2016

GNSS Spoof Detection Using Independent Range Information

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

Richard J. Hartnett

Kelly C. Seals

Citation/Publisher Attribution

Swaszek, Peter F., Hartnett, Richard J., Seals, Kelly C., "GNSS Spoof Detection using Independent Range Information," *Proceedings of the 2016 International Technical Meeting of The Institute of Navigation*, Monterey, California, January 2016, pp. 739-747.
Available at: https://www.ion.org/publications/abstract.cfm?jp=p&articleID=13457

GNSS Spoof Detection Using Independent Range Information

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 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. He is spending the 2015-16 academic year on sabbatical at the U.S. Coast Guard Academy.

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

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

ABSTRACT

Global Navigation Satellite Systems (GNSS) are well known to be accurate providers of position 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. Inexpensive jamming devices overpower or distort the GNSS receiver's input so as to completely deny the GNSS user of PNT information. While a serious concern when we expect PNT information to be available at all times, current generation GNSS receivers warn the user when PNT is unavailable; some of the more sophisticated receiver designs can also battle jamming. A second threat to GNSS integrity is spoofing, the creation of counterfeit GNSS signals. This type of attack is considered more dangerous than a jamming attack since an erroneous PNT solution is often worse than no solution at all.

A variety of approaches have been proposed in the literature to recognize spoofing and can vary widely based upon the assumed capabilities and a priori knowledge of the spoofer. Some of these are based on characteristics of the RF signal alone (e.g. vestigial peaks in the correlator outputs) or employ multiple antennae (e.g. beamforming) or multiple receivers (looking for consistent data).

Another spoof detection method is to compare the GNSS measurement to data from a sensor of a different type that cannot be spoofed; for example, several prior efforts have considered IMU data. This paper considers the use of range measurements (range only, no bearing) to detect spoofing. Range might be measured using RF signals (e.g. DME for avionics) although other modalities could be effective (e.g. a calibrated barometric altimeter). Assuming that the data set consists of a GNSS measurement and ranges to one or more fixed sites, this paper develops the binary hypothesis test between spoofing and no spoofing. The unknown positions naturally lead to a generalized likelihood approach. We initially focus on the simplest case of one range measurement and a simple Gaussian model for the GNSS position measurement; this scenario allows for a simple closed form solution from which we can examine the characteristics of the test (it is similar to RAIM) and to observe the interaction between the relative accuracy of the sensors (GNSS and range) on the form of the hypothesis test and its resulting performance at detecting spoofing. We then generalize the results to multiple ranges and correlated statistics.

INTRODUCTION

GNSS are well known to be accurate providers of position information across the globe. Because of high signal availabilities, capable/robust receivers, and well-populated satellite constellations, operators typically believe that the location information provided by their GNSS receiver is correct. More sophisticated users are concerned with the integrity of the derived location information; for example, RAIM algorithms were developed to address possible satellite failure modes.

Attacks on GNSS availability and integrity are known as jamming and spoofing. Both are based on the creation of radio signals in the GNSS band. Jamming involves the transmission of signals that interfere with GNSS reception so that the receiver is unable to provide a position or time solution. Various methods to detect jamming, and possibly overcome it, have been considered in the literature. Spoofing is the transmission of counterfeit GNSS signals so as to mislead a GNSS receiver into reporting an inaccurate position or time. If undetected, spoofing might be much more dangerous than a jamming attack.

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. Many of these are based on the RF signal alone and are, in some sense, the cheapest to implement. Of interest here are methods which compare GNSS information to measurements available from other, non-GNSS sensors. Over 10 years ago Warner and Johnston [1] suggested such methods, calling them *sanity checks*; unfortunately, they did not further develop the idea. Recently there have been a few examinations of combining GNSS and non-GNSS data toward spoof detection:

- In 2014 these authors considered the use of IMU data to detect spoofing of a Coast Guard ship [2]. Specifically, the pitch and roll measurements from the ship's gyrocompass were used to predict the relative spatial trajectory of a GPS antenna mounted high up on the ship. This movement was then correlated to the GPS measurements (with the linear motion of the ship being removed) to detect spoofing. The concept was that the spoofer would not correctly generate the "wiggle" due to the sea state and, hence, could be identified.

- In 2015 Tanil, Khanafseh, and Pervan employed RAIM residuals from a tightly coupled aircraft GPS/INS to detect spoofing [3]. In this case, the system tracked the aircraft's motion due to winds. As above, if the spoofer does not generate this wiggle correctly then it could be detected.

- In 2015 Carson and Bevly discussed the use of range and bearing information with GPS positions to detect spoofing for a platoon of vehicles [4]. They assumed the availability of Relative Position Vectors between pairs of vehicles from a radar sensor. To detect spoofing of a single vehicle they compare these vectors to the corresponding GPS difference vector, declaring spoofing if the difference is too great. Their focus is on a pair of vehicles only.

This work considers the use of range only (no bearing) information to detect GNSS spoofing. This range information might be available from Distance Measuring Equipment (DME) for aircraft, might be derivable from image data, could be measured from an RF signal in a different frequency band (e.g. Loran), a barometric measurement of altitude, or a laser range. The contribution of this paper is the explicit development and analysis of a GNSS spoof detection algorithm that fuses GNSS positions with such range measurements. The significance of this paper is that it adds to the limited, but important, literature on spoof detection by comparison to non-GNSS position data.

The paper starts by constructing the hypothesis testing problem, introducing the solution of the Generalized Likelihood Test under the assumption of Gaussian GNSS and range errors. The problem is then explored in a hierarchical way. First, the simplest case of a single range measurement is examined, fully developing the test, providing an exact analysis of its performance, and comparing/contrasting the situation for different parameterizations of sensor quality and spoofer characteristics. The methodology is then extended to multiple ranges; examples are presented showing the power of having more than one range. Finally, we allow for uncertainty in the location of the ranging sites and for correlation in the GNSS error model.

THE SETUP

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

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

We assume that a GNSS measurement of the position is available, denote it as $(\widehat{e}, \widehat{n})$, as are the range measurements, $\widehat{r_k}$.

The goal here is to test for spoofing which is defined as

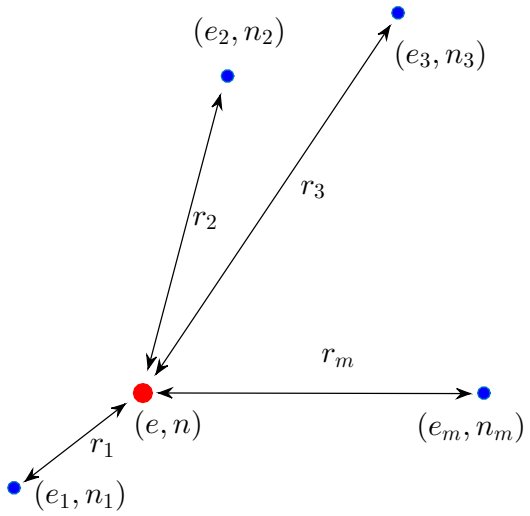

Figure 1: The general configuration of a mobile and m ranging sources.

the existence of radio signals that would result in an erroneous position solution at the GNSS receiver. It is assumed that spoofing does not impact the ranging measurements in any way. (More generally, the scenario is that the GNSS signals are themselves faulty and our interest is in employing the range measurements as an integrity check.) Define the null hypothesis, H_0, as the case in which no spoofer is present and the alternative hypothesis, H_1, for when a spoofer is present. Under both hypotheses the GNSS measurement is assumed to be Gaussian

$$(\widehat{e}, \widehat{n}) \sim \mathcal{N}\left(\mu_e, \mu_n, \sigma_g^2, \sigma_g^2, 0\right) \tag{1}$$

(this notation including the arguments of the two means, two variances, and the correlation coefficient; hence, independent east and north measurements with equal variances). Under H_0 the means are the true location, $\mu_e = e$ and $\mu_n = n$, while under H_1 the means are some other location, say $\mu_e = u$ and $\mu_n = v$. Meanwhile the range measurements are assumed to be unaffected by the spoofer. We assume a Gaussian model for each

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

providing for different levels of accuracy on the different range measurements. While this model is not perfect, that the range would never be negative, we assume that the actual ranges are much greater than the range accuracy and ignore the slight difference in the model. Further, all of the measurements are assumed to be statistically independent.

HYPOTHESIS TESTING

Hypothesis testing between a pair of hypotheses, H_0 and H_1, is usually implemented by computing a scalar function of the observed data, $T\,(\text{data})$, called the test statistic, and comparing this value to a constant called the threshold. If the test statistic exceeds the threshold, the test result is a decision for H_1; if not, H_0. Symbolically, this can be written as

$$T\,(\text{data}) \underset{\mathrm{H}_0}{\overset{\mathrm{H}_1}{\gtrless}} \lambda$$

in which λ represents the threshold (yet to be selected).

The goal here is to detect the occurrence of spoofing. Under the Neyman-Pearson approach the probability of false alarm (the probability of deciding for H_1 when H_0 is true) is limited (upper bounded) to some preselected value (often close to zero) and the test is constructed to maximize the probability of detection (the probability of correctly accepting H_1 when H_1 is true). For this criterion the optimum test statistic is well known to be the likelihood ratio [5]. Recognizing that the data consists of both the GNSS location measurement and the range measurements, this is the ratio of the conditional probability density functions (pdfs) of the measurements under the two hypotheses. Exploiting the assumed mutual independence of the measurements

$$T\,(\text{data}) = \frac{f\left(\widehat{e}, \widehat{n}\,|\mathrm{H}_1\right)}{f\left(\widehat{e}, \widehat{n}\,|\mathrm{H}_0\right)} \cdot \prod_{k=1}^{m} \frac{f\left(\widehat{r_k}\,|\mathrm{H}_1\right)}{f\left(\widehat{r_k}\,|\mathrm{H}_0\right)}$$

Since the spoofer is assumed to not impact the range measurement the product term in this expression is unity and the likelihood ratio reduces to the first term. While this cancellation of the range measurements seems anti-intuitive, that one expects to exploit those measurements as part of the test, they will reappear in the estimation of the parameters of this resulting likelihood ratio.

Substituting the pdf, taking the natural logarithm and dropping the additive constants, the test is

$$T = (\widehat{e} - e)^2 + (\widehat{n} - n)^2 - (\widehat{e} - u)^2 - (\widehat{n} - v)^2$$

Unfortunately, most of the variables in this expression are unknown: specifically, u and v under H_1 and e and n under H_0. A common approach, the generalized likelihood ratio test or GLRT, replaces each of these with its maximum likelihood estimate (MLE) [5].

To continue consider those MLEs, starting with the simpler case of H_1:

H_1: Under H_1 the likelihood function is

$$L_1 = \frac{1}{2\pi\sigma_g^2} e^{-\frac{1}{2\sigma_g^2}\left[(\widehat{e}-u)^2+(\widehat{n}-v)^2\right]} \times \prod_{k=1}^{m} \frac{1}{\sqrt{2\pi}\sigma_k} e^{-\frac{1}{2\sigma_k^2}(\widehat{r_k}-r_k)^2}$$

Note that only the first exponential term contains u and v, hence, the expression is trivially maximized at the MLEs

$$u = \widehat{e} \qquad \text{and} \qquad v = \widehat{n}$$

Substituting these MLEs for u and v into the optimum test, the GLRT reduces to

$$T = (e - \widehat{e}\,)^2 + (n - \widehat{n}\,)^2$$

the square of the distance between the MLE under H_0, (e, n), and the GNSS measurement, $(\widehat{e}, \widehat{n})$. This is a satisfying solution, if the location measurement is close to the location estimate including the range, then declare no spoofing; if it's far off, declare spoofing.

H_0: Under H_0 the likelihood function is

$$L_0 = \frac{1}{2\pi\sigma_g^2} e^{-\frac{1}{2\sigma_g^2}\left[(\widehat{e}-e)^2+(\widehat{n}-n)^2\right]} \times \prod_{k=1}^{m} \frac{1}{\sqrt{2\pi}\sigma_k} e^{-\frac{1}{2\sigma_k^2}(\widehat{r_k}-r_k)^2}$$

in which the r_k are implicitly functions of both e and n. At the MLE the derivatives with respect to e and n should equal zero. Focusing on e

$$\frac{\partial L_0}{\partial e} = L_0 \left[\frac{1}{\sigma_g^2}(\widehat{e} - e) + \sum_{k=1}^{m} \frac{1}{\sigma_k^2}(\widehat{r_k} - r_k)\frac{e - e_k}{r_k} \right]$$

For a zero derivative, the expression within the brackets must equal zero (the other term is a pdf, assumed to never equal zero); equivalently,

$$e = \widehat{e} + \sum_{k=1}^{m} \frac{\sigma_g^2}{\sigma_k^2}(\widehat{r_k} - r_k)\frac{e - e_k}{r_k} = \widehat{e} + \Delta_e \quad (2)$$

The n derivative yields another requirement at the MLE

$$n = \widehat{n} + \sum_{k=1}^{m} \frac{\sigma_g^2}{\sigma_k^2}(\widehat{r_k} - r_k)\frac{n - n_k}{r_k} = \widehat{n} + \Delta_n \quad (3)$$

While these expressions are quite sensible, that the MLE of the true position is the GNSS location plus an offset, (Δ_e, Δ_n) (and that the offset depends upon the relative accuracy of the GNSS and range measurements), this result is not yet useful in that the expressions for the corrections are themselves functions of the true positions and the true ranges. We return to these expressions below. Substituting the estimates for e and n into the optimum test, the GLRT reduces to

$$T = \Delta_e^2 + \Delta_n^2 \quad (4)$$

the square of the length of the MLE offset in the position domain.

To continue the development and analysis of the GLRT the required conditions for the MLE stated in Eq. (2) and (3) must be solved. The simple case of $m = 1$ is considered first, allowing for a complete analysis of the test performance; the extension to general m appears later in this manuscript.

ONE RANGE MEASUREMENT

To solve the coupled non-linear equations in Eqs. (2) and (3) when $m = 1$ we *assume* the form of the solution and then demonstrate that it fits the conditions. Further, as long as the actual range is much larger than the sensor accuracies, then the likelihood surface is unimodal and this extremum is the unique maximum. Specifically, the MLE occurs along the line connecting the location measurement to the known position

$$e = \widehat{e} + \beta\,(e_1 - \widehat{e}\,) \qquad n = \widehat{n} + \beta\,(n_1 - \widehat{n}\,)$$

for an appropriate chosen constant β. This relationship is shown in Figure 2. The green dot is the GNSS position, the blue dot is the location of the ranging site, and potential MLE locations are shown as red squares.

Define the GNSS developed range, the distance from the GNSS measured position to the fixed location as

$$\widetilde{r_1} = \sqrt{(\widehat{e} - e_1)^2 + (\widehat{n} - n_1)^2}$$

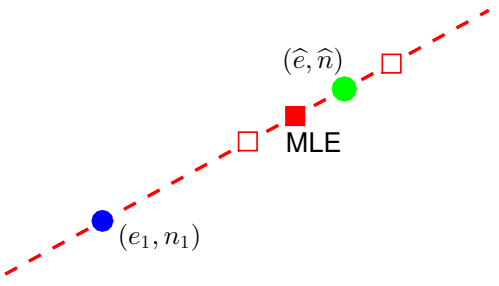

Figure 2: The location of the MLE for $m = 1$ ranging source.

(using a tilde) then the MLE's parameter is

$$\beta = \frac{\sigma_g^2}{\sigma_g^2 + \sigma_1^2} \left(\frac{\widetilde{r_1} - \widehat{r_1}}{\widetilde{r_1}} \right)$$

and the test statistic reduces to

$$T = \left(\frac{\sigma_g^2}{\sigma_g^2 + \sigma_1^2} \right)^2 \left(\widetilde{r_1} - \widehat{r_1} \right)^2$$

Ignoring the (positive) constant, the equivalent test statistic is

$$T = \left(\widetilde{r_1} - \widehat{r_1} \right)^2$$

This can be further simplified by taking a square root, but the test becomes two sided

$$T' = \mid \widetilde{r_1} - \widehat{r_1} \mid \underset{\mathrm{H_0}}{\overset{\mathrm{H_1}}{\gtrless}} \lambda \tag{5}$$

In words, the optimum test is a comparison of the measured range to the GNSS derived range; similar to RAIM. Unlike RAIM, which looks at the range residual of a single satellite to determine its validity, this test is considering the validity of all of the satellites simultaneously.

Performance Analysis

Recall that the GNSS derived range is

$$\widetilde{r_1} = \sqrt{\left(\widehat{e} - e_1 \right)^2 + \left(\widehat{n} - n_1 \right)^2}$$

With the measurements under $\mathrm{H_0}$ assumed to be Gaussian random variables each difference in this expression is also Gaussian and the square root of the sum of squares has a Rician distribution

$$f\left(\widetilde{r_1} \right) = \frac{\widetilde{r_1}}{\sigma_g^2} I_0 \left(\frac{r_1 \widetilde{r_1}}{\sigma_g^2} \right) e^{-\left(\widetilde{r_1}^2 + r_1^2 \right)/2\sigma_g^2}$$

for $\widetilde{r_1} > 0$, $I_0(x)$ is the modified Bessel function of zero order, and r_1 is the true range

Next, recall that $\widehat{r_1}$ is assumed to be Gaussian. Normally the pdf of the difference between $\widetilde{r_1}$ and $\widehat{r_1}$ would be found by convolving the density functions of $\widetilde{r_1}$ and $-\widehat{r_1}$. However, since r_1 is typically much larger than σ_g the Rician density function is well approximated as Gaussian

$$\widetilde{r_1} \sim \mathcal{N}\left(r_1, \sigma_g^2 \right)$$

so the difference is approximately Gaussian distributed under $\mathrm{H_0}$

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

This approximation provides an expression for the false alarm probability

$$\mathrm{P_{fa}} = \mathrm{Prob}\left(|\widetilde{r_1} - \widehat{r_1}| > \lambda \,|\mathrm{H_0}\, \right) \approx 2Q\left(\frac{\lambda}{\sqrt{\sigma_g^2 + \sigma_1^2}} \right)$$

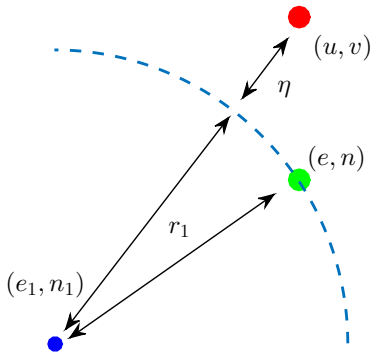

Figure 3: Definition of the spoofer offset η.

in which $Q(x)$ is the standard Gaussian tail probability. Equivalently, the threshold can be found as

$$\lambda = \sqrt{\sigma_g^2 + \sigma_1^2} \quad Q^{-1}\left(\frac{\mathrm{P_{fa}}}{2} \right)$$

The probability of detection depends upon the action of the spoofer. Figure 3 shows the relationship with the green and red dots representing the true and spoofed positions, respectively. Defining η as the extra distance from the ranging source beyond that attributable to the true location, then the distribution of the range difference under $\mathrm{H_1}$ is

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

so

$$\begin{aligned} \mathrm{P_d} &= \mathrm{Prob}\left(|\widetilde{r_1} - \widehat{r_1}| > \lambda \,|\mathrm{H_1}\, \right) \\ &\approx Q\left(\frac{\lambda + \eta}{\sqrt{\sigma_g^2 + \sigma_1^2}} \right) + Q\left(\frac{\lambda - \eta}{\sqrt{\sigma_g^2 + \sigma_1^2}} \right) \end{aligned}$$

Figures 4 and 5 show examples of the test's performance; both are receiver operating characteristic (ROC) curves plotting the probability of detection versus the probability of false alarm.

- The first of these (Figure 4) sets $\sigma_g = \sigma_1$ (equal quality sensors) and varies η, the along-range shift created by the spoofer in multiples of σ_g. Note that if $\eta = 0$, that the shift maintains the same range (i.e. the spoofed position (u, v) and the true position (e, n) are both on the same circle about the ranging source) then the spoofing is not detectable by a single range (and the performance is a coin toss, the straight line); of course, this could be mitigated by having a second ranging source non-colinear to the current one (this is demonstrated below). Further, significant shift by the

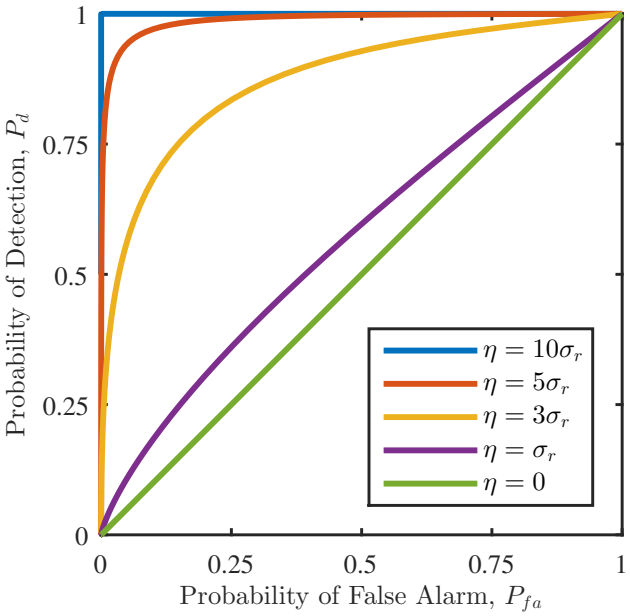

Figure 4: Sample performance for one range for various amounts of spoofer shift.

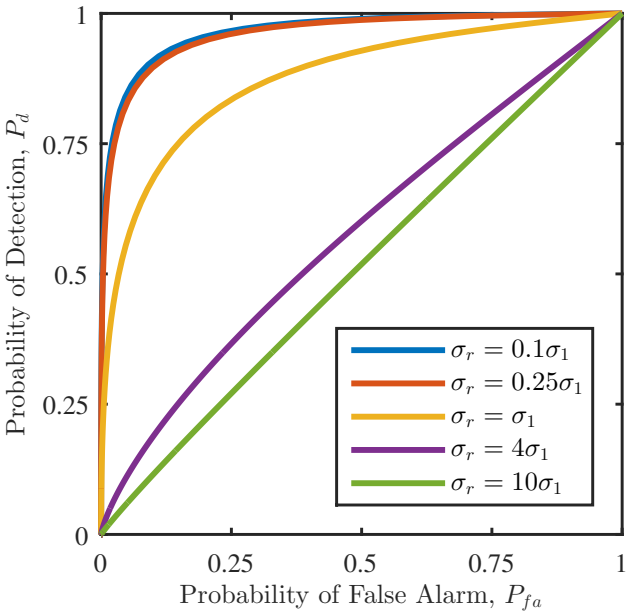

Figure 5: Sample performance for one range for different sensor quality ratios.

spoofer (on the order of 10 or more σ_g) is easily detected (the $\eta = 10\sigma_g$ is essentially a vertical line on the ROC).

- The second ROC (Figure 5) keeps $\eta = 3\sigma_g$ (the yellow curve in Figure 4) and considers various ratios for the sensor accuracies (up to where one sensor is ten times more accurate than the other). Note that the yellow curve in this figure matches the yellow curve in the prior figure (equal quality sensors) to provide a benchmark on performance. We observe that a range sensor that is more accurate than the GNSS sensor aids performance while a worse range sensor degrades performance. It appears that once the sensor ratio is 10 or larger, we have either maxed out detection performance or made the spoofing test irrelevant. This observation is useful in responding to questions on which sensor to purchase (it need not be more than 10 times better than GNSS) or even if a range measurement will help in detecting spoofing (a range accuracy of ± 50 meters is of no use).

TWO OR MORE RANGES

The successful development and analysis of the optimum test in the section above was predicated by there being only one range measurement; in general, the direct solution of the necessary conditions in (2) and (3) for more than one range is needed. Deferring to the development in [6] (and modified to the 2-D problem), define the m-by-2 matrix

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

whose rows consist of the unit vectors pointing from the GNSS position to the m ranging sources (θ_k corresponding to the azimuth from the GNSS position toward the k^{th} ranging source, North being 0° and the angles proceeding clockwise). Further, define the covariance matrix for the range measurements as

$$\mathbf{\Gamma} = \text{diag}\left(\sigma_1^2, \ldots, \sigma_m^2\right)$$

(diagonal since we assume independent measurement errors). Finally, define the column vector of differential range measurements as

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

in which $\widetilde{\mathbf{r}}$ is the vector of ranges from the GNSS position, $(\widehat{e}, \widehat{n})$, to the m ranging sources. With these definitions the MLE offset vector from the GNSS position under H_0 can be shown to be

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

in which $\mathbf{I}_2$ is a 2-by-2 identity matrix. Further, since the test statistic for our spoofing problem was shown in (4) to be the square of the length of this offset vector (or the length itself), the general form of the test is

$$\left| \left(\frac{1}{\sigma_g^2}\mathbf{I}_2 + \mathbf{d}^T\mathbf{\Gamma}^{-1}\mathbf{d}\right)^{-1} \mathbf{d}^T\mathbf{\Gamma}^{-1}\,\delta\mathbf{r} \right| \underset{\text{H}_0}{\overset{\text{H}_1}{\gtrless}} \lambda \qquad (6)$$

Note that if $m = 1$ then this result simplifies to that presented above.

An Example with Two Ranges

Consider two ranging sources, one to the East at GNSS range $\widetilde{r_1}$ from the GNSS location and one to the North East at GNSS range $\widetilde{r_2}$ so that

$$\mathbf{d} = \begin{bmatrix} 1 & 0 \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{bmatrix}$$

Set the range accuracies as

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

Evaluating the expressions above, the MLE offset has

$$\Delta_e = \frac{{\sigma_g}^2 \left({\sigma_g}^2 + 2\,{\sigma_2}^2 \right) (\widetilde{r_1} - \widehat{r_1}) + \sqrt{2}\,\sigma_g^2 {\sigma_1}^2 (\widetilde{r_2} - \widehat{r_2})}{{\sigma_g}^4 + 2\,{\sigma_g}^2\,{\sigma_1}^2 + 2\,{\sigma_g}^2\,{\sigma_2}^2 + 2\,{\sigma_{r,1}}^2\,{\sigma_2}^2}$$

and

$$\Delta_n = \frac{\sqrt{2}\,{\sigma_g}^2 \left(\sigma_g^2 + \sigma_1^2 \right) (\widetilde{r_2} - \widehat{r_2}) - {\sigma_g}^4 (\widetilde{r_1} - \widehat{r_1})}{{\sigma_g}^4 + 2\,{\sigma_g}^2\,{\sigma_1}^2 + 2\,{\sigma_g}^2\,{\sigma_2}^2 + 2\,{\sigma_1}^2\,{\sigma_2}^2}$$

Recall that with this offset, the test itself is defined in terms of Δ_e and Δ_n in (4).

As an example of this solution, Figure 6 shows the GNSS measurement (a black dot, placed at the origin on these axes for convenience) and the directions (the dashed lines) toward the ranging sources to the East (right, red) and North East (up and right, blue). The two solid lines (red and blue for the corresponding ranging sources) show the differential ranges (the differences between the measured ranges and the ranges developed from the GNSS solution); in this case both measured ranges are greater than the corresponding GNSS ranges, so both line segments are oriented away from the ranging sources. Assuming measurement standard deviations of 0.25 (GNSS), 0.1 (range 1), and 0.2 (range 2), the arcs are the contours of the likelihood function combining the measurements. The MLE found from the expressions above is shown as the green square; it clearly matches the extremum of the likelihood contours. Further, for this example the MLE clearly exploits the high accuracy of $\widehat{r_1}$ in that its horizontal component almost perfectly matches the date in $\widehat{r_1}$.

To demonstrate the performance with multiple ranging sources, consider the experimental configuration of Figure 7. The black diamond at the center represents the true location; the red and blue dashed lines again show the directions toward the two ranging sources. The 12 dots show possible locations that the spoofer is creating (i.e. they define η); the 2 green ones to the left and right should be easily caught by the sole ranging source to the East (the red direction), the 2 red

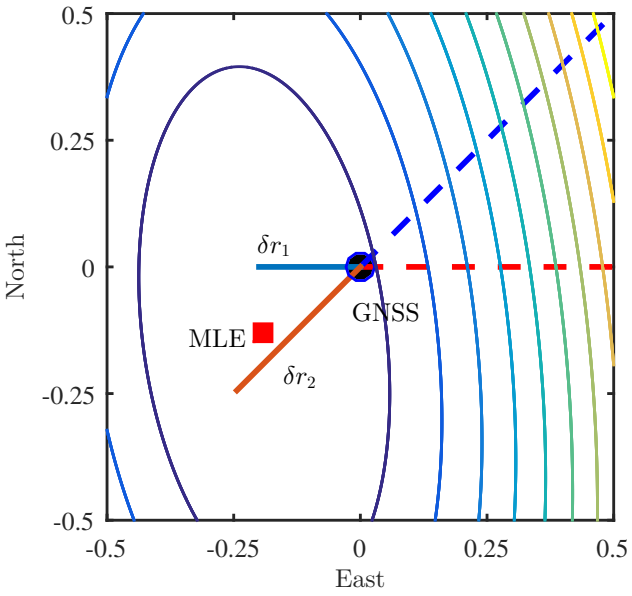

Figure 6: Graphical representation of locating the MLE for the two range example.

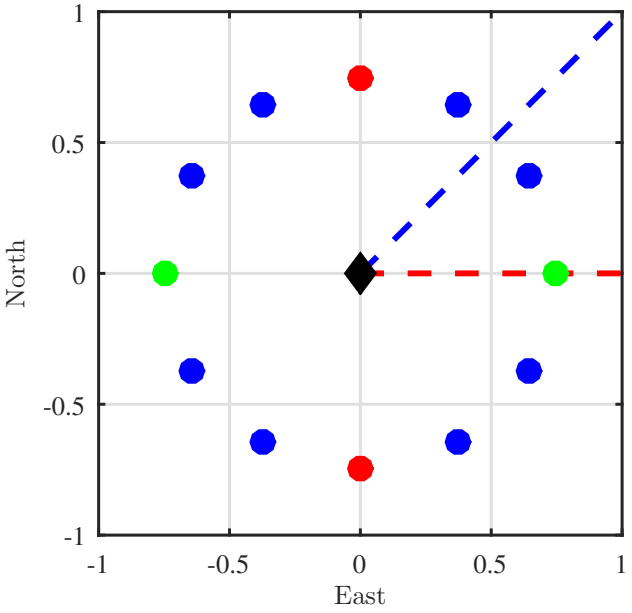

Figure 7: Geometry for the simulations.

ones on the top and bottom are essentially "invisible" to this range (so will demonstrate that the two range test does see them), and the 8 blue ones are partly visible to a single range test. Figure 8 shows the resulting ROC curves from simulations of the two range hypothesis test for all 12 spoofing locations. The observation is that the two range test effectively detects all of the spoofing events. The dotted lines in this figure show the results for a single range detector using the range measurement from the East ($\widehat{r_1}$) and are

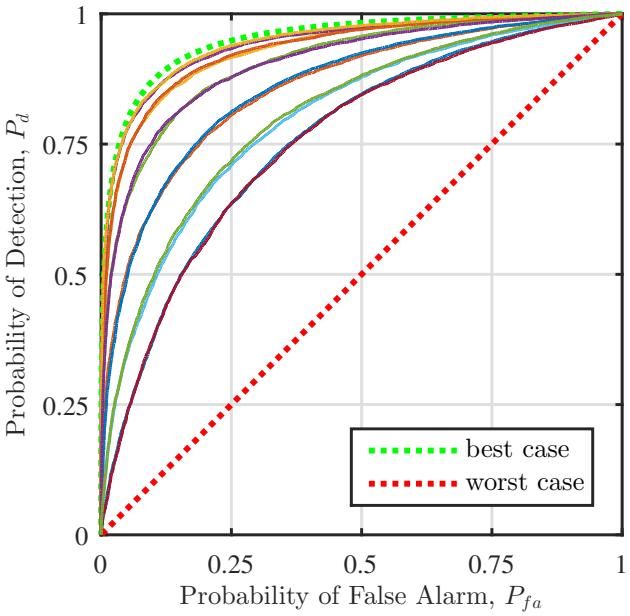

Figure 8: Simulation results with two ranging sources.

color coded to match the spoofer locations directly in line with the ranging source (the green locations) and the spoofer locations perpendicular to the direction to the ranging source (the red dots). The pair of ranging sources reduces this directional sensitivity.

EXTENSIONS

This section briefly describes two extensions to this work that we have considered, stating results without full development.

Randomness in the location of the ranging sources: Consider the situation in which the locations of the ranging sources themselves include some uncertainty (and use the notation $\widehat{e_k}$ and $\widehat{n_k}$ for the knowledge of the locations). Perhaps the locations are just not well known, or that they can move due to some external stimulus (e.g. tide, current, or wind moving a ranging source on a buoy). For example, for $m = 1$ consider a Gaussian model with a different standard deviation for the location of the ranging source

$$(\widehat{e_1}, \widehat{n_1}) \sim \mathcal{N}\left(e_1, n_1, \sigma_r^2, \sigma_r^2, 0\right)$$

It can be shown that the resulting GLRT is identical to that in (5); however, this additional uncertainty does impact the resulting performance. Specifically, the threshold is defined by

$$\lambda = \sqrt{\sigma_g^2 + \sigma_r^2 + \sigma_1^2} \quad Q^{-1}\left(\frac{\mathrm{P_{fa}}}{2}\right)$$

(notice the inclusion of σ_r in this expression) and defining η the same way as above, the probability of detection is

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

Qualitatively, noise on the location of the ranging source reduces the test's ability to detect spoofing. Further, these expressions are valid both under a static assumption on the means for the source's location or if the source measures its own (unspoofed) location and broadcasts this information to the receiver that is testing for spoofing.

Correlated GNSS errors: All of the results above assumed uncorrelated errors on the GNSS measurement. The model in (1) can be extended, allowing a more general covariance model for $\widehat{e}$ and $\widehat{n}$. Specifically, let $\mathbf{\Sigma}_g$ be this covariance

$$\mathbf{\Sigma}_g = \begin{bmatrix} \sigma_e^2 & \rho\sigma_e\sigma_n \\ \rho\sigma_e\sigma_n & \sigma_n^2 \end{bmatrix}$$

With this notation, the GLRT for the general m case can be shown to reduce to

$$\left| \left(\mathbf{\Sigma}_g^{-1} + \mathbf{d}^T\mathbf{\Gamma}^{-1}\mathbf{d}\right)^{-1} \mathbf{d}^T\mathbf{\Gamma}^{-1}\,\delta\mathbf{r} \right| \underset{\mathrm{H_0}}{\overset{\mathrm{H_1}}{\gtrless}} \lambda$$

a direct extension of (6).

CONCLUSIONS/FUTURE WORK

This paper shows how range measurements can be used to detect spoofing (or as an integrity check) of GNSS position measurements:

- A closed form solution and analysis was presented for the case of a single range measurement. These results provide analytical predictions of how well spoofing can be detected. Specifically, we have seen that spoofing offsets greater than $3\sigma_g$ can be detected with low probability of error and high probability of detection; hence, a mobile receiver can recognize spoofing before moving too far off of its desired path. However, a single range measurement is not a solution to all cases primarily due to geometry; it was seen in the development that a spoofer can defeat the test by proper selection of its imposed location.
- These single range results also promote an understanding of how the relative accuracies of the GNSS and range measurements interact to yield spoofing detectability. Specifically, a ranging sensor's precision need not be better than 10 times that of the GNSS sensor; higher precision yields only a very slight improvement in detectability.

Conversely, a range measurement with precision 10 times worse than that of the GNSS sensor provides essentially no information toward detecting spoofing.

- The spoofing test was fully developed for 2 or more range measurements; examples were presented showing that 2 ranges eliminate the spoofer's ability to defeat the test.
- The results were extended to uncertainty in the locations of the ranging sources and to correlated GNSS errors.

Future work includes allowing for configurations with more than one mobile receiver (e.g. the sensor network problem [7]) and investigating how biases in the range measurements would impact the test and its performance; examples include using a terrestrial RF system such as eLoran for the ranges and accommodating the additional secondary factor [8] or measuring altitude with an altimeter and accommodating changes in weather.

REFERENCES

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

[2] 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.

[3] 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.

[4] 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.

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

[6] P. F. Swaszek, R. J. Hartnett, and K. C. Seals, "Adding range information to GNSS positions," under review at *IEEE Trans. Aero. & Elect. Sys.*.

[7] L. Cheng, C. Wu, Y. Zhang, H. Wu, M. Li, and C. Maple "A survey of localization in wireless sensor network," *Intl. Jour. Dist. Sensor Networks*, 2012.

[8] G. Johnson, *et al*, "A procedure for creating optimal ASF grids for harbor entrance & approach," *Proc. ION GNSS 2006*, Fort Worth TX, Sept. 2006.