An Evaluation of the Vestigial Signal Defense for Civil GPS Anti-Spoofing

Kyle D. Wesson, Daniel P. Shepard, Jahshan A. Bhatti, and Todd E. Humphreys
The University of Texas at Austin

BIOGRAPHIES

Kyle D. Wesson is pursuing a Ph.D. in the Department of Electrical and Computer Engineering at The University of Texas at Austin. He received his B.S. in Electrical and Computer Engineering from Cornell University. He is a member of the UT Radionavigation Laboratory and the Wireless Networking and Communications Group. His research interests include GNSS security and interference mitigation.

Daniel P. Shepard is pursing a Ph.D. in the Department of Aerospace Engineering and Engineering Mechanics at The University of Texas at Austin, where he also received his B.S. He is a member of the UT Radionavigation Laboratory. His research interests are in GNSS security, estimation and filtering, and guidance, navigation, and control.

Jahshan A. Bhatti is pursuing a Ph.D. in the Department of Aerospace Engineering and Engineering Mechanics at The University of Texas at Austin, where he also received his B.S. and M.S. He is a member of the UT Radionavigation Laboratory. His research interests are in the development of small satellites, software-defined radio applications, space weather, and GNSS security and integrity.

Todd E. Humphreys is an assistant professor in the department of Aerospace Engineering and Engineering Mechanics at the University of Texas at Austin and Director of the UT Radionavigation Laboratory. He received a B.S. and M.S. in Electrical and Computer Engineering from Utah State University and a Ph.D. in Aerospace Engineering from Cornell University. His research interests are in estimation and filtering, GNSS technology, GNSS-based study of the ionosphere and neutral atmosphere, and GNSS security and integrity.

ABSTRACT

A receiver-autonomous non-cryptographic civil GPS anti-spoofing technique called the vestigial signal defense (VSD) is defined and evaluated. This technique monitors distortions in the complex correlation domain to detect spoofing attacks. Multipath and spoofing interference models are developed to illustrate the challenge of distinguishing the two phenomena in the VSD. A campaign to collect spoofing and multipath data is described, which specific candidate VSD techniques can be tested against. Test results indicate that the presence of multipath complicated the setting of an appropriate spoofing detection threshold.

I. INTRODUCTION

Civil GPS anti-spoofing research seeks to equip civil GPS receivers with tools to detect and mitigate spoofing attacks that if successful could cause significant economic damage or damage to critical national infrastructure. The goal of a spoofing attack is to deceive a victim GPS receiver into tracking counterfeit GPS signals, thereby causing it to report a spoofer-manipulated navigation or timing solution. Since the 2001 Volpe report [1], which highlighted the threat of spoofing and recommended further development of anti-spoofing techniques, researchers have made much progress toward this goal [2–12].

Anti-spoofing techniques can be categorized into two groups: cryptographic and non-cryptographic. Although no anti-spoofing technique is completely impervious to a sophisticated spoofing attack, cryptographic anti-spoofing techniques offer significant protection because they allow a receiver to differentiate authentic GPS signals from counterfeit signals with high likelihood. Cryptographic strategies rely on the unpredictability of so-called security codes that modulate the GPS signal [12]. The unpredictable codes force a spoofer who wishes to carry off a successful attack to (1) estimate the unpredictable chips on-the-fly (i.e., a security-code estimation and replay attack) or (2) record and playback authentic GPS spectrum (i.e., a meaconing attack) [11].

Three flavors of civil GPS cryptographic anti-spoofing have come under recent consideration. The first option, based on spread spectrum security codes (SSSC), is to make parts of civil GPS spreading codes periodically unpredictable [2]. Another strategy, called navigation message authentication (NMA), embeds public key digital signatures into the GPS civil navigation (CNAV) message [2, 11]. Although they both can be paired with the hypothesis test in Ref. [12] to offer civil GPS signal authentication, SSSC and NMA require modification to the GPS interface spec-

**Preprint of the 2011 ION GNSS Conference
Portland, OR, September 21–23, 2011**

ification (IS). Changes to the GPS IS are difficult to make due to the static nature of the GPS signal definitions [13]. The third approach correlates the unknown encrypted military P(Y) code between two civil GPS receivers to exploit carrier-phase and code-phase relationships [14]. This method avoids any modifications to the GPS IS but requires receivers to communicate with one another over a secure network.

Non-cryptographic techniques are enticing because they can be made receiver-autonomous, requiring neither security-enhanced civil GPS signals nor a network connection. One non-cryptographic method is the multi-antenna defense, which monitors differential carrier phase to detect GPS signals that emanate from a single point source as opposed to multiple GPS satellites [9]. Unless a spoofer can attack with multiple coordinated spoofers, all spoofed signals will originate from a single direction. Thus, the multi-antenna defense is effective against all but the most sophisticated spoofing attacks involving coordinated spoofers. Unfortunately, the multi-antenna defense needs two or more antennas spaced several centimeters apart, which is not feasible for many applications. A similar drawback exists for anti-spoofing techniques that that make use of inertial measurement units or other hardware: the additional hardware adds size, weight, or cost and would be prohibitive for many applications.

A promising non-cryptographic anti-spoofing technique is the vestigial signal defense (VSD), which is studied in this paper. The VSD is a stand-alone software-defined defense, which means that it has a low implementation cost and does not increase receiver size or weight. The VSD offers the promise of powerful, low-cost, receiver-autonomous spoofing detection.

The paper is organized as follows. First, it defines and sets goals for the VSD. Second, it presents and discusses models for spoofing and multipath signals in the complex correlation domain. Third, it describes previously-proposed VSD-type detection metrics and, fourth, evaluates these metrics with real experimental data. Finally, it proposes future directions to make a more effective VSD. The following sections are organized around these topics, followed by conclusions.

II. VESTIGIAL SIGNAL DEFENSE OVERVIEW

The VSD relies on the difficulty of suppressing the true GPS signal during a spoofing attack. Unless the spoofer generates a phase-aligned nulling signal at the phase center of the GPS receiver's antenna, a vestige of the authentic signal remains and manifests as a distortion of the complex correlation function. To generate a nulling signal, a spoofer requires (1) 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 (2) 100-picosecond-accurate knowledge of its processing and transmission delay. Without knowledge of these two quantities and accurate compensation, a spoofing attack will leave behind a vestige of the authentic GPS signal.

The difficulty of suppressing the authentic GPS signal is an opportunity for spoofing detection: during a spoofing attack, an admixture of the authentic and spoofing signal will likely be present, which manifests as a detectable corruption of the complex correlation function. The VSD, therefore, is defined as a technique for monitoring distortion in the complex correlation domain to determine if a spoofing attack is underway.

A significant issue for VSD to overcome is that the interaction of the authentic and spoofed GPS signals is similar to the interaction of multipath and direct-path GPS signals. In fact, the following section reveals that the models for multipath and spoofing signals are nearly identical. Differentiating the two types of interference is a significant challenge for any spoofing defense based on monitoring the complex correlation domain.

III. INTERFERENCE MODELS

The study of multipath effects and mitigation techniques on communication and navigation systems, specifically code division multiple access systems, provides a natural way to model GPS interference [15–18]. Multipath is often modeled in the complex correlation domain [19, 20]. This domain is also well suited to model spoofing.

Suppose the total received signal at the receiver is correlated to produce a complex correlation function $x(t, \tau)$ at time t and lag-offset τ:

$$x(t, \tau) = x_d(t, \tau) + x_m(t, \tau) + x_s(t, \tau) + n(t, \tau). \quad (1)$$

Here, $x(t, \tau)$ is the superposition of four complex correlation components: a direct-path GPS $x_d(t, \tau)$, a multipath component $x_m(t, \tau)$, a spoofing component $x_s(t, \tau)$, and additive white Gaussian noise $n(t, \tau)$. Note that the direct-path component is the correlation function corresponding to the authentic GPS signal. Typically, it is referred to as the direct-path signal when only multipath is involved and the authentic signal when only spoofing is involved. In this paper, direct-path and authentic are synonymous.

A complex correlation function $x(t, \tau)$ of time t and lag-

offset τ is produced when the receiver correlates its copy of the incoming pseudorandom spreading code with the incoming broadcast signal. Typically, the delay-locked loop operates on this function with only three correlation taps (i.e., early, prompt, and late taps) for signal tracking although some receivers, such as the one described in Ref. [21], produce many more. Additional taps offer more insight into distortions in the complex correlation domain than the early, prompt and late taps can alone. The complex correlation domain can be thought of as the continuous-time complex signal produced when a continuum of tap offsets are considered.

The direct-path correlation component $x_d(t,\tau)$ can be modeled as

$$x_d(t,\tau) = \alpha_d(t)R(\tau - \tau_d(t))e^{j\theta_d(t)}. \quad (2)$$

This shows that $x_d(t,\tau)$ is a time-shifted, amplitude-scaled, phase-modified replica of the auto-correlation function $R(\tau)$ where $0 \leq \alpha_d(t) \leq 1$ is the scaling factor, $\tau_d(t)$ is the delay in seconds, and $\theta_d(t)$ is the phase in radians, all of which are time-varying. If the receiver is tracking a direct-path signal only, then the delay-lock loop tries to set $\tau_d(t) = 0$ and the phase-locked loop tries to set $\theta_d(t) = 0$. It is convenient to model $\alpha_d(t) = 1$ in this case.

The auto-correlation function $R(\tau)$ is modeled as

$$R(\tau) \approx \begin{cases} 1 - |\tau|/T_c & \text{for } |\tau| < T_c \\ 0 & \text{otherwise.} \end{cases} \quad (3)$$

Here, $T_c \approx 1$ μs, which is the approximate chipping rate of the civil GPS L1 C/A signal. In practice, $R(\tau)$ varies slightly for each satellite's pseudorandom spreading code. These variations do not impact the model, and therefore Eq. 3 is a reasonable approximation.

Multipath in the correlation domain $x_m(t,\tau)$ can be modeled as a superposition of some number N of delayed direct-path signals [20]:

$$x_m(t,\tau) = \sum_{k=1}^{N} \alpha_{m,k}(t)R(\tau - \tau_{m,k}(t))e^{j\theta_{m,k}(t)}. \quad (4)$$

Here, the N multipath components each contribute some time-shifted, amplitude-scaled, phase-modified replica of $R(\tau)$ where the time-varying $\alpha_{m,k}(t)$, $\tau_{m,k}(t)$, and $\theta_{m,k}(t)$ are indexed by multipath component k. If no multipath is present, then $N = 0$. Because multipath signals are delayed copies of the direct-path signal, $0 < \tau_{m,k}(t)$. Also, the multipath signal is typically attenuated with respect to the direct-path signal such that $0 < \alpha_{m,k}(t) < \alpha_d(t)$, although in some cases, the direct-path signal can be more severely attenuated (e.g., by an overhanging roof) than a fortuitously-reflected multipath signal.

The model for a spoofing signal $x_s(t,\tau)$ in the complex correlation domain is

$$x_s(t,\tau) = (\alpha_s(t)R(\tau - \tau_s(t))e^{j\theta_s(t)}) \times \mathbf{1}_{\text{spoofing}}. \quad (5)$$

Again, the spoofing signal is a time-shifted, amplitude-scaled, phase-modified replica of $R(\tau)$ with time-varying $\alpha_s(t)$, $\tau_s(t)$, and $\theta_s(t)$. This model makes intuitive sense because if a spoofer is trying to deceive the victim receiver with a counterfeit signal that is a near-exact copy of the GPS signal, then $x_s(t,\tau)$ should be approximately $x_d(t,\tau)$. The only significant difference in the model for $x_s(t,\tau)$ is the indicator function $\mathbf{1}_{\text{spoofing}}$. It is reasonable to think a receiver is either being spoofed or is not; the indicator models this logic. The case of multiple spoofers is not considered.

Fig. 1 illustrates a noise-free example scenario that considers a spoofing attack underway in the presence of multipath. Although the figure does not illustrate the most sophisticated spoofing attack or the most challenging multipath environment, it depicts a plausible example. The spoofer is transmitting a counterfeit signal $x_s(t,\tau)$ with a reduced amplitude and slight delay with respect to $x_d(t,\tau)$. Aligning the carrier phase of the spoofed signal to the authentic signal is difficult for the spoofer [8]. Accordingly, the figure illustrates a case in which $\theta_s(t) \neq \theta_d(t)$; with the actual phasing shown in the upper-right I-Q plot. Notice that two multipath components are present, but their amplitudes are significantly reduced relative to $\alpha_d(t)$ and their delays are large. In this illustration, the multipath phase is nearly perpendicular to the phase of $x_d(t,\tau)$, but this need not be the case. As the satellite moves along its orbit, the multipath range changes with respect to the direct-path range, causing $\theta_{m,k}(t)$ to rotate. In the lower left, the magnitude plot reveals $|x(t,\tau)|$ is no longer the ideal triangular auto-correlation function $R(\tau)$. The three dots in the magnitude plot denote the early, prompt, and late correlator taps that a typical receiver might use for signal tracking. With only three taps, a GPS receiver could not adequately resolve the distortions in the complex correlation domain illustrated in this figure. Many more taps will be necessary for a strong VSD.

Distortions in the complex correlation domain can also be viewed in terms of the in-phase $I(t,\tau) = \Re[x(t,\tau)]$ and quadrature $Q(t,\tau) = \Im[x(t,\tau)]$ components of $x(t,\tau)$. In a scenario free of spoofing, multipath, and noise, $I(t,\tau) = R(\tau)$ and $Q(t,\tau) = 0$, but when spoofing, multipath, or noise are considered, $I(t,\tau)$ and $Q(t,\tau)$ distort. In Fig. 2, the same example scenario of Fig. 1 is illustrated except that the multipath components have been removed,

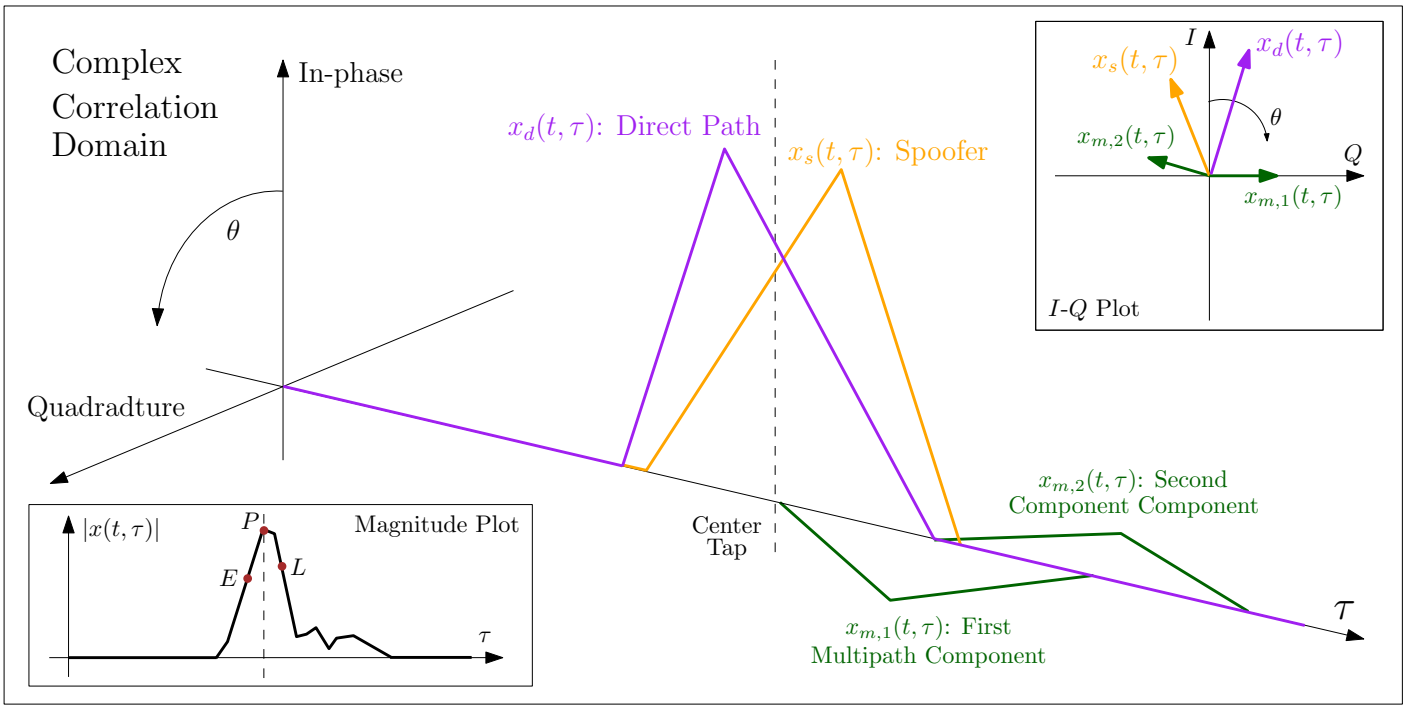

Fig. 1. Figure illustrating the complex correlation domain view of a spoofing attack and the corresponding I-Q and magnitude plots.

leaving only the direct and spoofing components. Here, $I(t,\tau)$ is a distorted version of $R(\tau)$ and $Q(t,\tau) \neq 0$. The delay-dependent distortion is due to delay-dependent phase-distortions in $x(t,\tau)$ caused by a non-carrier-phase-matched spoofing signal. For example at tap $\pm T_c/2$, the addition of $x_s(t,\tau)$ contributes to form a non-zero $Q(t,\tau)$, but because the spoofed signal is not carrier-phase aligned, distortions in $Q(t,\tau)$ are not constant [i.e., they vary in their deviation with $R(\tau)$]. That is, for $\theta_s(t) \neq \theta_d(t)$ and $\tau_s(t) \neq \tau_d(t)$, the triangular-shaped correlation function $R(\tau)$ enhances or attenuates the error in the quadrature component as a function of $\tau_s(t)$. Distortions in $I(t,\tau)$ occur for the same reason.

While Fig. 2 illustrated a spoofing attack, it is not difficult conceptually to consider a scenario where $x_s(t,\tau)$ is replaced with a strong multipath component $x_{m,1}(t,\tau)$. In this case, the same distortion would be present in $I(t,\tau)$ and $Q(t,\tau)$. Thus, the type of distortion shown in Fig. 2 is not a unique signature of spoofing.

IV. PREVIOUSLY-PROPOSED VSD-TYPE SPOOFING DETECTION METRICS

Several strategies have been proposed to detect spoofing based on distortions in the complex correlation domain [22,23]. These strategies apply prior research in the areas of signal quality monitoring and multipath detection techniques to the civil GPS spoofing problem [24–26]. Since the model for spoofing is nearly identical to the model for multipath, applying multipath detection techniques is a sensible suggestion for spoofing detection. Signal quality and multipath monitoring techniques seek to determine if and when the correlation function becomes distorted due to satellite failures or severe multipath, respectively. Generally, monitoring the complex correlation domain for distortion means computing a metric based on multiple samples of the complex correlation function. Numerous metrics exist and a summary of potential metrics is provided here.

A. Delta Metric

The delta metric $\Delta_\tau(t)$ is defined as [22,25]

$$\Delta_\tau(t) = \frac{I_{E,\tau}(t) - I_{L,\tau}(t)}{2I_P(t)}. \tag{6}$$

Here, $I_{E,\tau}(t)$ and $I_{L,\tau}(t)$ refer to an early and late tap spaced τ seconds ahead and behind the prompt tap $I_P(t)$ on the in-phase component at time t, respectively. The delta test is symmetric, so under multipath- and spoofed-free conditions $\mathbb{E}[\Delta_\tau(t)] = 0$. Reference [22] proposes the delta metric as a possible spoofing detection metric.

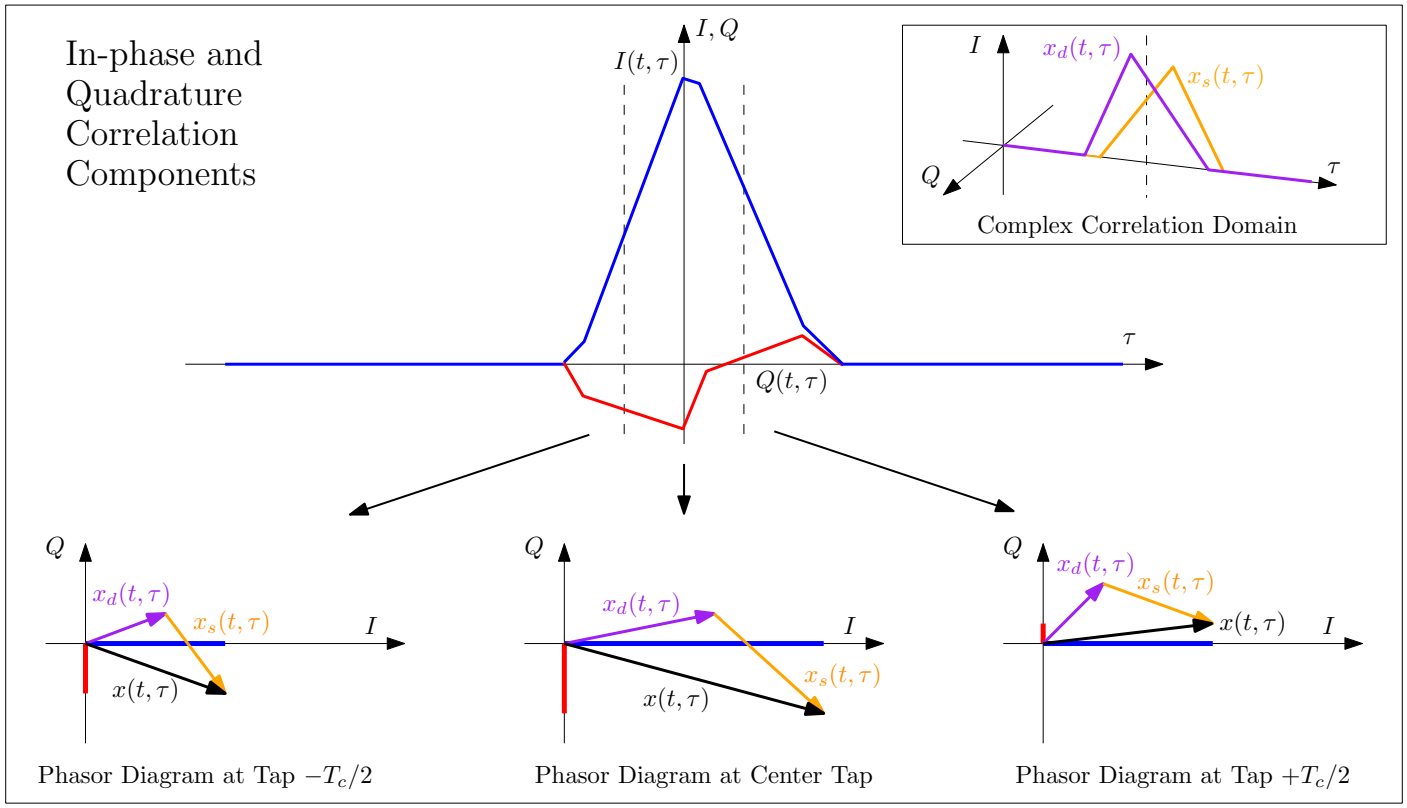

Fig. 2. Figure illustrating the distortions that can be present in the in-phase and quadrature components of $x(t,\tau)$ during a spoofing attack.

B. Ratio Metric

The ratio metric $RT_\tau(t)$ is defined as [22, 23, 25, 27]

$$RT_\tau(t) = \frac{I_{E,\tau}(t) + I_{L,\tau}(t)}{2I_P(t)}. \tag{7}$$

The ratio test is quite similar to the delta test, but its numerator is an addition of, not a difference of, the early and late in-phase taps. Assuming uncorrelated correlator taps, then under multipath- and spoofing-free conditions $\mathbb{E}[RT_\tau(t)] = 1 - \tau/T_c$ for $0 < \tau \leq T_c$ and otherwise zero. References [22, 27] and [23] propose the ratio metric as a possible spoofing detection metric.

C. Early-Late Phase Metric

The early-late phase metric $ELP_\tau(t)$ is a recently-proposed monitoring technique defined as [28]

$$ELP_\tau(t) = \tan^{-1}\left(\frac{Q_{L,\tau}(t)}{I_{L,\tau}(t)} - \frac{Q_{E,\tau}(t)}{I_{E,\tau}(t)}\right). \tag{8}$$

Here, $Q_{E,\tau}(t)$ and $Q_{L,\tau}(t)$ refer to an early and late tap spaced τ seconds ahead and behind the prompt tap on the quadrature component at time t, respectively. $I_{\cdot,\tau}(t)$ is defined in the same way as defined in Eq. 6.

$ELP_\tau(t)$ computes the phase difference between the early and late correlator taps. This metric has been proposed for multipath detection for L1 and L2C signals [28]. It is one of the only proposed signal quality metric to incorporate the quadrature component $Q(t,\tau)$ in calculations.

D. Magnitude Difference Metric

The magnitude difference metric $MD_\tau(t)$ is another plausible VSD-type spoofing detection metric:

$$MD_\tau(t) = \frac{|x_{E,\tau}(t)| - |x_{L,\tau}(t)|}{|x_P(t)|}. \tag{9}$$

Here, $|\cdot|$ denotes the magnitude of the correlation function for early $x_{E,\tau}(t)$, late $x_{L,\tau}(t)$, and prompt $x_P(t)$ values. The metric offers symmetry like $\Delta_\tau(t)$ but operates with the tap magnitude instead.

E. Other Metrics

Other metrics described in the literature usually take the form of simple ratios (e.g., $I_{E,\tau}/I_{L,\tau}$) or double-delta-differences [e.g., $\Delta_{\tau_1}(t) - \Delta_{\tau_2}(t)$] [26]. Neither of these forms appear to be applied as frequently in multipath monitoring applications. This observation does not imply, however, that they would not be useful for VSD.

V. EVALUATION OF PROPOSED VSD-TYPE SPOOFING DETECTION METRICS

The multipath and spoofing data collection campaign and the data collection tools described in this section provided an experimental dataset with which to evaluate potential VSD techniques. This section will first describe the data collection tools and data recording campaign. It will then provide experimental results demonstrating the performance of the ratio metric in Eq. 7, which was proposed for spoofing detection in Refs. [22, 23, 27]. For any of the proposed metrics described in Sec. IV to be considered effective, they must (1) reliably detect spoofing and (2) reliably differentiate spoofing from multipath. Most of the metrics in Sec. IV meet the first component of effectiveness but have difficulty achieving the second.

A. Data Collection Tools

A.1 National Instruments RFSA/RFSG Equipment

A National Instruments (NI) radio frequency signal analyzer (RFSA) is a tool that can downconvert signals centered at GPS L1 frequency to baseband and record 16-bit complex baseband samples. In the data collection campaign described subsequently, it digitized a 30-MHz real-time bandwidth spectral interval centered at the GPS L1 frequency. The recorded data can be later up-mixed and replayed using a NI radio frequency signal generator (RFSG), which converts complex baseband samples to an analog signal.

A.2 Civil GPS Spoofer

The civil GPS spoofer used for the data collection, shown in Fig. 3, is an advanced version of the spoofer reported in [8]. It is the only spoofer reported in open literature to date that is capable of precisely aligning the spreading code, data bits, and frequency of its counterfeit signals with those of the authentic GPS signals. Such alignment capability allows the spoofer to carry out a sophisticated spoofing attack in which no obvious clues remain or alerts are raised to suggest that an attack is underway [29].

A.3 DFE Receiver

The digitizing front-end (DFE) receiver, shown in Fig. 4, which is based on the GNSS complex ambiguity function (GCAF) engine, is an exquisite instrument for monitoring multipath and testing multipath detection and mitigation schemes [21, 30]. The DFE provides in-phase and quadrature (IQ) accumulations at 1 ms intervals for 512 correlator offsets spanning a range of ± 6.25 μs from the center tap.

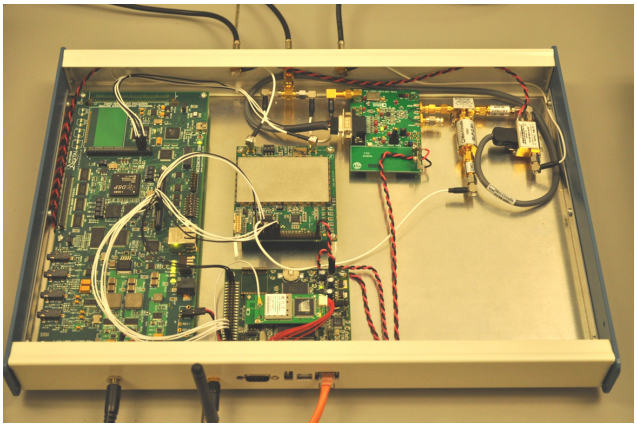

Fig. 3. Picture of the civil GPS spoofer used in the VSD evaluation experiments.

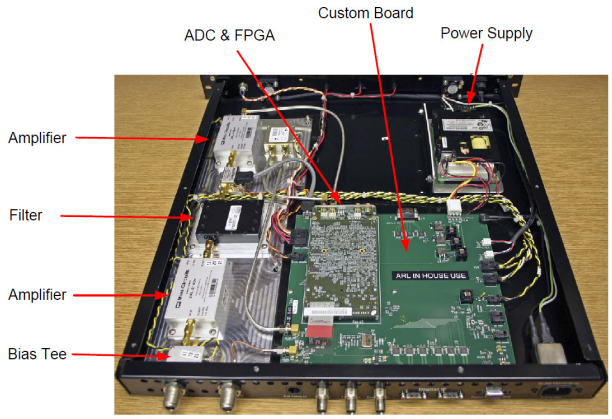

Fig. 4. Picture of the digitizing front-end receiver (figure adapted from Ref. [30] with permission).

B. Multipath Wardriving Campaign

To collect real-life dynamic platform dense urban multipath data, a so-called wardriving effort was performed in downtown Austin, Texas. The NI equipment along with the necessary computers, storage drives, and antennas were loaded into a pickup truck so that GPS spectrum could be recorded on a dynamic platform in a dense-urban environment. A full day of recording yielded more than 1 TB of spectral measurements at approximately 30 MHz bandwidth centered at the GPS L1 frequency. Manifestation of the severe multipath environment encountered during the campaign is seen in the crooked trajectory reported by a GPS receiver that operated on the replayed data as shown Fig. 5. Despite what is indicated by this trajectory, at no point during the test did the truck actually depart from the roadway.

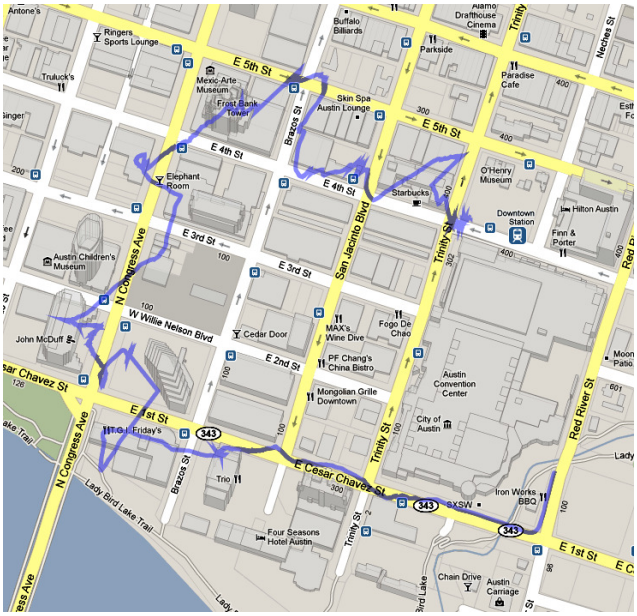

Fig. 5. Map showing a trace of the computed GPS navigation solution for a GPS receiver on a dynamic platform in a challenging dense-urban multipath environment.

C. Data Processing Setup

The wardriving data set was processed in The University of Texas Radionavigation Laboratory with the DFE. For the multipath tests, the wardriving data were replayed through the NI RFSG. This reproduced signal was input directly into the DFE. For the spoofing tests, GPS signals were received from an antenna on the roof of the W. R. Woolrich Laboratories Building at the University of Texas at Austin and fed into the spoofer via coaxial cable. These signals were tracked by the spoofer, which produced a set of corresponding spoofed signals. The spoofed signals were then summed with the authentic signals from the roof, and the combination of signals was fed via coaxial cable into the DFE. The output of both tests were time histories of 512 IQ taps of the complex correlation function at 1000 Hz.

D. Experimental Results

While the models in Sec. III suggest that spoofing and multipath have similar effects, models can be incorrect or misleading. It was therefore important to validate the models by locating within the experimental data set a multipath signal that distorted the complex correlation domain just like a spoofing attack would.

Examine the four plots in Table I. Here the top two figures show the in-phase and quadrature correlation components as was previously illustrated in Fig. 2. The figure on the left (Fig. 6) is a snapshot of the correlation function taken at the beginning of a spoofing attack while the figure on the right (Fig. 7) is a snapshot of a multipath reflection in the dense-urban environment. The bottom row of figures (Figs. 8 and 9) corresponds to the magnitude difference $MD_\tau(t)$ from Eq. 9 computed for all possible τ. The plots show that the complex correlation distortion induced by a spoofing attack can indeed look similar to the distortion caused by multipath. This observation suggests that the metrics of Sec. IV will be sensitive to both multipath and spoofing and may be unable to differentiate the two.

The figures in Table II further illustrate this shortcoming. The table shows six plots of the ratio metric $RT_\tau(t)$. The figures in row A show results for a test involving non-spoofed stationary receiver in a benign multipath environment. Fig. 10 plots $RT_\tau(t)$ for all τ while Fig. 11 examines $RT_{\tau\approx 1/2\mu s}(t)$ and plots horizontal bars at $\mu \pm 5\sigma$ where μ and σ are the empirically determined mean and standard deviation for the test, respectively. Note that $RT_\tau(t)$ stays within the error bars throughout the test.

Now consider the figures in row B, which correspond to a spoofing attack scenario on a stationary receiver. Figure 12, which plots the ratio test for all τ, indicates complex correlation distortion occurs even at taps not on the central peak (i.e., $\tau > 40$). Fig. 13 reveals that for $\tau \approx 1/2$ μs, $RT_\tau(t)$ exceeds the upper and lower 5σ delineation several times.

The figures in row C, which correspond to a non-spoofed receiver on a dynamic platform in a dense-urban environment, reveal the difficulty that the ratio metric has differentiating spoofing from multipath. Figure 14 indicates a potential deviation that begins at approximately 340 seconds. The distortion is also shown in Figure 15, which indicates that the recorded multipath exceeds the lower 5σ threshold for several seconds.

E. Discussion

As the experimental data set confirmed, the ratio test is not well suited to differentiate complex correlation distortion caused by multipath from the distortions caused by spoofing. Because none of the metrics in Sec. IV were developed with this issue in mind, they are all likely to suffer from this problem to varying degrees. Future development of VSD will need to overcome difficulty if VSD is to become an effective anti-spoofing technique. In fact, this is such a challenge that the goal of VSD should be modest: it can only attempt to reduce the degrees-of-freedom available to a spoofer, forcing the spoofer to mimic multipath to avoid detection. In other words, VSD seeks to "corner in" the spoofer and reduce the space of its possible attack

TABLE I

A TABLE OF FOUR PLOTS SHOWING THE COMPLEX CORRELATION FUNCTION AND THE MAGNITUDE DIFFERENCE METRIC $MD_\tau(t)$ FOR A SPOOFING TEST (LEFT) AND A MULTIPATH TEST (RIGHT).

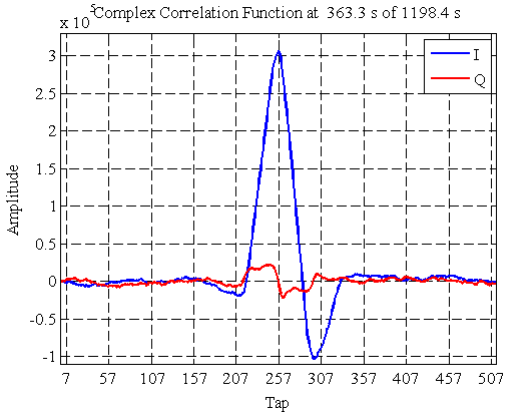

Fig. 6. Plot of the complex correlation function during a spoofing attack on a stationary receiver.

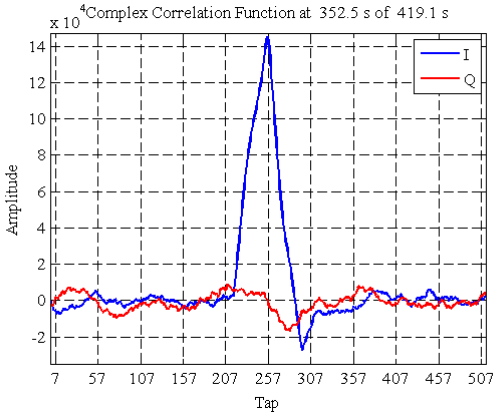

Fig. 7. Plot of the complex correlation function for a non-spoofed receiver on a dynamic platform.

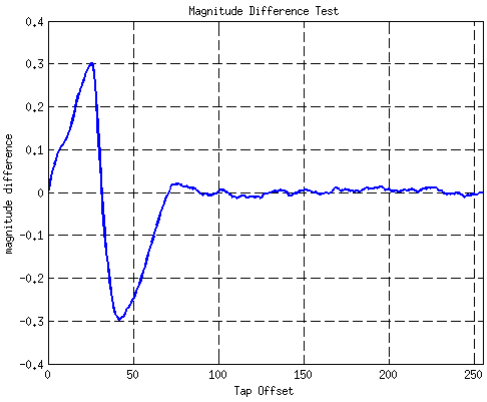

Fig. 8. Plot of $MD_\tau(t)$ showing the effect of a spoofing attack on a stationary receiver.

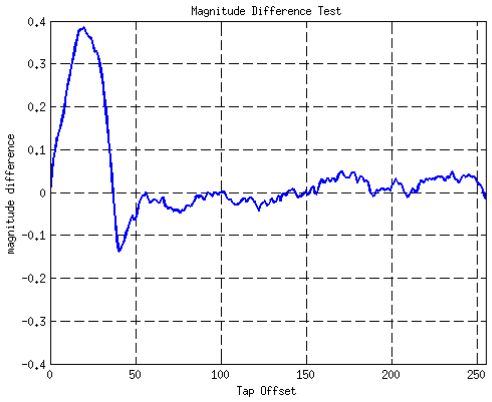

Fig. 9. Plot of $MD_\tau(t)$ showing the effect of multipath on a receiver on a dynamic platform.

vectors.

VI. FUTURE DIRECTIONS

Although the proposed metrics in Sec. IV do not appear to offer effective anti-spoofing because of their potentially high false alarm rate in the presence of significant multipath, there are several promising future directions for the VSD. A key difference between multipath and spoofing that is not revealed in the models of Sec. III is the difference in dynamics of multipath and spoofing signals. Because the spoofer acts with intent to deceive the victim receiver's tracking loops, $\{\alpha_s(t), \tau_s(t), \theta_s(t)\}$ will evolve in time differently than typical $\{\alpha_{m,k}(t), \tau_{m,k}(t), \theta_{m,k}(t)\}$. The following approaches seek to exploit the dynamics of a spoofing attack to detect spoofing and are the subject of ongoing research.

A. Maximum-Likelihood Techniques

A maximum-likelihood approach as described in Ref. [31] for tracking $\{\alpha_\cdot(t), \tau_\cdot(t), \theta_\cdot(t)\}$ would enable the following two approaches:

A.1 Bistatic-Radar-Based Approach

Stationary receivers could take advantage of a bistatic-radar-based VSD that could examine the spatial and temporal consistency of the received signals. In Ref. [32], the bias induced by multipath in the pseudorange measurement was extracted from the pseudo-Doppler observable using a dual frequency method for a set of data recorded over two years. Then, all of the multipath bias measurements in the recording interval were mapped to the corresponding satellite azimuth and elevation in a polar plot (see Ref. [32] Fig. 13), which shows clear patterns associ-

TABLE II

A TABLE OF SIX PLOTS SHOWING $RT_\tau(t)$ FOR THREE TEST CASES: (A) A NON-SPOOFED STATIONARY RECEIVER IN A BENIGN MULTIPATH ENVIRONMENT, (B) A SPOOFED STATIONARY RECEIVER, AND (C) A NON-SPOOFED RECEIVER ON A DYNAMIC PLATFORM. THE HORIZONTAL LINES SHOWN IN THE RIGHT COLUMN OF FIGURES ARE PLOTTED AT $\mu \pm 5\sigma$ WHERE μ AND σ ARE THE MEAN AND STANDARD DEVIATION OF THE TEST PRIOR TO SPOOFING OR MULTIPATH.

A

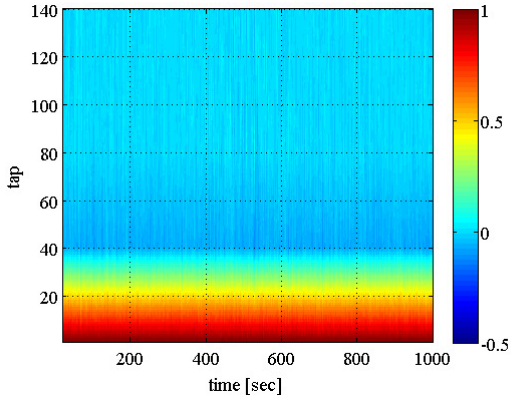

Fig. 10. Plot of $RT_\tau(t)$ at all τ.

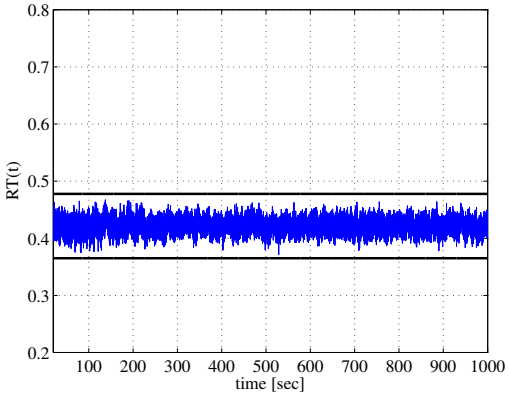

Fig. 11. Plot of $RT_{\tau \approx 1/2\mu s}(t)$.

B

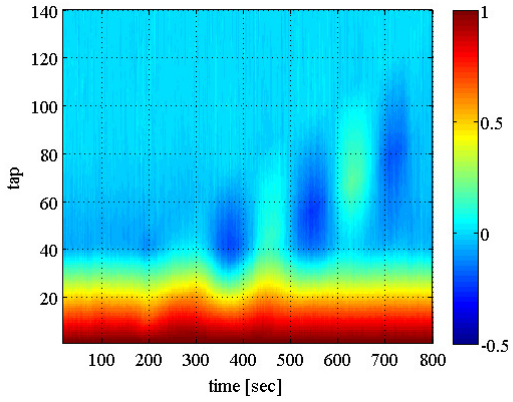

Fig. 12. Plot of the $RT_\tau(t)$ at all τ.

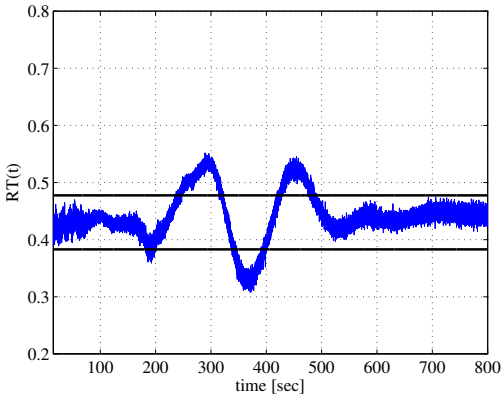

Fig. 13. Plot of $RT_{\tau \approx 1/2\mu s}(t)$.

C

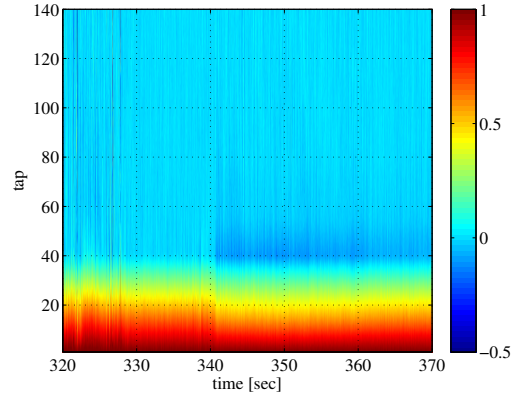

Fig. 14. Plot of the $RT_\tau(t)$ at all τ.

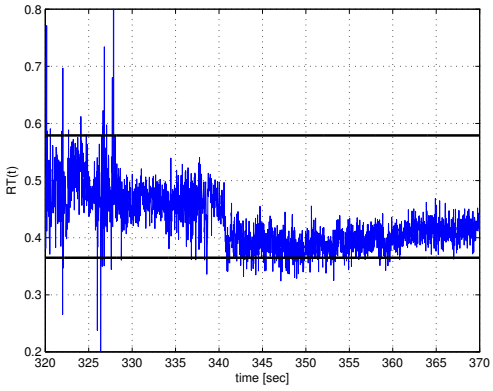

Fig. 15. Plot of $RT_{\tau \approx 1/2\mu s}(t)$.

ated with multipath due to the receiver's static environment. In Ref. [21], the ambiguity function in Doppler-range space for a twenty minute set of recorded data was mapped into physical space in an attempt to locate physical objects that generated multipath reflections. This approach revealed a cellular tower nearly 800 meters from the receiver that caused significant multipath.

These techniques suggest that a receiver could implement a spoofing defense that measures and detects inconsistencies between the measured multipath and the typical multipath background environment or flag multipath reflections that do not make physical sense. Of course, a spoofer could act like an incoming multipath signal to avoid detection, but this would mean VSD had achieved its modest goal of reducing the degrees-of-freedom available to a spoofer, forcing it to act like multipath.

A.2 Distribution Tests

Since the intent of spoofing is to commandeer the tracking loops of a victim receiver, a spoofer must at some point during the attack transmit a more powerful spoofing signal than the authentic signal (i.e., $\alpha_d(t) < \alpha_s(t)$) over a time scale on the order of the reciprocal of the delay-locked loop bandwidth (e.g., 10 sec). The probability distribution $p_{\alpha_m}(x)$ can be modeled as log-normal in typical GPS scenarios [15]. Chi-squared testing could be applied to observations of $\alpha(t)$ to assess the likelihood it was from the expected distribution. If it were found to be sufficiently unlikely that α was a sample from $p_{\alpha_m}(x)$ or $p_{\alpha_d}(x)$, then spoofing could be present. A difficulty of this approach is that the distribution for the spoofer $p_{\alpha_s}(x)$ may be nearly impossible to determine; therefore, only a probability of false alarm could be offered, and this only if $p_{\alpha_m}(x)$ could be properly defined.

B. Phase-Pseudorange Consistency Check

Another future technique could examine the consistency between the phase $\theta(t)$ and pseudorange $\rho(t)$ observables (i.e., similar to receiver autonomous integrity monitoring (RAIM) techniques). Between any time instants t_k and t_{k+1}, the phase difference $\Delta\theta(t_k) = \theta(t_k) - \theta(t_{k+1})$ should be consistent with the pseudorange difference $\Delta\rho(t_k) = \rho(t_k) - \rho(t_{k+1})$. A spoofer causes inconsistencies between these quantities if it attempts to alter the pseudorange while remaining locked in frequency to the authentic GPS signal as it may do to avoid introducing phase oscillations in the complex correlation function. A spoofer could circumvent this defense by carrying off the tracking loop very slowly or broadcasting the spoofing signal with a very high amplitude.

VII. CONCLUSIONS

The vestigial signal defense (VSD) is a GPS spoofing defense that relies on the difficulty of suppressing the authentic GPS signal during a spoofing attack. It is a receiver-autonomous non-cryptographic anti-spoofing technique that can be implemented at low cost in receiver software. The effectiveness of VSD is limited by the difficulty of differentiating spoofing from multipath. Experimental data collected from a dynamic platform in the dense-urban downtown of Austin, Texas revealed that previously proposed VSD-type detection metrics have difficulty differentiating spoofing from multipath. Future development of VSD will seek to exploit constraints in the dynamics of spoofing and multipath signals to distinguish the two.

ACKNOWLEDGMENTS

This work was generously supported in part by the Department of Defense through the National Defense Science and Engineering Graduate (NDSEG) Fellowship Program. The authors thank Ken Pesyna and Andrew Higdon of The University of Texas at Austin Radionavigation Laboratory for their support in collecting and processing the multipath and spoofing data. The authors also thank the engineers at The University of Texas at Austin Applied Research Laboratories for lending our laboratory the DFE receiver.

References

[1] Anon., "Vulnerability assessment of the transportation infrastructure relying on the Global Positioning System," John A. Volpe National Transportation Systems Center, Tech. Rep., 2001.

[2] L. Scott, "Anti-spoofing and authenticated signal architectures for civil navigation systems," in *Proceedings of the ION GNSS Meeting*. Portland, Oregon: Institute of Navigation, 2003, pp. 1542–1552.

[3] M. Kuhn, "An asymmetric security mechanism for navigation signals," in *Proc. of the 6th Int. Information Hiding Workshop*. Springer, May 2004, pp. 239–252.

[4] C. Wullems, O. Pozzobon, and K. Kubik, "Signal authentication and integrity schemes for next generation global navigation satellite systems," in *Proc. European Navigation Conference GNSS*, Munich, July 2005.

[5] G. Hein, F. Kneissl, J.-A. Avila-Rodriguez, and S. Wallner, "Authenticating GNSS: Proofs against spoofs, Part 1," *Inside GNSS*, pp. 58–63, July/August 2007.

[6] ——, "Authenticating GNSS: Proofs against spoofs, Part 2," *Inside GNSS*, pp. 71–78, September/October 2007.

[7] P. Papadimitratos and A. Jovanovic, "Protection and fundamental vulnerability of GNSS," in *IEEE Int. Workshop on Satellite and Space Communications*, 2008, pp. 167–171.

[8] 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 *Proceedings of the ION GNSS Meeting*. Savannah, GA: Institute of Navigation, 2008.

[9] P. Y. Montgomery, T. E. Humphreys, and B. M. Ledvina, "A multi-antenna defense: Receiver-autonomous GPS spoofing detection," *Inside GNSS*, vol. 4, no. 2, pp. 40–46, April 2009.

[10] O. Pozzobon, "Keeping the spoofs out: Signal authentication services for future GNSS," *Inside GNSS*, vol. 6, no. 3, pp. 48–55, May/June 2011.

[11] K. Wesson, M. Rothlisberger, and T. E. Humphreys, "Practical cryptographic civil GPS signal authentication," *NAVIGATION, Journal of the Institute of Navigation*, 2011, submitted for review; available at http://radionavlab.ae.utexas.edu/nma.

[12] T. E. Humphreys, "Detection strategy for cryptographic GNSS anti-spoofing," *IEEE Transactions on Aerospace and Electronic Systems*, 2011, submitted for review; available at http://radionavlab.ae.utexas.edu/detstrat.

[13] T. Stansell, "Location assurance commentary," *GPS World*, vol. 18, no. 7, p. 19, 2007.

[14] M. L. Psiaki, B. W. O'Hanlon, J. A. Bhatti, and T. E. Humphreys, "Civilian GPS spoofing detection based on dual-receiver correlation of military signals," in *Proceedings of the ION GNSS Meeting*. Portland, Oregon: Institute of Navigation, 2011.

[15] G. L. Turin, F. D. Clapp, T. L. Johnston, S. B. Fine, and D. Lavry, "A statistical model of urban multipath propagation," *IEEE Transactions on Vehicular Technology*, vol. VT-21, no. 1, Feb. 1972.

[16] A. J. V. Dierendonck, P. Fenton, and T. Ford, "Theory and performance of narrow correlator spacing in a GPS receiver," *NAVIGATION, Journal of the Institute of Navigation*, vol. 39, no. 3, pp. 265–283, Fall 1992.

[17] L. R. Weill, "Multipath mitigation: How good can it get with new signals?" *GPS World*, pp. 106–113, June 2003.

[18] M. Sahmoudi and R. J. Landry, "Multipath mitigation techniques using maximum-likelihood principle," *Inside GNSS*, pp. 24–29, November/December 2008.

[19] M. S. Braasch, "Autocorrelation sidelobe considerations in the characterization of multipath errors," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 33, no. 1, pp. 290–295, Jan. 1997.

[20] R. D. J. V. Nee, "Spread-spectrum code and carrier synchronization errors caused by multipath and interference," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 29, no. 4, pp. 1359–1365, Oct. 1993.

[21] J. York, J. Little, D. Munton, and K. Barrientos, "A fast number-theoretic transform approach to a GPS receiver," *NAVIGATION, Journal of the Institute of Navigation*, vol. 57, no. 4, pp. 297–307, 2010.

[22] B. M. Ledvina, W. J. Bencze, B. Galusha, and I. Miller, "An in-line anti-spoofing module for legacy civil GPS receivers," in *Proceedings of the ION ITM*, San Diego, CA, Jan. 2010.

[23] A. Cavaleri, M. Pini, L. L. Presti, M. Fantino, M. Boella, and S. Ugazio, "Signal quality monitoring applied to spoofing detection," in *Proceedings of the ION GNSS Meeting*, Portland, OR, Sept. 2011.

[24] 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 *Proceedings of the ION GPS Meeting*, Salt Lake City, UT, Sept. 2000.

[25] R. E. Phelts, "Multicorrelator techniques for robust mitigation of threats to GPS signal quality," Ph.D. dissertation, Stanford University, 2001.

[26] M. Irsigler and G. W. Hein, "Development of a real-time multipath monitor based on multi-correlator observations," in *Proceedings of the ION ITM*, Long Beach, CA, Sept. 2005.

[27] A. Cavaleri, B. Motella, M. Pini, and M. Fantino, "Detection of spoofed GPS signals at code and carrier tracking level," in *5th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing*, Dec. 2010.

[28] O. M. Mubarak and A. G. Dempster, "Analysis of early late phase in single- and dual frequency GPS receivers for multipath detection," *GPS Solut*, vol. 14, pp. 381–388, Feb. 2010.

[29] D. Shepard and T. E. Humphreys, "Characterization of receiver response to a spoofing attack," in *Proceedings of the ION GNSS Meeting*. Portland, Oregon: Institute of Navigation, 2011.

[30] J. York, J. Little, and D. Munton, "A direct-sampling digital-downconversion technique for a flexible, low-bias GNSS RF front-end," in *Proceedings of the ION GNSS Meeting*, Portland, OR, Sept. 2010.

[31] P. C. C. Fernandez-Prades and J. A. Fernandez-Rubino, "A bayesian approach to multipath mitigation in GNSS receivers," *IEEE Journal of Selected Topics in Signal Processing*, vol. 3, no. 4, pp. 695–706, Aug. 2009.

[32] R. B. Harris, "Evaluation, refinement and fusion of software-based pseudorange multipath mitigation techniques," in *Proceedings of the ION GNSS Meeting*, Portland, OR, Sept. 2002.