engineering proceedings

MDPI

Proceeding Paper

S-TrackS: A Secure Snapshot-Based Solution for Positioning and Timing †

Aram Vroom, Tom van den Oever, Joaquín Gañez Fernandez, Nick van der Hijden, Alexandra Zevenbergen * and Bas van der Hoeven

CGI Nederland B.V., 3068 Rotterdam, The Netherlands
* Correspondence: alexandra.zevenbergen@cgi.com
† Presented at the European Navigation Conference 2023, Noordwijk, The Netherlands, 31 May–2 June 2023.

Abstract: With the large-scale usage of satellite navigation, spoofing and jamming are considerable threats to civilian society. Recent developments, such as Galileo's Open Service Navigation Message Authentication and GPS's Chimera, mitigate these risks. However, they provide authentication of the navigation message or ranging code, but not a true position in the case of interference. In critical applications, a protected navigation service is desired, such as Galileo's Public Regulated Service (PRS). PRS provides an access-controlled navigation service for authorized governmental users, with fully encrypted ranging codes and data channels, providing users with higher robustness against interference. The main challenge of implementing PRS on a large scale is the need to protect the cryptographic material that is required to access the PRS signals inside the receiver. For many applications, a stand-alone receiver solution is unnecessary. These applications could use a remote server for PRS. In this methodology, the end-user device has only a radio frequency front-end which sends short samples to a secure server. The (classified) signal processing is then carried out on this secure server, removing the need for the user device to protect cryptographic material. Besides decreasing the device's security requirements and power consumption, it also allows to utilize the advantages of PRS in applications that would otherwise not be able to use PRS. In this approach the PRS usage authorization would only be required for the server operations, and not for the end-user devices. It furthermore allows for using additional processing power for unaided PRS acquisition in case of interference. Within the Netherlands, a remote server solution is developed by CGI: S-TrackS, making PRS accessible. In this paper, the application of PRS and architecture for various use cases is presented. It is shown that PRS usage based on a remote server is feasible and can increase the robustness for governmental applications.

Keywords: GNSS; satellite navigation; Galileo; spoofing; jamming; snapshot positioning; encrypted signals; Public Regulated Service; authentication

Citation: Vroom, A.; van den Oever, T.; Gañez Fernandez, J.; van der Hijden, N.; Zevenbergen, A.; van der Hoeven, B. S-TrackS: A Secure Snapshot-Based Solution for Positioning and Timing. *Eng. Proc.* **2023**, *54*, 31. https://doi.org/10.3390/ENC2023-15457

Academic Editors: Tom Willems and Okko Bleeker

Published: 29 October 2023

1. Introduction

Since the development of GPS, GNSS receivers have been integrated in many aspects of modern day society. Satellite signals are used to determine position, velocity, and time (PVT) solutions, which are subsequently used to, for example, position ships, land aircraft, monitor remote assets, and synchronize system clocks. Society is therefore dependent on safe and robust GNSS signals.

Although GNSS receivers provide many benefits, the signals used for navigation are extremely weak, namely −128.5 dBm and −127.25 dBm for GPS L1 C/A and Galileo E1BC, respectively [1,2]. Consequently, a small jammer with a signal power of 10 dBm can disrupt PVT determination over a multi-km area. The disruption of a jammer can be noticed by the lack of proper PVT determination. Alternatively, a spoofer can overpower and falsify the satellite signals, convincing a receiver of a false position and/or time.

Galileo's Open Service Navigation Message Authentication [3] and GPS's Chimera mitigate some risks related to spoofing. They provide authentication of the navigation message or ranging code, but not a true position in the case of interference. In applications where continuity of service is critical, a protected navigation service is desired, such as Galileo's Public Regulated Service (PRS). PRS provides an access-controlled navigation service for authorized governmental users [4], with fully encrypted ranging codes and data channels. Hence, it is not possible for an attacker to spoof PRS, as the encrypted ranging codes and navigation data cannot be reproduced without the required cryptographic information. In addition, PRS is transmitted over a wider bandwidth compared to the public GPS and Galileo signals, increasing its resilience against jamming.

The challenge of utilizing PRS is that a stand-alone receiver will contain classified cryptographic information, which means that the receiver needs to adhere to strict security requirements. In order to mitigate this burden, a server-assisted PRS solution is proposed, where short RF recordings or snapshots are captured and processed on a secure server. Authorized use cases can therefore make use of the server-assisted PRS positioning service, without the need for hosting classified information in the user equipment. These PRS position–time solutions can then be used to authenticate the Open Service (OS) positions, and provide a true solution in case of spoofing or jamming. In this context, CGI Nederland B.V. developed S-TrackS [5], a snapshot-based authentication service based on the server-assisted PRS concept.

In this paper, the concept of snapshot processing techniques is introduced, together with the architecture of S-TrackS. Following, the test setup for a demonstration with S-TrackS is described. Finally, the results of a test campaign are shared, assessing the accuracy, the performance of the authentication service and the impact of metadata errors.

2. Snapshot Processing Techniques

In conventional GNSS receivers, both the radio frequency (RF) data collection and processing stages are carried out on the device. Conversely, novel techniques allow the separation of the processing stage from the user device. For instance, a Software-Defined Radio (SDR) can be used to collect the GNSS signals, which can be remotely post-processed to find a position–time solution.

The main disadvantage of the separated approach is that the file size of the RF recordings can be prohibitive for practical use since they can easily reach sizes of several gigabytes per recorded minute. Hence, techniques are developed to minimize the required recording time to find a position–time solution. If the ephemeris data are externally provided, it will not be necessary to decode the navigation message. By doing so, the total length of the recording can be reduced to well below 100 ms. These short recordings are called snapshots and contain a short snippet of the RF signals, which is used to find a single position–time solution.

Snapshot-based navigation offers the following main advantages:

1. The user device only needs to be enabled for the recording duration. If a use case requires one snapshot per minute, the duty cycle of the device can be reduced.
2. The full spectrum is available, enabling a wide variety of post-processing options, such as the analysis of interference.
3. The separation between user device and processing allows for the decryption of classified signals in a secure area, as utilized in the server-assisted PRS approach. Therefore, the security requirements of the user device are relaxed.
4. The server on which the application runs can have more processing power than a GNSS receiver. This enables more computationally intensive calculations and algorithms.

S-TrackS is CGI Nederland B.V.'s server-assisted PRS authentication service. For authorized use-cases, snapshots are processed in order to authenticate position–time solutions, detect spoofing and resolve the true position–time based on PRS. An overview of S-TrackS can be seen in Figure 1.

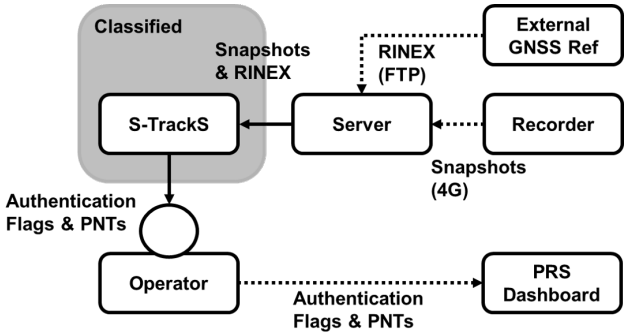


Figure 1. Overview of S-TrackS displaying the separated processing architecture [6].

An RF recorder can be used by a user in the field. For this purpose, prototype S-TrackS recorders are developed. S-TrackS is developed using open standards for RF recordings and is compatible with the ION GNSS-Metadata standard for Software-Defined Radio receivers [7]. Users of S-TrackS therefore have the possibility to utilize third party RF recording equipment and require no specific hardware from CGI Nederland B.V. The current S-TrackS recorder needs to be operated by a user, but commercially available RF front ends can be integrated in an existing track and trace chain. The collection of snapshots can then automatically be triggered based on events or timers.

The snapshots are automatically forwarded to a server through a REST API. The server then collects the snapshots and a RINEX navigation file from an external server. Within the classified environment, the snapshots are processed by S-TrackS, which includes the required infrastructure and classified information to process PRS.

Finally, the results can be inspected by an operator, and depending on the use case, shared with users through the PRS dashboard or interface of the user.

The architecture of S-TrackS is displayed in Figure 2.

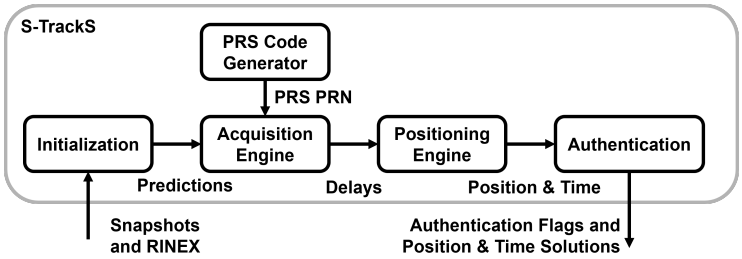


Figure 2. Architecture of S-TrackS.

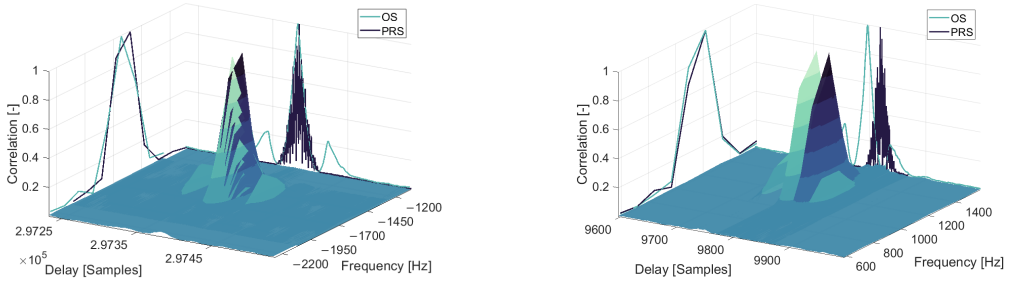
The following building blocks can be identified:

- Initialization. During the initialization, the coarse position–time data from the metadata file are used together with a RINEX navigation file to predict the visible satellites and their Doppler frequencies. The metadata file also contains information on the recording configuration such as bit depth, sampling rate, bandwidth, and number of channels.
- Acquisition Engine. The acquisition engine searches for the transmitted signals. Here, the parallel code–phase search technique is used. As there is no tracking loop involved, it is important that the code delay and Doppler frequency found by the acquisition engine are refined. The acquisition engine supports the following open signals: Galileo E1BC, Galileo E6BC and GPS L1 C/A. It furthermore supports the encrypted Galileo E1A and E6A PRS signals.
- Positioning Engine. Pseudoranges are generated based on the code delays for each acquired signal in the acquisition engine. These are then used to find the position–time solutions for the various signals. Without tracking, the time of week (TOW) from the navigation message cannot be used to construct the pseudorange. Hence,

the number of integer PRN codes between the satellite and receiver is unknown. To solve this, coarse time navigation and millisecond integer ambiguity fixing have been implemented. The latter of these works by choosing a reference satellite and computing the integer number of PRN codes for the other satellites based on this [8].

- Authentication. The position–time authentication is performed based on both the acquired signals and the found position–time solutions. This authentication is performed on two levels. Firstly, it is carried out by comparing the delay for each acquired Galileo OS and PRS signal. Secondly, the obtained public position–time are compared to the PRS position–time and their differences are determined. Authentication is then based on whether these differences are within the configured thresholds.

An example of a successful authentication and spoofing detection based on a delay between the Galileo OS and PRS signals can be seen in Figure 3.



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

Figure 3. Authenticated (**a**) and spoofed (**b**) correlation peaks. (**a**) Authenticated correlation peak, with overlapping PRS and OS delays. (**b**) Spoofed correlation peak, with an offset between PRS and OS delays.

Once the processing has completed, S-TrackS returns a result string containing the authentication flag for the specific snapshot and a true position–time based on Galileo PRS. These results can be:

- Authenticated. This flag is returned if the Galileo PRS results matches the Galileo OS results and all position–time solutions match within set thresholds.
- Spoofed. This flag is returned if the PRS delays do not match the OS delays, or the position–time solutions do not match within set thresholds.
- Warning. This flag is returned if the PRS component is missing and no comparison can therefore be made.

3. Test Setup and Data Collection

In order to demonstrate S-TrackS as a position–time authentication service, a test campaign is carried out. The objective is to demonstrate S-TrackS' capability to authenticate the public signals and resolve PRS positions. Therefore, snapshots are statically collected under various spoofing conditions.

One hour of clean RF data are recorded using the Labsat3 Wideband with the Ardusimple ANT3B survey antenna, capturing both the OS and PRS signals in the E1 and E6 bands. The IQ data are captured using 2 bits of quantization and 58 MHz sampling rate.

The test data are collected in the Prinsenpark near the CGI Nederland B.V. Rotterdam office (51°55′56.7″ N, 4°32′57.9″ E). This is an open environment without any obstructions.

3.1. Nominal Scenario

First, a set of nominal snapshots is recorded. Here, the RF data collected with the Labsat is directly replayed and recorded with the S-TrackS recorder. The recorder is configured to capture the E1 and E6 bands once every 15 s. The recorder configuration can be seen in Table 1.

Table 1. Recording specifications.

Parameter	Value
Sample Rate	80 MHz
Format	IF
Recording Time	25 ms
Bands	2 (E1 and E6)
Quantization	2 bits
File Size	1000 kB

Using this setup, a total of 240 snapshots are collected, in order to evaluate the nominal performance of S-TrackS. The performance is computed by comparing the resulting position–time solutions with a precise point positioning (PPP) solution. The performance metrics consist of the Circular Error Probable (CEP) and 2D root mean square error (2DRMS). Furthermore, any potential bias is computed by comparing the mean of obtained positions with the reference PPP position.

3.2. Impact of Signal Spoofing

Secondly, sets of snapshots with spoofed signals are recorded. As in the nominal scenario, the aforementioned test data are replayed and recorded with the S-TrackS recorder. As it is illegal to spoof GPS or Galileo over the air, simulated signals are inserted over the cable. In order to simulate a realistic scenario, a HackRF One SDR [9] is used together with a signal combiner to simulate spoofing.

Two GPS and one Galileo spoofing scenarios are carried out. The datasets consists of 240 snapshots for each scenario. GPS L1 C/A is spoofed to a distance of 200 m and 200 km. These two cases evaluate the situation where Galileo OS signals can still be used to aid the acquisition of PRS signals. In the third case, Galileo OS signals are spoofed to a distance of 200 km and PRS needs to be acquired without any aiding data.

3.3. Impact of the Coarse Position–Time

Thirdly, a sensitivity analysis is carried out on the quality of the assistance data. As the coarse position–time in the metadata file are used within the processing, inaccurate assistance data can lead to errors. An analysis is therefore performed to investigate the impact of errors in the coarse position–time on the performance of S-TrackS.

For this analysis, one snapshot is taken from the nominal scenario. This snapshot is then reprocessed with varying position–time errors added to the assistance data. The obtained position–time solutions are then compared to the nominal solution. The position error is increased from 0 to 500 km in a Northward direction with a step size of 10 km. The time error is increased from 0 to 600 s, with a step size of 12 s.

4. Results

The results of this study are presented in this section. For each test, the data are processed using S-TrackS, and relevant statistics are derived. The results provide insight in the performance with respect to accuracy, spoofing detection, and sensitivity to metadata.

Due to the classification of PRS, no accuracy statistics of the actual signal are disclosed. As it is processed using a similar approach using code-based measurements from Galileo satellites, results comparable to those of E1BC and E6BC are found.

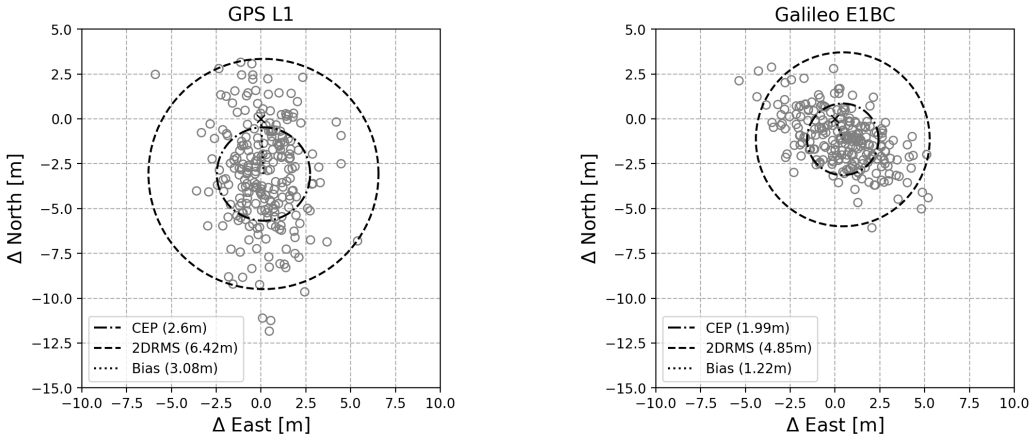
4.1. Nominal Results

The nominal results without spoofing are presented in this section. In total 240 positions are collected in the nominal dataset. The number and percentage of found position–time solutions per snapshot are shown in Table 2.

Table 2. Found position–time solutions within the nominal dataset.

Snapshots	GPS L1	E1BC	E1A	E6BC	E6A	Authenticated
Number	240	240	238	240	238	240
Percentage	100%	100%	99.17%	100%	99.17%	100%

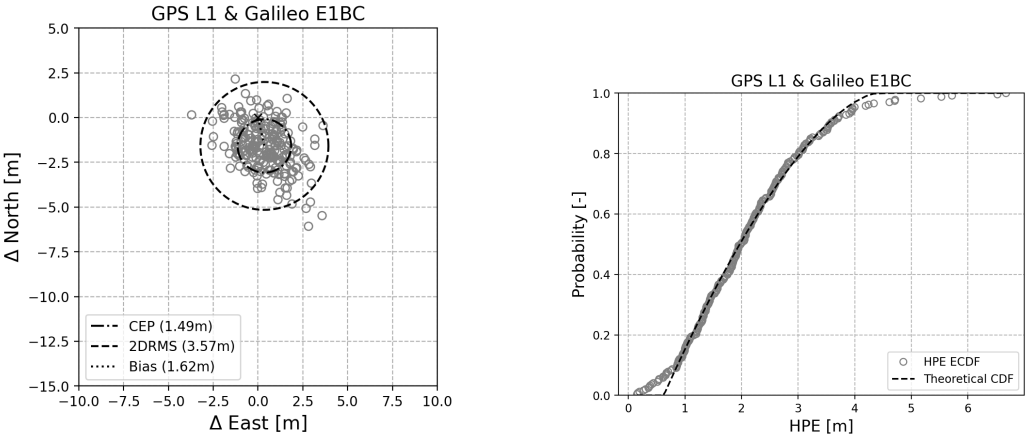
In four snapshots, either an E1A or an E6A position is not found, but the other is still determined. All snapshots have therefore been authenticated. The accuracies for the L1 C/A and E1BC position solutions are shown in Figure 4a,b.



(**a**) GPS L1 accuracy. (**b**) Galileo E1BC accuracy.

Figure 4. Accuracies derived using S-TrackS for GPS L1 C/A (**a**) and Galileo E1BC (**b**).

The 2DRMS's for GPS L1 and E1BC are found to be 6.42 m and 4.85 m, respectively. In addition, a bias of 3.08 m is found for GPS and 1.22 m for Galileo. In order to improve the accuracy, the observations of both GPS and Galileo are combined in a single position–time solution as shown in Figure 5a. In addition, the associated cumulative density function (CDF) of the horizontal position errors (HPE) is shown in Figure 5b.



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

Figure 5. Accuracies derived using S-TrackS for the combined Galileo E1BC and GPS L1 C/A position–time solutions (**a**) and the corresponding error distribution (**b**). (**a**) Combined GPS L1 and Galileo E1BC accuracy. (**b**) Distribution of errors for GPS L1 and Galileo E1BC.

When combining the GPS and Galileo observations in a single solution, it can be seen that the 2DRMS is reduced to 3.57 m. Furthermore, it can be seen that the bias is reduced from 3.08 m for GPS to 1.65 m for the combined GPS and Galileo solution.

It is found that the errors are not normally distributed and that the CDF therefore does not resemble a standard χ^2 distribution. This can also be seen from the difference between the mean position's bias in Figure 5a and the median shown in Figure 5b. This difference indicates a skewed distribution. In order to estimate the theoretical CDF more accurately, the generalized Pareto distribution (GPD) has therefore been chosen as in [10].

4.2. Impact of Signal Spoofing

The results of spoofed datasets are shown in Table 3, which includes whether or not the true PRS position–time were resolved, and which flag was returned by S-TrackS.

Table 3. Returned S-TrackS Results in various simulated scenarios.

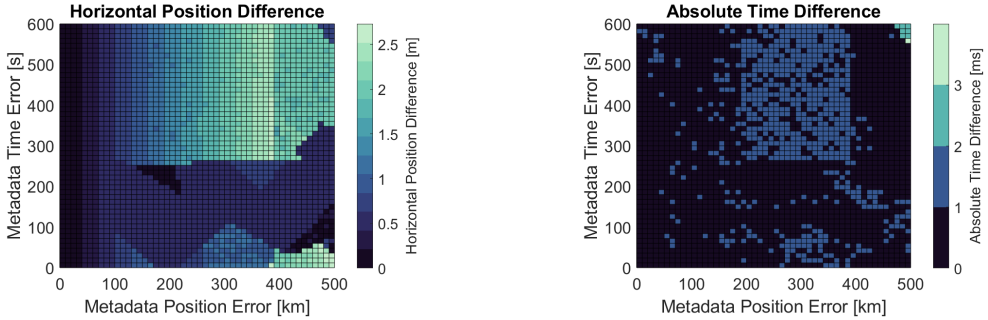
Spoofing	PRS Position–Time Found (%)	Authenticated Flag (%)	Spoofed Flag (%)	Warning Flag (%)
Nominal	100%	100%	0%	0%
GPS (200 m)	98.75%	0%	98.75%	1.25%
GPS (200 km)	98.75%	0%	98.75%	1.25%
Galileo (200 km)	100%	0%	100%	0%

During both the first and second spoofing scenario, a true PRS position was found in 98.75% of the cases. The spoofing was therefore detected as well in 98.75% of the instances. In 1.25% of these instances, PRS signals were not found, and a warning flag was returned. In the third spoofing scenario, the Galileo E1BC signal was spoofed and could not be used to aid the acquisition of E1A PRS signals. Although this requires more processing time, the PRS positioning and time were resolved in 100% of the instances. This demonstrates that S-TrackS can successfully obtain PRS position–time solutions, independent on the state of public GPS and Galileo signals.

4.3. Impact of the Coarse Position–Time

As not all tracking devices are able to provide an accurate position–time in the metadata file, the sensitivity of S-TrackS to errors in these values is analyzed.

The robustness of the millisecond ambiguity fixing depends on the duration of the PRN codes. When a longer PRN code is used, a larger offset can be present in the estimated position–time before a different integer number of codes are present between the satellite and receiver. Hence, the longer codes of Galileo E1BC can aid in resolving the integer number of PRN codes for GPS L1 C/A when used together with Galileo E1BC measurements. By choosing one of the Galileo satellites as reference satellite in the millisecond ambiguity algorithm, the number of PRN codes can be estimated more accurately for GPS L1 C/A. The horizontal position–time differences compared to the case where no metadata errors are added can be found in Figure 6.



(**a**) Position difference. (**b**) Time difference.

Figure 6. Impact of errors in the coarse position–time on the position (**a**) and time (**b**) found for GPS L1 C/A and Galileo E1BC.

In Figure 6a, it can be seen that the horizontal position difference stays within 2.73 m of the nominal case. Furthermore, one can see in Figure 6b that the timing difference also stays within 3 ms. Based on these results, it can be concluded that errors up to 500 km and 10 min in the coarse position–time only have a marginal impact on the obtained position–time solution.

5. Discussion

It was found that the number of obtained E1A position–time solutions was higher than for E6A. As each Galileo satellite transmits both E1 and E6, this is an unexpected result of the study. Two possible explanations are considered. First of all, the signal sensitivity of the RF front end within the S-TrackS recorder might be lower for E6 than it is for E1. Secondly, more interference sources might be present within the E6 band. More research is required on the question of why the E6 sensitivity was found to be lower than E1.

There is a trade-off between the file size of a snapshot and the robustness of resolving a PRS position–time solution. Within this paper, a snapshot length of 25 ms was selected, as it provides an acceptable level of robustness while minimizing the file size of a snapshot. For dedicated use cases, a higher level of robustness might be required. In these cases a longer snapshot recording time can be used to increase the acquisition sensitivity.

This paper showed that the accuracy of the coarse position–time provided in the metadata file marginally influences the performance. As most IoT devices have access to a coarse position–time within a few kilometers and a few minutes, this data can be used to obtain reliable position–time solutions. Even without such assistance data, knowing the approximate time and the country that the device is in can be accurate enough. However, performing Galileo PRS acquisition on E1A or E6A without any Galileo OS signals on either frequency will be significantly faster if an accurate time is known.

With respect to the test setup, a RTK receiver could be used to increase the accuracy of the reference position. A bias was furthermore observed between this reference position and the positions found by S-TrackS. Preliminary tests have shown that the usage of precise products, such as precise ephemerides, in S-TrackS can decrease this bias.

6. Conclusions

Snapshot positioning in combination with PRS can provide a high level of security for users who do not require an instantaneous verification of their position–time. Snapshot positioning therefore offers a solution with eased requirements on user equipment compared to a stand-alone PRS receiver. This paper has demonstrated that currently available RF front ends can be utilized to deploy snapshot services. Furthermore, the snapshot based concept allows flexibility and can be configured to the users' needs.

During the nominal test, 100% of the snapshots were successfully authenticated, demonstrating the robustness of S-TrackS. In this test the accuracy of S-TrackS was evaluated. A 2DRMS of 3.57 m with a bias of 1.62 m was obtained using GPS L1 C/A and Galileo E1BC signals.

It has been demonstrated that S-TrackS can be used to authenticate position–time solutions under various spoofing conditions. During the GPS spoofing test, spoofing was detected and the true position was found with the aid of PRS in 98.75% of the snapshots. In the Galileo spoofing test, the true position was found in all the snapshots. This demonstrates that S-TrackS can successfully obtain PRS position–time solutions, independent on the state of the public GPS and Galileo signals.

Lastly, the influence of errors in the coarse position–time provided in the metadata file was analyzed. It was shown that metadata values within 500 km and 10 min of the truth only had a marginal impact on the obtained position–time solution. Hence, it is demonstrated that S-TrackS can reliably be used as an authentication service if the position–time are approximately known.

7. Patents

The developments as described in this paper have led to innovative solutions for the future of secure navigation technology. The solution described in this paper has been patented through the European Patent Office, published in Patent Number EP3923032 [11].

Author Contributions: Conceptualization, A.V. and T.v.d.O.; methodology, A.V., T.v.d.O. and J.G.F.; software, A.V., T.v.d.O., J.G.F. and N.v.d.H.; validation, T.v.d.O. and J.G.F.; formal analysis, A.V., T.v.d.O., J.G.F. and N.v.d.H.; investigation, A.V. and J.G.F.; resources, J.G.F.; data curation, T.v.d.O., J.G.F. and N.v.d.H.; writing—original draft preparation, A.V., T.v.d.O. and J.G.F.; writing—review and editing, N.v.d.H. and A.Z; visualization, A.V. and N.v.d.H.; supervision, A.Z. and B.v.d.H.; project administration, A.Z. and B.v.d.H.; funding acquisition, A.Z. and B.v.d.H.; All authors have read and agreed to the published version of the manuscript.

Funding: The research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data supporting this research is not available due to commercial restrictions.

Acknowledgments: The authors of this paper would like to thank the Ministry of Infrastructure and Water Management, the CPA and the Netherlands Space Office for enabling PRS developments in The Netherlands.

Conflicts of Interest: The authors of this paper were employed by CGI Nederland B.V.

References

1. Anthony, T. NAVSTAR GPS Space Segment/Navigation User Segment Interfaces, IS-GPS-200. 22 August 2022. Available online: https://www.gps.gov/technical/icwg/IS-GPS-200N.pdf (accessed on 2 May 2023).
2. European Union. European GNSS (Galileo) Open Service—Signal in Space Interface Control Document, OS SIS ICD. January 2021. Available online: https://www.gsc-europa.eu/sites/default/files/sites/all/files/Galileo_OS_SIS_ICD_v2.0.pdf (accessed on 2 May 2023).
3. European Union. Galileo Open Service Navigation Message Authentication Signal-in-Space Interface Control Document, OSNMA SIS ICD. January 2021. Available online: https://www.gsc-europa.eu/sites/default/files/sites/all/files/Galileo_OSNMA_SIS_ICD_v1.0.pdf (accessed on 4 May 2023).
4. European Union Agency for the Space Programme. PRS. June 2021. Available online: https://www.euspa.europa.eu/european-space/galileo/services/prs (accessed on 4 May 2023).
5. CGI. S-TrackS: Reliable Positioning Validation. Available online: https://www.cgi.com/en/media/brochure/s-tracks-reliable-positioning-validation (accessed on 8 May 2023).
6. European Union Agency for the Space Programme. Power-Efficient Positioning for the Internet of Things—White Paper. 2020; ISBN 978-92-9206-048-0. Available online: https://www.euspa.europa.eu/sites/default/files/uploads/gsa_internet_of_things_white_paper.pdf (accessed on 4 May 2023).
7. Institute of Navigation. GNSS Software Defined Receiver Metadata Standard. January 2020. Available online: https://sdr.ion.org/ (accessed on 3 May 2023).
8. van Diggelen, F.S.T. *A-GPS: Assisted GPS, GNSS, and SBAS*; Artech House: Boston, MA, USA, 2009.
9. Great Scott Gadgets. HackRF One. Available online: https://greatscottgadgets.com/hackrf/one/ (accessed on 8 May 2023).
10. Ahmad, K.; Sahmoudi, M.; Macabiau, C. Characterization of GNSS Receiver Position Errors for User Integrity Monitoring in Urban Environments. In Proceedings of the ENC-GNSS 2014, European Navigation Conference, Rotterdam, The Netherlands, 15–17 April 2014.
11. Vroom, A.; van den Berg, A.; van den Oever, T.D.; Ciuban, S. Method for Detecting Potential Tampering with Satellite Navigation Signals and/or for Determining a Position. European Patent EP 3923032, 10 June 2020.