Guidelines for Galileo Assisted Commercial Authentication Service Implementation

Rafael Terris-Gallego*, Ignacio Fernandez-Hernandez†, José A. López-Salcedo*, Gonzalo Seco-Granados*

* Universitat Autònoma de Barcelona (UAB), IEEC-CERES, Barcelona, Spain
† DG DEFIS, European Commission, Brussels, Belgium

***Abstract*—The European Global Navigation Satellite System (GNSS), Galileo, is currently developing and implementing new added-value services aiming to provide increased security and robustness against malicious attacks (e.g. spoofing), like Open Service Navigation Message Authentication (OSNMA), to authenticate the data symbols, or Commercial Authentication Service (CAS), to authenticate the ranging signal. This paper analyses the impact, from a signal-level performance, of the different parameters involved in the service definition of the Assisted Commercial Authentication Service (ACAS) mode, and presents some guidelines for the implementation of this new service, focusing on the acquisition procedure. We also offer some simulation results showing the performance in different scenarios.**

***Index Terms*—GNSS, authentication, Galileo, ACAS, OSNMA**

I. Introduction

Almost three decades after the first GNSS became operational, positioning and navigation receivers have become a commodity. Billions of units are shipped every year, and the demand is continuously increasing as new applications and services are foreseen. The mass production and growing interest in the many navigation constellations available today have, however, a significant downside: it is relatively straightforward to generate and broadcast a fake GNSS signal with a relatively low-cost hardware, so any conventional receiver could be tricked to accept this counterfeit signal.

The need to mitigate this vulnerability has led to intensive research from the GNSS community to investigate effective countermeasures against it, as well as cryptographic protection, either for the navigation message or for the ranging codes. Indeed, the demand for techniques capable to authenticate these signals and detect spoofing attacks have increased notably in the last years [1].

A concept of GNSS authentication service was examined in [2], based on the idea that the presence of unpredictable information in the signal and data could be used to authenticate the signal, since a spoofer would not be able to predict this information. In [3] we find the first attempt to integrate an authentication mechanism for open signals in GNSS, which is based on secret spreading sequence. Another authentication scheme was proposed in [4], in which only the navigation data is authenticated. Since then, many approaches and techniques have been proposed and even implemented [5]. In this regard, Galileo has taken a lead over the rest of navigation systems, incorporating in its service baseline a Navigation Authentication Service (NMA) service, following recommendations from mission and feasibility studies launched in 2013 [6].

Proposed only some years ago [7], Galileo OSNMA, which consists of adding cryptographic information to the navigation data of the Open Service (OS) to ensure the data authenticity, has been recently made freely available to all users in the frame of a public observation phase [8], which is a clear commitment from the Galileo stakeholders to provide resilient location services to the GNSS community. Nevertheless, despite the many advantages of NMA-based schemes, their main aim is not to authenticate the ranging signal. They are not designed to provide a Position, Velocity and Timing (PVT) solution completely protected against the spoofing attacks, but rather to be an extra layer of security that will contribute to improve the user level authentication.

To increase location security, Galileo users may rely on the forthcoming CAS. 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 spoofing, in particular against replay attacks. Together with Galileo High Accuracy Service (HAS), Galileo will become the first GNSS to provide both authentication and high-accuracy data [9].

CAS is currently under development, but an early service is envisaged by 2024, which will provide an 'assisted' signal authentication mode known as ACAS, which will make use of some ancillary data from the E1-B signal allowing the receiver to decrypt the codes without the need of storing any secret key.

This paper is structured as follows. Section II explains the ACAS mode, as currently specified by the European Commission (EC), which is in charge of the service development. Section III analyses the impact at signal-level of the main parameters involved in the ACAS service, and provides some guidelines for the ACAS implementation, specially regarding the acquisition procedure and the related issues. Section IV presents the results obtained with a custom-built ACAS simulator, and finally, conclusions are drawn in Section V.

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. The content of this article does not necessarily reflect the official position the authors' organisations. Responsibility for the information and views set out in this article lies entirely with the authors.

978-1-6654-0575-1/22/$31.00

II. ACAS MODE

In this section, we review the concept of the ACAS, as stated in[10]. In this 'assisted' mode, fragments of the encrypted E6-C keystream are re-encrypted using the Timed Efficient Stream Loss-tolerant Authentication (TESLA) key provided by the OSNMA protocol in the E1-B signal, and published together with other useful information as files in the GNSS Service Centre (GSC) or any publicly accessible servers, at certain predefined instants and for a certain predefined duration.

These fragments are known as Re-Encrypted Code Sequences (RECSs). Once downloaded by the user's receiver, they can be decrypted using the corresponding key to obtain the related Encrypted Code Sequence (ECS), which are used to perform the correlation with the samples received from the E6-C signal. The main benefit of this approach is to allow the user receiver to operate in standalone mode for the duration of the pre-downloaded data (i.e., the RECSs files), and without the need of storing any secret key.

The predefined durations of the RECS are defined by the parameter RECS NChips, denoted $N_{c,\text{RECS}}$, which is the number of chips of these sequences. This is one of the key parameters in the ACAS design, since it determines the duration of the signal fragment used in the acquisition correlation. Together with the frequency bin size used for the Doppler search, if any, they will define the search space of the acquisition and, therefore, the ability to find the correlation peaks from the Cross Ambiguity Function (CAF), from which we generate the pseudoranges and the authenticated PVT solution.

The predefined instants at with the RECSs are chosen , i.e., the distance between to consecutive sequences, are defined by the parameter RECS period, denoted τ_{RECS}. This is another key parameter in ACAS, since it will determine how often the receiver can compute an authenticated solution. It has also significant impact on the computation of a solution when multiple integrations between different periods are performed.

The computed solution from ACAS is also useful for the the initialisation of the time synchronisation required by OSNMA, since the RECSs files are designed to include the transmission time associated to the corresponding ECS of the E6-C keystream, that can be used to resynchronise the receiver [11]. This is, however, beyond the scope of this paper.

The default ACAS operational mode is the snapshot mode. More details on the configuration parameters of ACAS, still under definition, can be found in [12].

Finally, it is worth noting that the TESLA keys used have the convenience to be already available to the user in the E1-B open signal. However, since its delivery is uncoupled from the reception of the E6-C signal, the receiver must store the required samples to perform the correlation, which will be done a-posteriori once the corresponding RECS is successfully decrypted. A simplified scheme of this assisted mode is shown in Fig.1. In this example, the RECS period is chosen to be 15 s, so each key is used to decrypt two RECSs, as the TESLA keys are disclosed every 30 s.

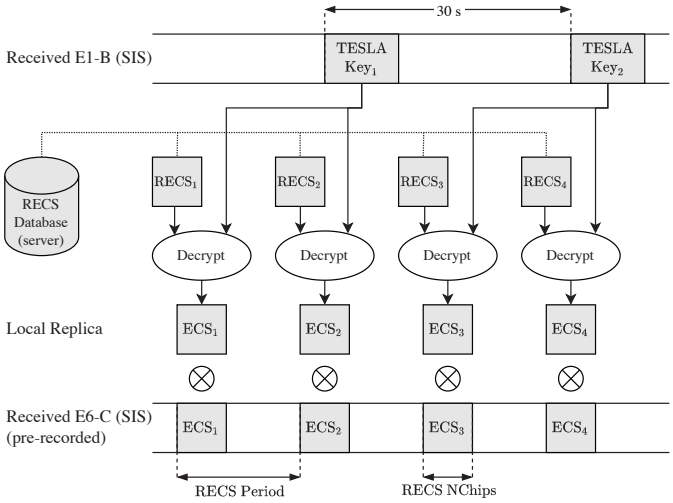

Fig. 1. Schematic representation of the ACAS operation at the user's receiver, once the TESLA keys are received from the Galileo E1-B signal.

III. ACAS IMPLEMENTATION

In this section, we focus on the implementation of the ACAS, considering the key parameters involved in the service that may impact the performance from an acquisition-level. Concretely, we analyse the correlation of the pre-recorded E6-C samples with the decrypted RECSs (i.e., the ECSs).

A. ECS location

In the ACAS, only a fragment of the keystream received from the E6-C signal is provided to the receiver. That makes a big difference in the acquisition procedure with respect to a conventional approach, since the receiver must first determine the location of this fragment.

As in the ACAS the receiver is tracking the E1-B signal to obtain the required TESLA keys for decrypting the RECSs, it is reasonable to assume that the E1-B time reference can be used to know precisely where the ECSs are located in the E6-C keystream. However, the open signal is more susceptible to be spoofed than the E6-C signal, so in what follows a more general framework is assumed, in which the user relies solely in the receiver clock and not on the received E1-B signal.

As specified in [12], for a given period, the corresponding ECS could be transmitted at the start of this period or delayed by some amount. Such delay is the sum of the RECS offset, denoted δ_{RECS}, and the RECS random delay, denoted $\text{D}\tau$. The RECS offset is the same for all periods and satellites, whereas the RECS random delay is chosen from 0 to RECS maximum random delay, denoted $\text{D}\tau_{\max}$, and could be different for each period and satellite. Thus, for p-th period and k-th satellite, the ECS is delayed with respect to the start of the period by:

$$\Delta\text{ECS}^{k}_{\text{tx},p} = \delta_{\text{RECS}} + \text{D}\tau^{k}_{p} \tag{1}$$

From the receiver point of view, the ECS will be subject to further delays with respect to the start of the RECS period due to the propagation delay and clock offsets. The latter, though,

could either introduce a delay or an advance depending on its sign. Hence, the sum of the propagation delay and the clock offsets for k-th satellite, called reception delay, is given by:

$$\tau^k = \tau^k_{\text{prop}} - \delta t^k_{\text{sat}} + \delta t_{\text{rx}} \tag{2}$$

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

However, 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:

$$\tau^k = \tau^k_{\min} + \Delta\tau^k \tag{3}$$

where $\tau^k_{\min} = \tau^k_{\text{prop,min}} - \delta t^k_{\text{sat,max}} + \delta t_{\text{rx,min}}$, and $\Delta\tau^k = \Delta\tau^k_{\text{prop}} + \Delta\delta t^k_{\text{sat}} + \Delta\delta t_{\text{rx}}$.

Hence, from the receiver perspective, the delay with respect to the start of the p-th RECS period and a k-th is given by:

$$\begin{aligned}\Delta\text{ECS}^k_{\text{rx},p} &= \Delta\text{ECS}^k_{\text{tx},p} + \tau^k \\ &= \tau^k_{\min} + \Delta\tau^k + \delta_{\text{RECS}} + \text{D}\tau^k_p\end{aligned} \tag{4}$$

B. Acquisition window

Once established where a given ECS can be found in the E6-C keystream, the receiver needs to determine the search space duration (hereafter, the acquisition window) from the E6-C keystream required to perform the offline correlation with the corresponding ECS obtained from the decryption of the RECS.

To determine the starting point of the acquisition window, one can realise that all the parameters in the term $\Delta\text{ECS}^k_{\text{rx},p}$ are already known by the receiver except $\Delta\tau^k$. Indeed, the RECS offset δ_{RECS} can be extracted from the RECS header [12], the random delay $\text{D}\tau^k_p$ can be obtained after the TESLA key of the related period p is disclosed, and the minimum reception delay $\tau^k_{\min}$ will depend only on the propagation delay, which can be lower bounded from the Galileo orbital specifications.

Therefore, the ECS cannot start earlier than $\Delta\text{ECS}^k_{\text{rx},p} - \Delta\tau^k_p$, so the starting point of the acquisition window for p-th period and k-th satellite is given by:

$$t^k_{\text{acq},p} = \delta_{\text{RECS}} + \text{D}\tau^k_p + \tau^k_{\min} \tag{5}$$

On the other hand, the length of the acquisition window is determined by the length of the ECS to be correlated, denoted T_{RECS}, and the maximum value that $\Delta\tau^k$ can reach, denoted $\Delta\tau^k_{\max}$. Thus, the length of the acquisition window for p-th period and k-th satellite is given by:

$$T^k_{\text{acq}} = \Delta\tau^k_{\max} + T_{\text{RECS}} \tag{6}$$

where $\Delta\tau^k_{\max} = \Delta\tau^k_{\text{prop,max}} + \Delta\delta t^k_{\text{sat,max}} + \Delta\delta t_{\text{rx,max}}$, $T_{\text{RECS}} = N_{c,\text{RECS}}/R_c$, being R_c the chip rate for E6-C codes [13].

It is worth noting that, while the starting point of the acquisition window depends on the period p processed (since the random delay $\text{D}\tau^k_p$ applied is different for each period), its length is constant for all the periods, since it only depends on the length of the sequence to be correlated and the maximum uncertainty $\Delta\tau^k_{\max}$, which depends only on the k-th satellite.

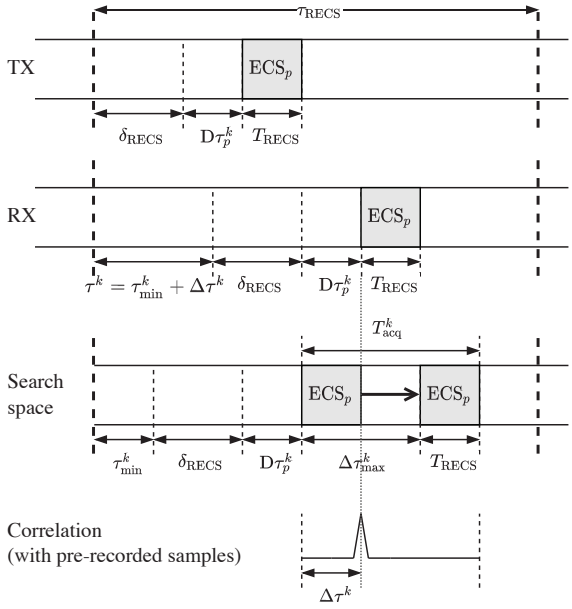

Fig. 2. ACAS acquisition procedure.

It is also worth noting that, if the uncertainty tends to zero, the length of the acquisition window coincides with the length of the ECS. Indeed, if there were no uncertainty at all, one could argue that, strictly speaking, the length would be exactly one sample, since the receiver will know perfectly the alignment of the sequence in the keystream. However, we assume that, at bare minimum, a correlation along the length of the ECS is performed in practice, i.e., $\Delta\tau_{\max} = T_{\text{RECS}}$.

This acquisition window length is, therefore, the key parameter that will drive the performance of the acquisition procedure in terms of probability of detection and false alarm. Indeed, the larger the window, the larger the search space of the CAF, and so, the probability of global false alarm. Besides, the time of processing would be also increased accordingly.

Finally, the correlation peak is obtained, that could be located anywhere in the defined acquisition window. According to these considerations, the acquisition procedure for ACAS for each k-th satellite to be processed is hereafter summarised, assuming that the RECSs have been already downloaded:

1) Obtain the p-th RECS from the receiver storage and decrypt it to obtain the corresponding ECS (the local replica) by means of the related TESLA key.
2) Determine the maximum uncertainty of the reception delay $\Delta\tau^k_{\max}$ and compute the starting point $t^k_{\text{acq},p}$ in (5) and length T^k_{acq} in (6) of the acquisition window.
3) Perform the correlation of the p-th ECS with the samples of the acquisition window from E6-C keystream.
4) Obtain the maximum correlation peak the p-th CAF.

An example of this procedure for p-th period and k-th satellite is shown in Fig. 2, where, without loss of generality, $\tau^k_{\min}$ is assumed to be positive.

C. Post-detection

Typically, due to the undesired effects of the noise, most GNSS receivers need to perform several integrations (coherent or non-coherent, or a combination of both) to decide if the sought signal is present or not. In ACAS, since the fragments to be combined are separated by the RECS period τ_{RECS}, particular attention should be paid. It not only hinders the computation of a PVT solution, since it makes harder to assign the corresponding reception time, but also hampers the use of coherent integrations, as we analyse below.

The maximum coherent integration time is mainly limited by the effects of the frequency doppler and the receiver clock instability (phase noise). When a conventional GNSS signal, resulting in a consecutive concatenation of spreading codes, is processed, these effects are considered for the total coherent integration time, i.e., for N_c code repetitions.

In ACAS, the effects of the Doppler and phase noise span now over N_c periods, i.e., $N_c\tau_{\text{RECS}}$, whereas the total coherent integration time is given by N_cT_{RECS}. For example, regarding the Doppler, typically the frequency bin size in acquisition is chosen to be half the inverse of the coherent integration time; in ACAS, this would translate in half the inverse of the total span time, i.e., $1/2N_c\tau_{\text{RECS}}$. It becomes apparent that to keep this size practical, the RECS period should be very small. For example, for $N_c = 3$ and $\tau_{\text{RECS}} = 100$ ms, the frequency bin size will be approximately 5 Hz, which combined with a typical frequency search range of $\pm$ 5 kHz, would result in 10k frequency bins, leading to a prohibitive acquisition time.

Therefore, if the receiver relies only on the E6-C signal, no multiple coherent integrations can be envisaged in practice. Nevertheless, in ACAS mode, as the E1-B signal is also processed, the receiver could exploit the frequency doppler estimate from the E1 band to estimate the doppler in the E6 band. In ideal conditions, the relationship between both bands is a scale factor between the carrier frequency of both bands. However, when considering the effect of ionosphere, one can realise that its effect is inversely proportional to the carrier frequency, so the E6-C frequency deviation cannot be perfectly estimated from the E1-B signal.

D. E6-band Doppler frequency estimation from E1

The contribution to the delay suffered by the signal is twofold: the effect of ionosphere and the Doppler effect. Thus, the total delay introduced in the signal for the Ei band, $i = \{1, 6\}$, expressed in cycles, is given by:

$$\Delta\tau_i = \frac{40.3 \text{ TEC}}{cf_{c,i}} - \frac{f_{c,i}}{c}vt \tag{7}$$

where TEC is the Total Electron Content, $f_{c,i}$ is the carrier frequency for the Ei-band, c is the speed of light in empty space, v the radial velocity between the satellite and the user. The reference of time t is irrelevant because it does not affect the rate of change of $\Delta\tau_i$.

The estimate for the E6 signal from the E1 signal, denoted $\Delta\tau_6'$, expressed in cycles of $f_{c,6}$, will be given by:

$$\Delta\tau_6' = \Delta\tau_1\frac{f_{c,6}}{f_{c,1}} = \frac{40.3 \text{ TEC}}{cf_{c1}^2}f_{c,6} - \frac{f_{c,6}}{c}vt \tag{8}$$

From the comparison of the previous expression and the estimate obtained directly from E6, we obtain that:

$$\Delta\tau_6 - \Delta\tau_6' = \frac{40.3 \text{ TEC}}{cf_{c,6}}\left(\frac{f_{c,1}^2 - f_{c,6}^2}{f_{c,1}^2}\right) = \frac{40.3 \text{ TEC}}{cf_{c,6}}I_6 \tag{9}$$

where $I_6 \approx 0.3412$ is the ratio which determines the residual error of the doppler frequency estimate for E6.

It is important to note that we are not interested in the absolute magnitude of the ionospheric error of (9), but in its variation over time, i.e., the slant ionospheric delay rate, since the first one can be considered within the acquisition search.

Next, in Table I, we compute the maximum integration times for some typical values of the ionospheric delay rate using the worst-case scenario shown in [14], which have been obtained for the L1-E1 band; the slant ionospheric delay rate in E6 band has been obtained by multiplying the E1 band slant rate by the $f_{c,1}^2/f_{c,6}^2$ ratio. The maximum integration time is computed considering that the maximum acceptable delay, to sum coherently, is around one quarter of the wavelength, which for the E1 and E6 frequency band, corresponds to approximately 4.8 cm and 5.9 cm, respectively.

Finally, in Table II, we compute the maximum integration times for the residual slant ionospheric delay rate in E6 band after doppler correction of E6 band from E1 band, which has been obtained by multiplying the slant ionospheric delay rate in E6 band by the correction ratio I_6 computed in (9).

Therefore, for large slant ionospheric rates, multiple coherent integrations among different RECS periods are only feasible if these periods are very small, e.g. around 300 ms if $N_c = 3$ integrations are envisaged. For slower rates, larger periods can be assumed, but still cannot exceed a few seconds.

It is worth noting that the maximum integration times obtained previously consider that no Doppler frequency search is performed; if it was done, these times could be increased.

TABLE I
MAXIMUM INTEGRATION TIME (E1 & E6 BANDS)

Slant iono. delay rate (E1)	**Confidence interval**	**Max. int. time**
0.8 cm/s	95 %	6 s
3.5 cm/s	99.9 %	1.4 s
10 cm/s	99.999 %	0.5 s
Slant iono. delay rate (E6)	**Confidence interval**	**Max. int. time**
1.2 cm/s	95 %	4.9 s
5.3 cm/s	99.9 %	1.1 s
15 cm/s	99.999 %	0.4 s

TABLE II
MAXIMUM INTEGRATION TIME (E6 BAND AFTER CORRECTION)

Slant iono. delay rate (E6)	**Confidence interval**	**Max. int. time**
0.4 cm/s	95 %	14.2 s
1.8 cm/s	99.9 %	3.3 s
5.2 cm/s	99.999 %	1.1 s

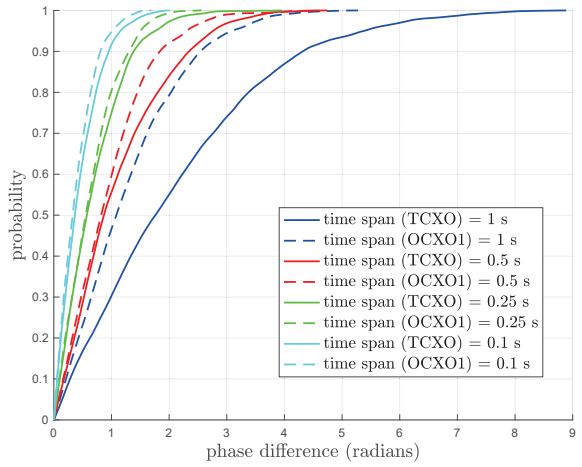

Fig. 3. Empirical CDF for the absolute phase difference (in radians) between two samples separated a given time span.

In any case, the correction in E6 based in E1 is still useful to reduce the uncertainty and, therefore, to reduce the number of frequency bins of the acquisition search space.

Regarding the phase noise, we are interested in evaluating how the phase change between the ECSs located in different periods, so this will determine if the sequences can be or not combined coherently. For this purpose, we compute the empirical Cumulative Distribution Function (CDF) for the absolute phase difference (in radians) between two samples separated a given time span. In Fig. 3 results are shown for common types of receiver clocks: Temperature-Controlled Crystal Oscillator (TCXO) and Oven-Controlled Crystal Oscillator (OCXO) [15].

The maximum coherent integration time will be mainly determined by the separation between the first and last sequences to be combined. As we can observe, for a quarter of the wavelength, which is the limit we consider to combine the sequences coherently, the maximum time span for an accumulated probability of 90% is around 250 ms for the TCXO case and around 500 ms for the OCXO case. Hence, the worst case (TCXO) implies using RECS periods of less than 100 ms to combine coherently 3 sequences, for example.

E. Samples storage

In the ACAS mode, the receiver needs to download and store the RECS files, which will determine its capacity to operate autonomously without relying on the server communication. However, the receiver must pre-record the required samples from the E6-C encrypted keystream corresponding to the time of authentication, which is related to the corresponding TESLA key for a given period. This will allow the receiver to perform the a-posteriori correlation between these samples and the corresponding ECS [10]. The number of pre-recorded samples will be determined by two parameters:

1) The length of the acquisition window, which will be approximately equal to the maximum uncertainty of the receiver clock offset (if case of no uncertainty, this will be approximately equal to the length of the ECS/RECS).
2) The RECS maximum random delay, since this parameter is only known when the RECS is decrypted with the disclosed OSNMA key, and therefore it must be considered by the receiver to locate the RECS in the E6-C keystream. Thus, it is recommended to keep this parameter as low as possible to avoid increasing the storage requirement of the receiver.

IV. Performance and Results

In this section, we evaluate the performance of the ACAS 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 [16]. For a given C/N_0, this performance is mainly determined by the length of the acquisition search space [17], which depends on two parameters, as detailed in Section III-B:

1) The length of the ECS, given by T_{RECS}.
2) The assumptions made by the user's receiver about the reception delay uncertainties, given by $\Delta\tau^{k}_{\max}$.

The RECS offset δ_{RECS} and RECS maximum random delay $\mathrm{D}\tau_{\max}$ are not considered, since they do not affect the search space size. The value of the RECS period τ_{RECS} is only specified when multiple integrations are performed, otherwise is chosen long enough to perform the correlation during the length of the ECS.

The results shown have been obtained using a custom-built ACAS simulator, based on MATLAB$^{\mathrm{TM}}$, that performs the acquisition using the well-know Parallel Code phase Search (PCS) acquisition method. In all the cases, a AWGN channel is considered, as well as a single satellite in view.

A. Impact of ECS length on the performance

To evaluate the impact of ECS length on the performance, the maximum uncertainty in the reception delay is set to the minimum previously considered, which is the length of the sequence to be correlated, i.e., $\Delta\tau_{\max} = T_{\mathrm{RECS}}$. Therefore, the length of the acquisition window, according to (6), is set to $T^{k}_{\mathrm{acq}} = 2T_{\mathrm{RECS}}$. The rest of the simulation parameters are assumed ideal, i.e., an infinite receiver bandwidth, doppler frequency perfectly estimated, and perfectly stable receiver clock (no phase noise).

Distinct C/N_0 scenarios have been simulated, ranging from 30 dBHz, which typically corresponds to a dense urban scenario, to 40 dBHz, which typically corresponds to an open sky scenario. The results obtained in Fig. 4, which averages 2000 Monte Carlo realisations, are summarised in Table III.

TABLE III
Minimum ECS length as function of C/N_0

$\mathbf{C/N_0}$	**Minimum ECS length**
40 dBHz	10240 chips ($\sim$ 2 ms)
35 dBHz	40960 chips ($\sim$ 8 ms)
30 dBHz	163840 chips ($\sim$ 32 ms)

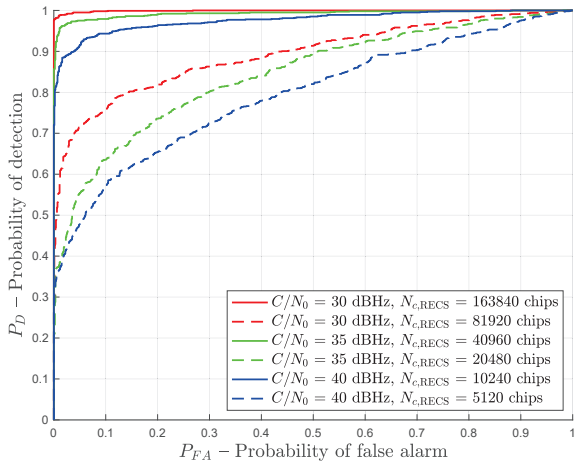

Fig. 4. ROC curves showing the impact of the ECS length, where $T^k_{\text{acq}} = 2T_{\text{RECS}}$.

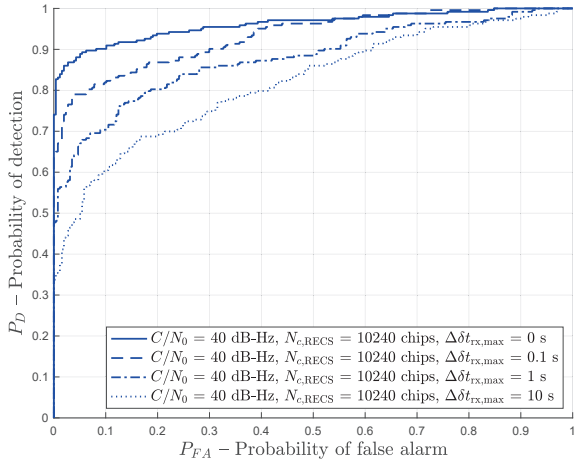

Fig. 5. ROC curve showing the impact of the reception delay uncertainty, where $T^k_{\text{acq}} = 20$ ms $+ \Delta\delta t_{\text{rx,max}} + T_{\text{RECS}}$.

B. Impact of reception delay uncertainty on the performance

As stated previously, the reception delay maximum uncertainty $\Delta\tau_{\max}$ depends on the uncertainty of three parameters: the receiver clock offset, the satellite clock offset and the propagation delay. The maximum uncertainties for the last two are bounded in practice, and so it is the value assumed for the receiver clock offset maximum uncertainty $\Delta\delta t_{\text{rx,max}}$ that mainly determines the impact of reception delay uncertainty on the performance.

In the simulations carried out, we consider $\Delta\delta t_{\text{sat,max}} = \Delta\delta t_{\text{prop,max}} = 10$ ms, and $\Delta\delta t_{\text{rx,max}}$ ranging from zero to several seconds, depending on the receiver clock calibration assumptions. Therefore, the length of the acquisition window, according to (6), is set to $T^k_{\text{acq}} = 20$ ms $+ \Delta\delta t_{\text{rx,max}} + T_{\text{RECS}}$. The rest of the simulation parameters are assumed ideal.

As shown in Fig. 5, which averages 500 Monte Carlo realisations, the degradation in terms of P_{D} for large uncertainties is very noticeable, even considering a relatively high C/N_0 of 40 dBHz. Indeed, since the RECS can be located in any position within the acquisition window, the search space of the CAF is increased, as it is the probability of false alarm, due basically by the increase of miss-detection probability. Given the sensitivity of the performance to this window, having trustable broadcast navigation, that bounds the satellite clock error and position (e.g. from NMA), can be advantageous.

V. Conclusion

This paper has analysed the impact on the acquisition performance of the parameters involved in the ACAS, currently under definition. Two main contributions have been made.

First, our analysis on the service implementation, in which we have determined the location of ECS to be correlated and the so-called acquisition window. We have shown that both the length of this sequence and the uncertainty assumed for the receiver clock offset are the main parameters to be considered at acquisition-level. We have established the minimum lengths for these sequences under ideal conditions for typical C/N_0 scenarios, and we have also shown that, as expected, large uncertainties have a significant degradation on the probability of detection. This uncertainty can be, however, reduced drastically if the satellite broadcast navigation is trustable, and even more, if the E1 PVT solution is considered trustable a priori.

Second, we have analysed the impact that the period between RECS has in the combination of multiple sequences. We show that, in practice, the length of this period is very limited for coherent integrations, otherwise non-coherent combinations are needed, but at the expenses of an increase in the time needed to compute the solution. More detailed simulations are being carried out to assess the sweet spot between the number of integrations and the length of this period.

These outcomes suggest that, on the one hand, working with large RECS may avoid the need to use multiple integrations and their drawbacks, since then the length of the RECS periods do not need to be restricted. A length of around 32 ms turns out to be enough for most scenarios where the ACAS is intended to operate (C/N_0 not lower than 30 dB). The downside of this approach is the increase in the size associated with the RECS and, consequently, the reduction in the autonomy of the user's receiver. At system level, this could be relieved by making different file sizes (for different RECS lengths) available on the server; the receiver would then download the more appropriate RECS file as function of its estimated C/N_0.

On the other hand, it is apparent that in order to search for the vestigial (non-faked) signal when the E1 is spoofed and its time reference cannot be trusted, the acquisition window length should be increased according to the receiver clock uncertainty, which leads to a significant degradation on the probability of detection. To keep this window to a minimum, an alternate approach could be to split it in shorter lengths and to look for the RECS of previous periods. At system level, this could be achieved by making available RECS files with different periods at the server.

References

[1] O. Pozzobon, L. Canzian, M. Danieletto, and A. D. Chiara, "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)*, 2010, pp. 1–6. DOI: 10.1109/NAVITEC.2010.5708065.

[2] P. F. MacDoran, M. B. Mathews, F. A. Ziel, *et al.*, *Method and apparatus for authenticating the location of remote users of networked computing systems*, May 1998.

[3] L. Scott, "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)*, 2003, pp. 1543–1552.

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

[5] M. L. Psiaki and T. E. Humphreys, "GNSS Spoofing and Detection," *Proceedings of the IEEE*, vol. 104, no. 6, pp. 1258–1270, 2016.

[6] I. Fernandez-Hernandez, G. Vecchione, and F. Díaz-Pulido, "Galileo authentication: A programme and policy perspective," in *69th International Astronautical Congress*, 2018.

[7] I. Fernandez-Hernandez, V. Rijmen, G. Seco-Granados, J. Simon, I. Rodríguez, and J. D. Calle, "A navigation message authentication proposal for the Galileo open service," *NAVIGATION, Journal of the Institute of Navigation*, vol. 63, no. 1, pp. 85–102, 2016.

[8] European Union Agency for the Space Programme (EUSPA), *OSNMA Public Observation Test Phase*. [Online]. Available: https://www.gsc-europa.eu/support-to-developers/osnma-public-observation-test-phase.

[9] P. Gutierrez, *Galileo Authentication and High-Accuracy Service: Coming on Fast*, Jul. 2021. [Online]. Available: https://insidegnss.com/galileo-authentication-and-high-accuracy-service-coming-on-fast/.

[10] European Commission, *Call for Tenders (DEFIS/2020/OP/0002) - Test Platform on Galileo HAS/CAS/OSNMA - Tender Specifications - Annex 7*, 2020. [Online]. Available: https://etendering.ted.europa.eu/cft/cft-display.html?cftId=6271.

[11] I. Fernandez-Hernandez, T. Walter, A. Neish, and C. O'Driscoll, "Independent time synchronization for resilient gnss receivers," in *Proceedings of the 2020 International Technical Meeting of The Institute of Navigation*, 2020, pp. 964–978.

[12] I. Fernandez-Hernandez, S. Cancela, R. Terris-Gallego, *et al.*, "Semi-Assisted Signal Authentication Based on Galileo ACAS," *arXiv preprint*, 2022.

[13] European Commission, *European GNSS (Galileo) Open Service – Signal-in-Space Interface Document v2.0*, Jan. 2021. [Online]. Available: https://www.gsc-europa.eu/sites/default/files/sites/all/files/Galileo_OS_SIS_ICD_v2.0.pdf.

[14] T. Walter, J. Blanch, L. De Groot, L. N. Novatel, and M. Joerger, "Ionospheric Rates of Change," in *Proceedings of the 31st International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2018)*, 2018.

[15] P. J. Teunissen and O. Montenbruck, *Handbook of Global Navigation Satellite Systems*. Springer, 2017.

[16] T. Fawcett, "ROC Graphs: Notes and Practical Considerations for Researchers," 2004.

[17] D. Borio, "A Statistical Theory for GNSS Signal Acquisition," Ph.D. dissertation, 2008.