# Feasibility of fault exclusion related to advanced RAIM for GNSS spoofing detection

Heidi Kuusniemi[1], Juan Blanch[2], Yu-Hsuan Chen[2], Sherman Lo[2], Anna Innac[3], Giorgia Ferrara[1], Salomon Honkala[1], M. Zahidul H. Bhuiyan[1], Sarang Thombre[1], Stefan Söderholm[1], Todd Walter[2], R. Eric Phelts[2], Per Enge[2]

[1]Department of Navigation and Positioning, Finnish Geospatial Research Institute, Finland
[2]Stanford University, USA
[3]Parthenope University of Naples, Italy

**BIOGRAPHIES**

Prof. Heidi Kuusniemi is the Director of the Department of Navigation and Positioning at the Finnish Geospatial Research Institute (FGI). She received her doctoral degree from Tampere University of Technology (TUT), Finland, in 2005. Part of her doctoral research was conducted in the PLAN group of the Department of Geomatics Engineering at the University of Calgary, Canada. From January to March 2017 she was a visiting scholar at the GPS laboratory of Stanford University.

Dr. Juan Blanch is a senior research engineer at the Stanford GPS Laboratory, where he works on integrity algorithms for Space-based Augmentation Systems and on Receiver Autonomous Integrity Monitoring. He holds a M.Sc. in Electrical Engineering and a Ph.D. in Aeronautics and Astronautics from Stanford University.

Dr. Yu-Hsuan Chen is a research engineer at the Stanford GPS Laboratory. He received his Ph.D. in Electrical Engineering from the National Cheng Kung University, Taiwan, in 2011.

Dr. Sherman Lo is a senior research engineer at the Stanford GPS Laboratory. He received the Ph.D. in Aeronautics and Astronautics from Stanford University in 2002.

.

Dr. Anna Innac is a researcher at Parthenope University of Naples where she received her Ph.D. in June 2017. In 2016 she was a visiting researcher at the Department of Navigation and Positioning at FGI, Finland.

Ms. N. Giorgia Ferrara is a researcher at the Department of Navigation and Positioning at FGI. She received her M.Sc. degree in telecommunications engineering from the University of Catania, Italy, in 2013.

Mr. Salomon Honkala is a researcher at the Department of Navigation and Positioning at FGI. He received his M.Sc. degree from the School of Electrical Engineering, Aalto University, Finland, in 2016.

Dr. M. Zahidul H. Bhuiyan is a research manager at the Department of Navigation and Positioning at FGI. He received his doctoral. degree from the Department of Electronics and Communications Engineering at TUT, Finland, in 2011.

Dr. Sarang Thombre is a research manager at the Department of Navigation and Positioning at FGI. He received his doctoral. degree from TUT, Finland, in 2014.

Mr. Stefan Söderholm is the research group leader of the satellite and radio navigation group at the Department of Navigation and Positioning at FGI, Finland, since 2013. From 2004 he headed the Fastrax software development team, and 2008 he became Vice-President of R&D at Fastrax Ltd. Söderholm has also worked as a Project Manager in the algorithm and signal processing team at u-blox Ltd. He received his M.Sc. degree from Åbo Akademi University and his Licentiate degree from University of Turku, Finland.

Dr. Todd Walter is a senior research engineer in the GPS Laboratory in the Department of Aeronautics and Astronautics at Stanford University. He received his Ph.D. from Stanford in 1993 and has worked extensively on the Wide Area Augmentation System (WAAS). He is currently working e.g. on dual-frequency, multi-constellation solutions for aircraft guidance. He received the Thurlow and Kepler awards from the ION. In addition, he is a fellow of the ION and has served as its president.

Dr. Eric Phelts is a research engineer in the Department of Aeronautics and Astronautics at Stanford University. He received his B.S. in Mechanical Engineering from Georgia Institute of Technology in 1995, and his M.S. and Ph.D. in Mechanical Engineering from Stanford University in 1997 and 2001, respectively.

Prof. Per Enge is a professor of Aeronautics and Astronautics at Stanford University, where he is the Vance D. and Arlene C. Coffman Professor in the School of Engineering. He directs the Stanford GPS Laboratory, which develops satellite navigation systems. He has been involved in the development of the Federal Aviation Administration's GPS Wide Area Augmentation System (WAAS) and Local Area Augmentation System (LAAS). He has received the Kepler, Thurlow, and Burka Awards from the ION. He also received the Summerfield Award from the American Institute of Aeronautics and Astronautics (AIAA) as well as the Michael Richey Medal from the Royal Institute of Navigation. He is a fellow of the Institute of Electrical and Electronics Engineers (IEEE), a fellow of the ION, a member of the National Academy of Engineering, and has been inducted into the Air Force GPS Hall of Fame. He received his Ph.D. from the University of Illinois in 1983.


## ABSTRACT

This paper will present an exercise to verify the usefulness of statistical testing of measurement residuals of an overdetermined position solution followed by measurement subset selection for spoofing detection and mitigation for certain spoofing events, to be especially beneficial when multi-GNSS is considered. Tests include utilizing dynamic GPS spoofing data from the TEXBAT testing battery. We will present that Advanced RAIM (Receiver Autonomous Integrity Monitoring) has benefits for spoof detection. RAIM is designed to catch inconsistencies in range measurements and is thus useful in defeating a surreptitious lift off spoofing attack. Inconsistencies in a lift off attack exist when the spoof signal mixes with the genuine signal of similar power levels (within a few dB). The mixing creates some measurements from genuine signals and some from the spoofed signals. ARAIM cannot however mitigate across all categories of spoofers and hence should not represent a stand-alone spoofing solution. Although pre- and post-correlation signal processing is definitely the most efficient way to detect and mitigate spoofing effects, checking the measurements in the navigation domain is not a lost cause, as presented herein.


## INTRODUCTION

In safety of life applications such as civil aviation or positioning of automated vehicles, integrity of the navigation functionality is of utmost importance. Global Navigation Satellite System (GNSS), the global and prevailing technology providing position, velocity and timing (PVT) capability, is however vulnerable to unintentional or malicious interference. Though GNSS jamming is generally a more widespread harm, spoofing is also a more and more encountered means of intentional interference where synthetic GNSS signals are being broadcast to try and trick a GNSS receiver into using false signals and obtaining an incorrect position and time solution. Spoofing totally breaks the reliability and integrity of the PVT solution. Reliability testing in the form of Receiver Autonomous Integrity Monitoring (RAIM) traditionally relies on statistical tests in order to isolate one erroneous measurement from position estimation and insuring solution integrity. Recursive statistical testing, where faults are identified one by one iteratively, can on the other hand handle multiple faults, also considering multi-frequency multi-system situations - particularly in challenging signal environments. In this paper, we look into the feasibility of such statistical testing for spoofing detection.

This paper investigates the feasibility of a fault exclusion methodology related to advanced RAIM, discussed extensively in [1], [27] and in the recent report [2], for detecting GNSS spoofing and therefore ensuring solution integrity for safety critical systems. Test results of this reliability monitoring applicability for spoofing detection will be demonstrated on a dynamic case from the standard spoofing evaluation toolkit of the Texas Spoofing Test Battery datasets described in, e.g., [3, 4, 5].

## METHODOLOGY

GNSS signal interference is a growing threat throughout disciplines worldwide. Various applications heavily rely on reliable location and time derived from satellite navigation, ranging anywhere from different transport modes, time synchronization, emergency services to scientific applications and precision agriculture. This section looks at the spoofing attacks in more detail threatening all these various applications and how they typically are fought against. Thereafter, it discusses reliability monitoring and its fault exclusion functionality that will be applied for spoofing detection in a dynamic scenario.

### *A. Spoofing techniques*

Spoofing is realized by transmitting false GNSS signals at a sufficient power to overcome the authentic signal. We can classify spoofing by characterizing the mechanism by which each component of a spoofing attack is generated. Two essential dimensions of a spoofed attack are signal generation (code, data) and capture. These dimensions and categories within them are shown in Figure 1 and discussed below.

The methods of generating the spoofing signal (signal generation) can be broadly divided into meaconing, simulator-based spoofing or receiver-based spoofing. In meaconing the GNSS signals are recorded and simply replayed after a set delay. In this case, the position computed by the target receiver will be that of the spoofer. This basic meaconing technique, while capable of spoofing encrypted signals, cannot generate an arbitrary trajectory. A more sophisticated meaconing attack is to use antenna

arrays to separate individual satellite signals and rearrange them. We classify this as a meacon attack as the bits are never estimated so the signal generation is analog. Once the signal is processed and used for spoofing, then we enter the realm of receiver-based spoofing.

As the civil GNSS signals are unencrypted and their signal specifications are public, anyone can produce signals which are identical to real ones. In simulator-based spoofing, a GNSS simulator can be used to replicate the signals as they would appear at a chosen location, misleading the receiver to produce an incorrect PVT solution.

In receiver-based spoofing, in order to capture and then drag-off the victim receiver's tracking loops, a spoofer makes use of a GNSS receiver. The receiver processes the authentic GNSS signals to extract the position, time and ephemeris, and the spoofing transmitter generates more plausible counterfeit signals with code phase and Doppler shift matching the true ones at the target's position. In this case, the spoofer requires knowledge of the victim receiver's relative position. A more sophisticated attack can be performed by transmitting the negative of the authentic signal, and hence cancelling it out. This type of attack is, however, difficult to realize as it requires also exact signal amplitude and carrier phase matching. Receiver-based spoofing attacks may be used on encrypted signals by estimating the encrypted code or data bits. A detailed description of the different spoofer attack strategies can be found in e.g. [6].

Signal injection is the means by which the spoofer overcomes or captures the target receiver. Common ways include: 1) direct injection, 2) overpower (such as jam and overpower) and 3) lift off. In direct injection, the spoofer is plugged directly to the receiver's antenna port. In an overpower attack, the spoofer overwhelms the genuine signal with a much more powerful signal. In a lift off attack, the spoofer matches the existing signal and then surreptitiously increases power to carry off the receiver tracking loops. This attack requires significant planning, sophistication and knowledge as the received spoofed signal needs to match the genuine signal while its power is at or just slightly above that of the genuine signal

Of course, there are other characteristics such as transmission mechanism and generation of spoofed PVT. Transmission mechanism is how the spoofing signal is transmitted. Most attacks will likely be made with a single antenna on the ground. However more sophisticated attacks may use direction, moving or multiple antennas and even multiple mobile or airborne antennas that can simulate the constellation geometry. Generation of spoofed PVT is what information is used to create a spoofed PVT. It can be 1) open loop (no outside information), 2) knowledge of initial state and 3) continuous knowledge.

| Signal Input | Replay on-air signal | Separate & replay on-air signal | Receiver-based spoofing | Simulator-based spoofing |
|---|---|---|---|---|
| Direct Injection | Limpet meacon | Sophisticated limpet meacon | Limpet spoofer [41] | Limpet spoofer |
| Overpower | Meaconing | Sophisticated meaconing | Overpower using [37] | Spoofing [38, 39] |
| Jam & Spoof | Jam, then meacon | Jam, then meacon | Jam spoofing | Jam spoofing in Black Sea [40] |
| Lift off | N/A | Lift off using on air signal | UT Austin spoofer [37] | N/A |

Signal (Code/Data) Generation

Figure 1. Characterizing spoofing by how it is generated and how it is transmitted (input) with examples of each (N/A means that there is no spoofing threat that is likely or applicable in this category)

### *B. Typical detection methods*

In order to ensure the integrity of the GNSS-based solution in the presence of spoofing, defense techniques that reveal the spoofer attacks must be adopted. Several strategies have been developed as a response to the spoofing threat, and a simplistic overview of them is provided in Figure 2. Four main categories can be identified: 1) cryptographic approaches, 2) methods

based on signal features and receiver behavior discontinuities, 3) techniques utilizing auxiliary navigation and positioning technologies, and 4) methods based on signal spatial and geometrical properties.

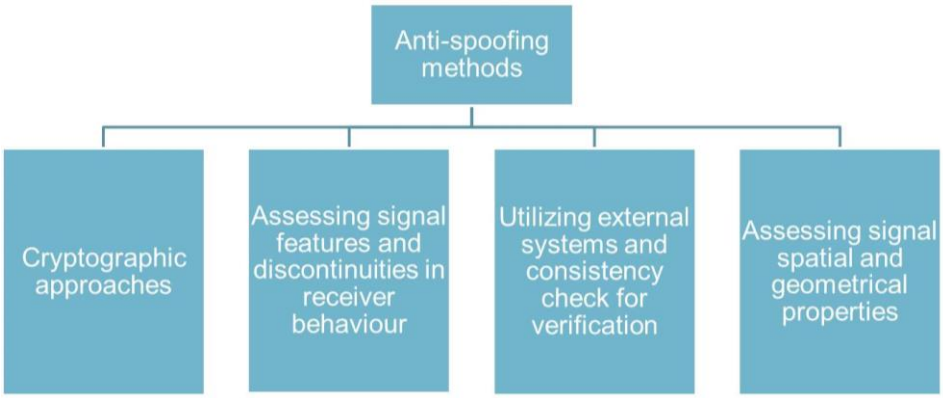


Figure 2. Brief overview of spoofing detection methods.

Cryptography is a very effective but not easily feasible countermeasure. Signal encryption generates an unpredictable version of the Pseudo-Random Noise (PRN) code or navigation message difficult for the spoofer to reproduce, but requires knowledge of the secret key at the receiver. Furthermore, modifications in the civil signal structure will need to be made. If an encrypted/military signal component is present at the same frequency, spoofing detection can be performed without the need to know the secret key at the receiver and change the civil signal structure. The publicly-known signal tracking data is used to isolate the part of the received signal that is encrypted, which is then compared to the encrypted signal stored at a reference receiver [7, 8, 29, 30]. However, in this case, a reference receiver and a communication link are required. Cryptographic approaches can also be authentication-based [9, 10], where specific signal features, such as the presence of random-like sequences in the PRN code or navigation message, are used as authentication keys to establish whether or not the received signal is trustworthy.

Several anti-spoofing techniques are based on monitoring signal features. Unless the spoofer is able to generate a phase-aligned nulling signal, residual authentic GNSS signal components remain in addition to the counterfeit signals. This causes a distortion in the correlation function that can be used as an indicator for detecting spoofing incidents [11, 12, 13]. Moreover, since, in the presence of spoofing, unusual changes may occur in the clock bias or in the Automatic Gain Control (AGC) value, spoofing detection can be performed by assessing discontinuities in the receiver behavior.

A third category of anti-spoofing approaches is based on the comparison of the GNSS PVT solution with one obtained by external systems providing location information, such as cellular networks, WiFi access points, and inertial measurement units (IMU). Inconsistent results would reveal a spoofing attack. Finally, spoofing detection can be done efficiently by assessing the signal spatial and geometrical properties. Genuine GNSS signals arrive from different directions from the various satellites in view, while counterfeit signals are usually broadcast by a single source. Examples of techniques based on monitoring the signals' direction of arrival can be found in [14, 15, 16].

### *C. Reliability monitoring*

Receiver Autonomous Integrity Monitoring (RAIM) algorithms are typically based on consistency testing of redundant measurements through a statistical hypothesis test of the Least Squares (LS) residuals, e.g. [17]-[22]. The statistical test assumes a null hypothesis $H_0$, denoting a fault-free situation, related to the probability distribution of a random variable. The null hypothesis represents the reference level from which any deviation of the alternative hypotheses ($H_a$) has to be detected by statistical tests. For any $H_0$, there is an infinite number of $H_a$ that is a statement in contradiction to the null hypothesis. To detect blunders influencing the set of measurements, residuals should thereby be statistically tested.

In the consistency test of (1), often denoted as the global test (GT) or the chi-square goodness-of-fit test, a simple consistency investigation is performed by assessing the distribution of the residuals. Thus, the GT includes comparing the weighted sum of the squared residuals, representing the decisional variable $T$ or test statistic, to a $\chi^2$-distribution:

$$H_a: (reliability\ failure)$$
$$T = \mathbf{v}_k^T \mathbf{R}^{-1} \mathbf{v}_k > \chi^2_{1-\alpha,n-p} \quad (1)$$

where

**R** Covariance matrix of the observations

α False alarm rate

$n$ Number of observations
$p$ Number of unknowns
$\mathbf{v}_k$ Range residuals defined as the differences between the expected measurements and the actual measurements.

If the statistical variable is larger than the threshold as in (1), the sum-of-squares of the residuals $T$ does not follow the expected distribution, consisting of a sum of squares of zero-mean Gaussians, and the null hypothesis $H_0$ is rejected in favour of $H_a$. If $H_0$ is rejected and $H_a$ accepted, the result of the GT is an inconsistency in the measurement set followed by closer data snooping, e.g. [23], or measurement subset testing to search for and eliminate blunders.

### *D. Fault exclusion related to ARAIM*

Advanced RAIM (ARAIM), e.g. [1, 2], is a fairly recently introduced method to realize integrity monitoring in multi-constellation satellite navigation algorithmically. ARAIM must be able to detect all hazardous faults in the underlying GNSSs within seconds. ARAIM can be divided into Horizontal, Offline and Online ARAIM depending on the essential integrity support message involved. ARAIM has many elements [24, 25], namely the integrity support message processing, the protection level calculation and the fault detection and exclusion (FDE). Here, the focus is on a variant of its FDE functionality and how it could be applied to spoofing detection and mitigation. We adopt a fault exclusion procedure based on a snapshot statistical scheme from least squares position estimation and focus on the assessment of single epoch solutions with only the current redundant measurements being used in the self-consistency check. The implemented algorithm consists of a geometry check step and subsequently the application of an observation subset testing procedure as the implemented FDE scheme, which is an exhaustive search for a fault-free measurement subset.

A feasibility geometry check is also put in place in the fault exclusion scheme, as presented in Figure 3. In harsh signal environments, poor satellite geometry may cause large dilution of precision (DOP) values and influence the navigation accuracy and redundancy [22]. Large errors can occur before the outliers are detected and a geometry check will thus screen out the poor geometries, which could imply erroneous detection. In [32], a geometry DOP (DOP) control scheme is applied. Here, if the measurement set passes a geometry check, i.e. its geometry is strong enough when looking at its horizontal protection level (HPL), subset testing, also discussed in [33], is applied for the goodness-of-fit detection and the exclusion of faulty measurements. Subset testing is here based uniquely on the GT, which is used to find the measurement subset without any blunders. If the all-in-view measurement set does not satisfy the GT, all the possible combinations of measurements are analysed, specifically all the possible subsets from $(n - 1)$ to $(p + 1)$ measurements. The subset with the smallest test-passing test statistic and the largest number of observations is selected for the computation of the navigation solution. The full scheme is shown in Figure 3. The subset testing procedure is computationally heavy as it is an exhaustive search where all combinations have to be checked. For multi-GNSS, a faster approach is necessary, such as the greedy search or the L1 norm minimization [26].

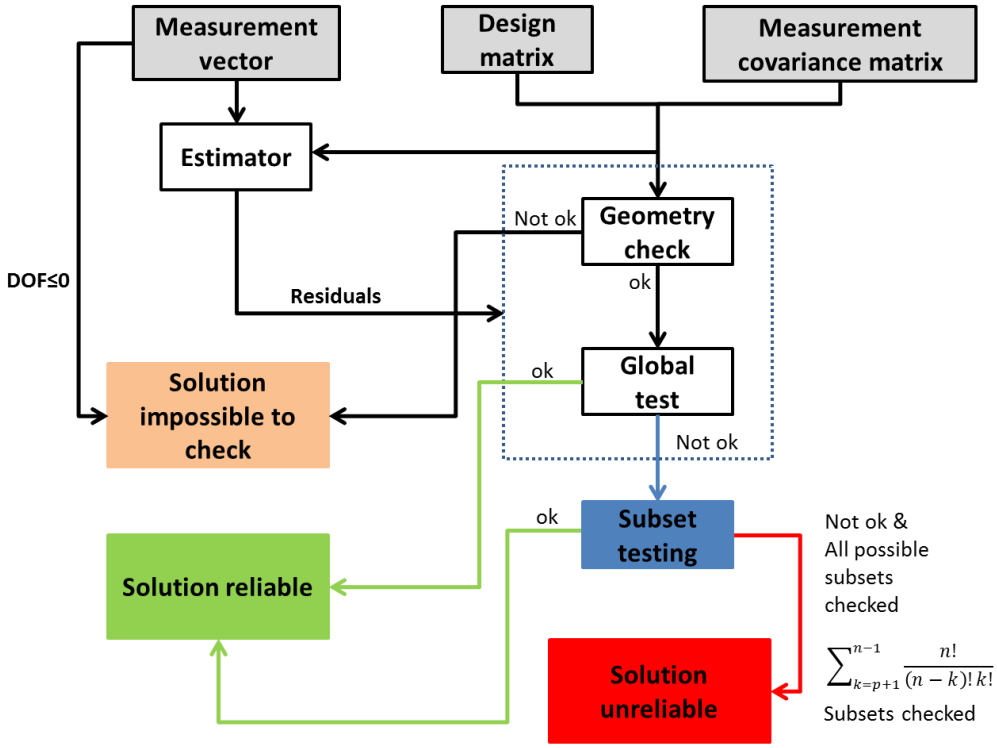


Figure 3. The Subset Testing algorithm (where *n* is the number of measurements, *p* is the number of unknowns, *k* is the number of excluded measurements and DOF the degrees of freedom)

### *A. Using ARAIM for spoof detection*

ARAIM has significant benefits also for spoof detection. It is designed to catch inconsistencies in range measurements and is thus useful in defeating a surreptitious lift off attack. Inconsistencies in lift off attack exist when the spoof signal mixes with genuine signal of similar power levels (within a few dB). The mixing creates some measurements from genuine signals and some from the spoofed signals. ARAIM is also suitable for implementation in most receivers as it uses existing receiver outputs (pseudoranges) and does not require significant computational capabilities. ARAIM and RAIM algorithms may already exist within the receiver for consistency checks and measurement selection, e.g. as presented by Septentrio in [31]. ARAIM is primarily being developed for aviation navigation [1].

ARAIM cannot mitigate across all categories of spoofers and hence should not represent a stand-alone spoofing solution. For example, if the spoofer can greatly overpower the genuine signal in capturing the user receiver, then inconsistent measurements may not exist, as also discussed later on in this paper. But while ARAIM can be foiled by an overpower attack, signal power checks using automatic gain control (AGC) and carrier-to-noise ratio ($C/N_0$) can detect these [34][35]. In fact, having these signal power checks forces a spoofing at a power level that can result in inconsistencies. Hence, this combination makes for a powerful spoof detection mechanism and it is assumed that ARAIM is used in conjunction with signal power checks.

## EXPERIMENTAL RESULTS

The verification of the subset testing, i.e. the exhaustive search, for detection of certain types of spoofing incidents is performed by using a dynamic GPS spoofing dataset published by the University of Texas at Austin, the **ds5** [4], which is a dynamic dataset with an over-powered time push spoofing being performed (9.9 dB power advantage). The TEXBAT datasets contain digital signal recordings of spoofing attack scenarios, intended for testing spoof resistance in civil GPS receivers. The spoofing device used is a receiver-based spoofer which generates GPS L1 C/A signals that are code-phase aligned with the authentic signals at the target location, and contain predicted navigation data bits. The challenge of spoofing detection on a dynamic platform is to distinguish spoofing effects from multipath.

Figure 4 presents how the subset testing (RAIM/FDE) presented in Figure 3 improves the 3D RMS (root mean square) error significantly in the dynamic spoofing scenario ds5 and Figure 5 shows the related groundplot in an East-North coordinate frame. Spoofing kicks off at around 170 s from the beginning of the test. The FDE significantly improves the accuracy due to measurement exclusions, from a maximum horizontal accuracy of nearly 450 m to 16 m. Figure 6 shows the range residuals experienced in the navigation filter when no FDE procedure is being implemented, highlighting the erroneous measurements

present due to the spoofing, and Figure 7 presents the case with FDE applied – largest erroneous observations having been removed from the solution. Figure 8 presents the number of exclusions resulting from the FDE procedure undertaken, up to 4 measurements. The FGI-GSRx (FGI's GNSS Software Receiver) receiver is used here for acquisition, tracking and navigation for the ds5 dataset. The FGI-GSRx is a Matlab-based software receiver research tool [28]. Analysis was also performed with measurements obtained from a commercial receiver by Septentrio Ltd. under this scenario (RINEX data observations processed in the FGI-GSRx navigation engine). Results with the Septentrio observations with and without the FDE scheme of Figure 3 are presented in Figures 9 and 10. Figure 9 shows the 3D RMS error and Figure 10 the groundplot in an East-North reference frame with the Septentrio observations, presenting the improvement provided by the analysed measurement exclusion procedure. Figure 10 includes also the internal Septentrio navigation result showcasing the excellent performance of a commercial receiver with spoofing resistance, portraying similar results as to when RAIM/FDE is applied in the FGI-GSRx navigation engine. With the FGI-GSRx software platform, however, whether it is with its own observations or Septentrio observations fed into the navigation engine, we can flexibly analyze the benefit of measurement exclusion via the accuracy improvement of the subset testing. The FGI-GSRx navigation engine is not optimized for the Septentrio observations (visible before the spoofing starts) and would need additional work to have improved results.

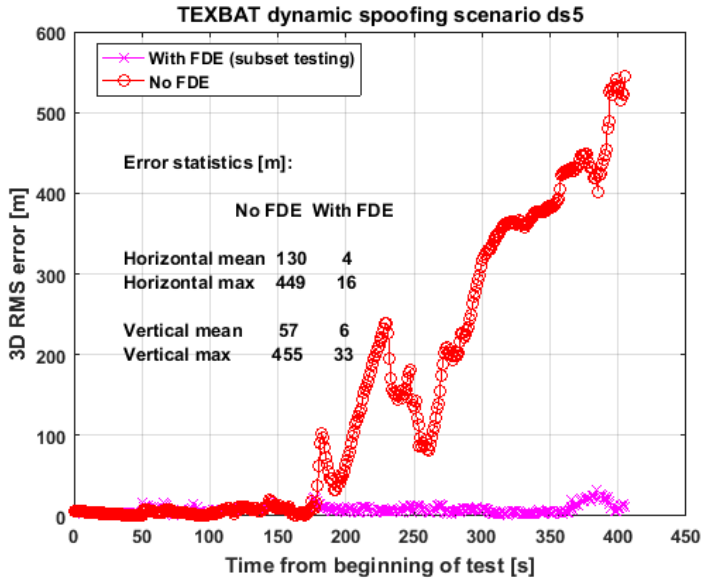


Figure 4. 3D RMS error of the ds5 dynamic scenario with the FGI-GSRx sw receiver with and without RAIM/FDE applied

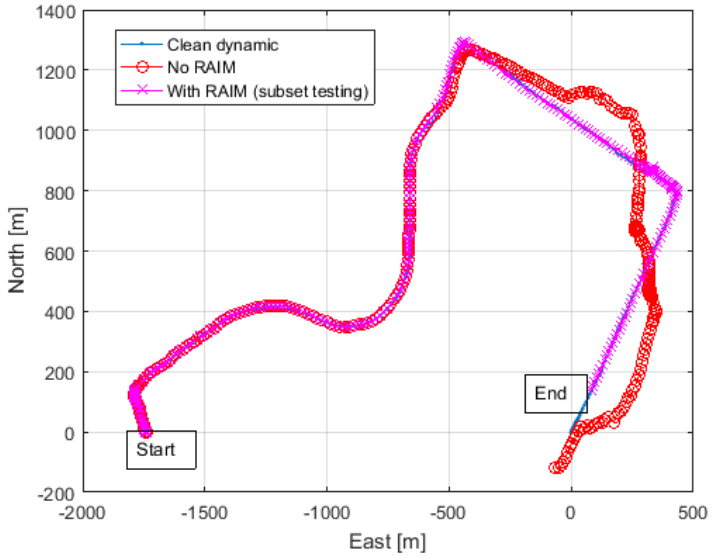


Figure 5. Groundplot of the ds5 dynamic scenario with the FGI-GSRx sw receiver with and without RAIM/FDE applied

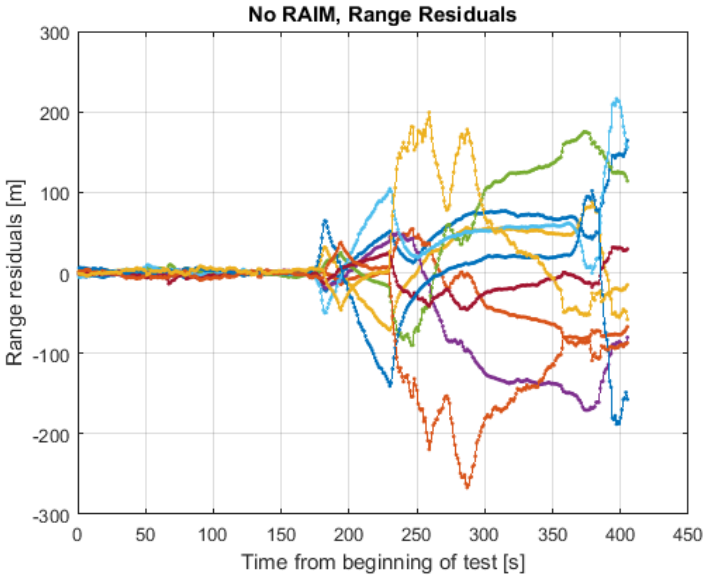


Figure 6. Range residuals with the FGI-GSRx of the ds5. Spoofing begins at around 170 s from the beginning of the test.

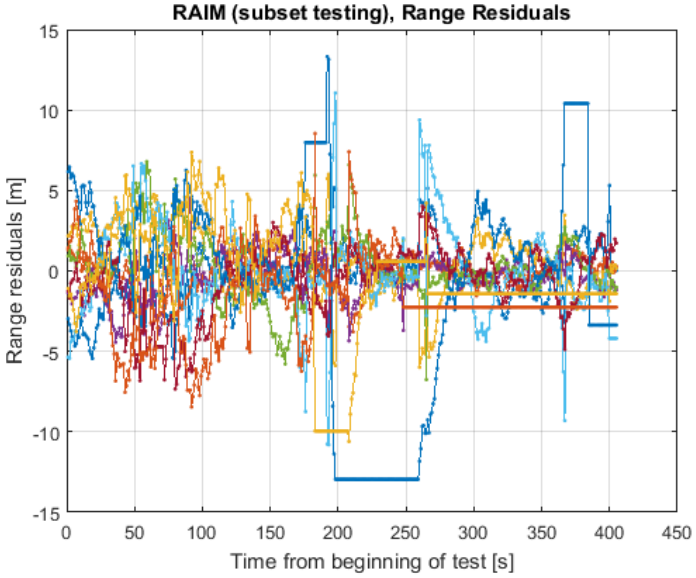


Figure 7. Range residuals with the FGI-GSRx of the TEXBAT ds5 and RAIM/FDE being implemented

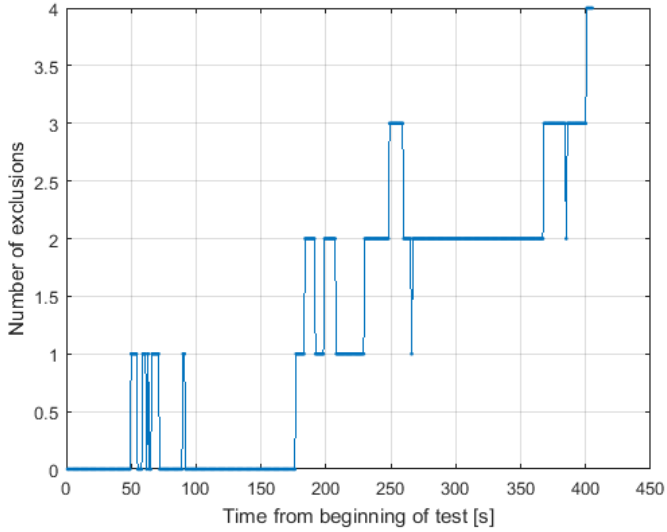


Figure 8. Measurement exclusions performed in the FDE procedure/subset testing with the FGI-GSRx of the TEXBAT ds5 dynamic scenario

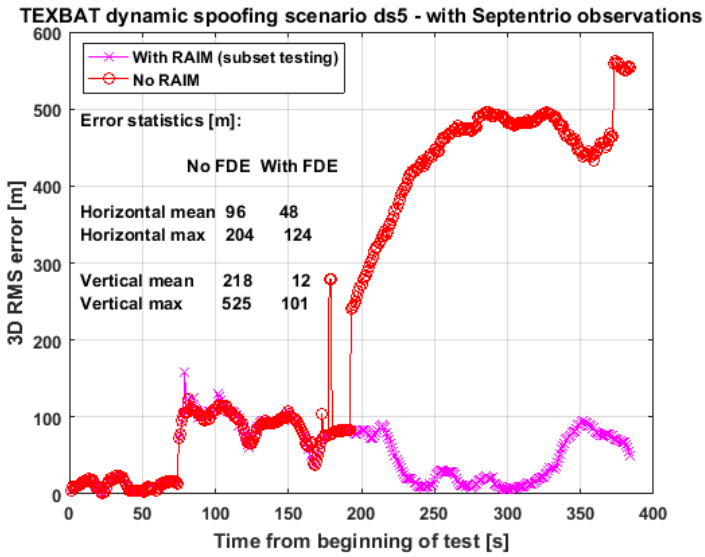


Figure 9. 3D RMS error of the TEXBAT ds5 dynamic scenario with the FGI-GSRx software receiver's navigation utilizing Septentrio observations (Rinex) with and without RAIM/FDE applied

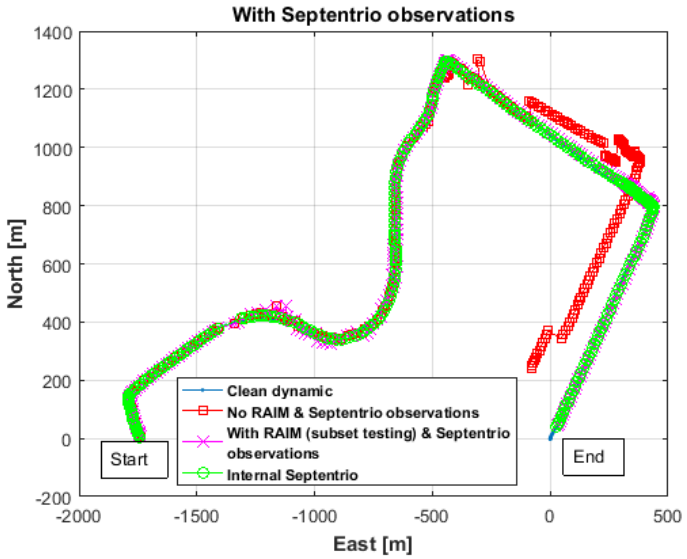


Figure 10. Groundplot of the TEXBAT ds5 dynamic scenario with the FGI-GSRx software receiver's navigation utilizing Septentrio observations (Rinex) with and without RAIM/FDE applied – also internal Septentrio result shown (green)

The ds5 is a frequency "unlocked" scenario where the code and carrier are not always moving at the same rate. This might be why the ds5 may be easier to detect with inconsistency testing. Namely, we did also look at another dynamic TEXBAT spoofing scenario, the ds6 where the frequency is locked and nearly power matched (0.8 dB spoofer advantage). The Subset testing FDE procedure did not improve performance at all with consistency testing and measurement exclusions, on the contrary - as shown in Figure 11. This results from 2 to 4 measurement exclusions out of up to 11. Thus, consistency testing is only marginally useful for mitigation, especially without any power checks or other detection and mitigation efforts for spoofing, that are all broadly discussed in e.g. [5]. However, ARAIM fulfilled its primary purpose of spoof detection in ds6. It did determine there were inconsistent measurements present, which already is useful information for spoof detection.

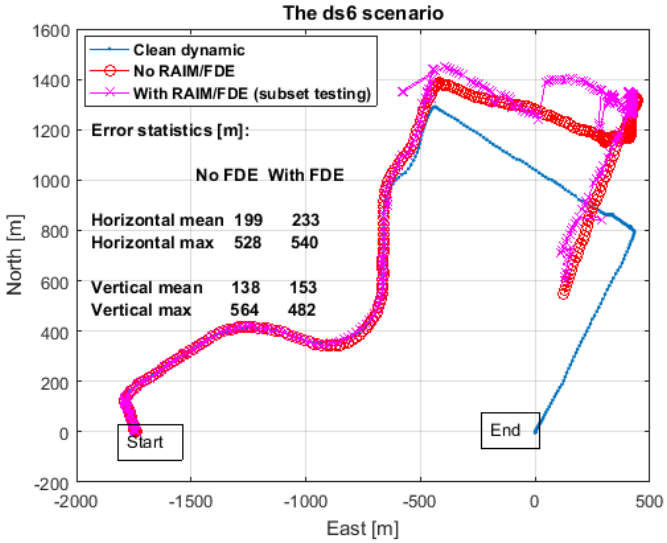


Figure 11. Groundplot of the TEXBAT ds6 dynamic scenario with the FGI-GSRx software receiver with and without RAIM/FDE applied, performance is worse

## CONCLUSIONS

This paper presented an exercise to assess the usefulness of statistical testing of measurement residuals of an overdetermined position solution followed by measurement subset selection for spoofing detection and mitigation for certain spoofing events especially when multi-GNSS is considered. Tests include utilizing a dynamic GPS spoofing dataset from the TEXBAT testing battery. ARAIM's FDE being used in conjunction with the important signal power checks can thus be beneficial in identifying spoofing presence and mitigating the effects. Future work looks into assessing true multi-constellation spoofing scenarios with spoofing signals at such power levels not to trigger power-level checks but benefiting from the inconsistency testing feasible to be implemented in the navigation filter. Future work will also include closer investigations of the overall limitations of consistency testing in various spoofing scenarios. One case is the probability of false alert, especially in the presence of natural phenomena such as scintillation and multipath.

## ACKNOWLEDGMENTS

This work is part of the project INSURE (Information Security of Location Estimation and Navigation Applications) funded by the Academy of Finland (Grant No. 303575), www.insure-project.org, and its research mobility period to Stanford University's GPS Laboratory.

## REFERENCES

[1] Blanch, J., Walter, T., Enge, P., Lee, Y., Pervan, B., Rippl, M., Spletter, A., "Advanced RAIM user Algorithm Description: Integrity Support Message Processing, Fault Detection, Exclusion, and Protection Level Calculation," Proc. of ION GNSS 2012, Nashville, TN, September 2012, pp. 2828-2849.

[2] EU-U.S. Cooperation on Satellite Navigation Working Group C-ARAIM Technical Subgroup Milestone 2 Report, available at http://ec.europa.eu/growth/tools-databases/newsroom/cf/itemdetail.cfm?item_id=8191

[3] Lemmenes A. , P. Corbell, and S. Gunawardena, "Detailed Analysis of the TEXBAT Datasets Using a High Fidelity Software GPS Receiver", Proc. ION GNSS+ 2016, Portland, OR, 2016, pp. 3027-3032.

[4] Humphreys T.E., J.A. Bhatti, D.P. Shepard, and K.D. Wesson, "The Texas Spoofing Test Battery: Toward a Standard for Evaluating GPS Signal Authentication Techniques," Proc. ION GNSS, Nashville, TN, 2012, pp. 3569 - 3583.

[5] Esteban Garbin Manfredini, *Signal processing techniques for GNSS anti-spoofing algorithms*, Doctoral Dissertation, Politecnico di Torino, May 2017.

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

[7] Psiaki M.L. , B. W. O'Hanlon, J. A. Bhatti, D. P. Shepard, and T. E. Humphreys, "Civilian GPS spoofing detection based on dual-receiver correlation of military signals," in *IEEE Transactions on Aerospace and Electronic Systems*, vol. 49, no. 4, pp. 2250-2267, October 2013.

[8] O'Hanlon B.W., M. L. Psiaki, J. A. Bhatti, D. P. Shepard, and T. E. Humphreys, "Real-time GPS spoofing detection via correlation of encrypted signals," *NAVIGATION*, Journal of The Institute of Navigation, vol. 60, no. 4, pp. 267-278, 2013.

[9] Wesson K., M., Rothlisberger, and T. Humphreys, "Practical cryptographic civil GPS signal authentication," *NAVIGATION*, Journal of The Institute of Navigation, vol. 59, no. 3, pp. 177–193, Fall 2012.

[10] Wesson K., M. P., Rothlisberger, and T. E. Humphreys, "A proposed navigation message authentication implementation for civil GPS antispoofing, " in Proc. of the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS), Portland, OR, Sep. 2011, pp. 3129 – 3140.

[11] Wesson K., D. P. Shepard, J. A. Bhatti, T. E. and Humphreys, T. E., "An evaluation of the vestigial signal defense for civil GPS anti-spoofing," in Proc. of the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS), Portland, OR, Sep. 2011, pp. 2646 – 2656.

[12] Ali K., E. G. Manfredini, and F. Dovis, "Vestigial signal defense through signal quality monitoring techniques based on joint use of two metrics," IEEE/ION Position, Location and Navigation Symposium-PLANS 2014. IEEE, 2014.

[13] Falletti E., B. Motella, and M. Troglia Gamba, "Post-correlation signal analysis to detect spoofing attacks in GNSS receivers," Signal Processing Conference (EUSIPCO), 2016 24th European. IEEE, 2016.

[14] Borio D. and C. Gioia, "A sum-of-squares approach to GNSS spoofing detection," in *IEEE Transactions on Aerospace and Electronic Systems*, vol. 52, no. 4, pp. 1756-1768, August 2016.

[15] Psiaki M.L., B. W. O'Hanlon, S. P. Powell, J. A. Bhatti, K. D. Wesson, T. E. Humphreys, and A. Schofield, A., "GNSS spoofing detection using two-antenna differential carrier phase," in Proc. of the 27th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+), Tampa, Florida, Sep. 2014, pp. 2776–2800.

[16] McMilin E.. Single Antenna Null-Steering for GPS and GNSS Aerial Applications, Ph.D. Dissertation, Stanford University, 2016. Available at: http://web.stanford.edu/group/scpnt/gpslab/pubs/theses/EmilyMcmilinThesis2016.pdf

[17] GPS, Global Positioning System: Papers Published in NAVIGATION (RAIM: Requirements, Algorithms, and Performance)," Volume V, Institute of Navigation (ION) RedBook, 1998

[18] Blanch J.A., Walter, Todd F., and Enge, Per K, "RAIM with Optimal Integrity and Continuity Allocations Under Multiple Failures", in *IEEE Transactions on Aerospace and Electronic Systems*, Vol. 46, No. 3, July 2010, pp. 1235-47.

[19] Kuusniemi, H., "User-Level Reliability and Quality Monitoring in Satellite-Based Personal Navigation" PhD thesis, Tampere University of Technology, Finland, 2005. Publication 544

[20] Castaldo G., A. Angrisano, S. Gaglione, and S. Troisi, "P-RANSAC: An Integrity Monitoring Approach for GNSS Signal Degraded Scenario," International Journal of Navigation and Observation, vol. 2014, Article ID 173818, 11 pages, 2014. doi:10.1155/2014/173818

[21] Angrisano A., C. Gioia, S. Gaglione, and G. del Core, "GNSS Reliability Testing in Signal-Degraded Scenario," International Journal of Navigation and Observation, vol. 2013, Article ID 870365, 12 pages, 2013. doi:10.1155/2013/870365

[22] Innac A., M.Z.H. Bhuiyan, S. Söderholm, H. Kuusniemi, and S. Gaglione, "Reliability testing for multiple GNSS measurement outlier detection", in: Proceedings of European Navigation Conference (ENC) 2016, 30th May-2nd June 2016, doi:10.1109/EURONAV.2016.7530540

[23] Baarda W., "A Testing Procedure for Use in Geodetic Networks, Netherlands Geodetic Commission", Publication on Geodesy, New Series 2, 5, Delft, The Netherlands, 1968.

[24] Blanch, J., Walter, T., Enge, P., "Exclusion for Advanced RAIM: Requirements and a Baseline Algorithm," *Proceedings of the 2014 International Technical Meeting of The Institute of Navigation*, San Diego, California, January 2014, pp. 99-107.

[25] Chen, Yu-Hsuan, Perkins, Adrien, Lo, Sherman, Akos, Dennis M., Blanch, Juan, Walter, Todd, Enge, Per, "Demonstrating ARAIM on UAS using Software Defined Radio and Civilian Signal GPS L1/L2C and GLONASS G1/G2," *Proceedings of the 2016 International Technical Meeting of The Institute of Navigation*, Monterey, California, January 2016, pp. 231-238.

[26] Brown R.G. and G. Y. Chin, "GPS RAIM: calculation of threshold and protection radius using chi-square methods-a geometric approach", Global Positioning System: Institute of Navigation, vol. 5, pp. 155–179, 1997.

[27] Blanch, J., Walter, T., Enge, P., "Fast Multiple Fault Exclusion with a Large Number of Measurements," Proceedings of the 2015 International Technical Meeting of The Institute of Navigation, Dana Point, California, January 2015, pp. 696-701.

[28] Söderholm, S., Bhuiyan, M. Z. H., Thombre, S., Ruotsalainen, L., and H. Kuusniemi (2016). A Multi-GNSS Software-defined Receiver: Design, Implementation and Performance Benefits. Annals of Telecommunications, pp. 1-12, DOI: 10.1007/s12243-016-0518-7.

[29] Levin; P., De Lorenzo; D. S., Enge; P. K., Lo; S. C., "Authenticating a signal based on an unknown component thereof," June 28 2011, US Patent # 7,969,354.

[30] Lo, Sherman, David DeLorenzo, Per Enge, Dennis Akos, Paul Bradley, "Security for Civil GNSS," InsideGNSS, September/October 2009

[31] Van Hees, J., Boon, F., Jacobs, P., Kleijer, F., Viana, J., Durinck, B., Simsky, A., "The Triple-frequency Multi-system RTK Engine for Challenging Environments," Proceedings of the 27th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2014), Tampa, Florida, September 2014, pp. 69-99.

[32] Zhu, Ni, Marais, Juliette, Bétaille, David, Berbineau, Marion, "Evaluation and Comparison of GNSS Navigation Algorithms including FDE for Urban Transport Applications," *Proceedings of the 2017 International Technical Meeting of The Institute of Navigation*, Monterey, California, January 2017, pp. 51-69.

[33] Berardo, M., & Lo Presti, L. (2016). On the Use of a Signal Quality Index Applying at Tracking Stage Level to Assist the RAIM System of a GNSS Receiver. *Sensors (Basel, Switzerland), 16*(7), 1029. http://doi.org/10.3390/s16071029

[34] Borowski H., O. Isoz, F. M. Eklöf, S. Lo, D. Akos, "Detection of False GNSS Signals using AGC," GPS World, April 2012.

[35] Gross J., T. E. Humphreys, "GNSS Spoofing, Jamming, and Multipath Interference Classification using a Maximum-Likelihood Multi-Tap Multipath Estimator," Proceedings of ION ITM 2017, Monterey, CA, USA, Jan 2017.

[36] T.E. Humphreys, B.M. Ledvina, M.L. Psiaki, B.W. O'Hanlon, P.M Kintner, Jr., "Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer," Proceedings of ION GNSS, The Institute of Navigation, Savanna, Georgia, 2008.

[37] L. Huang, Q. Yang, "GPS Spoofing, Low cost GPS Simulator," DEFCON 23, August 2015

[38] J. S. Warner, R. G. Johnston, "Think GPS Offers High Security? Think Again!", Talk for the Business Contingency Planning Conference, May 23-27, 2004 (Las Vegas, NV)

[39] C. Sebastian, “Getting lost near the Kremlin? Russia could be 'GPS spoofing',” CNN Tech, Dec 2 2016, http://money.cnn.com/2016/12/02/technology/kremlin-gps-signals/index.html

[40] D. Goward, “Mass GPS Spoofing Attack in Black Sea?”, The Maritime Executive, July 11 2017, http://maritime-executive.com/editorials/mass-gps-spoofing-attack-in-black-sea

[41] Humphreys, T.E., Bhatti, J.A., Ledvina, B.M., "The GPS Assimilator: A Method for Upgrading Existing GPS User Equipment to Improve Accuracy, Robustness, and Resistance to Spoofing," Proceedings of the 23rd International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2010), Portland, OR, September 2010, pp. 1942-1952.