Preliminary Evaluation of Galileo ACAS using Existing E1-E6 Open Signals and a Low-Cost SDR Platform

Rafael Terris-Gallego, José A. López-Salcedo, Gonzalo Seco-Granados, *Univ.Autònoma de Barcelona/IEEC, Spain*
Ignacio Fernandez-Hernandez, *DG DEFIS, European Commission, Belgium*

BIOGRAPHY

Rafael Terris-Gallego received the M.Sc. degrees in telecommunication engineering from the Polytechnic University of Catalonia (UPC) and in Digital Communications Systems from Telecom Bretagne, both in 2001. From 2001 to 2015 he worked as engineer for mobile and satellite communications. He is currently an Adjunct Lecturer at the Autonomous University of Barcelona (UAB) and researcher in GNSS at Space Studies Institute of Catalonia (IEEC).

José A. López-Salcedo received the Ph.D. degree in telecommunication engineering from the UPC in 2007. He is currently Professor in the Dept. of Telecommunication and Systems Engineering of UAB. His research interest lies on the field of signal processing for GNSS receivers.

Gonzalo Seco-Granados received the Ph.D. degree in telecommunications engineering from the UPC in 2000, and the MBA degree from the IESE Business School, Spain, in 2002. From 2002 to 2005, he was member of the European Space Agency. He is currently Professor in the Dept. of Telecommunication and Systems Engineering of UAB.

Ignacio Fernandez-Hernandez received the electronic engineering degree from ICAI, Spain, in 2001, the MBA degree from LBS, London, UK, in 2011, and the Ph.D. degree in electronic systems from Aalborg University, Denmark, in 2015. He is in charge of Galileo high accuracy and authentication at the European Commission, DG DEFIS.

ABSTRACT

Malicious attacks such as spoofing are a significant concern within the Global Navigation Satellite System (GNSS) community. The European Galileo program is actively developing new services to bolster the resilience of these systems, as outlined in (Fernandez-Hernandez et al., 2018). These services include Open Service Navigation Message Authentication (OSNMA), which offers authentication for navigation bits, and Commercial Authentication Service (CAS), designed to encrypt the spreading code chips. Similar concepts are being applied in Chips-Message Robust Authentication (CHIMERA) for Global Positioning Sytem (GPS).

In this paper we focus on Assisted Commercial Authentication Service (ACAS), which is currently under definition (European Commission, 2020b). It uses the Timed Efficient Stream Loss-tolerant Authentication (TESLA) keys supplied by OSNMA via the E1-B signal to re-encrypt specific fragments of the encrypted E6-C signal, referred to as Re-Encrypted Code Sequences (RECSs). These RECSs are then made accessible in the GNSS Service Centre (GSC). Once a compatible receiver downloads them, it can decrypt these fragments using the corresponding key and then correlate them with the broadcasted E6-C signal. If this process results in a correlation peak, the signal can be authenticated under certain conditions.

To enhance the probability of detecting this correlation peak, the proposed nominal operating mode for ACAS entails using the estimates provided by E1-B to reduce the uncertainty associated with the E6-C signal, given that these fragments are only accessible at specific predefined instants. This approach enables the receiver to accurately predict the locations of these fragments. The alignment between the E1-B and E6-C signals is of utmost importance for this operational mode. To assess it in a real-world context, a series of real datasets were captured using a low-cost Software Defined Radio (SDR) platform based on bladeRF. This platform enabled the synchronous acquisition of samples from both E1-B and E6-C bands. Additionally, the performance of ACAS in terms of acquisition-level probability of detection has been evaluated across various RECS lengths. This evaluation serves as a valuable tool for choosing the configuration of a receiver's hardware and as a performance reference for practical implementations.

 https://doi.org/10.33012/2023.19319

I. INTRODUCTION

From the original Commercial Service (CS) of Galileo, the European GNSS, several new services have emerged. The recently launched OSNMA in E1-B provides an affordable way to authenticate the Position, Velocity and Timing (PVT) using a Navigation Message Authentication (NMA) scheme (Fernandez-Hernandez et al., 2016). On the other hand, the High Accuracy Service (HAS), currently being deployed in E6-B, enables Precise Point Positioning (PPP) worldwide by providing orbit, clock and bias corrections (Gutierrez, 2021). These "added-value" services were intended to be offered for a fee, but they have been finally supplied for free (Fernandez-Hernandez et al., 2023a).

A third service, known as CAS, which implements Spreading Code Encryption (SCE) in E6-C, is currently being developed by the European Commission (EC) (European Commission, 2020b). As the name implies, it provides protection at chip-level by encrypting the spreading codes that form the GNSS signals, which allows a greater level of protection against malicious attacks such as spoofing, which has been the subject of many analysis (Scott, 2003; Pozzobon et al., 2010; Humphreys, 2013). Together with the OSNMA, it aims to offer a fully secure solution for authenticating the PVT. To achieve this without modifying the Galileo signal plan, an assisted mode known as ACAS has been proposed (European Commission, 2020a).

In this mode, the service selects specific fragments of the encrypted E6-C signal to be broadcasted and provides them as files, along with timestamps and other relevant information, in the publicly accessible GSC. These fragments, known as Encrypted Code Sequences (ECSs), are then re-encrypted using the (yet to be disclosed) TESLA keys used by OSNMA in E1-B, which results in RECSs. This allows any user's receiver to operate in standalone mode for the duration of the pre-downloaded data (i.e., the RECSs files), without the need to store any secret keys. Once the E6-C signal is broadcasted, the user's receiver captures snapshots at the times when the downloaded fragments are expected to be present. Subsequently, when the corresponding keys are disclosed in the E1-B signal, the receiver can decrypt the stored RECS and perform correlation with the pre-recorded snapshots. If a correlation peak is detected and certain conditions are met, the signal can be successfully authenticated (Fernandez-Hernandez et al., 2023b).

An example of how ACAS operates from the receiver's perspective is shown in Figure 1. The rate at which the RECSs become available (and consequently, when the ECSs are accessible) is specified by the RECS Period. In this particular scenario, where each TESLA key (in a hashed form) is employed to decrypt a unique RECS, the RECS Period aligns with the duration of an OSNMA I/NAV frame (30 seconds), which is the frequency at which the keys are disclosed in the E1-B signal. Alternative configurations may also be considered, where each key is used to decrypt multiple RECSs (Terris-Gallego et al., 2022b; Fernandez-Hernandez et al., 2023b). The duration of these ECSs, typically lasting for a few milliseconds, is determined by the RECS Length.

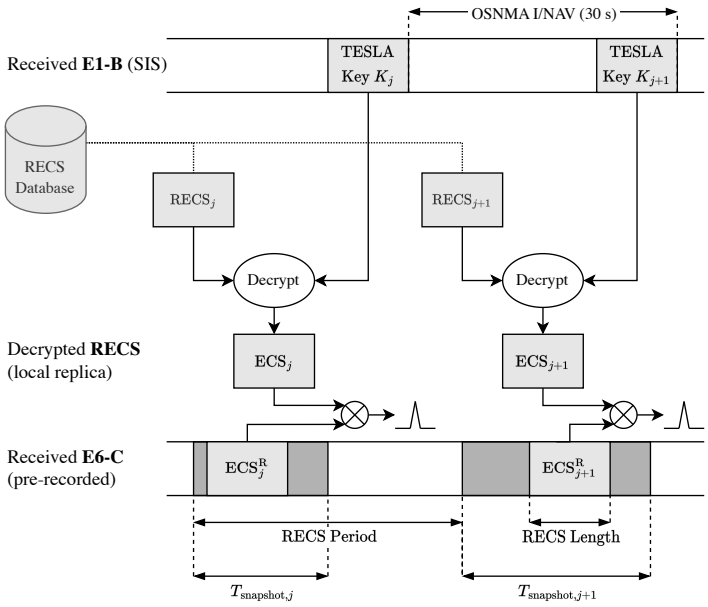

Figure 1: ACAS receiver schematics, where each TESLA key obtained from the E1-B signal is used to decrypt a unique RECS, previously downloaded by the receiver. The resulting ECSs are used to perform the correlation with the pre-recorded snapshots of E6-C samples. The duration of the snapshots (T_{snapshot}) may differ for each period depending on the configuration.

In the ACAS framework, the non-periodic nature of the encrypted E6-C signal can significantly reduce the probability of detecting the Received Encrypted Code Sequences (ECS^Rs), depending on the specific configurations of the RECS parameters (Terris-Gallego et al., 2022a). To address this challenge, the proposed nominal operating mode for ACAS leverages the estimates provided by E1-B, specifically the code phase and Doppler frequency, to mitigate the uncertainty associated with the E6-C signal. This approach enables the receiver to precisely determine the locations of these fragments (Fernandez-Hernandez et al., 2022).

The initial analysis of the ACAS (Terris-Gallego et al., 2022a,b) was undertaken as part of the EC-funded *Precise and Authentic User Location Analysis* (PAULA) project (European Commission, 2020b), which was responsible for defining the service. This analysis highlighted the advantages of this approach and provided implementation guidelines, particularly concerning acquisition methods, along with various simulated data results. To validate its feasibility in real-world scenarios, we have designed a cost-effective SDR platform using bladeRF. This platform, extensively described in (Terris-Gallego et al., 2023), allows for the synchronous acquisition of both E1-B and E6-C samples.

Synchronicity plays a pivotal role in the nominal operating mode of ACAS, as it depends on achieving accurate alignment between the E1-B and E6-C estimates. This alignment is crucial for streamlining the acquisition process to just a few correlations, as depicted in (Fernandez-Hernandez et al., 2022). The outcomes obtained using our platform confirm this alignment and facilitate the characterization of their relationship.

It is worth noting that the E6-C signal is currently broadcasted unencrypted, so the RECS need to be emulated for testing purposes. To do so, we have implemented a software that first acquires the E6-C secondary code and then performs a coherent integration for the required 1-ms primary spreading codes.

The rest of this paper is structured as follows: Section II provides an overview of the ACAS nominal operating mode, emphasizing the acquisition process and summarizing the key service aspects. Section III offers a brief overview of the low-cost SDR platform used to synchronously acquire E1 and E6 samples, along with details about the real datasets obtained from the current open signals. In Section IV, a preliminary evaluation of ACAS performance using the previously mentioned datasets is presented. Finally, Section V the paper's concluding remarks are provided.

II. GALILEO ACAS NOMINAL OPERATING MODE

1. Implementation

Setting aside cryptographic considerations that the interested reader can find in (Fernandez-Hernandez et al., 2023b), an ACAS receiver needs to tackle with the non-periodicity of the E6-C encrypted signal and the fact that only some fragments (i.e., the ECSs) of the received signal will be available to perform the correlation, once the local replicas (i.e., the downloaded RECSs properly decrypted by their corresponding TESLA keys once disclosed) become available. Furthermore, ACAS is intended to work by default in snapshot mode.

Therefore, the receiver should first determine the starting time and the duration of the snapshot to be recorded, in order to ensure that it includes the desired ECS. Without any further assistance, a straightforward search for these fragments (with a duration of some milliseconds typically) within the whole recorded snapshot (that can last for several seconds depending on the uncertainties) lead to a poor probability of detection in the acquisition, as detailed in (Terris-Gallego et al., 2022a).

That is why the nominal operating mode for ACAS relies on measurements obtained from the E1-B signal, as the receiver is expected to already track this signal for obtaining the corresponding TESLA keys from OSNMA. Nevertheless, this exhaustive search that relies only in the E6-C component can be useful in some cases, e.g., for threat mitigation purposes in post-processing, as detailed in (Terris-Gallego et al., 2022b; Winkel et al., 2023).

Since the E6 signal is aligned to the E1 signal, the time reference obtained from E1-B can be used to determine the starting point of the E6-C snapshot. In (Terris-Gallego et al., 2022a), different modes for obtaining this time reference are proposed.

Furthermore, thanks to the E1-B estimates, encompassing the code phase delay and the Doppler frequency, the search space for the E6-C signal can be significantly reduced. As depicted in (Fernandez-Hernandez et al., 2023b), just a few samples may suffice to perform the correlation in most cases, which allows increasing the probability of detection of the corresponding RECS and, such, the probability of authenticating the signal, which is the ultimate goal of ACAS. A block diagram of the operating nominal mode for ACAS is shown in Figure 2.

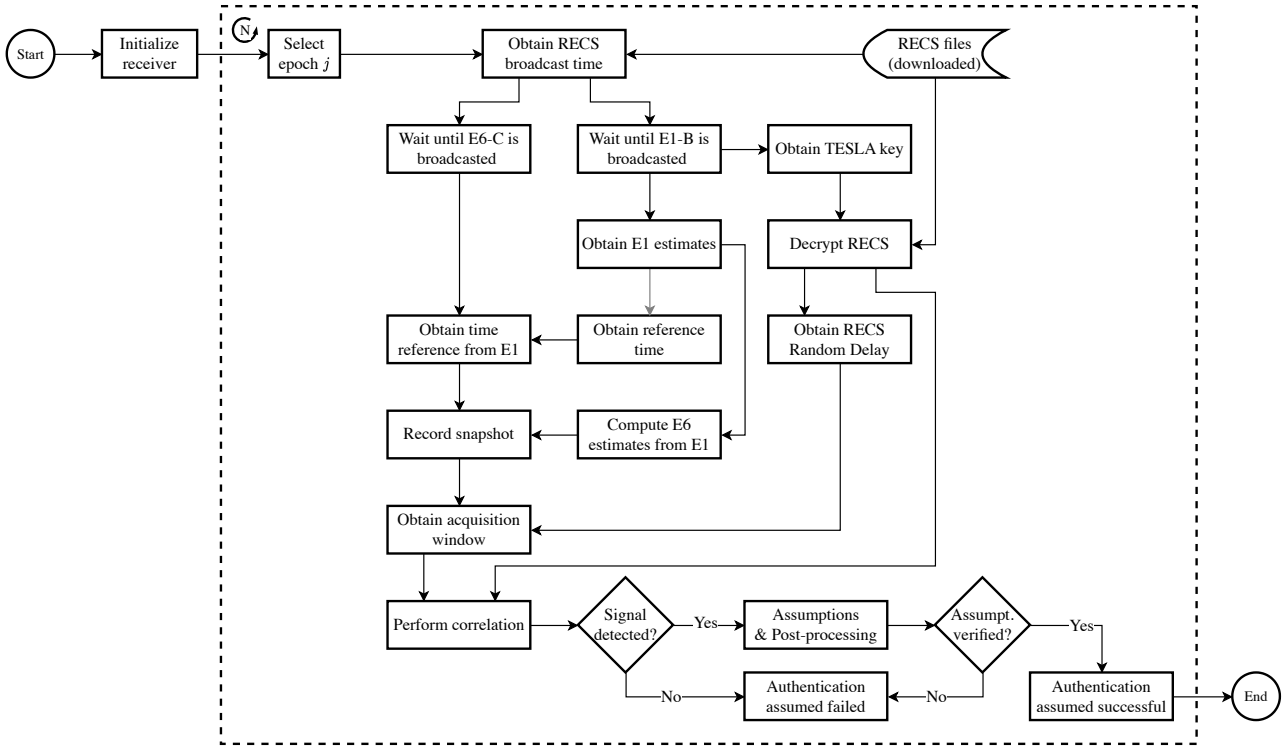

Figure 2: ACAS nominal operating mode schematics.

A detailed analysis of the ACAS implementation and the threat mitigation analysis is performed in (Winkel et al., 2023).

2. Acquisition Procedure

While the acquisition procedure details and implementation issues have already been discussed in (Terris-Gallego et al., 2022b) and (Fernandez-Hernandez et al., 2023b), this section provides a concise summary of the essential concepts. This serves to provide additional rationale for the simulations and results presented in Section IV.

Each of the RECS files downloaded by the receiver stars with a header that defines the parameters of the service, the most relevant of which are summarized in Table 1:

Table 1: Main ACAS parameters.

Notation	Description
t_{start}	Start time.
τ_{RECS}	RECS Period.
N_{chips}	Number of chips per RECS.
δ_{RECS}	Initial offset between the start time and the first RECS.
$\Delta\tau_{\max}$	RECS maximum random delay.

Thanks to the time reference obtained from the E1-B, the receiver could be synchronized with the Galileo System Time (GST). Therefore, the snapshot start time at the receiver for each satellite k and period j, denoted $t^k_{\text{snapshot-start},j}$, can be determined by the offset δ_{RECS}, and the corresponding propagation delays and satellite/receiver clock offsets, in addition to the inter-frequency time biases between E1 and E6 signals, as detailed in (Fernandez-Hernandez et al.,

2023b). Except for the initial predefined RECS offset and the receiver clock one, which is applicable to all periods and satellites, the rest of parameters is specific to each satellite, and are included in the parameter denoted as δ^k. Denoting as GST_j the second associated to the j-th period, the snapshot start time is given by:

$$t^k_{\text{snapshot-start},j} = \mathrm{GST}_j + \delta_{\mathrm{RECS}} + \delta^k \tag{1}$$

As defined in (European Commission, 2021), the position of the ECS in a given RECS period can be randomized, for each satellite and period, by means of the random delay parameter, denoted as $\Delta\tau^k_j$. Since this parameter is unknown at the time the receiver records the snapshot, the receiver must consider the maximum value this delay can attain, which is defined by the RECS maximum random delay described in Table 1.

Therefore, the snapshot end time for the k-th satellite and j-th period is given by:

$$t^k_{\mathrm{end},j} = t^k_{\mathrm{start},j} + \Delta\tau_{\max} + T_{\mathrm{RECS}} \tag{2}$$

where $T_{\mathrm{RECS}} = \frac{N_{\mathrm{chips}}}{R_c}$ is the length of the RECS/ECS, being N_{chips} the number of chips of the RECS, and $R_c = 5.115 \cdot 10^6$ the chip rate for E6-C.

In order for the snapshot to capture the $\mathrm{ECS}^{\mathrm{R}}$s for all the satellites, the snapshot duration should be extended to account for the minimum and maximum values that the offset δ^k can reach, as detailed in (Fernandez-Hernandez et al., 2023b). In practice, considering the range of values of $\Delta\tau_{\max}$, the snapshot can last a few seconds. This is an aspect that needs to be considered regarding the storage capacities of the receiver.

In Figure 3, the receiver acquisition procedure is illustrated.

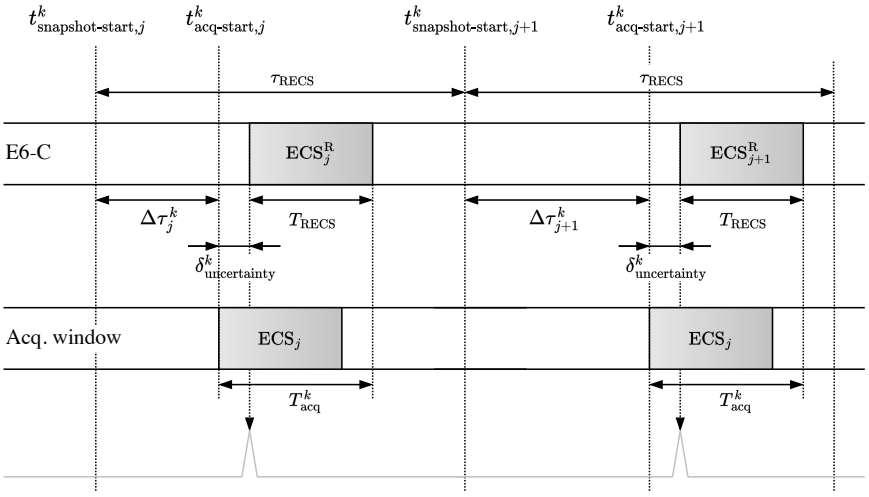

Figure 3: Receiver acquisition schematics.

Once the TESLA key corresponding to the RECS of the j-th period is disclosed, the receiver can calculate this random delay and subtract the associated offset $\Delta\tau^k_j$. This enables to obtain the start time of the acquisition window, which determine the samples of the snapshot will be used for the correlation. Under ideal conditions, as the E6 signal is aligned to the E1 signal, the length of acquisition window will be exactly the size of the ECS.

However, in practice, this alignment is not perfect, and some uncertainty need to be considered. This is due basically to the inter-frequency time bias between both bands, which includes the ionosphere effects, the Broadcast Group Delay (BGD) and the hardware differences. This uncertainty is denoted as $\delta^k_{\text{uncertainty}}$ for the k-th satellite. Hence, the length of the acquisition window for the k-th satellite is given by:

$$T^k_{\mathrm{acq}} = T_{\mathrm{RECS}} + \delta^k_{\text{uncertainty}} \tag{3}$$

The alignment between E1 and E6 offset is then crucial for the ACAS acquisition, since basically define the uncertainty to be considered by the receiver. In practice, considering just a few samples of uncertainty is sufficient to obtain a successful correlation in E6-C from the E1-B estimates, as depicted in (Fernandez-Hernandez et al., 2023b).

Once established this uncertainty, the receiver can perform the correlation of the samples of the acquisition window with the local replica (i.e., the decrypted RECS) and obtain the Cross Ambiguity Function (CAF). Typically, this implies a bi-dimensional search performed in the acquisition for both the time and frequency domains. However, as the E6-C Doppler frequency can be estimated from E1-B considering the carrier frequency ratios of both bands:

$$\hat{f}_{d,6} = \hat{f}_{d,1} \frac{f_{c,6}}{f_{c,1}} \tag{4}$$

where $\hat{f}_{d,i}$ and $f_{c,i}$ are, respectively, the Doppler frequency estimates and carrier frequencies for the Ei-th band ($i = \{1, 6\}$).

Therefore, in the ACAS nominal operating mode, the frequency search can be generally omitted, and acquisition search is reduced to only the time domain.

Finally, if the (absolute or squared) maximum value of the CAF exceeds a given threshold (typically predefined for a given probability of false alarm), the signal is considered detected and, under some circumstances, it could be considered authenticated (Terris-Gallego et al., 2022b).

III. LOW-COST SDR PLATFORM

To perform a preliminary evaluation of ACAS using the existing Open Signals, a low-cost SDR platform has been developed. The real datasets obtained with this platform are then processed with a custom MATLAB simulator to obtain the required estimates, which allow to establish a recommended configuration for the main service parameters.

1. Platform Description

The SDR platform developed is based on bladeRF micro boards from Nuand, whose specifications fulfills the requirements to test the ACAS acquisition performance. A detailed description of this platform is provided in (Terris-Gallego et al., 2023). Next, we summarize the most relevant features.

In order to acquire samples of both bands synchronously, two bladeRF boards are connected to the same multi-band antenna and share a common external reference. A Oven-Controlled Crystal Oscillator (OCXO) is used in our case, but a more affordable Temperature-Controlled Crystal Oscillator (TCXO) can also be used. This prevents the mismatches that may arise from using different clock sources. Alternatively, if no external clock is available, the internal clock of the master board can be used for the slave board, to ensure that both boards use the same reference. The schematics of the platform are shown in Figure4, and the prototype used is shown in Figure 5.

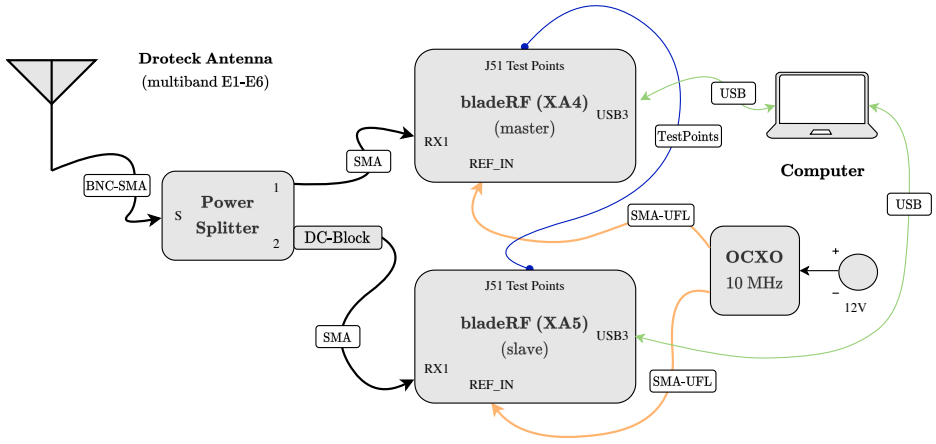

Figure 4: Low-cost SDR platform schematics.

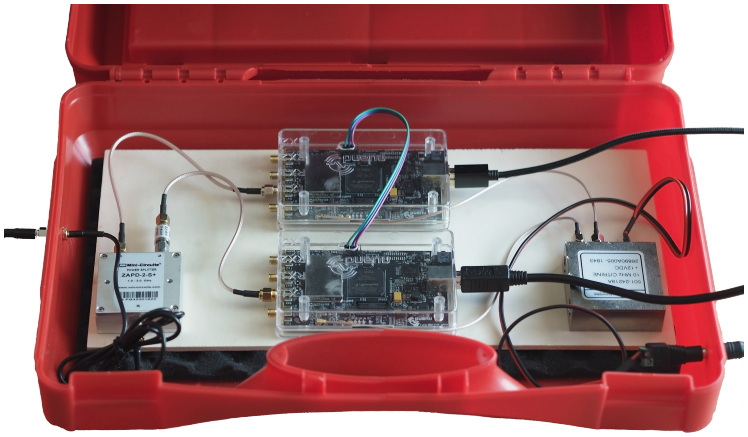

Figure 5: Low-cost SDR platform prototype.

The boards can be configured using the bladeRF's official library as in (Terris-Gallego et al., 2023), or using a compatible API like SoapySDR. The synchronized acquisition of E1 and E6 samples is achieved by connecting the J51 test points of both boards, and executing, in the order shown, the commands of Table 2. In the example shown, 200 million samples would be recorded.

Table 2: Synchronization commands using the bladeRF's official library.

Board	Command
master	`rx config file=snapshot_master_e6.bin n=200M timeout=10s`
master	`trigger j51-1 rx master`
slave	`rx config file=snapshot_slave_e1.bin n=200M timeout=10s`
slave	`trigger j51-1 rx slave`
master	`trigger j51-1 rx fire`

If the `timeout` option is omitted, a timeout of 1 second is used by default. This is typically enough when the commands are automated in a routine, but if the if the commands are executed manually, a timeout error is reported if the trigger on the master board is executed more than one second later than the slave receiver's configuration command. In such case, a larger timeout can be configured, as shown in Table 2.

It is worth noting that the configuration of the synchronization feature is not reported in the official Nuand's documentation, but has been inferred from a similar feature available in other boards of the same manufacturer.

2. Real Datasets using Existing Open Signals

The real datasets used in this paper were obtained in a rural area with clear-sky scenario. The recording spot is located near Girona (Spain), at a latitude of 41°59'35" N (41.9932) and a longitude of 2°47'43" E (2.7954). To emulate scenarios with lower carrier-to-noise ratios, the antenna was covered under building blocks of wood or concrete with different set-ups. The specific data for each dataset used are summarized in the Table 3.

Table 3: Information about the real datasets used in the paper.

Dataset ID	Recording Date/Time	Duration	Sampling rate
D1	2023-04-12 11:54 (GMT)	8 seconds	20 MHz
D2	2023-04-14 14:21 (GMT)	3.2 seconds	20 MHz

The sky plots of visible Galileo satellites for the recorded datasets with an elevation not lower than 20^{o} are shown in Figure 6 and Figure 7, which has been obtained with the web tool "GNSS-Radar" (`http://taroz.net/GNSS-Radar.html`). In Table 4 and Table 5 we list these satellites with their corresponding azimuth and elevation. The orbital and technical parameters for the Galileo satellites can be found in (European GNSS Service Center, 2023).

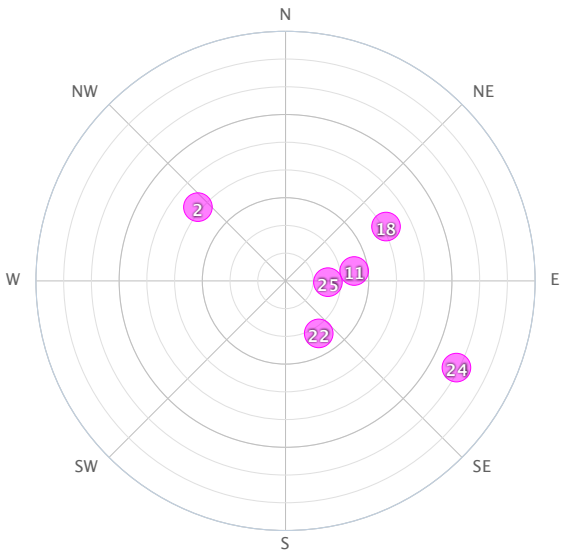

Figure 6: Visible Galileo satellites for dataset D1.

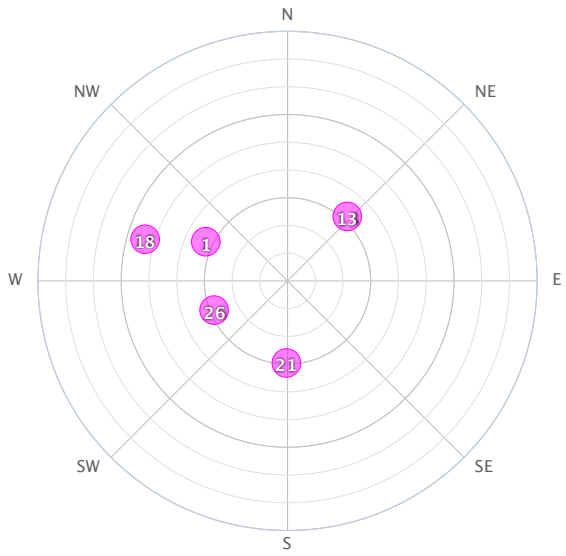

Figure 7: Visible Galileo satellites for dataset D2.

Table 4: Nominal Galileo satellites in dataset D1.

SVID	Azimut	Elevation
E02	310.1^{o}	48.7^{o}
E11	81.8^{o}	65.0^{o}
E18	61.6^{o}	48.8^{o}
E22	147.7^{o}	67.6^{o}
E24	113.4^{o}	24.3^{o}
E25	75.1^{o}	77.0^{o}

Table 5: Nominal Galileo satellites in dataset D2.

SVID	Azimut	Elevation
E01	295.6^{o}	57.2^{o}
E13	42.9^{o}	58.2^{o}
E18	286.3^{o}	36.6^{o}
E21	180.8^{o}	60.4^{o}
E26	248.4^{o}	61.6^{o}

It is worth noting that both SVID 18 and SVID 22 are auxiliary Galileo satellites, which have been omitted hereafter for our analysis. All the datasets of real samples recorded with the SDR platform used for this paper can be downloaded from `https://spcomnav.uab.es/resources/acas_datasets`.

IV. PRELIMINARY EVALUATION OF GALILEO ACAS

In this section we provide a preliminary evaluation of the Galileo ACAS using the existing open signals. Indeed, the current E6-C signal is broadcasted unencrypted and, hence, is a periodic signal. It is a pilot signal composed by 1-ms primary spreading codes, tiered with a known secondary code of 100 1-ms symbols (European Union, 2019).

Therefore, in order to evaluate the impact of the RECS length, we need to perform the equivalent coherent integration time by accumulating the required 1-ms primary spreading codes of E6-C open signal. Technically speaking, the definition of the RECS length may not be an exact multiple of 1-ms blocks, but the difference could be neglected for this preliminary evaluation.

Currently, this involves performing a secondary code acquisition on E6-C to obtain the corresponding Secondary Code Index (SCI) and proceed with the coherent integration. It is worth noting that this will not be required once the E6-C signal will be encrypted.

1. C/N_0 Estimation

To evaluate the ACAS performance in different scenarios, we first perform an estimation of the carrier-to-noise-density ratio of the E6-C signal for the snapshots recorded with the SDR platform. The estimator used is the following non-coherent post-correlation estimator presented in (Seco-Granados et al., 2012) and proposed in (Borre et al., 2022) for snapshot receivers:

$$\left(\frac{\hat{C}}{N_0}\right)_{\mathrm{NC}} \doteq \frac{R_{\mathrm{NC}}\left(\hat{\tau}_0, \hat{f}_{d,0}\right) B_n - T_{\mathrm{int,coh}} F_s^2 \hat{P}}{\left(T_{\mathrm{int,coh}} F_s\right)^2 \hat{P} - R_{\mathrm{NC}}\left(\hat{\tau}_0, \hat{f}_{d,0}\right)} \tag{5}$$

where $R_{\mathrm{NC}}\left(\hat{\tau}_0, \hat{f}_{d,0}\right)$ is the value of the (non-coherent) CAF for the estimated code phase delay $\hat{\tau}_0$ and the estimated Doppler frequency $\hat{f_{d,0}}$, B_n is the receiver noise equivalent bandwidth, $T_{\mathrm{int,coh}}$ is the coherent integration time, F_s is the sampling rate, and $\hat{P}$ is an estimate of the input signal power.

The non-coherent CAF can be expressed as:

$$R_{\mathrm{NC}}(\tau, f) \doteq \frac{1}{N_I} \sum_{k=0}^{N_I-1} \left|R_{\mathrm{C}}(\tau, f; k)\right|^2 \tag{6}$$

where N_I is the number of non-coherent integrations and R_{C} the (coherent) CAF.

This estimator includes a pre-correlation estimate of the noise power, and therefore is less sensitive to the errors in the code delay and Doppler frequency estimation that typically occurs in acquisition stage, which makes other traditional estimators less suitable for snapshot receivers.

As pointed out in (López-Risueño and Seco-Granados, 2005), this estimator exhibits a good performance when the probability of acquisition is high, that is, for large C/N_0 ratios or for large integration times. Indeed, under such conditions, it shows a bias smaller that 1 dB and the variances becomes very close to the Cramer-Rao Bound (CRB).

In Table 6 and Table 7 we show the C/N_0 estimates of the E6-C signal for all the visible satellites found in the real datasets used. The SCI for E6-C is also indicated, as it will be later used to emulate the required length for the RECS. The satellites selected for the preliminary evaluation are highlighted in red.

Table 6: Estimates for dataset D1.

SVID	C/N$_0$	SCI
E02	48 dB-Hz	20
E11	43 dB-Hz	24
E24	35 dB-Hz	13
E25	43 dB-Hz	23

Table 7: Estimates for dataset D2.

SVID	C/N$_0$	SCI
E01	43 dB-Hz	12
E13	42 dB-Hz	12
E21	40 dB-Hz	12
E26	45 dB-Hz	13

As expected, both the C/N_0 and SCI estimates are consistent with the position of the visible satellites for each snapshot, where the lower C/N_0's generally correspond to lower elevations. It is worth noting that, due to the non-uniformity of the blocks covering the antenna, some satellites could exhibit different attenuations than expected with respect to their specific elevation.

2. Results – E1-E6 Alignment

In this section, we analyze the alignment of both E1 and E6 estimates, which is of key importance for the ACAS nominal operating mode, as it allows to reduce the acquisition search space. A first analysis of this alignment was conducted in (Terris-Gallego et al., 2023), for open-sky scenarios with high C/N_0 larger than 45 dB-Hz.

The goal of this analysis is to check the consistency of these estimates, for different C/N_0's and RECS lengths. To accomplish this, a MATLAB simulator has been developed, which divides these snapshots into smaller chunks to be processed individually. For each of these chunks, the simulator obtains the estimates from the E1-B signal (code phase and Doppler frequency), which will be used to perform the acquisition for the E6-C signal in a reduced search space. The length of the acquisition window considered for this preliminary analysis is of 20 samples, even if fewer samples could be envisaged.

Next, we compare the estimates obtained in the E6-C with the ones obtained from E1-B, by computing the difference. The difference obtained in samples is then converted to the equivalent in meters, in order to obtain the Range Error (RE), which is calculated follows:

$$\mathrm{RE} = \frac{c}{F_s}\left[(\hat{\tau}_{0,1})_{\mathrm{mod}\, N_{\mathrm{scode}}} - \hat{\tau}_{0,6}\right] \quad [\mathrm{m}] \tag{7}$$

where F_s is the sampling rate, N_{scode} is the number of samples in a primary spreading code of E6-C (20.000 in our case), and $\hat{\tau}_{0,i}$ is the estimated code phase delay in samples for the Ei-th band. That is, a difference of one sample corresponds to a Range Error of approximately 15 meters, at the sampling rate used.

In Table 8 we detail the relationship of the figures with respect the satellite/dataset used in each case.

Table 8: E1-E6 alignment results.

Figure No.	Dataset ID	SVID	Estimated C/N$_0$	Num. chunks *
Figure 8	D2	E26	45 dB-Hz	500
Figure 9	D2	E21	40 dB-Hz	500
Figure 10	D1	E24	35 dB-Hz	200

* Number of chunks processed for the given snapshot (1 chunk = 16 ms)

The obtained distribution in histograms exhibits, as expected, a non-centered Gaussian-like shape, which variance is related to the sample Additive White Gaussian Noise (AWGN). A Gaussian curve (in red) is fitted to the experimental data (in blue) to interpolate the mean and variance for each case. It is worth noting that no ionospheric correction is applied.

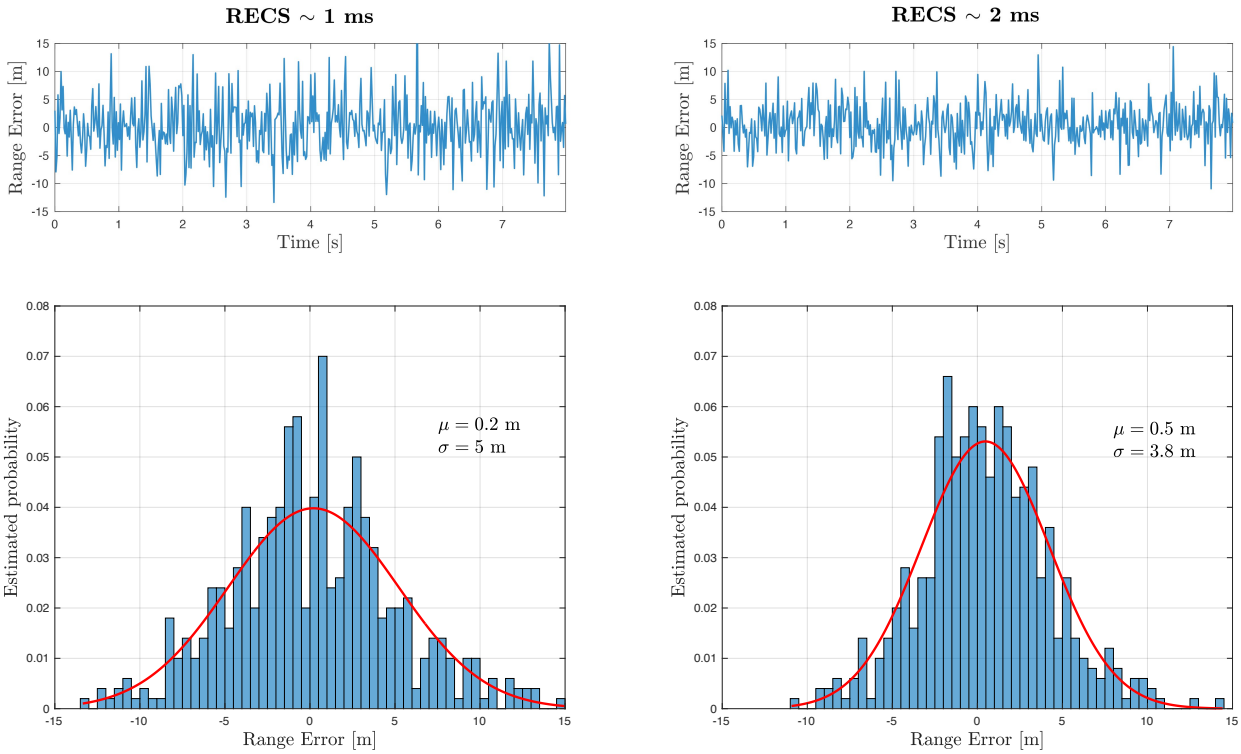

Figure 8: E1-B vs E6-C code phase evolution for SVID 26 in dataset D2 using RECS of 1 and 2 ms.

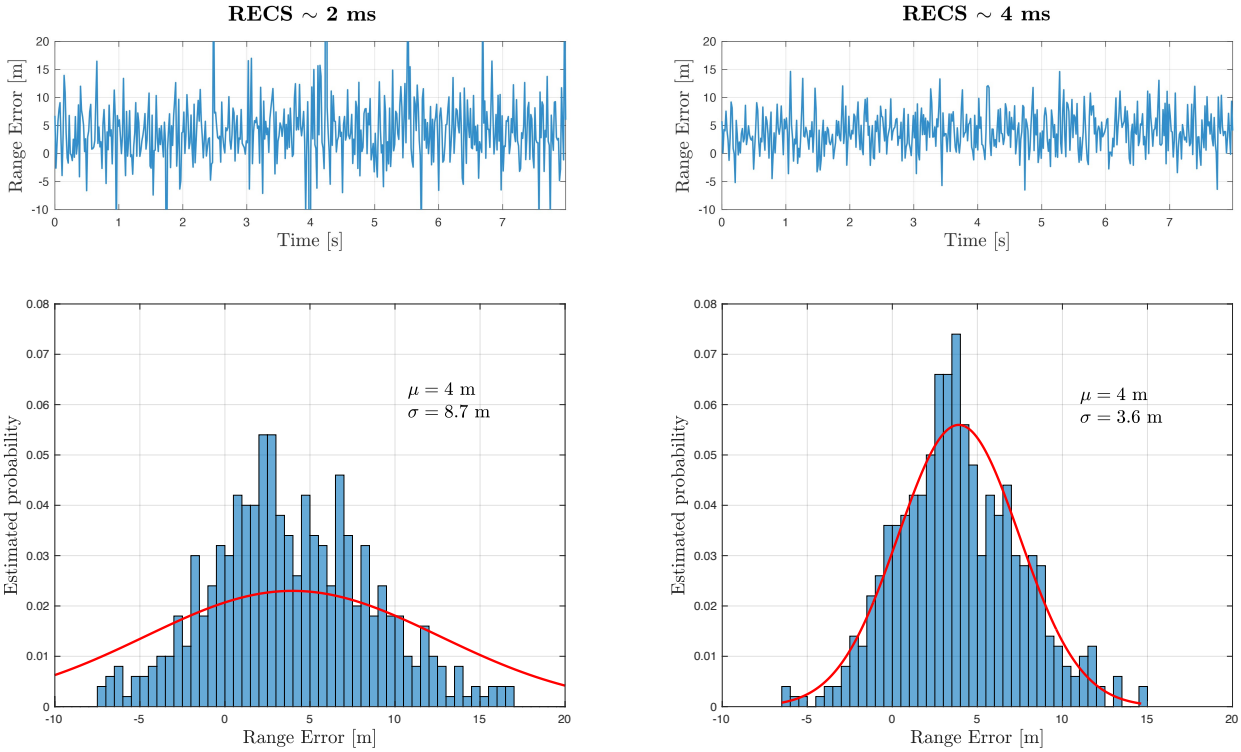

Figure 9: E1-B vs E6-C code phase evolution for SVID 21 in dataset D2 using RECS of 2 and 4 ms.

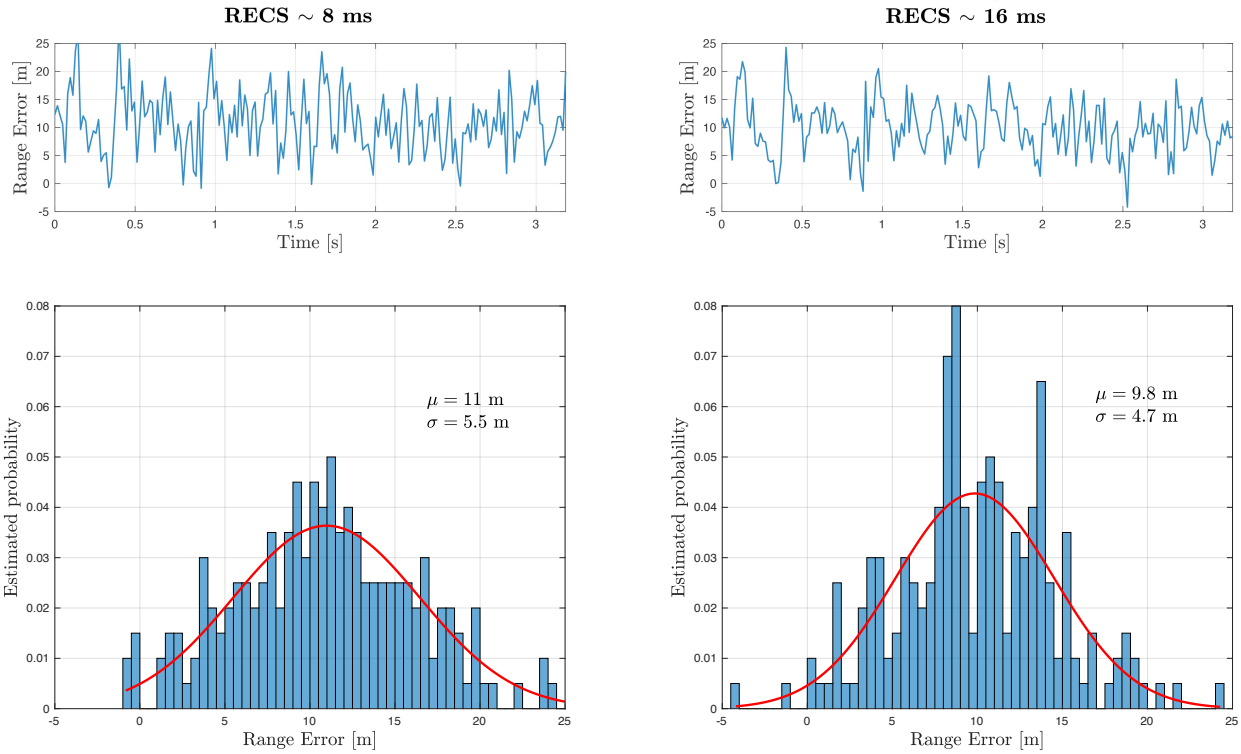

Figure 10: E1-B vs E6-C code phase comparison for SVID 24 in dataset D1 using RECS of 8 and 16 ms.

In Table 9 we summarize the results obtained regarding the code phase estimates comparison. The recommended RECS lengths are highlighted in red, according to the obtained variance, considering a $3\sigma < 15$ meters (corresponding to 1 sample at the sampling rate used).

Table 9: Summary of results of E1-E6 code phase (range error) comparison.

Estimated C/N$_0$	**RECS Length**	**Estimated variance**
45 dB-Hz	$\sim$ 1 ms	$\sigma = 5.0$ m
45 dB-Hz	$\sim$ 2 ms	$\sigma = 3.8$ m
40 dB-Hz	$\sim$ 2 ms	$\sigma = 8.7$ m
40 dB-Hz	$\sim$ 4 ms	$\sigma = 3.6$ m
35 dB-Hz	$\sim$ 8 ms	$\sigma = 5.5$ m
35 dB-Hz	$\sim$ 16 ms	$\sigma = 4.7$ m

3. Results – ROC Curves

To assess the performance of the acquisition we compute the Receiver Operating Characteristic (ROC) curves (Fawcett, 2004), which compare the probability of detection, denoted P_{D}, against the probability of false alarm, denoted P_{FA}, for a given C/N_0. This probability of detection depends mainly on the C/N_0 of the received signal and the length of the local replica used (Borio, 2008) which, for ACAS, is determined by the number of chips used for the RECS.

To compute the ROC curves, each recorded snapshot is divided in chunks of 16 milliseconds. For each chunk, the MATLAB simulator obtains the required acquisition metric (taking the maximum value from the squared CAF) and

finally plots the corresponding curve for a given satellite. To emulate the alternative hypothesis (i.e., the absence of signal), the signal read from the snapshot is multiplied by a random binary sequence that does not correspond with the actual Pseudo-Random Noise (PRN) sequence of the satellite analyzed.

The results are shown in Figure 11, where different configurations have been used, using the previously selected satellites of the real datasets D1 and D2 (see Table 8). The curves correspond to the results obtained with ACAS nominal procedure, i.e., reducing the acquisition search space to just a few samples (20 in our case), thanks to the estimates obtained from the E1-B signal.

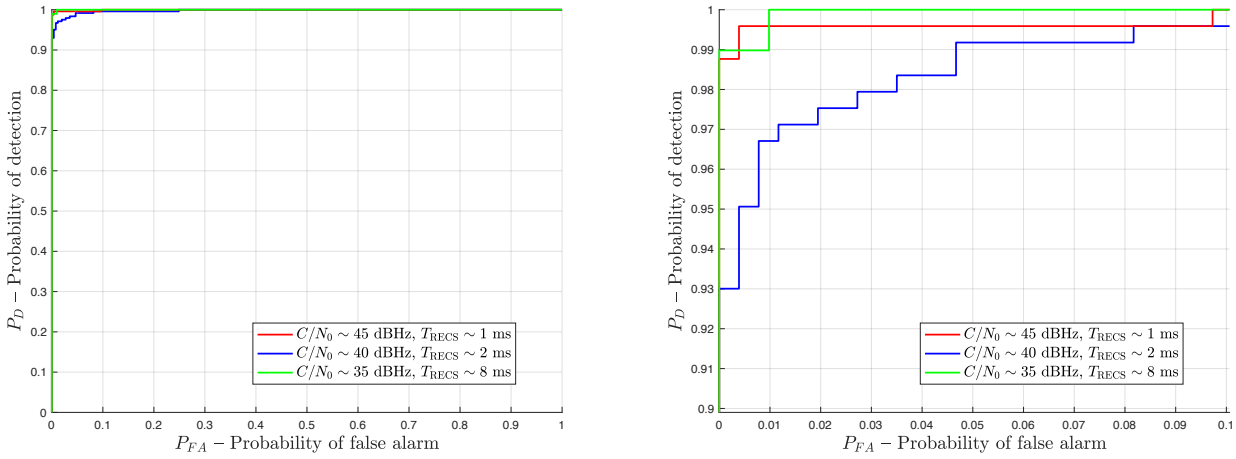

Figure 11: ROC curve for a selection of satellites visible in real datasets selected (on the right, zoomed version for $P_D \geq 0.9$).

As we can observe, just a 1-ms RECS for $C/N_0 = 45$ dB-Hz, 2-ms RECS for $C/N_0 = 40$ dB-Hz and 8-ms RECS for $C/N_0 = 35$ dBHz will suffice to obtain a $P_D > 0.95$ for a $P_{\text{FA}} \sim 10^{-2}$. For lower probabilities of false alarm, doubling at least the size of the RECS will be required (~ 2 ms for $C/N_0 = 45$ dB-Hz, ~ 4 ms for $C/N_0 = 40$ dB-Hz and 16 ms for $C/N_0 = 35$ dB-Hz), which matches the recommendations stated previously in Table 9.

V. CONCLUSION

As detailed in (Fernandez-Hernandez et al., 2023b), the ACAS will be the first service based on the Commercial Service that will provide authentication for the ranging codes. It is an 'assisted' mode since it uses the OSNMA TESLA keys available on the E1-B signal to implement an authentication mechanism that prevents storing any secret key in the receivers. It has also the advantage of using the current signal plan of Galileo, including the E6-C pilot component that will be encrypted when the service starts operating.

The fact of using two frequency bands allows the compatible receivers use the estimates provided by E1 to perform the acquisition on the E6-C signal with very low resources, as just a few correlations may suffice to authenticate the signal. To validate the proof-of-concept of this nominal operating mode envisaged for ACAS, presented in (Fernandez-Hernandez et al., 2023b), a low-cost platform based on bladeRF boards have been developed, which allows acquiring both E1 and E6 samples synchronously. As described in (Terris-Gallego et al., 2023), this platform allows to compare the estimates (specifically the code phase delay and the Doppler frequency) of both bands and corroborate the assumptions which ACAS is based on.

Furthermore, the real datasets obtained with this platform has been used to characterize the probability of detection of the acquisition peak by means of the ROC curves, for different C/N_0 scenarios. That allows to determine the minimum required length for the RECS to be used in each case, which complements the preliminary analysis performed with synthetic data (Terris-Gallego et al., 2022b). These results have been obtained using the existing open signals, emulating RECSs by using the required number of coherent integrations on the E6-C signal to match the RECS Length. Such results should be validated once the E6-C component become encrypted.

Finally, it may be beneficial to explore additional scenarios, especially those involving reduced carrier-to-noise density ratios, such as indoor environments. In situations where C/N_0 is significantly lowered, it might be necessary to

consider multiple combinations of RECSs, achieved through coherent or non-coherent integration of sequences across various RECS Periods. A preliminary analysis was conducted in (Terris-Gallego et al., 2022a) and (Terris-Gallego et al., 2022b), but remains an open point to be further investigated.

ACKNOWLEDGEMENTS

We would like to thank all the participants of the PAULA project (European Commission, 2020b), which is in charge of analyzing the forthcoming ACAS. This work was supported in part by the European Commission Defence Industry and Space Satellite Navigation (DEFIS) contract DEFIS/2020/OP/0002 and in part by the Spanish Agency of Research project PID2020-118984GB- I00 and by the Catalan ICREA Academia Programme. Finally, we would also like to thanks Aleix Galán, GNSS DSP Engineer at Septentrio and former member of SPCOMNAV at UAB, who collaborates in the synchronization configuration tasks of the bladeRF boards used in this paper.

REFERENCES

Borio, D. (2008). *A Statistical Theory for GNSS Signal Acquisition*. PhD thesis.

Borre, K., Fernandez-Hernandez, I., López-Salcedo, J. A., Zahidul, M., and Bhuiyan, H. (2022). *GNSS Software Receivers*. Cambridge University Press.

European Commission (2020a). Call for Tenders (DEFIS/2020/OP/0002) - Test Platform on Galileo HAS/CAS/OSNMA - Tender Specifications - Annex 7.

European Commission (2020b). Call for Tenders (DEFIS/2020/OP/0002) – Test Platform on Galileo HAS/CAS/OSNMA – Tender Specifications.

European Commission (2021). Galileo Assisted Commercial Authentication Service (ACAS) Specification Proposal v1.0.

European GNSS Service Center (2023). Orbital and Technical Parameters. *https://www.gsc-europa.eu/system-service-status/orbital-and-technical-parameters*.

European Union (2019). Galileo E6-B/C Codes Technical Note.

Fawcett, T. (2004). ROC Graphs: Notes and Practical Considerations for Researchers.

Fernandez-Hernandez, I., Cancela, S., Terris-Gallego, R., López-Salcedo, J. A., Seco-Granados, G., O'driscoll, C., Winkel, J., Dalla Chiara, A., Sarto, C., Rijmen, V., Blonski, D., and De Blas, J. (2022). Semi-Assisted Signal Authentication Based on Galileo ACAS. *arXiv preprint*.

Fernandez-Hernandez, I., Damy, S., Susi, M., Martini, I., Winkel, J. O., Cancela-Diaz, S., Chamorro-Moreno, A., Calle, J. D., De Blas, F. J., Simón, J., Blonski, D., and Ibanez-Izquierdo, D. (2023a). Galileo Authentication and High Accuracy: Getting to the Truth. *Inside GNSS*.

Fernandez-Hernandez, I., Rijmen, V., Seco-Granados, G., Simon, J., Rodríguez, I., and Calle, J. D. (2016). A navigation message authentication proposal for the Galileo open service. *NAVIGATION, Journal of the Institute of Navigation*, 63(1):85–102.

Fernandez-Hernandez, I., Vecchione, G., and Díaz-Pulido, F. (2018). Galileo authentication: A programme and policy perspective. In *69th International Astronautical Congress*.

Fernandez-Hernandez, I., Winkel, J., O'Driscoll, C., Cancela, S., Terris-Gallego, R., Seco-Granados, G., López-Salcedo, J. A., Dalla Chiara, A., Sarto, C., Blonski, D., and de Blas, J. (2023b). Semi-Assisted Signal Authentication for Galileo: Proof of Concept and Results. *IEEE Transactions on Aerospace and Electronic Systems*.

Gutierrez, P. (2021). Galileo Authentication and High-Accuracy Service: Coming on Fast.

Humphreys, T. E. (2013). Detection Strategy for Cryptographic GNSS Anti-Spoofing. *IEEE Transactions on Aerospace and Electronic Systems*, 49(2):1073–1090.

López-Risueño, G. and Seco-Granados, G. (2005). CN0 Estimation and Near-Far Mitigation for GNSS Indoor Receivers. In *2005 IEEE 61st Vehicular Technology Conference, Vol.4*, pages 2624–2628.

Pozzobon, O., Canzian, L., Danieletto, M., and Chiara, A. D. (2010). Anti-spoofing and open GNSS signal authentication with signal authentication sequences. In *5th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC)*, pages 1–6.

Scott, L. (2003). Anti-spoofing & authenticated signal architectures for civil navigation systems. In *Proceedings of the 16th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GPS/GNSS)*, pages 1543–1552.

Seco-Granados, G., López-Salcedo, J. A., Jiménez-Baños, D., and López-Risueno, G. (2012). Challenges in indoor global navigation satellite systems: Unveiling its core features in signal processing. *IEEE Signal Processing Magazine*, 29(2):108–131.

Terris-Gallego, R., Fernandez-Hernandez, I., López-Salcedo, J. A., and Seco-Granados, G. (2022a). Guidelines for Galileo Assisted Commercial Authentication Service Implementation. In *Proceedings of the International Conference on Localization and GNSS (ICL GNSS)*, Tampere.

Terris-Gallego, R., López-Salcedo, J. A., Seco-Granados, G., and Fernandez-Hernandez, I. (2022b). Operating Modes and Performance Evaluation of Galileo Assisted Commercial Authentication Service. In *Institute of Navigation Conference (ION+ GNSS 2022)*.

Terris-Gallego, R., López-Salcedo, J. A., Seco-Granados, G., and Fernandez-Hernandez, I. (2023). E1-E6 SDR platform based on bladeRF for testing Galileo Assisted Commercial Authentication Service. In *European Navigation Conference, ESA ESTEC*, Noordwijk, The Netherlands.

Winkel, J., Fernandez-Hernandez, I., and O'Driscoll, C. (2023). Implementation Considerations for ACAS and Simulation Results. *ArxiV Preprint*.