2016

GNSS Spoof Detection Using Passive Ranging

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

Richard J. Hartnett

See next page for additional authors

Citation/Publisher Attribution
Swaszek, P., Hartnett, R. J., & Seals, K. C. (2016). GNSS Spoof Detection Using Passive Ranging. Paper presented at the *ION GNSS + Conference*, Portland, OR.
Available at: https://www.ion.org/gnss/abstracts.cfm?paperID=4024

GNSS Spoof Detection Using Passive Ranging

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

Advances in electronics technology have enabled the creation of malicious RF interference of GNSS signals. For example jamming completely denies the GNSS user of position, navigation, and time (PNT) information. While a serious concern when we expect PNT at all times, current generation GNSS receivers often warn the user when PNT is unavailable. A second threat to GNSS integrity is spoofing, the creation of counterfeit GNSS signals with the potential to confuse the receiver into providing incorrect PNT information. This type of attack is considered more dangerous than a jamming attack since erroneous PNT is often worse than no solution at all.

A variety of approaches have been proposed in the literature to recognize spoofing and can vary widely based upon the assumed capabilities and a priori knowledge of the spoofer. One method is to compare the GNSS result to data from a non-GNSS sensor. At the January 2016 ION ITM these authors developed and analyzed a spoof detection algorithm based upon measurements from an active ranging system (distances, but no heading). This paper expands the class of signals viable for this spoofing detection approach to passive ranging; equivalently, to range measurements which depend upon knowledge of precise time (effectively pseudoranges).

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, many GNSS users typically believe that the PNT information provided by their GNSS receiver is perfectly accurate. More sophisticated users look beyond accuracy and are also concerned with the integrity of the PNT 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 information 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 [1]. 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.

This paper discusses a technique to detect the occurrence of spoofing. Previously developed methods can be divided into two categories: those that self check the GNSS signals themselves and those that compare the PNT information to data from other trusted sources:

- GNSS RF only – This could be advanced signal processing of the combined GNSS and spoofed RF signals (e.g. looking for inconsistent or additional correlator peaks, comparing carrier phases, beamforming, etc., see, for example, [2–6]) or multi-receiver methods that exploit the fact that the spoofing signal from a point source spoofer distorts the multiple receivers' PNT in an identical fashion (e.g. [7]).

- Other data – typically this is the comparison of the PNT output of the GNSS receiver to secure (i.e. non-spoofed) external measurements such as IMU data [8, 9], radar returns [10], or range measurements [11].

In [11] these authors developed and analyzed a spoof detection algorithm based upon range measurements. For example, distance measuring equipment (DME) is a well established system that provides slant ranges to aircraft from fixed ground sites. In [11] we assumed that the data used to test for GNSS spoofing was a set of noisy range measurements from the GNSS equipped vehicle to one or more known locations. We constructed the hypothesis test (spoof versus no spoof) using a composite statistical model, combining the random errors in the GNSS and range measurements. The additional unknowns of this formation were estimated from the GNSS and range data as part of a generalized likelihood approach. We fully characterized the hypothesis test, provided expressions for the probabilities of false alarm and detection for the case of one range, and examined several interesting examples via simulation. It was seen that two or more moderate quality range measurements were quite effective at detecting spoofing (with only one range available, some spoofing events are undetectable).

That paper assumed unbiased range measurements. This current paper expands the class of signals viable for this spoofing detection approach to passive ranging; equivalently, to range measurements which depend upon knowledge of precise time (pseudoranges). In this class we consider any RF signal that emanates from a known location (we will call them "beacons") and that can be time referenced back to UTC (so-called signals of opportunity [12]). Examples of government signals could include AIS (automatic identification system) broadcasts from a base station and eLoran (where available). Other signals of opportunity could be considered if an alternative data link to time reference the signal back to UTC were available.

The development in this paper envisions that m such passive range signals are available, potentially of different types with different levels of accuracy. To convert the measurements to actual ranges we assume that the spoof detection algorithm knows of and removes any time offsets between UTC and transmission times at the beacons. Further, to remove the residual time offset from UTC at the local receiver, we assume that the algorithm has access to the estimate of UTC from the GNSS receiver, removing this bias from the pseudorange as well. Clearly this use of the GNSS receiver's time output has an impact on performance:

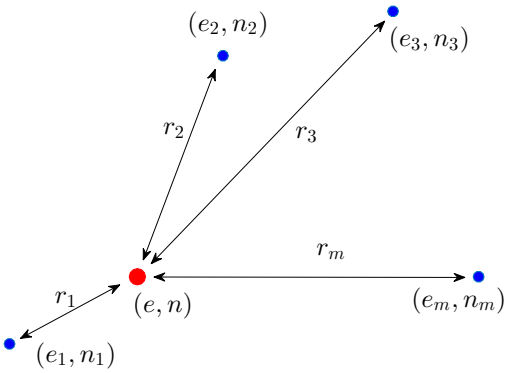

Figure 1: The configuration of a mobile and m ranging sources.

- Under no spoofing the error in this GNSS time estimate, then, adds to the inaccuracy of the resulting ranges and limits the resulting false alarm probability.

- When spoofing is present the GNSS time might not only be noisier, but might also be wrong!

The paper is organized as follows: (1) the results from [11] are summarized; (2) computation of the false alarm and detection probabilities for the general case of $m > 1$ ranges is developed (this was missing from [11]; (3) the extension to passive ranging is developed – performance with a single beacon, the meaconing case, and the general case are all considered. The paper concludes with some final thoughts. The Appendix includes details of material relevant to the review of the work in [11], but not included in that prior paper.

REVIEW OF [11] – ACTIVE RANGING

Consider a two dimensional positioning problem as depicted in Figure 1. The red dot represents a mobile vehicle whose location is of interest; the variables e and n represent its true east and north coordinates, respectively, in some local coordinate frame. We assume that a GNSS measurement of the position is available with a simple circular Gaussian error model

$$(\widehat{e}, \widehat{n}) \sim \mathcal{N}\left(\mu_e, \mu_n, \sigma_g^2, \sigma_g^2, 0\right)$$

In our notation hats are used to represent measurements, μ_e and μ_n represent the GNSS means (equal to the true location under no spoofing; otherwise equal to whatever the spoofer is trying to create), and σ_g is the GNSS error standard deviation.

In the figure the blue dots represent ranging sources, or beacons, at known locations (e_k, n_k), $k = 1, 2, \ldots m$. The true ranges are

$$r_k \equiv \sqrt{(e - e_k)^2 + (n - n_k)^2}$$

For these beacons define the matrix of direction cosines

$$\mathbf{d} = \begin{bmatrix} \sin\theta_1 & \cos\theta_1 \\ \vdots & \vdots \\ \sin\theta_m & \cos\theta_m \end{bmatrix}$$

whose rows consist of the unit vectors pointing from the GNSS position to those m ranging sources. The range measurements are assumed to be unbiased, have Gaussian errors with variances σ_k, and be independent of the GNSS measurement and each other

$$\widehat{r_k} \sim \mathcal{N}(r_k, \sigma_k)$$

For convenience, define the covariance matrix for the vector of range measurements, $\mathbf{r}$, as

$$\mathbf{\Gamma} = \begin{bmatrix} \sigma_1^2 & 0 & \cdots & 0 \\ 0 & \sigma_2^2 & \cdots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \cdots & \sigma_m^2 \end{bmatrix}$$

diagonal due to the assumption of mutual independence.

It is convenient to define the GNSS-induced ranges as

$$\widetilde{r_k} \equiv \sqrt{(\widehat{e} - e_k)^2 + (\widehat{n} - n_k)^2}$$

or $\widetilde{\mathbf{r}}$ for the length m vector of these computations. Finally, let $\delta_{\mathbf{r}}$ represent the vector of differences between the measured ranges and the GNSS-induced ranges

$$\delta_{\mathbf{r}} = \widehat{\mathbf{r}} - \widetilde{\mathbf{r}}$$

Assuming a Neyman-Pearson criterion, [11] showed that the generalized likelihood ratio test (GLRT) to detect spoofing is of the form

$$|\mathbf{A}\,\delta_{\mathbf{r}}| \underset{\mathrm{H_0}}{\overset{\mathrm{H_1}}{\gtrless}} \lambda \tag{1}$$

in which the 2-by-m matrix $\mathbf{A}$ is

$$\mathbf{A} = \left(\frac{1}{\sigma_g^2}\mathbf{I}_2 + \mathbf{d}^T\mathbf{\Gamma}^{-1}\mathbf{d}\right)^{-1}\mathbf{d}^T\mathbf{\Gamma}^{-1} \tag{2}$$

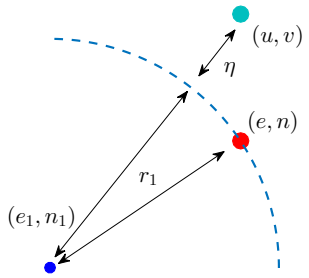

Figure 2: The situation for one range.

and λ is the test threshold (Appendix A of this paper provides some additional development of this result missing from [11]). Effectively, the test is looking for similarity in two vectors of ranges, one due to the range sensor and the other based on the GNSS receiver's output; the premultiplication by $\mathbf{A}$ scales these differences dependent upon the accuracies of the sensors and the directions to the beacons.

Several simulation examples appeared in [11] for $m = 2$ beacons showing the effectiveness of this spoof detection approach. The case of one range was analyzed in [11] in detail. It was argued that while $\widetilde{r_1}$ strictly follows a Rician distribution, it could be well approximated by a Gaussian distribution. Specifically, under $\mathrm{H_0}$

$$\widetilde{r_1} \sim \mathcal{N}(r_1, \sigma_g)$$

while under $\mathrm{H_1}$

$$\widehat{r_1} \sim \mathcal{N}(r_1 + \eta, \sigma_k)$$

in which η equals the amount by which the spoofer has distorted the true position in the direction toward the ranging source (see Figure 2). With this approximation expressions for the probabilities of false alarm and detection of this test are

$$\mathrm{P_{fa}} \approx 2Q\left(\frac{\lambda}{\sqrt{\sigma_g^2 + \sigma_1^2}}\right) \tag{3}$$

in which $Q(x)$ is the standard Gaussian tail probability and

$$\mathrm{P_d} \approx Q\left(\frac{\lambda + \eta}{\sqrt{\sigma_g^2 + \sigma_1^2}}\right) + Q\left(\frac{\lambda - \eta}{\sqrt{\sigma_g^2 + \sigma_1^2}}\right) \tag{4}$$

Finally, it was noted in [11] that if the spoofed position results in $\eta = 0$ (i.e. along the circle of constant radius from the beacon, the dotted curve in Figure 2) a single range measurement cannot detect spoofing. Additional range measurements make all spoofing events detectable.

COMPUTING PERFORMANCE, $m > 1$

The test statistic in Eq. (1) is based on

$$\delta_{\mathbf{r}} = \widehat{\mathbf{r}} - \widetilde{\mathbf{r}}$$

the vector difference between the measured range and the range due to the GNSS position. Let's first characterize this vector statistically:

- By assumption the measured ranges include independent Gaussian noise variates

  $$\widehat{r_k} = r_k + \epsilon_k$$

  with

  $$\epsilon_k \sim \mathcal{N}\left(0, \sigma_k^2\right)$$

- Writing the GNSS measurements as $\widehat{e} = \mu_e + \epsilon_e$ and $\widehat{n} = \mu_n + \epsilon_n$, the means plus errors, the elements of the GNSS derived range vector are

  $$\begin{aligned}\widetilde{r_k} &= \sqrt{(\widehat{e} - e_k)^2 + (\widehat{n} - n_k)^2} \\ &= \sqrt{(\mu_e + \epsilon_e - e_k)^2 + (\mu_n + \epsilon_n - n_1)^2} \\ &\equiv f_k(\epsilon_e, \epsilon_n)\end{aligned}$$

  functions of the position errors. These errors are Gaussian variates

  $$(\epsilon_e, \epsilon_n) \sim \mathcal{N}\left(0, 0, \sigma_g^2, \sigma_g^2, 0\right)$$

- Assuming that ϵ_e and ϵ_n are small with respect to the actual ranges (so that $\mathbf{d}$ is approximately constant), expand the definition of $\widetilde{r_k}$ in a Taylor series on these two variables and keep only the linear terms

  $$\begin{aligned}\widetilde{r_k} &= f_k\left(\epsilon_e, \epsilon_n\right) \\ &= f_k(0,0) + \epsilon_e \frac{\partial f_k\left(\epsilon_e, \epsilon_n\right)}{\partial \epsilon_e}\bigg|_{0,0} \\ &\qquad + \epsilon_n \frac{\partial f_k\left(\epsilon_e, \epsilon_n\right)}{\partial \epsilon_n}\bigg|_{0,0} + \ldots \\ &\approx f_k(0,0) + \epsilon_e \frac{e - e_k}{r_k} + \epsilon_n \frac{n - n_k}{r_k} \\ &\approx f_k(0,0) + \sin\theta_k \epsilon_e + \cos\theta_k \epsilon_n\end{aligned}$$

  so the difference is

  $$\begin{aligned}\widehat{r_k} - \widetilde{r_k} &\approx r_k + \epsilon_k - f_k(0,0) - \sin\theta_k \epsilon_e - \cos\theta_k \epsilon_n \\ &\approx \underbrace{r_k - f_k(0,0)}_{bias} + \underbrace{\epsilon_k - \sin\theta_k \epsilon_e - \cos\theta_k \epsilon_n}_{noise}\end{aligned}$$

  The result is that each element of the differential range vector is a Gaussian random variable; the bias represents the mean of each:

  - Under H_0 $f_k(0,0) = r_k$ and the bias is zero for all k.
  - Under H_1 this bias is the amount that the spoofer has *moved* the GNSS position in the direction toward the k^{th} ranging source; paralleling the development above define these shifts as the η_k (or vector $\boldsymbol{\eta}$).

  Being linear functions of Gaussian variates, the vector versions of the measured ranges and the GNSS ranges are jointly Gaussian. Their difference is also Gaussian so can be characterized by its mean vector

  $$E\left\{\delta_{\mathbf{r}}\right\} = \begin{cases} \mathbf{0} & ; \quad \mathrm{H}_0 \\ \boldsymbol{\eta} & ; \quad \mathrm{H}_1 \end{cases}$$

  and covariance matrix

  $$\mathrm{Cov}(\delta_{\mathbf{r}}) = \boldsymbol{\Gamma} + \sigma_g^2 \mathbf{d}\mathbf{d}^T$$

  More generally, allowing for correlated errors in the GNSS measurements, this is

  $$\mathrm{Cov}(\delta_{\mathbf{r}}) = \boldsymbol{\Gamma} + \mathbf{d}\boldsymbol{\Sigma}_{gnss}\mathbf{d}^T$$

Next, let's consider the linear transformation of this difference vector

$$\mathbf{y} = \mathbf{A}\delta_{\mathbf{r}}$$

with $\mathbf{A}$ defined in Eq. (2). Noting that $\mathbf{A}$ is 2-by-m and that $\delta\mathbf{r}$ is m-by-1, then this product is 2-by-1; i.e. $\mathbf{y}$ is bivariate Gaussian. Since this is a linear transformation the mean of $\mathbf{y}$ is

$$E\left\{\mathbf{y}\right\} = \begin{cases} \mathbf{0} & ; \quad \mathrm{H}_0 \\ \mathbf{A}\boldsymbol{\eta} & ; \quad \mathrm{H}_1 \end{cases}$$

and its covariance matrix is

$$\begin{aligned}\mathrm{Cov}(\mathbf{y}) &= \mathbf{A}\ \mathrm{Cov}(\delta\mathbf{r})\mathbf{A}^T \\ &= \mathbf{A}\left(\Gamma + \mathbf{d}\Sigma_{gnss}\mathbf{d}^T\right)\mathbf{A}^T \equiv \boldsymbol{\Sigma}_{\mathbf{y}}\end{aligned}$$

(Note that the development of the test in Eq. (1) did *not* use knowledge of the covariance of the GNSS measurements. This development of the performance does; hence, we have a somewhat sub-optimum test but accept this suboptimality as we expect that the GNSS covariance is changing more quickly than does $\mathbf{d}$.) We note that under H_0 this is a bivariate Gaussian random variable with zero mean and covariance $\boldsymbol{\Sigma}_{\mathbf{y}}$; under H_1 the mean changes.

The test in Eq. (1) compares the magnitude of $\mathbf{y}$ against a threshold; squaring both sides the equivalent test is

$$|\mathbf{y}|^2 = \mathbf{y}^T\mathbf{y} \underset{\mathrm{H}_0}{\overset{\mathrm{H}_1}{\gtrless}} \lambda^2$$

a test of a quadratic form in $\delta_{\mathbf{r}}$

$$\mathbf{y}^T\mathbf{y} = \left(\mathbf{A}\,\delta_{\mathbf{r}}\right)^T\left(\mathbf{A}\,\delta_{\mathbf{r}}\right) = \delta_{\mathbf{r}}^T\,\mathbf{A}^T\mathbf{A}\,\delta_{\mathbf{r}}$$

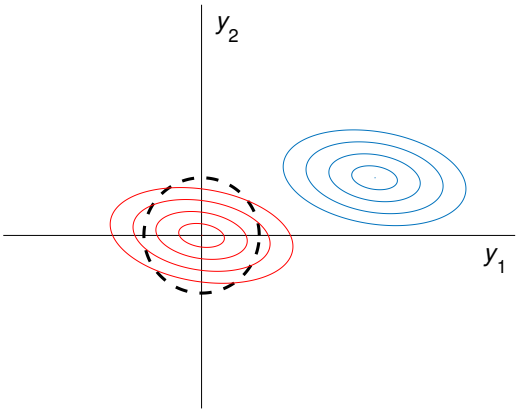

Figure 3: Typical density functions for $\mathbf{y}$.

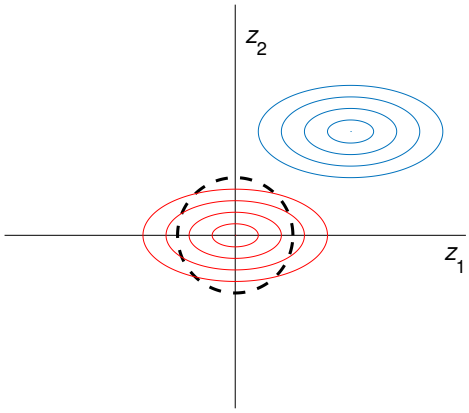

Figure 4: Typical density functions for $\mathbf{z}$.

Figure 3 portrays the situation, showing contours of constant probability for $\mathbf{y}$ (variables y_1 and y_2) under both H_0 (red) and H_1 (blue); the black dotted circle has radius λ. The false alarm probability is the volume of the red pdf outside of the circle; the detection probability is the volume under the blue pdf.

To facilitate doing these computations, it is convenient to rotate the data so that the major axis of the ellipses are parallel to the horizontal axis. Specifically, defining the rotated coordinates

$$\mathbf{z} = \mathbf{\Phi y} \qquad \text{with} \qquad \mathbf{\Phi} = \begin{bmatrix} \cos\zeta & -\sin\zeta \\ \sin\zeta & \cos\zeta \end{bmatrix}$$

and

$$\zeta = -\frac{1}{2}\tan^{-1}\frac{2\rho\sigma_1\sigma_1}{\sigma_1^2 - \sigma_2^2}$$

in which σ_1, σ_2, and ρ are the standard deviations and correlation coefficient of $\mathbf{y}$ (this is the negative of the angle of the major angle of the ellipse in the pdf of (y_1, y_2) [13]). The pdfs for $\mathbf{z}$ under the two hypotheses are still both Gaussian with parameters

$$E\{\mathbf{z}\} = \begin{cases} \mathbf{0} & ; \quad H_0 \\ \mathbf{\Phi A \eta} = \begin{bmatrix} \mu_a \\ \mu_b \end{bmatrix} & ; \quad H_1 \end{cases}$$

and

$$\mathbf{\Sigma_z} = \mathbf{\Phi \Sigma_y \Phi}^T = \begin{bmatrix} \sigma_a^2 & 0 \\ 0 & \sigma_b^2 \end{bmatrix}$$

With this change of variables the equivalent picture in terms of the random variables $\mathbf{z}$ is shown in Figure 4. (As intended, the ellipses are now aligned with the horizontal axis.)

With this representation the false alarm probability is

$$P_{\text{fa}} = 1 - \iint_{\Omega} \frac{1}{2\pi\sigma_a\sigma_b} e^{-\frac{1}{2}\left[\frac{z_1^2}{\sigma_a^2} + \frac{z_2^2}{\sigma_b^2}\right]} dz_1 dz_2$$

in which Ω is the disk about the origin of radius λ. This can be evaluated as

$$P_{\text{fa}} = 1 + \exp\left(-\frac{\sigma_1^2 + \sigma_2^2}{4\sigma_1^2\sigma_2^2}\lambda\right) I_0\left(\frac{\sigma_1^2 - \sigma_2^2}{4\sigma_1^2\sigma_2^2}\lambda\right) - 2Q\left(\frac{\sigma_1 - \sigma_2}{2\sigma_1\sigma_2}\sqrt{\lambda}, \frac{\sigma_1 + \sigma_2}{2\sigma_1\sigma_2}\sqrt{\lambda}\right) \tag{5}$$

using results in [14]. Similarly, the detection probability is

$$P_{\text{d}} = 1 - \iint_{\Omega} \frac{1}{2\pi\sigma_a\sigma_b} e^{-\frac{1}{2}\left[\frac{(z_1-\mu_a)^2}{\sigma_a^2} + \frac{(z_2-\mu_b)^2}{\sigma_b^2}\right]} dz_1 dz_2 \tag{6}$$

While considerably more complicated, several infinite series representations of this probability are available (see [14–16]).

PASSIVE RANGING

The results above assumed unbiased range measurements as might result from an active ranging system. As mentioned in the Introduction, our interest is in extending these concept to passive ranging; equivalently, pseudorange measurements.

Imagine a set of pseudoranges, $\widehat{\rho_k}$, one to each beacon. The model for each is

$$\widehat{\rho_k} = r_k + t_k + b + \epsilon_k$$

in which r_k is the true range, t_k is the offset of the time of transmission of the beacon signal with respect to UTC, b is the offset of the local receiver with respect to UTC, and ϵ_k is the noise on the estimate. We include t_k in that the beacon signal might not be directly synchronized to UTC (e.g. eLoran), but has

a deterministic time relationship; we assume that t_k is known. The GNSS receiver's clock offset, b, is included in that it provides a link back to UTC at the local vessel platform. Specifically, we assume that the receiver converts a specific pseudorange to a range by subtracting out both t_k and the GNSS receiver's estimate of b, $\widehat{b}$. Clearly this use of the GNSS receiver's time output has an impact on performance:

- Under no spoofing the error in this GNSS receiver's time offset, then, adds to the inaccuracy of the resulting ranges and must be taken into account when selecting the threshold for the desired false alarm probability. For simplicity we assume that this time estimate's error is Gaussian with zero mean and variance σ_b^2,

  $$\widehat{b} \sim \mathcal{N}\left(0, \sigma_b^2\right)$$

  and is independent of the receiver's East and North errors.

- When spoofing is present the GNSS time might also be wrong! Our model in this case is also Gaussian, but with non-zero mean g

  $$\widehat{b} \sim \mathcal{N}\left(g, \sigma_b^2\right)$$

Algebraically, the range measurements are

$$\begin{aligned}\widehat{r_k} &= \widehat{\rho_k} - t_k - \widehat{b} \\ &= r_k + t_k + b + \epsilon_k - t_k - \widehat{b} \\ &= r_k + \left(b - \widehat{b}\right) + \epsilon_k\end{aligned}$$

Including the statistical model for $\widehat{b}$, under H_0

$$\widehat{r_k} \sim \mathcal{N}\left(r_k, \sigma_k^2 + \sigma_b^2\right)$$

while under H_1

$$\widehat{r_k} \sim \mathcal{N}\left(r_k - g, \sigma_k^2 + \sigma_b^2\right)$$

Further, since all of the psuedoranges are corrected by this same clock estimate, the vector of ranges are correlated with covariance matrix

$$\mathbf{\Gamma} = \begin{bmatrix} \sigma_1^2 + \sigma_b^2 & \sigma_b^2 & \cdots & \sigma_b^2 \\ \sigma_b^2 & \sigma_2^2 + \sigma_b^2 & \cdots & \sigma_b^2 \\ \vdots & & \ddots & \vdots \\ \sigma_b^2 & \sigma_b^2 & \cdots & \sigma_m^2 + \sigma_b^2 \end{bmatrix} \tag{7}$$

Finally, since the pseudoranges have been converted to ranges, we conjecture that the optimum test is still of the form presented in Eq. (1) but with the new $\mathbf{\Gamma}$ taking into account the impact of $\widehat{b}$.

One Pseudorange

For a single pseudorange measurement the test again simplifies to the form

$$\mid \widehat{r_1} - \widetilde{r_1} \mid \underset{\mathrm{H}_0}{\overset{\mathrm{H}_1}{\gtrless}} \lambda$$

Under hypothesis H_0

$$\widehat{r_1} - \widetilde{r_1} \sim \mathcal{N}\left(0, \sigma_g^2 + \sigma_1^2 + \sigma_b^2\right)$$

while under H_1

$$\widehat{r_1} - \widetilde{r_1} \sim \mathcal{N}\left(\eta + g, \sigma_g^2 + \sigma_1^2 + \sigma_b^2\right)$$

in which η still describes the position offset toward the beacon and g represents the time offset (in units of distance) due to the spoofer.

With these characterizations the false alarm probability is

$$\mathrm{P}_{\mathrm{fa}} \approx 2Q\left(\frac{\lambda}{\sqrt{\sigma_g^2 + \sigma_1^2 + \sigma_b^2}}\right)$$

just a slight modification of Eq. (3). The detection probability is

$$\begin{aligned}\mathrm{P}_{\mathrm{d}} \approx\ & Q\left(\frac{\lambda + \eta + g}{\sqrt{\sigma_g^2 + \sigma_1^2 + \sigma_b^2}}\right) \\ & + Q\left(\frac{\lambda - \eta - g}{\sqrt{\sigma_g^2 + \sigma_1^2 + \sigma_b^2}}\right)\end{aligned}$$

a slight modification of Eq. (4). In general spoofing is detectable by one pseudorange unless the time distortion cancels the location change ($g + \eta = 0$); with more than one pseudorange this is, of course, impossible.

Meaconing

Meaconing, both innocent and malicious, is when a valid GNSS signal from one location is reradiated to nearby GNSS receivers (as has occurred at some airports with open hanger doors). In this case the "spoofed" GNSS position is the position of the source of the reradiated signal and the time offset, g, is equal to the additional propagation time from the reradiator to the receiver on the vessel of interest. Figure 5 describes the geometry.

First, we notice that the position offset is limited by the distance to the meaconer

$$-g \leq \eta \leq g$$

Further, when the meaconer is between the mobile and the beacon it is easiest to detect as $\eta + g = 2g$; similarly,

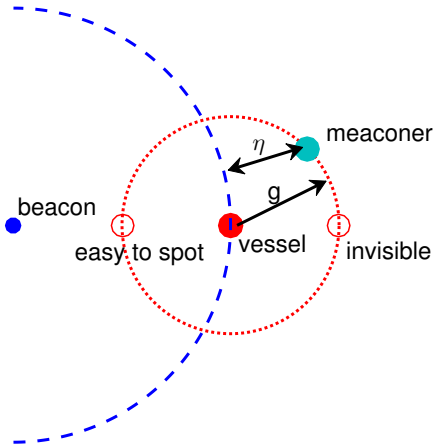

Figure 5: The geometry of meaconing.

when the meaconer is opposite to the direction to the beacon, it is undetectable ($\eta + g = 0$).

Two or More Pseudoranges

The test statistic for detecting spoofing using pseudoranges is of the same form as above in Eq. (1) except that the new definition of $\mathbf{\Gamma}$ in Eq. 7 includes the correlation due to the use of $\widehat{b}$; hence, the expressions for the probabilities of false alarm and detection in Eqs. (5) and (6), respectively, still hold after that modification.

CONCLUSIONS/FUTURE WORK

This paper shows how pseudorange measurements can be used to detect spoofing of GNSS position measurements:

- The Neyman-Pearson detection was characterized and analyzed; this included the case of one pseudorange, meaconing, and multiple pseudoranges.
- Note that signals of opportunity whose time of transmission offsets, the t_k, must be estimated can also be included in these results if the additional error of this estimate is combined with the measurement error.

Future work includes:

- Proving that correcting the pseudoranges is the *best* use of $\widehat{b}$ toward spoof detection.
- Modify the performance expressions to allow for correlation between the error in $\widehat{b}$ and the errors in $\widehat{e}$ and $\widehat{n}$.

APPENDIX A

This appendix develops the MLE solution for the more general m ranges case by casting the problem as one involving the position solution from a combination of range and pseudorange measurements. The development in [11] referenced this result to an unpublished paper; hence, is included here for completeness.

For convenience we work in three dimensions, recognizing that the reduction to two dimensions is easily accomplished.

Recall that GNSS pseudorange measurements include the actual range to the satellite plus the receiver clock bias

$$\rho_k = d_k + b + w_k$$

in which ρ_k is the pseudorange measurement for satellite k, b is the clock bias, and w_k represents the white Gaussian measurement noise (assumed to be independent over k with zero means and common variance σ_s^2). The unknowns in the standard 3-dimensional GNSS problem are the receiver's position and the clock's bias

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

and the observables are the n pseudoranges

$$\boldsymbol{\rho} = \begin{bmatrix} \rho_1 & \rho_2 & \cdots & \rho_n \end{bmatrix}^T$$

Starting at an assumed solution

$$\mathbf{x}_0 = \begin{bmatrix} x_0 & y_0 & z_0 & b_0 \end{bmatrix}^T$$

the nonlinear range equations can be linearized yielding a set of n linear equations in the pseudorange perturbation $\delta\boldsymbol{\rho}$ (equal to the ranges from the satellites to (x_0, y_0, z_0) plus the clock estimate minus the measured ranges) and the solution perturbation $\delta\mathbf{x}$ (the correction to the current position and the clock term)

$$\delta\mathbf{x} = \begin{bmatrix} \delta x & \delta y & \delta z & \delta b \end{bmatrix}^T$$

In vector form the equations are

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

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

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

with ψ_k the elevation and ϕ_k the azimuth of the k^{th} satellite from the assumed solution.

The weighted least squares solution (with typical weight matrix $\mathbf{W} = \frac{1}{\sigma_s^2}\mathbf{I}_n$) for the correction to the assumed solution is

$$\delta\mathbf{x}_0 = \left(\mathbf{H}^T\mathbf{W}\mathbf{H}\right)^{-1}\mathbf{H}^T\mathbf{W}\,\delta\boldsymbol{\rho}_0$$

so the actual solution is

$$\mathbf{x}_1 = \mathbf{x}_0 + \delta\mathbf{x}_0$$

New pseudorange residuals, say $\delta\boldsymbol{\rho}_1$, can be computed at this new solution and $\mathbf{H}$ can be recomputed in terms of the new elevations and azimuths for solution $\mathbf{x}_1$. If $\mathbf{H}$ has changed then a new correction can be found; if not the iteration stops and the residuals satisfy

$$\left(\mathbf{H}^T\mathbf{W}\mathbf{H}\right)^{-1}\mathbf{H}^T\mathbf{W}\,\delta\boldsymbol{\rho} = \mathbf{0}_4$$

where $\mathbf{0}_m$ is a column vector of m zeros.

Returning to the problem of spoof detection with range measurements, a set of range measurements to m fixed locations can be treated as additional pseudoranges, but with zero clock bias. To include this in the position solution the observation vector is augmented with the additional measurements

$$\boldsymbol{\rho}_+ = \left[\begin{array}{ccccccc} \rho_1 & \cdots & \rho_n & \widehat{r_1} & \cdots & \widehat{r_m} \end{array}\right]^T = \left[\begin{array}{cc} \boldsymbol{\rho}^T & \widehat{\mathbf{r}}^T \end{array}\right]^T$$

in which $\widehat{\mathbf{r}}$ is a column vector of the measured ranges. The direction matrix also gets additional rows; in partitioned form, this is

$$\mathbf{H}_+ = \left[\begin{array}{cc} \mathbf{D} & \mathbf{1}_n \\ \mathbf{d} & \mathbf{0}_m \end{array}\right]$$

in which $\mathbf{D}$ is the first three columns of $\mathbf{H}$,

$$\mathbf{d} = \left[\begin{array}{ccc} \cos\psi_{r,1}\sin\phi_{r,1} & \cos\psi_{r,1}\cos\phi_{r,1} & \sin\psi_{r,1} \\ \vdots & \vdots & \vdots \\ \cos\psi_{r,m}\sin\phi_{r,m} & \cos\psi_{r,m}\cos\phi_{r,m} & \sin\psi_{r,m} \end{array}\right]$$

$\psi_{r,j}$ and $\phi_{r,j}$ corresponding to the additional ranging sources (the m-by-3 matrix consisting of the unit vectors pointing to the ranging sources), and $\mathbf{1}_n$ is a column vector of n ones. Similarly, write the differential observations in partitioned form

$$\delta\boldsymbol{\rho}_+ = \left[\begin{array}{c} \delta\boldsymbol{\rho} \\ \delta\mathbf{r} \end{array}\right]$$

Consider the situation under H_0 in which the measured ranges $\widehat{r_j}$ are nearly correct for the GNSS location $(\widehat{e}, \widehat{n}\,)$. The actual GNSS pseudoranges have yielded a solution $\mathbf{x}_0$ so $\mathbf{H}$ is essentially correct. With the additional range measurements the perturbation in the solution that results in the MLE (the MLE matching the solution to this Gaussian problem) is

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

where $\mathbf{W}_+$ takes into account the unequal weighting due to the range measurements

$$\mathbf{W}_+ = \left[\begin{array}{cc} \frac{1}{\sigma_s^2}\mathbf{I}_n & \mathbf{0}_{n,m} \\ \mathbf{0}_{m,n} & \boldsymbol{\Gamma}^{-1} \end{array}\right]$$

In this expression the notation $\mathbf{0}_{j,k}$ corresponds to a j-by-k matrix of zeros and the bottom right submatrix, $\boldsymbol{\Gamma}^{-1}$, is a diagonal matrix with entries equal to the reciprocals of the range measurement variances

$$\boldsymbol{\Gamma}^{-1} = \mathrm{diag}\left(\frac{1}{\sigma_1^2}, \ldots, \frac{1}{\sigma_m^2}\right)$$

Using the form of $\mathbf{H}_+$ and multiplying matrices

$$\delta\mathbf{x}_+ = \left[\begin{array}{cc} \frac{1}{\sigma_s^2}\mathbf{D}^T\mathbf{D} + \mathbf{d}^T\boldsymbol{\Gamma}^{-1}\mathbf{d} & \frac{1}{\sigma_s^2}\mathbf{D}^T\mathbf{1}_n \\ \frac{1}{\sigma_s^2}\mathbf{1}_n^T\mathbf{D} & \frac{1}{\sigma_s^2}n \end{array}\right]^{-1} \times \left[\begin{array}{cc} \frac{1}{\sigma_s^2}\mathbf{D}^T & \mathbf{d}^T\boldsymbol{\Gamma}^{-1} \\ \frac{1}{\sigma_s^2}\mathbf{1}_n^T & 0 \end{array}\right]\delta\boldsymbol{\rho}_+$$

To continue this development the inverse of the first matrix is needed. Consider the $(n+m)$-by-$(n+m)$ partitioned matrix

$$\mathbf{A} = \left[\begin{array}{cc} A_{11} & A_{12} \\ A_{21} & A_{22} \end{array}\right]$$

Assuming that the diagonal submatrices are themselves square (A_{11} being n-by-n, A_{22} being m-by-m) and that their inverses exist, then there is the identify

$$\mathbf{A}^{-1} = \left[\begin{array}{cc} B_{11} & B_{12} \\ B_{21} & B_{22} \end{array}\right]$$

with

$$B_{11} = \left(A_{11} - A_{12}A_{22}^{-1}A_{21}\right)^{-1}$$

$$B_{12} = -\left(A_{11} - A_{12}A_{22}^{-1}A_{21}\right)^{-1}A_{12}A_{22}^{-1}$$

$$B_{21} = -\left(A_{22} - A_{21}A_{11}^{-1}A_{12}\right)^{-1}A_{21}A_{11}^{-1}$$

and

$$B_{22} = \left(A_{22} - A_{21}A_{11}^{-1}A_{12}\right)^{-1}$$

Using this result, and mixing notation for a few lines

$$\delta\mathbf{x}_+ = \left[\begin{array}{cc} \frac{1}{\sigma_s^2}B_{11}\mathbf{D}^T + \frac{1}{\sigma_s^2}B_{12}\mathbf{1}_n^T & B_{11}\mathbf{d}^T\boldsymbol{\Gamma}^{-1} \\ \frac{1}{\sigma_s^2}B_{21}\mathbf{D}^T + \frac{1}{\sigma_s^2}B_{22}\mathbf{1}_n^T & B_{21}\mathbf{d}^T\boldsymbol{\Gamma}^{-1} \end{array}\right]\delta\boldsymbol{\rho}_+$$

or in terms of the differentials

$$\left[\begin{array}{c} \delta x \\ \delta y \\ \delta z \\ \delta b \end{array}\right] = \left[\begin{array}{cc} \frac{1}{\sigma_s^2}B_{11}\mathbf{D}^T + \frac{1}{\sigma_s^2}B_{12}\mathbf{1}_n^T & B_{11}\mathbf{d}^T\boldsymbol{\Gamma}^{-1} \\ \frac{1}{\sigma_s^2}B_{21}\mathbf{D}^T + \frac{1}{\sigma_s^2}B_{22}\mathbf{1}_n^T & B_{21}\mathbf{d}^T\boldsymbol{\Gamma}^{-1} \end{array}\right] \times \left[\begin{array}{c} \delta\boldsymbol{\rho} \\ \delta\mathbf{r} \end{array}\right]$$

Of this vector result the position differential is

$$\begin{bmatrix} \delta x \\ \delta y \\ \delta z \end{bmatrix} = \left(\frac{1}{\sigma_s^2} B_{11} \mathbf{D}^T + \frac{1}{\sigma_s^2} B_{12} \mathbf{1}_n^T \right) \delta \boldsymbol{\rho} + B_{11} \mathbf{d}^T \boldsymbol{\Gamma}^{-1} \, \delta \mathbf{r}$$

It can be shown that the first of these terms is zero. Substituting the sub matrices, this is

$$\begin{bmatrix} \delta x \\ \delta y \\ \delta z \end{bmatrix} = \left(\frac{1}{\sigma_s^2} \mathbf{D}^T \mathbf{D} + \mathbf{d}^T \boldsymbol{\Gamma}^{-1} \mathbf{d} - \frac{1}{n\sigma_s^2} \mathbf{D}^T \mathbf{1}_n \mathbf{1}_n^T \mathbf{D} \right)^{-1} \times \mathbf{d}^T \boldsymbol{\Gamma}^{-1} \, \delta \mathbf{r}$$

Furthermore part of this expression can be related to the underlying GNSS position performance

$$\frac{1}{\sigma_s^2} \mathbf{D}^T \mathbf{D} - \frac{1}{n\sigma_s^2} \mathbf{D}^T \mathbf{1}_n \mathbf{1}_n^T \mathbf{D} = \boldsymbol{\Sigma}_{xyz}^{-1}$$

in which $\boldsymbol{\Sigma}_{xyz}$ is the covariance in (x, y, z) of the GNSS solution (assumed to be $\sigma_g^2 \mathbf{I}_3$ for the work above). The result, then, becomes

$$\begin{bmatrix} \delta x \\ \delta y \\ \delta z \end{bmatrix} = \left(\boldsymbol{\Sigma}_{xyz}^{-1} + \mathbf{d}^T \boldsymbol{\Gamma}^{-1} \mathbf{d} \right)^{-1} \mathbf{d}^T \boldsymbol{\Gamma}^{-1} \, \delta \mathbf{r}$$

Interestingly, while this Appendix began with the goal of computing the MLE in the range domain (imagining that the pseudoranges were available), the result only needs the direction vectors to the ranging sources and the GNSS covariance matrix.

Finally, reducing this development to the two dimensional equivalent with variables e and n instead of x and y

$$\begin{bmatrix} \Delta_e \\ \Delta_n \end{bmatrix} = \left(\boldsymbol{\Sigma}_{en}^{-1} + \mathbf{d}^T \boldsymbol{\Gamma}^{-1} \mathbf{d} \right)^{-1} \mathbf{d}^T \boldsymbol{\Gamma}^{-1} \, \delta \mathbf{r}$$

For independent and identically distributed GNSS errors in e and n (covariance $\boldsymbol{\Sigma}_{en} = \sigma_g^2 \mathbf{I}_2$) this becomes

$$\begin{bmatrix} \Delta_e \\ \Delta_n \end{bmatrix} = \left(\frac{1}{\sigma_g^2} \mathbf{I}_2 + \mathbf{d}^T \boldsymbol{\Gamma}^{-1} \mathbf{d} \right)^{-1} \mathbf{d}^T \boldsymbol{\Gamma}^{-1} \, \delta \mathbf{r}$$

This final result leads directly to the test statistic in Eq. (1).

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] 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.

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

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

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

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

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

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

[13] N. L. Johnson and S. Kotz, *Distributions in Statistics: Continuous Multivariate Distributions*, New York: Wiley, 1972.

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

[15] 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.

[16] 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.