A Combined Symmetric Difference and Power Monitoring GNSS Anti-Spoofing Technique

Kyle D. Wesson and Brian L. Evans
Department of Electrical and
Computer Engineering
The University of Texas at Austin
Email: kyle.wesson@utexas.edu, bevans@ece.utexas.edu

Todd E. Humphreys
Department of Aerospace Engineering and
Engineering Mechanics
The University of Texas at Austin
Email: todd.humphreys@mail.utexas.edu

***Abstract*—Civil Global Navigation Satellite System (GNSS) signals are vulnerable to spoofing attacks that deceive a victim receiver into reporting counterfeit position or time information. The primary contribution of this paper is a non-cryptographic GNSS anti-spoofing technique that "sandwiches" a spoofer between a correlation function distortion monitor and a total in-band power monitor. The defense exploits the difficulty of mounting an effective spoofing attack that simultaneously maintains a low-enough counterfeit signal power to avoid power monitoring alarms while minimizing distortions of the received cross-correlation profile that are indicative of a spoofing attack. Results presented in this paper demonstrate the defense's effectiveness against a sophisticated spoofing attack.**

***Index Terms*—Satellite Navigation Systems, Communication System Security, Detection Algorithms**

I. Introduction

Civil Global Navigation Satellite System (GNSS) signals are broadcast unencrypted worldwide according to an open standard. The virtues of an open standard and global availability have made GNSS a huge success. Yet the transparency and predictability of these signals makes them easy to counterfeit, or spoof. During a spoofing attack, a malefactor broadcasts forged GNSS signals that deceive a victim receiver into reporting the spoofer-controlled navigation or timing solution [1]. Given the extensive integration of civil GNSS into critical national infrastructure and safety-of-life applications, a successful spoofing attack could have serious consequences [2].

Practical and effective space-segment-side cryptographic anti-spoofing techniques have been proposed that would offer worldwide GNSS signal authentication [3], [4]. But the long wait time needed to realize such approaches motivates development and implementation of nearer-term space-segment-independent anti-spoofing techniques. This paper proposes a receiver-autonomous signal-processing anti-spoofing technique that could be implemented immediately. The technique relies on the difficulty of carrying out a successful spoofing attack that simultaneously maintains a low-enough counterfeit signal power to avoid power monitoring alarms while minimizing distortions of the received cross-correlation profile that are indicative of a spoofing attack. The technique could be implemented in a simple firmware change on a wide range of consumer receivers, which makes it an attractive near-term option for anti-spoofing.

II. The Distortion-Power Tradeoff

The hallmark distortions of a spoofing attack result from the interactions of authentic and spoofing signals [5], [6]. There are only two ways by which a spoofer can eliminate an authentic signal impinging on a victim receiver: (1) by generating an antipodal, or nulling, signal, or (2) by blocking reception of the authentic signal. For the former, a spoofer requires both (a) centimeter-accurate knowledge of the relative three-dimensional position vector from the phase center of its antenna to the phase center of the victim receiver's antenna, and (b) 100-picosecond-accurate knowledge of its processing and transmission delay. For the latter, the spoofer requires physical access to the victim receiver. Assuming the former is impractical and the latter is preventable, an admixture of authentic and spoofing signals will be present during a spoofing attack.

Falling short of eliminating the authentic signal, the spoofer could alternatively broadcast a spoofing signal with a significantly higher power than the authentic signal. In the limit as the spoofed signals overpower the authentic signals, the spoofer's power advantage will force the despread authentic signals below the thermal noise floor, thereby eliminating the tell-tale distortions indicative of a spoofing attack. To prevent such a workaround, the "sandwich" defense proposed here employs a power monitor that limits the spoofer's power advantage factor over the corresponding authentic signal, thereby ensuring tell-tale distortions are present for the correlation-distortion monitor to detect.

Both the power monitor and the correlation-distortion monitor were proposed separately as self-contained anti-spoofing techniques in [7] and [8], respectively. But these approaches, taken independently, are inadequate because of their high false alarm rates. Power monitoring techniques are sensitive to jamming, and correlation distortion monitors can trigger on severe multipath [5]. The combination of the two approaches, however, provides a higher efficacy and lower false alarm rate than either one alone and offers a low-complexity anti-spoofing technique.

A significant challenge for the proposed sandwich defense is the similarity between the interaction of the authentic and spoofed GNSS signals and the interaction of multipath

Preprint of the 2013 IEEE Global Conference on Signal and Information Processing (GlobalSIP), Austin, TX, Dec 3–5, 2013

and direct-path GNSS signals [5]. To address this problem, the technique leverages a set of recorded spoofing attacks against the Global Positioning System (GPS) called the Texas Spoofing Test Battery (TEXBAT) [6]. High-fidelity empirical probability distribution functions based on TEXBAT and additional multipath-laden recordings, reveal that multipath can be reliably distinguished from effective spoofing provided that the spoofing signals' power advantage over the authentic signals is strictly limited.

III. System Model

Let $R^i(\tau)$ be the noise-free autocorrelation function that results from correlating the pseudorandom spreading code of satellite i with itself at offset τ. For satellite i, the receiver computed autocorrelation function ξ can be modeled as

$$\xi^i(t,\tau) = \alpha_d^i(t)R^i(\tau - \tau_d^i(t))e^{j\theta_d^i(t)} + m^i(t,\tau) + s^i(t,\tau) + n^i(t,\tau) \quad (1)$$

Here, at time t, $\alpha_d^i(t)$ is a real-valued scaling factor, $\tau_d^i(t)$ is a time delay relative to the local signal replica, and $\theta_d^i(t)$ is a phase delay relative to the local signal replica, each corresponding to the direct-path (i.e., authentic) signal d. Also, $j = \sqrt{-1}$. The quantity $m^i(t,\tau)$ represents multipath reflections impinging on the receiver's antenna. Multipath can be modeled as a superposition of N_m indirect signals [9]:

$$m^i(t,\tau) = \sum_{n=1}^{N_m} \alpha_n^i(t)R^i(\tau - \tau_n^i(t))e^{j\theta_n^i(t)} \quad (2)$$

Here, N_m multipath components contribute an amplitude-scaled, time-shifted, phase-modified replica of $R^i(\tau)$ where the time-varying amplitude $\alpha_n^i(t)$, time shift $\tau_n^i(t)$, and phase $\theta_n^i(t)$ correspond to multipath component n. For multipath, $\tau_n^i(t) > 0$. The model assumes that reflections from other satellites $l \neq i$ are zero, which is nearly true in practice.

The quantity $s^i(t,\tau)$ represents a spoofing attack on the computed autocorrelation function [5], modeled as:

$$s^i(\lambda,\phi) = \alpha_s^i(t)R^i(\tau - \tau_s^i(t))e^{j\theta_s^i(t)} \times \mathbf{1}_s \quad (3)$$

The indicator function $\mathbf{1}_s$ indicates the presence or absence of spoofing. Note the similarities in the model of multipath in (2) and spoofing in (3); spoofing looks like a single multipath reflection. The quantity $n^i(t,\tau)$ in (1) represents thermal front-end noise, typically modeled as zero-mean complex Gaussian noise with variance σ^2 (i.e., white noise).

When sampled at time $t = kT_s$, the autocorrelation function becomes $\xi_k^i(\tau) = \xi^i(t,\tau)|_{t=kT_s}$; an illustration of this function under a combined multipath and spoofing scenario is shown in Fig. 1.

IV. The Sandwich Measurements

The sandwich defense makes two independent measurements of the incoming signal: a measure of the complex symmetric difference D between an early-late correlator pair, and a measure of the total received in-band power P. To reduce the data rate and noise, each measurement is taken at 10 Hz with a coherent integration time of 100 ms.

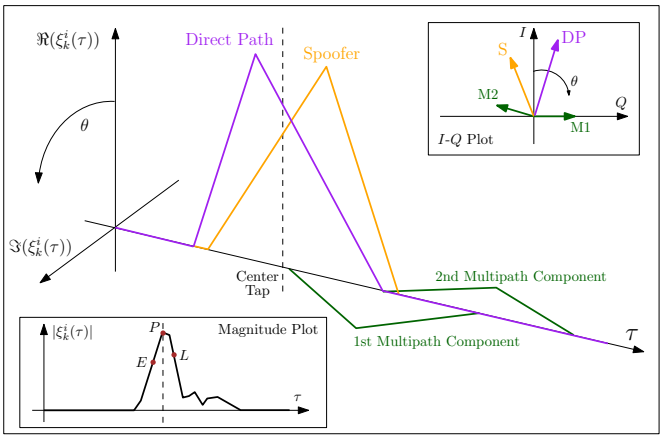

Fig. 1. Figure illustrating the components of the autocorrelation function $\xi_k^i(\tau)$ in a combined multipath and spoofing scenario.

A. Symmetric Difference

For signal i at time $t = kT_s$, the symmetric difference is given by

$$D_k^i(\tau_s) = \xi_k^i(\tau_c - \tau_s) - \xi_k^i(\tau_c + \tau_s) \quad (4)$$

where τ_c is the prompt, or center, tap and τ_s is the symmetric difference tap offset. The symmetric difference measures distortions in ξ_k^i that can be caused by either multipath or spoofing. Under ideal noise-, multipath-, and spoofing-free conditions, ξ_k^i is symmetric and $D_k^i(\tau_s) = 0$ for all τ_s. In practice, $D_k^i(\tau_s)$ is always non-zero, but a large $D_k^i(\tau_s)$ can indicate the presence of a spoofer. The sensitivity of $D_k^i(\tau_s)$ to distortions depends on the choice of τ_s. Narrow correlator spacing has been shown to offer tracking and multipath mitigation benefits [10]; however, rounding of the autocorrelation function due to non-infinite sampling rates limit the narrowness of τ_s. In this paper, $\tau_s = 0.1$ chip, which is as close to the peak of the autocorrelation function as possible while remaining below its rounded peak.

$D_k^i(\tau_s)$ is a powerful spoofing statistic because (a) it is insensitive to the non-linear distortions in the correlation function due to finite precorrelation bandwidth, and (b) it is insensitive to differences in correlation function slope due to peak-flush and peak-adjacent sidelobes that vary with satellite i. A similar but normalized form of the symmetric difference called the delta test was proposed for signal quality monitoring [11], GNSS augmentation systems [12], and spoofing detection [8], [13]. The symmetric difference applied in the sandwich defense remains un-normalized because the noise statistics of $D_k^i(\tau_s)$ under H_0 remain independent of the receiver's carrier-to-noise ratio if left un-normalized.

B. Total In-Band Power

The total in-band power P received by a GNSS receiver has been proposed for radio-frequency interference monitoring [14] and for spoofing detection [7]. The purpose of the power monitor in this defense is to measure the nominal in-band power levels and detect when additional power is present due

to spoofed signals, thereby limiting the power advantage of the spoofer. The power for signal i at time $t = kT_s$ is given by P_k^i.

To measure P_k^i, the power spectral density estimate of the received signal was computed via Welch's overlapped segment averaging estimator with a Hanning window and a discrete Fourier transform length of 4096. For the sandwich defense, P_k^i was measured in a bandwidth of 5 MHz centered at 1575.42 MHz (i.e., the GPS L1 frequency). The choice of a 5 MHz bandwidth instead of the 2 MHz GPS L1 bandwidth is based on the fact that spoofers may generate modulation distortions such as mixing, image, and jamming signals outside of the 2 MHz main lobe of the GPS L1 C/A signal. Because the power measured here was relative and not absolute, P_k^i was normalized so that its mean was zero under a thermal-noise, non-spoofing scenario.

C. Detection Statistic

$D_k^i(\tau_s)$ and P_k^i can be combined into a single detection statistic under the generalized notion of a probabilistic anti-spoofing framework [15]:

$$\boldsymbol{z}_k^i = [D_k^i(\tau_s), P_k^i]^T \tag{5}$$

Under this framework, $\boldsymbol{z}_k^i$ is tested against three hypotheses for the receiver operating regime: H_0, thermal noise (non-multipath); H_1, multipath; and H_2, spoofing and/or jamming. The success of the approach hinges on an accurate characterization of the probability distribution of the measurements under the three hypotheses, denoted as $p_{\boldsymbol{z}|H_j}(\boldsymbol{\psi}|H_j)$ for $j = 0, 1, 2$. The probability of false alarm P_F defined for this defense is when either H_0 or H_1 is detected as H_2:

$$P_F \triangleq \frac{1}{2}\int_R \left(p_{\boldsymbol{z}|H_0}(\boldsymbol{\psi}|H_0) + p_{\boldsymbol{z}|H_1}(\boldsymbol{\psi}|H_1)\right) d\boldsymbol{\psi} \tag{6}$$

Here, R is the region corresponding where H_j and H_2 share probability mass and where $p_{\boldsymbol{z}|H_j}(\boldsymbol{\psi}|H_j) < \lambda$ for $j = 0, 1$ and a particular choice of λ.

V. Operational Sandwich Defense Evaluation

To evaluate the sandwich defense, this paper leverages the Texas Spoofing Test Battery (TEXBAT) [6], which offers data sets containing clean and spoofed radio-frequency recordings for evaluating the operational performance of anti-spoofing techniques. TEXBAT serves as an expedient way to generate empirically $p_{\boldsymbol{z}|H_j}(\boldsymbol{\psi}|H_j)$ for $j = 0, 2$ for static and dynamic receiver platforms. For brevity, this paper only presents results for static TEXBAT scenarios, but the proposed technique is extensible to mobile receivers.

A. Empirical Density Functions

Because of the large amount of data offered in TEXBAT, a binning strategy is applied to segment the probability density space of $\boldsymbol{z}$. The range of D in both the real and imaginary axis was $\pm 10 \times 10^5$ with a bin size of 8×10^4. The range of P was ± 10 dB with a bin size of 0.5 dB. This is a total of 25000 probability bins per hypothesis. A three-dimensional histogram corresponding to all measurements $\boldsymbol{z}_k^i$ under a given hypothesis is created (i.e, there is one empirical density per hypothesis). To form the probability distribution, the number of measurements falling into a single probability bin is divided by the total number of measurements. The result is a three-dimensional matrix of probabilities of a particular bin.

B. Characterizing H_0: Thermal Noise

Characterizing $p_{\boldsymbol{z}|H_0}(\boldsymbol{\psi}|H_0)$ is well-suited for an analytic solution assuming the thermal noise $n(t, \tau)$ takes on a Gaussian distribution. Here, D is the difference between two Gaussian random variables, which is also Gaussian. Due to interference not well modeled in Eq. 1, D is not always Gaussian. Over 1 hr of clean, multipath-free data was used to form the data shown in the top two plots of Fig. 2. Here, the clean data fits into a relatively small area with a probability contour of $p \geq 0.0001$ for P = 0 dB.

C. Characterizing H_1: Multipath

Characterizing $p_{\boldsymbol{z}|H_1}(\boldsymbol{\psi}|H_1)$ is suited to a combined analytic and empirical approach. Analytic multipath models exist [16] but real-world recordings offer a richer characterization of $p_{\boldsymbol{z}|H_1}(\boldsymbol{\psi}|H_1)$ than models alone. Multipath-laden recordings of more than 3 hr were taken to generate the data shown in the bottom two plots of Fig. 2. These recordings were taken in the presence of large buildings that served to generate short- and long-delay multipath. There is over a 60% overlap of shared probability space between $p_{\boldsymbol{z}|H_0}(\boldsymbol{\psi}|H_0)$ and $p_{\boldsymbol{z}|H_1}(\boldsymbol{\psi}|H_1)$. A fallout benefit of the multi-hypothesis test is the ability to identify strong multipath environments—if the data are not H_0 or H_2, then H_1 is a strong possibility.

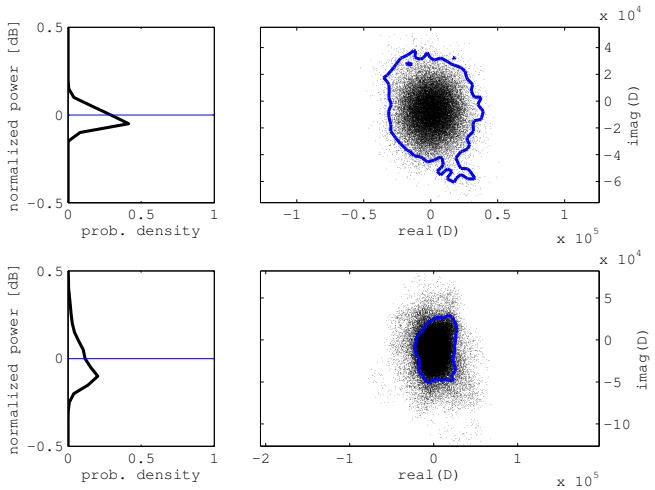

Fig. 2. The normalized power probability density function (left) and a scatter plot of D (right) for a clean scenario (top) and a multipath scenario (bottom). The contour line contains the probability space where $p \geq 0.0001$ at the power level indicated by the horizontal line in the power density plot.

D. Characterizing H_2: Spoofing

Characterizing $p_{\boldsymbol{z}|H_2}(\boldsymbol{\psi}|H_2)$ is only possible empirically and partially. Too many spoofing attack vectors exist, and only

a subset can be considered. TEXBAT spoofing data provided over 2 hr of spoofing recordings that were combined to form the data shown in Fig. 3. Here the top two plots show the features of a static overpowered time push spoofing attack with a power advantage of 10 dB, while the bottom plots show the results for a static matched-power position push spoofing attack with a power advantage of 1.3 dB.

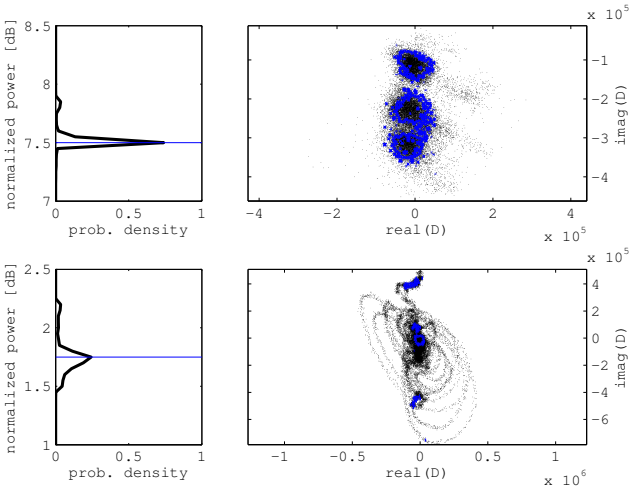

Fig. 3. The normalized power probability density function (left) and a scatter plot of D (right) for the static overpowered time push (top) and the static matched-power position push (bottom). The contour line contains the probability space where $p \geq 0.0001$ at the power level indicated by the horizontal line in the power density plot.

E. Sandwich Defense Efficacy

To test the sandwich defense efficacy, a static spoofing attack scenario not included in the formation of $p_{\boldsymbol{z}|H_2}(\boldsymbol{\psi}|H_2)$ was tested against the defense. Detection statistics were generated for the new spoofing attack recording, and one of the hypothesis was selected based on $p_{\boldsymbol{z}|H_j}(\boldsymbol{\psi}|H_j)$ for $j = 0, 1, 2$. Fig. 4 shows the selected hypothesis. Note that the spoofing attack started at 112 s into the test, and the first 20 s of data were removed because the receiver was still locking onto the signal. The probability of false alarm of this test based on the generated empirical densities was $P_F = 0.009$ for $\lambda = 0.001$.

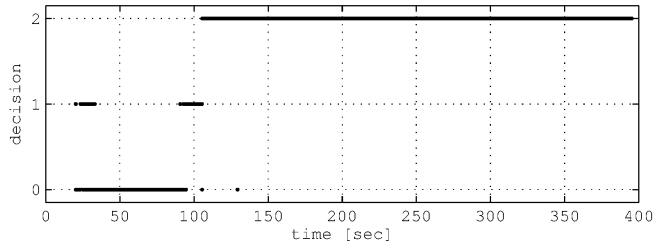

Fig. 4. Plot showing the selected hypothesis of the defense when tested against a recording of a spoofing attack that begins at 112 s.

VI. Conclusion

This paper contributes a GNSS spoofing "sandwich defense" that combines a symmetric difference autocorrelation distortion monitor and a total in-band power monitor to detect spoofing attacks. The defense was built up from and evaluated against the Texas Spoofing Test Battery, which is a data set that includes recordings of sophisticated spoofing attacks. Results presented herein demonstrate that (1) multipath and spoofing can be distinguished empirically based on the combined and independent measurements of the symmetric difference and total in-band power and that (2) the sandwich defense proved effective against a sophisticated spoofing attack while maintaining a low probability of false alarm.

Acknowledgments

K. Wesson received Government support via DoD, Air Force Office of Scientific Research, National Defense Science and Engineering Graduate Fellowship, 32 CFR §168a.

References

[1] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon, and P. M. Kintner, Jr., "Assessing the spoofing threat: development of a portable GPS civilian spoofer," in *Proc. ION GNSS*, 2008.

[2] D. P. Shepard, T. E. Humphreys, and A. A. Fansler, "Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks," *Int. J. Critical Infrastructure Protection*, vol. 5, no. 3-4, pp. 146–153, 2012.

[3] K. D. Wesson, M. Rothlisberger, and T. E. Humphreys, "Practical cryptographic civil GPS signal authentication," *NAVIGATION*, vol. 59, no. 3, pp. 177–193, 2012.

[4] T. E. Humphreys, "Detection strategy for cryptographic GNSS anti-spoofing," *IEEE Trans. Aero. Elec. Sys.*, vol. 49, no. 2, pp. 1073–1090, 2013.

[5] 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," in *Proc. ION GNSS*, 2011.

[6] T. E. Humphreys, J. A. Bhatti, D. P. Shepard, and K. D. Wesson, "The Texas spoofing test battery: Toward a standard for evaluating GNSS signal authentication techniques," in *Proc. ION GNSS*, 2012, data set available online at http://radionavlab.ae.utexas.edu/TEXBAT.

[7] D. M. Akos, "Who's afraid of the spoofer? GPS/GNSS spoofing detection via automatic gain control (AGC)," *NAVIGATION*, vol. 59, no. 4, pp. 281–290, 2012.

[8] B. M. Ledvina, W. J. Bencze, B. Galusha, and I. Miller, "An in-line anti-spoofing module for legacy civil GPS receivers," in *Proc. ION Tech. Meetings*, 2010.

[9] R. D. J. van Nee, "Spread-spectrum code and carrier synchronization errors caused by multipath and interference," *IEEE Trans. Aero. Elec. Sys.*, vol. 29, no. 4, pp. 1359–1365, 1993.

[10] A. J. Van Dierendonck, P. Fenton, and T. Ford, "Theory and performance of narrow correlator spacing in a GPS receiver," *NAVIGATION*, vol. 39, no. 3, pp. 265–283, 1992.

[11] R. E. Phelts, *Multicorrelator Techniques for Robust Mitigation of Threats to GPS Signal Quality*. Ph.D. dissertation, Stanford University, 2001.

[12] A. M. Mitelman, R. E. Phelts, D. M. Akos, S. P. Pullen, and P. K. Enge, "A real-time signal quality monitor for GPS augmentation systems," in *Proc. ION GPS*, 2000.

[13] M. Irsigler and G. W. Hein, "Development of a real-time multipath monitor based on multi-correlator observations," in *Proc. ION Tech. Meetings*, 2005.

[14] P. W. Ward, "GPS receiver RF interference monitoring, mitigation, and analysis techniques," *NAVIGATION*, vol. 41, no. 4, pp. 367–391, 1994.

[15] K. D. Wesson, B. L. Evans, and T. E. Humphreys, "A probabilistic framework for Global Navigation Satellite System signal timing assurance," in *Proc. Asilomar Conf. Sig. Sys. Comp.*, 2013, submitted.

[16] G. L. Turin, F. D. Clapp, T. L. Johnston, S. B. Fine, and D. Lavry, "A statistical model of urban multipath propagation," *IEEE Trans. Veh. Tech.*, vol. VT-21, no. 1, Feb. 1972.