engineering proceedings

MDPI

Proceeding Paper

GNSS Radio Frequency Interference Mitigation in Collins Commercial Airborne Receivers †

Angelo Joseph, Patrick Bartolone, Joseph Griggs, Bernard Schnaufer, Huan Phan and Vikram Malhotra *

Navigation Systems Engineering, Collins Aerospace, 795 W NASA Blvd, Building 312, Melbourne, FL 32901, USA; patrick.bartolone@collins.com (P.B.)

* Correspondence: vikram.malhotra@collins.com

† Presented at the European Navigation Conference 2023, Noordwijk, The Netherlands, 31 May–2 June 2023.

Abstract: Nowadays, commercial aeronautical Global Navigation Satellite Systems (GNSS) receivers are more and more exposed to Radio Frequency Interference (RFI) threats from GNSS jammers and spoofers. On commercial aircraft GNSS, receiver outputs, in general, are integrated or cross-monitored with other navigation sensors such as IRS and DME, etc., and, in many cases, the GNSS receiver outputs are used directly by on-board aircraft systems. The advent of modernized dual-frequency and multi-constellation signals will improve the availability and integrity of GNSS receivers in the presence of RFI. To be further resilient to the various types of RFI threats, the airborne GNSS receiver will need to perform additional receiver-based detection/mitigation techniques and should be able to determine position integrity in the presence of spoofers. This paper focuses specifically on two techniques under development that will be incorporated via a field loadable software update to the GLU-2100. The first method, Receiver Autonomous Signal Authentication (RASA), and a second type of technique, Staggered Examination of Non-Trusted Receiver Information (SENTRI). The paper will provide a brief description of the RASA and SENTRI algorithms, followed by results from both simulation and real-world tests. Finally, the limitations of the algorithms will also be provided.

Keywords: GNSS; RFI; anti-spoofing

Citation: Joseph, A.; Bartolone, P.; Griggs, J.; Schnaufer, B.; Phan, H.; Malhotra, V. GNSS Radio Frequency Interference Mitigation in Collins Commercial Airborne Receivers. *Eng. Proc.* **2023**, *54*, 18. https://doi.org/10.3390/ENC2023-15420

Academic Editors: Tom Willems and Okko Bleeker

Published: 29 October 2023

1. Introduction

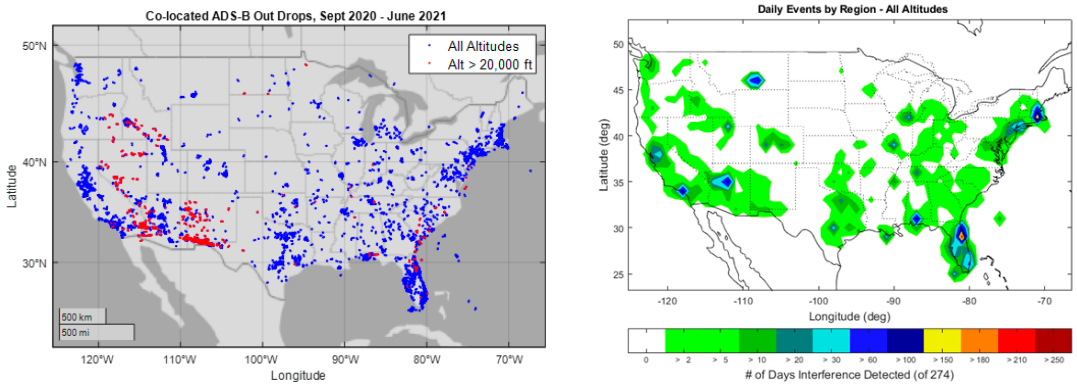
Nowadays, commercial aeronautical GNSS receivers are more and more exposed to RFI threats from GNSS jammers and spoofers. Worldwide reports from air navigation service providers and Collins customers have confirmed that commercial airborne GNSS receiver products have been exposed to both jamming and spoofing. The following three publications, Collins Aerospace RFI Assessment [1], SIB EASA's Safety information bulletin [2], and the 2022 ITU RRB circular [3] particularly show the increasing RFI threats and vulnerabilities of commercial airborne GNSS receivers.

1.1. EASA Related RFI Events

Through its safety information bulletin released in February 2023 [2], the European Union Aviation Safety Agency (EASA) reported a significant increase in jamming and or possible spoofing of GNSS since the beginning of 2022. The bulletin lists the areas affected by these events and provides a list of issues such as an inability to use GNSS for waypoint navigation, a loss of RNAV and RNP operations, inconsistent aircraft positions, a loss of ADS-B, wind shear and surface functionalities, the failure or degradation of ATM/ANS/CNS and aircraft systems which use GNSS as a time reference, potential airspace infringements, and/or route deviations that a degradation of GNSS signal could generate. EASA has recommended a series of mitigating measures to address issues related to GNSS jamming and spoofing. These measures focus on being prepared with alternate procedures when GNSS is unavailable due to jamming and spoofing.

1.2. Collins Aerospace RFI FlightAware Data Analysis

Collins developed a method using FlightAware's Firehose service to identify airborne GNSS RFI by detecting ADS-B Out drops within a given time interval from co-located aircraft equipped with ADS-B Out transponders [1]. This analysis shows that, while less than 1% of all flights over the CONUS during the time period of analysis were impacted by RFI, sustained RFI-related outages were observed in specific regions (Figure 1). Validation of the results showed that the method was successful at detecting RFI when and where intentional RFI was expected via aviation NOTAMs.



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

Figure 1. Map of GNSS RFI threats with respect to ADS-B FlightAware data analysis.

1.3. Circular from the ITU the Radiocommunication Bureau

The ITU Radio Regulations Board (RRB) has advanced a circular letter [3] to member states with recommendations for mitigating harmful interference to RNSS receivers using measures such as reinforcing navigation systems' resilience to interference, increasing collaboration between regulatory and enforcement authorities, and retaining conventional navigation infrastructure for contingency support in case of RNSS outages.

2. The Collins Aerospace GLU-2100 Multi-Mode Receiver (MMR)

The Collins Aerospace GLU-2100 MMR features a hardware, software, and firmware baseline that has been certified on Airbus and Boeing platforms. It is an ARINC 755-4 compliant unit whose GNSS navigation is currently based on GPS and SBAS L1 signals. The baseline GLU-2100 software, hardware, and firmware are designed to Level A DO-178C [4] and DO-254 [5] standards. Further, a dual thread processing architecture is used to meet the safety requirements of a unit whose failure could lead to catastrophic conditions. The hardware baseline architecture allows the GLU-2100 to be upgraded via a software/firmware field load to support GPS, SBAS, Galileo, and Beidou dual frequency signals.

The baseline GNSS engine within the GLU-2100 supports a Universal Channel Architecture [6] that can be configured at run-time to track any of the supported signal types. The DFMC capability of the GLU-2100 was demonstrated as part of the Boeing ecoDemonstrator [7] program. Further, as part of the European Union MUGG project, the universal channel architecture was leveraged to implement the core GNSS acquisition, tracking, and demodulation functions as defined in the DFMC MOPS ED-259A [8]. The navigation software was updated to support future navigation modes such as DFMC SBAS and H-ARAIM.

3. Overview of the RFI Technology in Collins Aerospace GNSS Solutions

Collins Aerospace has the following three-pronged strategy to address GNSS RFI threats, as illustrated in Figure 2:

- RFI Detect—generic flag to warn the user of the presence of RFI.

- RFI Mitigate—identify more precisely the magnitude of induced position errors, jammer strengths, or the specific satellite signals that are being spoofed.
- RFI Playthrough—play through jammer and spoofer attacks by continuing to output authentic position solutions.

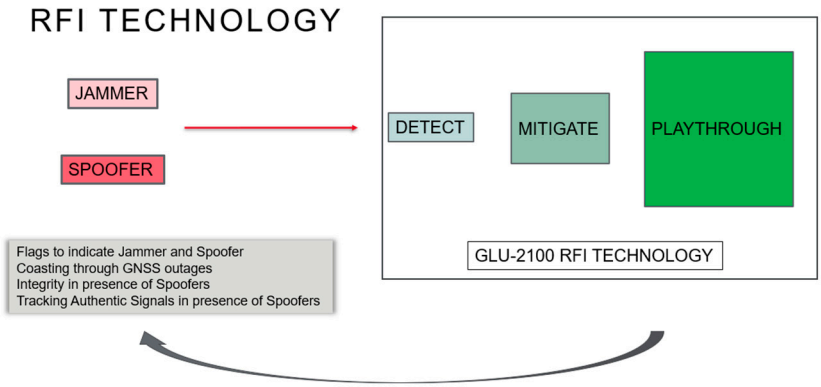
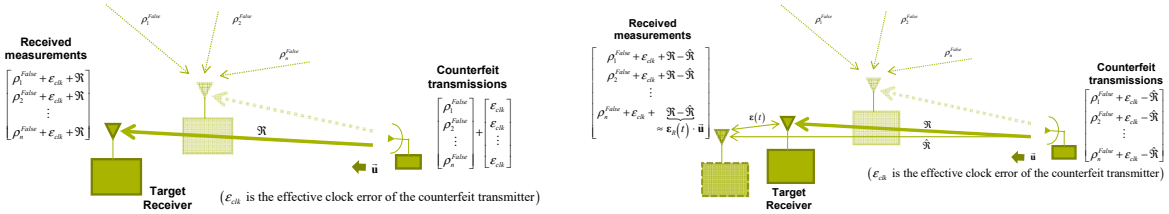


Figure 2. Collins RFI Response Strategy.

The next generation of Collins Aerospace GNSS receivers will introduce multiple RFI resilience techniques via field loadable software updates to satisfy the goals of the RFI mitigation strategy. The remainder of this paper will focus on two techniques known as RASA and SENTRI that will be used for spoofer detection.

4. Receiver Autonomous Signal Authentication (RASA)

RASA [9,10] is a Collins patented technique that uses the effect of the spoofer that is observed on the receiver's clock bias estimate to detect the presence of spoofers. When spoofed GNSS signals are received from a single transmitter, the path lengths between the transmitter and the aircraft are common to all the spoofed signals and so affect the estimated receiver clock bias (unsynchronized spoofing, Figure 3a). Even if the path length is estimated and accounted for by the spoofer (synchronized spoofing, Figure 3b), the clock bias estimate will be impacted by the error in this estimate. If the baseline no-fault behavior of the clock is known under worst-case environmental conditions such as vibration and temperature ramps, the change in the clock behavior due to spoofing can be used to detect a spoofer at a fixed P_{FA}. The clock behavior is assessed by computing the Allan variance of the clock bias, with the performance varying based on the τ (time between clock samples) and averaging period over which the Allan variance is computed.

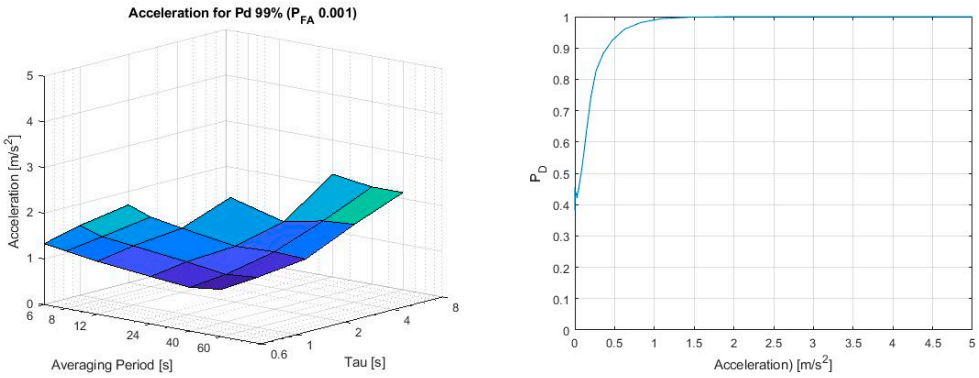


(**a**) (**b**)

Figure 3. GNSS receiver operation in the presence of unsynchronized (**a**) and synchronized (**b**) spoofing.

An RASA detection performance analysis was performed with live-sky authentic measurement logs captured with multiple GLU-2100 units during flight trials and other dynamic scenarios, as well as scenarios generated on a GNSS RF simulator. The RASA statistic was computed offline over the full duration of each scenario for each simulated spoofer. The simulation is somewhat conservative, as it assumes that the spoofer can track and rebroadcast the spoofed measurements without any errors. Figure 4 shows the performance of different combinations of τ and Allan variance averaging periods in terms

of the relative LoS acceleration with the worst-case fixed P_{fa} threshold to achieve a detection rate of 99%, as well as the detection performance of the chosen τ of 1 s and averaging period of 24 s.

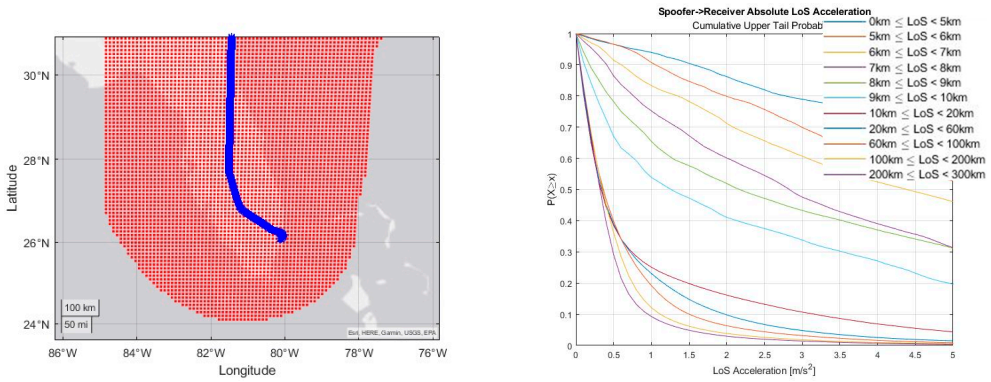


(**a**) (**b**)

Figure 4. LoS Acceleration for a fixed detection performance (**a**) and performance (probability of detection P_D) of the fixed threshold over acceleration for fixed $P_{FA} = 10^{-3}$, $\tau = 1$ s and 24 s averaging period (**b**).

4.1. RASA Simulations: Real World Commercial Flight Dynamics

Twenty real world flight trajectories of different lengths and aircraft types were analyzed to produce statistics of the LoS acceleration between static ground-based spoofers and aircraft position throughout the duration of flight (Figure 5a).



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

Figure 5. Example simulated spoofer locations (red dots) versus aircraft trajectory (blue line) as far as LoS distance to horizon per altitude (**a**) and real-world LoS acceleration distribution (**b**).

Figure 5b shows the cumulative upper tail probability function of the aggregate LoS acceleration. With the tunable parameters already discussed and a 99% probability of detection at an LoS acceleration of 1 m/s^2, RASA could be expected to achieve a total P_D of around 95% (per sample) for an unsynchronized spoofer within 5 km of the aircraft, decreasing to around 45% for a spoofer between 9 and 10 km.

4.2. RASA Simulations: Mixed Sets

The following simulation results show the effectiveness of RASA when a combination of authentic LoS and spoofed signals are tracked. The ratio of authentic to counterfeit signals used in RASA offline processing, as well as the specific set of spoofed measurements within the same ratios, were varied. The results shown in Figure 6 indicate that RASA detection performance was not significantly reduced if the LoS acceleration was

greater than ~1.1 m/s^2, even when only one of the measurements used in the navigation solution was counterfeit. As the LoS acceleration was reduced below this value, the performance diminished.

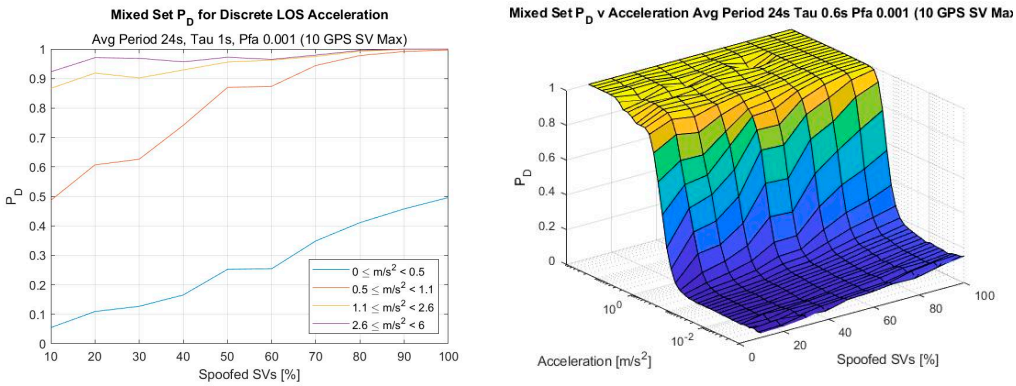


Figure 6. Mixed set detection performance for discrete acceleration bins (**a**) and as a function of acceleration (**b**).

4.3. RASA Simulations: Synchronized Spoofers

Residual estimation error from an in imperfectly synchronized spoofer was simulated with a first-order Gauss Markov model. This spoofer model generalizes the estimation error to a time variation of error magnitude along the LoS vector. The ASA detection performance in the presence of this model is shown in Figure 7. A standard deviation greater than 6 cm is detectable at 100% per sample.

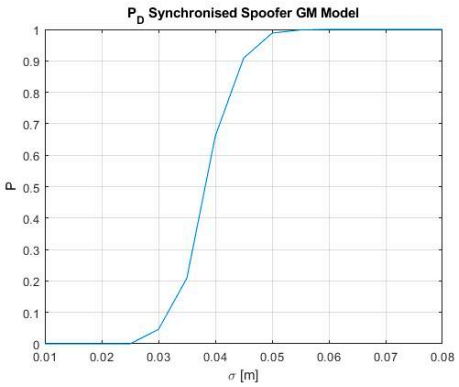


Figure 7. Synchronized spoofer detection performance.

5. Staggered Examination of Non-Trusted Receiver Information (SENTRI)

SENTRI (Figure 8) is a Collins patented [11] technique that uses multiple inertial coasted position solutions as trusted sources to protect a master GNSS position solution. Initially, the master solution will be the L1 SBAS solution or the L1 GPS-only solution, but in the future, the master solution can be a DFMC SBAS or H-ARAIM solution. In this architecture, the error estimation Kalman Filter maintains a fully blended GNSS-Inertial position solution. Three staggered coasting solutions (1, 2, and 3) are derived from the blended solution by propagating their solutions on pure inertial data without any GNSS measurements. The premise behind the SENTRI algorithm is that, when the GNSS measurements are being spoofed, the master solution will deviate from the coasting solutions. Depending on the stability of the IRS, the coasting solutions will gradually degrade in position accuracy, but they will not be tainted by the spoofed measurements. When considering a single coasted solution, the optimal performance of the of the SENTRI detector is achieved when the start of coasting occurs just before the GNSS measurements are spoofed. In this case, the coasting solution is untainted by the spoofed measurements

and the master solution deviates maximally from the coasted solution. In the case where the start of a coasting solution occurs just after the GNSS measurements are spoofed, the master solution deviates minimally from the coasted solution. Since the start time of the spoofer is unknown, the coasted solutions are staggered in time such that the spoofer can be detected regardless of the relationship between the coasting start and spoofer start times. In the GLU-2100, SENTRI is implemented with three staggered coasted solutions, each with a coasting time of 30 s and staggered with an offset of 10 s between them.

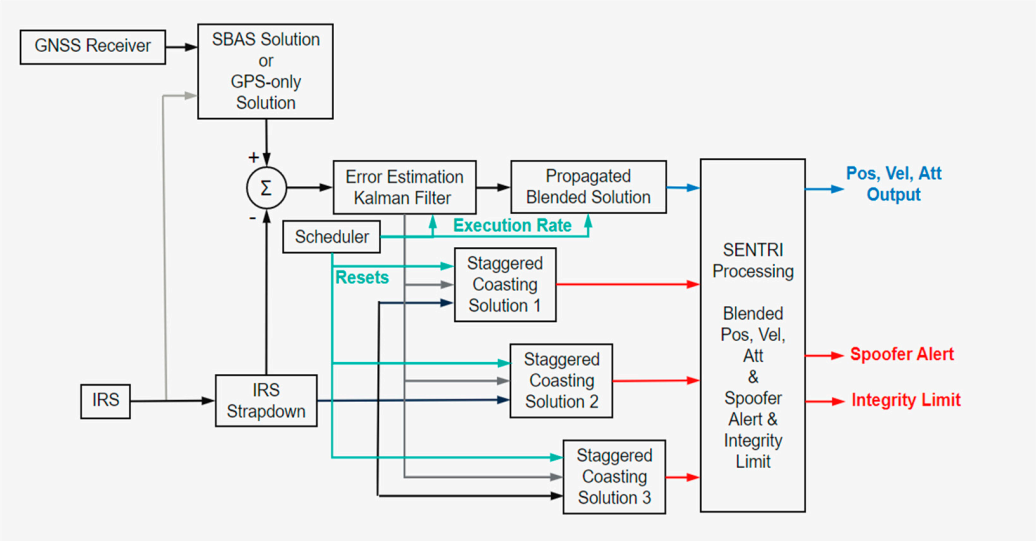


Figure 8. SENTRI Architecture.

SENTRI uses parity space techniques to determine a protection bound of the spoofing-induced master solution position error. The fault detection and protection level computation are mechanized by considering the measurement vector of the least square solution to be composed of the coasting solution coordinate (in either x, y, or z direction of the local level frame) and the corresponding master solution coordinate. The parity vector is dependent on the difference between the master and coasted solution coordinates. Standard parity space methods are used to derive fault detection and protection level statistics.

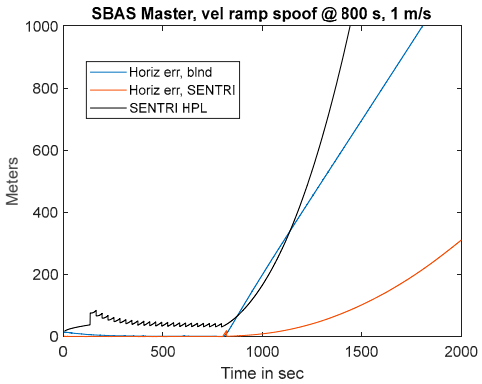
5.1. SENTRI Simulations and Performance

The RTCA MOPS for GNSS-Aided Inertial Systems DO-384 [12] Appendix Q defines the simulation approach to generating performance data to populate spoofer claim tables. Three types of spoofers are considered, position step, velocity step, and acceleration step. The scenario includes initialization time, exposure time, and recovery time. In general, the detection performance of the SENTRI algorithm in the presence of different spoofer types is dependent on the aircraft dynamics and the accuracy of the master solution. For this analysis, the aircraft dynamics were divided into normal and abnormal dynamics, as defined in Section 2.1.2.5 of DO-229E [13]. The GPS navigation mode and SBAS PA (Precision Approach) navigation mode accuracy values were used to model the master solution accuracy.

As seen in Table 1, the SENTRI algorithm performs better under normal dynamics and when the master solution is a more accurate solution such as the SBAS master solution. The above results are preliminary in nature and were determined via simulations that used the same model that is used to generate the code that is executed on the GLU-2100. For purposes of illustration, one run of the SENTRI simulation is shown below to demonstrate the spoofer detection capability when a velocity ramp of 1 m/s is introduced in SBAS mode. In Figure 9, the 1 m/s velocity ramp spoofing begins at 800 s into the run. The SENTRI alert occurs at 820 s and the SENTRI HPL bounds the master solution error.

Table 1. SENTRI Detection for GPS L1 and SBAS L1 Master.

	Normal Dynamics		Abnormal Dynamics	
	GPS L1	**SBAS L1**	**GPS L1**	**SBAS L1**
Min Position Step (m)	40	30	45	35
Min Velocity Step (m/s)	1.5	1.0	2.5	2.0
Min Acceleration Step (m/s^2)	0.24	0.15	0.28	0.20



Horiz err, blnd – Horizontal error of GNSS/IRS blended solution.

Horiz err, SENTRI – Horizontal error of master solution before detect and error of coasted solution after detects

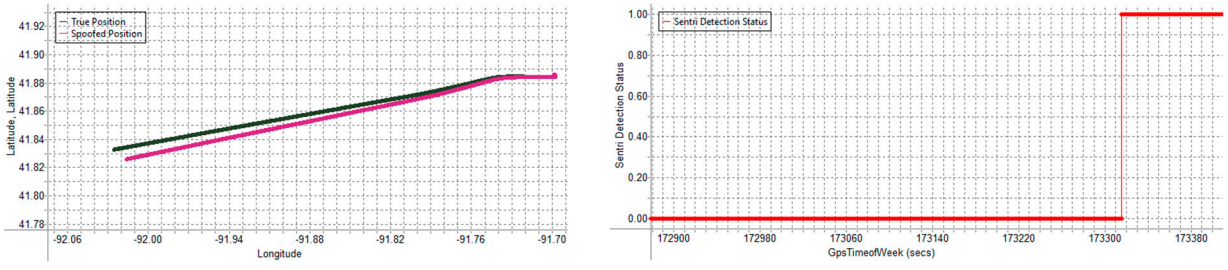
SENTRI HPL – SENTRI Integrity bound of the master solution before spoofer detection

Figure 9. SBAS master velocity ramp (1 m/s).

5.2. Real-Time Demonstration of SENTRI Spoofer Detection Capability

In this test, the performance of the Real-Time SENTRI software (version 2.0) was tested in the lab with hardware in the loop by connecting a GLU-2100 unit loaded with the SENTRI software to a GNSS signal simulator. The NAV grade inertial data were simulated by generating the attitude and inertial position data from the simulator scenario and then adding the IMU noise to the simulated data by using the model of an NAV grade inertial system. The simulated IRS ARINC 429 labels were then sent to the GLU-2100 on the IRS input bus, thus mimicking the aircraft installation conditions. For purposes of illustration, the results from a scenario that mimics a true flight test on a Collins 604 Challenger Flight Test aircraft are discussed below. In this scenario, the spoofer was generated to gradually drift the GNSS signal simulated position from the true flight path.

In Figure 10, it is seen that the spoofer attempts to gradually drift the aircraft position from the true position. The SENTRI algorithm raises a spoofer alert before the position error exceeds the protection level.



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

Figure 10. Challenger 604 simulation trajectory (**a**) and SENTRI detection flag (**b**).

6. Integration of RASA and SENTRI in the GLU-2100

The previous sections demonstrated the spoofer detection performance of the RASA and SENTRI algorithms. The limitations of the algorithms were also presented. The RASA algorithm was shown to have a poor detectability when the line-of-sight acceleration between the aircraft and spoofer was low. Further a protection bound cannot be calculated

for the RASA detector. RASA also has a longer time-to-detect and it generally requires the probability of false alarm to be high to reliably detect spoofers. The SENTRI algorithm provides a protection bound around the spoofer detection. SENTRI requires that it is initialized with authentic signals. In the GLU-2100, the complementary benefits of RASA and SENTRI are used together to improve the resilience of the GNSS to spoofing. RASA (with a higher probability of false alarm) is initially used to confirm that all the signals being tracked are authentic signals. Once this authentication is confirmed, the GNSS measurements are passed on to SENTRI to initialize the blending filters. After SENTRI initialization, RASA continues to execute in the background and its detector outputs are only used for maintenance logging. SENTRI is used to detect the presence of spoofers and, if spoofers are detected, the GLU-2100 may enter a pure inertial coasting mode. Once a spoofer is detected, the SENTRI processing is terminated, and RASA is once again activated to monitor for authentic signals. Upon the successful acquisition of authentic signals, SENTRI is once again re-initialized and the RASA-SENTRI workflow repeats again.

The SENTRI protection level is expected to be used only when inertial coasting is triggered because of spoofer detection. The use of the SENTRI protection level has the potential to reduce the availability of GNSS integrity. Until a standardized availability analysis for spoofer detection is accepted by the avionics community, the GLU-2100 will not output the SENTRI protection level as part of its integrity levels under normal operation when spoofing has not been detected.

In summary, while the combination of RASA and SENTRI techniques has proven to be highly effective in detecting and mitigating GPS spoofing attacks, it is important to be aware of their limitations and to implement appropriate measures to address these challenges. By doing so, we can ensure that our GPS systems remain secure and reliable, even in the face of sophisticated spoofing attacks.

7. Conclusions

GNSS RFI threats have become increasingly common and are being reported regularly on a worldwide basis. GNSS receivers that are used in all applications, including commercial aviation, will need to consider implementing techniques to address the threats of GNSS spoofing and jamming. Collins Aerospace plans to introduce features via a software field loadable update to the GLU-2100 product to improve its resiliency to GNSS spoofing and jamming. This update introduces two techniques, RASA and SENTRI, that can be used together in a complementary fashion to reliably detect the presence of spoofers. Additionally, this update will provide improved robustness to data spoofing attacks that induce errors in ephemeris, almanacs, and GPS time jumps, etc. Further, this update will enable the GLU-2100 to coast through GNSS outages that are induced due to spoofing or jamming. Future technologies will leverage antenna techniques, signal analysis, DFMC signals, and APNT to increase the robustness to new and evolving threats. The goal of this RFI mitigation roadmap is to continue to ensure that GNSS can be used in a safe and reliable manner in civil aviation.

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

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

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

References

1. Kazmierczak, J.; Joseph, A.; Cook, G. Aviation GNSS Interference Analysis Based on ADS-B Out Data. In Proceedings of the 34th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2021), St. Louis, MO, USA, 20–24 September 2021; pp. 1108–1121.
2. Operations–ATM/ANS, EASA Safety Information Bulletin. Global Navigation Satellite System Outage Leading to Navigation/Surveillance Degradation. Available online: https://www.easa.europa.eu/en/newsroom-and-events/news/easa-updates-sib-gnss-outage-and-alterations (accessed on 1 February 2023).
3. ITU Radiocommunication Bureau (BR) Circular Letter CR/488, 8 July 2022. Available online: https://www.itu.int/dms_pub/itu-r/md/00/cr/cir/R00-CR-CIR-0488!!PDF-E.pdf (accessed on 1 February 2023).
4. *DO-178C:2011*; Software Considerations in Airborne Systems and Equipment Certification. RTCA: Washington, DC, USA, 2011.
5. *DO-254:2000*; Design Assurance Guidance for Airborne Electronic Hardware. RTCA: Washington, DC, USA, 2011.
6. Joseph, A.J.; Wahab, S.R. Universal Channel for Location Tracking System. U.S. Patent 9,702,979, 11 July 2017.
7. Joseph, A.; Kazmierczak, J.; Harris, M.; Schlais, P.; Murphy, T. Global Flight Test Results for a DFMC Primary Navigator on a Civil Air Transport Aircraft. In Proceedings of the 33rd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2020), Online, 21–25 September 2020; pp. 140–160.
8. *ED-259A*; Minimum Operational Performance Standard For GALILEO/Global Positioning System/Satellite-Based Augmentation System Airborne Equipment. EUROCAE: Lucerne, Switzerland, 2021.
9. Hwang, P.Y.; McGraw, G.A. Receiver Autonomous Signal Authentication (RASA) based on clock stability analysis. In Proceedings of the 2014 IEEE/ION Position, Location and Navigation Symposium-PLANS 2014, Monterey, CA, USA, 5–8 May 2014; pp. 270–281.
10. Hwang, P.Y. GNSS Receiver Autonomous Signal Authentication Using Signal Stability Analysis System and Related Method GNSS Receiver Autonomous Signal Authentication Using Signal Stability Analysis System and Related Method (RASA). U.S. Patent US9094392B1, 28 July 2015.
11. Doty, J.H.; Anderson, D.A.; Hwang, P.Y. Staggered Examination of Non-Trusted Receiver Information (SENTRI). U.S. Patent US11337034B1, 17 May 2022.
12. *DO-384:2020*; Minimum Operational Performance Standards (MOPS) for GNSS Aided Inertial Systems. RTCA: Washington, DC, USA, 2020.
13. *DO-229E:2016*; Minimum Operational Performance Standards for Global Positioning System/Satellite-Based Augmentation System Airborne Equipment. RTCA: Washington, DC, USA, 2016.