1-2015

GNSS Spoof Detection Based on Pseudoranges from Multiple Receivers

David S. Radin

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

Kelly C. Seals

Richard J. Hartnett

Citation/Publisher Attribution

Radin, David, Swaszek, Peter F., Seals, Kelly C., Hartnett, Richard J., "GNSS Spoof Detection Based on Pseudoranges from Multiple Receivers," *Proceedings of the 2015 International Technical Meeting of The Institute of Navigation*, Dana Point, California, January 2015, pp. 657-671.
Available at: http://www.ion.org/publications/abstract.cfm?jp=p&articleID=12658

GNSS Spoof Detection Based on Pseudoranges from Multiple Receivers

GNSS Spoof Detection Based Upon Pseudoranges from Multiple Receivers

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

BIOGRAPHIES

David S. Radin is a Lieutenant on active duty in the U.S. Coast Guard currently pursuing a Masters Degree in Electrical Engineering at the University of Rhode Island. He received a B.S. in Electrical Engineering from the U.S. Coast Guard Academy in May 2009.

Peter F. Swaszek is a Professor in the Department of Electrical, Computer, and Biomedical 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.

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.

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.

ABSTRACT

Spoofing is the common term used for describing the intentional broadcasting of false radio frequency signals intended to disrupt and mislead systems that depend on accurate position, navigation, and timing information provided by Global Navigation Satellite Systems (GNSS). Spoofing is an increasingly recognized threat garnering increased interest from researchers and users, both military and civilian.

This paper presents a GNSS spoof detection algorithm that exploits the geometric distribution of a horizontal array of GNSS receiver antennae and the geometric configuration of visible navigation satellites. Using a Neyman-Pearson hypothesis testing formulation, a spatial correlation test is developed that can accurately and dependably detect a GNSS spoofing event. This paper develops the generalized likelihood ratio test using standard statistical models of the GNSS range measurements and maximum likelihood estimates of the unknown variables. An analysis is presented showing the performance effects of the number of receivers used, internal receiver clock bias estimation, unknown antenna array orientation, and temporal and spatial locations of the detector.

Simulations were conducted using a GNSS simulator and receiver combination to further substantiate theoretical claims. Furthermore, comparisons to similar prior work using position solutions shows a marked improvement in performance.

INTRODUCTION

Global Navigation Satellite Systems (GNSS) are well known to be accurate providers of position 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 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 position information is resistant to several possible satellite failure modes.

Advances in electronics technology have enabled the creation of malicious RF interference of GNSS signals. Jamming (devices for which are widely available on the web at very low cost) involves the creation of an RF signal that overpowers or distorts the GNSS receiver's input so as to completely deny the GNSS user of any position, navigation, or time (PNT) information. Clearly jamming is a serious concern when we expect accurate PNT information at all times. Fortunately current generation GNSS receivers warn the user when PNT is unavailable, so can detect jamming; some of the more sophisticated receivers can also combat jamming. Recent demonstrations have highlighted another threat to GNSS integrity, the intentional creation of RF signals so as to provide counterfeit information to a GNSS receiver; so called "spoofing" [1]. Since current generation GNSS receivers are not expecting to experience spoofing, 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 and vary widely based upon the assumed capabilities and *a priori* knowledge of the spoofer. Methods for a single GNSS receiver include monitoring the power levels of the GNSS signals (absolute, relative, and across satellites), checking that the observed constellation is correct for the given time (e.g. number of and IDs of the satellites), testing the accuracy of the clock component, and checking the computed position against that derived from some non-GNSS source (e.g. an INS) [2]. Other methods include correlating the P(Y) code at the RF level [3], looking for vestigial peaks in the correlator outputs [4], comparing to trusted reference signals [5, 6], using an antenna array to spatially locate and identify signals [7], and other multi-antenna methods. While these ideas are certainly viable for recognizing spoofing, much of the treatment in the literature has been a description of the methods; there has been little analysis of their performance at effectively detecting spoofing.

Further, implementation of many of the proposed spoof detection methods requires a complete redesign of the GNSS receiver since the detection algorithms are based upon internal signal measurements unavailable outside of the receiver. Our approach to spoof detection for the past two years has been to focus on techniques that exploit the output already provided by current generation, commercial-off-the-shelf (COTS) receivers. In other words, spoof detection that can be implemented via a software tool interfacing to existing GNSS hardware. For example, at last year's ION ITM [8] we presented a spoof detection algorithm based upon the position solutions estimated by an array of COTS GNSS receivers. We developed the method using classical hypothesis testing and provided a complete analysis of its performance under the Neyman-Pearson criterion. For example, we were able to show excellent spoof detection performance (false alarm probability of 10^{-5} and detection probability of 0.99) using 4 receivers with antennae distributed on a circle of radius 10 meters.

Continuing this approach, the current paper develops and analyses the performance of a GNSS spoof detection algorithm based on the (pseudo)ranges estimated by an array of COTS receivers. The motivation for this approach is: (1) range data (perhaps through residuals) is available as a standard output from some COTS receivers, (2) the position based spoofing detection algorithm mentioned above [8] works quite well, and (3) the conversion from pseudoranges to the position solution is lossy from an information theoretic (and hypothesis testing) perspective; hence, better spoof detection performance should be achievable by testing with the original (pseudorange) data.

The primary contribution of this paper is the development of a GNSS spoof detection algorithm that exploits the pseudorange information provided by some COTS GNSS receivers. The resulting algorithm can be interpreted as a spatial matched filter, comparing the differential pseudoranges observed at the separate antennae to their expected values given the geometry of the antenna pattern. We then provide an analysis of performance (providing expressions for both the probability of false alarm and the probability of detection) to show the improvement over our previous position based method. The paper is organized as follows: (1) first we establish notation for the signals of interest, (2) we present the statistics of the two hypotheses (no spoof vs spoof) based on an additive white Gaussian noise channel for the pseudoranges, (3) we develop the optimum hypothesis test under a Neyman-Pearson criterion, (4) we analyze the theoretical performance of the test, and (5) we describe and present experimental work to verify the theoretical predictions of performance.

NOTATION AND SOME MATHEMATICAL PRELIMINARIES

Imagine a configuration of m GNSS receivers with their antennae located on a horizontal plane, evenly distributed about a circle of radius r. (In this treatment we assume that $m \geq 3$; the important case of $m = 2$ is considered in [9].) For convenience, let us employ a local east, north, up (ENU) coordinate frame with the center of the circle at its origin. The individual antennae locations ($k = 1, ...m$) in this same reference frame, then, are

$$\begin{bmatrix} e_k \\ n_k \\ u_k \end{bmatrix} = \begin{bmatrix} r \sin \theta_k \\ r \cos \theta_k \\ 0 \end{bmatrix}$$

where

$$\theta_k = \frac{2\pi (k-1)}{m} + \theta$$

This angle term describes the equiangular distribution of the antennae about the circle relative to north in which θ allows for a clockwise rotation of the entire antennae platform.

The sky view presented to this antennae array is assumed to consist of N satellites which will be indexed by n ($n = 1, \dots N$). We will use the notation ψ_n to represent the elevation ($0 \leq \psi_n \leq 90°$) and ϕ_n for the azimuth ($0 \leq \phi_n \leq 360°$) of satellite n relative to the center of the ENU reference frame. Satellites below the local horizon are ignored; in fact, it is common to also ignore low elevation satellites (say below 5°). Since the antennae are assumed to be closely spaced (r is small) then the set of visible satellites and their angles is identical for each antenna.

For spoof detection each antenna is assumed to independently process the RF signals it receives, yielding pseudoranges to the observed satellites. Let $d_{0,n}$ represent the true distance (range) from the center of the antennae array $\left([0,0,0]^T\right)$ to the n^{th} satellite. In terms of the elevation and azimuth angles, the position of this satellite in the local ENU coordinate system is

$$\begin{bmatrix} e \\ n \\ u \end{bmatrix} = \begin{bmatrix} d_{0,n} \cos\psi_n \sin\phi_n \\ d_{0,n} \cos\psi_n \cos\phi_n \\ d_{0,n} \sin\psi_n \end{bmatrix}$$

and the range from the k^{th} antenna to the n^{th} satellite is

$$\begin{aligned} d_{k,n} = &\Big[\left(d_{0,n}\cos\psi_n \sin\phi_n - e_k\right)^2 \\ &+ \left(d_{0,n}\cos\psi_n\cos\phi_n - n_k\right)^2 \\ &+ \left(d_{0,n}\sin\psi_n - u_k\right)^2\Big]^{\frac{1}{2}} \\ = &\big(d_{0,n}{}^2 \\ &- 2d_{0,n} r\cos\psi_n\left[\sin\phi_n\sin\theta_k + \cos\phi_n\cos\theta_k\right] \\ &+ r^2\big)^{\frac{1}{2}} \end{aligned}$$

Since the satellite range is much, much larger than the spacing between antennae ($d_{0,n} \gg r$), this range can be approximated

$$d_{k,n} \approx \ d_{0,n}\sqrt{1 - 2\frac{\delta_{k,n}}{d_{0,n}}}$$

in which $\delta_{k,n}$ is

$$\begin{aligned} \delta_{k,n} &= r\cos\psi_n\left[\sin\phi_n\sin\theta_k + \cos\phi_n\cos\theta_k\right] \\ &= r\cos\psi_n\cos\left(\phi_n - \theta_k\right) \end{aligned}$$

The square root function in the approximation to the range can be expanded in a Taylor series in terms of the variable x ($= \delta_{k,n}/d_{0,n}$) about $x = 0$

$$\begin{aligned} \sqrt{1-2x} &= \sum_{k=0}^{\infty} \frac{x^k}{k!}\left(\frac{\partial^k}{\partial x^k}\sqrt{1-2x}\right)\Bigg|_{x=0} \\ &= 1 - x - \frac{x^2}{2} + ... \\ &\approx 1 - x \end{aligned}$$

where the approximation holds since x is small. In terms of $\delta_{k,n}$ and $d_{0,n}$, this is

$$\begin{aligned} d_{k,n} &\approx d_{0,n}\left(1 - \frac{\delta_{k,n}}{d_{0,n}}\right) \\ &\approx d_{0,n} - \delta_{k,n} \end{aligned}$$

so

$$d_{k,n} - d_{0,n} \approx -\delta_{k,n}$$

In other words, the difference in the expected range measurement between a specific antenna and a specific satellite relative to the corresponding range measurement for that same satellite to the center of the antennae array is approximately equal to $-\delta_{k,n}$.

Finally, GPS pseudorange measurements combine the actual range with the receiver clock bias and noise. An equation for this simple measurement model is

$$\rho_{k,n} = d_{k,n} + b_k + w_{k,n}$$

in which $\rho_{k,n}$ is the pseudorange measurement for satellite n at antenna k, b_k is the clock bias of receiver k, and $w_{k,n}$ represents white Gaussian noise (assumed to be independent over k and n). As each receiver estimates and removes its own clock bias, the resulting model on the measured ranges is then

$$\widehat{d_{k,n}} = \rho_{k,n} - b_k = d_{k,n} + w_{k,n}$$

This expression assumes that the clock bias estimate is perfect so that all that remains is the additive noise. We return to this issue later in this paper.

THE HYPOTHESES

We consider two situations, the null hypothesis, H_0, in which no spoofer is present and the alternative hypothesis, H_1, in which a spoofer is present:

- H_0: With no spoofer present each individual range measurement is an accurate estimate of the actual range for that antenna and satellite pair.

  $$\widehat{d_{k,n}} = d_{k,n} + w_{k,n} = d_{0,n} - \delta_{k,n} + w_{k,n}$$

  for $k = 1, 2, ...m$ and $n = 1, 2, ...N$.

- H_1: With a spoofer present we assume that the individual antennae all receive identical RF signals, that we have a single point spoofer; hence, all would provide noisy estimates of the same ranges. (With only one radiator, a spoofer can create only one possible position solution [10]. Further, while the antennae will see the RF at slightly different times, due to the difference in propagation distance from the spoofer to each antenna, these time delays are absorbed by the receiver clock bias; hence, the receivers see identical RF.) Letting $d_n^{(s)}$ represent the spoofed range for satellite n, we have the observation model

  $$\widehat{d_{k,n}} = d_n^{(s)} + w_{k,n}$$

  for $k = 1, 2, ...m$ and $n = 1, 2, ...N$. Note that these are independent of the antennae positions and the rotation angle.

For simplicity we model each noise term, $w_{k,n}$, using independent Gaussian statistics with zero means and variance, σ^2, under both hypotheses. Under hypothesis H_0 and H_1, the pseudorange distributions are then

$$\widehat{d_{k,n}} \sim \mathcal{N}\left(d_{0,n} - \delta_{k,n}, \sigma^2\right) \quad \text{and} \quad \widehat{d_{k,n}} \sim \mathcal{N}\left(0, \sigma^2\right)$$

respectively. The notation $x \sim \mathcal{N}\left(\mu, \sigma^2\right)$ implies that the random variable x has a Gaussian distribution with mean μ and variance σ^2.

HYPOTHESIS TESTING

We imagine a Neyman-Pearson formulation for this problem and wish to develop a binary hypothesis test wtih fixed probability of false alarm (the probability of inaccurately deciding H_1 when H_0 is true). Hypothesis testing is implemented by computing a scalar function of the observation data, $T\left(\widehat{d_{1,1}}, ...\widehat{d_{m,N}}\right)$, called the test statistic, and comparing this value to a constant called the threshold. If the test statistic exceeds the threshold, we decide H_1; if not, we decide H_0. Symbolically we write this as

$$T\left(\left\{\widehat{d_{k,n}}\right\}\right) \underset{\mathrm{H}_0}{\overset{\mathrm{H}_1}{\gtrless}} \lambda$$

in which case we use the notation $\left\{\widehat{d_{k,n}}\right\}$ to represent the full set of mN range measurements. The optimum test statistic for the Neyman-Pearson formulation is well known to be the likelihood ratio [11]

$$T\left(\left\{\widehat{d_{k,n}}\right\}\right) = \frac{f\left(\left\{\widehat{d_{k,n}}\right\}\right)|\mathrm{H}_1}{f\left(\left\{\widehat{d_{k,n}}\right\}\right)|\mathrm{H}_0}$$

which is the ratio of the conditional probability density functions (pdfs) of the measurements under the two hypotheses. Usually, one simplifies the algebraic form of this test by taking monotonic functions of the result (e.g. the natural logarithm is very common for independent observations) and ignoring any additive and positive multiplicative terms that are independent of the data. As noted in the section above, we will assume that the pdfs are Gaussian.

If one has a complete characterization of the two hypotheses, then the development of the test statistic is usually quite straightforward. The work, then, is the development of the expressions for the probability of false alarm (so that the threshold can be selected) and the probability of detection, the resulting performance. If some of the parameters are unknown, additional analysis and/or approximations are required.

Under the statistical assumptions stated above the the likelihood ratio test is

$$T\left(\left\{\widehat{d_{k,n}}\right\}\right) = \prod_{k=1}^{m}\prod_{n=1}^{N} \frac{\frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{\left(\widehat{d_{k,n}} - d_n^{(s)}\right)^2}{2\sigma^2}}}{\frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{\left(\widehat{d_{k,n}} - d_{0,n} + \delta_{k,n}\right)^2}{2\sigma^2}}}$$

Taking the natural logarithm, simplifying the algebra, and ignoring any additive or positive multiplicative constants yields an equivalent test statistic

$$T\left(\left\{\widehat{d_{k,n}}\right\}\right) = \sum_{k=1}^{m}\sum_{n=1}^{N} \widehat{d_{k,n}} \left[d_n^{(s)} - d_{0,n} + \delta_{k,n}\right]$$

An obvious problem with this test statistic is that it requires knowledge of the position through the occurrence of $d_n^{(s)}$ and $d_{0,n}$ in the computation, both of which are unknown. One common approach, the generalized likelihood ratio test (GLRT) [11], estimates the unknown parameters under the two hypotheses (typically a maximum likelihood estimate, MLE) and substitutes those values into the test statistic. We consider two cases depdending upon whether or not the orientation of the antenna array, through the variable θ, is known. The known orientation case is derived in [9] while the interesting unknown orientation case is developed in Appendix A.

- **Known Orientation:** It is shown in [9] that the MLE of $d_n^{(s)}$ and $d_{0,n}$ are identical; hence, if θ is known then the hypothesis test reduces to

  $$T\left(\left\{\widehat{d_{k,n}}\right\}\right) = \sum_{k=1}^{m}\sum_{n=1}^{N} \widehat{d_{k,n}} \delta_{k,n} \underset{\mathrm{H}_0}{\overset{\mathrm{H}_1}{\gtrless}} \lambda$$

for some threshold λ. This detector can be interpreted as a spatial correlator.

- **Unknown Orientation:** In this case the MLEs of $d_n^{(s)}$ and $d_{0,n}$ are still equal, and we must use the MLE of θ. Denoting $\widehat{\delta_{k,n}}$ as the estimated $\delta_{k,n}$ using $\hat{\theta}$, the hypothesis test is

$$T\left(\left\{\widehat{d_{k,n}}\right\}\right) = \sum_{k=1}^{m}\sum_{n=1}^{N}\widehat{d_{k,n}}\widehat{\delta_{k,n}} \overset{\mathrm{H}_0}{\underset{\mathrm{H}_1}{\gtrless}} \lambda^2$$

with λ^2 a threshold yet to be determined. After manipulation (see Appendix A), this can be shown to be equivalent to the test

$$T_s^2 + T_c^2 \overset{\mathrm{H}_0}{\underset{\mathrm{H}_1}{\gtrless}} \lambda^2$$

with

$$T_s = \sum_{n=1}^{N}\sum_{n=1}^{N}\widehat{d_{k,n}} \cos\psi_n \sin\left(\phi_{n,0} - \frac{2\pi\,(k-1)}{m}\right)$$

and

$$T_c = \sum_{n=1}^{N}\sum_{n=1}^{N}\widehat{d_{k,n}} \cos\psi_n \cos\left(\phi_{n,0} - \frac{2\pi\,(k-1)}{m}\right)$$

In comparison to the known orientation test above, note that the direction of the threshold test has changed. Further, this test can be interpreted as a non-coherent form of the spatial correlator.

Note – due to the symmetry of the $\delta_{k,n}$ (and the $\widehat{d_{k,n}}$) any satellite specific term in $\widehat{d_{k,n}}$ contributes zero in the test statistic in either case. For example, any additional delay due to the ionosphere, troposphere, orbital error, or satellite clock issue that is common to all receivers for a specific satellite has no impact on the spoof detection; hence initially ignoring those terms in our measurement model is not a limitation on the results.

PERFORMANCE OF THE TEST WITH KNOWN ORIENTATION

As a linear combination of Gaussian variables, the test statistic

$$T\left(\left\{\widehat{d_{k,n}}\right\}\right) = \sum_{k=1}^{m}\sum_{n=1}^{N}\widehat{d_{k,n}}\delta_{k,n}$$

is also Gaussian distributed. Specifically (and see [9] for details) under hypotheses H_0 and H_1, the distributions are

$$T \sim \mathcal{N}\left(\mu_0, \sigma_T^2\right) \quad \text{and} \quad T \sim \mathcal{N}\left(0, \sigma_T^2\right)$$

respectively, with

$$\mu_0 = -\frac{mr^2}{2}\sum_{n=1}^{N}\cos^2\psi_n$$

and

$$\sigma_T^2 = \frac{mr^2\sigma^2}{2}\sum_{n=1}^{N}\cos^2\psi_n$$

For a hypothesis test with Gaussian statistics the false alarm probability is

$$\mathrm{P_{fa}} = \mathrm{Prob}(T > \lambda|\mathrm{H}_0) = Q\left(\frac{\lambda-\mu}{\sigma_T}\right)$$

(Q(·) being the Gaussian tail probability). If $\mathrm{P_{fa}}$ is fixed (which is typical for a Neyman-Pearson formulation), then we can solve for the threshold as

$$\lambda = \sigma_T Q^{-1}(\mathrm{P_{fa}}) + \mu_0$$

The power, or the detection probability, of the test is then

$$\begin{aligned}\mathrm{P_d} &= \mathrm{Prob}(T > \lambda|\mathrm{H}_1) = Q\left(\frac{\lambda-\mu_1}{\sigma_T}\right)\\ &= Q\left(Q^{-1}(\mathrm{P_{fa}}) + \frac{\mu_0-\mu_1}{\sigma_T}\right)\end{aligned}$$

Substituting in our expressions for the means ($\mu_1 = 0$) and variance, and simplifying, yields

$$\mathrm{P_d} = Q\left(Q^{-1}(\mathrm{P_{fa}}) - \sqrt{\frac{mr^2}{2\sigma^2}\sum_{n=1}^{N}\cos^2\psi_n}\right)$$

This result has the expected characteristics: $\mathrm{P_d}$ increases for larger m and/or larger r; it decreases with larger σ. It is interesting to see the dependence on the number of satellites (N) and their elevations (ψ_n); more and lower satellites improve performance.

Let's define the spatial SNR as

$$\mathrm{SSNR} \equiv \frac{mr^2}{2\sigma^2}\sum_{n=1}^{N}\cos^2\psi_n$$

Clearly the larger this term is, the better the performance is. Further, define the scale parameter

$$\gamma = \frac{r}{\sigma}$$

then

$$\mathrm{SSNR} = \frac{m}{2}\gamma^2\sum_{n=1}^{N}\cos^2\psi_n$$

In other words, a decrease in σ (the user range error, URE) allows for a corresponding decrease in the antenna pattern radius r without a change in performance. Next, consider the satellite dependent term

$$\mathit{Sky\ Term} \equiv \sum_{n=1}^{N} \cos^2 \psi_n$$

While we cannot reduce this analytically as it is a complex function of the sky view, we can use GPS almanacs to explore its variation in time. For example, at longitude 072°W and latitude 41°N (near the authors' work locations) the *Sky Term* ranges from 3 to 10 with an average of approximately 6 as shown in Figure 1. An sample assessment of North America [9] shows a daily average value ranging from 5 to 9.

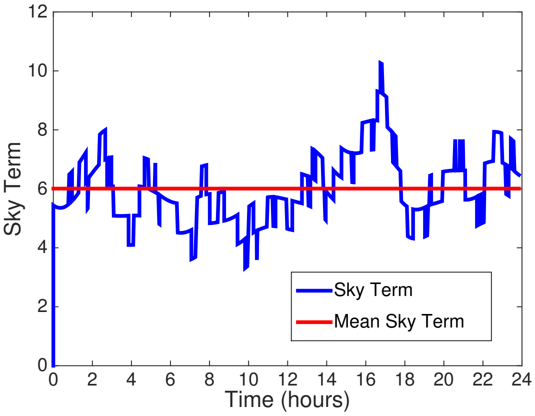

Figure 1: Example of *Sky Term* over 24-hour period.

As an example, Figures 2 and 3 show the receiver operating characteristic (ROC) for $\gamma = 1$, $m = 3$ receivers, and $\mathit{Sky\ Term} = 5$. The left subplot is the full ROC; the right subplot zooms in for low $\mathrm{P_{fa}}$. Even at a value of $\gamma = 1$ performance is quite good!

PERFORMANCE OF THE TEST WITH UNKNOWN ORIENTATION

With unknown orientation, the hypothesis test is

$$T_s^2 + T_c^2 \underset{\mathrm{H}_1}{\overset{\mathrm{H}_0}{\gtrless}} \lambda^2$$

with T_s and T_c defined above. On the (T_s, T_c) plane this is a test of falling inside or outside a circle of radius λ (with, in general, a different λ from the known orientation test above).

Appendix B addresses the statistics of these two test variables. Specifically, they are jointly Gaussian under

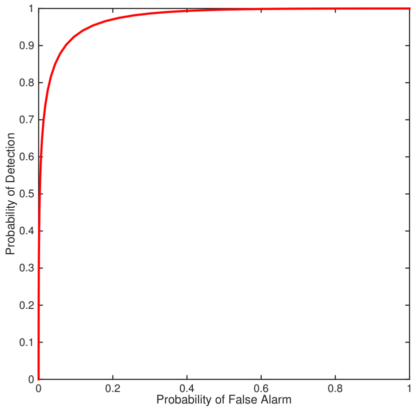

Figure 2: Typical ROC for the test with known orientation ($\gamma = 1, m = 3$, and $\mathit{Sky\ Term} = 5$).

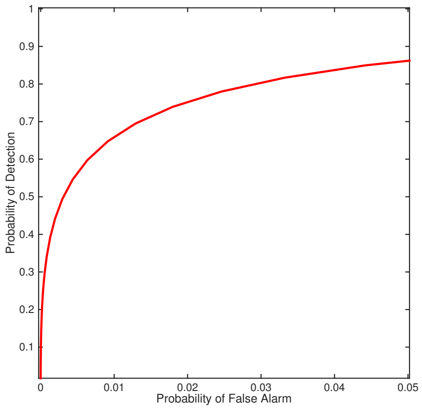

Figure 3: Typical ROC for the test with known orientation ($\gamma = 1, m = 3$, and $\mathit{Sky\ Term} = 5$).

both hypotheses:

$$\{T_s, T_c\}_{\mathrm{H}_0} \sim \mathcal{N}\left(\mu_{s,0}, \mu_{c,0}, \sigma_T^2, \sigma_T^2, 0\right)$$

and

$$\{T_s, T_c\}_{\mathrm{H}_1} \sim \mathcal{N}_g\left(0, 0, \sigma_T^2, \sigma_T^2, 0\right)$$

(this notation lists the two means, two variances, and the correlation coefficient, respectively, of the bivariate Gaussian pdf) with

$$\mu_{s,0} = \frac{mr}{2} \sin\theta \sum_{n=1}^{N} \cos^2 \psi_n$$

$$\mu_{c,0} = \frac{mr}{2} \cos\theta \sum_{n=1}^{N} \cos^2 \psi_n$$

and

$$\sigma_T^2 = \frac{m\sigma^2}{2} \sum_{n=1}^{N} \cos^2 \psi_n$$

Of significance in these results is the common variances and the zero correlation coefficients; the joint pdfs of the test statistic have contours of constant probability that are circles under both hypotheses.

The probability of detection is the probability under H_1 that the test statistic is smaller than the threshold

$$\mathrm{P_d} = \mathrm{Prob}_{\mathrm{H}_1}\left(T_s^2 + T_c^2 < \lambda^2\right)$$

Since $\{T_s, T_c\}$ are bivariate Gaussian with zero means and equal variances under H_1 then

$$\mathrm{P_d} = \iint\limits_{\Omega} \frac{1}{2\pi\sigma_T^2} e^{-\frac{1}{2\sigma_T^2}\left(T_s^2+T_c^2\right)} dT_s dT_c$$

in which Ω is the disk about the origin of radius λ. Changing variables to polar coordinates of magnitude s (chosen to avoid using r with two definitions) and phase angle ϕ yields

$$\mathrm{P_d} = \int_0^{2\pi}\int_0^{\lambda} \frac{s}{2\pi\sigma_T^2} e^{-\frac{s^2}{2\sigma_T^2}} ds d\phi$$

in which we have explicitly described the limits of integration of Ω. Integrating first over ϕ, then over s yields

$$\mathrm{P_d} = 1 - e^{-\frac{\lambda^2}{2\sigma_T^2}}$$

The probability of false alarm of the test is the probability under H_0 that the test statistic is smaller than the threshold

$$\mathrm{P_{fa}} = \mathrm{Prob}_{\mathrm{H}_0}\left(T_s^2 + T_c^2 < \lambda^2\right)$$

Again, $\{T_s, T_c\}$ are bivariate Gaussian, but with nonzero means, so

$$\mathrm{P_{fa}} = \iint\limits_{\Omega} \frac{1}{2\pi\sigma_T^2} e^{-\frac{(T_s-\mu_{s,0})^2+(T_c-\mu_{c,0})^2}{2\sigma_T^2}} dT_s dT_c$$

Changing to polar coordinates yields

$$\mathrm{P_{fa}} = \int_0^{\lambda} \frac{s}{\sigma_T^2} e^{-\frac{s^2+\mu_{s,0}^2+\mu_{c,0}^2}{2\sigma_T^2}} \left[\int_0^{2\pi} \frac{1}{2\pi} e^{\frac{s\sqrt{\mu_{s,0}^2+\mu_{c,0}^2}}{\sigma_T^2}\cos(\phi-\theta)} d\phi\right] ds$$

where θ is the unknown orientation of the antennae array. Now, the inner integral in brackets can be manipulated by changing variables to $\zeta = \phi - \theta$, using the periodicity of the cosine function to shift the integration limits, and recognizing the definition of the modified Bessel function of the first kind. The result for the false a alarm probability is then

$$\mathrm{P_{fa}} = \int_0^{\lambda} \frac{s}{\sigma_T^2} e^{-\frac{s^2+\mu_{s,0}^2+\mu_{c,0}^2}{2\sigma_T^2}} I_0\left(\frac{s\sqrt{\mu_{s,0}^2+\mu_{c,0}^2}}{\sigma_T^2}\right) ds$$

This final form for $\mathrm{P_{fa}}$ can be written in terms of Marcum's Q function [11]

$$\mathrm{P_{fa}} = 1 - Q\left(\gamma\sqrt{\frac{m}{2} Sky\ Term}, \frac{\lambda}{\sigma_T}\right)$$

At this point we have expressions for $\mathrm{P_{fa}}$ and $\mathrm{P_d}$ in terms of the system parameters of number of antennae m, spacing of antennae r, user range error σ^2, and the geometric $Sky\ Term$. We can invert the $\mathrm{P_d}$ expression for the threshold λ

$$\lambda = \sigma_T\sqrt{-2\ln(1-\mathrm{P_d})}$$

Inserting this result into the expression for $\mathrm{P_{fa}}$ we have

$$\mathrm{P_{fa}} = 1 - Q\left(\sqrt{\frac{mr^2}{2}\sum_{n=1}^{N}\cos^2\psi_n}, \sqrt{-2\ln(1-\mathrm{P_d})}\right)$$

We acknowledge that some might think that this expression is backwards, that it is more usual in hypothesis testing to write the detection probability as a function of the false alarm probability. However, the utility of this closed-form expression is that for a fixed $\mathrm{P_d}$ and measurement noise variance, σ^2, the known monotonically of Marcum's Q function in its arguments implies that our test's performance improves with increasing r,m, and $Sky\ Term$.

As an example, Figures 4 and 5 shows the ROC for $\gamma = 1$, $m = 3$ receivers, and $Sky\ Term = 5$. For comparison, the performance with known orientation is also shown. As presented previously, the first plot is the full ROC; the second plot zooms in for low $\mathrm{P_{fa}}$. While an unknown orientation does result in some performance loss, performance is still quite good!

THE EFFECT OF CLOCK ERROR

We noted above that the actual GNSS measurements are pseudoranges

$$\rho_{k,n} = d_{k,n} + b_k + w_{k,n}$$

in which $d_{k,n}$ is the true range, b_k is the clock bias of receiver k, and $w_{k,n}$ represents white Gaussian noise (assumed to be independent over k and n). Further, our initial assumption was that each receiver estimates

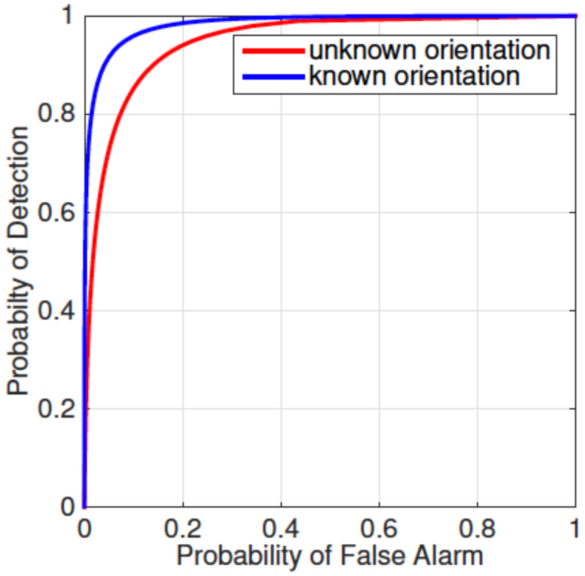

Figure 4: ROC comparison for unknown orientation vs. known orientation

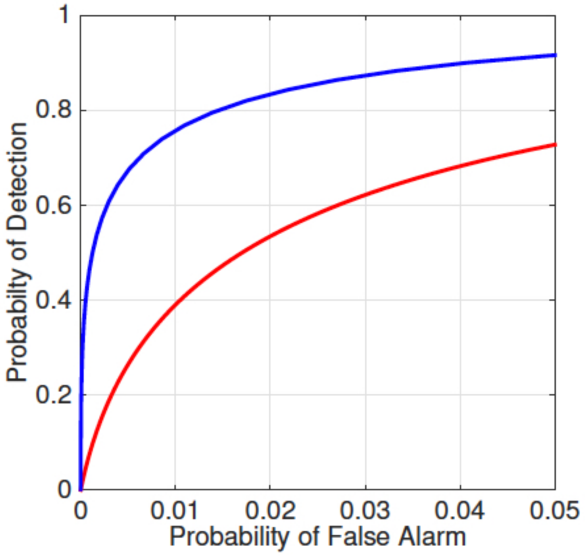

Figure 5: ROC comparison for unknown orientation vs. known orientation (zoomed in)

and removes its own clock bias and that the estimate is perfect so that

$$\widehat{d_{k,n}} = \rho_{k,n} - b_k = d_{k,n} + w_{k,n}$$

More realistically, however, the bias is not known perfectly and the receiver employs an estimate $\widehat{b_k}$, so

$$\begin{aligned}\widehat{d_{k,n}} &= \rho_{k,n} - \widehat{b_k} \\ &= d_{k,n} + b_k - \widehat{b_k}_{w_{k,n}} \\ &= d_{k,n} + \epsilon_k + w_{k,n}\end{aligned}$$

in which we define the clock bias error as $\epsilon_k = b_k - \widehat{b_k}$.

Appendix C characterizes the joint statistics of ϵ_k and $w_{k,n}$. The utility of these results is that we can reconsider the statistics of the test. Consider the known orientation case. Expanding the relevant test statistic

$$\begin{aligned}T\left(\left\{\widehat{d_{k,n}}\right\}\right) &= \sum_{k=1}^{m}\sum_{n=1}^{N}\widehat{d_{k,n}}\delta_{k,n} \\ &= \sum_{k=1}^{m}\sum_{n=1}^{N}\left(d_{k,n} + \epsilon_k + w_{k,n}\right)\delta_{k,n} \\ &= \sum_{k=1}^{m}\sum_{n=1}^{N}d_{k,n}\delta_{k,n} + \sum_{k=1}^{m}\sum_{n=1}^{N}\left(\epsilon_k + w_{k,n}\right)\delta_{k,n}\end{aligned}$$

The first term is the mean of the test statistic, which is the same as that appearing in the analysis in [9]; the second term is a more complicated noise term. The mean of this noise term is still zero (as it was above) but, in contrast to the original analysis, the occurance of the ϵ_k terms changes the variances. Specifically, the test statistic's variance increases to

$$\sigma_{T'}^2 = \sigma^2\mathbf{h}^T\mathbf{h}\sum_{k=1}^{m}\left(\sum_{n=1}^{N}\delta_{k,n}\right)^2 + \sigma^2\sum_{k=1}^{m}\sum_{n=1}^{N}\delta_{k,n}^2$$

($\mathbf{h}$ is defined in Appendix C) which decreases performance.

As an example, Figure 6 extends the results shown in Figure 3 above, showing the ROC when the clock noise is included ($\gamma = 1$, $m = 3$ receivers, and $Sky\ Term = 5$). For comparison, the performance with no clock effect is also shown. While the clock bias reduces performance, the drop is quite small.

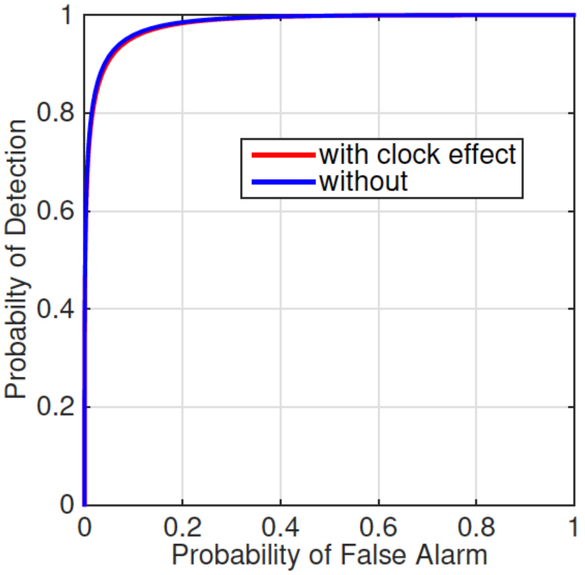

Figure 6: ROC showing test with known orientation including clock noise

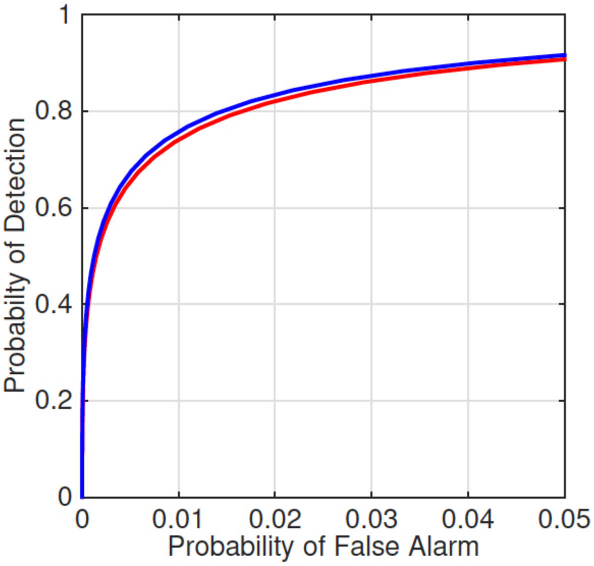

Figure 7: ROC showing test with known orientation including clock noise (zoomed-in)

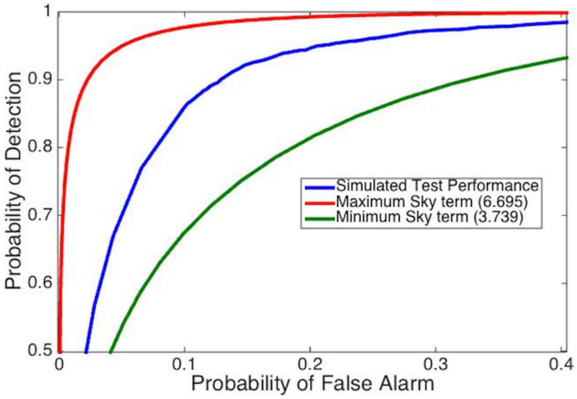

Figure 8: Simulation ROC curve with performance bounds

SIMULATION RESULTS

The ROC curves presented thus far were generated using the theoretical performance equations for $\mathrm{P_{fa}}$ and $\mathrm{P_d}$ given above. Seeking to further substantiate the performance claims for this detection algorithm, a simulation was conducted using a Spirent GSS 8000 simulator to generate a model GPS constellation and feed the RF into a Novatel ProPak v3 GPS receiver. The receiver's range measurements and satellite azimuth/elevation information were output to a companion laptop for post-processing. The above detection test statistics were calculated every second and a performance curve drawn modeling the realized performance.

Figure 8 shows the observed performance (plotted in blue) against upper and lower bound theoretical performance curves. These two curves used the maximum and minimum $Sky\ Term$ values observed throughout the course of the 24-hour test. A significant observation worth noting is that the observed performance curve appears to be (and in fact is, in a way) an average of the maximum and minimum $Sky\ Term$ curves. As noted multiple times above, the performance is dependent on this constantly changing $Sky\ Term$; no two snapshots are exactly the same. This means a unique threshold is calculated for each snapshot, and if a performance curve was plotted for each calculated threshold, they would fill in all the space between these performance bounds.

COMPARISON TO PRIOR WORK

It is of interest to compare the performance results of spoof detection based on pseudoranges to our prior results for detection based solely on the position solutions from the receivers.

Our ION GNSS+ 2013 paper [?] developed the form of the test when the only data available is the receiver position x_k (east and north components, written as a complex quantity). Assuming known rotation θ and antenna positions d_k, the optimum test was shown to be

$$T' = \sum_{k=1}^{m} 2\Re\left\{-d_k^* e^{-j\theta} x_k\right\} \underset{\mathrm{H}_0}{\overset{\mathrm{H}_1}{\gtrless}} \lambda'$$

Effectively this test first undoes the rotation by θ, then correlates the complex observations, the x_k, against the known orientation components, the d_k; this is a spatial correlator. If the orientation is unknown, the optimum test was shown to be

$$T'(x_1, \dots x_m) = -\left|\sum_{k=1}^{m} d_k^* x_k\right| \underset{\mathrm{H}_0}{\overset{\mathrm{H}_1}{\gtrless}} \lambda'$$

a "non-coherent" spatial correlator.

Our ION ITM 2014 paper [8] employed a better model of the errors in the position observation for use in analyses of both of these tests. For the spatial correlation (known orientation), the performance was shown to be

$$\mathrm{P_d} = Q\left(Q^{-1}(\mathrm{P_{fa}}) - \sqrt{\frac{2mr^2}{\sigma^2 \mathrm{HDOP}^2}}\right) \qquad (1)$$

The performance for the non-coherent version was shown to be

$$\mathrm{P_{fa}} = 1 - Q\left(\sqrt{\frac{2mr^2}{\Gamma}}, \sqrt{-2\ln(1-\mathrm{P_d})}\right) \qquad (2)$$

Based on pseudoranges (and ignoring clock bias estimation effects), the current paper develops performance expressions as well. With known orientation, we have performance

$$\mathrm{P_d} = Q\left(Q^{-1}(\mathrm{P_{fa}}) - \sqrt{\frac{mr^2}{2\sigma^2}\sum_{n=1}^{N}\cos^2\psi_n}\right)$$

Comparing back to Eq. 1 the only difference is the term under the square root and we note that we would like the largest square root term possible. In other words, expecting that the pseudorange test should perform better than the position based test, we expect

$$\frac{2mr^2}{\sigma^2 \mathrm{HDOP}^2} < \frac{mr^2}{2\sigma^2}\sum_{n=1}^{N}\cos^2\psi_n \qquad (3)$$

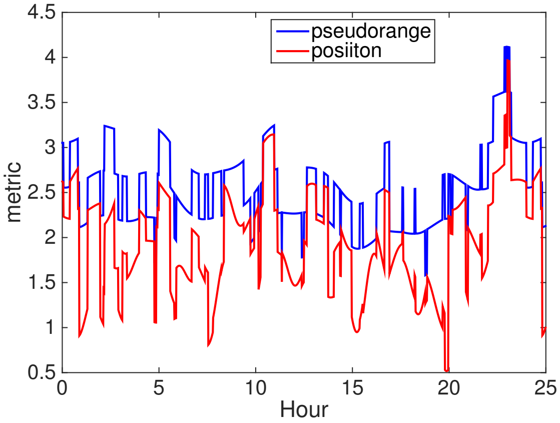

Figure 9: Performance metric for spoof detection with unknown orientation; pseudorange and position based tests.

and want to explore how much the difference is.

With unknown orientation (but still zero clock bias) the pseudorange based test's performance is

$$\mathrm{P_{fa}} = 1 - Q\left(\sqrt{\frac{mr^2}{2\sigma^2}\sum_{n=1}^{N}\cos^2\psi_n}, \sqrt{-2\ln(1-\mathrm{P_d})}\right)$$

Comparing back to Eq. 2 the only difference is the expression under the square root of the first argument which we note is the same expression as seen in the known orientation case, and again we would like the largest square root term possible.

The terms for comparision appears in Eq. 3. Canceling common terms (r, σ^2, and m) the expression is

$$\frac{1}{2}\sum_{n=1}^{N}\cos^2\psi_n > \frac{2}{\mathrm{HDOP}^2}$$

Figure 9 compares these two metrics over the course of 24 hours at our location. Recall that larger values are better from a detection performance perspective. As expected, the pseudorange based detector has superior performance.

We can characterize the increase by taking the ratio and converting to a decibel scale

$$\text{gain} = 10\log_{10}\left(\frac{\mathrm{HDOP}^2}{4}\sum_{n=1}^{N}\cos^2\psi_n\right)$$

This gain is plotted in Figure 10; the average observed improvement is 1.4 dB. The performance gain varies greatly with time; a look at Figures 11 and 12 provides some insight into the explanation. Although the

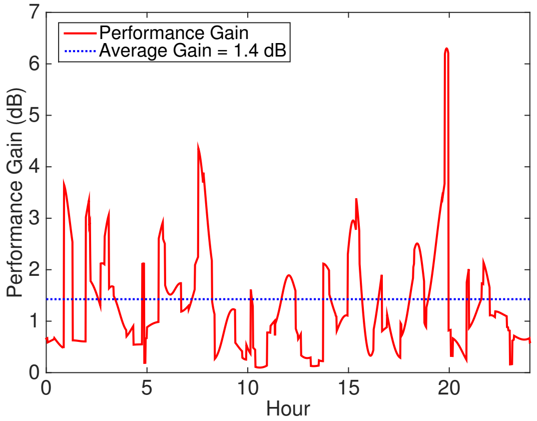

Figure 10: Performance gain of pseudorange testing over position testing (in dB).

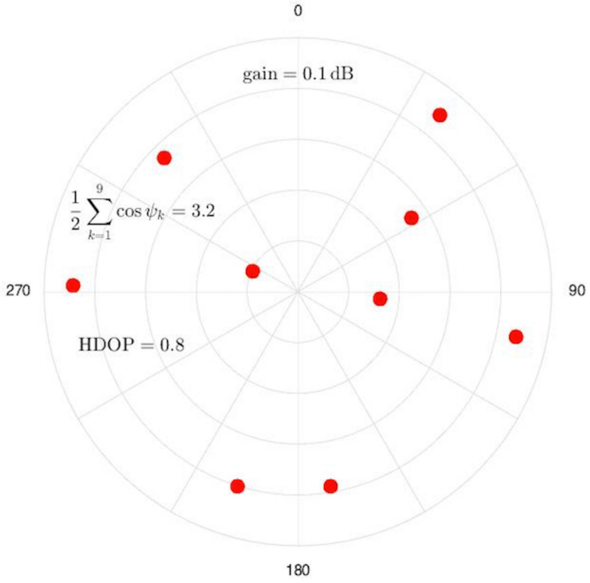

Figure 11: Sky view when the pseudorange is only marginally better than the position based test.

Sky Term is roughly 30% greater in Figure 11, the HDOP is less than half of that in Figure 12. This indicates the both the robustness of the pseudorange based test (continuous strong performance) and the volatility of the position solution based test. While low-elevation satellites are more heavily weighted in the pseudorange test, the loss of performance in the position solution test due to the increased HDOP from these same low-elevation satellites proves the stronger dependence on this term.

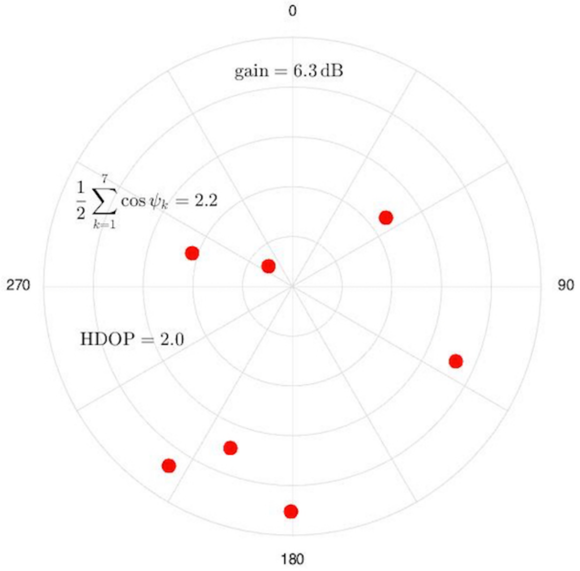

Figure 12: Sky view when the pseudorange is much better than the position based test.

CONCLUSIONS

In conclusion, this paper has demonstrated a new approach for detecting GNSS spoofing attacks leveraging pseudorange measurements from an array of receivers. The performance of this method was shown to depend on the number of antennas and the distance they are spaced within the multi-antennae array as well as the geometry of the visible GNSS satellite constellation. Imperfect clock bias measurements or an unknown array orientation can further impact the detector performance, but upon analysis the detector is quite robust against these detriments. Lastly, when compared to prior work using a similar approach with final GPS position solutions, the presented detector proved superior; the average improvement over the simulated period was 1.4dB increase in performance.

APPENDIX A – SIMPLIFYING THE UNKNOWN ORIENTATION TEST

Recall that the effect of θ is through the pseudorange offsets, $\delta_{k,n}$, which are themselves functions of the θ_k. Evaluated at the MLE of θ, these are

$$\widehat{\delta_{k,n}} = r\cos\psi_n \left[\sin\phi_n \sin\left(\frac{2\pi(k-1)}{m} + \widehat{\theta}\right) \dots \right.$$
$$\left. + \cos\phi_n \cos\left(\frac{2\pi(k-1)}{m} + \widehat{\theta}\right)\right]$$

Expanding the sine and cosine of the sum of angles and then recombining in a different order

$$\widehat{\delta_{k,n}} \quad = \quad r\cos\psi_n \left[\begin{array}{c} \cos\left(\phi_n - \dfrac{2\pi(k-1)}{m}\right)\cos\widehat{\theta} \\ +\sin\left(\phi_n - \frac{2\pi(k-1)}{m}\right)\sin\widehat{\theta} \end{array} \right]$$

so we need the cosine and sine of $\widehat{\theta}$.

For brevity, let us define η as

$$\eta = \phi_n - \frac{2\pi(k-1)}{m}$$

We have

$$\tan\widehat{\theta} = \frac{\displaystyle\sum_{n=1}^{N}\sum_{k=1}^{m}\widehat{d_{k,n}}\cos\psi_n\sin(\eta)}{\displaystyle\sum_{n=1}^{N}\sum_{k=1}^{m}\widehat{d_{k,n}}\cos\psi_n\cos(\eta)}$$

so

$$\cos\widehat{\theta} = \frac{\displaystyle\sum_{n=1}^{N}\sum_{k=1}^{m}\widehat{d_{k,n}}\cos\psi_n\cos(\eta)}{D}$$

and

$$\sin\widehat{\theta} = \frac{\displaystyle\sum_{n=1}^{N}\sum_{k=1}^{m}\widehat{d_{k,n}}\cos\psi_n\sin(\eta)}{D}$$

in which common denominator term is

$$D = \sqrt{\begin{array}{c}\left(\displaystyle\sum_{n=1}^{N}\sum_{k=1}^{m}\widehat{d_{k,n}}\cos\psi_n\cos(\eta)\right)^2 \\ +\left(\displaystyle\sum_{n=1}^{N}\sum_{k=1}^{m}\widehat{d_{k,n}}\cos\psi_n\sin(\eta)\right)^2\end{array}}$$

Substituting yields the resulting test.

APPENDIX B – ANALYSIS WITH UNKNOWN ORIENTATION

With unknown orientation the test statistic is

$$\left(\sum_{n=1}^{N}\sum_{k=1}^{m}\widehat{d_{k,n}}\cos\psi_n\sin(\eta)\right)^2 + \left(\sum_{n=1}^{N}\sum_{k=1}^{m}\widehat{d_{k,n}}\cos\psi_n\cos(\eta)\right)^2 = {T_s}^2 + {T_c}^2$$

in which we've provided names for the two terms in parentheses so that we can examine them individually. We note that both T_s and T_c are linear functions of the $\widehat{\rho_{k,n}}$. Further, recall that each $\widehat{d_{k,n}}$ is a random variable, either

$$\widehat{d_{k,n}} = \rho_{k,n} + w_{k,n} = d_{0,n} - \delta_{k,n} + w_{k,n}$$

or

$$\widehat{d_{k,n}} = d_n^{(s)} + w_{k,n}$$

depending upon the hypothesis. As we are assuming that the $w_{k,n}$ are iid Gaussian random variables, then T_s and T_c are jointly Gaussian under both hypotheses:

$$\{T_s, T_c\}_{\mathrm{H}_0} \sim \mathcal{N}\left(\mu_{s,0}, \mu_{c,0}, \sigma_{s,0}^2, \sigma_{c,0}^2, \rho_0\right)$$

and

$$\{T_s, T_c\}_{\mathrm{H}_1} \sim \mathcal{N}\left(\mu_{s,1}, \mu_{c,1}, \sigma_{s,1}^2, \sigma_{c,1}^2, \rho_1\right)$$

(the parameters being the two means, two variances, and correlation coefficient). To continue we need these parameters under both hypotheses.

Under H_0 taking expectations yields

$$\mu_{s,0} \quad = \quad \sum_{n=1}^{N}\sum_{k=1}^{m} d_{k,n}\cos\psi_n\sin(\eta)$$

and

$$\mu_{c,0} \quad = \quad \sum_{n=1}^{N}\sum_{k=1}^{m} d_{k,n}\cos\psi_n\cos(\eta)$$

while under H_1 both reduce further to $\mu_{s,1} = 0$ and $\mu_{c,1} = 0$.

To compute the variances, note that the individual terms of the summations in both T_s and T_c are themselves independent (since the $w_{k,n}$ are iid); hence, after tedious algebra we have

$$\sigma_{s,1}^2 = \sigma_{s,0}^2 \quad = \quad \frac{m\sigma^2}{2}\sum_{n=1}^{N}\cos^2\psi_n$$

Similarly,

$$\sigma_{c,0}^2 = \sigma_{c,1}^2 = \sigma_{s,0}^2$$

All four variances are equal.

The remaining parameter is the correlation coefficient, ρ, under both hypotheses. As a characteristic of the random variables without their means, ρ will be the same under both hypotheses. Substantial algebra yields zero for both hypotheses.

To conclude this Appendix, we note that trigonometric manipulation allows us to simplify the $\mu_{s,0}$ and $\mu_{c,0}$ terms to

$$\mu_{s,0} = \frac{mr}{2}\sin\theta\sum_{n=1}^{N}\cos^2\psi_n$$

and

$$\mu_{c,0} = \frac{mr}{2}\cos\theta\sum_{n=1}^{N}\cos^2\psi_n$$

Further, we note that

$$\sqrt{\mu_{s,0}^2 + \mu_{c,0}^2} = \frac{mr}{2} \sum_{n=1}^{N} \cos^2 \psi_n$$

APPENDIX C – CLOCK BIAS EFFECTS

This appendix considers the pseudoranges and clock bias for a single receiver (i.e. we drop the subscript k) since the process of solving for an estimate of the clock bias is independent from receiver to receiver.

Recall that the GNSS pseudorange measurements combine the actual range with the receiver clock bias and noise

$$\rho_n = d_n + b + w_n$$

in which ρ_n is the pseudorange measurement for satellite n, b is the clock bias, and w_n represents the white Gaussian measurement noise (assumed to be independent over n). In the spoofing detection algorithm development and analysis above we assumed that each receiver estimates and removes its own clock bias perfectly so that the measurement consisted of only the true range and noise

$$\widehat{d_n} = \rho_n - b = d_n + w_n$$

This appendix explores this issue further.

First, let's define the estimate of the clock bias as $\widehat{b}$; the range measurement is, then

$$\widehat{d_n} = \rho_n - \widehat{b} = d_n + w_n + b - \widehat{b} = d_n + w_n + \epsilon$$

Our goal is to show that the clock estimation error, ϵ, is just an additional noise term.

The unknowns in the standard GNSS problem are the receiver position and the clock bias

$$\mathbf{x} = \begin{bmatrix} x \\ y \\ z \\ b \end{bmatrix}$$

and the observables are the N pseudoranges

$$\boldsymbol{\rho} = \begin{bmatrix} \rho_1 \\ \rho_2 \\ \vdots \\ \rho_N \end{bmatrix}$$

Suppose that $\mathbf{x}$ is the least squares solution for the given observables, then for small perturbations $\delta\boldsymbol{\rho}$ and $\delta\mathbf{x}$ we have

$$\delta\boldsymbol{\rho} = \mathbf{H}\,\delta\mathbf{x}$$

where $\mathbf{H}$ is the geometry matrix

$$\mathbf{H} = \begin{bmatrix} \cos\psi_1 \sin\phi_1 & \cos\psi_1 \cos\phi_1 & \sin\psi_1 & 1 \\ \cos\psi_2 \sin\phi_2 & \cos\psi_2 \cos\phi_2 & \sin\psi_2 & 1 \\ \vdots & \vdots & \vdots & \vdots \\ \cos\psi_N \sin\phi_N & \cos\psi_N \cos\phi_N & \sin\psi_N & 1 \end{bmatrix}$$

Equivalently, at the solution to the least squares problem, we have

$$\delta\mathbf{x} = \left(\mathbf{H}^T\mathbf{H}\right)^{-1} \mathbf{H}^T\,\delta\boldsymbol{\rho}$$

This expression relates changes in the measurements to changes in the solution; of interest here is the last element of $\delta\mathbf{x}$, the clock bias estimate.

We note the following:

- Consider the case of pseudoranges with a constant bias b, but no noise

  $$\rho_n = d_n + b$$

  so that each $\delta\boldsymbol{\rho}$ is the constant vector $[b, b, \ldots, b]^T$. In this case each $\delta\mathbf{x}$ is zero except for the clock term

  $$\delta\mathbf{x} = \left(\mathbf{H}^T\mathbf{H}\right)^{-1} \mathbf{H}^T\, b\mathbf{1} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ b \end{bmatrix}$$

  with $\mathbf{1} = [1, 1, \ldots 1]^T$.

- Consider the case of pseudoranges with zero bias and white noise with standard deviation σ

  $$\rho_n = d_n + w_n$$

  so that each $\delta\boldsymbol{\rho}$ is the iid noise vector $[w_1, w_2, \ldots, w_N]^T$. In this case the DOP matrix provides the covariance matrix of the solution

  $$\Sigma_{\mathbf{x}} = \left(\mathbf{H}^T\mathbf{H}\right)^{-1} \sigma^2$$

  Most importantly, the clock estimate error, ϵ, has variance determined by the bottom right element of this matrix

  $$\sigma_z^2 = \left(\mathbf{H}^T\mathbf{H}\right)^{-1}_{[4,4]} \sigma^2$$

  The multiplier is the TDOP (time dilution of precision).

- The estimate of the clock bias is a deterministic function of the true clock bias, the pseudorange measurement noise, and the geometry matrix

  $$\widehat{b} = b + \mathbf{h}^T\,\mathbf{w}$$

in which b is the deterministic bias, $\mathbf{w} = [w_1, w_2, \ldots, w_N]^T$ is the noise, and $\mathbf{h}^T = [h_1, h_2, \ldots, h_n]$ is the 4^{th} row of $\left(\mathbf{H}^T\mathbf{H}\right)^{-1}\mathbf{H}^T$ (the transpose is employed so that all vectors are column vectors). Further, since the clock bias error is $\epsilon = b - \widehat{b}$, in terms of the noise it is

$$\epsilon = -\mathbf{h}^T\,\mathbf{w}$$

- The clock bias error, ϵ, is a Gaussian random variable with distribution

  $$\epsilon \sim \mathcal{N}\left(0, \sigma^2\mathbf{h}^T\mathbf{h}\right) = \mathcal{N}\left(0, \sigma^2\mathrm{TDOP}^2\right)$$

  in which TDOP is the 4,4 element of the DOP matrix. Further, since the clock bias estimate satisfies $\widehat{b} = b - \epsilon$, $\widehat{b}$ is also a Gaussian random variable

  $$\widehat{b} \sim \mathcal{N}\left(b, \sigma^2\mathbf{h}^T\mathbf{h}\right)$$

  The covariance of ϵ and the individual noise terms, the w_n, is

  $$\mathrm{Cov}\left(\epsilon, w_n\right) = -\sigma^2 h_n$$

- Defining the combined noise on the pseudorange $\widehat{d_n}$ as

  $$q_n = w_n + \epsilon$$

  then its distribution is

  $$q_n \sim \mathcal{N}\left(0, \sigma^2\left(1 - 2\,h_n + \mathbf{h}^T\mathbf{h}\right)\right)$$

- The covariance of the pseudorange errors are

  $$E\left\{q_n\,q_p\right\} = \sigma^2\left(\delta[n-p] - h_n - h_p + \mathbf{h}^T\mathbf{h}\right)$$

  in which $\delta[\cdot]$ is the Kronecker delta.

The utility of the above facts is that we can reconsider the statistics of the proposed hypothesis tests. Recall the known orientation case; the test statistic is

$$T\left(\left\{\widehat{d_{k,n}}\right\}\right) = \sum_{k=1}^{m}\sum_{n=1}^{N}\widehat{d_{k,n}}\delta_{k,n}$$

In terms of the measurement equation, this statistic is

$$\begin{aligned} T\left(\left\{\widehat{d_{k,n}}\right\}\right) &= \sum_{k=1}^{m}\sum_{n=1}^{N} d_{k,n}\delta_{k,n} \\ &\quad + \sum_{k=1}^{m}\sum_{n=1}^{N}\left(\epsilon_k + w_{k,n}\right)\delta_{k,n} \end{aligned}$$

The first part of this expression is the mean of the test statistic which is identical to the original analysis in [9]. The second part shows the effect of noise on the test statistic.

The mean of this noise term is still zero although, in contrast to the original analysis, the occurrence of the ϵ_k terms changes the variance.

Paralleling the analysis in [9] for known orientation,

$$\sigma^2_{T'} = \mathrm{Var}\left(\sum_{k=1}^{m}\sum_{n=1}^{N}\left(\epsilon_k + w_{k,n}\right)\delta_{k,n}\right)$$

Using the fact that the variance of a sum is the sum of all of the variances and covariances we have

$$\begin{aligned} \sigma^2_{T'} &= \sigma^2\mathbf{h}^T\mathbf{h}\sum_{k=1}^{m}\sum_{n=1}^{N}\sum_{p=1}^{N}\delta_{k,n}\delta_{k,p} \\ &\quad -2\sigma^2\sum_{k=1}^{m}\sum_{n=1}^{N}\delta_{k,n}\left(\sum_{p=1}^{N}\delta_{k,p}h_p\right) \\ &\quad +\sigma^2\sum_{k=1}^{m}\sum_{n=1}^{N}\delta^2_{k,n} \end{aligned}$$

It appears that

$$\sum_{p=1}^{N}\delta_{k,p}h_p = 0$$

so

$$\sigma^2_{T'} = \sigma^2\mathbf{h}^T\mathbf{h}\sum_{k=1}^{m}\left(\sum_{n=1}^{N}\delta_{k,n}\right)^2 + \sigma^2\sum_{k=1}^{m}\sum_{n=1}^{N}\delta^2_{k,n}$$

REFERENCES

[1] T. Humphreys, B. Ledvina, M. Psiaki, B. OHanlon, and P. Kinter, “Assessing the spoofing threat: development of a portable GPS civilian spoofer,” *Proc. ION GNSS 2008*, Savannah, GA, Sept. 2008.

[2] J. S. Warner and R. G. Johnston, “GPS spoofing countermeasures,” *Homeland Security Jour.*, Dec. 2003.

[3] M. L. Psiaki, B. W. OHanlon, J. A. Bhatti,. D. P. Shepard, and T. E. Humphreys, “Civilian GPS spoofing detection based on dual-receiver correlation of military signals,” *Proc. ION GNSS*, Portland, OR, Sept. 2011.

[4] K. D. Wesson, D. P Shepard, J. A. Bhatti, and T. E. Humphreys, “An evaluation of the vestigial signal defense for civil GPS anti-spoofing,” *Proc. ION GNSS*, Portland, OR, Sept. 2011.

[5] B. M. Ledvina, W. J. Bencze, B. Galusha, and I. Miller, “An in-line anti-spoofing device for legacy civil GPS receivers,” *Proc. ION ITM*, San Diego, CA, Jan. 2010.

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

[7] S. Daneshmand, A. Jafarnia-Jahromi, A. Broumandon, and G. Lachapelle, “A low-complexity GPS anti-spoofing method using a multi-antenna array,” *Proc. ION GNSS 2012*, Nashville, TN, Sept. 2012.

[8] P. F. Swaszek and R. J. Hartnett, “A multiple COTS receiver GNSS spoof detector - extensions,” *Proc. ION ITM*, San Diego, CA, Jan. 2014.

[9] D.S Radin, **GPS Spoofing Detection Using Multiple Antennas and Individual Space Vehicle Pseudoranges**, M.S. thesis, Dept. ECBE, URI, Kingston, RI, 2015, unpublished.

[10] N. O. Tippenhauer, C. P̈opper, K.B. Rasmussen, and S. Čapkun, “On the requirements for successful GPS spoofing attacks,” *Proc. ACM CCS 2011*, Chicago, IL, Oct. 2011.

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