engineering proceedings

MDPI

Proceeding Paper

Efficient Detection of Galileo ACAS Sequences using E6-B Aiding †

Rafael Terris-Gallego [1], Ignacio Fernandez-Hernandez [2], José A. López-Salcedo [1] and Gonzalo Seco-Granados [1,*]

[1] Department of Telecommunications and Systems Engineering, School of Engineering, Universitat Autònoma de Barcelona (UAB), IEEC-CERES, 08193 Bellaterra, Barcelona, Spain; rafael.terris@uab.cat (R.T.-G.); jose.salcedo@uab.cat (J.A.L.-S.), gonzalo.seco@uab.cat (G.S.-G.)
[2] Directorate-General for Defence Industry and Space (DG DEFIS), European Commission, 1049 Bruxelles/Brussel, Belgium; ignacio.fernandez-hernandez@ec.europa.eu (I.F.-H.)
* Correspondence: rafael.terris@uab.cat
† Presented at the European Navigation Conference 2024, Noordwijk, The Netherlands, 22 May–25 May 2024.

Abstract: Galileo Assisted Commercial Authentication Service (ACAS) is an assisted signal authentication capability under development by Galileo, designed to enhance robustness of the European Global Navigation Satellite System (GNSS) against malicious attacks like spoofing. It operates by providing information about some fragments of the unknown spreading codes in the E6-C signal. Unlike other approaches, ACAS uniquely employs Timed Efficient Stream Loss-tolerant Authentication (TESLA) keys provided by Open Service Navigation Message Authentication (OSNMA) in the E1-B signal for decryption, avoiding the need for key storage in potentially compromised receivers. The encrypted fragments are made available to the receivers before the broadcast of the E6-C signal, along with their broadcast time. However, if the receiver lacks an accurate time reference, searching for these fragments—which typically last for milliseconds and have periodicities extending to several seconds—can become impractical. In such cases, the probability of detection is severely diminished due to the excessively large search space that results. To mitigate this, initial estimates for the code phase delay and Doppler frequency can be obtained from the E1-B signal. Nevertheless, the alignment between E1-B and E6-C is not perfect, largely due to the intrinsic inter-frequency biases they exhibit. To mitigate this issue, we can leverage auxiliary signals like E6-B, processed by High Accuracy Service (HAS)-compatible receivers. This is a logical choice as E6-B shares the same carrier frequency as E6-C. This could help in obtaining more precise estimates of the location of the encrypted fragments and improving the probability of detection, resulting in enhanced robustness for the ACAS authentication process. This paper presents a comparison of uncertainties associated to the use of the E1-B and E6-B signals, based on real data samples obtained with an ACAS evaluation Software Defined Radio (SDR)-based platform. The results show the benefits of including E6-B in ACAS processing, with minimal implementation cost.

Keywords: GNSS; Galileo; ACAS; authentication; acquisition; snapshot; SDR; bladeRF; E6-B; E6-C

Citation: To be added by editorial staff during production.

Academic Editor: Firstname Lastname

Published: date

1 Introduction

Spoofing represents a significant concern within satellite navigation, as it can manipulate the location information of any GNSS receiver. The recent launch of OSNMA [1], provided free-of-charge by Galileo, has emerged as a pivotal development in this domain by offering authentication of the navigation message. To complement this encryption at data (symbol) level, Galileo is currently testing a new service known as ACAS, a proposal of CAS aimed at providing protection at signal (chip) level. For this purpose, ACAS is based on the E6-C Galileo signal, whose spreading codes are anticipated to be encrypted soon. Galileo ACAS is currently being renamed to Galileo SAS (Signal Authentication Service), but we will still refer to ACAS for the rest of this paper.

The operation of ACAS, detailed in [2], can be divided into two parts. From the system side, segments of the encrypted E6-C, called Encrypted Code Sequences (ECS), are re-encrypted using TESLA keys from OSNMA in the E1-B signal. These Re-Encrypted Code Sequences (RECSs), along with other information needed for PVT computation, are stored on a public server like the GNSS Service Center (GSC) before the Galileo signals are broadcast.

On the receiver side, the user downloads the necessary RECS files from the server to operate autonomously for a desired period. When the E6-C signal is broadcast, the receiver captures a snapshot around the expected ECS time, which can be determined from the RECS file headers. Once the TESLA key is released in the E1-B signal, it is used to decrypt the RECS and obtain the ECS, which serves as a local replica for correlating with the recorded E6 samples. If the ECS is detected during acquisition, the user can authenticate the received signal, given certain conditions are met [2]. Figure 1 shows receiver's side ACAS operation.

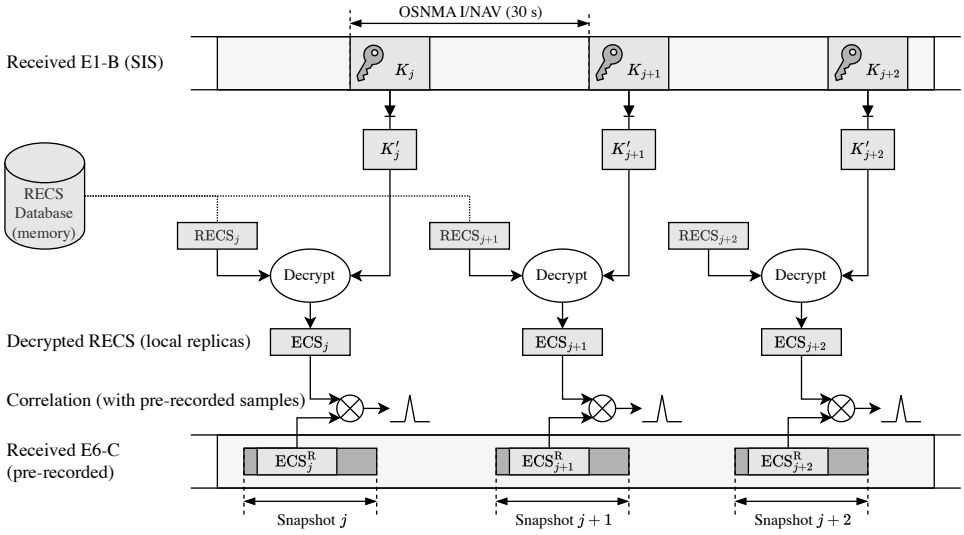


Figure 1. Illustration of ACAS operation: in this example, each TESLA key decrypts a single RECS, so the periodicity of the RECSs (and thus the ECSs) is 30 s, matching the duration of one I/NAV subframe. The superscript 'R' on the ECS indicates the received ECS, which is corrupted by noise, distinguishing it from the original ECS obtained by decrypting the downloaded RECS.

This approach facilitates the computation of an authenticated PVT without modifying Galileo's current signal plan or requiring the receiver to store any secret key [3]. However, as discussed in [4], providing only specific fragments of the E6-C signal to the receiver requires optimizing the detection of the ECS. Given the non-repeating nature of the encrypted E6-C signal, the search for a small fragment –RECS are expected to last only a few milliseconds– within large snapshots could result in poor detection capabilities.

Having an accurate time reference to align the broadcast time of the ECS/RECS with the samples recorded by the receiver allows for minimizing the snapshot size. Without such precision, the snapshot duration must be extended to account for time reference uncertainty [4]. To avoid reliance solely on the receiver clock, the nominal operating mode of ACAS is expected to use the E1-B signal to infer an accurate time reference, as this signal is already used to obtain the required TESLA keys. This can be achieved by using PVT computed from the E1-B signal or from the transmit GST contained in E1-B samples [5]. This method assumes the E1-B signal is trustable; however, in the event of a spoofing attack that compromises this assumption, additional safeguards must be considered, as analyzed in [6].

The E1-B signal is also employed in the proposed ACAS authentication process proposed [2]. This mechanism uses the trusted ranging signal (E6-C) as an anchor for another signal from the same satellite (E1-B for the ACAS nominal mode). If the difference between the measurements to the anchor and the other signal falls below a predefined threshold, an unauthenticated measurement may be deemed trustworthy and usable for PVT [7].

However, the alignment between the E1-B and E6-C components is not perfect, primarily due to inter-frequency biases. Consequently, using the E6-B signal instead of, or in addition to, the E1-B signal for ACAS could help to reduce the authentication threshold and yield more precise estimates. This aspect is further analyzed in Section 2.

Nevertheless, the use of E6 extends beyond refining the authentication process. It could also be used to obtain a sufficiently accurate time reference using the E6 snapshot recorded by the receiver, provided that the required TESLA keys for decrypting the RECS can be accessed through an alternative channel (e.g., a remote server). This approach would permit the avoidance of processing the E1-B signal, enabling the use of simpler, single-frequency receivers for ACAS. The E6-B assisted snapshot mode for ACAS is analyzed in Section 3.

The results that support the preceding analysis are detailed in Section 4, using real data snapshots acquired via a custom-built evaluation platform for ACAS, which is described in [8]. Finally, the paper's conclusions are presented in Section 5.

2 Detecting Galileo ACAS Sequences Using Handover from E6-B

The non-repeating nature of E6-C has important implications for the receiver. Without further assistance, the acquisition search space could be prohibitively large. This is why, in ACAS, the use of an auxiliary signal is assumed, which helps to reduce this search space. The natural choice for this auxiliary signal is the E1-B component, as it is the signal that provides the TESLA keys required for the RECS decryption. Indeed, the ACAS specification outlines the corresponding E1-E6 BGD files, which are made available at the GSC along with the companion RECS files. These resources that can be effectively leveraged by the receiver.

Therefore, in a nominal ACAS operation, the receiver would take advantage of the measurements provided by E1-B –specifically, the code phase delay and the Doppler frequency, denoted τ_{E1B} and f_{E1B}, respectively– to derive the measurements estimates for E6-C, denoted $\hat{\tau}_{\mathrm{E6C\text{-}E1B}}$ and $\hat{f}_{\mathrm{E6C\text{-}E1B}}$, respectively. These estimates can be obtained by adding the corresponding offsets between E1-B and E6-C signals:

$$\hat{\tau}_{\mathrm{E6C\text{-}E1B}} = \tau_{\mathrm{E1B}} + \hat{\delta}_{\mathrm{E6C\text{-}E1B}} \tag{1}$$

$$\hat{f}_{\mathrm{E6C\text{-}E1B}} = f_{\mathrm{E1B}} + \widehat{\Delta f}_{\mathrm{E6C\text{-}E1B}} \tag{2}$$

The difference in Doppler frequency measurements between the two bands is mainly determined by the ratio of their carrier frequencies, denoted $f_{c,i}$ for the i-th band [4]:

$$\widehat{\Delta f}_{\mathrm{E6C\text{-}E1B}} = f_{\mathrm{E1B}}\left(\frac{f_{c,\mathrm{E6}}}{f_{c,\mathrm{E1}}} - 1\right) \tag{3}$$

The offset in code phase measurements between the two bands has three main contributors: satellites bias or Broadcast Group Delay (BGD), ionospheric effect, and hardware bias, denoted $\hat{\delta}^{\mathrm{BGD}}_{\mathrm{E6C\text{-}E1B}}$, $\hat{\delta}^{\mathrm{iono}}_{\mathrm{E6C\text{-}E1B}}$ and $\hat{\delta}^{\mathrm{HWB}}_{\mathrm{E6C\text{-}E1B}}$, respectively. Such offset can be expressed as [2]:

$$\hat{\delta}_{\mathrm{E6C\text{-}E1B}} = \hat{\delta}^{\mathrm{BGD}}_{\mathrm{E6C\text{-}E1B}} + \hat{\delta}^{\mathrm{iono}}_{\mathrm{E6C\text{-}E1B}} + \hat{\delta}^{\mathrm{HWB}}_{\mathrm{E6C\text{-}E1B}} \tag{4}$$

Notably, the ionosphere also affects frequency estimation, as specified in (3), but this impact depends on the rate of change of TEC over time, not its absolute value [4].

In an ideal scenario, transitioning from the E1-B to the E6-C would provide to the receiver the exact location of the $\mathrm{ECS}^{\mathrm{R}}$ in the recorded snapshot. However, in practice, due to the ionospheric and multipath effects, in addition to the potential errors in the previous estimates, the receiver must account for an uncertainty. This will define the search space for the Cross Ambiguity Function (CAF) during the acquisition. The number of search cells will be the product of the cells needed for both the code phase delay and Doppler frequency.

Nevertheless, the Doppler search can generally be avoided, and using the Doppler bin provided by the E1-B measurement should suffice. This results in computing only a limited number of cells in the time domain due to code phase delay uncertainty, denoted $\Delta\tau_{\mathrm{max}}$. An example is shown in Figure 2 for the case of the code phase delay measurements.

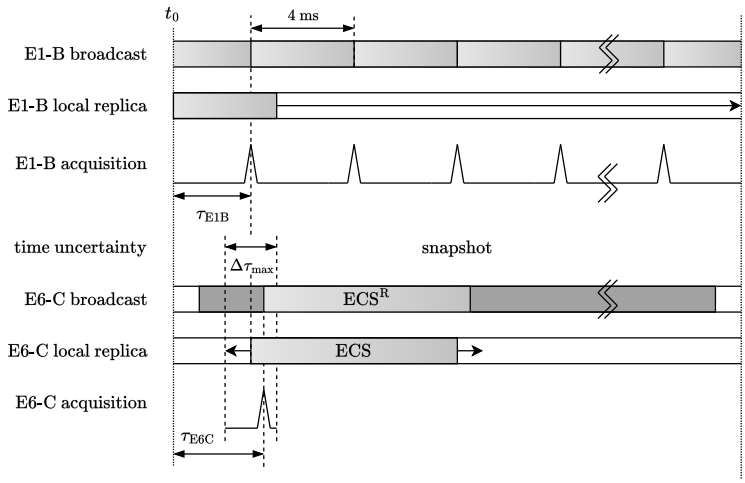


Figure 2. Measuring the code phase in E6-C using handover from E1-B measurement. The instant t_0 indicates an arbitrarily initial time used by the receiver for computing the delays.

Using the E6-B component as the auxiliary signal further reduces the uncertainty associated with E6-C measurements. This does not require additional hardware within the receiver, as E6-B shares the same frequency as E6-C. The main advantage of using E6-B over E1-B is that a handover from E6-B does not involve any inter-frequency biases, leading to more precise estimates, particularly in relation to the ionosphere contributions. This is depicted in Figure 3. Indeed, the term $\Delta f_{\max,E6C-E6B}$ can be neglected in practice, as differences, if any, are likely only due to different processing of different of the E6-C and E6-B.

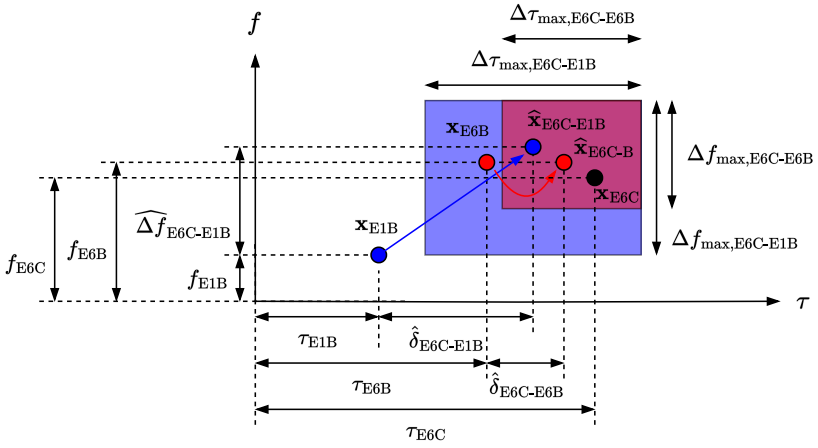


Figure 3. Estimating E6-C code phase and Doppler frequency from E1-B and E6-B estimates. The figure is not to scale and $\mathbf{x}_i = (\tau_i, f_i)$ represents the code phase delay and Doppler frequency bins used for acquisition. In practice, searching in the frequency dimension may be unnecessary.

The accuracy of these estimates has a direct impact on the authentication mechanism used in the nominal operating mode of ACAS. Specifically, the measurement is considered authenticated only if the difference between the code phase delay measured on E6-C and the code phase delay estimated for E6-C from E1-B is lower than a predefined threshold, denoted γ_{auth} [2]. The same applies for the code phase estimated from E6-B:

$$|\tau_{E6C} - \hat{\tau}_{E6C\text{-}E1B}| \leq \gamma_{\text{auth}} \rightarrow \text{measurement authenticated} \quad (5)$$

$$|\tau_{E6C} - \hat{\tau}_{E6C\text{-}E6B}| \leq \gamma'_{\text{auth}} \rightarrow \text{measurement authenticated} \quad (6)$$

Since the threshold depends on the characterization of the error contributions in the estimation process, it becomes evident that using an estimate of E6-C from E6-B could

facilitate a reduction in the threshold ($\gamma'_{\text{auth}} \leq \gamma_{\text{auth}}$) , thereby enhancing the authentication mechanism. A comparison of the code phase delays estimated from E1-B and E6-B is presented in Section 4. The results provided corroborate the analysis discussed previously.

3 Snapshot Positioning using E6-B

The main goal of ACAS is to authenticate the PVT, but the specific method of obtaining this PVT will vary depending on the receiver's implementation. In the nominal operating mode of ACAS, the E1-B signal can be used to obtain the PVT, which could subsequently be authenticated with E6-C if the corresponding ECS is found where expected. Such an approach could yield high accuracy in position determination, as the receiver will be tracking the E1-B signal. However, this method requires the use of dual-frequency receivers that process both E1-B and E6-C signals and account for the inter-frequency biases between them to accurately estimate the code phase delay and Doppler frequency, as discussed in Section 2.

However, single-frequency ACAS receivers can be considered if the E6-B signal is used instead of E1-B. In this approach, it is assumed that the TESLA keys required to decrypt the RECS are provided through alternative means (i.e., remote server) rather than through processing E1-B. With this setup, the receiver could rely on the snapshot of E6 samples it records to compute the PVT, as this snapshot would contain both E6-B and E6-C components.

Snapshot positioning entails certain nuances compared to the conventional "acquisition & tracking" approach, such as peak interpolation and block-wise implementation. For more details, see Chapter 9 of [9]. The accuracy of the PVT derived from the snapshot largely depends on the snapshot size and the carrier bandwidth, which, for E6-B, is substantial – approximately 10 MHz two-sided bandwidth for the main lobe.

3.1 E6 Snapshot Size

The size of the E6 snapshot is critical for the accuracy of snapshot-based positioning in ACAS. This size is mainly influenced by two factors: the RECS configuration and the accuracy of the time reference available at the receiver. According to the latest ACAS specification [10], RECS parameters affecting snapshot size include the number of satellites being tracked and the chosen randomization settings. Since RECS are provided per satellite, more satellites require a larger snapshot size to account for variations in propagation delays and satellite clock offsets. For Galileo, propagation delays span about 20 ms. Depending on randomization parameters, the ECS may be transmitted at the specified broadcast time or delayed by a few milliseconds. Considering these factors, snapshot sizes typically range from 25 to 150 ms. Table 1 illustrates snapshot sizes for various ACAS configurations.

Table 1 Examples of snapshots sizes for different ACAS configurations. The definition of the parameters RAND and KDI can be found in the latest ACAS specification published (v1.2) [10].

RECS length	RAND	KDI	Snapshot length
4 ms	0	0	~ 25 ms
4 ms	0	2	~ 50 ms
16 ms	1	0	~ 100 ms
16 ms	1	2	~ 150 ms

3.2 Comparison of E1-B tracking with E6-B snapshot acquisition accuracy

Depending on receiver processing, the accuracy from the limited E6-B snapshot samples may be lower than that from continuous E1-B signal tracking. However, from an ACAS perspective, the accuracy provided by E6-B snapshot acquisition may be sufficient for many applications, where an authenticated solution is more important than precise PVT.

Next, we provide a preliminary analysis of the expected accuracies from both approaches. For continuous tracking of the E1-B signal, we refer to the simplified model in (7). The selected parameters are typical for a conventional commercial receiver: 0.1 chips for

early-late spacing, 40 dB-Hz of C/N_0, and 1 Hz for DLL bandwidth (see Chapter 4 of [9]). The K factor measures the sharpness of the correlation curve relative to a Binary Pulse Shift Keying (BPSK) signal. For Binary Offset Carrier (BOC) (1,1) processing of E1-B, this factor is 3. The chip period T_c is about 1 μs for E1-B [11], with c representing the speed of light. A refined model is discussed in Chapter 5 of [12], which offers a general expression for the thermal noise code tracking jitter for a noncoherent Delay Lock Loop (DLL) discriminator.

$$\sigma_{\mathrm{DLL}} \approx cT_c \sqrt{\frac{B_{\mathrm{DLL}}\, d_{\mathrm{E-L}}}{2\, K\, C/N_0}} \approx 0.5 \ \ [\mathrm{m}] \tag{7}$$

For snapshot acquisition on E6-B, the Cramer-Rao Lower Bound (CRLB) for time delay estimation can be applied (see Chapter 3 of [13]). This sets a lower bound for the variance of time delay using Maximum Likelihood Estimation (MLE), which is equivalent to the estimation of the code phase delay by comparing the received signal with all possible delay values during the receiver's acquisition stage. This bound depends on the Signal-to-Noise (SNR) ratio at the correlators output, given by the $\mathrm{C/N_0}$, the coherent integration time used for the correlation (T_{int}), and the quadratic mean square bandwidth (Gabor or Mean Square bandwidth, B_{ms}). Thus, the ranging accuracy for snapshot positioning can be expressed as:

$$\sigma_{\mathrm{snp}} \geq c \sqrt{\frac{1}{2\, C/N_0\ T_{\mathrm{int}}\, B_{\mathrm{ms}}}} \ \ [\mathrm{m}] \tag{8}$$

Alternative approaches can be considered to derive specific expressions of the CRLB for the GNSS signals (see Appendix D of [14]). Table 2 shows the achievable accuracies for different combinations of snapshot sizes and C/N_0's ratios, assuming 10 MHz receiver bandwidth that enables the capture of the entire main lobe of the E6-B signal spectrum.

Table 2 Maximum code phase delay accuracies attainable for various E6 snapshot sizes.

Snapshot size	$\mathbf{C/N_0}$	**Accuracy (σ_{snp})**
25 ms	45 dB-Hz	0,7 m
25 ms	40 dB-Hz	1,3 m
50 ms	40 dB-Hz	0,9 m
100 ms	40 dB-Hz	0,6 m
100 ms	35 dB-Hz	1,1 m
150 ms	35 dB-Hz	0,9 m

In the absence of data symbols, non-coherent integration is required for E6-B, resulting in some square losses compared to coherent integration. However, these losses are negligible for the C/N_0 values in this analysis and primarily affect indoor scenarios. Nonetheless, the accuracy remains comparable to that of a DLL, mainly due to the high Gabor bandwidth of the E6-B signal.

4 Results

4.1 Evaluation Platform and Test Samples

To support the theoretical analysis presented in previous sections, we next provide results using real data samples obtained with a custom-built evaluation platform designed specifically for ACAS. This platform employs bladeRF Software-Defined Radio (SDR) boards from Nuand, which meet the specifications necessary to evaluate the ACAS performance. A comprehensive description of this platform can be found in [8]. The real datasets used in this study comprises two snapshots of samples (E1+E6) recorded synchronously with the evaluation platform. The recording spot was a rural area located near Girona, Spain, at a latitude of 41°59′35″ N (41.9932) and a longitude of 2°47′43″ E (2.7954). Two datasets are used in this paper, as shown in Table 3.

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

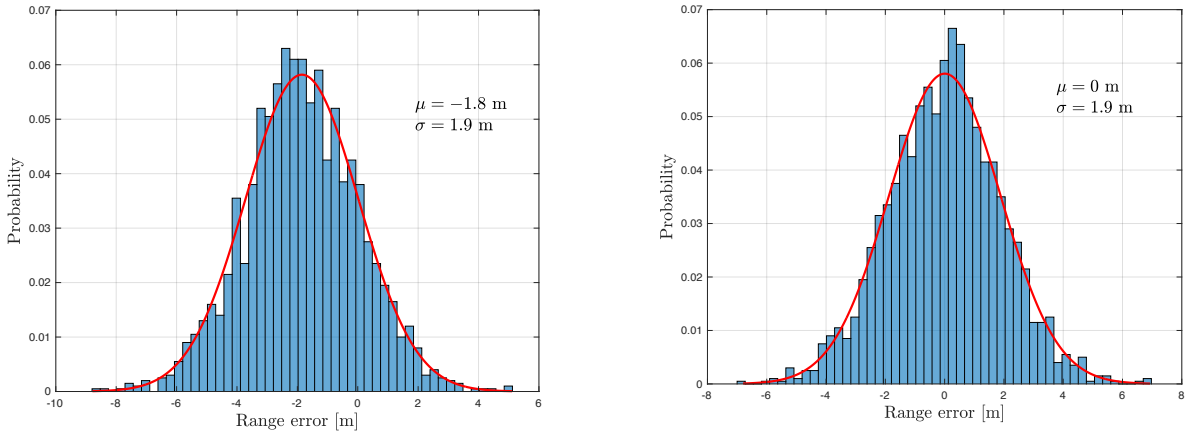
Dataset ID	Recording Date/Time	Duration	Sampling rate
D1	2023-02-20 16:54 (GMT)	10 seconds	60 MHz
D2	2023-04-14 14:21 (GMT)	3.2 seconds	20 MHz

4.2 E6-C vs E6-B Code Phase Delay Comparison

The initial results analyze the alignment of code phase delays, which is crucial for the ACAS nominal operating mode. This alignment reduces the acquisition search space and affects the authentication process. The dataset used (D1) was collected in a clear-sky scenario with an estimated C/N_0 of at least 45 dB-Hz. Snapshots from the SDR platform are processed with a custom MATLAB simulator to obtain estimates for E6-C and the auxiliary signal (E1-B or E6-B). The snapshots are segmented into smaller chunks for individual processing, where acquisition is performed for the required RECS length to obtain code phase delay and Doppler frequency estimates. These estimates are averaged for statistical analysis. Here, 10-second snapshots are divided into 2000 chunks of 4 ms each.

Since the E6-C signal is currently broadcast unencrypted, the dataset snapshots capture the existing periodic pilot open signal, which consists of 1-ms primary spreading codes tiered with a known 100-symbol, 1-ms secondary code [15]. Therefore, it is necessary to emulate the RECS. This is done by first acquiring the secondary code on E6-C to determine the Secondary Code Index (SCI) for each satellite. Then, a conventional acquisition method is used, coherently integrating the required 1-ms primary spreading codes to obtain the desired RECS length, set to 4 ms, which has been shown to provide high detection probabilities in most clear-sky scenarios [16].

The results are shown in Figure 4, showing the code phase delay differences between E6-C and E1-B (a) and between E6-C and E6-B (b). As expected, the distributions exhibit a Gaussian-like shape, with variance related to the sample's thermal noise. For E6-C vs. E1-B, the Gaussian is non-centered due to inter-frequency biases, while for E6-C vs. E6-B, there is no bias. A Gaussian curve (in red) is fitted to the experimental data (in blue) to interpolate the mean and standard deviation for each case.



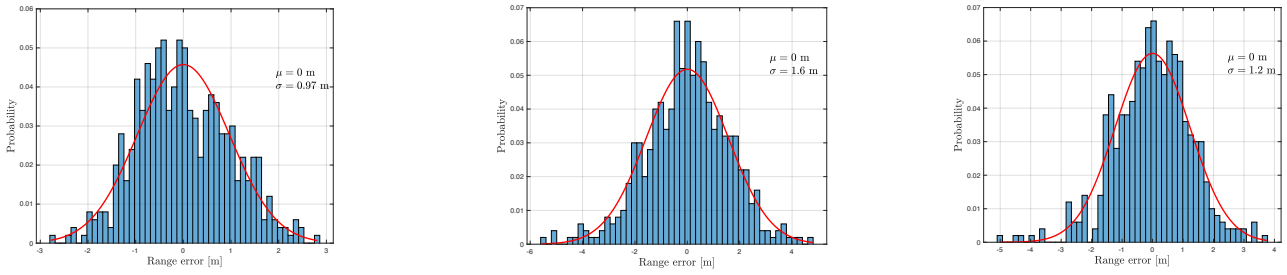
(**a**) (**b**)

Figure 4. Histograms of the code phase delay difference between E6-C and the auxiliary signal using dataset D. (**a**) E1-B vs E6-C; (**b**) E6-B vs E6-C.

4.3 E6-B Snapshot Code Phase Delay Estimation

The subsequent results focus on estimating the ranging accuracy from processing snapshots of E6-B samples. The dataset used (D2) was recorded under clear-sky conditions with the antenna covered by concrete blocks to simulate different C/N_0 levels. As in Section 4.2, the snapshots are processed with a custom MATLAB simulator, but, in this case, they are divided into smaller segments of the required sizes, as shown in Table 2.

For each segmented snapshot, the code phase delay is estimated. As expected, owing to the Doppler frequency effect, the code phase delay estimates exhibit a linear trend over time. This trend line is subtracted from the estimates to obtain an estimation of the ranging accuracy by estimating the standard deviation of the interpolated Gaussian distribution.



(**a**) (**b**) (c)

Figure 5. Code phase delay estimates histograms, after removing the trend line, using E6-B snapshots of different lengths and C/N_0's. (**a**) 25 ms, 45 dBHz; (**b**) 25 ms, 40 dBHz; (**c**) 50 ms, 40 dBHz.

The results are shown in Figure 5. The standard deviations estimated for ranging accuracy are consistent with the CRLBs in Table 2. The slight discrepancies may arise to factors like non-ideal filters in the SDRs or the method used to estimate of ranging accuracy, achieved by removing the trend line from the code phase delay estimates, which may not precisely reflect the disparity between the estimated and true measurements.

5 Conclusions

Galileo ACAS offers an effective method for authenticating ranging signals by encrypting the E6-C signal. A key feature is the use of an auxiliary signal to speed up RECS detection, crucial for ACAS's nominal operation. While the E1-B signal remains the default choice, adding signals like E6-B could enhance future ACAS receivers' robustness without adding significant complexity. The E6-B signal, already present in the samples that receivers must record, also avoids inter-frequency biases, offering a way to improve ACAS authentication.

The results of this study, based on real data samples, highlight the advantages of using E6-B for ACAS as an additional verification layer and for receivers relying solely on the E6 signal, provided TESLA keys are accessible through alternative channels instead of the E1-B signal. E6-B could also aid Vestigial Signal Search (VSS) techniques crucial for detecting spoofed signals during attacks. Further research is needed to explore the potential benefits of integrating E6-B, ensuring ACAS remains secure and reliable against evolving threats.

Author Contributions: Software, validation, writing—original draft preparation, R.T.-G.; supervision, writing—review and editing, I.F.-H., J.A.L.-S. and G.S.-G. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported, in part, by the European Commission Defence Industry and Space Satellite Navigation (DEFIS) contracts DEFIS/2020/OP/0002 and DEFIS/2023/OP/0011, and, in part, by the Spanish Agency of Research project PID2020-118984GB-I00 and by the Catalan ICREA Academia Program.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The datasets recorded with the SDR platform used in this paper can be downloaded from https://spcomnav.uab.es/resources/acas_datasets (accessed on 1 May 2024).

Acknowledgments: The authors would like to thank J. Winkel and C. O'Driscoll, involved in the definition of Galileo ACAS, for their discussions and contributions.

Conflicts of Interest: The authors declare no conflict of interest.

References

[1] 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.

[2] I. Fernandez-Hernandez *et al.*, "Semiassisted Signal Authentication for Galileo: Proof of Concept and Results," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 59, no. 4393–4404, Aug. 2023.

[3] I. Fernandez-Hernandez *et al.*, "Galileo Authentication and High Accuracy: Getting to the Truth," *Inside GNSS*, Feb. 13, 2023. Accessed: Mar. 02, 2023. [Online]. Available: https://insidegnss.com/galileo-authentication-and-high-accuracy-getting-to-the-truth/

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

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

[6] J. Winkel, I. Fernandez-Hernandez, and C. O'Driscoll, "Implementation Considerations for ACAS and Simulation Results," *ArxiV Preprint*, Jul. 2023, [Online]. Available: http://arxiv.org/abs/2307.12398

[7] F. Ardizzon, G. Caparra, I. Fernandez-Hernandez, and C. O'Driscoll, "A Blueprint for Multi-Frequency and Multi-Constellation PVT Assurance," in *NAVITEC*, Apr. 2022.

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

[9] K. Borre, I. Fernandez-Hernandez, J. A. López-Salcedo, H. Bhuiyan, and M. Zahidul, *GNSS Software Receivers*. Cambridge University Press, 2023. doi: 10.1017/9781108934176.

[10] European Commission – DG DEFIS, "Galileo Assisted Commercial Authentication Service (ACAS) – Specification Proposal v1.2," 2023.

[11] European Union, "Galileo Open Service Signal in Space Interface Control Document (OS SIS ICD) – Issue 2.1," Nov. 2023. doi: 10.2878/39727.

[12] E. Kaplan and C. Hegarty, *Understanding GPS - Principles and Applications*, 2nd ed. 2006.

[13] S. M. Kay, *Fundamentals of statistical signal processing: estimation theory*. Prentice-Hall, Inc., 1993.

[14] N. B. Delgado, "Signal Processing Techniques in Modern Multi-Constellation GNSS Receivers," Lisbon, Portugal, 2011. doi: 10.13140/RG.2.1.2739.4165.

[15] European Union, "Galileo E6-B/C Codes Technical Note," Jan. 2019. Accessed: Mar. 14, 2022. [Online]. Available: https://www.gsc-europa.eu/sites/default/files/sites/all/files/E6BC_SIS_Technical_Note.pdf

[16] R. Terris-Gallego, J. A. López-Salcedo, G. Seco-Granados, and I. Fernandez-Hernandez, "Preliminary Evaluation of Galileo ACAS using Existing E1-E6 Open Signals and a Low-Cost SDR Platform," in *Institute of Navigation Conference (ION+ GNSS 2023)*, Denver, Sep. 2023.