2017

APNT for GNSS Spoof Detection

Peter F. Swaszek
University of Rhode Island, swaszek@uri.edu

Richard J. Hartnett

Kelly C. Seals

Citation/Publisher Attribution
Swaszek, Peter F., Hartnett, Richard J., Seals, Kelly C., "APNT for GNSS Spoof Detection," *Proceedings of the 2017 International Technical Meeting of The Institute of Navigation*, Monterey, California, January 2017, pp. 933-941.
Available at: https://www.ion.org/ptti/abstracts.cfm?paperID=4630

APNT for GNSS Spoof Detection

Peter F. Swaszek, *University of Rhode Island*
Richard J. Hartnett, *U.S. Coast Guard Academy*
Kelly C. Seals, *U.S. Coast Guard Academy*

BIOGRAPHIES

Peter F. Swaszek is a Professor of Electrical Engineering at the University of Rhode Island. His research interests are in statistical signal processing with a focus on digital communications and electronic navigation systems.

Richard J. Hartnett is a Professor of Electrical Engineering at the U.S. Coast Guard Academy, having retired from the USCG as a Captain in 2009. His research interests include efficient digital filtering methods, improved receiver signal processing techniques for electronic navigation systems, and autonomous vehicle design.

Kelly C. Seals is the Chair of the Electrical Engineering program at the U.S. Coast Guard Academy in New London, Connecticut. He is a Commander on active duty in the U.S. Coast Guard and received a PhD in Electrical and Computer Engineering from Worcester Polytechnic Institute.

ABSTRACT

Global Navigation Satellite Systems (GNSS) are well known to be accurate providers of position, navigation, and time (PNT) information across the globe. With capable receivers and well-populated satellite constellations, GNSS users typically believe that the position and time information provided by their GNSS receiver is perfectly accurate. More sophisticated users look beyond accuracy and are also concerned with the integrity of the GNSS information.

Advances in electronics technology have enabled the creation of malicious RF interference of GNSS signals. Inexpensive jamming devices overpower or distort the GNSS receivers input so as to completely deny the GNSS user of PNT information. A second threat to GNSS integrity is spoofing, the creation of counterfeit GNSS signals. This type of attack is considered more dangerous than a jamming attack since an erroneous PNT solution is often worse than no solution at all. The detection of spoofing is the subject of this paper.

A variety of approaches have been proposed in the literature to recognize spoofing; many of these are based on the RF signal alone, including multi-antenna and multi-receiver methods. Another class of spoof detection algorithm is to compare the GNSS result to data from another, non-GNSS (hence, non-spoofed) sensor. In this paper we imagine that the trusted signal is the output of an Alternative PNT (APNT) receiver.

APNT refers to stand alone, non-GNSS systems that are intended to provide PNT information during periods in which GNSS is unavailable The wide recognition of the vulnerabilities of the GPS in the Volpe report spurred the search for APNT systems; examples include the development of eLoran in the U.S. and Europe, general work on signals of opportunity ranging, DME-DME positioning, and, quite recently, R-Mode in Europe (we note that none of these systems is currently operational). The intent is that an integrated receiver, either loosely or tightly coupled, would merge the two systems' observables to yield the best PNT information possible; in practice, since the APNTs' solutions are typically of lower accuracy than the GNSS solutions, the combined result is nearly equal to the GNSS-alone solution.

The goal of this paper is to show that these APNT solutions should be used at ALL times; as a substitute for GNSS PNT when GNSS is unavailable and as an integrity check (e.g. spoof detector) when GNSS is available. At a cursory level spoof detection using APNT appears simple; just compare the two position outputs to see if they are close. This paper looks deeper, considering the questions: How can we use the time estimates to detect position spoofing? How close is close enough in this context? What is the probability of error in the decision? How do the geometries of both systems impact the test itself and its resulting performance? What happens if the receivers are providing different information?

INTRODUCTION

Global Navigation Satellite Systems (GNSS) are well known to be accurate providers of position, navigation, and time (PNT) information across the globe; as such, they are commonly used to locate and navigate craft in various transportation modes. Because of high signal availabilities, capable receivers, and well-populated satellite constellations, GNSS users typically believe that the position and time information provided by their GNSS receiver is perfectly accurate. More sophisticated users look beyond accuracy and are also concerned with the integrity of the GNSS information; for example, RAIM algorithms were developed to ensure users that the provided information is resistant to several possible satellite failure modes.

Advances in electronics technology have enabled the creation of malicious RF interference of GNSS signals. Inexpensive jamming devices overpower or distort the GNSS receivers input so as to completely deny the GNSS user of PNT information. While a serious concern when we expect PNT at all times, current generation GNSS receivers warn the user when PNT is unavailable; some of the more sophisticated receiver designs can also battle jamming. A second threat to GNSS integrity is spoofing, the creation of counterfeit GNSS signals. This type of attack is considered more dangerous than a jamming attack since an erroneous PNT solution is often worse than no solution at all.

A variety of approaches have been proposed in the literature to recognize spoofing; many of these are based on the RF signal alone (for example, examining the power levels of the signals, looking for vestigial peaks in the correlator outputs, etc.), including multi-antenna and multi-receiver methods. Another class of spoof detection algorithm compares the GNSS result to data from another, non-GNSS (hence, non-spoofed) sensor. One obvious choice is an inertial unit recognizing that the spoofer might be unable to match the random motion in the vehicle; examples include monitoring the roll/pitch of a Coast Guard vessel due to waves [1] and the effect of wind gusts on an aircraft [2]. A second sensor choice is radar, exploiting the relative position vector available from the radar returns between vehicles in a convoy [3]. Yet another possibility is to employ ranges [4] or pseudoranges [5] from fixed beacons, comparing the GNSS derived ranges to those measurements. These last two efforts are of particular relevance to the work presented herein.

The examinations in [4,5] characterized the binary hypothesis test of spoofing/no spoofing, developed the generalized likelihood test statistic, and solved for the tests' probabilities of false alarm and detection. The formulation in these papers was for any number of range/pseudorange measurements and involved solving the data fusion problem of combining the GNSS position with the additional range/pseudorange measurements. The examples considered one or two such measurements; it was observed that two measurements could be quite effective at detecting spoofing. If more range/pseudorange measurements were available, enough to compute an separate position solution (often referred to as Alternative PNT or APNT), one might ask *"How do we implement a spoof detector based on only the GNSS and APNT solutions?"* This question is relevant if one does not have access to the actual measurements used by the APNT system or might just be preferred as a simpler system to implement. By the data processing theorem we expect that a detector based on the APNT solution would experience worse detection performance than that of [4, 5] (as the conversion from ranges/pseudoranges to position is non-invertible), but wonder how much loss there really is. In this paper, then, we explore spoofing detection using a trusted signal and envision that that trusted signal is the output of an Alternative PNT (APNT) receiver.

As developed in the navigation literature APNT usually refers to separate, non-GNSS systems that could provide PNT during periods in which GNSS is unavailable. The wide recognition of the vulnerabilities of the GPS [6] spurred the search for APNT systems; examples include the development of eLoran in the U.S. and Europe [7], general work on signals of opportunity ranging [8], DME-DME positioning [9], and, quite recently, R-Mode in Europe [10] (we note that none of these systems is currently operational). The intent is that an integrated receiver, either loosely or tightly coupled, would merge the two systems' observables to yield the best PNT information possible; in practice, since the APNT estimates are typically of lower accuracy than the GNSS positions, the combined solution is nearly equal to the GNSS-alone solution.

The point of this paper is to show that these signals should be used at ALL times; as a substitute for GNSS PNT when GNSS is unavailable and as an integrity check (e.g. spoof detector) when GNSS is available. At a cursory level spoof detection using APNT appears to be quite simple; just compare the two position outputs to see if they are close. Going deeper, various question emerge:

- Since time is probably provided by both receivers, how do we use these measurements to detect position

spoofing? How do we use position information to detect time spoofing?

- How close is "close enough" in this context? What is the probability of error of the decision?
- How do the geometries of both systems (essentially the Geometric Dilution of Precision, GDOP) impact the test itself and its resulting performance?
- What happens if the receivers are providing different information, for example, 3-dimensional position versus latitude-longitude?

This paper develops the hypothesis test and analyzes the performance of such an spoofing detector assuming the use of a stand alone APNT receiver. Specifically, we assume that the APNT and GNSS receivers are not coupled, do *not* share pseudoranges, and base the integrity test on the position and time outputs of the two receivers. The next section characterizes the binary hypothesis test of spoofing/no spoofing for the combination of GNSS and APNT receiver outputs and develops the generalized likelihood test statistic. This is followed by examples, both position and time spoofing, with a Monte Carlo simulation of detector performance. The detector results are then extended to the case in which the APNT receiver provides a reduced set of information; examples of a APNT without time or vertical position is considered.

FORMULATION

In vector form, let $\mathbf{x}$ be the true PNT information (three position variables plus time) and $\widehat{\mathbf{x}_G}$ and $\widehat{\mathbf{x}_A}$ be the estimates of this information from GNSS and APNT systems, respectively. Assuming conditional independence, we characterize these two measurements under the relevant hypotheses:

H_0: Under no spoofing both solutions are assumed to be accurate (unbiased) and their errors are dependent upon their own covariance matrices

$$\widehat{\mathbf{x}_G} \sim \mathcal{N}\left(\mathbf{x}, \mathbf{\Sigma}_G\right) \qquad \widehat{\mathbf{x}_A} \sim \mathcal{N}\left(\mathbf{x}, \mathbf{\Sigma}_A\right)$$

in which the notation $\mathcal{N}\left(\boldsymbol{\mu}, \mathbf{\Sigma}\right)$ represents a multivariate Gaussian distribution with mean vector $\boldsymbol{\mu}$ and covariance matrix $\mathbf{\Sigma}$. For the GNSS solution the covariance matrix $\mathbf{\Sigma}_G$ is a function of the satellite geometry and the user range error; for the APNT estimate it will depend upon the technology employed. For example, if the APNT is provided by another ranging/pseudoranging system, its covariance is also determined by the geometry of the transmitters.

H_1: With spoofing the statistics of $\widehat{\mathbf{x}_A}$ is assumed to be unchanged, but the GNSS information is now inaccurate

$$\widehat{\mathbf{x}_G} \sim \mathcal{N}\left(\boldsymbol{\mu}, \mathbf{\Sigma}_S\right) \qquad \widehat{\mathbf{x}_A} \sim \mathcal{N}\left(\mathbf{x}, \mathbf{\Sigma}_A\right)$$

For simplicity we still assume Gaussian statistics for $\widehat{\mathbf{x}_G}$, but use $\boldsymbol{\mu}$ to represent the (unknown) spoofed mean vector and $\mathbf{\Sigma}_S$ as the spoofed GNSS covariance (potentially different than $\mathbf{\Sigma}_G$).

Assuming a Neyman-Pearson formulation of the detection problem (i.e. maximize the probability of detection for a fixed probability of false alarm) the likelihood ratio test is well known to be the optimum detector [11]. For the two measurement scenario above, the likelihood ratio test is

$$T = \frac{f\left(\widehat{\mathbf{x}_G}, \widehat{\mathbf{x}_A} | \mathrm{H}_1\right)}{f\left(\widehat{\mathbf{x}_G}, \widehat{\mathbf{x}_A} | \mathrm{H}_0\right)} = \frac{f\left(\widehat{\mathbf{x}_G} | \mathrm{H}_1\right)}{f\left(\widehat{\mathbf{x}_G} | \mathrm{H}_0\right)} \cdot \frac{f\left(\widehat{\mathbf{x}_A} | \mathrm{H}_1\right)}{f\left(\widehat{\mathbf{x}_A} | \mathrm{H}_0\right)} \underset{\mathrm{H}_0}{\overset{\mathrm{H}_1}{\gtrless}} \lambda$$

(using the conditional independence of measurements from the two systems) in which λ is a threshold selected to fix the false alarm probability (the probability of deciding for spoofing when spoofing is *not* present, typically a small probability on the order of 0.01 or less). Since the statistics of $\widehat{\mathbf{x}_A}$ are identical under both hypotheses, the second ratio equals unity; employing the Gaussian model, taking the natural logarithm, and ignoring constants yields the equivalent test

$$T = \left(\widehat{\mathbf{x}_G} - \mathbf{x}\right)^T \mathbf{\Sigma}_G^{-1} \left(\widehat{\mathbf{x}_G} - \mathbf{x}\right) - \left(\widehat{\mathbf{x}_G} - \boldsymbol{\mu}\right)^T \mathbf{\Sigma}_S^{-1} \left(\widehat{\mathbf{x}_G} - \boldsymbol{\mu}\right) \underset{\mathrm{H}_0}{\overset{\mathrm{H}_1}{\gtrless}} \lambda$$

This test is unrealizable due to it containing several unknown parameters. To continue we invoke the concept of Generalized Likelihood Ratio Tests (GLRTs) [11] and replace the unknown parameters by their maximum likelihood estimates (MLEs). Specifically, under H_1 the MLE of $\boldsymbol{\mu}$ is $\widehat{\boldsymbol{\mu}} = \widehat{\mathbf{x}_G}$ so that the GLRT test statistic is

$$T = \left(\widehat{\mathbf{x}_G} - \mathbf{x}\right)^T \boldsymbol{\Sigma}_G^{-1} \left(\widehat{\mathbf{x}_G} - \mathbf{x}\right) \underset{\mathrm{H}_0}{\overset{\mathrm{H}_1}{\gtrless}} \lambda$$

Under H_0 the MLE of $\mathbf{x}$ is

$$\widehat{\mathbf{x}} = \left(\boldsymbol{\Sigma}_G^{-1} + \boldsymbol{\Sigma}_A^{-1}\right)^{-1} \left[\boldsymbol{\Sigma}_G^{-1}\widehat{\mathbf{x}_G} + \boldsymbol{\Sigma}_A^{-1}\widehat{\mathbf{x}_A}\right]$$

Defining $\delta\mathbf{x}$ as the difference in the two positions, $\delta\mathbf{x} = \widehat{\mathbf{x}_G} - \widehat{\mathbf{x}_A}$, then the test statistic becomes

$$T = \delta\mathbf{x}^T \underbrace{\left(\boldsymbol{\Sigma}_A\boldsymbol{\Sigma}_G^{-1}\boldsymbol{\Sigma}_A + 2\boldsymbol{\Sigma}_A + \boldsymbol{\Sigma}_G\right)^{-1}}_{\mathbf{A}} \delta\mathbf{x} \tag{1}$$

a quadratic form in $\delta\mathbf{x}$. Details of the development of these last two expressions appear in Appendix A.

PERFORMANCE

This section contains an example to demonstrate the capabilities of the proposed, basic test to detect spoofing. For a Neyman-Pearson formulation of the detection problem we describe performance by two quantities, the probabilities of false alarm and detection:

- The probability of false alarm, $\mathrm{P_{fa}}$, is the probability that we decide spoofing (H_1) when no spoofing exists

  $$\mathrm{P_{fa}} = \mathrm{Prob}\left(T > \lambda | \mathrm{H}_0\right) = \mathrm{Prob}\left(\delta\mathbf{x}^T\,\mathbf{A}\,\delta\mathbf{x} > \lambda | \mathrm{H}_0\right)$$

  Typically we want this probability to be low, often below 0.01 (a 1% false alarm rate). We note that under H_0 the distribution of $\delta\mathbf{x}$ is Gaussian with a zero mean vector

  $$\delta_{\mathbf{x}} \sim \mathcal{N}\left(\mathbf{0}, \boldsymbol{\Sigma}_G + \boldsymbol{\Sigma}_A\right)$$

- The probability of detection, $\mathrm{P_d}$, is the probability that we decide spoofing (H_1) when spoofing actually exists

  $$\mathrm{P_{fa}} = \mathrm{Prob}\left(T > \lambda | \mathrm{H}_1\right) = \mathrm{Prob}\left(\delta\mathbf{x}^T\,\mathbf{A}\,\delta\mathbf{x} > \lambda | \mathrm{H}_1\right)$$

  The likelihood ratio test maximizes this probability for a fixed value of $\mathrm{P_{fa}}$. We note that under H_1 the distribution of $\delta\mathbf{x}$ is also Gaussian

  $$\delta_{\mathbf{x}} \sim \mathcal{N}\left(\boldsymbol{\mu} - \mathbf{x}, \boldsymbol{\Sigma}_S + \boldsymbol{\Sigma}_A\right)$$

  but with different parameters.

Typically the probability of false alarm is plotted against the probability of detection as the Receiver Operating Characteristic (ROC) curve. For such a representation the further to the left and up the curve is, the better is the resulting detector performance. On such a graphic, a line at a slope of unity, $\mathrm{P_d} = \mathrm{P_{fa}}$, is the performance of a (terrible) system that merely guesses between H_0 and H_1. For the proposed optimum test these probabilities are both based on quadratic forms of multivariate Gaussian vectors. There are analytical approaches to computing both of these probabilities [12–14]. As these are complicated, infinite series representations with difficult convergence issues we defer to Monte Carlo simulation for the examples here.

Imagine a GNSS environment with covariance for East, North, Up, and Time equal to

$$\boldsymbol{\Sigma}_G = \begin{bmatrix} 0.796 & -0.122 & 0.027 & -0.082 \\ -0.122 & 0.907 & -0.170 & 0.086 \\ 0.027 & -0.170 & 2.42 & -1.03 \\ -0.082 & 0.086 & -1.03 & 0.732 \end{bmatrix}$$

(such a covariance results for seven GNSS satellites with azimuths 30°, 45°, 80°, 150°, 215°, 285°, and 290° and elevations 10°, 70°, 15°, 10°, 15°, 85°, and 10°, respectively, and a User Range Error, URE, of 2 meters). For the

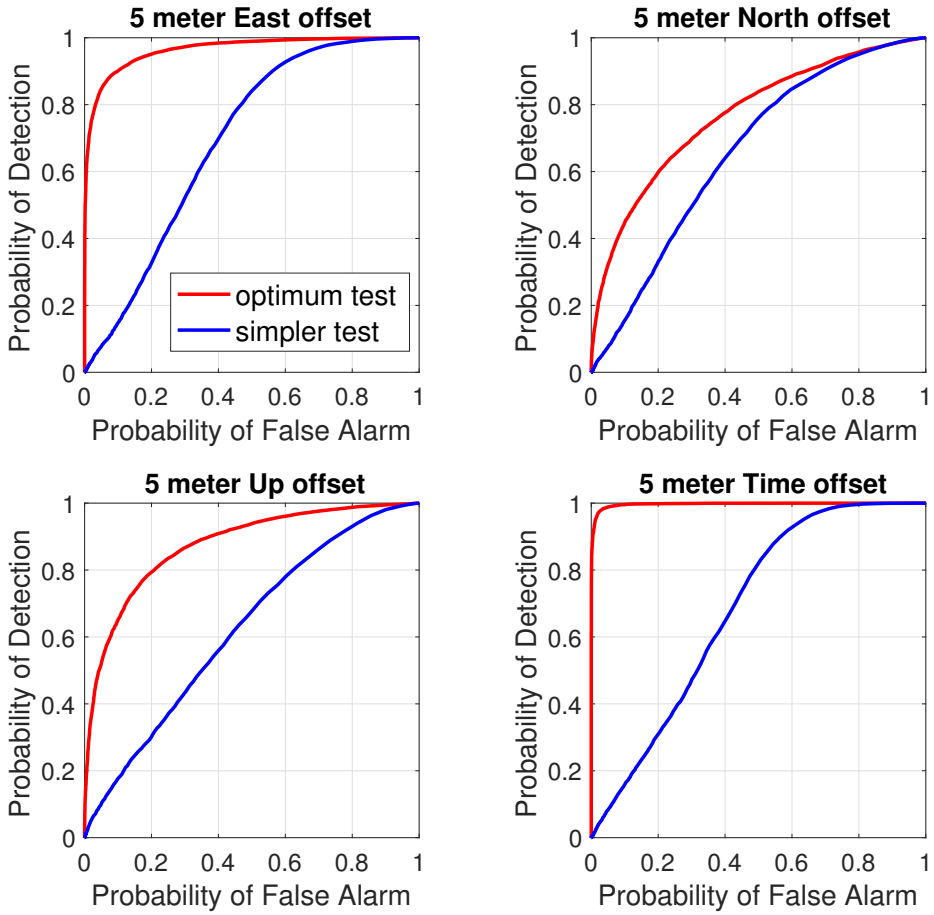

Figure 1: Simulated performance of the detector for a 5-meter spoofing shift.

APNT system we assume a considerably noisier set of measurements with East, North, Up, and Time covariance matrix

$$\boldsymbol{\Sigma}_A = \begin{bmatrix} 1.60 & 1.43 & 1.74 & -1.03 \\ 1.43 & 11.0 & 13.4 & -7.18 \\ 1.74 & 13.4 & 27.7 & -14.1 \\ -1.03 & -7.18 & -14.1 & 7.96 \end{bmatrix}$$

(as might results from 4 satellites with azimuths 60°, 120°, 240°, and 300° and elevations 20°, 30°, 60°, and 10°, respectively, and URE of 3 meters although the APNT need *not* be satellite based). Figure 1 (the red curves) shows the results of four Monte Carlo estimates of the false alarm and detection probabilities for the proposed spoof detector: spoofing offset to the East, North, Up, and in Time, respectively. In each example, we assumed that the spoofer created the same covariance matrix, $\boldsymbol{\Sigma}_S = \boldsymbol{\Sigma}_G$, and moved the measurement by 5 meters (for Time, this is approximately 16.7 nsec). Even with these small offsets the detector is quite effective, providing reasonably high probability of detection for small probability of false alarm (detecting some offsets better than others due to the underlying covariance structures of both the GNSS and APNT measurements).

The optimum test in Eq. (1) is complicated by the weighting matrix $\mathbf{A}$ in the quadratic form, a function of both the GNSS and APNT covariances. One might wonder if this complexity is really necessary, that the correlation structure displayed in both $\boldsymbol{\Sigma}_G$ and $\boldsymbol{\Sigma}_A$ impact detector performance. To explore this idea we consider the *simpler* hypothesis test that ignores the covariance structures and merely looks at the magnitude (squared) of the difference

vector between the two receivers' outputs

$$T_{simple} = \delta\mathbf{x}^T \, \delta\mathbf{x} \underset{\mathrm{H_0}}{\overset{\mathrm{H_1}}{\gtrless}} \lambda$$

(this is equivalent to $\mathbf{A}$ being replaced by an identity matrix). Figure 1 also include simulation results for this simpler test (shown as solid blue lines). We note that in both cases its performance is grossly inferior to that of the optimum test; that the covariance based weighting (via $\mathbf{\Sigma}_A$) is important.

MISMATCH OF THE OUTPUT COMPONENTS

The test statistic developed above assumes that both $\mathbf{x}_G$ and $\mathbf{x}_A$ are of the same size and in the same coordinate frame; both representing a three-dimensional position solution, (x, y, z) or (e, n, u) and time. The question for this section is to consider the case in which the two PNT solutions do not match in dimension. For example, a terrestrial APNT system might only provide East and North position estimates, no vertical term, or an APNT receiver might not provide a GNSS time estimate.

Let the GNSS solution vector $\widehat{\mathbf{x}_G}$ be decomposed into two subvectors: $\widehat{\mathbf{y}_G}$ whose components correspond to those measured by the APNT receiver (with output $\widehat{\mathbf{y}_A}$) and $\widehat{\mathbf{z}_G}$ as the remaining components. Further, define the difference vector of the common components as $\delta\mathbf{y} = \widehat{\mathbf{y}_G} - \widehat{\mathbf{y}_A}$. Referring to Appendix B for details, the optimum test in this case is still a quadratic form, but on this reduced dimension difference

$$T = \delta\mathbf{y}^T \, \mathbf{B} \, \delta\mathbf{y} \underset{\mathrm{H_0}}{\overset{\mathrm{H_1}}{\gtrless}} \lambda \qquad \text{with} \qquad \mathbf{B} = \left(\mathbf{\Sigma}_A \mathbf{\Sigma}_{Gy}^{-1} \mathbf{\Sigma}_A + 2\mathbf{\Sigma}_A + \mathbf{\Sigma}_{Gy} \right)^{-1} \tag{2}$$

in which $\mathbf{\Sigma}_{Gy}$ is the covariance matrix of just the $\widehat{\mathbf{y}_G}$ portion of $\widehat{\mathbf{x}_G}$. This test is, of course, perfectly reasonable in view of the development above; the test compares whatever data is available using the statistics of that data.

As an example, consider a terrestrial APNT system based on range measurements yielding only east and north position information. Assume that the covariance matrix is

$$\mathbf{\Sigma}_A = \begin{bmatrix} 6.32 & -2.98 \\ -2.98 & 4.74 \end{bmatrix}$$

For the statistics of the GNSS solution we reuse the example above; restricting attention to the East and North components, the covariance matrix is

$$\mathbf{\Sigma}_{Gy} = \begin{bmatrix} 0.796 & -0.122 \\ -0.122 & 0.907 \end{bmatrix}$$

Figure 2 shows simulated ROC curves for the test in Eq. (2) as the solid red curve for spoofing offsets to the East and North, respectively. The blue curves are, in this case, simulations for a better APNT measurement, whose covariance matrix is scaled by 0.25.

CONCLUSIONS/FUTURE WORK

While begun as an extension of our earlier work on using range/pseudorange measurements to detect GNSS spoofing (or, more generally, integrity of the GNSS information), the results above are valid for any APNT system, not just range/pseudorange based, as long as a statistical model of the APNT solution is available (specifically, the covariance matrix $\mathbf{\Sigma}_A$). While the raw measurables of the APNT system are expected to contain more information about spoofing, we observe that even a simple comparison of receiver outputs (with proper weighting) can effectively detect small amounts of spoofing.

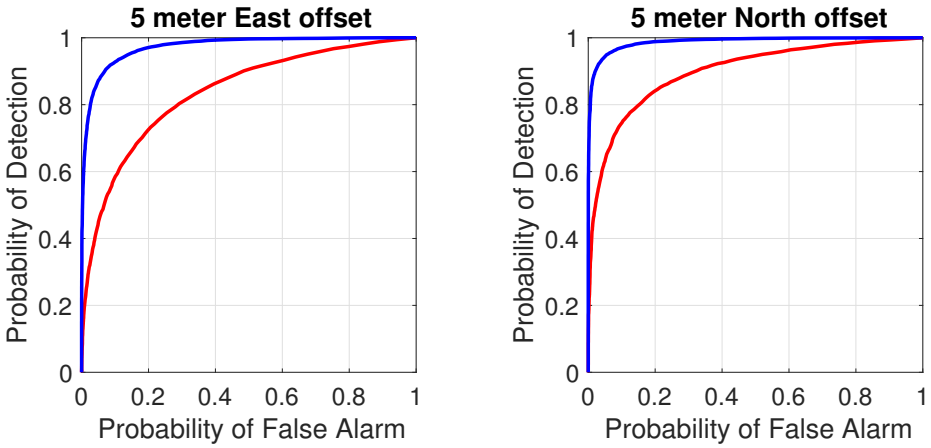

Figure 2: Simulated performance of the detector for a 5-meter shift in position; no vertical or time measurements by the APNT system.

REFERENCES

[1] "GNSS spoof detection using shipboard IMU measurements," P. F. Swaszek, K. C. Seals, S. A. Pratz, B. N. Arocho, and R. J. Hartnett, *Proc. ION GNSS+ 2014*, Tampa FL, Sept. 2014.

[2] "Impact of wind gusts on detectability of GPS spoofing attacks using RAIM with INS coupling," C. Tanil, S Khanafseh, and B. Pervan, *Proc. 2015 ION Pacific PNT*, Honolulu HA, Apr. 2015.

[3] "A robust method for spoofing prevention and position recovery in attacks against networked GPS receivers," N. Carson and D. Bevly, *Proc. ION ITM*, San Diego CA, Jan. 2015.

[4] "GNSS spoof detection using range information," P. F. Swaszek, R. J. Hartnett, and K. C. Seals, *Proc. ION ITM 2016*, Monterey CA, Jan. 2016.

[5] "GNSS spoof detection using passive ranges," P. F. Swaszek, R. J. Hartnett, and K. C. Seals, *Proc. ION GNSS+ 2016*, Portland OR, Sept. 2016.

[6] "Vulnerability assessment of the transportation infrastructure relying on the Global Positioning System," Volpe National Transportation Systems Center, Boston MA, Aug. 2001.

[7] "An evaluation of eLoran as a backup navigation sensor for ADS-B," G. W. Johnson, C. Oates, M. Wiggens, J. V. Carroll, P. F. Swaszek, and R. J. Hartnett, *Proc. ION NTM*, San Diego CA, January 2008, pp. 411-419.

[8] "Navigation using signals of opportunity," J. Raquet, *GPS World Discussion Forums*, 2006.

[9] "Design of a passive ranging system using existing Distance Measuring Equipment (DME) signals & transmitters," S. C. Lo, P. K. Enge, and M. J. Narins, *Navigation*, vol. 62, no. 2, Summer 2015, pp. 131-149.

[10] "The feasibility of R-Mode to meet resilient PNT requirements for e-navigation," G. W. Johnson, P. F. Swaszek, J. Alberding, M. Hoppe, and J.H. Oltmann, *Proc. ION GNSS+ 2014*, Tampa FL, Sept. 2014.

[11] H. L. Van Trees, *Detection, Estimation, and Modulation Theory, Part I*, New York: Wiley, 1968.

[12] M. K. Simon, *Probability Distributions Involving Gaussian Random Variables*, New York: Springer-Verlag, 2006.

[13] S. Kotz, N. L. Johnson, and D. W. Boyd, "Series representations of distributions of quadratic forms in normal variables. I. Central case," *Ann. Math. Statist.*, 38, 1967.

[14] S. Kotz, N. L. Johnson, and D. W. Boyd, "Series representations of distributions of quadratic forms in normal variables. I. Non-central case," *Ann. Math. Statist.*, 38, 1967.

APPENDIX A

This first appendix develops the MLE of $\mathbf{x}$ under H_0 based upon the two measurements, $\widehat{\mathbf{x}_G}$ and $\widehat{\mathbf{x}_A}$. The likelihood function under H_0 is

$$L(\mathbf{x}) = f\left(\widehat{\mathbf{x}_G}|\mathrm{H}_0\right) \cdot f\left(\widehat{\mathbf{x}_A}|\mathrm{H}_0\right)$$

Recall that under H_0

$$\widehat{\mathbf{x}_G} \sim \mathcal{N}\left(\mathbf{x}, \mathbf{\Sigma}_G\right) \qquad \text{and} \qquad \widehat{\mathbf{x}_A} \sim \mathcal{N}\left(\mathbf{x}, \mathbf{\Sigma}_A\right)$$

Substituting the Gaussian forms for the density functions, taking a natural logarithm, and dropping constants, the log-likelihood is

$$l(\mathbf{x}) = -\frac{1}{2}\left(\widehat{\mathbf{x}_G} - \mathbf{x}\right)^T \mathbf{\Sigma}_G^{-1}\left(\widehat{\mathbf{x}_G} - \mathbf{x}\right) - \frac{1}{2}\left(\widehat{\mathbf{x}_A} - \mathbf{x}\right)^T \mathbf{\Sigma}_A^{-1}\left(\widehat{\mathbf{x}_A} - \mathbf{x}\right)$$

The MLE is that value of $\mathbf{x}$ which maximizes this expression. A necessary condition for the maximum is that the vector derivative is equal to zero

$$\frac{\partial l(\mathbf{x})}{\partial \mathbf{x}} = \mathbf{\Sigma}_G^{-1}\left(\widehat{\mathbf{x}_G} - \mathbf{x}\right) + \mathbf{\Sigma}_A^{-1}\left(\widehat{\mathbf{x}_A} - \mathbf{x}\right) = \mathbf{0}$$

Solving for $\mathbf{x}$ yields the MLE

$$\widehat{\mathbf{x}}_{MLE} = \left(\mathbf{\Sigma}_G^{-1} + \mathbf{\Sigma}_A^{-1}\right)^{-1}\left[\mathbf{\Sigma}_G^{-1}\widehat{\mathbf{x}_G} + \mathbf{\Sigma}_A^{-1}\widehat{\mathbf{x}_A}\right]$$

With this result the difference in the test statistic's quadratic form is

$$\widehat{\mathbf{x}_G} - \mathbf{x} = \widehat{\mathbf{x}_G} - \left(\mathbf{\Sigma}_G^{-1} + \mathbf{\Sigma}_A^{-1}\right)^{-1}\left[\mathbf{\Sigma}_G^{-1}\widehat{\mathbf{x}_G} + \mathbf{\Sigma}_A^{-1}\widehat{\mathbf{x}_A}\right] = \left(\mathbf{\Sigma}_G^{-1} + \mathbf{\Sigma}_A^{-1}\right)^{-1}\mathbf{\Sigma}_A^{-1}\left(\widehat{\mathbf{x}_G} - \widehat{\mathbf{x}_A}\right)$$

Defining $\delta\mathbf{x}$ as the difference in the two solutions, $\delta\mathbf{x} = \widehat{\mathbf{x}_G} - \widehat{\mathbf{x}_A}$, then the test statistic becomes

$$T = \delta\mathbf{x}^T \mathbf{A}\, \delta\mathbf{x}$$

a quadratic form with

$$\begin{aligned}
\mathbf{A} &= \mathbf{\Sigma}_A^{-1}\left(\mathbf{\Sigma}_G^{-1} + \mathbf{\Sigma}_A^{-1}\right)^{-1}\mathbf{\Sigma}_G^{-1}\left(\mathbf{\Sigma}_G^{-1} + \mathbf{\Sigma}_A^{-1}\right)^{-1}\mathbf{\Sigma}_A^{-1} \\
&= \left(\mathbf{\Sigma}_A\left(\mathbf{\Sigma}_G^{-1} + \mathbf{\Sigma}_A^{-1}\right)\mathbf{\Sigma}_G\left(\mathbf{\Sigma}_G^{-1} + \mathbf{\Sigma}_A^{-1}\right)\mathbf{\Sigma}_A\right)^{-1} \\
&= \left(\mathbf{\Sigma}_A\mathbf{\Sigma}_G^{-1}\mathbf{\Sigma}_A + 2\mathbf{\Sigma}_A + \mathbf{\Sigma}_G\right)^{-1}
\end{aligned}$$

APPENDIX B

This second appendix redevelops the MLEs under H_0 assuming that $\widehat{\mathbf{x}_A}$ has fewer components than $\widehat{\mathbf{x}_G}$. For simplicity of the development let $\widehat{\mathbf{x}_G}$ measure the pair of vectors $\mathbf{y}$ and $\mathbf{z}$ while $\widehat{\mathbf{x}_A}$ only measures $\mathbf{y}$.

The components of the likelihood function under H_0 are

$$\widehat{\mathbf{y}_G}, \widehat{\mathbf{z}_G} \sim \mathcal{N}\left(\begin{bmatrix} \mathbf{y} \\ \mathbf{z} \end{bmatrix}, \mathbf{\Sigma}_G\right) \qquad \text{and} \qquad \widehat{\mathbf{y}_A} \sim \mathcal{N}\left(\mathbf{x}, \mathbf{\Sigma}_A\right)$$

Letting

$$\mathbf{\Sigma}_G^{-1} = \begin{bmatrix} \mathbf{\Psi_{yy}} & \mathbf{\Psi_{yz}} \\ \mathbf{\Psi_{zy}} & \mathbf{\Psi_{zz}} \end{bmatrix}$$

the log-likelihood is

$$\begin{aligned}
l(\mathbf{y}, \mathbf{z}) = &-\frac{1}{2}\left(\widehat{\mathbf{y}_G} - \mathbf{y}\right)^T \mathbf{\Psi_{yy}}\left(\widehat{\mathbf{y}_G} - \mathbf{y}\right) - \left(\widehat{\mathbf{y}_G} - \mathbf{y}\right)^T \mathbf{\Psi_{yz}}\left(\widehat{\mathbf{z}_G} - \mathbf{z}\right) \\
&- \frac{1}{2}\left(\widehat{\mathbf{z}_G} - \mathbf{z}\right)^T \mathbf{\Psi_{zz}}\left(\widehat{\mathbf{z}_G} - \mathbf{z}\right) - \frac{1}{2}\left(\widehat{\mathbf{y}_A} - \mathbf{y}\right)^T \mathbf{\Sigma}_A^{-1}\left(\widehat{\mathbf{y}_A} - \mathbf{y}\right)
\end{aligned}$$

The MLEs for $\mathbf{y}$ and $\mathbf{z}$ are those values that maximize this expression; we can find them by setting vector derivatives equal to zero. The $\mathbf{z}$ derivative is

$$\frac{\partial l(\mathbf{y},\mathbf{z})}{\partial \mathbf{z}} = \mathbf{\Psi_{zy}}\left(\widehat{\mathbf{y}_G} - \mathbf{y}\right) + \mathbf{\Psi_{zz}}\left(\widehat{\mathbf{z}_G} - \mathbf{z}\right) = \mathbf{0}$$

so

$$\widehat{\mathbf{z}_G} - \mathbf{z} = -\mathbf{\Psi_{zz}^{-1}\Psi_{zy}}\left(\widehat{\mathbf{y}_G} - \mathbf{y}\right)$$

The $\mathbf{y}$ derivative is

$$\frac{\partial l(\mathbf{y},\mathbf{z})}{\partial \mathbf{y}} = \mathbf{\Psi_{yy}}\left(\widehat{\mathbf{y}_G} - \mathbf{y}\right) + \mathbf{\Psi_{yz}}\left(\widehat{\mathbf{z}_G} - \mathbf{z}\right) + \mathbf{\Sigma}_A^{-1}\left(\widehat{\mathbf{y}_A} - \mathbf{y}\right) = \mathbf{0}$$

or

$$\mathbf{\Psi_{yy}}\left(\widehat{\mathbf{y}_G} - \mathbf{y}\right) - \mathbf{\Psi_{yz}\Psi_{zz}^{-1}\Psi_{zy}}\left(\widehat{\mathbf{y}_G} - \mathbf{y}\right) + \mathbf{\Sigma}_A^{-1}\left(\widehat{\mathbf{y}_A} - \mathbf{y}\right) = \mathbf{0}$$

so the MLE of $\mathbf{y}$ is

$$\mathbf{y} = \left[\mathbf{\Sigma}_A^{-1} + \mathbf{\Psi_{yy}} - \mathbf{\Psi_{yz}\Psi_{zz}^{-1}\Psi_{zy}}\right]^{-1}\left(\left[\mathbf{\Psi_{yy}} - \mathbf{\Psi_{yz}\Psi_{zz}^{-1}\Psi_{zy}}\right]\widehat{\mathbf{y}_G} + \mathbf{\Sigma}_A^{-1}\widehat{\mathbf{y}_A}\right)$$

With this two subvector notation the test statistic is

$$T = \begin{bmatrix} \widehat{\mathbf{y}_G} - \mathbf{y} \\ \widehat{\mathbf{z}_G} - \mathbf{z} \end{bmatrix}^T \mathbf{\Sigma}_G^{-1} \begin{bmatrix} \widehat{\mathbf{y}_G} - \mathbf{y} \\ \widehat{\mathbf{z}_G} - \mathbf{z} \end{bmatrix}$$

or

$$T = \left(\widehat{\mathbf{y}_G} - \mathbf{y}\right)^T \mathbf{\Psi_{yy}}\left(\widehat{\mathbf{y}_G} - \mathbf{y}\right) + 2\left(\widehat{\mathbf{y}_G} - \mathbf{y}\right)^T \mathbf{\Psi_{yz}}\left(\widehat{\mathbf{z}_G} - \mathbf{z}\right) + \left(\widehat{\mathbf{z}_G} - \mathbf{z}\right)^T \mathbf{\Psi_{zz}}\left(\widehat{\mathbf{z}_G} - \mathbf{z}\right)$$

Note that

$$\widehat{\mathbf{y}_G} - \mathbf{y} = \left[\mathbf{\Sigma}_A^{-1} + \mathbf{\Psi_{yy}} - \mathbf{\Psi_{yz}\Psi_{zz}^{-1}\Psi_{zy}}\right]^{-1}\mathbf{\Sigma}_A^{-1}\left(\widehat{\mathbf{y}_G} - \widehat{\mathbf{y}_A}\right)$$

and

$$\begin{aligned}\widehat{\mathbf{z}_G} - \mathbf{z} &= -\mathbf{\Psi_{zz}^{-1}\Psi_{zy}}\left(\widehat{\mathbf{y}_G} - \mathbf{y}\right) \\ &= -\mathbf{\Psi_{zz}^{-1}\Psi_{zy}}\left[\mathbf{\Sigma}_A^{-1} + \mathbf{\Psi_{yy}} - \mathbf{\Psi_{yz}\Psi_{zz}^{-1}\Psi_{zy}}\right]^{-1}\mathbf{\Sigma}_A^{-1}\left(\widehat{\mathbf{y}_G} - \widehat{\mathbf{y}_A}\right)\end{aligned}$$

Using these expressions in the form for the test and defining the difference in the common measurements between the GNSS and APNT system, $\delta\mathbf{y} = \widehat{\mathbf{y}_G} - \widehat{\mathbf{y}_A}$, then

$$T = \delta\mathbf{y}^T\,\mathbf{B}\,\delta\mathbf{y}$$

another quadratic form with

$$\mathbf{B} = \left(\mathbf{\Sigma}_A\left[\mathbf{\Psi_{yy}} - \mathbf{\Psi_{yz}\Psi_{zz}^{-1}\Psi_{zy}}\right]\mathbf{\Sigma}_A + 2\mathbf{\Sigma}_A + \left[\mathbf{\Psi_{yy}} - \mathbf{\Psi_{yz}\Psi_{zz}^{-1}\Psi_{zy}}\right]^{-1}\right)^{-1}$$

Note that this is really the same as the final line in Appendix A if we recognize that $\left(\mathbf{\Psi_{yy}} - \mathbf{\Psi_{yz}\Psi_{zz}^{-1}\Psi_{zy}}\right)^{-1}$ is the covariance matrix of $\widehat{\mathbf{y}_G}$, $\mathbf{\Sigma}_{Gy}$.

$$\mathbf{B} = \left(\mathbf{\Sigma}_A\mathbf{\Sigma}_{Gy}^{-1}\mathbf{\Sigma}_A + 2\mathbf{\Sigma}_A + \mathbf{\Sigma}_{Gy}\right)^{-1}$$

We demonstrate this final point as follows. At the beginning of this appendix we defined

$$\mathbf{\Sigma}_G^{-1} = \begin{bmatrix} \mathbf{\Psi_{yy}} & \mathbf{\Psi_{yz}} \\ \mathbf{\Psi_{zy}} & \mathbf{\Psi_{zz}} \end{bmatrix}$$

Inverting this matrix should take us back to the covariance matrix for $\widehat{\mathbf{x}_G}$ in block form

$$\mathbf{\Sigma}_G = \begin{bmatrix} \mathrm{Cov}(\widehat{\mathbf{y}_G},\widehat{\mathbf{y}_G}) & \mathrm{Cov}(\widehat{\mathbf{y}_G},\widehat{\mathbf{z}_G}) \\ \mathrm{Cov}(\widehat{\mathbf{z}_G},\widehat{\mathbf{y}_G}) & \mathrm{Cov}(\widehat{\mathbf{z}_G},\widehat{\mathbf{z}_G}) \end{bmatrix} = \begin{bmatrix} \mathbf{\Psi_{yy}} & \mathbf{\Psi_{yz}} \\ \mathbf{\Psi_{zy}} & \mathbf{\Psi_{zz}} \end{bmatrix}^{-1}$$

Employing the block version of the matrix inversion lemma

$$\begin{bmatrix} \mathbf{\Psi_{yy}} & \mathbf{\Psi_{yz}} \\ \mathbf{\Psi_{zy}} & \mathbf{\Psi_{zz}} \end{bmatrix}^{-1} = \begin{bmatrix} \left(\mathbf{\Psi_{yy}} - \mathbf{\Psi_{yz}\Psi_{zz}^{-1}\Psi_{zy}}\right)^{-1} & term \\ term & term \end{bmatrix}$$

where *term* is inserted for the three terms of little interest here. The upper left term matches our result, so is clearly the covariance matrix of the $\mathbf{y}$ component of the GNSS solution.