Operating Modes and Performance Evaluation of Galileo Assisted Commercial Authentication Service

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 2004 he worked at Wavecom France, and from 2005 to 2015 he worked at Indra Barcelona as engineer for 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, 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 M.B.A. 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, UAB.

Ignacio Fernandez-Hernandez is in charge of Galileo high accuracy and authentication at the European Commission, DG DEFIS. He is an ICAI engineer, holds an MBA by LBS and a PhD in electronic systems by Aalborg University.

ABSTRACT

The European Global Navigation Satellite System (GNSS), Galileo, is currently leading the development of new services focused on the authentication of the position to mitigate the vulnerabilities of common receivers. It has recently incorporated the Open Service Navigation Message Authentication (OSNMA) in its E1-B signal, which allows to authenticate the navigation data symbols, but it is also working in the encryption of the spreading codes to provide increased security and robustness against malicious attacks like spoofing ones. This last technique will be provided in the forthcoming Commercial Authentication Service (CAS) operating in the E6-C signal. Currently, an 'assisted' mode is being defined, known as Assisted Commercial Authentication Service (ACAS), which aims to authenticate the ranging signal without the need of storing any secret key at the receiver. This paper reviews the key aspects of this service and its implementation issues and analyses the different operating modes that arise from this implementation, identifying the possible threats to face off.

I. INTRODUCTION

The GNSS market has experienced a massive growth in the past decades, and the demand for new applications and services for positioning and navigation is continuously increasing. However, the ubiquity of GNSS receivers and the development of Software Defined Radio (SDR) tools has paved the way for any user, equipped with a relatively low-cost hardware, to be able to potentially broadcast a fake signal. This has led to an increased interest in the GNSS community to provide enhanced robustness and security for the user's receivers against these vulnerabilities.

Clearly, spoofing attacks are one of main threats the current systems face (Kerns et al., 2014), which poses a security

problem that should be treated carefully, especially when dealing with safety-of-life applications, but also for services that need to obtain an authenticated position. At this regard, many techniques have been analyzed in the literature (Pozzobon et al., 2010), which include Receiver Autonomous Integrity Monitoring (RAIM) techniques, but also proposals to integrate cryptographic protection in the GNSS signals (MacDoran et al., 1998; Scott, 2003; Wullems et al., 2005).

Galileo, the European GNSS, has been the first to develop a service which consists of the digital signature of the navigation message to ensure the data authenticity. This service, known as OSNMA (Fernandez-Hernandez et al., 2016) has been recently made freely available to all users in the E1-B component in the frame of a public observation phase (European Union, 2021), and is expected to be in operational capability by next year.

On the other hand, together with Galileo High Accuracy Service (HAS), which aims to provide high-accuracy Position, Velocity and Timing (PVT) solutions, Galileo is currently working in a new added-value service, named CAS, to provide a full secure solution. It is based on the encryption of the E6-C component at signal level to provide Spreading Code Authentication (SCA), which allows a greater level of protection against signal replay attacks (Gutierrez, 2021). While OSNMA adds some unpredictability to the signals which can be exploited agains replay attacks (Humphreys, 2013), exploiting this feature requires that the receiver is tracking the authentic signal in its initial state (Seco-Granados et al., 2021). This is not the case for SCA.

An early capability of CAS is envisaged by 2024, which will provide an 'assisted' signal authentication mode known as ACAS. In this 'assisted' mode, the need of storing any secret key is avoided, while providing the user receiver with the ability to operate autonomously for long periods of time. This is achieved by selecting some fragments of the encrypted E6-C signal yet to be transmitted, identified as Encrypted Code Sequences (ECSs), and re-encrypting them with a key yet to be disclosed, resulting in the so-called Re-Encrypted Code Sequences (RECSs). These re-encrypted fragments, together with some other useful information like their start and end broadcast times, are made available as files in the GNSS Service Centre (GSC), from which the receiver can download them.

The re-encryption of the ECS prevents any user, including a spoofer, from generating a fake signal once these fragments are downloaded, since it will not be able to decrypt these sequences before the disclosure of the key. The use of the Timed Efficient Stream Loss-tolerant Authentication (TESLA) key provided by the OSNMA protocol is the chosen option in ACAS, which has the convenience to be already available to the user in the E1-B open signal.

Once the E6-C signal is broadcasted, the receiver records a snapshot of samples at the time where the Received Encrypted Code Sequence (ECS^R) is expected, and waits for the key to be disclosed in the E1-B signal; once disclosed, the receiver can then decrypt the RECS to obtain the corresponding ECSs (i.e., the local replica) and perform the correlation with the pre-recorded samples from the E6-C signal. This operative is schematized in Figure 1.

The autonomy of the receiver to operate in standalone mode can be increased by making available a larger amount of the RECSs in advance, which eliminates the need of a continuous receiver-server communication. Of course, the autonomy of the receiver will depend on its storage capacity, which will ultimately determine the number of the RECSs that can be downloaded in its memory.

As the ACAS is currently being consolidated and is not operating yet, it is crucial to analyze the impact of the different parameters involved in the service, as well as assessing the performance at signal-level in as many scenarios as possible. This can be useful to select the configuration of a hardware's receiver and as a performance reference baseline for practical implementations.

To achieve this goal, we start analyzing, in Section II, the ACAS implementation issues and highlighting the key parameters involved, based on the guidelines and analysis drawn from (Terris-Gallego et al., 2022) and (Fernandez-Hernandez et al., 2022), authors which are currently involved in the service definition. A general model for the acquisition procedure is here provided. In Section III, different operating modes envisaged for ACAS are detailed, which depend on how the receiver obtains the time reference. A preliminary analysis of the threats faced off is also performed. In Section IV, some simulations are also provided to assess the impact of some key parameters. Finally, the conclusions are given in Section V.

II. ACAS IMPLEMENTATION CONSIDERATIONS

This section details the ACAS implementation at acquisition level. It first reviews the ACAS parameters involved in the service definition, and then it presents a generic model for the acquisition process, which takes into account the specificities of ACAS. Also, it depicts the post-detection issues to be considered.

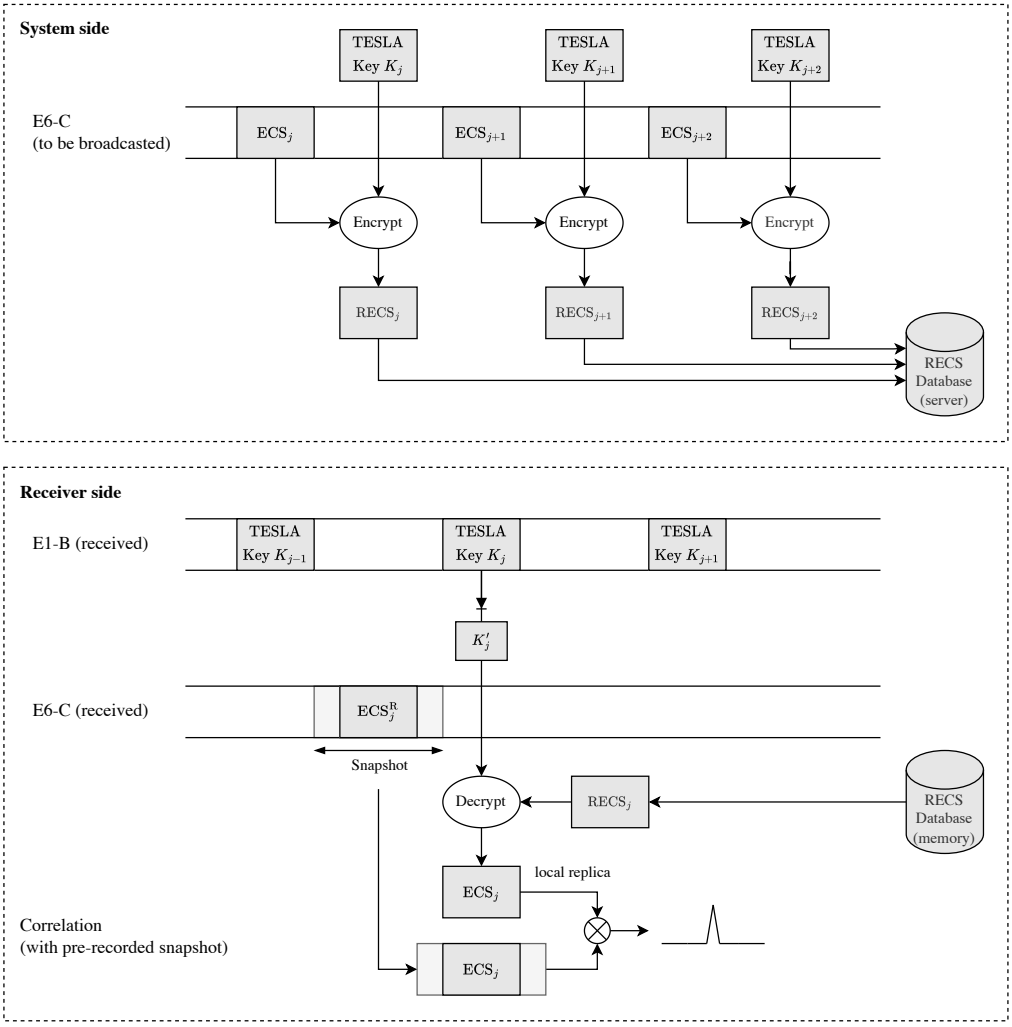

Figure 1: Schematic representation of the ACAS operation.

1. ACAS parameters review

With respect to a conventional GNSS service, in which the signal is made up of a concatenation of known spreading codes, in the ACAS, only a fragment of the E6-C signal (the RECS) is provided to the receiver. Two key parameters follow from this difference: the duration of these fragments and the instants at which these fragments are chosen.

The first parameter is defined as the RECS NChips, denoted $N_{c,\mathrm{RECS}}$, which is the number of chips of these sequences. It determines the duration of the signal fragment used in the acquisition correlation: the longer the RECS is, the higher the processing gain will be and, therefore, the lower the C/N_0 the receiver will be able to operate. Of course, the downside of working with large RECS is the increase in the size associated with the files to be downloaded and stored and, consequently, the reduction in the autonomy of the user's receiver.

The second parameter is defined as the RECS Period, denoted τ_{RECS}, which defines the distance between two consecutive RECS. It determines how often the receiver can compute an authenticated PVT solution. It has also significant impact on the computation of a solution when multiple integrations between different periods are performed.

Besides the RECS NChips and RECS Period, the ACAS service definition takes into account other parameters that have an impact of the implementation, which are detailed in (Fernandez-Hernandez et al., 2022): the RECS Offset, denoted δ_{RECS}, and the RECS Maximum Random Delay, denoted Dτ_{max}, are used to delay and randomize the position of the RECS within a given period; the RECS Length is the duration for with the RECS are provided, that determines the size of the file downloaded from the server by the receiver; finally, the RECS Key Delay, denoted D_K,

is used to determine the delay between the OSNMA key and the related RECS (in multiples of I/NAV subframes, i.e., 30 s).

In the example shown in Figure 2, each OSNMA TESLA key K_j has been used to encrypt two RECSs, from which a hashed version K'_j is obtained to decrypt the corresponding RECSs, i.e., $\text{RECS}_{j,1}$ and $\text{RECS}_{j,2}$. As these keys are disclosed every 30 s in the E1-B signal, which is the duration of a OSNMA I/NAV frame, the RECS Period turns out to be 15 s. In this example, for the sake of simplicity, both the RECS Offset and RECS Maximum Random Delay are considered equal to 0, so the ECSs are always located at the very beginning of each RECS Period. Finally, the RECS Key Delay is equal to 1, as the key of the epoch $j+1$ is used to decrypt the RECSs of the epoch j.

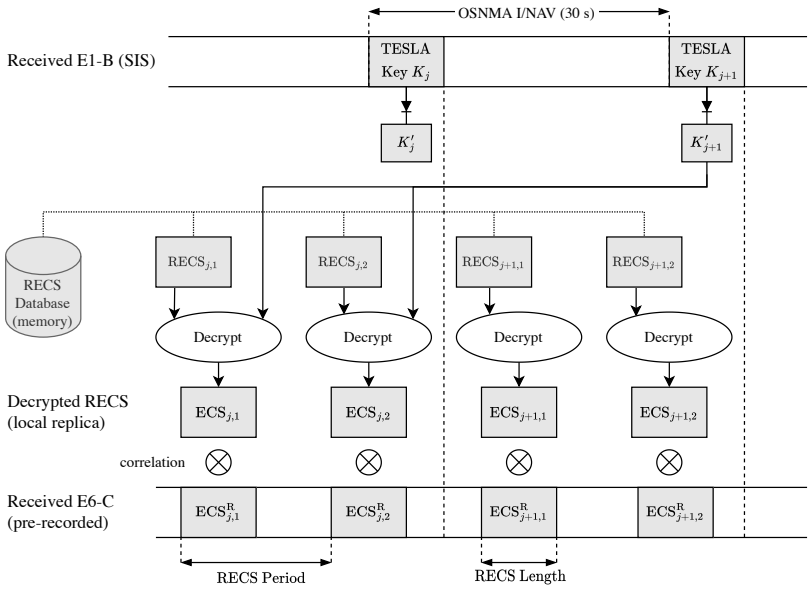

Figure 2: Schematic representation of the ACAS operation at the user's receiver.

A summary of all the parameters involved in the service definition is given in Table 1.

Table 1: Definition and notation of RECS parameters as defined in (Fernandez-Hernandez et al., 2022)

Notation	Definition
$N_{c,\text{RECS}}$	RECS NChips specified in chips.
T_{RECS}	RECS Length specified in seconds.
τ_{RECS}	RECS Period specified in seconds.
$\text{D}\tau_{\max}$	RECS Maximum Random Delay specified in seconds.
L_{RECS}	RECS File Length specified in seconds.
δ_{RECS}	RECS Offset specified in seconds.
D_K	RECS Key Delay specified in I/NAV subframes (30 seconds).

2. Acquisition procedure implementation

Unlike a conventional GNSS acquisition procedure, where the receiver can start correlating the local replica as soon as the broadcasted signal of interest is received, the ACAS receiver should first determine the snapshot to be recorded from the E6-C signal, and then store it until the corresponding key is disclosed in the E1-B, to perform then the a-posteriori correlation.

To determine the starting time of this snapshot, we assume, without loss of generality, that each key is used to encrypt a unique ECS, so each j-th key corresponds to a unique p-th RECS period. As specified in (Fernandez-Hernandez et al., 2022), for a given period, each ECS could be transmitted at the start of the period or delayed by some amount, which is the sum of the RECS Offset and some random value up to the RECS Maximum Random Delay. However, as this value is unknown by the receiver at this stage, this will not affect the length of the snapshot.

Furthermore, with respect to the transmitted ECS, the ECS^{R} will be affected by the propagation delay and clock offsets (which could either introduce a delay or an advance depending on its sign). These terms can be grouped into what it is defined as the reception delay that, for the k-th satellite, is given by:

$$\tau^k = \tau^k_{\text{prop}} - \delta t^k_{\text{sat}} + \delta t_{\text{rx}} \tag{1}$$

where τ^k_{prop} is the propagation delay from the k-th satellite, δt^k_{sat} is the k-th satellite clock offset, and δt_{rx} is the receiver clock offset.

However, as detailed in (Terris-Gallego et al., 2022), it is more convenient to express this delay in terms of its uncertainty (i.e., the maximum variation it can reach), rather than its absolute magnitude. Hence, the previous equation can be equivalently expressed as:

$$\tau^k = \underbrace{\tau^k_{\text{prop,min}} - \delta t^k_{\text{sat,max}} + \delta t_{\text{rx,min}}}_{\tau^k_{\text{min}}} + \underbrace{\Delta\tau^k_{\text{prop}} + \Delta\delta t^k_{\text{sat}} + \Delta\delta t_{\text{rx}}}_{\Delta\tau^k} \tag{2}$$

Actually, it is worth noting that the only term unknown by the receiver is $\Delta\tau^k$, since the term τ^k_{min} could be estimated a priori from the propagation characteristics and clocks specifications. Thus, we can also define $\Delta\tau^k_{\text{max}}$ as the maximum reception delay uncertainty, which is the sum of the maximum uncertainties of its terms:

$$\Delta\tau^k_{\text{max}} = \Delta\tau^k_{\text{prop,max}} + \Delta\delta t^k_{\text{sat,max}} + \Delta\delta t_{\text{rx,max}} \tag{3}$$

For example, considering that the propagation time in Galileo varies typically between 77 ms and 97 ms, we could establish that $\tau^k_{\text{prop,min}} \approx 77$ ms, $\Delta\tau^k_{\text{prop}} \approx [0-20]$ ms, and, therefore, $\Delta\tau^k_{\text{prop,max}} \approx 20$ ms. For the sake of clarity, a summary of all the parameters defined in this Section is given in Table 2.

Therefore, the starting time of the snapshot for the p-th period and the k-th satellite is given by:

$$t^k_{\text{snp},p} = t^k_{\text{startRECS}} + (p-1)\tau_{\text{RECS}} + \delta_{\text{RECS}} + \tau^k_{\text{min}} \tag{4}$$

where $t^k_{\text{startRECS}}$ is the start time of the RECS extracted from the RECS file for the k-th satellite.

The last expression takes into account only the k-th satellite. For the receiver to take into account all satellites, we rewrite the previous equation as:

$$t_{\text{snp},p} = t_{\text{startRECS}} + (p-1)\tau_{\text{RECS}} + \delta_{\text{RECS}} + \tau_{\text{min}} \tag{5}$$

where $t_{\text{startRECS}} = \min_k(t^k_{\text{startRECS}})$ and where τ_{min} account for the sum of the minimum (or maximum, depending on the sign) values of the terms included in the aforementioned reception delay for all satellites, that is:

$$\tau_{\text{min}} = \min_k(\tau^k_{\text{min}}) = \min_k(\tau^k_{\text{prop,min}}) - \max_k(\delta t^k_{\text{sat,max}}) + \delta t_{\text{rx,min}} \tag{6}$$

The length of the snapshot is given by:

$$T_{\text{snp}} = T_{\text{RECS}} + \text{D}\tau_{\text{max}} + \Delta\tau_{\text{max}} \tag{7}$$

where $T_{\text{RECS}} = N_{c,\text{RECS}}/R_c$ is the length of the ECS/RECS, being R_c is the chip rate of E6-C, and $\Delta\tau_{\text{max}} = \max_k(\Delta\tau^k_{\text{max}})$ is the maximum reception delay uncertainty for all satellites.

This snapshot will be stored in the receiver, waiting for the p-th key, used to encrypt the p-th ECS, to be disclosed. Once this key is disclosed, the receiver can compute (Fernandez-Hernandez et al., 2022) the corresponding random delay that has been applied for the k-th satellite and the p-th period, denoted $\mathrm{D}\tau_p^k$, and shorten the snapshot that will be used for the acquisition, that will be referred as the acquisition window hereafter.

Therefore, the starting time of the acquisition window that will be used for the correlation for the k-th satellite and p-th period is be given by:

$$t_{\mathrm{acq},p}^k = t_{\mathrm{snp},p} + \mathrm{D}\tau_p^k = t_{\mathrm{startRECS}}^k + (p-1)\tau_{\mathrm{RECS}} + \delta_{\mathrm{RECS}} + \tau_{\mathrm{min}}^k + \mathrm{D}\tau_p^k \tag{8}$$

It is worth noting that whilst the starting point of the snapshot is taken considering the uncertainties for all the satellites, the starting point of the acquisition window will depend on the k-th satellite processed.

The length of the acquisition window is given by:

$$T_{\mathrm{acq}} = T_{\mathrm{snp}} - \mathrm{D}\tau_{\mathrm{max}} = T_{\mathrm{RECS}} + \Delta\tau_{\mathrm{max}} \tag{9}$$

It is also worth noting that the length of both the snapshot and acquisition window is constant regardless the satellite or period considered.

An example of the acquisition procedure for two given periods $p = 1, 2$ and k-th satellite is shown in Fig. 3, where, without loss of generality, τ_{min}^k is assumed to be positive, and τ^k is assumed to be shorter than the RECS period.

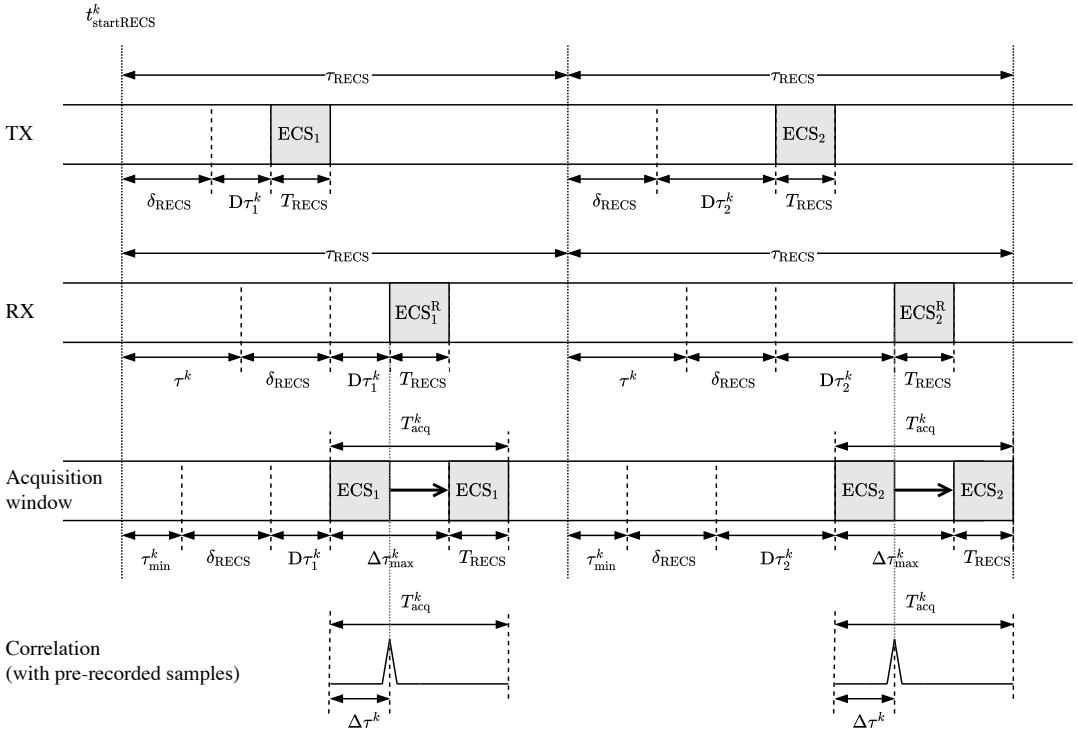

Figure 3: ACAS acquisition procedure for the k-th satellite.

3. Acquisition considerations

The acquisition implementation presented in Section II.2 can be considered as a generic procedure which provides a method for performing the correlation relying solely on the reference time obtained from the RECS file and the receiver clock. The calibration assumptions that can be made from this clock basically determine the value of $\Delta\tau_{\mathrm{max}}$,

Table 2: Definition and notation of parameters

Notation	Definition
$\mathrm{D}\tau_p^k$	RECS Random Delay for p-period and k-th satellite.
τ_{prop}^k	Propagation Delay from k-th satellite to receiver specified in seconds.
$\tau_{\mathrm{prop,min}}^k$	Minimum Propagation Delay (from nearest satellite to receiver) specified in seconds.
$\Delta\tau_{\mathrm{prop}}^k$	Propagation Delay Uncertainty specified in seconds.
$\delta t_{\mathrm{sat}}^k$	Satellite Clock Offset for k-th satellite specified in seconds.
$\delta t_{\mathrm{sat,max}}^k$	Maximum Satellite Clock Offset (from worst case satellite) specified in seconds.
$\Delta\delta t_{\mathrm{sat}}^k$	Satellite Clock Offset Uncertainty for SV-satellite specified in seconds.
δt_{rx}	Receiver Clock Offset specified in seconds.
$\delta t_{\mathrm{rx,min}}$	Minimum Receiver Clock Offset specified in seconds.
$\Delta\delta t_{\mathrm{rx}}$	Receiver Clock Offset Uncertainty specified in seconds.
τ^k	Reception Delay for k-th satellite specified in seconds.
τ_{min}^k	Minimum Reception Delay specified in seconds.
$\Delta\tau^k$	Reception Delay Uncertainty for k-th satellite specified in seconds.
$\Delta\tau_{\mathrm{max}}^k$	Maximum Reception Delay Uncertainty specified in seconds.
$t_{\mathrm{snp},p}^k$	Starting point of the E6-C samples snapshot for k-th satellite specified in seconds.
T_{snp}	Length of the E6-C samples snapshot specified in seconds.
$t_{\mathrm{acq},p}^k$	Starting point of the acquisition window for p-period and k-th satellite specified in seconds.
T_{acq}	Length of the acquisition window specified in seconds.
R_c	Chip rate (of the E6-C signal).

since both the propagation delay and satellite clock offset uncertainties are bounded in practice: in (Terris-Gallego et al., 2022) a value of around 20 ms is used as a bound for these two last parameters.

Therefore, as depicted in eq. (9), if the receiver accounts for a perfectly-calibrated clock without no uncertainty (i.e., $\Delta\delta t_{\mathrm{rx,max}} = 0$), the length of the acquisition window will last for only for some ms, depending of the length of the ECS used. With these values, one can expect a similar performance that could be obtained when dealing with a conventional GNSS signal (concatenation of spreading codes).

However, when the receiver clock is not calibrated, the receiver might have to increase the acquisition window, up to several seconds or more, which would imply a significant degradation of the performance in terms of probability of detection/false alarm. The simulations carried out in (Terris-Gallego et al., 2022) show an example of this severe degradation.

Nevertheless, as in ACAS the receiver needs to track the E1-B signal to obtain the TESLA keys, it is possible to use the time reference obtained from the E1-B signal. This allows not to depend on the receiver clock and, hence, avoid increasing the acquisition window depending on its calibration. This is equivalent to consider $\Delta\tau_{\mathrm{max}} \approx 0$ in the aforementioned generic approach presented previously. This approach allows to substantially improve the acquisition performance in terms of probability of detection, but also exposes the receiver to malicious attacks in the E1-B signal, in addition to the possible attacks in the E6-C signal.

The consequences of using a time reference based on the E1-B signal are further analysed in Section III, where different approaches are considered.

4. Impact of ACAS parameters at acquisition level

In (Terris-Gallego et al., 2022), the impact of the RECS Length on the acquisition performance in terms of probability of detection is analyzed for typical scenarios where the ACAS is intended to operate (C/N_0 not lower than 30 dB). The results shown are obtained assuming ideal conditions (i.e., an infinite receiver bandwidth, doppler frequency perfectly estimated, and perfectly stable receiver, etc.) and for the generic framework presented (that is, without using any aid from E1-B signal). In Section IV we analyze the impact of the RECS Length these results with more realistic scenarios, and also for the case of using the time reference from E1-B signal, which is expected to be the default operating mode for ACAS.

As expected, using larger RECS/ECS has a direct impact of the autonomy of the user's receiver, since the shorter the length, the bigger the number of sequences that can be stored in the receiver's storage, which determines its capacity to operate autonomously without requiring a new connection to the server. Hence, whenever it is possible, the receiver should use the minimum length based on its estimated C/N_0.

For scenarios with higher noise levels, the receiver could combine the RECS located in consecutive periods to increase the probability of detection during the acquisition. However, the RECS Period has a significant impact on the gain that can achieved. Indeed, performing multiple combinations between different RECS poses several issues. First, it hampers the computation of a PVT solution when the RECS period is large and the users's receiver is not static, due to the difficulty of assigning the corresponding reception time. Second, the coherent integration between these RECS is severely limited, especially for large RECS periods, due to the dynamics of the receiver's clock phase noise and the Doppler frequency. Some results are given in in (Terris-Gallego et al., 2022), and additional ones are provided later in Section IV to assess the impact of the RECS Period.

Therefore, it is desirable to avoid the need of using multiple integrations whenever possible, by downloading larger RECS if available in the server (doubling the number of chips will roughly allow to work with 3 dB less of C/N_0). In case it is not possible, non-coherent integration should be envisaged, relegating the coherent combinations only for very specific cases (basically, for small RECS periods). Again, this has an impact on the user's autonomy, since, for a given number of sequences stored in the receiver, the shorter the period is, the smaller this autonomy will be.

It is worth noting that the RECS Offset, the RECS Key Delay and the RECS Maximum Random Delay have no impact on the acquisition performance, since they do not affect the search space size.

III. ACAS OPERATING MODES

Due to the characteristics of the ACAS mode, multiple operating modes can be envisaged, depending on how the receiver obtains the time reference from which it records the snapshot of E6-C samples and performs the a-posteriori correlation with the decrypted RECS.

1. Time reference source

In (Terris-Gallego et al., 2022), a generic approach was presented, in which the receiver relies solely on its own clock to obtain a time reference. The uncertainty assumptions that could be made from it, which will depend basically on its calibration status, in addition to the propagation delay and satellite clock offset uncertainties, will increase or reduce the space search (i.e., the length of the acquisition window) accordingly.

Nevertheless, as in ACAS the E1-B signal is also being tracked to obtain the corresponding TESLA keys, this could be used to obtain a time reference that would not depend on the receiver's clock uncertainty. One possible approach is to use the PVT solution obtained with the E1-B signal. Here, as the time reference is derived from the E1-B PVT, the only uncertainties the receiver will need to account will be the propagation delay and the satellite clock offset. The model presented in (Fernandez-Hernandez et al., 2022) is based on this approach, which we refer to us PVT-based approach.

An alternative approach, based also on the E1-B signal, is to use the transmit Galileo System Time (GST) in the E1-B samples. Here, as the time reference is obtained directly from the samples, the only uncertainty to account will be the satellite clock offset. It is also worth noting that, in this so-called signal-based approach, the receiver operates satellite by satellite, working at signal level without the need of computing any position.

Indeed, each approach responds to different hardware setups, and it is able to authenticate distinct outputs. In the generic approach, the receiver makes only use to the TESLA keys obtained from the E1-B signal and, therefore, the

receiver clock time could be authenticated if the ECS is found where expected. Then the receiver could compute the E6-C pseudoranges and E6-C PVT.

In the PVT-based one, the receiver typically has only access to the E1-B observables/PVT solution, and if the ECS is found where expected, the time derived from E1-B PVT could be authenticated; therefore, to authenticate the PVT, the receiver would need to compute the E6-C pseudoranges. Then the receiver could compare these pseudoranges with the E1-B ones, or use them to compute the E6-C PVT, and compare it with the E1-B PVT.

In the signal-based approach, the receiver has access to the samples of the E1-B signal, and if the ECS is found where expected, is the transmit GST which could be authenticated. This means that the E1-B signal has not been delayed by a spoofer, and therefore the E1-B pseudorange can be trusted. If the same check is applied to several satellites, then the E1-B PVT can be directly authenticated without the need of computing the E6-C PVT as in the PVT-based approach.

In Table 3, we summarize the characteristics of the presented approaches, where $\delta_{\mathrm{E1,E6}}$ models the time bias estimation between the E1 and E6 pseudoranges, and includes the estimation of the satellite bias, the offset of the due to the effects of the ionosphere, and the receiver hardware bias, as detailed in (Fernandez-Hernandez et al., 2022).

Table 3: Operating modes approaches

	Generic	**PVT-based**	**Signal-based**
Time reference source	Receiver clock	Time derived from E1-B PVT	Transmit GST from E1-B
δt_{rx}	Uncertainty	Not needed	Not needed
τ_{prop}	Uncertainty	To be computed	Not needed
δt_{sat}	Uncertainty	To be computed	To be computed (E1-E6 difference)
$\delta_{\mathrm{E1,E6}}$	Not needed	Uncertainty	Uncertainty

2. Threats identification

Certainly, using a time reference based on the E1-B signal (either the PVT-based or the signal-based approach) prevents the receiver to depend on the reliability of its own clock, and may benefit of a reduced acquisition window that leads to an increased probability of detection. Nonetheless, that can make the receiver more vulnerable to some threats.

Therefore, it is meaningful to identify the threat levels that a receiver could have to deal with, and to deduce which assumptions can be arisen from each case. The following levels are here considered:

- Threat level 1 (T1): E1-B signal can be spoofed; E6-C signal cannot be spoofed.
- Threat level 1 (T2): E1-B and E6-C signals can be spoofed.

Clearly, if the receiver does not find the ECS where expected (signal is not detected), the authentication process fails no matter the threat level considered. However, if the receiver finds the ECS where expected (signal is detected), the assumptions that can be made will depend on the threat level considered. Under T1, the authentication will be considered successful; but, under T2, an additional check to discard the presence of the vestigial signal (the "true" one) is advisable. Only if this check is passed, the authentication can be considered successful.

Of course, even when the ECS is not found where expected, the search for the vestigial signal can be useful, for example, to determine the delay of a replay attack. Moreover, not detecting the signal at the first attempt, does not necessarily imply that the signal has been spoofed. Indeed, the receiver could be operating in a low C/N_0 scenario: in such case, the received E6-C signal could be too weak, and the receiver could try using a longer sequence (if available) to compensate this situation. This 'E6-C weak signal' assumption can be also confirmed or discarded by checking the E6-B component: if the signal level of the last one is suspiciously higher than the E6-C level, there are high chances that the E6-C could be spoofed.

Note that the receiver can implement T1 or T2 logic in different circumstances. For example, it may implement T2 logic at startup or with a certain periodicity, in background, while implementing only T1 logic for the regular authentication verifications. This will depend on the level of robustness sought by the manufacturer based on the

intended application, and the receiver's capabilities. It is also worth noting that, depending on its implementation, the search for the vestigial signal could imply recording quite long snapshots and, hence, using large amounts of memory in the receiver.

In Figure 4, we provide a schematized flux diagram of the possible operating modes considering the two threat levels previously defined, detailing the vestigial signal search process in Figure 5. Finally, in Table 4 we summarize the possible outcomes and authentication assumptions that can be made depending on the threat level considered and the signals detected.

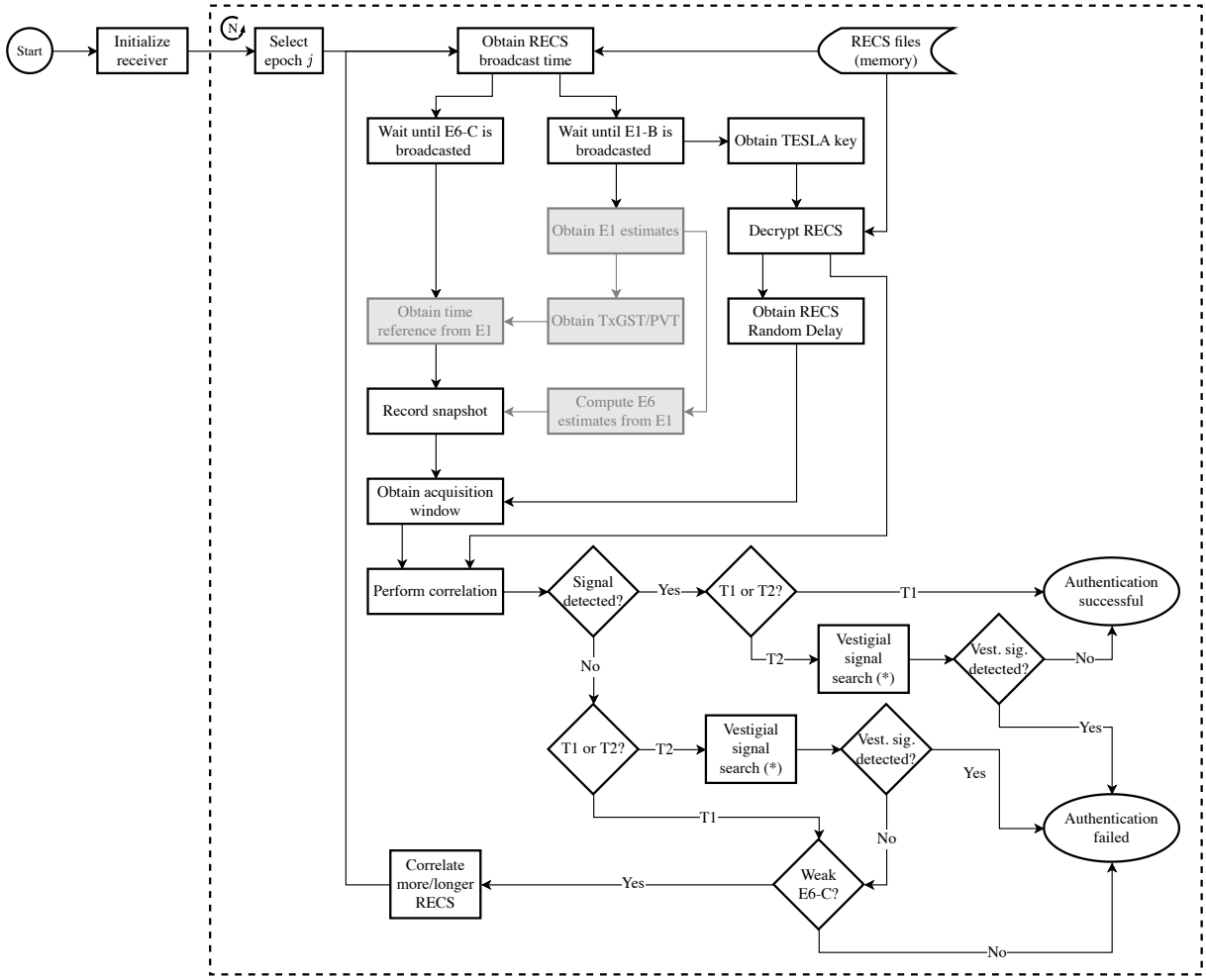

Figure 4: Flux diagram of the ACAS operating modes at the user's receiver: when the grey boxes are omitted, the generic approach is considered; when applied, the PVT-based or signal-based approaches are considered, depending on the time reference obtained from the E1-B signal. (* The vestigial signal search is detailed in Figure 5)

Table 4: Authentication assumptions

Threat level	ECS found in expected location	Vestigial ECS found in another location (1)	Authentication	Assumptions
T1	Yes	N.A.	Successful	-
T1	No	N.A.	Failed	E1-B spoofed, or weak E6-C signal
T2	Yes	Yes	Failed	E1-B and E6-C spoofed (2)
T2	Yes	No	Successful	-
T2	No	Yes	Failed	E1-B spoofed, or E1-B and E6-C spoofed
T2	No	No	Failed	E1-B spoofed, or weak E6-C signal

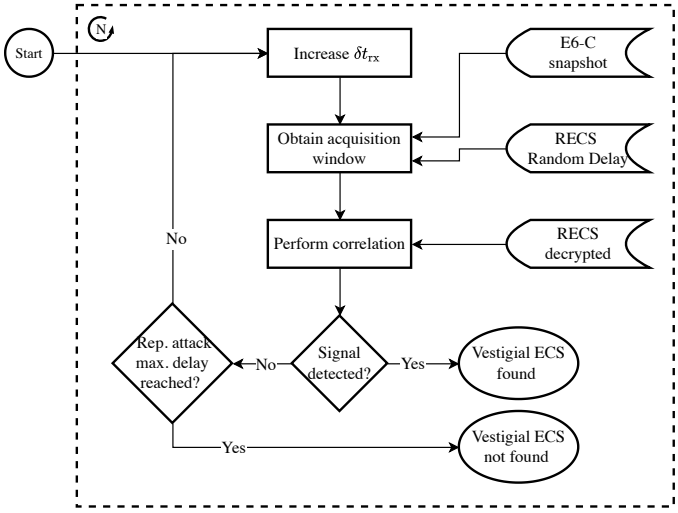

Figure 5: Flux diagram of the vestigial signal search procedure.

(1) It is assumed that, by default, the search for the vestigial signal is performed for the maximum reception delay uncertainty assumed by the receiver; in practice, depending on the memory limitations and other factors, this search could be reduced and, therefore, this will have some implications on the assumptions that can be made.

(2) Multipath considerations may affect the assumptions made in this case.

IV. PERFORMANCE EVALUATION

In this section, we evaluate the impact of the key ACAS parameters in the performance of the acquisition in terms of probability of detection vs probability of false alarm, denoted P_{D} and P_{FA}, respectively, using the Receiver Operating Characteristic (ROC) curves (Fawcett, 2004). The results shown have been obtained using a custom-built ACAS simulator, based on MATLAB™.

1. Impact of RECS Length

As expected, the length of the sequence to be correlated, which is determined by the number of chips used for the RECS/ECS, is one of the main ACAS parameters that drive this performance at acquisition level. In (Terris-Gallego et al., 2022), the minimum recommended lengths for these sequences are determined as a function of the carrier to noise density ratio, for a generic approach (non E1-B-aided).

However, as depicted in Section III, using the E1-B signal could help to reduce the effective uncertainty to just a few samples. In Figure 6 we show the impact of the RECS length in such case, considering and uncertainty of 20 samples, so the length of the acquisition window is roughly the length of a single RECS/ECS. For these simulations, ideal conditions have been assumed, since we aim to evaluate the minimum required RECS Lengths, which are summarised in Table 5.

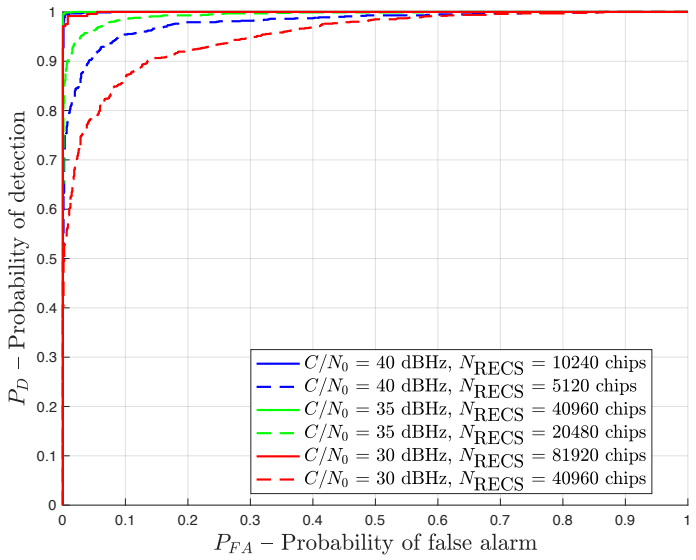

Figure 6: ROC curves, averaged using 2000 Monte Carlo realizations, showing the impact of different RECSs lengths and C/N_0's, considering that the E6 parameters have been estimated from the E1-B signal to reduce the effective uncertainty. The RECS Period is chosen long enough to perform the correlation during the length of the ECS.

Table 5: Minimum ECS length based on C/N_0 under ideal conditions.

$\mathbf{C/N_0}$	**Minimum ECS length**
40 dBHz	10240 chips ($\sim$ 2 ms)
35 dBHz	20480/40960 chips ($\sim$ 4/8 ms)
30 dBHz	81920 chips ($\sim$ 16 ms)

In Figure 7, we compare these results with a more realistic scenario, to assess the degradations with respect the ideal scenario. The realistic scenario simulates a TCXO-type receiver clock, a (two-sided) bandwidth receiver of half the sampling frequency (a frequency sampling of 20 MHz is considered), multiple satellite interference (7 satellites in view with same power level), and aLand-Mobile Satellite (LMS) channel (at 50 km/h), instead of the Additive White Gaussian Noise (AWGN) used under ideal conditions. As in the previous simulation, we consider than the E6 parameters have been estimated form the E1-B signal. As we can observe, with respect to the ideal scenario, larger RECS could be needed to compensate the losses for a given C/N_0, in order to achieve a satisfactory probability of detection.

2. Impact of RECS Period

For low signal to noise ratios, it may be necessary to perform multiple combinations of the RECS sequences. As detailed in Section II.4, the maximum coherent integration time that can be achieved will be mainly determined by the separation between the first and last sequences to be (coherently) combined. In the case of the phase noise, according to the aforementioned results, this turns in the order of some hundreds of ms, depending on the clock type

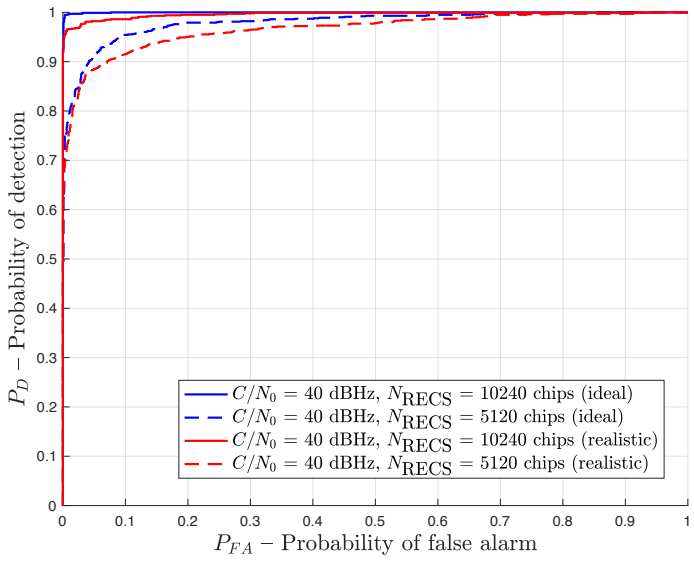

Figure 7: ROC curves, averaged using 2000 Monte Carlo realizations, for RECSs of 5120 and 10240 chips ($\sim$ 1 and 2 ms) and $C/N_0 = 40$ dBHz, showing the comparison of ideal (blue lines) and realistic scenarios (red lines). The RECS Period is chosen long enough to perform the correlation during the length of the ECS.

used in the receiver. In Figure **??**, a simulation is performed to assess how this separation affects the probability of detection when using coherent integration. In this case, an ideal scenario is assumed, in order to evaluate only the impact of the RECS Period. Also, a reference using non-coherent integrations is provided (which does not depend on the RECS Period simulated).

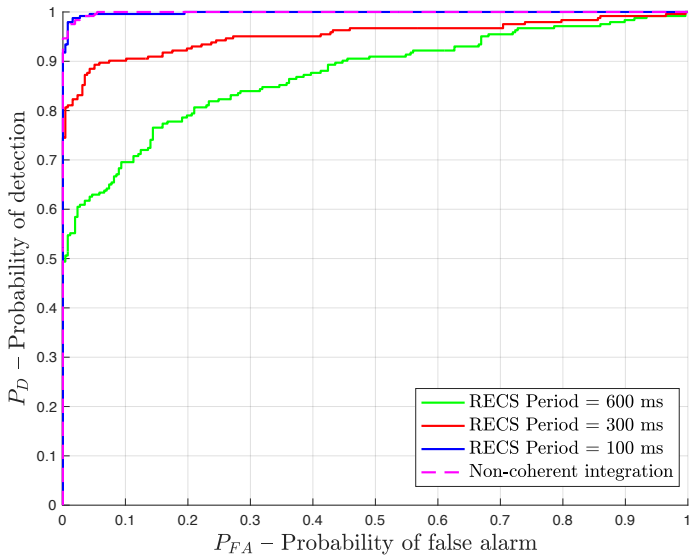

Figure 8: ROC curves, averaged using 500 Monte Carlo realizations, for RECSs sequences of 10240 chips ($\sim$ 2 ms), $C/N_0 =$ 35 dBHz, and a TCXO-type receiver clock, showing the impact of different RECS Periods when $N_c = 3$ coherent integrations are performed. Also, a simulation is performed for $N_i = 3$ non-coherent integrations.

As we can observe, the probability of detection is rapidly degraded when the RECS Period is increased when only

coherent integrations are used, taking only into account the effect of phase noise. This degradation could be larger, of course, in the case of considering the Doppler frequency effect. In any case, the RECS Period severely limits the ability to perform coherent integrations.

V. CONCLUSION

Our contribution is twofold. On the one hand, starting from the first guidelines presented in (Terris-Gallego et al., 2022), we have analyzed in detail the implementation issues of the forthcoming ACAS, highlighting the key parameters involved in the service definition that could impact its performance at signal level, and providing a generic model for the acquisition procedure. This model details the determination of the snapshot and acquisition window required for ACAS as function of the time reference used, and highlights the impact of the reception delay uncertainty considered. Also, some simulations have been carried out to evaluate the performance of these key parameters.

On the other hand, we have described some of the possible operating modes that can be used for ACAS, which mainly depend on how the time reference is obtained. As we have shown, each operating mode responds to a different hardware setup and as such will have different implications from the manufacturer's side. Also, we have identified two levels of threats regarding the spoofing attacks, and we have analyzed how these threats could affect the authentication process of the receiver, depending on the assumptions considered.

From these contributions and the results obtained, it is reasonable to assume that the default operating mode for an ACAS receiver will be using a time reference from the E1-B signal, either from the PVT or the transmit GST, to reduce the reception delay uncertainty to its minimum. The simulations show that, under this circumstances, the acquisition performance in terms of probability of detection are very satisfactory using relatively short RECS Lengths, what will allow a reasonable autonomy for the receiver. Moreover, from a computational point of view, a few correlations will suffice in this approach, that will mainly depend on the accuracy of the estimates obtained from E1-B.

However, as previously analyzed, this E1-B-based approach makes the receiver also vulnerable to spoofing attacks in the E1-B signal, which are also more likely to occur than the ones in the E6-C signal, since the latter is intended to be encrypted at chip level. For that purpose, the receiver may need to implement different mechanisms depending on the assumptions and threat levels considered. In the event of a successful attack on the E1-B signal (or both the E1-B and E6-C signals), a search for the vestigial signal may help to increase the robustness of the receiver, at the expenses of using larger amounts of memory and computation capabilities. Nevertheless, in this search process, as the receiver can only rely in the time reference provided by its own clock, the probability of detecting the signal in a different location than expected could be severely degraded in the case of large clock offset uncertainties. The implementation of this process is still an open point that must be carefully analysed.

ACKNOWLEDGEMENTS

We would like to thanks all the participants of the *Precise and Authentic User Location Analysis* (PAULA) project (European Commission, 2020), 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.

REFERENCES

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

European Union (2021). OSNMA User ICD for the Test Phase, Issue 1.0.

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

Fernandez-Hernandez, I., Cancela, S., Terris-Gallego, R., Seco-Granados, G., López-Salcedo, J. A., 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., 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.

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.

Kerns, A. J., Shepard, D. P., Bhatti, J. A., and Humphreys, T. E. (2014). Unmanned Aircraft Capture and Control via GPS Spoofing. *Journal of Field Robotics*.

MacDoran, P. F., Mathews, M. B., Ziel, F. A., Gold, K. L., Anderson, S. M., Coffey, M. A., and Denning, D. E. (1998). Method and apparatus for authenticating the location of remote users of networked computing systems.

Pozzobon, O., Canzian, L., Danieletto, M., and Chiara, A. D. (2010). Anti-spoofing and open GNSS signal authentication with signal authentication sequences. In *2010 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 2003)*, pages 1543–1552.

Seco-Granados, G., Gómez-Casco, D., López-Salcedo, J. A., and Fernandez-Hernandez, I. (2021). Detection of replay attacks to GNSS based on partial correlations and authentication data unpredictability. *Gps Solutions*, 25(2):1–15.

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

Wullems, C., Pozzobon, O., and Kubik, K. (2005). Signal authentication and integrity schemes for next generation global navigation satellite systems. In *European Navigation Conference (ENC-GNSS 2005)*.