2013

Analysis of a Simple, Multi-Receiver GPS Spoof Detector

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

Richard J. Hartnett

See next page for additional authors

Citation/Publisher Attribution

Swaszek, Peter F., Hartnett, Richard J., Kempe, Matthew V., Johnson, Gregory W., "Analysis of a Simple, Multi-Receiver GPS Spoof Detector," *Proceedings of the 2013 International Technical Meeting of The Institute of Navigation*, San Diego, California, January 2013, pp. 884-892.
Available at: http://www.ion.org/publications/abstract.cfm?jp=p&articleID=10877

Authors
Peter F. Swaszek, Richard J. Hartnett, Matthew V. Kempe, and Gregory W. Johnson

Analysis of a Simple, Multiple Receiver GPS Spoof Detector

Peter F. Swaszek, *University of Rhode Island*
Richard J. Hartnett and Matthew V. Kempe, *United States Coast Guard Academy*
Gregory W. Johnson, *Alion Science and Technology*

BIOGRAPHY

Peter F. Swaszek is a Professor in the Department of Electrical, Computer, and Biomedical Engineering at URI. He received his PhD in Electrical Engineering from Princeton University in 1982. His research interests are in statistical signal processing with a focus on digital communications and electronic navigation systems. He spent the 2007-08 academic year on sabbatical at the USCGA working on a variety of RF navigation systems.

Richard J. Hartnett is a Professor in Electrical and Computer Engineering at USCGA, having retired from the USCG as a Captain in the summer of 2009. He received his B.S.E.E. degree from USCGA, the M.S.E.E. degree from Purdue University, and his Ph.D. in E.E. from URI. His research interests include efficient digital filtering methods, improved receiver signal processing techniques for electronic navigation systems, and autonomous ground vehicle design.

Gregory W. Johnson served on active duty in the USCG from 1983 to 2002 including tours managing Advanced Communications at the USCG Research and Development Center (RDC) and teaching Electrical Engineering at USCGA. He continues to serve as a Captain in the USCG Reserve. Since 2002 he has managed the Alion Science & Technology, New London Office, primarily supporting RDT&E efforts for the USCG RDC, USCGA, and C3CEN. Dr. Johnson has over 20 years of experience in electrical engineering and project management. He has published over 75 technical papers. He is a member of the IEEE, ION, ILA, and a Life Member of AFCEA.

ABSTRACT

GPS spoofing is a hot topic of late; technical discussions vary widely based upon the assumed capabilities and *a priori* knowledge of the spoofer. For a single GPS receiver, various methods to detect a spoofing event have been proposed in the literature. These range from simple ideas (e.g. monitoring the power levels of the GPS signals) to more complex concepts (e.g. looking for vestigial peaks in the correlator outputs) to the comparison to non-GPS signals (e.g. an IMU). Much of this prior work has been on the conceptual level with limited experimentation; little appears to have been done to analyze the resulting detection performance.

The detector of interest here monitors the GPS signals using not one, but two or more receivers with their antennas at known relative positions. The assumption is that during a spoofing event these multiple receivers will receive the same spoofer RF signal in that the satellites' characteristics (i.e. relative times of arrival) are identical at all of the antennas. With no spoofer present, each antenna would receive a unique RF signal, consistent with its position in space. The concept of the detector, then, is that the presence of spoofing is discernible from the near equivalence of the receivers' receptions. While one could compare these multiple receptions at the RF level, we compare the position solutions across receivers, declaring a spoofing event if the resulting position solutions are too close to each other as compared to the (known) relative locations of the antennas. The primary advantage of such an approach is that the hypothesis test does not require receiver hardware modification or even access to software GPS methods; a separate processor could easily monitor the positions output from the receivers.

In this paper we analyze such a detector from a Neyman-Pearson perspective assuming Gaussian statistics on the position solution data. We consider four cases: (1) two receivers with fixed (known) locations, (2) two receivers with fixed separation and known orientation (but unknown absolute position), (3) two receivers with fixed separation and unknown orientation, and (4) a three receiver example.

INTRODUCTION

The Global Positioning System (GPS) is well known to be an accurate provider of position and time information across the globe. Consulting a dictionary, the term "spoof" or "spoofing" generally refers to a light-hearted deception. When combined together, GPS spoofing refers to intentional (and considered malicious) interference of a GPS user's inputs so as to distort the position and/or time information gained from the system.

GPS spoofing is a hot topic of late; technical discussions can vary widely based upon the assumed capabilities and *a priori* knowledge of the spoofer. In 2003 Warner and Johnston [1] suggested several possible methods to detect a spoofing event: monitoring the power levels of the GPS signals (absolute, relative, and across satellites), checking that the constellation itself is correct for the given time (e.g. number and IDs of the satellites), testing the accuracy of the clock component, and even checking against some non-GNSS source (e.g. an IMU). Since then various authors have experimented with spoofing and suggested detectors including correlating the P(Y) code at the RF level, looking for vestigial peaks in the correlator outputs, comparing to trusted reference signals, and using antenna arrays to spatially identify signals (see e.g. [2-10]). Much of this prior work has been on the conceptual level with limited analysis of the resulting detection performance.

In this paper we examine a spoofing detection concept and attempt to assess its performance. We assume that the spoofer, with only one broadcast antenna, has the ability to present a realistic, but incorrect RF signal at the user's location; this would be possible currently using one of the inexpensive GPS simulators available on the market. We also assume that the spoofer does not have the ability to interfere with the receiver itself; hence, this is spoofing by an external entity, not the operator of a vehicle trying to deceive his/her local GPS.

The detector of interest here monitors the GPS signals using not one, but two or more receivers with their antennas at known relative positions. The assumption is that during a spoofing event these multiple receivers will receive the same spoofer RF signal (since the spoofer can only create one) and that each satellite's characteristic in this signal is identical at all of the antennas. With no spoofer present, each antenna would receive a unique RF signal consistent with its position in space. The concept of the detector, then, is that the presence of spoofing is discernible from the near equivalence of the receivers' receptions. A conceptual discussion of such a detector, and its ability to detect a single spoofer, was presented by Tippenhauer et al [11].

While one could compare these multiple receptions at the RF level (and several of the authors listed above have proposed such detection schemes), a simpler approach that could be implemented with existing GPS receivers would be to have each antenna/receiver compute its position and compare the results across receivers. With such a detector, one could declare a spoofing event if the resulting position solutions are too close to each other as compared to the known, perhaps relative, locations of the antennas. The primary advantage of such an approach is that the hypothesis test does not require receiver hardware modification or even access to software GPS algorithms; a separate processor could easily monitor the positions output from the receivers. Given the uncertainty of the statistics of the signal generated by the spoofer, in this paper we describe the problem as a hypothesis test and analyze the detector from a Neyman-Pearson perspective. We note that our analysis might also be useful for spoof detection schemes based on comparing sequential positions of a vehicle with a single receiver traversing a known trajectory [12].

Assuming *m* antenna/receiver pairs, the hypothesis test of no spoofer versus spoofer is based upon *m* sets of computed positions. Under the null hypothesis (no spoofer), each position solution corresponds to the actual antenna position plus a random offset due to noise. Under the alternative hypothesis (spoofer present), the positions' means would be equal across receivers and the noise statistics could be different. Assuming Gaussian statistics on the position solution offsets, we present detection and false alarm probabilities for several cases: (1) two antennas with fixed (known) locations, (2) two antennas with fixed separation and known orientation (but unknown absolute position), (3) two antennas with fixed separation and unknown orientation, and (4) an example with three receivers/antennas.

The organization of the paper is as follows: (1) we first review the terminology of the detection problem and present the assumed statistics of the data observed, (2) we present some experimental results as a sanity check of the assumptions of the data model, and (3) we develop detection procedures for the 4 distinct cases listed above. Recognizing that our efforts are initial and limited, we conclude with suggested directions for future work (some obvious and easy, some not so).

HYPOTHESIS TESTING

The development of an algorithm to recognize a spoofing event is an example of a binary hypothesis test. To describe our spoofing results, we will employ standard terminology to specify the test between two hypotheses, H_0 and H_1:

H_0: no spoofer

H_1: spoofer

The detector decides for either H_0 or H_1 based upon some observed data. Usually this is implemented by evaluating some scalar function (called the test statistic) of the data, *T*(*data*), and comparing this value to a fixed value (called the threshold), λ. Common notation for this concept is

$$T(data) \underset{H_0}{\overset{H_1}{\gtrless}} \lambda$$

In this representation it is imagined that the test statistic is larger in value under the hypothesis H_1; we can, and will below, occasionally reverse the directions of the threshold test when convenient.

This form of detection approach results in a binary decision (H_0 or H_1, no third result such as "it cannot be determined" is allowed); hence, two types of errors are possible:

- A *false alarm* occurs when the detector decides for H_1, but H_0 is actually true.
- A *miss* occurs when the detector decides for H_0, but H_1 is actually true.

Recognizing that each of these errors has different costs to the user, we might want to treat them differently. For example, a false alarm might mean waiting and attempting some task later on new data while a miss might have more dire consequences. As such, we follow the Neyman-Pearson formulation of detection:

- Set the level of the test, its probability of false alarm, p_{fa}, to some allowable, but small value (often written as α):

$$p_{\text{fa}} = \Pr\{T(data) > \lambda \mid H_0\} \le \alpha$$

- Try to maximize the power, or probability of detection, p_{d}, of the test where power is defined as one minus the probability of a miss

$$p_{\text{d}} = 1 - p_{\text{miss}} = \Pr\{T(data) > \lambda \mid H_1\}$$

As stated in the Introduction above, the data available for the detection method is the (assumed simultaneous) position estimates from a set of m GPS receivers. For convenience, we assume that each of these 3-dimenional vectors is available in a common east, north, up (ENU) reference frame; so that we have the vector observations

$$\hat{\mathbf{p}}_k = \begin{bmatrix} \hat{e}_k \\ \hat{n}_k \\ \hat{u}_k \end{bmatrix}$$

for k ranging over 1 to m (we use hats on variables to indicate that they are noisy estimates). For most of the work below we will consider two receivers, so $k = 1$ or 2.

To develop and analyze detectors, we need to specify the statistics of the data under the two hypotheses. For simplicity, we will make the assumption that the estimation error is Gaussian (due to assumptions of Gaussian receiver noise and/or the linear nature of the position solution algorithms); the specifics of the model vary under the two hypotheses as follows:

- Under H_0 (no spoofing), the mean of each position estimate is the true position of the receiver's antenna (no hats)

$$E_0\{\hat{\mathbf{p}}_k\} = \begin{bmatrix} E_0\{\hat{e}_k\} \\ E_0\{\hat{n}_k\} \\ E_0\{\hat{u}_k\} \end{bmatrix} = \begin{bmatrix} e_k \\ n_k \\ u_k \end{bmatrix} = \mathbf{p}_k$$

The covariance matrix for each $\hat{\mathbf{p}}_k$ is some nominal matrix Σ_0 (due to local noise, satellite DOP, etc) and is independent of k since the receivers are assumed to be near each other. Finally, the estimates across the different receivers are assumed independent; in other words, the cross covariance matrix for $\hat{\mathbf{p}}_j$ and $\hat{\mathbf{p}}_k$ is a 3-by-3 zero matrix.

- Under H_1 (spoofing), the mean of each position estimate is an unknown position, $\mathbf{p}_s$, determined by the spoofer

$$E_1\{\hat{\mathbf{p}}_k\} = \begin{bmatrix} E_1\{\hat{e}_k\} \\ E_1\{\hat{n}_k\} \\ E_1\{\hat{u}_k\} \end{bmatrix} = \mathbf{p}_s$$

Of significance is that this mean is independent of k (!), all receivers "see" the same position. Further, the covariance matrix for each $\hat{\mathbf{p}}_k$ is determined by the spoofer and is unknown to the GPS user; we will employ the notation Σ_1. As was stated for H_0, we will assume that this within receiver covariance is independent of k. Finally, the cross covariance matrix for $\hat{\mathbf{p}}_j$ and $\hat{\mathbf{p}}_k$ is written as Σ_{1jk} and may not be zero as it was under H_0.

A SANITY CHECK ON THE MODEL

While a Gaussian model is a good place to start an examination of a problem such as this (hopefully to lead to tractable results), it is natural to wonder about the stated assumptions on the means and covariances. Toward that end we experimented with a pair of GPS sensors at the Coast Guard Academy. To assess the no spoofer hypothesis, H_0, we mounted the receivers at a known separation (approximately 20 feet) on a rooftop and collected several days of data (at a rate of 1-second updates). For spoofing, we brought the same receivers indoors and employed a commercial GPS reradiator (the equivalent of a meaconing spoofer) and collected another data set of similar size. The feed of this reradiator was also on the rooftop, in between the two receiver positions for the no spoofer test. The observation, then, is a series of 6 dimensional position vectors:

$$\left[\hat{e}_1, \hat{n}_1, \hat{u}_1, \hat{e}_2, \hat{n}_2, \hat{u}_2\right]^T$$

From this data set, we examined the usual navigation performance via the horizontal scatter and then some basic statistics.

First, Figure 1 shows the horizontal (east and north) scatter for the rooftop test, no spoofer. The two receivers were mounted with an almost north-south orientation. The average position of the more southerly receiver was defined as the zero point for the scatter; typical individual points are shown in red, the mean as a black dot at the origin, and the 95% containment circle had radius of 4.35 meters. The performance of the second receiver, approximately 20 feet to the north, is represented in blue (some of the blue points obscure red ones). Note that its mean falls just where we expected that it would be (the second black dot) and the 95% radius is almost the same as the first receiver at 4.33 m.

Figure 2 shows the result under the H_1 spoofing experiment (meaconing). Now both means appear as a single black dot slightly to the north of zero (again, our reraditor antenna was somewhat to the north of our defined origin) and the 95% circles are smaller and of somewhat different radii. We expect that this difference is due to the higher quality of the reradiator antenna, its amplification, and that when mounted indoors, one of the two test receivers was closer to the reradiator than the other.

From the scatter presented it is clear that the means of the observations clearly meet our assumptions – accurate under no spoofing and equal under spoofing. We also computed sample covariance matrices under both hypotheses. These were

$$\mathbf{\Sigma}_0 = \begin{bmatrix} 2.29 & -0.56 & 0.32 & 0.08 & -0.10 & -0.20 \\ -0.56 & 3.16 & -0.00 & -0.13 & 0.07 & -0.01 \\ 0.32 & -0.00 & 11.0 & -0.08 & 0.13 & 0.34 \\ 0.08 & -0.13 & -0.08 & 2.29 & -0.38 & -0.33 \\ -0.10 & 0.07 & 0.13 & -0.38 & 3.22 & 0.33 \\ -0.20 & -0.01 & 0.34 & -0.33 & 0.33 & 10.8 \end{bmatrix}$$

and

$$\mathbf{\Sigma}_1 = \begin{bmatrix} 0.90 & -0.06 & -0.09 & 0.58 & -0.09 & 0.14 \\ -0.06 & 1.64 & 0.32 & -0.0 & 0.97 & 0.33 \\ -0.09 & 0.32 & 4.84 & 0.09 & 0.22 & 3.32 \\ 0.58 & -0.0 & 0.09 & 1.76 & -0.15 & -0.35 \\ -0.09 & 0.97 & 0.22 & -0.15 & 2.84 & 0.36 \\ 0.14 & 0.33 & 3.32 & -0.35 & 0.36 & 9.55 \end{bmatrix}$$

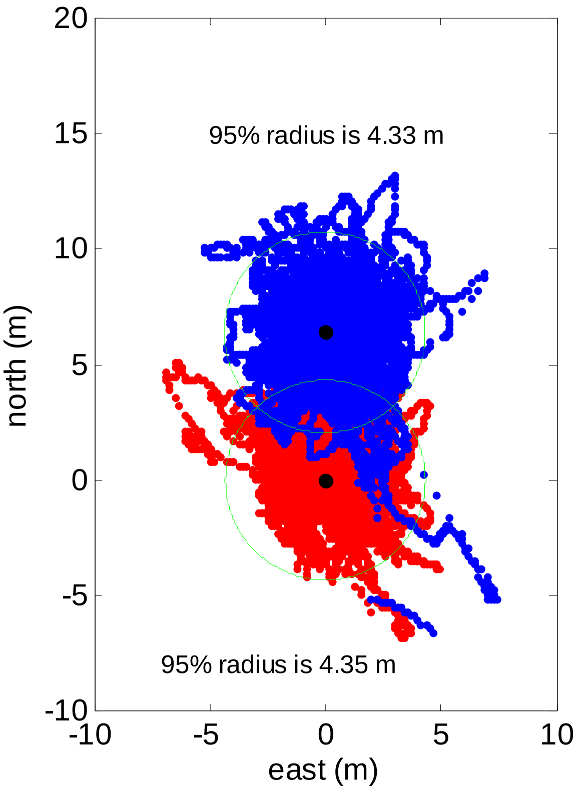

Figure 1 – Sample horizontal scatter under H_0.

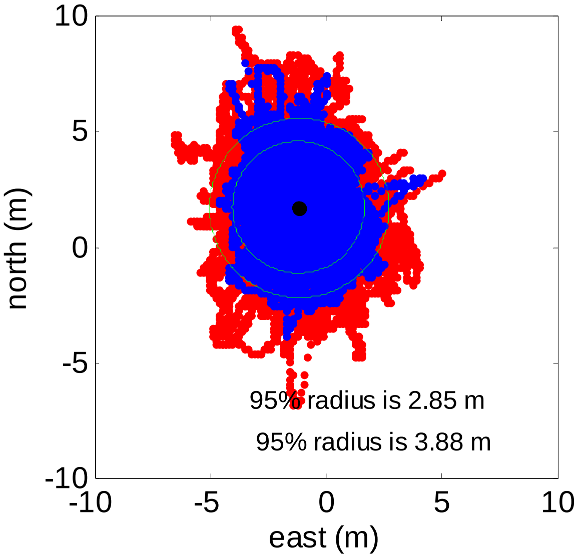

Figure 2 – Sample horizontal scatter under H_1.

We observe that many of the elements of these two arrays are approximately zero; hence, we propose the following simple model for the covariances of our two receiver detector:

- Under H_0 the covariance is

$$\mathbf{\Sigma}_0 = \begin{bmatrix} \mathbf{\Sigma}_{0a} & \mathbf{0} \\ \mathbf{0} & \mathbf{\Sigma}_{0b} \end{bmatrix}$$

  with

$$\mathbf{\Sigma}_{0a} = \mathbf{\Sigma}_{0b} = \begin{bmatrix} \sigma_{e0}^2 & 0 & 0 \\ 0 & \sigma_{n0}^2 & 0 \\ 0 & 0 & \sigma_{u0}^2 \end{bmatrix}$$

  This simplistic model has all of the components being independent and the variances being direction dependent.

- Under H_1 the covariance is

$$\mathbf{\Sigma}_1 = \begin{bmatrix} \mathbf{\Sigma}_{1a} & \mathbf{\Sigma}_{1ab}^T \\ \mathbf{\Sigma}_{1ab} & \mathbf{\Sigma}_{1b} \end{bmatrix}$$

  with

$$\mathbf{\Sigma}_{1a} = \mathbf{\Sigma}_{1b} = \begin{bmatrix} \sigma_{e1}^2 & 0 & 0 \\ 0 & \sigma_{n1}^2 & 0 \\ 0 & 0 & \sigma_{u1}^2 \end{bmatrix}$$

  and

$$\mathbf{\Sigma}_{1ab} = \begin{bmatrix} \rho\sigma_{e1}^2 & 0 & 0 \\ 0 & \rho\sigma_{n1}^2 & 0 \\ 0 & 0 & \rho\sigma_{u1}^2 \end{bmatrix} = \rho\mathbf{\Sigma}_{1a}$$

  In this model the components for each receiver are still independent with directionally dependent covariances. The covariances across receivers is now not zero; specifically, the east, north, and up components are correlated. In our sanity check data, this correlation coefficient was 0.4.

SPOOF DETECTORS

Below we develop and analyze detectors for four different user scenarios with the spoofing model described above; primarily we focus on the case of two receivers. We note that the independent Gaussian assumption under H_0 will make the development of the detectors and their false alarm analyses tractable. However, the unknown statistics (mean and covariance) under H_1, even though the model assumed is quite simple, make the development of an optimum detector impossible. Hence, we develop sensible detectors, analyze them under H_0 to solve for the threshold in terms of the desired/acceptable false alarm probability, and then, as possible, consider what happens to the detection probability.

CASE 1 – KNOWN LOCATIONS

First, we imagine that the location of the two receivers is precisely known. In that case, the hypotheses are

- H_0: the position observation is a Gaussian random vector in 6-dimensional space with mean vector and covariance matrix

$$\mu = \begin{bmatrix} \mathbf{p}_1 \\ \mathbf{p}_2 \end{bmatrix}, \; \mathbf{\Sigma}_0 = \begin{bmatrix} \mathbf{\Sigma}_{0a} & \mathbf{0} \\ \mathbf{0} & \mathbf{\Sigma}_{0b} \end{bmatrix}$$

- H_1: the position observation is a Gaussian random vector in a 6-dimensional space with mean vector and covariance matrix

$$\mu = \begin{bmatrix} \mathbf{p}_s \\ \mathbf{p}_s \end{bmatrix}, \; \mathbf{\Sigma}_1 = \begin{bmatrix} \mathbf{\Sigma}_{1a} & \mathbf{\Sigma}_{1ab}^T \\ \mathbf{\Sigma}_{1ab} & \mathbf{\Sigma}_{1b} \end{bmatrix}$$

How should the detector exploit this statistical difference? One obvious method is to compute the size (radius squared) of the Gaussian ellipsoid about the mean vector under H_0 that contains the observation point and compare this size parameter to a threshold. If the ellipsoid is large, then we are likely experiencing spoofing. The resulting test is

$$\begin{aligned} T(\hat{\mathbf{p}}_1, \hat{\mathbf{p}}_2) = {} & (\hat{\mathbf{p}}_1 - \mathbf{p}_1)^T \Sigma_{0a}^{-1} (\hat{\mathbf{p}}_1 - \mathbf{p}_1) \\ & + (\hat{\mathbf{p}}_2 - \mathbf{p}_2)^T \Sigma_{0b}^{-1} (\hat{\mathbf{p}}_2 - \mathbf{p}_2) \end{aligned}$$

$T < \lambda$ decide H_0
$T > \lambda$ decide H_1

Beyond being a reasonable test, it uses the knowledge of the true positions and is amenable to statistical analysis under H_0. Specifically, under H_0 the test statistic, T, is distributed as a chi-squared random variable with 6 degrees of freedom. The false alarm probability is then

$$p_{\text{fa}} = e^{-\frac{\lambda}{2}} \sum_{k=0}^{5} \frac{\lambda^k}{k! 2^k}$$

From this expression, the threshold can be found numerically. For example, $\lambda = 26$ yields $p_{\text{fa}} \approx 1\%$. The probability of detection, p_{d}, is, in general, intractable due to its dependence on $\mathbf{p}_{\text{s}}$. We note that it might be possible to do a worst case analysis (lowest p_{d}); for simple choices of $\mathbf{\Sigma}_1$ this might occur if $\mathbf{p}_{\text{s}}$ is the mean of $\mathbf{p}_1$ and $\mathbf{p}_2$. Such an event is probably not very useful from the perspective of the spoofer, however, so a worst case analysis in this case appears to be of little use.

CASE 2 – KNOWN SEPARATION AND ORIENTATION

Next, imagine that both receivers' locations have some unknown offset, but that the vector difference in the locations is known. Said another way, we are assessing spoofing on a moving vehicle that has additional sensors (e.g. a compass) to indicate orientation. In that case, a natural transformation of the observation data is to the difference of the observations

$$\hat{\mathbf{d}} = \hat{\mathbf{p}}_1 - \hat{\mathbf{p}}_2 = \begin{bmatrix} \hat{e}_1 - \hat{e}_2 \\ \hat{n}_1 - \hat{n}_2 \\ \hat{u}_1 - \hat{u}_2 \end{bmatrix}$$

With this modified data set, the hypotheses are

- H_0: $\hat{\mathbf{d}}$ is a 3-dimensional Gaussian random vector with mean $\mathbf{d} = \mathbf{p}_1 - \mathbf{p}_2$ and covariance $2\boldsymbol{\Sigma}_{0a}$

$$\hat{\mathbf{d}} \sim N(\mathbf{d}, 2\boldsymbol{\Sigma}_{0a})$$

- H_1: $\hat{\mathbf{d}}$ is a 3-dimensional Gaussian random vector with mean $\mathbf{0}$ (since the receivers are assumed to have equal positions under spoofing) and different covariance

$$\hat{\mathbf{d}} \sim N(\mathbf{0}, 2\boldsymbol{\Sigma}_{1a} - 2\boldsymbol{\Sigma}_{1ab})$$

The unknown covariances under H_1 still make an optimum test impossible to construct; however, a natural test for a difference in mean vectors is to project (under H_0) the observed difference onto that known difference, so we consider

$$T(\hat{\mathbf{d}}) = \mathbf{d}^T \boldsymbol{\Sigma}_{0a}^{-1} \hat{\mathbf{d}} \underset{H_1}{\overset{H_0}{\gtrless}} \lambda$$

(Note that the threshold test is reversed from the normal definition; a large projection corresponds to H_0.)

As in Case 1, this second test is amenable to statistical analysis. Specifically, under H_0 the test statistic, T, is Gaussian distributed

$$T(\hat{\mathbf{d}}) \sim N\left(\mathbf{d}^T \boldsymbol{\Sigma}_{0a}^{-1} \mathbf{d}, 2\mathbf{d}^T \boldsymbol{\Sigma}_{0a}^{-1} \mathbf{d}\right)$$

It is also Gaussian under H_1, but with zero mean and a different (and unknown) covariance matrix

$$T(\hat{\mathbf{d}}) \sim N\left(\mathbf{0}, 2\mathbf{d}^T \boldsymbol{\Sigma}_{0a}^{-1} \left(\boldsymbol{\Sigma}_{1a} - \boldsymbol{\Sigma}_{1ab}\right) \boldsymbol{\Sigma}_{0a}^{-1} \mathbf{d}\right)$$

Using these parameters, we can solve for the false alarm probability

$$p_{\text{fa}} = \Pr\left(T(\hat{\mathbf{d}}) < \lambda \mid \mathrm{H}_0\right) = 1 - Q\left(\frac{\lambda - \mathbf{d}^T \boldsymbol{\Sigma}_{0a}^{-1} \mathbf{d}}{\sqrt{2\mathbf{d}^T \boldsymbol{\Sigma}_{0a}^{-1} \mathbf{d}}}\right)$$

We can invert this expression to find the threshold

$$\lambda = \mathbf{d}^T \boldsymbol{\Sigma}_{0a}^{-1} \mathbf{d} + \sqrt{2\mathbf{d}^T \boldsymbol{\Sigma}_{0a}^{-1} \mathbf{d}}\; Q^{-1}\left(1 - p_{\text{fa}}\right)$$

and, hence, write the probability of detection as

$$\begin{aligned} p_{\text{d}} &= \Pr\left(T(\hat{\mathbf{d}}) < \lambda \mid \mathrm{H}_1\right) \\ &= 1 - Q\left(\frac{\mathbf{d}^T \boldsymbol{\Sigma}_{0a}^{-1} \mathbf{d} + \sqrt{2\mathbf{d}^T \boldsymbol{\Sigma}_{0a}^{-1} \mathbf{d}}\; Q^{-1}(1 - p_{\text{fa}})}{\sqrt{2\mathbf{d}^T \boldsymbol{\Sigma}_{0a}^{-1} \left(\boldsymbol{\Sigma}_{1a} - \boldsymbol{\Sigma}_{1ab}\right) \boldsymbol{\Sigma}_{0a}^{-1} \mathbf{d}}}\right) \end{aligned}$$

In all of these expression, Q() is the usual Gaussian tail probability.

As an example of these results, consider the case of a horizontal platform ($u_1 = u_2$) and equal horizontal covariances at the two receivers under H_0

$$\boldsymbol{\Sigma}_{0a} = \boldsymbol{\Sigma}_{0a} = \begin{bmatrix} \sigma_0^2 & 0 & 0 \\ 0 & \sigma_0^2 & 0 \\ 0 & 0 & \sigma_{u0}^2 \end{bmatrix}$$

Then the detector simplifies

$$T(\hat{\mathbf{d}}) = \frac{\mathbf{d}^T \hat{\mathbf{d}}}{\sigma_0^2} \underset{H_1}{\overset{H_0}{\gtrless}} \lambda$$

(Strictly, in this inner product the contribution of the up term is zero.) Further, assume under H_1 that the covariances are

$$\boldsymbol{\Sigma}_{1a} = \boldsymbol{\Sigma}_{1b} = \begin{bmatrix} \sigma_1^2 & 0 & 0 \\ 0 & \sigma_1^2 & 0 \\ 0 & 0 & \sigma_{u1}^2 \end{bmatrix}$$

and

$$\boldsymbol{\Sigma}_{1ab} = \begin{bmatrix} \rho\sigma_1^2 & 0 & 0 \\ 0 & \rho\sigma_1^2 & 0 \\ 0 & 0 & \rho\sigma_{u1}^2 \end{bmatrix}$$

then the performance is

$$p_{\text{d}} = 1 - Q\left(\frac{|\mathbf{d}| + \sqrt{2}\,\sigma_0\; Q^{-1}(1 - p_{\text{fa}})}{\sigma_1 \sqrt{2(1 - \rho)}}\right)$$

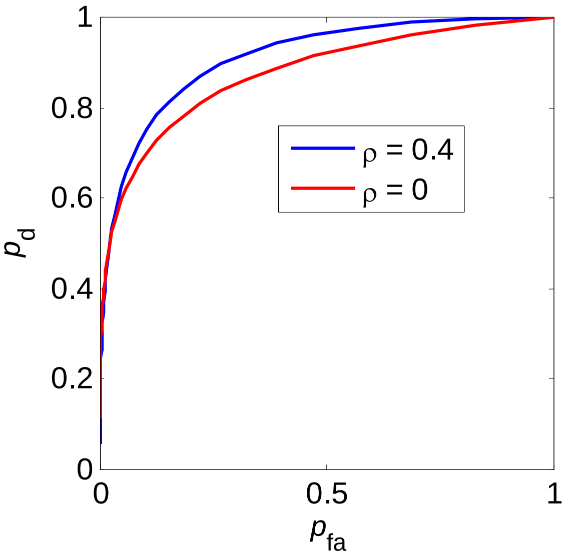

Figure 3 – Example receiver operating characteristic (ROC) curve for Case 2.

As a numerical example, let $\sigma_1 = \sigma_0 = \sigma$ and $|\mathbf{d}| = 2\sigma$. Figure 3 shows the receiver operating characteristic (ROC) curve, a plot of the false alarm and detection probabilities as implicit functions of the threshold, for two choices of correlation coefficient, 0 and 0.4. Our observation from this simple example is that any potential (positive) correlation between the two spoofed receivers improves the ability to detect the spoofer. This performance would also improve if the receivers have a greater separation (larger $|\mathbf{d}|$).

CASE 3 – KNOWN SEPARATION ONLY

To lessen the amount of information known to the detection algorithm, imagine that we know only the spacing between the receivers' locations, that the orientation and absolute locations are unknown. As in Case 2, we transform the observation data to the difference of the observations

$$\hat{\mathbf{d}} = \hat{\mathbf{p}}_1 - \hat{\mathbf{p}}_2$$

Without orientation information (and paralleling the concepts introduced in Case 1), our choice for a test statistic is the scale of the 3-dimenional ellipsoid (under H_0) about the origin (the $\mathbf{0}$ vector) that contains $\hat{\mathbf{d}}$; equivalently, the distance (under H_0) between the two estimated positions. If this ellipsoid is small, we decide for a spoofer; if large, no spoofer:

$$T(\hat{\mathbf{d}}) = \hat{\mathbf{d}}^T \mathbf{\Sigma}_{0a}^{-1} \hat{\mathbf{d}} \underset{H_1}{\overset{H_0}{\gtrless}} \lambda$$

Under H_0 this test statistic is a non-central chi-squared random variable with 3 degrees of freedom; the non-centrality parameter is based on the distance between the receivers. Generally under H_1 the distribution is intractable.

To proceed further, once again consider the case of a horizontal platform ($u_1 = u_2$) with equal horizontal covariances under H_0

$$\mathbf{\Sigma}_{0a} = \mathbf{\Sigma}_{0a} = \begin{bmatrix} \sigma_0^2 & 0 & 0 \\ 0 & \sigma_0^2 & 0 \\ 0 & 0 & \sigma_{u0}^2 \end{bmatrix}$$

then

$$T(\hat{\mathbf{d}}) = \frac{|\hat{\mathbf{d}}|^2}{\sigma_0^2} \underset{H_1}{\overset{H_0}{\gtrless}} \lambda$$

(again, the up component of the positions are ignored). Equivalently, by multiplying through by σ_0^2, this is

$$T(\hat{\mathbf{d}}) = (\hat{e}_1 - \hat{e}_2)^2 + (\hat{n}_1 - \hat{n}_2)^2 \underset{H_1}{\overset{H_0}{\gtrless}} \lambda'$$

or taking the square root, we have an equivalent test on the distance between the estimated positions

$$T(\hat{\mathbf{d}}) = \sqrt{(\hat{e}_1 - \hat{e}_2)^2 + (\hat{n}_1 - \hat{n}_2)^2} \underset{H_1}{\overset{H_0}{\gtrless}} \lambda''$$

Now, under H_0, since the east and north components are iid Gaussian, the differences are also Gaussian (with non-zero means and variances $2\sigma_0^2$), so T has a Rician distribution. Under H_1, if we assume that

$$\mathbf{\Sigma}_{1a} = \mathbf{\Sigma}_{1b} = \begin{bmatrix} \sigma_1^2 & 0 & 0 \\ 0 & \sigma_1^2 & 0 \\ 0 & 0 & \sigma_{u1}^2 \end{bmatrix}$$

and

$$\mathbf{\Sigma}_{1ab} = \begin{bmatrix} \rho\sigma_1^2 & 0 & 0 \\ 0 & \rho\sigma_1^2 & 0 \\ 0 & 0 & \rho\sigma_{u1}^2 \end{bmatrix}$$

then the differences have zero means and variances equal to $2(1-\rho)\sigma_1^2$, so T is Rayleigh distributed. With these assumptions

$$p_{\text{fa}} = 1 - Q_1\left(\frac{|\mathbf{d}|}{\sqrt{2\sigma_0^2}}, \frac{\lambda}{\sqrt{2\sigma_0^2}}\right)$$

($Q_1(\cdot,\cdot)$ is Marcum's Q function – see a digital communications text), λ can be found by numerically inverting this expression, and

$$p_{\text{d}} = 1 - \exp\left(-\frac{\lambda^2}{4\sigma_1^2(1-\rho)}\right)$$

CASE 4 – THREE RECEIVERS

The two receiver formulation above naturally led to test statistics based upon the distance between the two estimated positions. To extend our spoofing detector concept to more receivers, we keep this focus on inter-receiver distances.

Rather than pursuing a general result, we continue with the assumptions above of a horizontal platform and equal horizontal covariances. The test statistic will be the sum of the estimated distances between the receivers. For three receivers, this is

$$T(\hat{d}_{12}, \hat{d}_{23}, \hat{d}_{13}) = \hat{d}_{12} + \hat{d}_{23} + \hat{d}_{13} \underset{\text{H}_1}{\overset{\text{H}_0}{\gtrless}} \lambda'$$

in which

$$\hat{d}_{jk} = \sqrt{(\hat{e}_j - \hat{e}_k)^2 + (\hat{n}_j - \hat{n}_k)^2}$$

Again, this distance is expected to be small under spoofing.

A new and significant issue regarding the use of three or more receivers to detect spoofing is deciding upon their spatial configuration. To start to explore this issue, we compare below two setups: a linear configuration and an equilateral triangular configuration. These can be seen in Figure 4. For comparison's sake, we will set the inter-receiver spacing so that the total of the three distances is a constant (note that for the linear configuration, this also includes the distance between receivers 1 and 3).

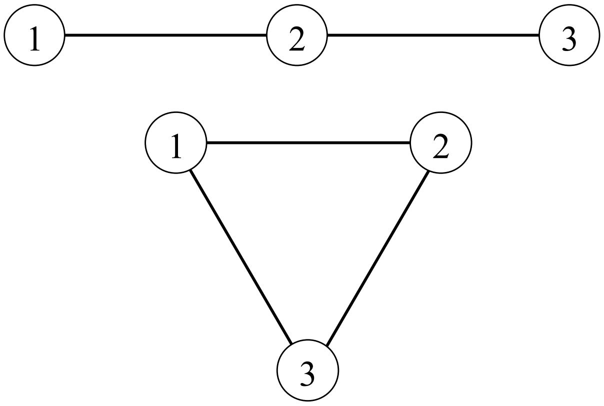

Figure 4 – Configurations of 3 receivers considered: linear and triangular.

Even with the simplicity of the assumed statistical model, the correlations inherent in the pair wise differences combined with the squaring and square-root functions make the statistics of the test statistic, T, intractable. So, instead, we consider a simple example via simulation. Specifically, we scale the receiver spacing so that

$$d_{12} + d_{13} + d_{23} = 10\sigma_0$$

Further, we assume that under H$_1$ we have equal variances, $\sigma_1^2 = \sigma_0^2$, and that the receivers are statistically independent, $\rho = 0$. Figure 5 shows the ROC curve based upon a Monte Carlo simulation comparing the two receiver configurations. Since a ROC curve that appears more toward the upper left of the diagram is better for detection, we see that the triangular configuration is better than the linear in this example.

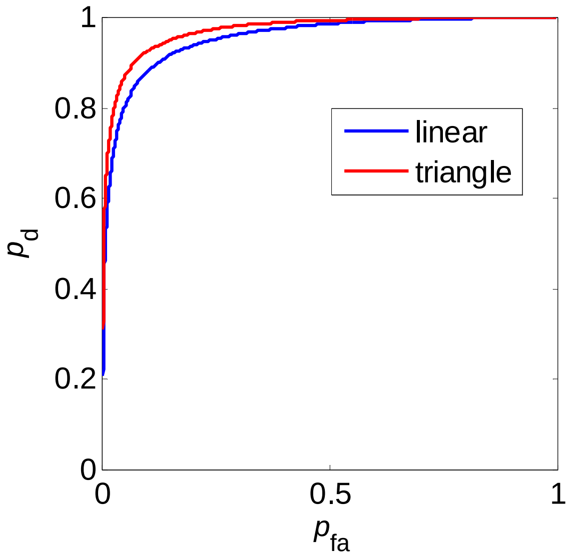

Figure 5 – ROC curves for 3 receivers in linear and triangular configurations by simulation.

CONCLUSIONS

Our goal in this paper was to initiate the analysis of GPS spoofing detection methods. While we have chosen a simple detection scheme, based upon multiple, spatially separated GPS receivers, and have made a number of simplifying statistical assumptions in order to proceed, we feel that we have achieved that goal and look forward to further results on the design and analysis of spoofing detection.

FUTURE WORK

As far as we have been able to deduce, this paper presents the first statistical analysis of a multi-receiver spoofing detection algorithm. To make some initial headway on the problem, a number of simplifying assumptions have been made; much room for improvement is possible. Specifically, we propose that the following extensions could be addressed:

- While we assumed independence for mathematical simplicity, some simple correlation models under H_0 could be employed; the equal variance assumption for the horizontal position variables (east and north) could easily be replaced by values determined from the DOP.
- Further experimentation and analysis effort should be expended on selecting realistic models for the data under H_1; we should try to find the worst case choices for $\mathbf{p}_s$ and $\mathbf{\Sigma}_1$.
- A more general analysis of the 3 receiver case should be developed; other arrangements of 3 receivers should be considered; the case of 4 receivers in rectangular and diamond-shaped configurations should be considered.
- As some receivers make the pseudoranges themselves available, one could develop test statistics on them directly; as noted by one audience member during the conference, these same techniques could be applied to comparing the phase relationship of GPS signals at closely spaced antennas.
- As the proposed tests are "snapshot" methods employing just a single set of positions, sequential tests that exploit the inter-receiver correlations under spoofing, yet allow a decision of "I don't know yet" could be quite effective.
- So far we have assumed a static platform with synchronized positions; this should be expanded to moving vehicles and time offsets between receivers.

DISCLAIMER

The views expressed herein are those of the authors and are not to be construed as official or reflecting the views of the U.S. Coast Guard.

REFERENCES

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

[2] Papadimitratos, P., and Jovanovic, A., "GNSS-based positioning: attacks and countermeasures," *Proc. IEEE MILCOM*, Nov. 2008.

[3] Montgomery, P. Y., Humphreys, T. E., and Ledvina, B. M., "Receiver-autonomous spoofing detection: experimental results of a multi-antenna receiver defense against a portable civil GPS spoofer," *Proc. ION ITM*, Jan 2009.

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

[5] O'Hanlon, B. W., Psiaki, M. L., Humphreys, T. E., and Bhatti, J. A., "Real-time spoofing detection in a narrow-band civil GPS receiver," *Proc. ION GNSS*, Sept. 2010.

[6] Cavaleri, A., Motella, B., Pini, M., and Fantion, M., "Detection of spoofed GPS signals at code and carrier tracking level," *Proc. NAVITEC*, Dec. 2010.

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

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

[9] Meurer, M., Konovaltsev, A., Cuntz, M. and Hättich, C., "Robust joint multi-antenna spoofing detection and attitude estimation using direction assisted multiple hypothesis RAIM," Proc. *ION GNSS*, Sept. 2012.

[10] Jafarnia-Jahromi, A., Broumandon, A., Nielsen, J., and Lachapelle, G., "GPS vulnerability to spoofing threats and a review of antispoofing techniques," *Int'l. Jour. Navigation and Observation*, 2012.

[11] Tippenhauer, N. O., Pöpper, C., Rasmussen, K. B., and Čapkun, S., "On the requirements for successful GPS spoofing attacks," *Proc. ACM CCS*, Oct. 2011.

[12] Nielsen, J., Broumandan, A., and LaChapelle, G., "GNSS spoofing detection for single antenna handheld receivers," *Navigation*, Winter 2011.