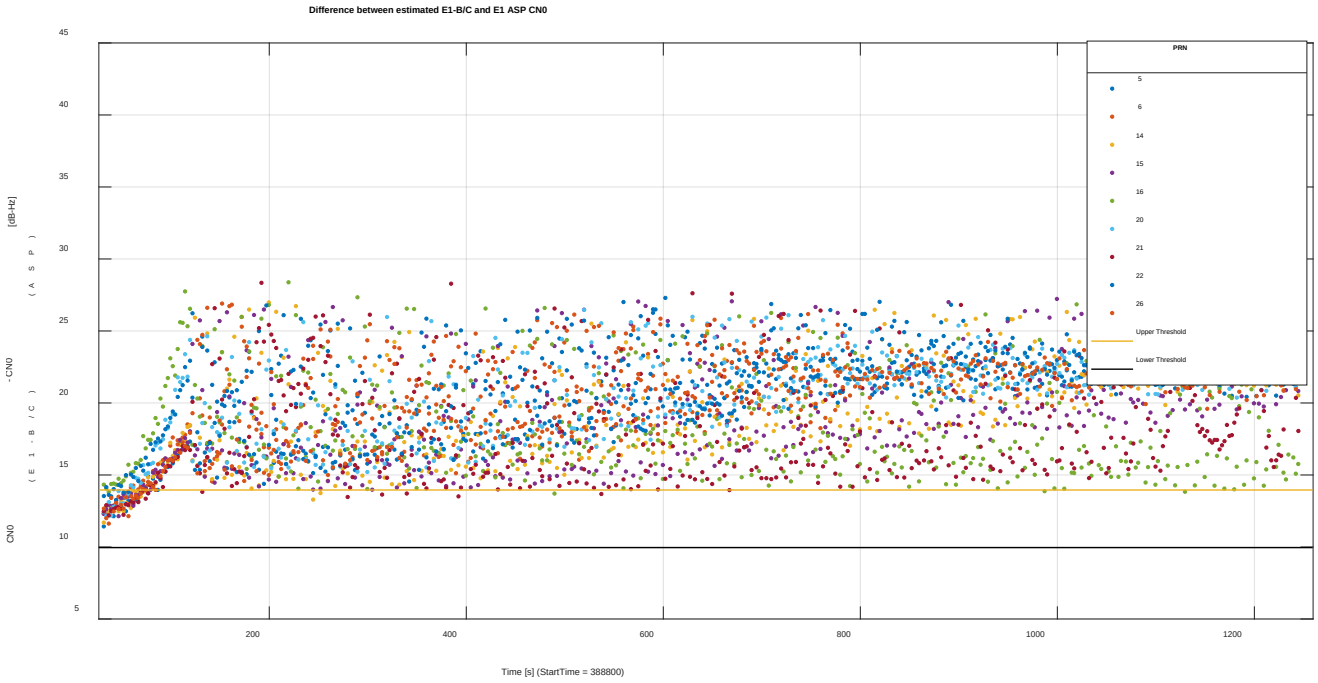

Figure 10. Validation procedure of the detected E1-N ASP component for the static AWGN channel under SCER attack and a signal reception of 50 dB-Hz

A similar result is obtained for the dynamic LMS channel scenario. Figure 11 presents the validation process of the detected ASP snapshots for a receiver under spoofing attack. The main difference with the spoofing attack under static AWGN channel conditions is that the attack induces a small deviation towards the South w.r.t. the real user trajectory (see Figure 5). However, as the navigation and authentication data are retransmitted by the spoofer at a power advantage of 6 dB, the ASP validation process is still capable of

detecting that an attack is happening. The slight South component of the spoofing trajectory is observed is the slight increase of the estimated power difference, mainly noticeable at the end of the simulated time.

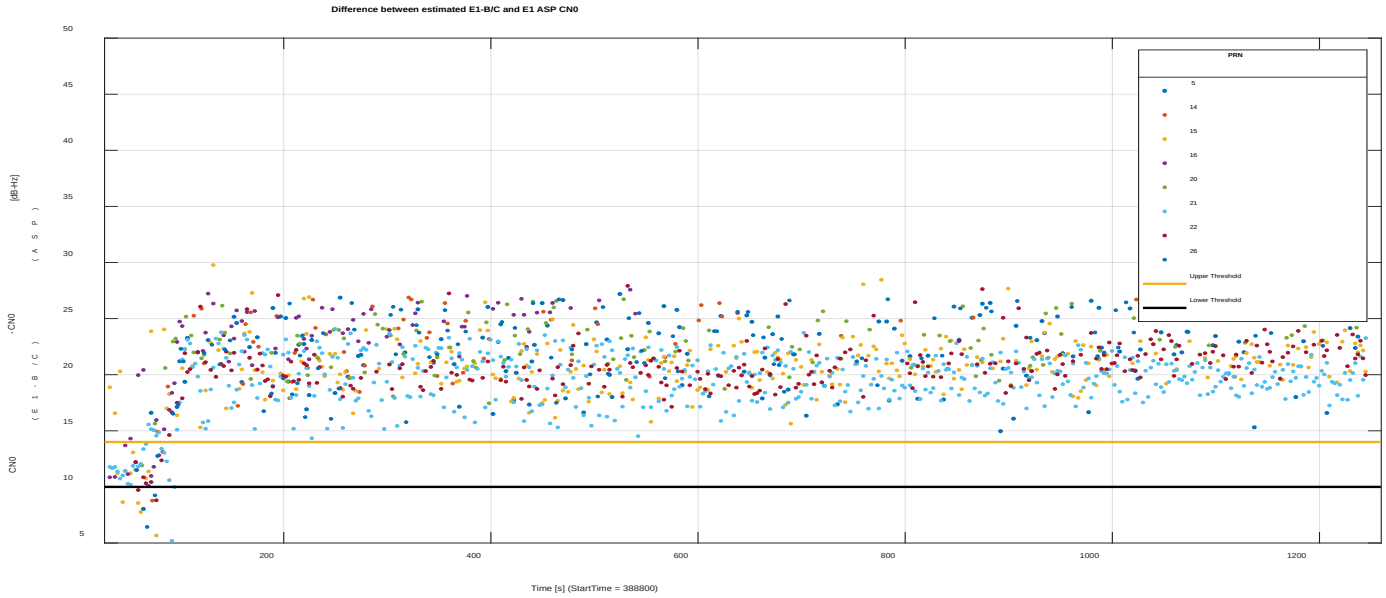

Figure 11. Validation procedure of the detected E1-N ASP component for the dynamic LMS channel under spoofing attack and a signal reception of 50 dB-Hz

On the other hand, Figure 12 shows the ASP validation process of a receiver in dynamic LMS channel conditions and under SCER attack. Similar to the static AWGN receiver case, the estimated power difference is higher than in the spoofing attack scenario due to the chip estimation procedure. The main point of SCER attack is the increased estimated power difference between the E1-B/C and the ASP component, so that there are several validated ASP snapshots. However, at those timestamps the user position is not considered to be authenticated, as there are not four or more satellites simultaneously validated.

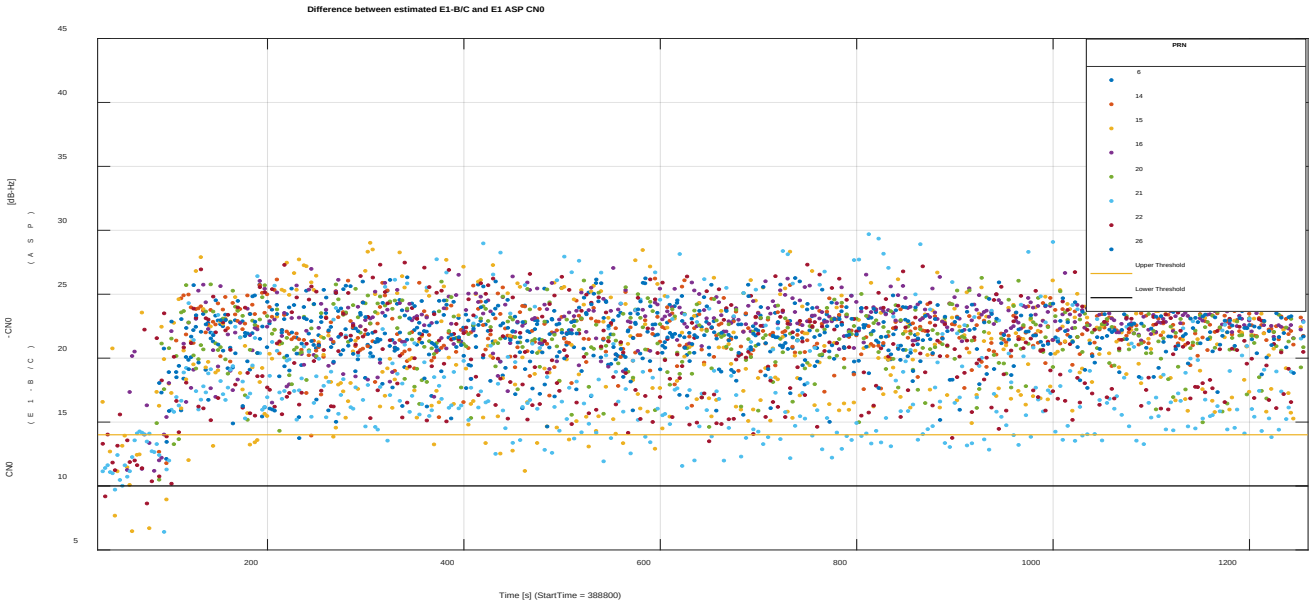

Figure 12. Validation procedure of the detected E1-N ASP component for the dynamic LMS channel under SCER attack and a signal reception of 50 dB-Hz

Table 1 presents further key performance indicators (KPIs) for the simulated static AWGN and dynamic LMS scenarios under spoofing and SCER attacks. The KPIs presented are: the mean error rate of the decoded navigation (I/NAV) and authentication data bits, which are computed based on the CRC checks; authentication data availability, which indicates the successful data extraction rate for the ASP seed, ASP seed signature, and I/NAV signature from the authentication data component; authentication availability, which provides the authentication rate in terms of ASP detection and validation, ASP seed signature verification, and I/NAV signature verification; and finally, the probability of detection (PD), which determines the attack detection rate computed by using the NMA and SCA algorithms as defined in Figure 7. A remark that must be considered is that the I/NAV signature is continuously being authenticated under both attack scenarios. Finally, it must be noted that the main mechanism that detected the attacks was the SCA authentication mechanism.

Table 1. Simulation results for the static AWGN and dynamic LMS channels under spoofing and SCER attack

KPI	Scenario	Attack Mode		Comments
		Spoofing	**SCER**	
MER	Static AWGN	0.23 % 15.48 %		I/NAV Auth data
	Dynamic LMS	22.4 % 12.81 %		I/NAV Auth data
Auth. Data Availability	Static AWGN	100 % 100 % 97.67 %		ASP seed ASP seed sign. I/NAV sign.
	Dynamic LMS	100 % 100 % 75.5%		ASP seed ASP seed sign. I/NAV sign.
Auth. Availability	Static AWGN	4.42 % 100 % **97.67 %**	4.9 % 99.59 % **95.75 %**	ASP detection ASP seed sign. I/NAV sign.
	Dynamic LMS	0.99 % 100 % **86.87 %**	3.9 % 99.59 % **85.47 %**	ASP detection ASP seed sign. I/NAV sign.
PD	Static AWGN	96 %	96 %	
	Dynamic LMS	100 % (No TTFAF)	100 % (No TTFAF)	

RECEIVER LIMITATIONS AND PITFALLS

During the test scenarios several observations have been made. First of all, a common ASP seed for all satellites is required to increase the successful ASP seed and ASP seed signature extraction from the authentication data component. Optionally, the ASP seed can be provided over alternative communication services, as current mass-market GNSS receiver use additional communication modules.

Regarding the ASP receiver protocol, this is required to be simple and application specific. The main parameters associated with the ASP receiver protocol are:

- ASP snapshot rate,
- minimum number of authenticated satellites,
- the power difference margin, and
- the integration time.

For each GNSS application requiring signal authentication, a trade-off between false alarm and misdetection needs to be performed, where the values of the above-mentioned parameters are studied.

In addition to the NMA and SCA protocols, a receiver might benefit from a spectral monitoring before ASP peak detection, which can help to avoid false peaks due to narrow tone interference, as they usually correlate with any PRN code, and therefore a peak is always detected. By performing a spectral monitoring, the narrow tone interferences can be easily detected and removed from the incoming signals.

Finally, a random trigger of the ASP snapshots is recommended as it can help receiver to be protected against synchronized jamming and spoofing attacks, such as the ones presented in [19].

CONCLUSIONS

A generic receiver authentication protocol has been defined, which can be employed in any signal based anti-spoofing protocol. The presented receiver protocol has been implemented in a bit-true simulation and tested for Galileo E1-B/C with a new authentication signal (E1-N) with NMA and SCA protocols. The test scenario included static AWGN and dynamic LMS channel conditions under synchronized spoofing and SCER attacks. Furthermore, the effectiveness of the protocol has been studied and the receiver pitfalls have been observed. Finally, it must be noted that SCA has been observed to be a more robust, flexible and powerful authentication tool against sophisticated spoofing attacks in comparison to NMA.

REFERENCES

1. 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.
2. Margaria, D., Motella, B., Anghileri, M., Floch, J., Fernandez-Hernandez, I., Paonni, M., "Signal Structure-Based Authentication for Civil GNSSs: Recent Solutions and Perspectives," in *IEEE Signal Processing Magazine*, vol- 34, no. 5, pp. 27-37, Sept. 2017
3. Ioannides, R. T., Pany, T., Gibbons, G., "Known Vulnerabilities of Global Navigation Satellite Systems, Status, and Potential Mitigation Techniques," in *Proceedings of the IEEE*, vol. 104, no. 6, pp. 1174-1194, June 2016
4. Fernández-Hernández, I., Rijmen, V., Seco Granados, G., Simón, J., Rodríguez, I., "Design Drivers, Solutions and Robustness Assessment of Navigation Message Authentication for the Galileo Open Service," *Proceedings of the 27th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+ 2014), Tampa, FL, September 2014*, pp. 2810-2827.
5. Fernández-Hernández, I., Seco Granados, G., "Galileo NMA Signal Unpredictability and Anti-Replay Protection," in *2016 + International Conference on Localization and GNSS (ICL-GNSS), Barcelona, Spain, June 2016*
6. Caparra, G., Sturaro, S., Laurenti, N., Wullems, C., "Evaluating the Security of One-way Key Chains in TESLA-based GNSS Navigation Message Authentication Schemes," in *2016 International Conference on Localization and GNSS (ICL-GNSS), Barcelona, Spain, June 2016*
7. Fernandez-Hernandez, I., "GNSS Authentication: Design Parameters and Service Concepts," *Proceedings of the European Navigation Conference GNSS 2014*
8. Psiaki, M. L., Humphreys, T. E., "GNSS Spoofing and Detection," in *Proceedings of the IEEE*, vol. 104, no. 6, pp. 1258-1270, June 2016
9. Humphreys, T. E., "Detection Strategy for Cryptographic GNSS anti-spoofing" *IEEE Transactions on Aerospace and Electronic Systems*, vol. 49, no. 2, pp. 1073-1090
10. Schnorr, C.P. "Efficient Identification and Signatures for Smart Cards". In: *G. Brassard, eds. Advances in Cryptology – CRYPTO' 89 Proceedings. CRYPTO 1989. Lecture Notes in Computer Science, vol 435. Springer*, New York, NY.
11. Pany, T., Dötterböck, D., Gomez-Martinez, H., Subhan Hammed, M., Hörkner, F., Kraus, T., Maier, D., Sanchez-Morales, D., Schütz, A., Klima, P., Ebert, D., "The Multi-Sensor Navigation Analysis Tool (MuSNAT) – Architecture, LiDAR, GPU/CPU GNSS Signal Processing," *Proceedings of the 32nd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2019), Miami, FL, September 2019*, pp. 4087-4115.
12. ITU-R. 681-11, "Propagation data required for the design systems in the land mobile-satellite service", *Recommendation ITU-R P.681-11 (08/2019)*
13. Interface Specification IS-AGT-100, Chip Message Robust Authentication (Chimera) Enhancement for the L1C Signal: Space Segment/User Segment Interface, 2019.

14. Anderson, J., Carroll, K., DeVilbiss, N., Gillis, J., Hinks, J., O'Hanlon, B., Rushanan, J., Scott, L., "Chips-Message Robust Authentication (Chimera) for GPS Civilian Signals," *NAVIGATION-Journal of The Institute of Navigation*, 2017, pp. 2388-2416.
15. Julien, O., Macabiau, C., Issler, J.-L., Ries, L., "Galileo E1 OS/SoL acquisition, tracking and data demodulation performances for Civil Aviation," *2010 5th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC), Noordwijk, December 2010*, pp. 1-8.
16. Won, J.-H., Pany, T., (2017) Signal Processing. In: Teunissen, P.J., Montenbruck, O., (eds) Springer Handbook of Global Navigation Satellite Systems. Springer Handbooks.
17. Dötterböck, D., Hameed, M.S., Pany, T., Lesjak, R., Prechtl, T., "Retrieval of Encrypted PRN Sequences via a Self-calibrating 40-element Low-cost Antenna Array: Demonstration of Proof-of-concept," *Proceedings of the 33rd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2020), Virtual, September 2020*
18. Van der Merwe, J. R., Bartl, S., O'Driscoll, C., Rügamer, A., Förster, F., Berglez, P., APopugaev, A., Felber, W., "GNSS Sequence Extraction and Reuse for Navigation," *Proceedings of the 33rd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2020), Virtual, September 2020*
19. Curran, J. T., Bavaro, M., Closas, P., Navarro, M., "On The Threat of Systematic Jamming of GNSS," *Proceedings of the 29th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2016), Portland, OR, September 2016*, pp. 313-321.