Testing receiver resilience against signal replay attacks

Simón Cancela, Javier Navarro, David Calle, Eckart Göhler, Andrea Dalla Chiara, Giacomo da Broi, Ignacio Fernández-Hernández, Gonzalo Seco-Granados, Javier Simon

Testing receiver resilience against signal replay attacks

S. Cancela, J. Navarro, D. Calle, *GMV*
E. Göhler, *Ifen*
A. Dalla Chiara, G. Da Broi *Qascom*
I. Fernández-Hernández, *European Commission*
G. Seco-Granados, *Universidad Autónoma de Barcelona*
J. Simón, *European GNSS Agency*

Email: scancela@gmv.com

BIOGRAPHIES

Simón Cancela holds an MSc in Advanced Mathematics by the Universidad Complutense de Madrid. He joined GMV in 2015 and he has been working in the Galileo Commercial Service Demonstrator validation and experimentation activities and he is currently working on the development of a Commercial Service enhanced PVT resilient platform.

Javier Navarro holds a BSc in Systems Telecommunications Engineering by the Polytechnic University of Madrid. He joined GMV in 2018 and he is currently working on the development of a Commercial Service enhanced PVT resilient platform.

David Calle holds a MSc. in Computer Engineering from the University of Salamanca. He joined GMV in 2008 and he has been working in the GNSS business unit involved in the design and development of GNSS algorithms, applications and systems. He is currently Head of GNSS Services Section coordinating the activities related to the Galileo Commercial Service, Open Service Authentication and High Accuracy provision services.

Andrea Dalla Chiara is designer and project manager at Qascom, with focus on GNSS simulators and receivers and authentication techniques both at signal and data level. He is an electronic engineer, and has a PhD in Information Technologies by University of Padova.

Giacomo Da Broi is a designer and developer of GNSS and TT&C simulators at Qascom, specialized in authentication techniques both at signal and data level. He holds a MSc degree in Telecommunications Engineering from University of Padova.

Eckart Göhler received his Diploma in physics from the University Tübingen and his Ph.D. from the Institute for Astronomy and Astrophysics, Tübingen. He worked as a lead software engineer at IFEN GmbH in the receiver technology department. Today he is employed at OHB System AG in the instrument software group.

Ignacio Fernández-Hernández is the Galileo service definition coordinator at the European Commission, DG ENTR. He is an ICAI engineer, holds an MBA by LBS and a PhD in electronic systems by Aalborg University.

Gonzalo Seco-Granados is associate professor with the Dept of Telecom. Eng. of Univ. Autónoma de Barcelona (UAB) and head of the Signal Processing for Navigation and Communications (SPCOMNAV) group. Previoulsy, he was staff member at the Radionavigation Section in ESTEC/ESA, and involved in the Galileo project and in the development of GNSS receivers and applications.

Javier Simon is Service Design Engineer within the European GNSS Agency, currently contributing to the definition and design of the Galileo OSNMA and CS services. He holds a MSc. degree in Telecommunications Engineering from the Polytechnic University of Madrid, Spain. Before joining GSA he participated in several projects for the study and design of future GNSS algorithms and systems

ABSTRACT

The Galileo program is implementing enhancements with respect to standard GNSS services. Some of these enhancements relate to complementing the Galileo Open Service with Navigation Message Authentication (NMA) and providing signal authentication through the Commercial Service. These new features will improve resilience of the GNSS applications and reduce the likelihood of successful attacks to GNSS users. However, these upcoming Galileo services still require a step to be completed on the user side: the definition and implementation of algorithms to successfully exploit them. In this context, the European Commission launched the Navigation Authentication through Commercial Service-Enhanced Terminals (NACSET) project aiming at investigating and implementing techniques to detect and mitigate spoofing attacks, improving user-level resilience.

As part of the NACSET project, a resilient user terminal has been developed based on a high-end multi-GNSS receiver. This GNSS receiver is complemented with

a software module that implements several protection techniques that exploit Galileo authentication. This module includes standalone techniques such as direction of arrival estimation, clock monitoring, IMU hybridization, AGC-C/N_0 monitoring, a navigation message authentication (NMA) module and an anti-replay technique based on the use of NMA unpredictable symbols.

This paper focuses on the proposed anti-replay technique. While plenty of literature is already available on GNSS spoofing and replay attacks [2] [6] , most of the research available is based theoretical models and simulations. The paper details a hardware and software implementation of anti-replay capabilities in a real high-end receiver in order to complement the existing work. The implementation is then tested in real time against a simulated attack implemented explicitly for the technique validation. Results and conclusions are derived and presented.

1 INTRODUCTION

This section introduces the NACSET project and the platform architecture [Figure 1]. The NACSET project's main objective is to develop a resilient User Terminal able to implement and combine a wide range of anti-spoofing algorithms which can benefit from Galileo authentication services, including Commercial Service authentication and Open Service NMA. These capabilities are complemented with specific equipment such as IMUs, barometers and high-performance clocks to support standalone spoofing detection techniques. In order to provide the PVT resilience thanks to assisted authentication, the project includes a Synchronization and Authentication Server (SAS). This module is the responsible for providing assisted navigation and signal authentication capabilities to the User Terminal as well as accurate time synchronization. For the distribution of the cryptographic information, such as the Commercial Service keys and OSNMA information, a dedicated Key Management Simulator is also developed to emulate all the required interfaces.

This paper is mainly focused on the anti-replay technique, implemented in the User Terminal. This technique provides protection against zero-delay SCER attacks based on the use of NMA unpredictable symbols [6] . Throughout the paper first, it is described the NACSET platform architecture, with special detail on the NACSET receiver (User Terminal). Then, it describes the anti-replay technique implemented in the receiver. Later, it explains how Security Code Estimate-Replay (SCER) attacks are simulated in the NACSET test environment. Finally, the results of a set of validation tests are presented exercising different configurations of the SCER attacks against the developed receiver and a COTS one in order to evaluate the effectiveness of the proposed anti-replay technique in the detection process.

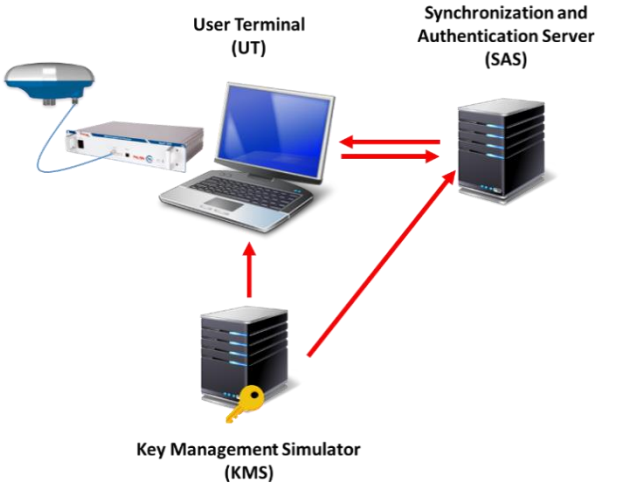

Figure 1 - NACSET platform architecture

2 USER TERMINAL

The user terminal (UT) developed comprises of a high-end multi-GNSS receiver capable of processing all Galileo signals including E1B open service and E6-B/C signals, either encrypted or open. The receiver is able to provide signal samples along with observables and navigation data to the software module in charge of implementing the protection techniques [Figure 2]. The software module processes the signal samples and the receiver data to perform the required analysis for threats detection. The receiver also implements the Galileo OSNMA authentication protocol alongside the abovementioned techniques.

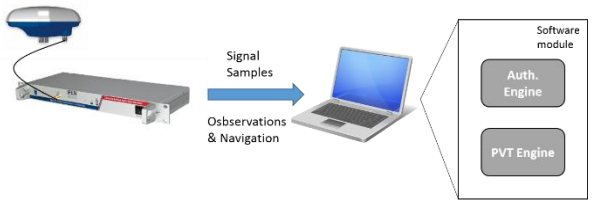

Figure 2 – User Terminal Architecture

2.1 Hardware receiver

The hardware receiver consists on the NavX-NTR Receiver [Figure 3] developed by Ifen gmbh and a Two-element GNSS antenna array designed by Fraunhofer. The NavX-NTR is based on a digital main-board, an analogue front-end including AD-conversion, and a NavCarrier board, carrying up to three base band pre-processor boards. The RF front-end board allows up to four different standard or customer-selected RF signals to be down-converted to an analogue intermediate frequency. A four channel, high-speed analogue-to-digital converter (ADC) on the RF front-end board digitizes the analogue signal.

Figure 3 – NavX-NTR Receiver

The base band processing supports the complete Galileo spectrum including OS E1 CBOC, E6-B/C and E5 AltBOC, GPS L1 (including TMBOC), L2 (semi-codeless P(Y), L2C) and L5, SBAS L1 and L5, BeiDou and GLONASS G1 and G2. In addition, the GNSS antenna is a two antenna array with the specifications described in Table 1.

Table 1 – Antenna specification

Specifications	
Galileo Signals	E1, E5a, E5b, E5a+b (AltBOC), E6
GPS Signals	L1, L2
Element Distance	< λ/2 at 1591 MHz (94 mm)
Passive Gain	Elev. 90° (zenith): > 3.5 dBic Elev. 60°: > -3 dBic Elev. 15°: > -10 dBic
LNA Power Gain	~30 dB
LNA Noise factor	< 2 dB

The two antenna are placed at 94 mm distance inside the radome protective case as shown in Figure 4.

Figure 4 – Receiver GNSS two-antenna array

2.2 Software Module

The GNSS receiver is commanded and complemented by a software module installed in a standard laptop and physically connected to the hardware receiver. The software module is in charge of implementing a portfolio of anti-spoofing measures and includes a PVT module able to compute a trustable position with the protection techniques outcomes. The receiver module processes the data from the Signal-In-Space and forwards the GNSS observations and navigation along with the E1B signal samples for the software module to process.

The anti-spoofing and authentication techniques implemented are listed below:

- Anti-replay protection
- Dual-antenna measures analysis
- IMUs Hybridization
- Clock Monitoring
- AGC-C/N_0 Monitoring
- Galileo Open Service Navigation Message Authentication (see [4])
- Assisted signal authentication on Galileo E6 (see [8])

Next sections provides the implementation details and early results of the anti-replay protection technique developed within the NACSET user terminal.

3 ANTIREPLAY PROTECTION

If a GNSS signal stream contains data that is authenticated, a spoofer can only alter the pseudorange measurements to spoof the receiver position. This attack falls under the category of signal replay attacks. In order to protect pseudoranges from replay attacks, the pseudoranges can include authentication features. Ideally, these authentication features can be implemented at spreading-code level. However, if the data modulated includes unpredictable symbols, this unpredictability can be also exploited against replay attacks. One of the novel features of the User Terminal is the inclusion of anti-replay protection measures based on the unpredictability bits of NMA data present on a GNSS signal, as introduced in [6] .

Anti-replay solutions can address zero-delay SCER (Security Code estimation and replay) attacks. To execute this attack an attacker estimates and rebroadcasts the original signal with a zero or almost negligible delay, taking control of the tracking loop and gradually modifying the signal. The NACSET terminal implements a method that takes advantage of the existence of unpredictable bits and symbols in the navigation thanks to NMA cryptographic information provided through the SIS. In order to conduct a zero-delay SCER attack on a signal containing NMA data, the attacker shall predict the unknown symbols with minimal or none information. The technique is based on the analysis of the signal correlation loss caused by the imperfect estimation of the signal chips corresponding to the mentioned unpredictable symbols.

The first step is to verify that the satellite data is authentic, as well as the correctness of the unpredictable symbols used for the anti-replay check, this is performed through the NMA verification. The NMA solution used for this implementation is the Galileo Open Service NMA (OSNMA) defined to be included in the I/NAV data that is transmitted through the in Galileo E1-B. The Galileo I/NAV is transmitted in the signals E1 (1575.42 MHz) and E5b (1207.14 MHz). NMA is currently designed for the E1-B (data) component. Satellites transmit a navigation frame every 750 seconds, composed by 25 subframes of 30 seconds duration each. Every subframe is divided into fifteen 2-second pages, each of which contains one word and some other fields [3] . The I/NAV effective bit rate is 120 bps. The I/NAV message bits are convolutionally

encoded and interleaved into two symbols for each bit, to which a 10-symbols pattern is added for page synchronization. This sums to a rate of 250 symbols per second. This makes 4092 signal chips per symbol as the Ranging Code Chip-Rate of the E1-B signal is 1023 MChips per second. The convolutional encoding shall be carefully considered for the definition of unpredictable symbols. Every page has a 40-bit field, which is proposed to be used for the transmission of the OSNMA data as described in [4]. This OSNMA data includes cryptographic material, such as pseudorandom generated keys which makes part of the I/NAV data unpredictable and thus, subject to be used for the anti-replay protection.

As opposed to a standard receiver, which performs a continuous signal correlation, different subsets of chips can be selected in the NACSET receiver for the correlation process. The purpose of this feature is to perform specific correlations on, or including, parts of the signal that are considered unpredictable. These subsets may be chosen according to different criteria: fixed subsets, random subsets or based on a statistical analysis. Finally, the correlation values are analyzed to check whether the signal is authentic or not. These correlation values will depend on the number of chips stored per symbol and the power of the signal. This implementation allows performing statistical analysis to optimize the false alarms and missed detection probabilities for different applications and environments.

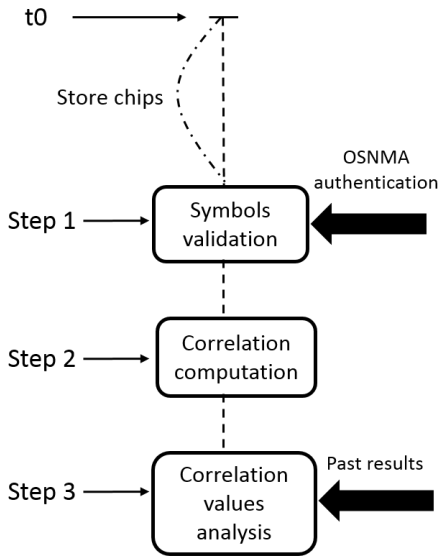

Figure 5 – Anti-replay processing schema

In the following sections, these three main processes implementation will be explained thoroughly.

4 OSNMA UNPREDICTABLE SYMBOLS

As it is mentioned before, the aim of the technique is to exploit the unpredictability of the cryptographic data included in an NMA scheme, as proposed e.g. in [5]. The Galileo OSNMA data is sent inside the I/NAV pages in batches of 40 bits. The OSNMA protocol consists of transmitting two types of data, Digital Signature Messages (DSMs) and Message Authentication Codes (MACs) with a private key (see [4]). The DSM is repeated over time so it cannot be considered unpredictable, and it is transmitted using 8 of the previously mentioned 40 bits of the I/NAV page. Hence, at most, only the MACs and the keys can be considered fully unpredictable, i.e. 32 symbols per I/NAV page, and they may not be homogenously distributed in all the I/NAV pages. Other consideration may be taken into account to protect from brute force attack in the last bits of the MACs and keys as explained in [6] . The unpredictable bits available thanks to the OSNMA scheme have been analyzed in different publications (see [6] and [7]) with similar results than the ones obtained in the analysis herein conducted. Next figures are taken from [6] and depict the position of the unpredictable symbols in green, assuming 32 unpredictable bits per I/NAV page, which is the assumption taken for this work. Note also that the unpredictability in the I/NAV CRC, which is computed on the NMA bits, varies the position of the unpredictable symbols with respect to the below figures, although this does not alter the paper conclusions.

1	9	17	25	33	41	49	57	65	73	81	89	97	105	113	121	129	233
2	10	18	26	34	42	50	58	66	74	82	90	98	106	114	122	130	234
3	11	19	27	35	43	51	59	67	75	83	91	99	107	115	123	131	235
4	12	20	28	36	44	52	60	68	76	84	92	100	108	116	124	132	236
5	13	21	29	37	45	53	61	69	77	85	93	101	109	117	125	133	237
6	14	22	30	38	46	54	62	70	78	86	94	102	110	118	126	134	238
7	15	23	31	39	47	55	63	71	79	87	95	103	111	119	127	135	239
8	16	24	32	40	48	56	64	72	80	88	96	104	112	120	128	…	240

Figure 6 – I/NAV unpredictable symbols before interleaving

The position of the symbols inside the I/NAV page is also necessary to be determined in order to store the samples to be analyzed. For this, the Galileo I/NAV encoding and interleaving has to be considered. As explained before the I/NAV page is encoded in 240 symbols which then are interleaved with a block interleaver with dimensions of 30 columns x 8 rows.

1	9	17	25	33	41	49	57	65	73	81	89	97	105	113	121	129	233
2	10	18	26	34	42	50	58	66	74	82	90	98	106	114	122	130	234
3	11	19	27	35	43	51	59	67	75	83	91	99	107	115	123	131	235
4	12	20	28	36	44	52	60	68	76	84	92	100	108	116	124	132	236
5	13	21	29	37	45	53	61	69	77	85	93	101	109	117	125	133	237
6	14	22	30	38	46	54	62	70	78	86	94	102	110	118	126	134	238
7	15	23	31	39	47	55	63	71	79	87	95	103	111	119	127	135	239
8	16	24	32	40	48	56	64	72	80	88	96	104	112	120	128	…	240

Figure 7 – I/NAV unpredictable symbols after interleaving

For the UT implementation the number and position of the unpredictable bits can be configured to test different OSNMA configuration and security assumptions.

5 ANTI-REPLAY IMPLEMENTATION

Throughout this section the actual implementation of the theoretical technique described in section 3 will be presented. The anti-replay technique as presented earlier is a software program external to the hardware receiver that processes its data to implement the proposed protection technique.

The hardware receiver processes the GNSS signals and provides a continuous stream of E1B signal samples to the

receiver. The receiver also generates the Doppler values for the satellites in view for the technique.

The anti-replay module has to process the E1B signal samples in order to compute the needed correlations. The first step is to execute the acquisition process. In order to speed up the acquisition process and symbol decoding, the Doppler values from the receiver are used. The module starts processing the received samples data as soon as the PRN of the satellites in view and their respective Doppler values are provided from the receiver.

As the sample stream is not provided synchronized to the symbol, the module needs to compute the beginning of each symbol inside the stream. For this, the symbol code offset (sco), a number between 0 and 4092, gives us the information of when a new symbol starts in the samples stream. The computation process requires several milliseconds of data to ensure a proper processing. As Figure 8 shows, the beginning of the samples does not have to coincide with the beginning of a symbol. In most of the cases, the receiver starts to sample after the beginning of a symbol. The number of samples of the first chip (n_1) is lower than the number of samples of the second chip (n_2) because the second symbol is completely sampled.

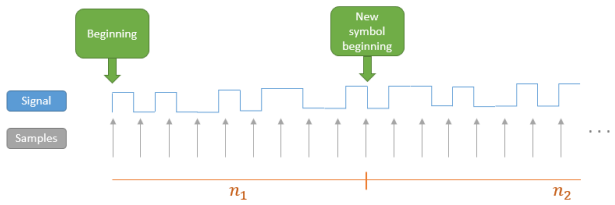

Figure 8 – Signal sampled

If the sampling frequency (fs) is not proportional to the E1b code chip (1,023 MHz), the number of samples of some symbols will be different. If the sco is lower than half Galileo E1b code length (4092/2) the number of samples of each symbol (n) is modelled as

$$n = \left\lfloor fs * ts_{e1b} \frac{(cl_{e1b} - sco)}{cl_{e1b}} \right\rfloor$$

where n is the number of samples to seek to the beginning of the symbol, fs is the sampling frequency, ts_{e1b} is the time of symbol (in Galileo E1b is 0.004 seconds), cl_{e1b} is the code length (in Galileo E1b is 4092), and sco is the symbol code offset. But if sco is equal or higher than half Galileo E1b code length, n is modelled as

$$n = \left\lfloor fs * ts_{e1b} \frac{(2 * cl_{e1b} - sco)}{cl_{e1b}} \right\rfloor$$

As explained in the previous section, in order to detect the zero-delay SCER attacks, the antireplay method stores N_c chips (in samples) of the N_U unpredictable symbols over a given interval. To find the chips related only to the unpredictable symbols, a tracking process is carried out. The module decodes the I/NAV symbols and aligns to page level searching for the I/NAV page synchronization pattern. Then the antireplay solution, which knows the value of the unpredictable symbol, select a subset of chips from the symbol and correlates the chips with the public spreading code of each satellite. It is likely that the SCER attacker estimates wrongly the first chips of each unpredictable symbol, therefore, these are the most appropriate chips to consider against this type of attacks. In the implemented solution, two different processing modes are supported for the chip selection: fixed and random selection. The fixed selection mode extracts the chips at the beginning of each symbol, and random mode extracts it randomly through the whole unpredictable symbol. The results reported are based on the fixed selection mode. The number of chips per symbol to be used are also configurable.

The correlation values are stored for a twofold purpose: First, to check the possible loss of correlation gain produced by a spoofer and update the thresholds for the correlation values checks. Therefore, the correlations of each unpredictable symbol are accumulated and, as a result, we obtain the correlation of each independent 2-second page. The other purpose of storing the correlation values is to generate statistics to detect when an unusual correlation loss has occurred. When the technique is enabled, the first 30 seconds are stored in a correlation window to calculate a mean correlation value. This mean correlation is updated with a sliding window every 2 seconds. The computed value is used to establish an expected value to be compared with the new correlation computed. A logical threshold difference between them is defined taking into account the probabilities of false alarm (FA) and missed detection (MD), with threshold configuration. This threshold and reference values are used to give a warning if the correlation gain is too low. The technique will raise a warning to the user in case the correlation checks are not met. These checks are performed when the unpredictable symbols subject to analysis are validated, i.e. the OSNMA verification result successful.

The sample processing technique is summarized as follows: after correct initialization, the module starts processing the signal samples and performing required correlations nominally. The generated correlation values are internally stored waiting for navigation authentication messages and events. Once the data is authenticated by the OSNMA protocol, the signal-level checks are executed, raising an alarm whether a correlation loss is observed in the chips analyzed.

6 SCER ATTACK SIMULATION

In order to demonstrate the functionality of the anti-replay technique, a SCER attack simulator has been developed. Considering the current status of the Galileo Services, which do not provide the OSNMA service through the SIS yet, the signal containing the OSNMA symbols has to be simulated. For this purpose, a tool able to generate both trusted and spoofed signals to simulate the attack has been implemented. The tool consists of two elements: a software module and the HackRF software-defined radio (SDR) platform.

The HackRF One from Great Scott Gadgets is a Software Defined Radio peripheral capable of transmission or reception of radio signals from 1 MHz to 6 GHz. It is an open source hardware platform that can be used as a USB peripheral or programmed for stand-alone operation, and its output format is 8-bit quadrature samples (8-bit I and 8-bit Q). The HackRF is needed to convert to RF the GNSS baseband signal data streams generated and replay it with the antenna.

Figure 9 – HackRF One

The software module is in charge of simulating the zero delay SCER attack. It has two main duties, generate the "genuine" Galileo E1B signals and generate the signals needed to simulate the SCER spoofer in a realistic way.

The generation of the Galileo signals is based on a GPS software simulator developed by Takuji Ebinuma ([9]) modified to generate both GPS L1 and Galileo E1 signals, including pseudoranges, navigation, signal power variations and inject Galileo OSNMA information in the navigation.

The signal generated is a simulated GNSS signal in clear open sky conditions. The software produces the signal with three specific inputs:

- Navigation RINEX for GNSS system status simulation
- User position in NMEA format, either kinematic or static
- OSNMA data
- SCER attack configuration, mainly errors introduced in the chips and time-to-start the attack.

The OSNMA data is generated by means of the Commercial Service Demonstrator (CSDemo) platform developed in the frame of the AALECS, project managed by the European Commission (see [10])

It is important to highlight that a Zero-delay SCER attack tries to estimate and rebroadcast a GNSS signal with the intention to force the receiver to lock to it instead of the original signal. Before the attack starts, we assume that the genuine signal is being tracked by the receiver. The attacker is steadily transmitting a signal with zero-delay, or a delay that is so close to zero that it does not represent any difference in the symbol detection process. The spoofer generates the security code w_k estimating each successive security chip, and immediately injecting it into a signal replica. The resulting signal is modelled as

$$\hat{s}_k = \hat{w}_k c(\hat{\tau}_k) cos(2\pi f_{IF} t_k + \hat{\theta}_k)$$

where $\hat{w}_k$ is the security code estimate, c is the known spreding code array and $c(\hat{\tau}_k)$ is the spreading code value at the code offset estimate $\hat{\tau}_k$, f_{IF} is the intermediate frequency after receiver front-end down-conversion, $\hat{\theta}_k$ is the carrier phase estimate, and t_k is time, all evaluated at samples index k. Zero-delay attacks force the attacker to estimate the symbols in a short time, and the presence of unpredictable symbols makes this task more difficult and causes an imperfect estimation of the symbols. The antireplay technique looks at that imperfect estimations of unpredictable symbols demodulated by the receiver before the Viterbi decoding. Further details on security code estimation and replay attack can be found in [3].

In order to simulate the SCER attack the developed tool generates two signals at the same time. The first signal reproduces the real signal coming from the satellites, while the second is the spoofed signal, coming from a transmitter that tries to accomplish the attack. The real signal is similar to the spoofed signal but the security code w_k, the code offset τ_k and the carrier phase θ_k are not estimated.

$$r_k = w_k c(\tau_k) cos(2\pi f_{IF} t_k + \theta_k)$$

The transmitted signal is formed by the real and the spoofed signal, and is modelled as

$$y_k = w_k c(\tau_k) cos(2\pi f_{IF} t_k + \theta_k) + \hat{w}_k c(\hat{\tau}_k) cos(2\pi f_{IF} t_k + \hat{\theta}_k)$$

The spoofed signal starting time is configurable. The scenario begins with only the trusted signal being tracked, and it evolves to a spoofing attack when the second signal, the spoofed one, starts.

The simulation of the attack can be divided in three phases:

- **Phase 1**: Only the signal without spoofing is generated. The receiver tracks only this real signal.
- **Phase 2**: The spoofing signal perfectly aligned with the real signal, simulating a theoretical perfect zero delay.
- **Phase 3**: After some time, when the receiver tracks the spoofing signal, the spoofing signal starts delaying the signal to spoof the receiver position

The steps are shown in the Fig. 9 in a timeline diagram:

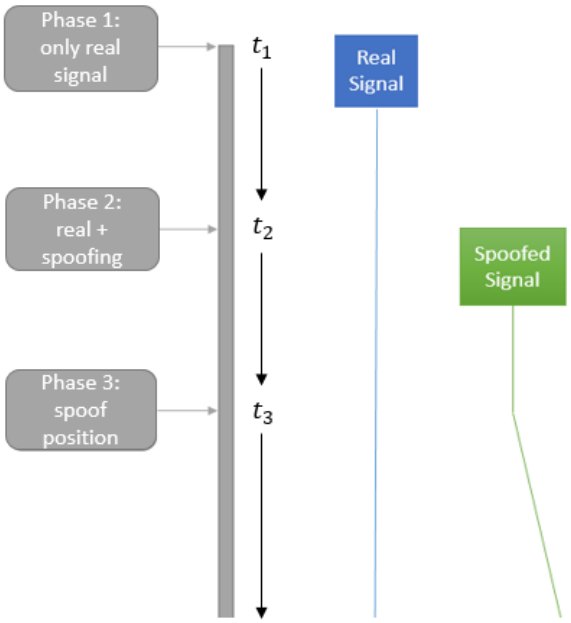

Figure 10 – Spoofing attack steps

The imperfect estimation of the symbols is simulated by modifying the sample chips on the spoofed signals. This imperfect estimation can be complemented with different levels of signal power in the spoofer. In some cases, the signal coming from the spoofer may have a higher power than the real signal, in order to induce the receiver to track this signal instead of the real signal. The scenarios under test, as well as the results, are described in more detail in the next section.

7 RESULTS

A dedicated testing campaign to validate both the SCER attack implementation and the effectiveness of the protection technique has been conducted. The first step was to identify an independent COTS receiver to compare the results with respect to the NACSET User Terminal. The selected receiver is a u-Blox M8T which supports Galileo E1 and GPS L1 amongst other constellations.

For the test set–up, the UT is used to test the performances of the implemented anti-replay technique and the COTS receiver is used to test how a mass-market receiver without any anti-replay protection behaves receiving the signals generated by the SCER simulator (see Figure 11).

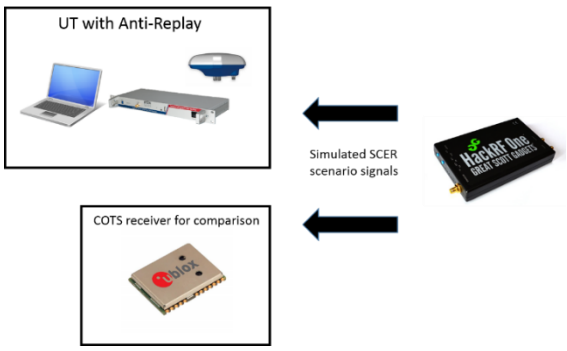

Figure 11 – Test environment set-up

Throughout this section the results of the anti-replay checks will be presented as variations in the correlation mean values and the impact in the COTS receiver, showing that the SCER simulator is able to successfully spoof the receiver position without the anti-replay protection.

The initial configuration applied to the User Terminal anti-replay module is described in the Table 2.

Table 2 – Anti-replay technique configuration

Parameter	Value
Sampling frequency	8192000 Hz
Threshold	40 % maximum correlation loss from the mean.
Unpredictable symbols	32 per page
Chips to be correlated per unpredictable symbol.	10 at the beginning of the symbol

The SCER simulator is configured as defined in the following table:

Table 3 – SCER simulator configuration

Phase	Duration	Notes
Phase 1	60s	Real signal simulating position in LLH: (40.59º, -3.7º), 806 m
Phase 2	20s	Both spoofing signal and real simulate position (40.59º, -3.7º), 806 m with one chip delay
Phase 3	60s	Spoofing signal deviate receiver position in a linear trajectory.

Apart from this configuration, three types of attacks depending on the spoofer estimation errors and transmission power have been modeled and executed. They are listed below and described in more detail in the rest of the section.

- **Reference attack**: Pseudorandom errors are introduced in the estimation of the unpredictable symbols (50% of chip errors at the beginning of each symbol) and no modification of the signal power is done.
- **Intermediate attack**: low error rate in the estimation of the unpredictable symbols (30% of chip errors at the beginning of each symbol) and no modification of the signal power is done.

- **High-power attack**: low errors rate in the estimation of the unpredictable symbols (30% of chip errors at the beginning of each symbol) and modification of the signal power per symbol to mask the errors in the estimation process.

The results of the tests executed with the U-Blox receiver show the behavior of the normal receiver against spoofing attacks. Figure 12 shows the satellite C/N_0 in dB at the beginning with only genuine signals. This power profile is the nominal one in all the tests.

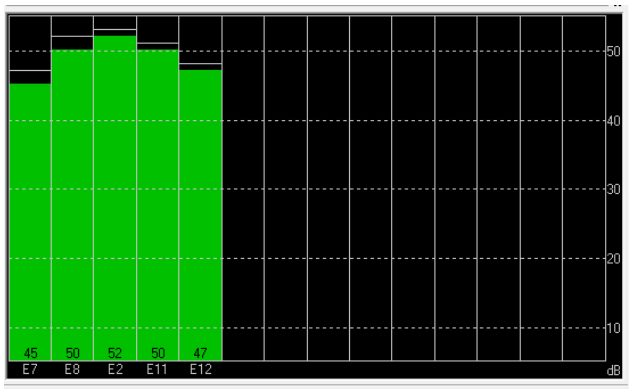

Figure 12 – C/N_0 (in dB) values observed in the COTS receiver with no spoofed signal

7.1 Reference attack

The "reference attack" is proposed by simulating 5 erroneous chips of the first 10 chips at the beginning of each unpredictable symbol and no power supply modification. This attack is considered the worst case scenario from the spoofer perspective, hence it is used to demonstrate the detection performances of the technique and compare with the other attack cases that are presented within the paper. It is observed that this kind of spoofing attack is not detected by COTS receivers, but the anti-replay technique detects drastic changes in the correlation of the spoofed signal. Even if the success rate of this attack is considered pessimistic for the spoofer (the successful symbol estimation probability cannot be lower than 0.5), it is considered useful to show the detection capabilities of the spoofing detector in a best-case scenario for the receiver and compare it with the other cases.

The beginning of the Phase 2 is shown in Figure 13. Several changes in the C/N_0 are observed when new signals appear in the spectrum.

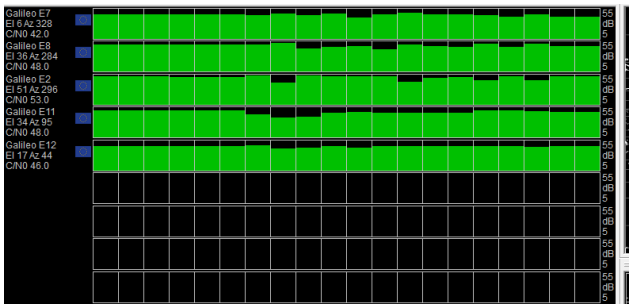

Figure 13 – Reference attack - spoofed signal beginning in COTS receiver

In Figure 14 the C/N_0 values at the moment of the beginning of the attack are depicted. The overall pattern is considered similar to the ones in nominal conditions but the C/N_0 values have decreased.

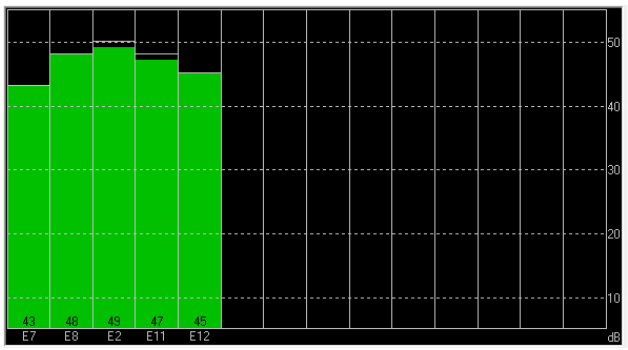

Figure 14 – C/N_0 (in dB) values observed in the COTS receiver with the Reference attack

In Phase 3, the position of the COTS receiver is spoofed in a linear trajectory as defined in the attack. Figure 15 shows the evolution of the COTS receiver position.

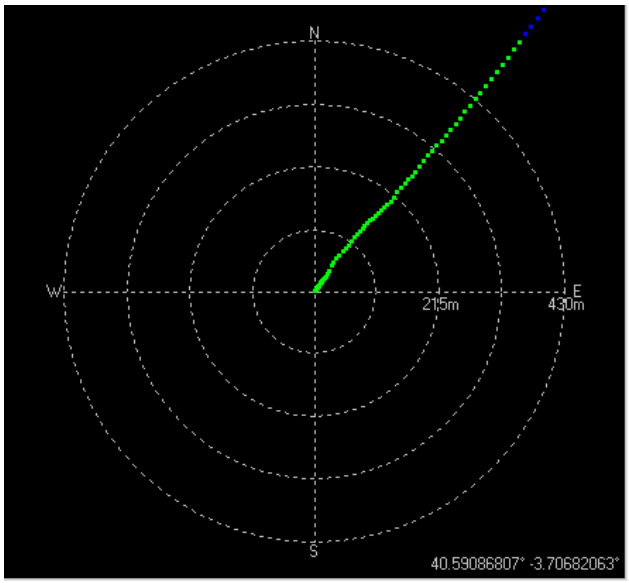

Figure 15 – Reference attack Map View

In the NACSET receiver, when the spoofed signal appears, the monitored correlation values decrease significantly per satellite as it can be seen in Figure 16. So, it is considered that the NACSET receiver is able to detect the attack and stops computing the positioning solution. Therefore, it can be concluded that the anti-replay technique works successfully against that kind of attack.

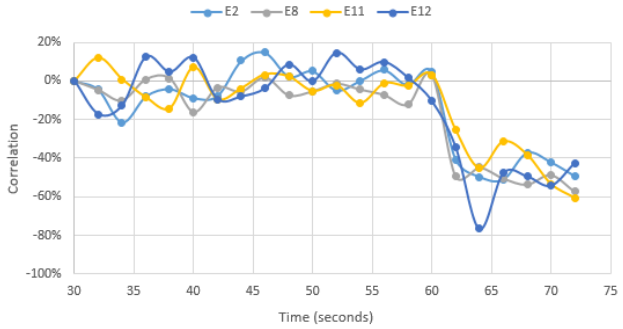

Figure 16 – Reference attack - correlation variation

Table 4 shows the variation of the correlation outcomes per satellite comparing to the mean of the last subframe outcomes.

Table 4 – Reference attack - correlation results variation

	E02	E08	E11	E12
Reference attack	-45%	-51%	-42%	-51%

7.2 Intermediate attack

An "intermediate" spoofing attack is proposed introducing 2 error chips at the beginning of each unpredictable symbol and no power supply modification. Even if a spoofer can guess at least half of the time the unpredictable symbols, and therefore the chips, the gain loss that it produces models is equivalent to a wrong guess of twice the error chips (4 chips in this case) half of the times. Therefore this simplification is considered as representative. In this case, the anti-replay technique detects smoother variations in the correlation of the unpredictable symbols, which confirm the need of previous fine tuning of the techniques thresholds to achieve a fine detection of the spoofed signal.

The beginning of the Phase 2 is shown in Figure 17.

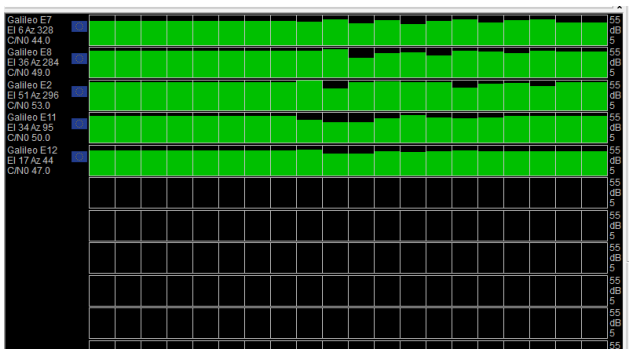

Figure 17 – Intermediate attack - spoofed signal beginning in COTS receiver

In Figure 18 the C/N_0 values at the moment of the beginning of the attack are shown. The C/N_0 overall pattern is consistent with the nominal scenario and slightly better than in the "reference attack".

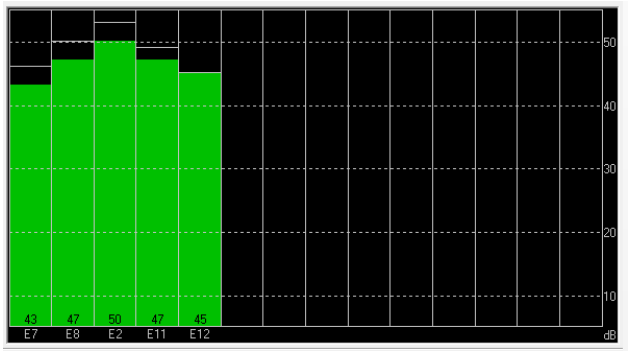

Figure 18 – C/N_0 (in dB) values observed in the COTS receiver with the Intermediate attack

In Phase 3, the position of the COTS receiver is spoofed in a linear trajectory. The result is equivalent to the Reference attack. Figure 19 shows the modification of the COTS receiver position.

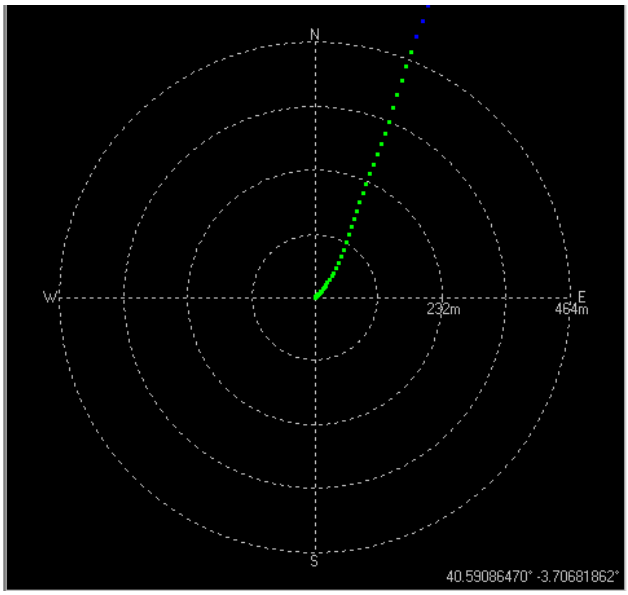

Figure 19 – Intermediate attack Map View

On the other hand, in the NACSET receiver, when the spoofed signal starts, the correlation indicator decreases less clearly than in the previous case because of the fewer estimation errors. This can be observed in Figure 20, but it is still able to detect the attack and stops computing the positioning solution.

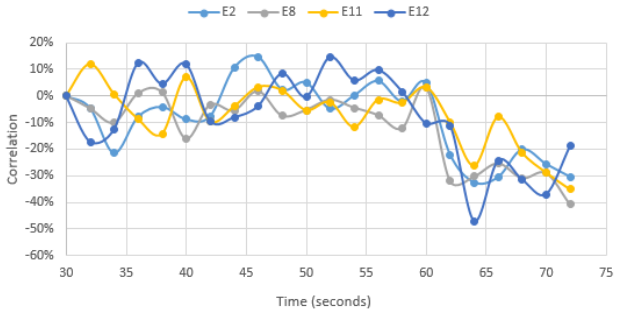

Figure 20 – Intermediate spoofing correlation variation

Table 5 shows the variation of the correlation outcomes comparing to the mean of the last subframe outcomes.

Table 5 – Intermediate attack correlation results variation

	E02	E08	E11	E12
Intermediate attack	-27%	-31%	-21%	-28%

7.3 High-power attack

The "high-power" spoofing attack modeled has 2 error chips at the beginning of each symbol and a power increase of a factor two, i.e 3 dB, in the spoofed signal with respect to the genuine signal. In this case, the variation of the correlations are much more subtle due to the masking of the estimation errors by the attacker. It is difficult to detect the attack without restricting the technique thresholds. In this case, the combination of the technique with another anti-spoofing monitoring based on power monitoring such as C/N_0 and AGC would be recommended.

The beginning of the spoofed signal produces as a result a tracking transition which is shown in Figure 14. The spoofed signal employs higher power, as we see in the Figure 21 recorded by a COTS receiver.

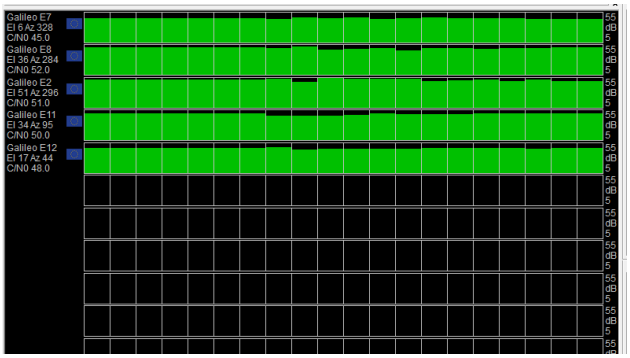

Figure 21 – High power spoofed signal beginning

Figure 22 shows that the satellites' signal power has increased significantly because of the spoofed signal.

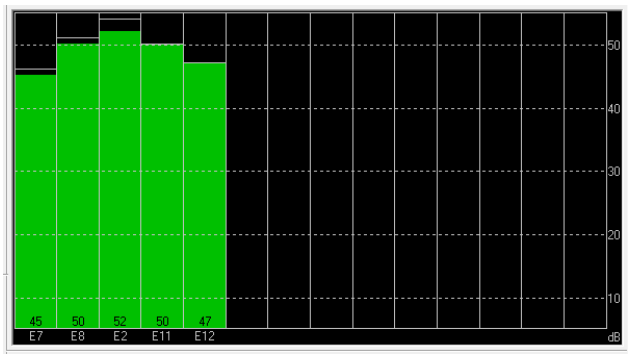

Figure 22 – C/N_0 (in dB) values observed in the COTS receiver with the High power attack

When this configuration of the attack, the difference of the receiver position with respect to the genuine signals (static position) in 4 minutes of radiation is higher than 3 km in the COTS. These results show that the receiver tracks the spoofed signal alone when it starts as it can be observed in the evolution of the positions computed by the COTS receiver (linear trajectory as defined in Table 3).

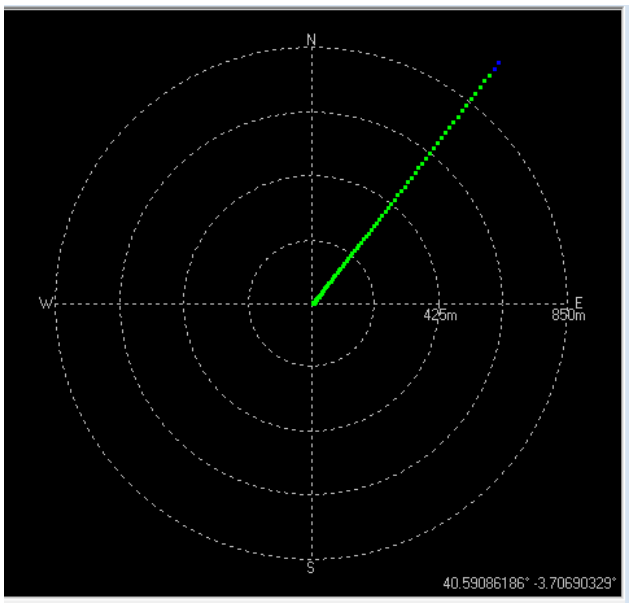

Figure 23 – High Power Map view

Two different values of power increases has been tested, 3dB and 5dB. In the first case, a 3dB increase has been simulated resulting in a variation of the correlation that can be seen in Figure 24. It is observed that the correlation variation is more subtle than in the previous cases but a general correlation loss can be identified.

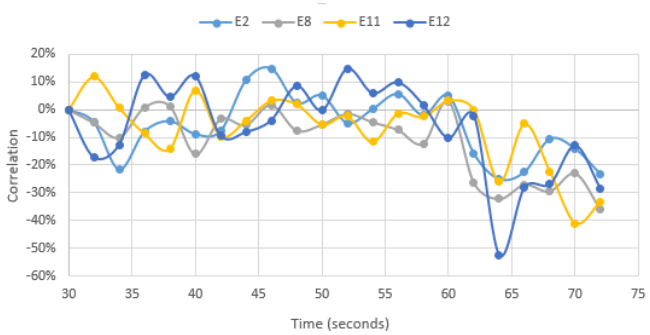

Figure 24 –High-power attack (3dB increase) spoofing correlation variation

Table 6 –High-power attack (3dB increase) correlation results variation

	E02	E08	E11	E12
High-power attack (3dB)	-19%	-29%	-21%	-25%

In the second case, an increase of 5dB has been tested, in this test the NACSET receiver is unable to clearly detect the attack, as it is quite difficult to propose a firm decision based on the correlation values. Figure 25 shows that once the attack is started the correlation values computed deviate more than before but very erratically.

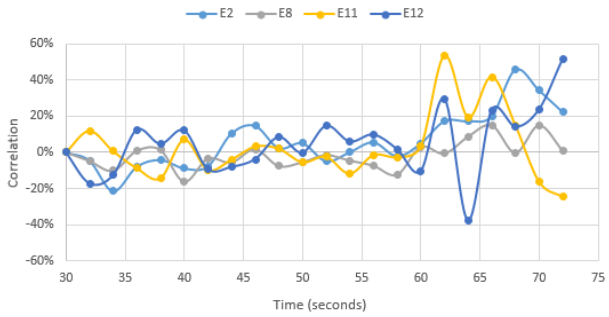

Figure 25 – High-power attack (5dB increase) spoofing correlation variation

As proposed before, in this type of attacks complementing the technique with a signal power monitoring could help the detection process since 5dB change in the signal power can be easily detected.

Table 7 – Correlation results variation

	E02	E08	E11	E12
High-power attack (5dB)	26%	6%	15%	17%

8 CONCLUSIONS

Throughout the paper, an implementation of a solution for protecting against zero delay SCER attacks has been described and tested against a simulated attack.

It has been demonstrated that the technique behaves well against standard zero-delay SCER attacks for open-sky, being able to detect the spoofing signal as soon as it starts tracking it. The results for spoofers that vary the power of the signal considering the symbol estimation outcomes, show that further improvements can be made to the technique in terms of correlation analysis, selection of number of chips, as well as combination with other signal power-related indicators, such as AGC or C/N_0.

In summary, from the validation tests, it can be concluded that the unpredictable symbols inside a GNSS signals can be exploited to detect certain types of SCER attacks, leaving the door open for future improvements of the concept. Further work will consist on proving the technique with real SIS and in harsher environments (e.g. urban static, kinematic and tree canopies) and characterize the probability of false alarm, time to alert and refine the statistical analysis to work in those environments.

REFERENCES

[1] Todd E Humphreys, "Detection strategy for cryptographic gnss antispoofing," Aerospace and Electronic Systems, IEEE Transactions on, vol. 49, no. 2, pp. 1073–1090, 2013.
[2] Gianluca Caparra, Nicola Laurenti, Rigas T Ioannides, and Massimo Crisci, "Improving secure code estimate-replay attacks and their detection on gnss signals"," Proceedings of NAVITEC 2014, 2014.
[3] The European Union, European GNSS (Galileo) Open Service Signal In Space Interface Control Document, 2015.
[4] Ignacio Fernández-Hernández, Vincent Rijmen, Gonzalo Seco-Granados, Javier Simon, Irma Rodríguez, and J David Calle, "A navigation message authentication proposal for the galileo open service," Navigation, vol. 63, no. 1, pp. 85–102, 2016.
[5]K. Wesson, M. Rothlisberger, and T. E. Humphreys, "Practical cryptographic civil GPS signal authentication," NAVIGATION, Journal of the Institute of Navigation, 2011, available at http://radionavlab.ae.utexas.edu/nma.
[6] I. Fernández-Hernández, G. Seco-Granados, "Galileo NMA Signal Unpredictability and Anti-Replay Protection", ICL-GNSS 2016, 2016
[7] James T. Curran, Cillian O'Driscoll,"Message Authentication, Channel Coding & Anti-Spoong", Proceedings of the ION GNSS+ Meeting, 2016.
[8] S. Cancela, D. Calle, G. Arroyo, A. Dalla Chiara, G. Da Broi, O. Pozzobon, C. Sarto, J. Winkle, I. Krol, P. Webster, I. Fernández, J. Simón, G. Seco-Granados. "Designing and evaluating next generation of resilience receivers", Proceedings of the ION GNSS+ Meeting, 2017.
[9] https://github.com/osqzss/gps-sdr-sim, Takuji Ebinuma
[10] C. Sarto, O. Pozzobon, S. Fantinato, S. Montagner, I.F. Hernández, J. Simón, J.D. Calle, S. Cancela, P. Walker, D. Burkey, G. Seco-Granados, E. Göhler, "Implementation and testing of OSNMA for Galileo", Proceedings of the ION GNSS+ Meeting, 2017