Limiting the Potential Impact of SBAS Spoofing

Todd Walter, *Stanford University*
Rebecca Wang, *Stanford University*
Juan Blanch, *Stanford University*

Abstract
Satellite Based Augmentation Systems (SBASs) were developed to protect against potential satellite clock and ephemeris errors as well as to reduce the impact of ionospheric delays. Most importantly SBASs provide strict upper limits on the remaining errors after applying such corrections. The SBAS signals are generated using trusted processes and their contents are certified to be safe for aviation use. SBAS aviation receivers are designed to trust these signals absolutely. However, the initial development did not include protections against the possibility of spoofing as it was not perceived as a significant threat at that time. Since that initial timeframe, spoofing has now become properly recognized as a significant threat, and the community is working to implement protections against spoofed SBAS signals.

SBAS providers are actively developing the standards to implement SBAS message authentication. When finally fielded, SBAS message authentication will protect against the risk of spoofed SBAS signals creating erroneous positioning information. Unfortunately, applying message authentication to the very limited SBAS message bandwidth is a complicated endeavor requiring significant changes for both the providers and the users. Fully developed standards are still several years away, and implementation and fielding will take even longer.

This paper describes simple methods to limit the error that SBAS spoofing could potentially induce on an SBAS user's position solution. One method examines the magnitude of the correction errors and flags the SBAS signal when its corrections exceed the satellite range error commitments from the constellation service providers. Another method evaluates the relative distance between the SBAS and uncorrected position solutions.

1. INTRODUCTION

Satellite Based Augmentation Systems (SBASs) were designed to provided trusted navigation information to aviation users (Walter, 2017). The SBAS information includes corrections to the broadcast positions and clocks, as well as confidence values to bound the remaining error after applying such corrections (RTCA, 2020). SBAS content is developed to stringent integrity requirements, and the signals are certified to support safety-of-life. Avionics are designed to completely trust the SBAS data content. However, there is a risk that an attacker could generate their own SBAS signal and that these could contain misleading information. To combat this threat, SBAS providers are developing a message authentication protocol that is backwards compatible with legacy signals and that will effectively prevent any receiver from accepting SBAS information from anyone aside from the true SBAS provider (Dennis et al., 2024) (Anderson, 2024). Unfortunately, the development of the SBAS message authentication protocol is time consuming and it will not be in place for several more years.

We propose simple algorithms that could be implemented much more quickly and that will reduce the potential magnitude of position errors induced by SBAS spoofing. One proposal is to limit the accepted SBAS correction magnitudes to be consistent within the error limits as described by constellation service providers (ICAO, 2023). When SBASs were first conceived, GPS implemented a deliberate degradation called Selective Availability (SA) (Zumberge & Gendt, 2001). To counter the effects of SA, SBAS corrections were made quite large; more that 250 m for clock errors and over 128 m in each of three orbital axes. However, in 2001 GPS eliminated SA and has subsequently committed to significantly smaller errors (US DoD, 2020). However, the L1 SBAS standards were set prior to SA's removal and the potential to introduce large errors through erroneous corrections remains a part of the legacy SBAS L1 standard. Another proposal here is to compare the position estimate provided by SBAS against another trusted position estimate that is independent of SBAS, for example from Receiver Autonomous Integrity

Monitoring (RAIM) (Lee et al., 1996) (Blanch et al., 2022). These algorithms will be further detailed and examined below.

2. SBAS SPOOFING RISK

The SBAS data stream represents a unique and vulnerable vector for spoofers to attack GNSS positioning. GPS enables users to determine their position. SBAS makes this position estimate more accurate and assures users that it is safe to use. SBAS allows users to perform operations that have safety-of-life implications. Further, SBAS provides this assurance through a single signal which all SBAS receivers are designed to process and trust. SBAS provides a set of corrections and confidences (RTCA, 2020). The corrections are used to shift the position from the baseline GNSS position solution to the new SBAS determined position. The confidences are used to determine upper bounds on the possible error on the position estimate. These upper bounds are called protection levels (Walter et al., 2010)(RTCA, 2020). Normally, the SBAS position is more accurate, and the protection levels describe a box that is assured to contain the actual user location. However, a spoofed SBAS signal can move the "corrected" position quite far from the true position and at the same time create very small protection levels that fail to include the true location. Because only a signal corresponding to a single SBAS satellite needs to be sent, and this signal may modify the measured ranges to all satellites in use, many spoofing mitigation strategies will not be able distinguish a spoofed SBAS signal from a valid one.

SBAS spoofing is considered a particularly concerning threat as it can be done using a single PRN and need not overpower any existing signals. Further it can introduce a bias to the position without affecting the GPS derived velocity or acceleration making comparisons against other sensors for these elements ineffective. In this analysis we assume that the GPS signals are not spoofed, because if they were, there would be no need to spoof the SBAS signal. It is potentially more complicated and more limiting to also spoof the SBAS when arbitrary position offsets can be achieved by spoofing the GPS signals themselves.

The SBAS corrections can be used to create pseudorange errors that are up to about 160 m on L5 (EUROCAE WG-62, 2023) or over 600 m on L1 (RTCA, 2020). The L5 corrections only contain satellite clock and orbit values, these are limited to ~64 m on adjustments to the clock and the three cartesian orbital coordinates. The cartesian (XYZ) orbital adjustments can be mapped into radial, along-track, and cross-track (RAX) adjustments whose upper values are dependent satellite location. At least 97% of the radial error maps into user pseudorange error while no more than 24% of the along-track and cross-track errors will map into user pseudorange error. The L1 corrections are larger as they were designed to handle selective availability and ionospheric corrections. The Fast Correction (FC) clock corrections can be as large as 256 m, the Long-Term Corrections (LTC) include orbital XYZ terms that can go up to 128 m and a clock term that can be as large as 143 m. Depending on satellite location and elevation angle the projected pseudorange errors can range from 530 m to 675 m if using only FC's and LTC's.

The above description does not take into account the rate correction terms, which could make these correction errors more than an order of magnitude larger by making the time of applicability hours into the past. This undesirable property was recently recognized, and the MOPS are being changed to have the receiver limit the time period over which the rate terms could apply. Rather than potentially creating kilometers of error they will be limited to roughly half the magnitude of the above correction terms. Altogether the pseudorange errors from the satellite clock and orbit correction and correction rates can be of order 250 m on L5 or 650 m on L1.

An SBAS spoofer would also have control over which satellites the receiver uses and what their confidence values are, so they could create geometries with worse properties than would typically be experienced. Typically, a pseudorange error will be multiplied by a value less than three when mapped into a position error. However, the spoofer can significantly increase this factor by controlling which satellites get used for the position solution and how much weight to assigned to each. The relationship between the pseudorange errors and the position error can be expressed as:

$$\Delta \boldsymbol{y} = \mathbf{G} \cdot \Delta \boldsymbol{x} \tag{1}$$

where $\Delta\boldsymbol{y}$ is the pseudorange error error vector, $\mathbf{G}$ is the geometry matrix and $\Delta\boldsymbol{x}$ is the position error vector. The inverse relationship is given by

$$\Delta\boldsymbol{x} = \mathbf{S} \cdot \Delta\boldsymbol{y} \tag{2}$$

where $\mathbf{S}$ is the projection matrix given by:

$$\mathbf{S} = (\mathbf{G}^{\mathrm{T}} \cdot \mathbf{W} \cdot \mathbf{G})^{-1} \cdot \mathbf{G}^{\mathrm{T}} \cdot \mathbf{W} \tag{3}$$

and $\mathbf{W}$ is the weighting matrix based on the uncertainty values provided by the SBAS signal (see Appendix J of (RTCA, 2020)). We ran a simulation over 24 hours using the default 24 satellite constellation and users located around North America. The spoofer can control the magnitude and sign of each satellite *j* in $\Delta\boldsymbol{y}$ as well as maximize the projection along any direction *i* in $\mathbf{S}$. Thus, by maximizing the error magnitudes for each satellite *j* and the sum of the absolute values of the projection matrix elements along row *j* corresponding to a particular direction (e.g., East, North, or Vertical) the spoofer will maximize the error it can create along that direction. At each user location and timestep we evaluated every subset geometry that could be made to support a 50 m Vertical Alert Limit (VAL) and 40 m Horizontal Alert Limit. Like the spoofer, our simulation has the ability to choose the User Differential range Errors (UDREs) and Grid Ionospheric Vertical Errors (GIVEs) for L1 or the Dual Frequency Range Errors (DFREs) for L5. Low values for these parameters allow the alert limits to be made quite small for geometries that ordinarily would not be available for use.

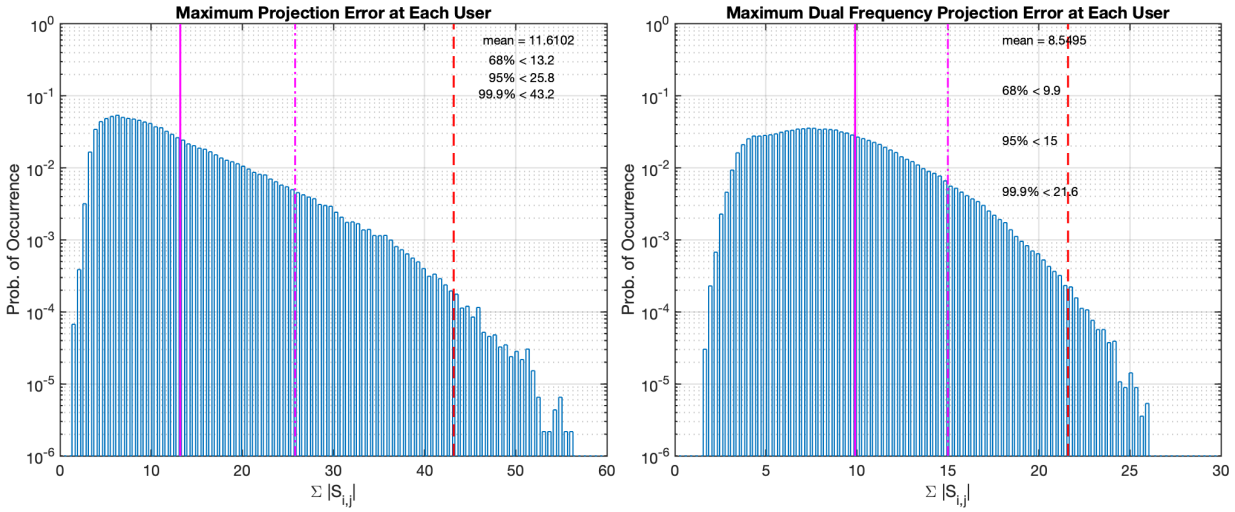

Figure 1. Histograms of the maximum projected ratio between the pseudorange error and the position error for L1 (left) and L5 (right)

Figure 1 shows histograms of the sum of the absolute value of the projection matrix values across all satellites in view for L1 users (left) and L5 users (right). The individual histograms for each direction (East, North, Up) all ended up looking nearly identical. Figure 1 contains the ones for the vertical direction. As can be seen, the pseudorange errors could be multiplied by factors of order 10 to 50 for L1 or from 5 to 25 for L5 depending on the underlying geometry of the GPS satellites. This means that a spoofer could create position errors as large as 32 km for L1 and up to 6 km. for L5. This threat inspired the need for SBAS message authentication. In the sections below, we propose methods to limit these potential effects of spoofed correction errors.

3. CONSTELLATION COMMITMENTS

Each Constellation Service Provider (CSP) has made certain commitments about their constellation performance in order to enable their use by the aviation community (ICAO, 2025)(US DoD, 2020)(European Union, 2023). These commitments are made in their performance standards and are being put into the Standards and Recommended Practices (SARPS) of the International Civil Aviation Organization (ICAO) (ICAO, 2025) (ICAO, 2023). Table 1 contains

the commitments for four core constellations: GPS, GLONASS, Galileo, and Beidou. The most relevant parameters are: σ_{URA}, a zero mean Gaussian overbound of nominal signal in space ranging errors; P_{sat}, the probability that a satellite has an error not overbounded by σ_{URA}, independently of all other satellites; P_{const}, the probability that a single fault will affect more than one satellite within the constellation, and *MFD*, the mean fault duration.

GPS satellites broadcast their own σ_{URA} values which can change over time, particularly if the satellite ephemeris has not been refreshed for many hours. It is most often set to 2.4 m. Figure 2 shows a histogram of the frequency of occurrence of the broadcast URA values from 2008 through 2025. Approximately 92% of the time a value of 2.4 meters is sent, 7.1% a value of 3.4 m is sent, less than 1% a value of 4.85 m is sent and slightly more than 0.1% a value larger than 5 m is sent. GPS has set P_{const} to be less than 10^{-8}. Thus, it is extremely unlikely that GPS will have two or more faulty satellites at any given time. The definition of a fault for GPS is that the satellite clock and ephemeris errors together project to greater than a 4.42 σ_{URA} error for any user. This corresponds to a 10.6 m upper limit most of the time. Unfortunately, none of the other constellations make such a strong commitment.

Table 1. Constellation Performance Commitments

	GPS	GLONASS	Galileo	BDS
Default ISD Parameters				
$P_{const,\ default}$	1×10^{-8}	1×10^{-4}	2×10^{-4}	6×10^{-5}
$P_{sat,\ default}$	1×10^{-5}	1×10^{-4}	3×10^{-5}	1×10^{-5}
$R_{const,\ default}$	1×10^{-8}/h	1×10^{-5}/h	1×10^{-4}/h	6×10^{-5}/h
$R_{sat,\ default}$	1×10^{-5}/h	3.4×10^{-5}/h	2×10^{-5}/h	1×10^{-5}/h
$MFD_{const,\ default}$	1 hour	10 hours	-	1 hour
$MFD_{sat,\ default}$	1 hour	3 hours	-	1 hour
$\sigma_{URA\ dual\ frequency}$	IAURA	9 m	6 m	7 m
$\sigma_{URA,\ single\ frequency}$	IAURA	9 m	6.5 m (E1), 7.5 m (E5a)	7 m

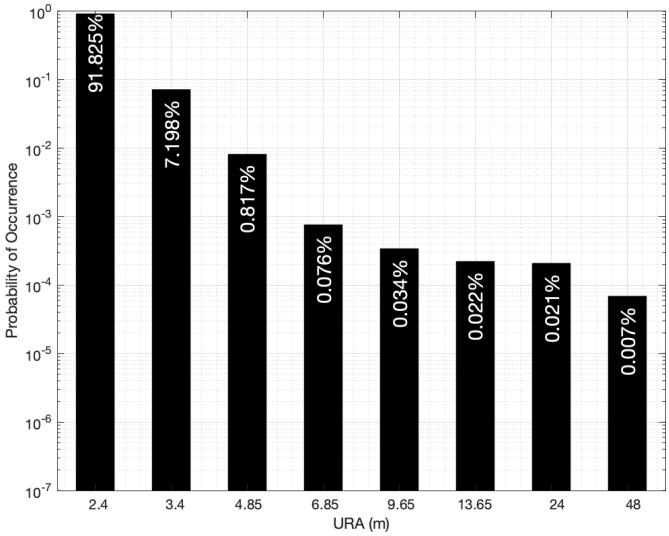

Figure 2. Frequency of occurrence values for broadcast GPS URA values from 2008 through 2025.

4. OBSERVED CONSTELLATION BEHAVIOR

The left side of Figure 3 shows the observed GPS performance from 2008 through 2025. It shows the maximum projected clock and ephemeris error for the satellite with the largest absolute error at each given time in blue and the satellite with the second largest concurrent error in red. On June 17, 2012, the maximum error grew to 448 m which is off the top of the plot. All other maximum projected errors over this time period have been below 50 m.

The second largest concurrent error observed in that time frame was 5.64 m. Notice that in early 2024, changes in operation significantly improved the overall accuracy of GPS. The right side of side of Figure 3 shows the same data but now divided by the broadcast value of σ_{URA}. Only rarely are the blue values greater than 4.42, which is the value that when exceeded is declared a GPS fault. All data is shown except the June 17, 2012, fault which corresponded to 187 times σ_{URA}. These instances correspond to the nine fault events that have occurred in this eighteen-year period. No simultaneous faults have been observed, confirming the extreme rarity of simultaneous faults, and the number of independent faults is well below the expected number corresponding to the committed value of P_{sat}.

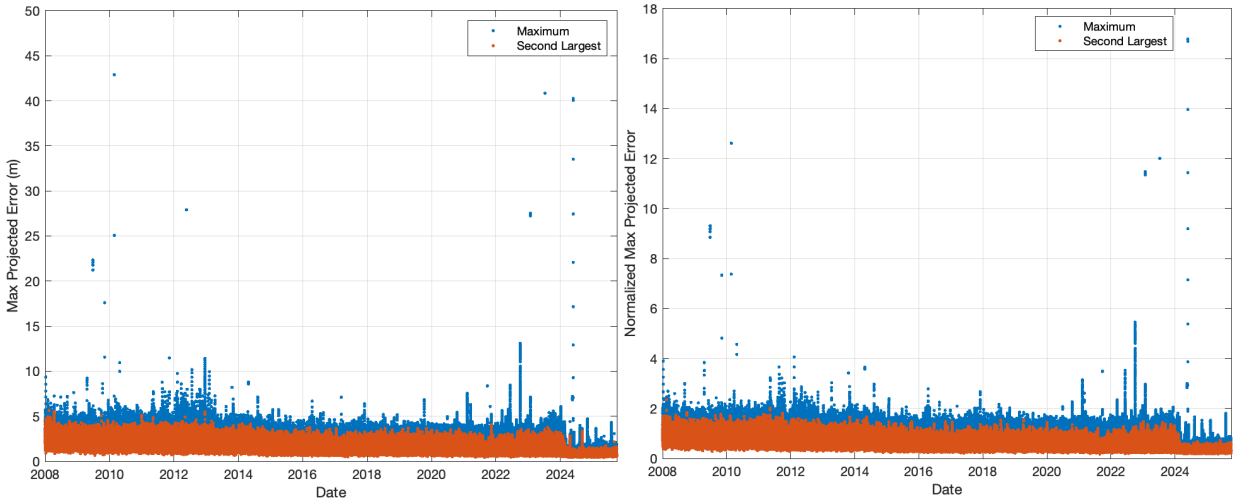

Figure 3. Largest and second largest projected GPS errors (left) and normalized projected errors (right)

The left side of Figure 4 shows the observed Galileo performance from 2020 through 2025. It shows the largest and second largest projected errors in blue and red respectively. There were five errors over this period that were larger than 18 m. They occurred on January 21, 2021; September 5, 2021; April 29, 2022; August 31, 2022; and July 21, 2024. All other projected errors have been below 18 m. The second largest concurrent error observed in that time frame was 1.85 m. The right side of side of Figure 4 shows the same data but now divided by the fixed σ_{URA} value of six meters. The largest fault occurred in September 2021, and it corresponded to a 540 m fault or 90 times σ_{URA}. There were five fault events that were observed in this five-year period. No simultaneous faults have been observed, and the number of independent faults is well below the expected number corresponding to the committed value P_{sat}.

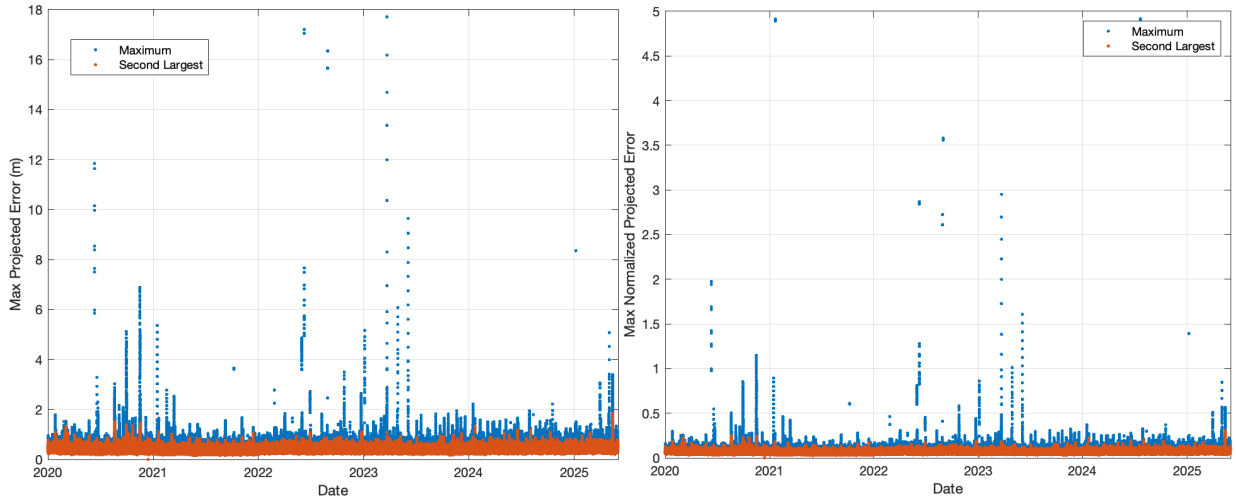

Figure 4. Largest and second largest projected Galileo errors (left) and normalized projected errors (right)

5. CORRECTION DOMAIN ALGORITHM

The observed data shows that large errors are rare on GPS and Galileo and simultaneous large errors have not been observed. The constellation commitment from GPS assures that this will remain so in the future. Therefore, receiving large corrections from an SBAS for multiple GPS satellites could serve as an indication of a spoofed signal. Here we propose a test to implement this concept. The algorithm must account for any common time offset between GPS time and the SBAS Network Time (SNT). It must also account for the uncertainty in the SBAS correction itself. We propose a corresponding threshold that can be used to test the correction magnitude. As above, we label the projected clock and ephemeris correction for satellite *j* to the user receiver as Δy_j . We then remove a common time offset component by differencing this with the median value from all such projected corrections. The median is chosen as it is robust estimator against a small number of outliers. This difference can then be compared against the expected uncertainty in the GPS error magnitude according to σ_{URA} and the uncertainty in the SBAS correction accuracy according to σ_{UDRE}. For dual frequency evaluations σ_{UDRE} is replaced by σ_{DFRE}.

$$\left|\Delta y_j \ - median(\Delta \boldsymbol{y})\right| > 4.42\sqrt{\sigma_{URA,j}^2 + \sigma_{UDRE,j}^2} \tag{4}$$

Both the σ_{URA} and σ_{UDRE} terms represent conservative overbounds of the expected errors, and we expect that it will be exceedingly rare for 4.42 multiplied by either term to fail to bound their respective errors. Therefore, we should not see more than one GPS satellite exceed the inequality in (4) at any given time (it will be very uncommon for even one to do so). The key idea of this proposed algorithm is then: if two or more projected GPS corrections exceed this threshold, then the user should deselect this SBAS signal and use a different one.

When σ_{URA} and σ_{UDRE} are small, this places much tighter limits on the correction magnitudes than the existing message structure allows. Assuming that the GPS signals are genuine, we have shown above that σ_{URA} is below 4.85 m nearly 99.9% of the time. The σ_{UDRE} can be much larger, but if it is made larger than 4.6 m, it cannot be used for vertical guidance per requirement [R229-227] of (RTCA, 2020). Further, increases in the σ_{UDRE} will be reflected in increased protection levels and decreased availability. Therefore, (4) effectively limits the correction error magnitude to $4.42\sqrt{4.85^2 \ + 4.56^2} \ \cong 29.4\ m.$

The above approach still leaves one satellite vulnerable to the possibility of a much larger spoofing error. We can add a further condition that if a GPS satellite has a correction value that satisfies (4) and its correction magnitude is greater than 30 m, then that GPS satellite should be excluded from the SBAS position solution. This can be expressed as:

$$\begin{gathered}\left|\Delta y_j \ - median(\Delta \boldsymbol{y})\right| > 4.42\sqrt{\sigma_{URA,j}^2 + \sigma_{UDRE,j}^2} \\ \text{and} \\ \left|\Delta y_j \ - median(\Delta \boldsymbol{y})\right| > 30 \text{ m}\end{gathered} \tag{5}$$

Based on the data in Figure 3, there have only been four events in the last 18 years where a GPS satellite could have met the conditions of (5) and then have been excluded. It is very likely that the satellite would have also been set unusable by the SBAS during these events, as they demonstrated sudden large changes in the clock or orbital behavior. Thus, it is unlikely excluding a GPS satellite based on (5) would have any noticeable effect on availability.

Given a 30 m upper bound on GPS correction error, this method would place an upper limit on the position error ranging from roughly 300 to 1500 m for L1 and 150 to 750 m for L5 for erroneous corrections caused by spoofing. However, a limitation of this approach is that it does not address the risk that erroneous ionospheric corrections may pose for the L1 service nor the risk that erroneous Galileo corrections may pose for the L5 service. Further, the spoofer may still introduce arbitrarily large errors if it exploits GEO/SBAS Satellite ranging. Still the above algorithm is very simple and does place some guardrails around the potential impact of SBAS spoofing, despite not providing complete protection.

6. OBSERVED SBAS BEHAVIOR

In this section we examine the observed behavior of the existing SBAS services to ensure that the risk of false alarms would be sufficiently low. The left side of Figure 5 shows the largest and second largest normalized projected corrections for WAAS on a typical day. The plotted data is described by

$$\frac{\left|\Delta y_j - median(\Delta y)\right|}{\sqrt{\sigma^2_{URA,j}+\sigma^2_{UDRE,j}}} \tag{6}$$

Where the blue value is the largest projected error at any given time step and the red is the second largest error at that same time step. These values are across all possible users that can see the GPS satellite above 5°, whether or not the user is under the footprint of the SBAS GEO. Further, the two data points for the same timestep in this plot are not necessarily at the same location. The user that can see this maximum second largest value, likely sees a smaller largest value. As is evident, both the largest and the second largest terms are well below the 4.42 suggested threshold. The second largest is below 1.3 for WAAS. The right side of Figure 5 shows the second largest quantity for EGNOS, MSAS, GAGAN, KASS, and South PAN for the same day using the same method. GAGAN's second largest value was just above 2 while the others were all below 1.5.

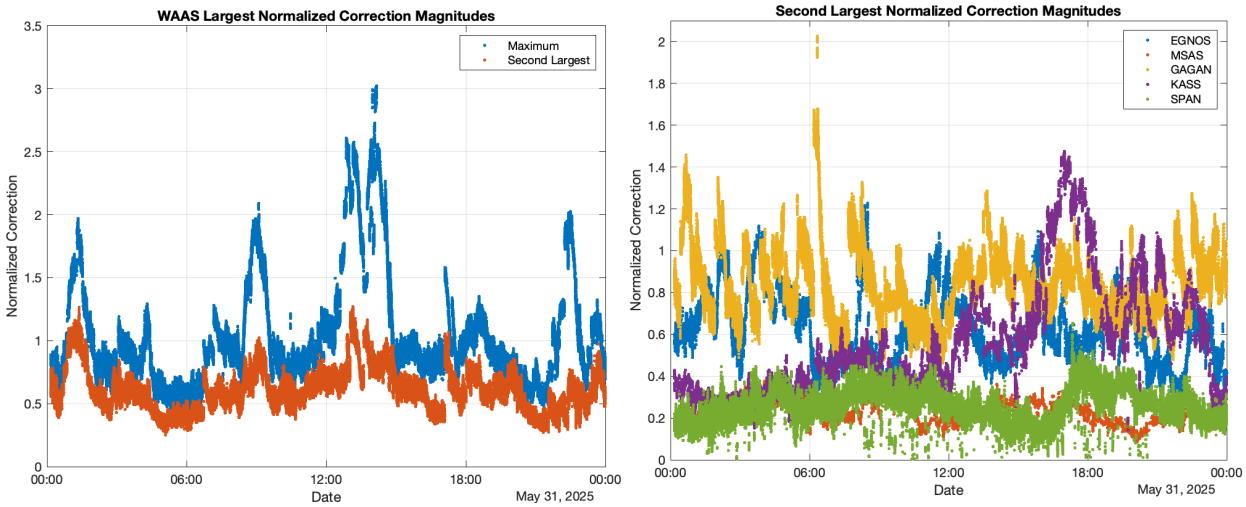

Figure 5. Largest and second largest normalized projected corrections for WAAS (left) and second largest normalized SBAS projected corrections for EGNOS, MSAS, GAGAN, KASS, and South PAN (right)

We have examined other days, included days with GPS faults, and obtained very similar upper limits on the observed second largest normalized projected error. The possibility of false alarm from unnecessarily large SBAS corrections appears to be very small, with all SBASs having values less than half of the 4.42 threshold required to trip the inequality in (4).

7. POSITION DOMAIN ALGORITHM'

The above method is very simple and sought to avoid having the receiver calculate two separate position solutions, as doing so had previously been identified as undesirable. However, should the receiver have the capability to calculate both SBAS and RAIM/ARAIM solutions at the same time, a direct comparison between the two can be very effective. RAIM/ARAIM is suggested as the comparison point as it also produces a trusted position estimate and associated protection levels. The protection levels are particularly important for defining a rigorous threshold to use for decision-making. Historically, the accuracy of SBAS and ARAIM/ARAIM solutions is substantially better than the upper bounds provided by the protection levels. However, the protection levels provide associated bounding assurances that are unlikely to lead to false alerts. For this algorithm, the receiver will calculate a position (and time) fix associated with the SBAS corrections: $\boldsymbol{x}_{SBAS}$ and one associated with the relevant Fault Detection (FD) algorithm (RAIM/ARAIM): $\boldsymbol{x}_{FD}$. These will have associated protection levels in the horizontal and vertical dimensions for given by HPL_{SBAS} & VPL_{SBAS} and HPL_{FD} & VPL_{FD}. Note that the VPLs are not always specified in the MOPS (RTCA,

2020)(EUROCAE WG-62, 2023) for all phases of flight, but nevertheless can be calculated in a similar manner to the HPLs even when in a horizontal only guidance mode (e.g. L1-only GPS RAIM).

Given that under non-adversarial conditions, the errors in $\boldsymbol{x}_{SBAS}$ are bounded by HPL_{SBAS} and VPL_{SBAS}, while the errors in $\boldsymbol{x}_{FD}$ are bounded by HPL_{FD} and VPL_{FD}, the difference between the two position estimates will then be bounded by sum of the respective protection levels. That is, when spoofing is not present, the following shall be met:

$$\sqrt{\left(x_{SBAS,E} - x_{FD,E}\right)^2 + \left(x_{SBAS,N} - x_{FD,N}\right)^2} \leq HPL_{SBAS} + HPL_{FD} \tag{7}$$

and

$$\left|x_{SBAS,U} - x_{FD,U}\right| \leq VPL_{SBAS} + VPL_{FD} \tag{8}$$

Condition (7) will be met for all horizontal flight operations and both (7) and (8) will be met for all vertical flight operations when spoofing is not present. Given that many of the underlying pseudorange errors are common mode, even tighter thresholds are certainly possible. However, to properly account for this effect, differences in which satellites are used in each position estimate, weights given to each satellite, ionospheric corrections applied, etc. must be properly modelled. This is the subject of future studies and will require a more detailed calculation. This paper will only describe the simple upper bound of adding the protection levels together.

Figure 6 shows the HPL_{FD} (left) and VPL_{FD} (right) for the L1 RAIM solution based on the MOPS 24 satellite GPS constellation. The plot shows the 99% upper bound at each user location, meaning the protection levels at those locations would be equal to or smaller than the indicated value 99% of the time. In the horizontal dimension, this is below 250 m at most locations and below 556 m at all locations. In the vertical dimension, it is below 556 m at many locations and below 1.11 km at nearly all locations. Areas with good SBAS coverage will have HPL_{SBAS} values below 40 m and VPL_{SBAS} values below 50 m. Thus, the threshold values in (7) and (8) will typically be below ~300 m and 1 km respectively. This is better than the correction domain algorithm and also covers any potential error introduced by the spoofer through ionospheric and/or SBAS satellite ranging.

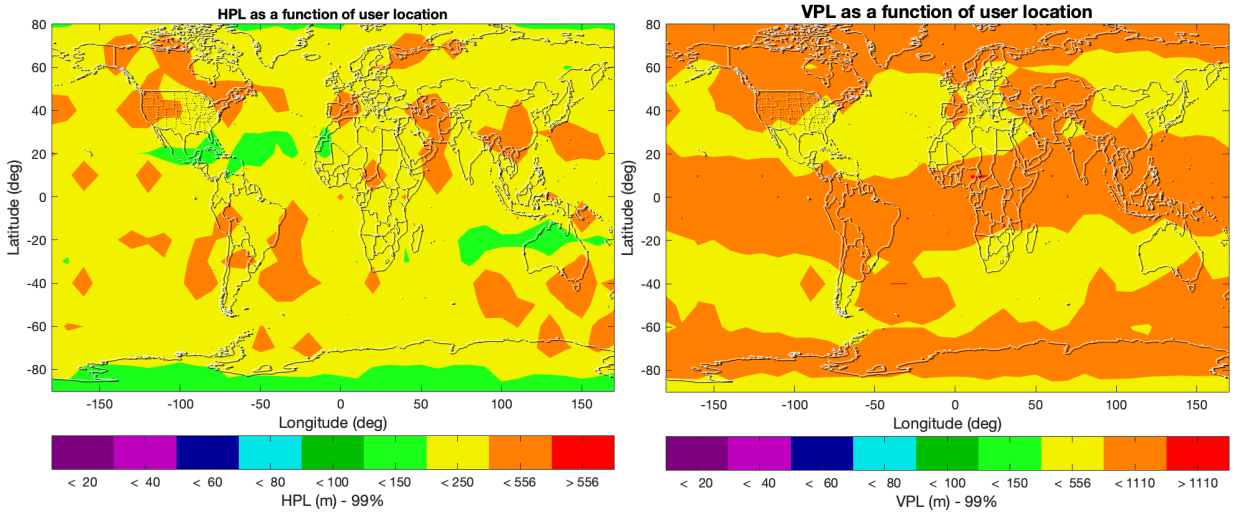

Figure 6. 99% Upper bounds on HPL_{FD} (left) and VPL_{FD} (right) for L1 – only RAIM using the MOPS 24 satellite GPS constellation

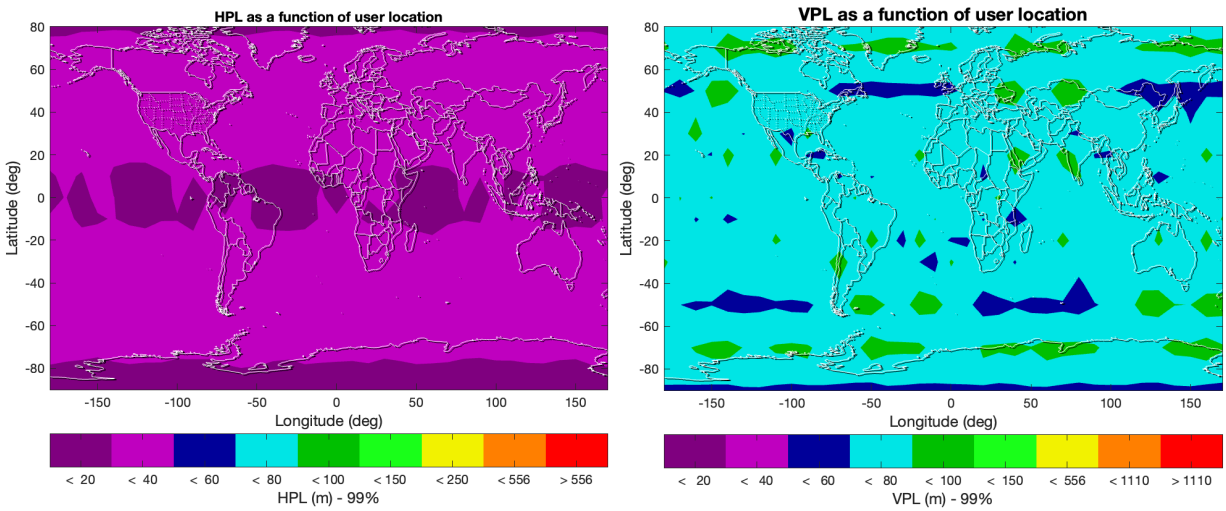

Figure 7. 99% Upper bounds on HPL_{FD} (left) and VPL_{FD} (right) for dual frequency ARAIM using the MOPS 24 satellite GPS constellation with a 24 satellite Galileo constellation

Figure 7 similarly shows the HPL_{FD} (left) and VPL_{FD} (right) for the dual frequency ARAIM solution based on the MOPS 24 satellite GPS constellation together with a 24 satellite Galileo constellation. Here the 99% bounds are substantially reduced due to the elimination of the ionospheric uncertainty and the improved satellite geometries. In the horizontal dimension, this is below 40 m at all locations. In the vertical dimension, it is below 80 m at almost locations and below 100 m at all locations. Dual frequency protection levels will also be greatly reduced, but even if we were to compare dual frequency ARAIM against L1 SBAS we would see thresholds below 80 m horizontally and 150 m vertically. This comparison significantly outperforms the L1 RAIM comparison and the correction domain algorithm

8. CONCLUSION

The proposed algorithms are both extremely simple and provide improved protection against the threat of SBAS spoofing. The correction domain algorithm is fully aligned with GPS commitments as well as expected and observed SBAS performance. While it is not feasible to validate all SBAS performances over similar time frames as we did for GPS, we believe that the proposed thresholds would rarely be exceeded and therefore the algorithm would not measurably impact operational availability or continuity. It would reduce the potential impact of L1 SBAS spoofing by at least a factor of 20 (650 m / 30 m) and provide a eight-fold reduction for L5 SBAS. The proposed correction domain algorithm and corresponding thresholds need to be evaluated by the larger GPS and SBAS community to ensure that it is compatible with current and expected system performances. This evaluation can occur over a much shorter timescale than the current path for implementing SBAS data authentication. Further, it should be fully compatible with existing SBAS receiver hardware. Therefore, it could be implemented as part of a software update to existing equipage.

The position domain algorithm requires parallel computation of the SBAS and fault detection position solutions and associate protection levels. This is marginally more computationally demanding than the correction domain algorithm but provides much better and much more complete protection against the threat of SBAS spoofing. Clearly if the receiver has the resources to implement this method, it will be the most effective.

These proposals do not obviate the need for SBAS message authentication. While the proposed algorithms significantly reduce the potential impact of SBAS spoofing, they do not ensure that spoofed position estimates will be smaller than their associated protection levels. SBAS data authentication will provide this assurance by preventing spoofers from being able to successfully inject their own corrections into SBAS receivers. Therefore, SBAS data authentication should continue to be pursued and implemented as quickly as possible. However, in the meantime, receiver manufacturers should adopt either of these approaches to provide significant protection in the nearer term.

ACKNOWLEDGEMENTS
The authors gratefully acknowledge the support by the FAA for this research under MOA # 693KA8-22-N-00015.

REFERENCES

Anderson, J. (2024). *Designing cryptography systems for GNSS data and ranging authentication*. Stanford University.

Blanch, J., Walter, T., Milner, C., Joerger, M., Pervan, B., & Bouvet, D. (2022). Baseline Advanced RAIM User Algorithm: Proposed Updates. *Proceedings of the 2022 International Technical Meeting of The Institute of Navigation*, 229–251. https://doi.org/10.33012/2022.18254

Dennis, J., Walter, T., Anderson, J., Fernandez-Hernandez, I., Canestri, E., Mabilleau, M., & Châtre, E. (2024). *SBAS Authentication Standards*. 465–481. https://doi.org/10.33012/2024.19687

EUROCAE WG-62. (2023). *ED-259A Minimum Operational Performance Standard for Galileo / Global Positioning System / Satellite-Based Augmentation System Airborne Equipment*.

European Union. (2023). *Galileo open service - Service definition document (OS SDD)* (Issue 1.3). https://doi.org/10.2878/08361

ICAO. (2023). *Annex 10 STandards and Recommended Practices (SARPS) Volume I Radio Navigation Aids*.

ICAO. (2025). *ARAIM CONOPS NSP JWGs/3 WP38*.

Lee, Y., Van Dyke, K., Decleene, B., Studenny, J., & Beckmann, M. (1996). Summary of RTCA SC-159 GPS Integrity Working Group Activities. *Navigation, Journal of the Institute of Navigation*, *43*(3), 307–338. https://doi.org/10.1002/j.2161-4296.1996.tb02579.x

RTCA. (2020). *RTCA DO-229F Minimium Operational Performance Standards (MOPS) for Global Positioning System/Satellite-Based Augmentation System Ariborne Equipment*.

US DoD. (2020). Global Positioning System Standard Positioning Service Performance Standard. In *Www.Gps.Gov* (Issue 5th Edition). https://www.gps.gov/technical/ps/

Walter, T. (2017). Satellite Based Augmentation Systems. In *Springer Handbook of Global Navigation Satellite Systems* (pp. 339–361). Springer International Publishing. https://doi.org/10.1007/978-3-319-42928-1_12

Walter, T., Blanch, J., & Enge, P. (2010). Vertical protection level equations for dual frequency SBAS. *23rd International Technical Meeting of the Satellite Division of the Institute of Navigation 2010, ION GNSS 2010*, *3*.

Zumberge, J. F., & Gendt, G. (2001). The demise of selective availability and implications for the international GPS service. *Physics and Chemistry of the Earth, Part A: Solid Earth and Geodesy*, *26*(6–8), 637–644. https://doi.org/10.1016/S1464-1895(01)00113-2