The Texas Spoofing Test Battery: Toward a Standard for Evaluating GPS Signal Authentication Techniques

Todd Humphreys, Jahshan Bhatti, Daniel Shepard, and Kyle Wesson,
The University of Texas at Austin, Austin, TX

BIOGRAPHIES

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. He specializes in applying optimal estimation and signal processing techniques to problems in radionavigation. His recent focus is on radionavigation robustness and security.

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.

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.

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.

ABSTRACT

A battery of recorded spoofing scenarios has been compiled for evaluating civil Global Positioning System (GPS) signal authentication techniques. The battery can be considered the data component of an evolving standard meant to define the notion of spoof resistance for commercial GPS receivers. The setup used to record the scenarios is described. A detailed description of each scenario reveals readily detectable anomalies that spoofing detectors could target to improve GPS security.

INTRODUCTION

Authentication of civil Global Positioning System (GPS) signals is increasingly a concern. Spoofing attacks, in which counterfeit GPS signals are generated for the purpose of manipulating a target receiver's reported position and time, have been demonstrated with low-cost commercial equipment against a wide variety of GPS receivers [1], [2], [3], [4]. Such attacks threaten the integrity of financial transactions, communications, and power grid monitoring operations that depend on GPS signals for accurate positioning and timing [5], [6], [7].

Whereas the military GPS waveform was originally designed to be unpredictable and therefore resistant to spoofing [8], the civil GPS waveforms are precisely specified in publicly-available documents [9]. Also, although not entirely constrained by the signal specifications, the navigation data messages modulated onto the civil waveforms are highly predictable. Known signal structure and data bit predictability make civil GPS signals susceptible to spoofing attacks.

Several researchers have proposed techniques for overlaying unpredictable but verifiable modulations on existing and future civil GPS signals [10], [11], [12], [13], [14]. These space-segment-side cryptographic techniques offer the promise of effective globally-available signal authentication without requiring additional hardware such as multiple antennas [15] or inertial measurement equipment [16], which would be impractical in cost-sensitive applications.

Unfortunately, even while many of the technical challenges of implementing space-segment-side cryptographic civil GPS authentication have been overcome, daunting procedural and financial hurdles remain. This sobering reality has lead several researchers to conclude that efforts to authenticate civil GPS signals over the next decade should focus on strategies that do not require support from the GPS space segment. Examples of such space-segment-independent authentication strategies can be categorized as (1) receiver-autonomous signal-processing-oriented techniques, which require no antenna motion or specialized antenna hardware [17], [18], [19]; (2) receiver-autonomous antenna-oriented techniques, which

Preprint of the 2012 ION GNSS Conference Nashville, TN, September 18–21, 2012

require antenna motion or specialized antenna hardware [20], [15], [21]; and (3) techniques that exploit the existing encrypted military signals to offer civil GPS signal authentication for networked GPS receivers [22], [23], [24], [25].

All existing or proposed civil GPS signal authentication schemes are premised on hypothesis tests involving statistical models for the authentic and counterfeit GPS signals. These models make simplifying assumptions that permit tractable analytical treatment of the detection problem. In general, the statistics of the null hypothesis (only authentic signals present) are readily verifiable by laboratory experiment but the statistics of the alternative hypothesis (spoofing attack underway) are not easily verified. This is because sophisticated signal generation hardware capable of code- and carrier-phase-aligned spoofing attacks is neither commercially available nor straightforward to construct. Thus, for example, experimental validation of the authentication technique proposed in [22] was limited to the null hypothesis.

A testbed capable of simulating realistic spoofing attacks is needed so that the efficacy of proposed civil GPS signal authentication techniques can be experimentally evaluated. A generic testbed capable of evaluating all known authentication techniques would be prohibitively expensive (e.g., it would require a large anechoic chamber for evaluating receiver-autonomous antenna-oriented techniques). But if the scope of evaluation is limited to receiver-autonomous signal-processing-oriented techniques and networked techniques (categories (1) and (3) above), then it is possible not only to develop an inexpensive testbed but to share the testbed's data component so that the tests can be replicated in laboratories across the globe.

This paper presents the Texas Spoofing Test Battery (TEXBAT), a set of six high-fidelity digital recordings of live static and dynamic GPS L1 C/A spoofing tests conducted by the Radionavigation Laboratory of the University of Texas at Austin. The battery can be considered the data component of an evolving standard meant to define the notion of spoof resistance for civil GPS receivers. According to this standard, successful detection of or imperviousness to all spoofing attacks in TEXBAT, or a future version thereof, could be considered sufficient to certify a civil GPS receiver as spoof resistant, as suggested in recent congressional testimony [26]. In what follows, the setup and procedure used to record the various TEXBAT scenarios is described. Thereafter, each scenario is detailed and analyzed, revealing obvious anomalies that future GPS receivers could be designed to detect.

BANDWIDTH AND QUANTIZATION CONSIDERATIONS

The initial version of TEXBAT, as presented in this paper, is focused solely on evaluating techniques for authenticating the civil GPS L1 C/A signals. Accordingly, one might argue that the TEXBAT recordings need only capture the main lobe of the C/A power spectrum, which is approximately 2-MHz wide and, due to the C/A code's $\text{sinc}^2(f/f_c)$-shaped power profile for chip rate f_c, contains more than 90% of the total C/A signal power.

But a narrow 2-MHz bandwidth would be inadequate to support evaluation of authentication techniques such as the Vestigial Signal Defense [18] that are based on a detailed characterization of the broadcast GPS-signals, a characterization that captures not only the signals' theoretical structure but also any filtering or other effects imposed by the transmitter. For these techniques, a wide radio frequency capture bandwidth is necessary to prevent signal distortion that could be interpreted as spoofing and lead to false alarms. A wideband recording is also necessary to support evaluation of GPS signal authentication techniques that rely on the presence of the military P(Y) signals, whose main lobe is 10 times wider than that of the C/A signals.

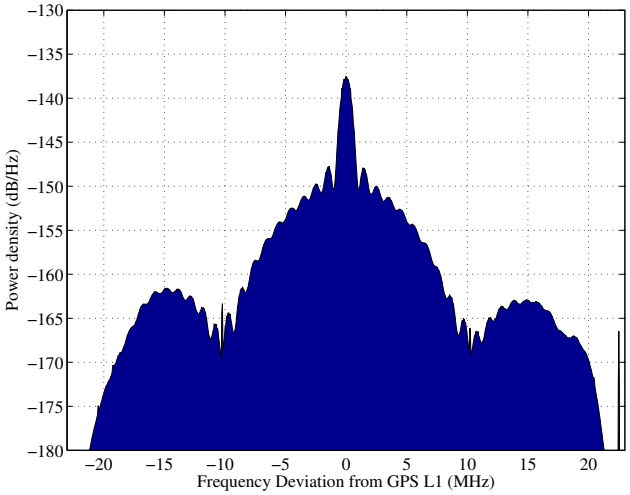

Fig. 1. Power spectral density estimate of the GPS signal corresponding to PRN 31 as received on 22 April, 2003 by the Stanford 46-meter-diameter radio telescope (original data courtesy of Dennis Akos). The complex sampling rate of the digitized data was 46.08 Msps.

To appreciate the richness of data in a wide band around L1, consider Fig. 1, which shows a power spectral density estimate of the GPS signal corresponding to pseudorandom number (PRN) code 31 as received in April 2003 by a high-gain (52 dBi) radio telescope. Besides a gentle asymmetry, the spectrum reveals that the full bandwidth of the transmitted GPS signals is approximately 30 MHz (the filtering effects visible beyond 30 MHz are likely dominated by the satellite's transmission hardware rather than the recording equipment, which was sampling at 46.08 Msps). Therefore, a bandwidth exceeding 30-MHz would be required to capture all C/A signal information that may be

relevant to authentication.

However, recognizing a practical need to minimize the size of recorded files, the recordings in TEXBAT were limited to a complex sampling rate of 25 Msps, which, with the high-quality front-end filtering employed, provides a flat frequency response over a 20-MHz bandwidth around L1. With a 20-MHz captured bandwidth, only 0.04 dB of C/A signal power is lost and filtering effects on the C/A signal due to the TEXBAT recording hardware are negligible.

Given its civil GPS focus, it is not necessary for TEXBAT to avoid filtering (distorting) the P(Y) signals, which, according to Fig. 1 would require a bandwidth exceeding 30 MHz. Instead, TEXBAT need only provide enough P(Y) signal power so that the networked authentication techniques discussed in [22], [23], [24], [25], which rely on cross-correlation with the P(Y) signals, can function properly. A 20-MHz bandwidth preserves all but 0.44 dB of the P(Y) spectral power, which should be adequate to support such techniques.

Now consider quantization. As discussed in [27], quantization causes bandpass signal power to "spill" out of the band of the original, unquantized signal. This has approximately the same effect on GPS signals as reducing the signal power and increasing the broad-band noise power. The net result of these two effects is a decrease in each received signal's carrier-to-noise ratio (C/N_0). Thus, one consideration when choosing the number of quantization levels N for TEXBAT recordings is to determine an acceptable loss in C/N_0 for the authentic and counterfeit signals.

Hegarty shows in [28] that when the captured bandwidth is wide compared with the main $\text{sinc}^2(f/f_c)$ lobe, the C/N_0 loss for N-level quantization is 2.06 dB for $N = 2$ (1 bit), 0.64 dB for $N = 4$ (2 bit), 0.26 dB for $N = 8$ (3 bit), and 0.14 dB for $N = 16$ (4 bit). Thus, if maintaining signal C/N_0 were the only imperative, no more than 4-bit quantization would practically be required.

But TEXBAT quantization must also accommodate a wide dynamic range. In potential TEXBAT scenarios, the difference in power between the authentic and counterfeit signal ensembles could be large. In these cases a high number of quantization levels makes it possible to recover the weaker signals from the data, which may be a key strategy for some signal authentication technique. Therefore, TEXBAT complex samples were recorded with 16-bit quantization to ensure a more-than-adequately-wide dynamic range.

RECORDING SETUP

This section discusses the TEXBAT recording setup, which is depicted graphically in Fig. 2. Each principal component of the setup will be treated in turn.

The GPS Spoofer

The central component of the TEXBAT recording setup is the University of Texas (UT) GPS spoofing device, whose design and operation are described in [1], [29], [30], [3], [4]. The latest version of the UT spoofing device is much improved compared to the original version introduced in [1]. For example, the current version has greater throughput: it is capable of simultaneously tracking and spoofing up to 14 GPS L1 C/A signals while continuing to perform background acquisition of emerging GPS satellite signals. Other key features of the spoofer relevant to TEXBAT are phase alignment, navigation data bit prediction, variable output attenuation, and noise padding.

Phase Alignment

The UT spoofer receives authentic civil GPS L1 C/A and GPS L2C signals and generates counterfeit GPS L1 C/A signals that are closely code-phase aligned with their authentic counterparts. The spoofer is currently not capable of generating signals that are carrier-phase aligned with the authentic signals at the location of a target receiver; indeed, it appears that such carrier-phase alignment is a practical impossibility for any spoofing device except under controlled laboratory conditions in view of the precise (cm-level) relative position knowledge required.

But neither do the carrier phases of the UT spoofer's signals wander arbitrarily with respect to those of the authentic signals. As the spoofer attempts to induce a position or timing deviation in the target receiver by shifting the code phase of its counterfeit signals, it can adopt either of two strategies with respect to carrier phase generation. In the default mode, the rate of change of its signals' carrier phase is proportional to the rate of change of the corresponding code phase. If $\dot{\tau}$ and $\dot{\phi}$ represent the rate of change of code phase and carrier phase, in seconds per second and cycles per second, respectively, then in the spoofer's default mode these are related by

$$\dot{\phi} = f_c \dot{\tau}$$

where f_c is the GPS L1 frequency in Hz.

In an alternative mode, the so-called frequency lock mode, the UT spoofer maintains approximately fixed whatever initial phase offset arises between its counterfeit signals and the authentic signals, and continues to maintain this fixed carrier phase offset even while it shifts the code phase of its counterfeit signals to induce a position or timing deviation in the target receiver. This ability to lock the relative (counterfeit-to-authentic) carrier phase even while shifting the relative (counterfeit-to-authentic) code phase enables the spoofer to evade some spoofing detection strategies that are designed to watch for the rapid amplitude variations caused by interacting authentic and counterfeit phasors of comparable magnitude when the authentic and counterfeit $\dot{\phi}$ values differ.

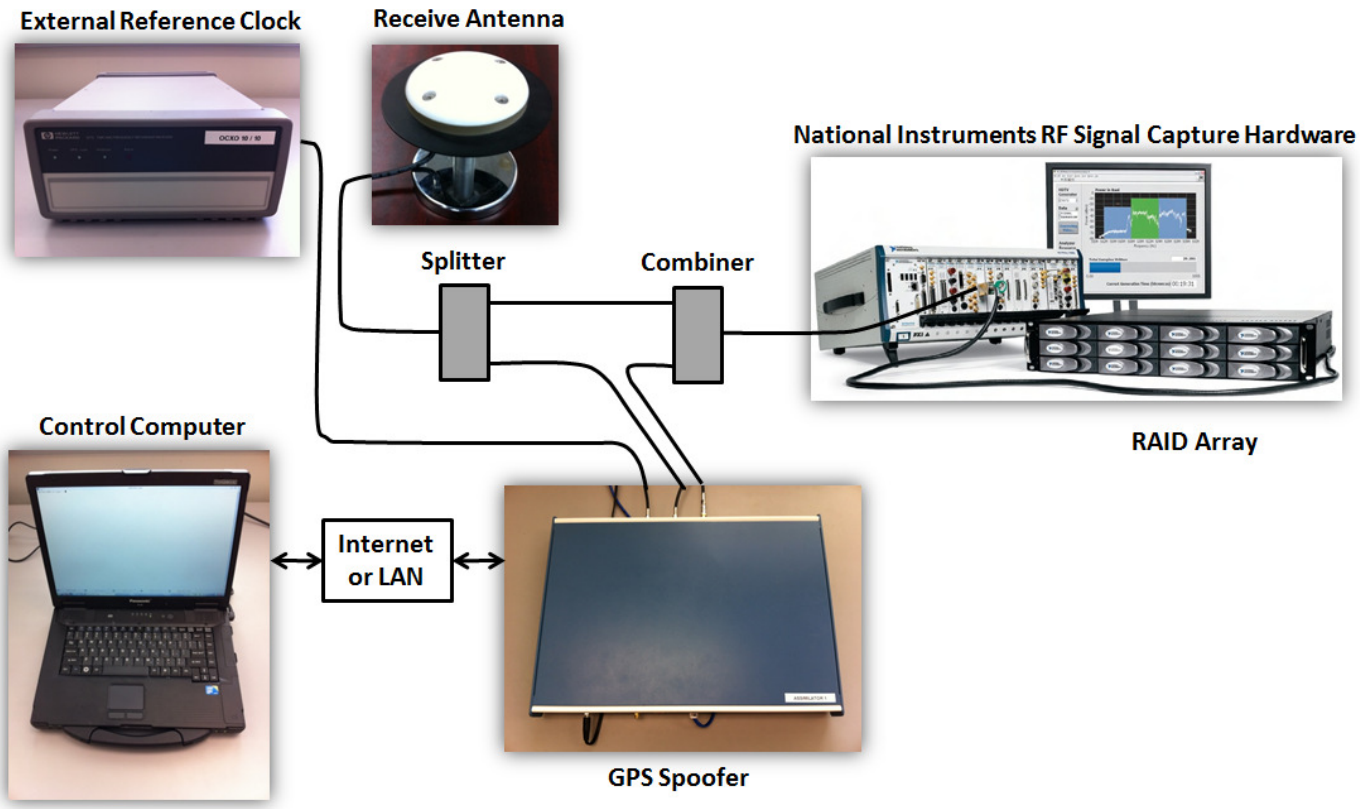

Fig. 2. Diagram of the TEXBAT recording setup.

Navigation Data Bit Prediction

To initialize an attack with an induced position, velocity, and timing (PVT) solution that is indistinguishable from the authentic PVT solution, it is not enough for the spoofer to achieve code-phase alignment with the authentic signals, it must also align its simulated navigation data bit stream with that of the authentic signals. But, due to processing, geometrical, and cable delays, it is impossible for the spoofer to read the value of the incoming navigation data bits off the air and immediately replay them so that they arrive at the target receiver perfectly aligned with the authentic data bits and having the correct value over the entire length of each data bit. Indeed, this impossibility is precisely what makes navigation message authentication effective for GPS signal authentication, as discussed in [13] and [14].

Rather than read the navigation data bits off the air for immediate replay, the UT spoofer takes advantage of the near perfect predictability of the navigation data that modulate the GPS L1 C/A signals. Over the course of a 12.5-minute navigation data superframe, the spoofer collects the data bits corresponding to each tracked GPS satellite. Alternatively, the spoofer can obtain the 12.5-minute superframe for each satellite from its control computer. Thereafter, the spoofer compensates for its ∼5-ms processing delay and for geometrical and cable delays by predicting the value of the navigation data stream slightly more than 5 ms in advance. In this way, the spoofer can achieve meter-level alignment between its signals and the authentic ones at the location of the target receiver.

Variable Output Attenuation

Before exiting the spoofer, counterfeit signals pass through a digital attenuator with a 31.5-dB range whose attenuation value can be set dynamically by the control computer. This enables the spoofer to finely adjust the so-called spoofer power advantage, or the ratio of the power of the counterfeit signal ensemble to the power of the authentic signal ensemble as seen by the target receiver.

Noise Padding

The analog signal ensemble generated by the UT spoofer contains only a modest amount of noise interference. In other words, the native noise floor of the output signal ensemble is low—much lower than the noise floor present at the output of a high-quality GPS antenna's low-noise amplifier (LNA). To appreciate the consequence of this low native noise floor, consider that if the UT spoofer is config-

ured to generate only a single output GPS L1 C/A signal (corresponding to a single PRN code), the native C/N_0 of the output signal exceeds 60 dB-Hz. Of course, when more simulated GPS signals are added to the ensemble, the C/N_0 associated with any one of the signals drops because the other signals act as interference.

A low native noise floor would not be a problem for the spoofer if it were always configured to match the power of each counterfeit signal to that of the corresponding authentic signal at the location of the target receiver's antenna, or in the case of a direct cable injection test, at the radio frequency (RF) input to the target receiver. In this case, the noise floor observed by the target receiver is essentially determined by the LNA in the receiver's antenna or in the receiver's own front-end.

But in many cases it may be advantageous for the spoofer to significantly overpower the authentic signals; for example, to eliminate interaction with them. Or it may be necessary to directly inject a powerful spoofing signal ensemble into the RF front-end of a receiver under test. In these cases, if the spoofer is generating less than ∼13 simulated signals, the C/N_0 values registered by the target receiver for each received GPS signal become unnaturally high, owing to the low native noise floor of the spoofer's output ensemble. (When generating 13 or more signals, the signals' mutual interference is sufficient to establish an appropriate noise floor from the perspective of any particular signal.)

To prevent unnaturally high C/N_0 values in these cases, the UT spoofer can be configured to add a variable level of "noise padding"—broadband interference—to its own output ensemble. In this way, the spoofer can dictate a maximum C/N_0 value for each of its output signals even while transmitting at high power.

Receive Antenna

Prior to and during a spoofing attack, the spoofer draws in authentic GPS signals from a reference antenna. For the static scenarios in TEXBAT the reference antenna was a Trimble Geodetic Zephyr II antenna located on the WRW building on the campus of the University of Texas. For the dynamic scenarios, the antenna was a vehicle-mounted Antcom 53G1215A-XT-1 antenna. The reference antenna output is also combined with the spoofer output and fed into the RF signal capture system as the authentic signal stream.

Reference Clock

The GPS spoofer is fed with a stable reference from an external 10-MHz oven controlled crystal oscillator (OCXO). An identical oscillator (not shown in Fig. 2) is used to drive the mixer and digitizer in the RF signal capture system.

RF Signal Capture System

A National Instruments PXIe-5663 6.6 GHz vector signal analyzer (VSA) was used to downmix and digitize the combined authentic and spoofing signals in each TEXBAT spoofing scenario. In accordance with the conclusions of the earlier section on bandwidth and quantization considerations, the VSA was configured to capture complex 16-bit samples at a rate of 25 Msps. The digitized data were then stored to disc.

RF Signal Replay System

The TEXBAT scenarios can be replayed through a National Instruments PXIe-5673E 6.6 GHz vector signal generator (VSG). Other VSGs may also be capable of replaying the data, which are stored simply as binary 16-bit inphase and quadrature samples. A separate XML file accompanying each scenario's binary data file provides all parameters relevant to data replay.

RECORDING PROCEDURE

Contrary to what Fig. 2 implies, the authentic signal stream in the recorded TEXBAT scenarios did not come directly from the receive antenna. Instead, two "clean" (spoof-free) data sets were initially recorded, one static and one dynamic. The clean static data set was replayed through the NI VSG to serve as the authentic signal stream for TEXBAT scenarios 1-4. The clean dynamic data set was used similarly for scenarios 5 and 6. The clean dynamic data set was originally recorded from an antenna mounted atop a vehicle traveling in Austin, TX. Both clean data sets are provided as part of TEXBAT. This procedure for generating the TEXBAT recordings ensures that users of TEXBAT can observe the behavior of their systems under nominal unspoofed conditions and then repeat the test controlling for all variables except for the presence of spoofing.

Users of TEXBAT data will observe the effects of up to three different clocks in the carrier phase time histories produced by their receiver under test: (1) the oscillator that drove the VSA when recording the original clean data set, (2) the oscillator that drives the VSG when the TEXBAT user replays a scenario, and (3) the reference oscillator of the user's receiver under test. A stable external OCXO reference oscillator was used to drive the VSA and VSG at each stage of recording and playback to ensure that clock effects on the recorded TEXBAT data would be mild. Most likely, the clock effects imprinted on the data by the recording hardware will be less significant than those imprinted by the receiver under test. Note that during a TEXBAT scenario recording the VSG replaying the

authentic signal stream and the VSA recording the combined spoofed and authentic signal streams are driven by the same external oscillator; thus, this stage of the recording procedure does not introduce any additional clock effects.

Each of the six TEXBAT spoofing scenarios is approximately 7 minutes (420 seconds) long. No spoofing signals were injected during the first 100 seconds or so to allow time for receivers under test to brace for the attack by acquiring all authentic signals present and obtaining a clean navigation and timing solution.

DETAILED DESCRIPTION OF TEXBAT SCENARIOS

TEXBAT includes six spoofing attack scenarios plus two clean data sets on which the scenarios are based. Table I summarizes the essential parameters of each of the six scenarios. "Spoofing Type" indicates the dimension along which the spoofing occurs, whether position or time. If position, the spoofer gradually induces an erroneous 600-meter position offset in the target receiver's perceived Earth-centered, Earth-fixed (ECEF) position coordinates; if time, it gradually induces an erroneous 2-μs (600-meter-equivalent) offset in the receiver's perceived GPS time. "Platform Mobility" indicates whether the GPS navigation solution derived from the underlying clean data set is static or dynamic. Scenarios 1-4 are static scenarios based on the clean static data set; scenarios 5 and 6 are dynamic scenarios based on the clean dynamic data set. "Power Adv." indicates the spoofer's power advantage, or the ratio of the power of the counterfeit signal ensemble to the power of the authentic signal ensemble as seen by the target receiver. Power advantage is expressed in dB. "Frequency Lock" indicates whether the spoofer was configured to operate in its frequency lock mode or in its default unlocked mode, as described previously. "Noise Padding" indicates whether the spoofer was configured to noise-pad its output signals ("Enabled") or transmit without additional noise padding ("Disabled"). "Size" indicates the size of the binary file in which the scenario data are recorded, in GB.

To facilitate development of spoofing detection techniques, a discussion of each TEXBAT scenario follows. The response of a particular GPS L1 C/A receiver, the science-grade UT/Cornell/ASTRA CASES sensor [31], [32], [33], to each scenario's spoofing attack will be presented graphically. It will become clear that each scenario offers obvious clues indicating the presence of spoofing.

Scenario 1: Static Switch

Scenario 1 involves a near-instantaneous switch from an exclusively authentic signal stream to an exclusively counterfeit stream. This scenario is meant to represent a case where the spoofer operator has physical access to the target receiver's antenna and can cleanly substitute, either by blocking the authentic signals or by cable switch-out, the counterfeit signals for the authentic ones.

The counterfeit signal ensemble in Scenario 1 is much weaker than the (amplified) authentic ensemble, so the switch event is obviously evident in the time history of normalized signal power at about the 100-second mark in Fig. 3. Clearly, an in-band power indicator would have easily detected a disruption in the antenna environment or RF chain in this case. But it should be borne in mind that the spoofer easily could have matched the pre- and post-switch in-band power levels; thus, in-band power is not a robust spoofing indicator for a case involving a switch attack.

Figure 4 shows that after the switch event the C/N_0 of a representative GPS signal falls by several dB (top panel). A simple spoofing detection strategy could be designed to trigger on this discontinuity. However, it should be noted that the spoofer could have reduced or eliminated the discontinuity by decreasing the level of its noise padding. Moreover, there is no indication either in the Doppler time history $f_D(t)$ or in the phase trauma flag that spoofing is present.

Figure 5 shows the time history of the receiver ECEF position deviation from the mean. Comparing the blue and green traces, it is clear that no reliable indicator of spoofing can be extracted from the navigation solution alone in this case. Similarly, Fig. 6 shows that the receiver clock offset rate $\delta\dot{t}_R$ (bottom panel) would not be a reliable indicator in this case. The receiver clock offset δt_R (top panel) shows a $\sim$10-meter discontinuity at the switch event. This indicates that there was a $\sim$30-ns common-mode error (advance) in the spoofer's alignment with the authentic signals. This may seem like a telltale signature on which a detector could trigger, but it is not a reliable indicator given that there is nothing inherently difficult in compensating for this common code phase advance inside the spoofer.

It should be pointed out that even though in this scenario the spoofer did not attempt to drag the target receiver off in time, it well could have, and at a rate gradual enough to be within the drift envelope of the target's reference oscillator.

Figure 7 shows, for a short interval spanning the switch event, the navigation-data-free output time history of 21 complex correlation taps uniformly spaced at an interval of 0.1 C/A code chips and centered at the receiver's prompt tap. These in-phase (top panel) and quadrature (bottom panel) strip charts are highly informative for spoofing detection. In fact, it can be shown that these data (at an arbitrarily short accumulation interval and including the data bit modulation) and a total in-band power measurement together constitute the complete information set

TABLE I
TEXAS SPOOFING TEST BATTERY: SCENARIO SUMMARY

Scenario Designation	Spoofing Type	Platform Mobility	Power Adv. (dB)	Frequency Lock	Noise Padding	Size (GB)
1: Static Switch	N/A	Static	N/A	Unlocked	Enabled	43
2: Static Overpowered Time Push	Time	Static	10	Unlocked	Disabled	42.5
3: Static Matched-Power Time Push	Time	Static	1.3	Locked	Disabled	42.6
4: Static Matched-Power Pos. Push	Position	Static	0.4	Locked	Disabled	42.6
5: Dynamic Overpowered Time Push	Time	Dynamic	9.9	Unlocked	Disabled	38.9
6: Dynamic Matched-Power Pos. Push	Position	Dynamic	0.8	Locked	Disabled	38.9

available for GPS signal authentication. It is obvious from Fig. 7 that a disruption began between 90 and 100 seconds. Not only did the amplitude of the in-phase accumulations change, but also the correlation shape changed slightly. Moreover, a Fourier transform of the complex time history from any single tap would reveal the post-attack emergence of anomalous frequencies in the complex accumulations.

Unfortunately, in the case of a switch attack, a sophisticated spoofer could be designed to avoid causing these and other distortions of the complex correlation function. The absence of interaction between the authentic and counterfeit signals allows the spoofer to focus on refining its switchover procedure and the shape and behavior of its induced complex correlation function. This implies that the switch attack is an especially potent one for the spoofer.

Fortunately, analysis of subsequent scenarios will reveal that, for attacks in which both authentic and counterfeit signals are present at significant levels, it is exceedingly challenging for the spoofer to prevent distortion of the complex correlation function due to interaction between the authentic and counterfeit signals.

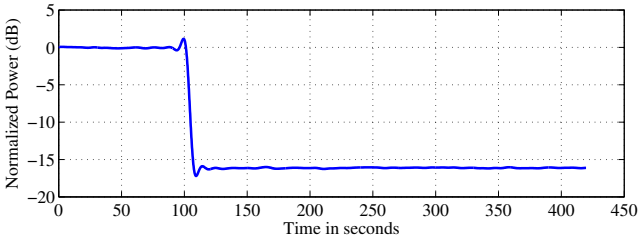

Fig. 3. Scenario 1: Time history of normalized power in a 2-MHz band centered at GPS L1.

Scenario 2: Static Overpowered Time Push

In Scenario 2, the spoofer executes a timing attack with a 10-db power advantage over the authentic signal ensemble. The sequence of figures depicting the effects of the attack is the same as for Scenario 1 (this is also true for all subsequent scenarios).

Attacking with overwhelming power is to the spoofer's ad-

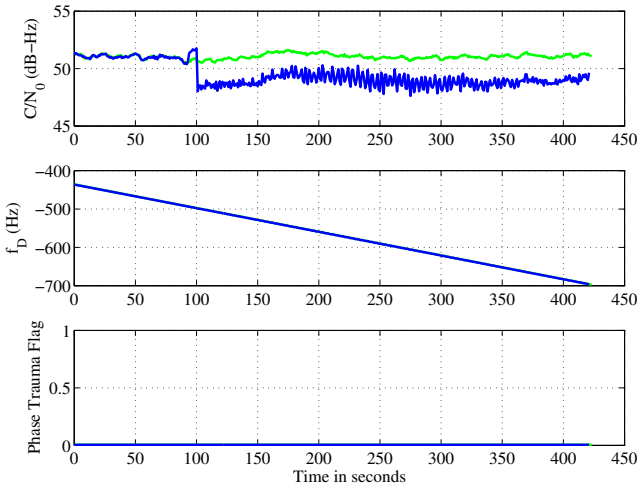

Fig. 4. Scenario 1: Time history of C/N_0 (top panel), f_D (center panel), and the phase trauma indicator (bottom panel) corresponding to a single signal being spoofed. In each panel, the green trace shows the receiver's unspoofed response and the blue trace shows the receiver's spoofed response.

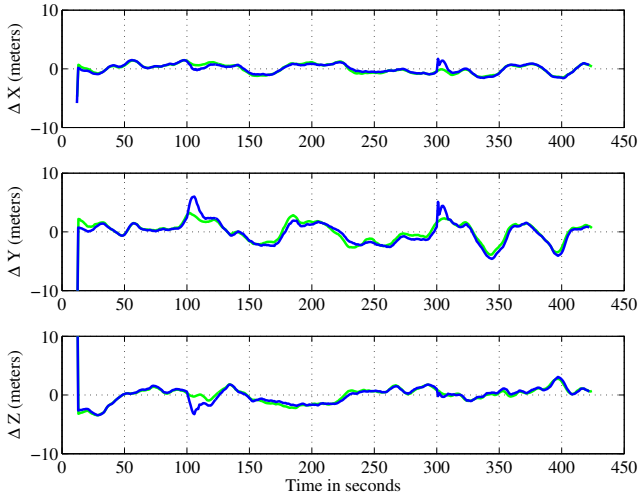

Fig. 5. Scenario 1: Time history of receiver ECEF position deviation from mean. In each panel, the green trace shows the receiver's unspoofed response and the blue trace shows the receiver's spoofed response.

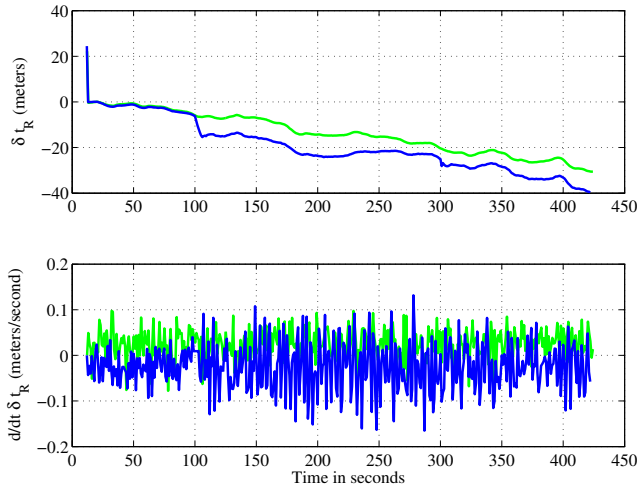

Fig. 6. Scenario 1: Time history of δt_R (top panel) and $\dot{\delta t_R}$ (bottom panel). In each panel, the green trace shows the receiver's unspoofed response and the blue trace shows the receiver's spoofed response.

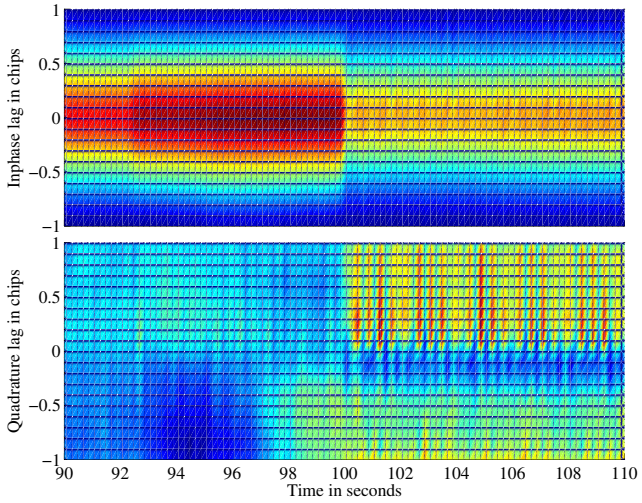

Fig. 7. Scenario 1: Navigation-data-free output time history of 21 complex correlation taps uniformly spaced at an interval of 0.1 C/A code chips and centered at the receiver's prompt tap. In-phase (top panel) and quadrature (bottom panel) accumulations are based on 2-second coherent summations.

vantage in the sense that the authentic signals are forced into the noise floor by the action of the target receiver's automatic gain control function. Thus, the weak vestigial authentic signals do not interact significantly with the counterfeit signals, which implies that a high-power attack's correlation signature may look no more suspicious than that of a switch attack.

However, the target receiver can readily detect a high-power attack by monitoring its in-band received power. Figure 8 makes this evident: the spoofer's 10-dB power advantage reveals itself as an abrupt 8-dB increase in the in-band power. While it is true that the spoofer could slow the rate at which it increases power (i.e., make the slope in Fig. 8 shallower), such a gradual increase would expose the spoofer to detection by techniques looking for interaction between the authentic and counterfeit signals. Hence, in a non-switch attack the spoofer can be effectively "boxed in" by a combination of in-band power monitoring and complex correlation function monitoring.

Figure 9 shows that the spoofer in Scenario 2 significantly increased the C/N_0 of a representative GPS signal as it initiated its attack. There is also an obvious deviation in f_D due to the spoofer's effecting the time spoofing in its default frequency unlocked mode. As it moves the target receiver off in time, the spoofer adjusts the induced Doppler f_D to be appropriately proportional to the rate of change in the common code phase. It is interesting to note in the lower panel in Fig. 9 that both the initial takeover (at around 80 seconds) and the initial time pull-off (at around 115 seconds) disturb the composite carrier phase enough to trigger the target receiver's phase trauma indicator.

Because Scenario 2 involves only a time attack, there is little effect on the target receiver's ECEF position history, though, as with the phase trauma indicator, there is some disturbance at initial capture and initial time pull-off (Fig. 10).

The profile of the timing attack is evident in Fig. 11. In its frequency unlocked mode, the spoofer induces a common offset in f_D on all signals. The offset follows a trapezoidal trajectory, which translates to a trapezoidal excursion in $\dot{\delta t_R}$ (lower panel) that is obviously well outside the envelope of this particular receiver's native clock variations. But with a shallower acceleration profile, or a less-stable receiver clock, the variation in $\dot{\delta t_R}$ may not appear anomalous.

As was true for Scenario 1, the complex correlation function plots (Fig. 12) reveal a great deal about Scenario 2. Most striking is the oscillation that begins just after 110 seconds. This has an intuitive explanation. Because frequency lock is disabled, the relative (counterfeit to authentic) phase angle begins to ramp, following a profile proportional to the ramp of δt_R in the upper panel of Fig. 11. Consequently, the composite counterfeit and authentic signal phasor, which is the one actually being tracked by the receiver's phase lock loop, begins to experience amplitude variations: the counterfeit and authentic phasors interact now constructively, now destructively. Note that a strong oscillation is evident even though the counterfeit phasor is 3.1 times longer (10 time more powerful) than the authentic one.

Clearly, such an oscillation raises suspicion of a spoofing attack. It is, however, not conclusive given than strong natural multipath signals tend to cause a similar oscillation [18], [34]. Moreover, the spoofer can prevent the telltale oscillation by decoupling the code and carrier phase in the

signals it generates, as the UT spoofer does in its frequency lock mode.

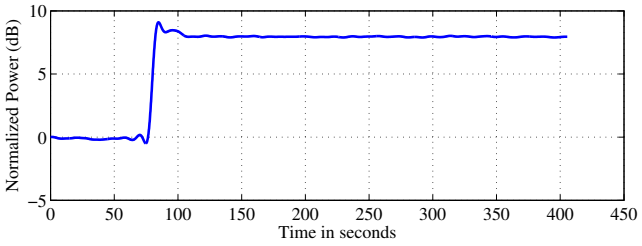

Fig. 8. Scenario 2: Time history of normalized power in a 2-MHz band centered at GPS L1.

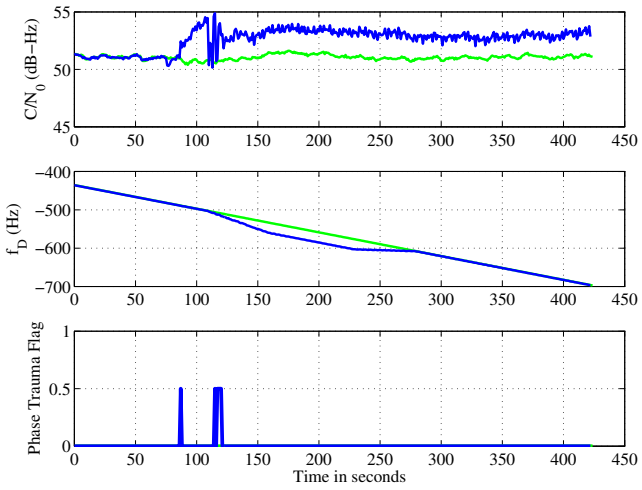

Fig. 9. Scenario 2: Time history of C/N_0 (top panel), f_D (center panel), and the phase trauma indicator (bottom panel) corresponding to a single signal being spoofed. In each panel, the green trace shows the receiver's unspoofed response and the blue trace shows the receiver's spoofed response.

Scenario 3: Static Matched-Power Time Push

Scenario 3 is identical to Scenario 2 except that the spoofer's power advantage is reduced from 10 dB to 1.3 dB and the spoofer's frequency lock mode is enabled. The reduction in power advantage is evident in Fig. 13, which shows that the 1.3 dB power advantage leads to an increase in in-band power of only 2.3 dB, compared to 8 dB for Scenario 2. Scenario 3 is meant to represent a case in which the spoofer attempts to approximately match its ensemble power to that of the authentic signals.

Figures 15 to 17 reveal the consequences of having frequency lock enabled and nearly-matched counterfeit and authentic signal ensemble power. The absence of phase trauma events and anomalous excursions in f_D and $\dot{\delta t_R}$ reflect the fact that the spoofer's induced carrier phase is well-behaved—approximately locked at some relative phase angle to the corresponding authentic signal's carrier phase. However, Figs. 14 and 17 make it clear that

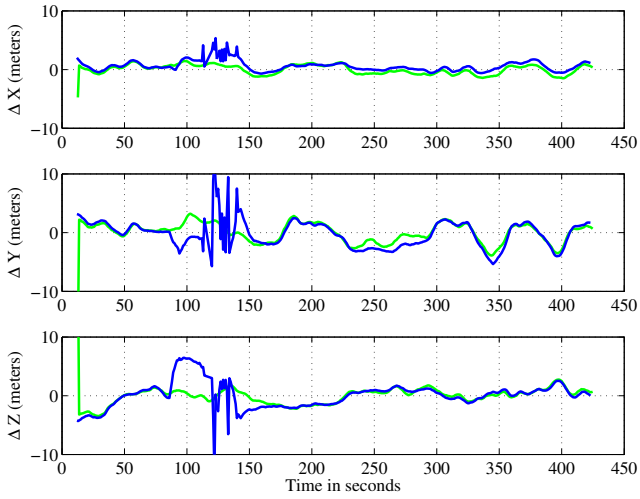

Fig. 10. Scenario 2: Time history of receiver ECEF position deviation from mean. In each panel, the green trace shows the receiver's unspoofed response and the blue trace shows the receiver's spoofed response.

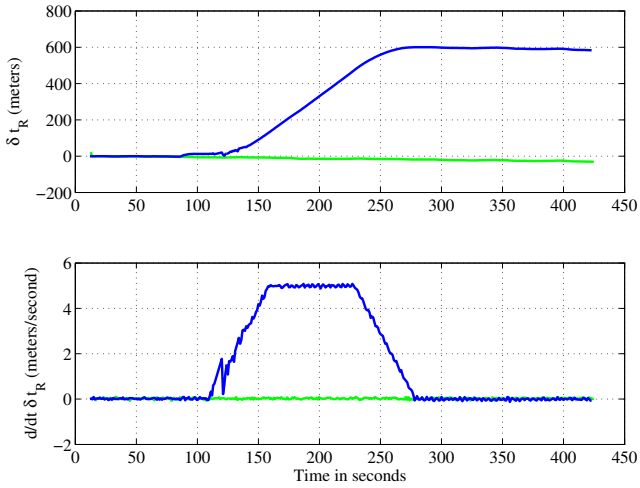

Fig. 11. Scenario 2: Time history of δt_R (top panel) and $\dot{\delta t_R}$ (bottom panel). In each panel, the green trace shows the receiver's unspoofed response and the blue trace shows the receiver's spoofed response.

the UT spoofer's frequency locking behavior is not perfect: there exists a slight residual differential Doppler that causes the counterfeit and authentic phasors, now approximately matched in magnitude, to slowly rotate with respect to each other. This slow beating gives rise to sustained intervals of constructive (high C/N_0) and destructive (low C/N_0) interference whose C/N_0 values differ by 10 dB. Such beating could only be ascribed to multipath in a narrow set of circumstances in which the direct-path signal has been attenuated and the multipath and direct signals exhibit a slight differential Doppler. But such cases could be distinguished from the present one because in the former the in-band signal power would not be expected to rise.

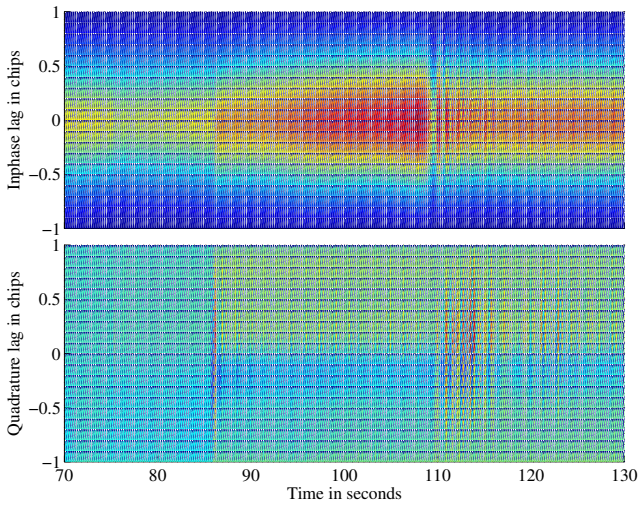

Fig. 12. Scenario 2: Navigation-data-free output time history of 21 complex correlation taps uniformly spaced at an interval of 0.1 C/A code chips and centered at the receiver's prompt tap. In-phase (top panel) and quadrature (bottom panel) accumulations are based on 2-second coherent summations.

Note that although the slow beating in this case is an artifact of the UT spoofer's inability to achieve perfect frequency lock, it remains true that when counterfeit and authentic signals are approximately matched in power the spoofer can hardly avoid some kind of constructive or destructive interference. This follows from the spoofer's presumed inability to precisely control the initial relative counterfeit-to-authentic carrier phase.

Note also that although in this scenario the spoofer successfully induced a 600-meter ($\sim$2-μs) offset in δt_R in the particular receiver targeted, the pulloff was not smooth. Without the benefit of overwhelming signal power and without the frequency aiding from the target receiver's phase lock loop (a consequence of the spoofer's having frequency lock enabled), the spoofer struggles to induce the target receiver's delay lock loops to track its signals instead of the authentic ones. The large excursions in ECEF position (Fig. 15) and the rough initial departure of δt_R (upper panel of Fig. 16) are evidence of a struggle between the counterfeit and authentic signals for control of the target receiver's delay lock loops.

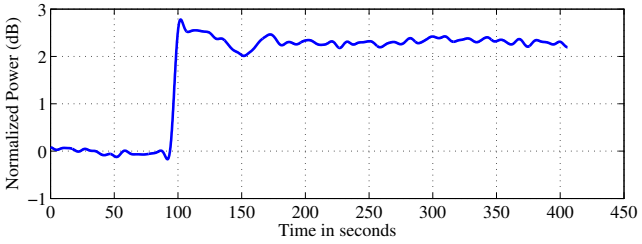

Fig. 13. Scenario 3: Time history of normalized power in a 2-MHz band centered at GPS L1.

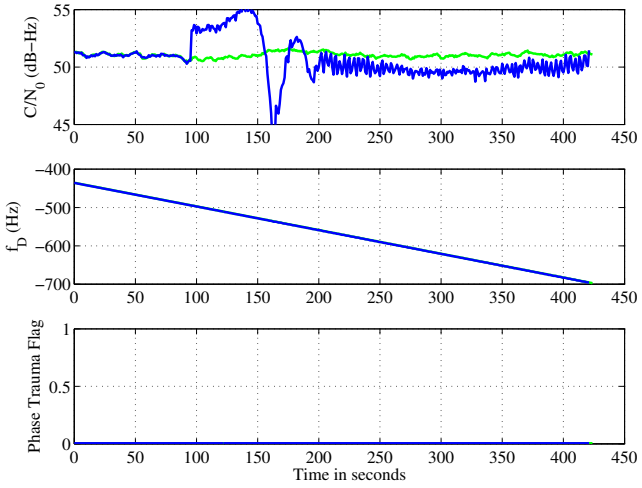

Fig. 14. Scenario 3: Time history of C/N_0 (top panel), f_D (center panel), and the phase trauma indicator (bottom panel) corresponding to a single signal being spoofed. In each panel, the green trace shows the receiver's unspoofed response and the blue trace shows the receiver's spoofed response.

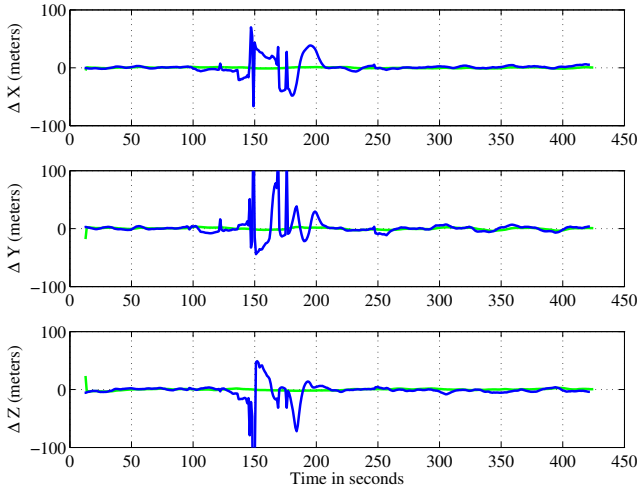

Fig. 15. Scenario 3: Time history of receiver ECEF position deviation from mean. In each panel, the green trace shows the receiver's unspoofed response and the blue trace shows the receiver's spoofed response.

Scenario 4: Static Matched-Power Position Push

Scenario 4 is identical to Scenario 3 except that the spoofer's power advantage has been reduced still further (from 1.2 to 0.4 dB) and the spoofing drives the target receiver off in position instead of time—specifically, an offset of 600 m in the Z-coordinate.

The spoofer's near-zero-dB power advantage is evident in two ways in Fig. 18. First, the steady-state increase in in-band power is low—less than 2 dB. Second, there arises an oscillation in the in-band power during initial pulloff. This oscillation reflects a substantial coherence in the spoofing signals: their constructive and destructive interaction with

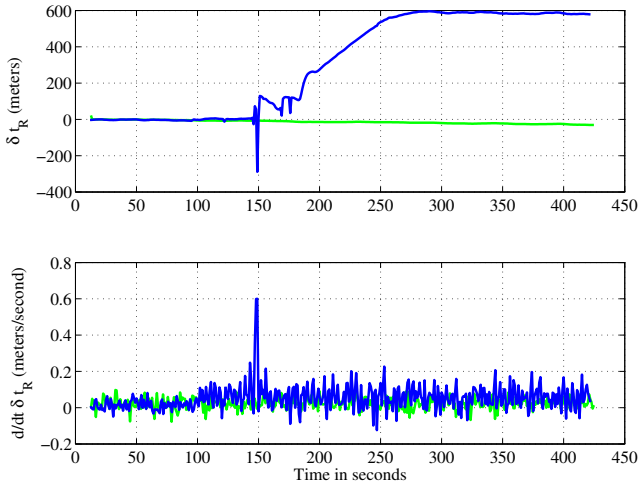

Fig. 16. Scenario 3: Time history of δt_R (top panel) and $\dot{\delta t}_R$ (bottom panel). In each panel, the green trace shows the receiver's unspoofed response and the blue trace shows the receiver's spoofed response.

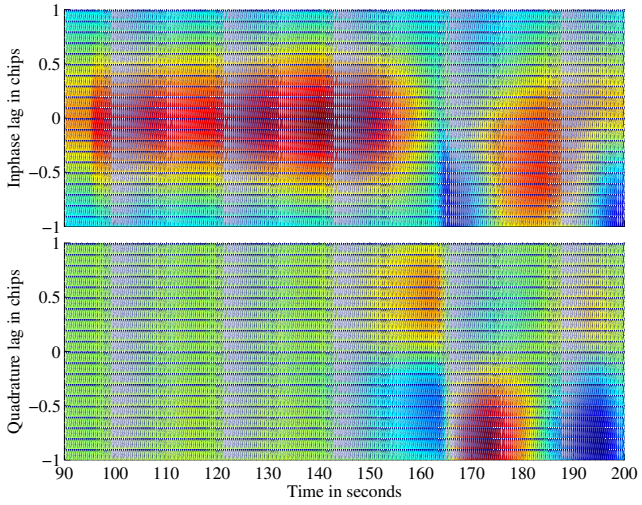

Fig. 17. Scenario 3: Navigation-data-free output time history of 21 complex correlation taps uniformly spaced at an interval of 0.1 C/A code chips and centered at the receiver's prompt tap. In-phase (top panel) and quadrature (bottom panel) accumulations are based on 4-second coherent summations.

the authentic signals tends to occur in unison. An oscillation is also manifest in Scenario 3's in-band power (Fig. 13), but its amplitude is less because the counterfeit and authentic signal powers are not so evenly matched.

Even more than with Scenario 3, the spoofer's low power advantage and the approximately locked counterfeit-to-authentic carrier phase make pulloff of the target receiver's delay lock loops a challenge. In fact, the persistent offset in ΔX (Fig. 15) and δt_R (Fig. 16), despite the spoofing being solely in the Z dimension, suggests that at least one of the target receiver's channels remained locked to the authentic signal in this case. This again highlights that for the spoofer a low power advantage is perilous.

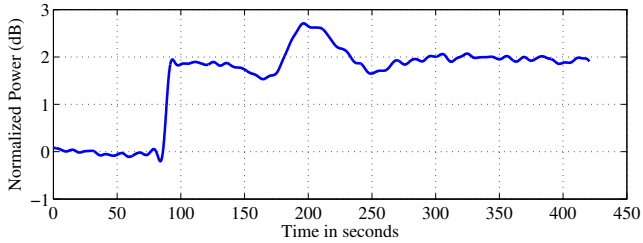

Fig. 18. Scenario 4: Time history of normalized power in a 2-MHz band centered at GPS L1.

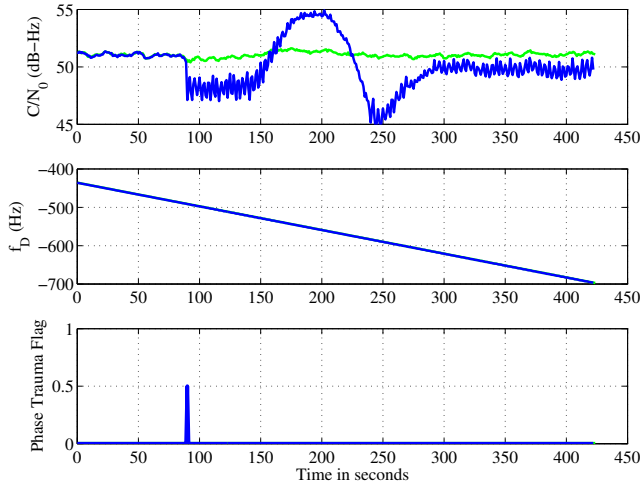

Fig. 19. Scenario 4: Time history of C/N_0 (top panel), f_D (center panel), and the phase trauma indicator (bottom panel) corresponding to a single signal being spoofed. In each panel, the green trace shows the receiver's unspoofed response and the blue trace shows the receiver's spoofed response.

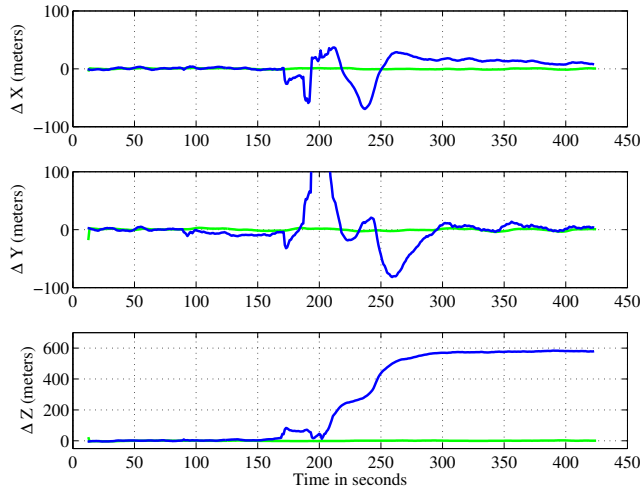

Fig. 20. Scenario 4: Time history of receiver ECEF position deviation from mean. In each panel, the green trace shows the receiver's unspoofed response and the blue trace shows the receiver's spoofed response.

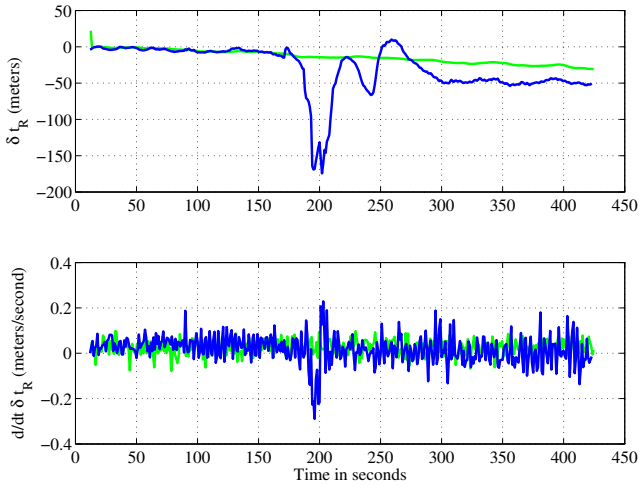

Fig. 21. Scenario 4: Time history of δt_R (top panel) and $\dot{\delta t}_R$ (bottom panel). In each panel, the green trace shows the receiver's unspoofed response and the blue trace shows the receiver's spoofed response.

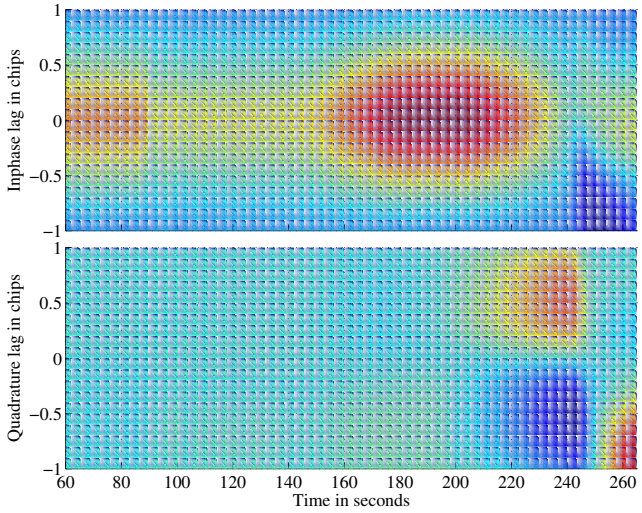

Fig. 22. Scenario 4: Navigation-data-free output time history of 21 complex correlation taps uniformly spaced at an interval of 0.1 C/A code chips and centered at the receiver's prompt tap. In-phase (top panel) and quadrature (bottom panel) accumulations are based on 4-second coherent summations.

Scenario 5: Dynamic Overpowered Time Push

Scenario 5 is similar to Scenario 2 except that the receiver platform is dynamic rather than static and the spoofer's frequency lock feature is disabled. The target receiver's ability to defend itself from a spoofing attack is much eroded in this case. While as before the spoofer's inelegant takeover leaves behind telltale variations in C/N_0 and some phase trauma, the target receiver, considering its dynamic platform, may easily confuse these for natural phenomena. The challenge of spoofing detection on a dynamic platform is to distinguish spoofing effects from natural fading and multipath.

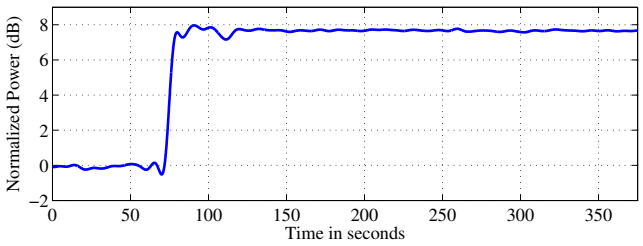

Fig. 23. Scenario 5: Time history of normalized power in a 2-MHz band centered at GPS L1.

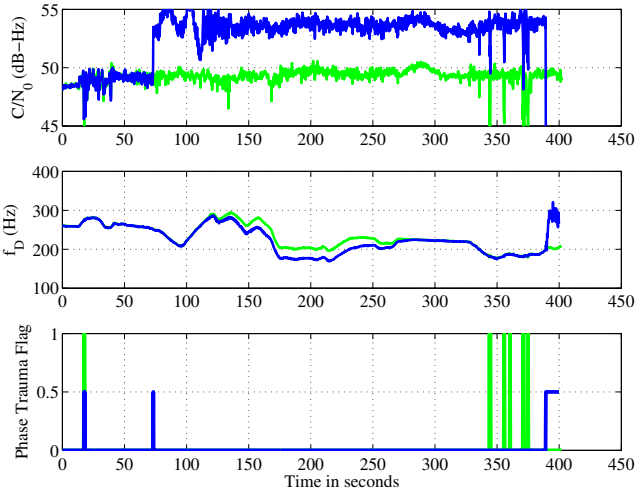

Fig. 24. Scenario 5: Time history of C/N_0 (top panel), f_D (center panel), and the phase trauma indicator (bottom panel) corresponding to a single signal being spoofed. In each panel, the green trace shows the receiver's unspoofed response and the blue trace shows the receiver's spoofed response. The unspoofed and spoofed phase trauma indicators have different amplitudes only for visual clarity.

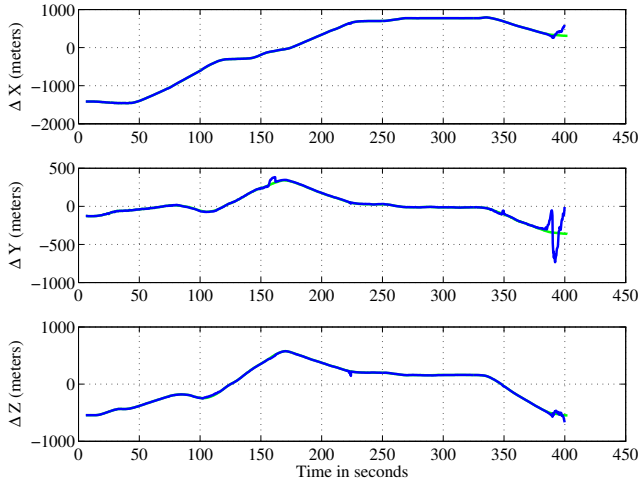

Fig. 25. Scenario 5: Time history of receiver ECEF position deviation from mean. In each panel, the green trace shows the receiver's unspoofed response and the blue trace shows the receiver's spoofed response.

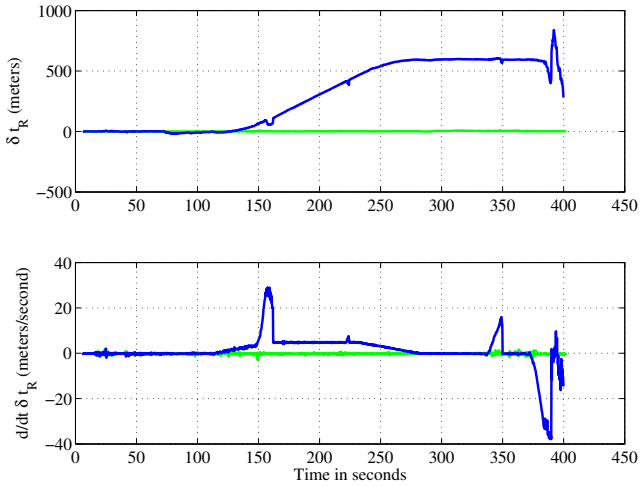

Fig. 26. Scenario 5: Time history of δt_R (top panel) and $\delta \dot{t}_R$ (bottom panel). In each panel, the green trace shows the receiver's unspoofed response and the blue trace shows the receiver's spoofed response.

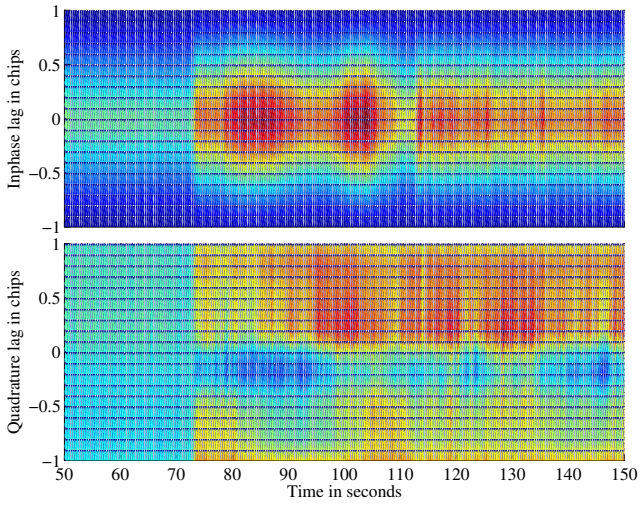

Fig. 27. Scenario 5: Navigation-data-free output time history of 21 complex correlation taps uniformly spaced at an interval of 0.1 C/A code chips and centered at the receiver's prompt tap. In-phase (top panel) and quadrature (bottom panel) accumulations are based on 4-second coherent summations.

Scenario 6: Dynamic Matched-Power Position Push

Scenario 6 is similar to Scenario 4 except that the receiver platform is dynamic rather than static. Again, the spoofer's modest power advantage and frequency lock setting complicate its takeover of the target receiver's tracking loops, forcing it to leave behind clues of its presence. To defend itself, the target receiver must distinguish these clues from similar variations that arise naturally on a dynamic platform.

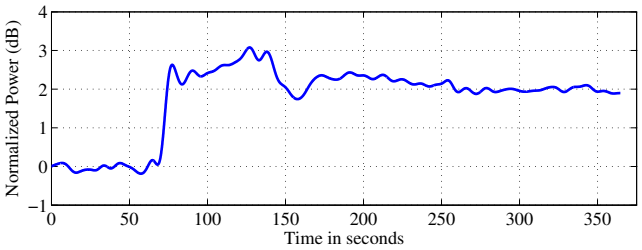

Fig. 28. Scenario 6: Time history of normalized power in a 2-MHz band centered at GPS L1.

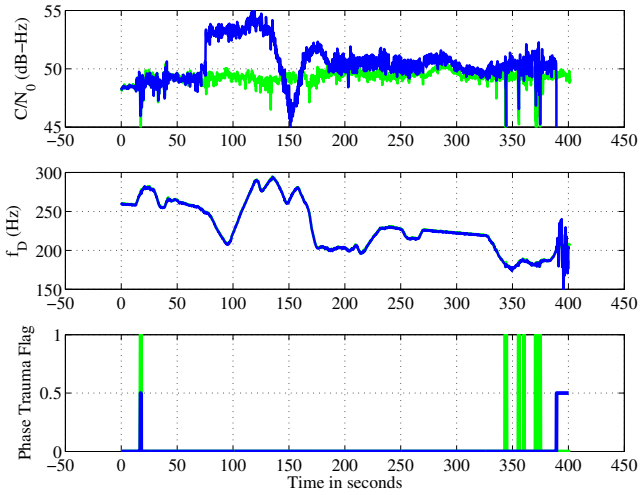

Fig. 29. Scenario 6: Time history of C/N_0 (top panel), f_D (center panel), and the phase trauma indicator (bottom panel) corresponding to a single signal being spoofed. In each panel, the green trace shows the receiver's unspoofed response and the blue trace shows the receiver's spoofed response. The unspoofed and spoofed phase trauma indicators have different amplitudes only for visual clarity.

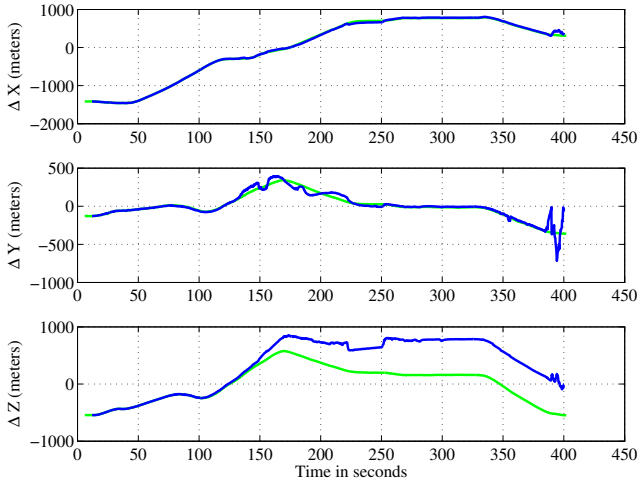

Fig. 30. Scenario 6: Time history of receiver ECEF position deviation from mean. In each panel, the green trace shows the receiver's unspoofed response and the blue trace shows the receiver's spoofed response.

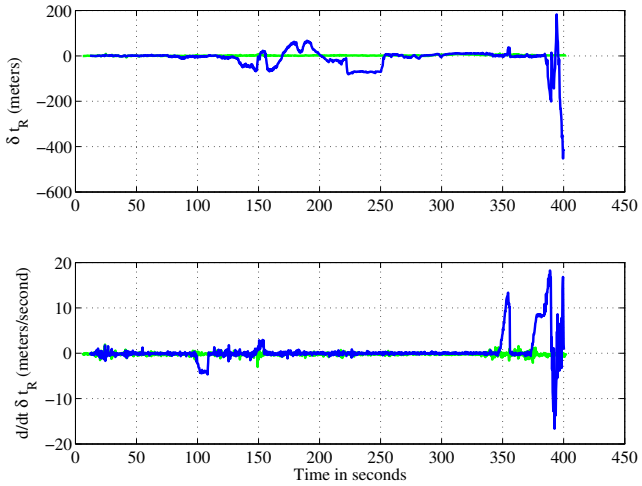

Fig. 31. Scenario 6: Time history of δt_R (top panel) and $\delta \dot{t}_R$ (bottom panel). In each panel, the green trace shows the receiver's unspoofed response and the blue trace shows the receiver's spoofed response.

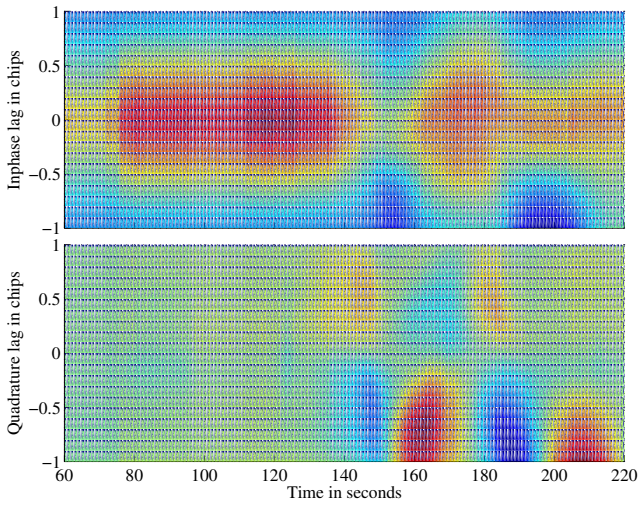

Fig. 32. Scenario 6: Navigation-data-free output time history of 21 complex correlation taps uniformly spaced at an interval of 0.1 C/A code chips and centered at the receiver's prompt tap. In-phase (top panel) and quadrature (bottom panel) accumulations are based on 4-second coherent summations.

CONCLUSIONS

The Texas Spoofing Test Battery (TEXBAT), a set of six high-fidelity digital recordings of live static and dynamic GPS L1 C/A spoofing tests, was introduced as a data set for the development and evaluation of civil GPS signal authentication techniques. TEXBAT can also be thought of as the data component of a draft standard for defining the notion of spoofing resistance for civil GPS receivers. The TEXBAT recording setup was designed to ensure that the recorded scenarios are, insofar as is practical, a faithful representation of the corresponding live attacks. The effects of each of the six scenarios on a particular target receiver were analyzed, revealing numerous anomalies that could be targeted for spoofing detection. In this regard, the target receiver's complex correlation function is especially fraught with spoofing clues.

An admixture of counterfeit and authentic signals of comparable power inevitably leads to interaction between the two, which, if the target receiver can distinguish from natural multipath and fading effects, is a useful spoofing indicator. In-band power monitoring effectively limits a spoofer's ability to eliminate interaction by increasing its signal power advantage. Hence, in a non-switch attack the spoofer can be effectively "boxed in" by a combination of in-band power monitoring and complex correlation function monitoring. This is especially effective for static receivers because the nominal local multipath and fading environment can be characterized and thus distinguished from spoofing.

ENDNOTE

The University of Texas Radionavigation Laboratory has teamed with National Instruments to offer TEXBAT as a free data set to researchers, manufacturers, and government entities wishing to develop and test GPS L1 C/A signal authentication techniques. Please visit `radionavlab.ae.utexas.edu` and click on "RNL Public Data Sets" for information on how to dowload TEXBAT.

References

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

[2] Shepard, D. and Humphreys, T. E., "Characterization of Receiver Response to a Spoofing Attack," *Proceedings of the ION GNSS Meeting*, Institute of Navigation, Portland, Oregon, 2011.

[3] Shepard, D., Bhatti, J., and Humphreys, T., "Evaluation of Smart Grid and Civilian UAV Vulnerability to GPS Spoofing Attacks," *Proceedings of the ION GNSS Meeting*, Institute of Navigation, Nashville, Tennessee, 2012.

[4] Shepard, D. P., Humphreys, T. E., and Fansler, A. A., "Evaluation of the Vulnerability of Phasor Measurement Units to GPS Spoofing Attacks," *International Journal of Critical Infrastructure Protection*, 2012, to be published.

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

[6] Anon., "Global Positioning System Impact To Critical Civil Infrastructure (GICCI)," Tech. rep., Mission Assurance Division, Naval Surface Warfare Center, 2009.

[7] Kroener, U. and Dimc, F., "Hardening of civilian GNSS trackers," *Proceedings of the 3rd GNSS Vulnerabilities and Solutions Conference*, Royal Institute of Navigation, Krk Island, Croatia, Sept. 2010.

[8] Spilker, Jr., J. J., *Global Positioning System: Theory and Applications*, chap. 3: GPS Signal Structure and Theoretical Per-

formance, American Institute of Aeronautics and Astronautics, Washington, D.C., 1996, pp. 57–119.

[9] Anon., "Global Positioning System Directorate Systems Engineering and Integration Interface Specification IS-GPS-200F," Tech. rep., 2011, http://www.gps.gov/technical/icwg/.

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

[11] Hein, G., Kneissl, F., Avila-Rodriguez, J.-A., and Wallner, S., "Authenticating GNSS: Proofs against spoofs, Part 2," *Inside GNSS*, September/October 2007, pp. 71–78.

[12] Pozzobon, O., "Keeping the Spoofs Out: Signal Authentication Services for Future GNSS," *Inside GNSS*, Vol. 6, No. 3, May/June 2011, pp. 48–55.

[13] Wesson, K., Rothlisberger, M., and Humphreys, T. E., "Practical Cryptographic Civil GPS Signal Authentication," *NAVIGATION, Journal of the Institute of Navigation*, Vol. 59, No. 3, 2012, pp. 177–193.

[14] Humphreys, T. E., "Detection Strategy for Cryptographic GNSS Anti-Spoofing," *IEEE Transactions on Aerospace and Electronic Systems*, 2011, to be published; available at `http://radionavlab.ae.utexas.edu/detstrat`.

[15] Montgomery, P. Y., Humphreys, T. E., and Ledvina, B. M., "A Multi-Antenna Defense: Receiver-Autonomous GPS Spoofing Detection," *Inside GNSS*, Vol. 4, No. 2, April 2009, pp. 40–46.

[16] White, N., Maybeck, P., and DeVilbiss, S., "Detection of interference/jamming and spoofing in a DGPS-aided inertial system," *Aerospace and Electronic Systems, IEEE Transactions on*, Vol. 34, No. 4, 1998, pp. 1208–1217.

[17] Ledvina, B. M., Bencze, W. J., Galusha, B., and Miller, I., "An In-Line Anti-Spoofing Module for Legacy Civil GPS Receivers," *Proceedings of the ION ITM*, San Diego, CA, Jan. 2010.

[18] Wesson, K., Shepard, D., Bhatti, J., and Humphreys, T. E., "An Evaluation of the Vestigial Signal Defense for Civil GPS Anti-Spoofing," *Proceedings of the ION GNSS Meeting*, Institute of Navigation, Portland, Oregon, 2011.

[19] Dehghanian, V., Nielsen, J., and Lachapelle, G., "GNSS Spoofing Detection Based on Receiver C/No Estimates," *Proceedings of the ION GNSS Meeting*, Institute of Navigation, Nashville, Tennessee, 2012.

[20] Lorenzo, D. S. D., Gautier, J., Rife, J., Enge, P., and Akos, D., "Adaptive Array Processing for GPS Interference Rejection," *Proceedings of the ION GNSS Meeting*, Institute of Navigation, Long Beach, CA, Sept. 2005.

[21] Broumandan, A., Jafarnia-Jahromi, A., Dehgahanian, V., Nielsen, J., and Lachapelle, G., "GNSS Spoofing Detection in Handheld Receivers based on Signal Spatial Correlation," *Proceedings of the IEEE/ION PLANS Meeting*, Institute of Navigation, Myrtle Beach, SC, April 2012.

[22] Lo, S., DeLorenzo, D., Enge, P., Akos, D., and Bradley, P., "Signal Authentication," *Inside GNSS*, Vol. 0, No. 0, Sept. 2009, pp. 30–39.

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

[24] Psiaki, M., O'Hanlon, B., Bhatti, J., Shepard, D., and Humphreys, T., "GPS Spoofing Detection via Dual-Receiver Correlation of Military Signals," *IEEE Transactions on Aerospace and Electronic Systems*, 2012, to be published; available at `http://web.mae.cornell.edu/psiaki/`.

[25] O'Hanlon, B., Psiaki, M., Bhatti, J., and Humphreys, T., "Real-Time Spoofing Detection Using Correlation Between two Civil GPS Receiver," *Proceedings of the ION GNSS Meeting*, Institute of Navigation, Nashville, Tennessee, 2012.

[26] Humphreys, T. E., "Statement on the vulnerability of civil unmanned aerial vehicles and other systems to civil GPS spoofing," `http://homeland.house.gov/sites/homeland.house.gov/files/Testimony-Humphreys.pdf`, July 2012.

[27] Curran, J., Borio, D., Lachapelle, G., and Murphy, C., "Reducing Front-End Bandwidth May Improve Digital GNSS Receiver Performance," *Signal Processing, IEEE Transactions on*, Vol. 58, No. 4, april 2010, pp. 2399 –2404.

[28] Hegarty, C., "Analytical model for GNSS receiver implementation losses," *NAVIGATION, Journal of the Institute of Navigation*, Vol. 58, No. 1, 2011, pp. 29.

[29] Humphreys, T. E., Ledvina, B. M., Psiaki, M. L., O'Hanlon, B. W., and Kintner, Jr., P. M., "Assessing the spoofing threat," *GPS World*, Vol. 20, No. 1, Jan. 2009, pp. 28–38.

[30] Humphreys, T. E., Bhatti, J., and Ledvina, B., "The GPS Assimilator: a Method for Upgrading Existing GPS User Equipment to Improve Accuracy, Robustness, and Resistance to Spoofing," *Proceedings of the ION GNSS Meeting*, Institute of Navigation, Portland, Oregon, 2010.

[31] B.Deshpande, K., Bust, G. S., Clauer, C. R., Kim, H., Macon, J. E., Humphreys, T. E., Bhatti, J. A., Musko, S. B., Crowley, G., and Weatherwax, A. T., "Initial GPS Scintillation results from CASES receiver at South Pole, Antarctica," *Radio Science*, 2012, in preparation after favorable reviews.

[32] O'Hanlon, B., Psiaki, M., Powell, S., Bhatti, J., Humphreys, T. E., Crowley, G., and Bust, G., "CASES: A Smart, Compact GPS Software Receiver for Space Weather Monitoring," *Proceedings of the ION GNSS Meeting*, Institute of Navigation, Portland, Oregon, 2011.

[33] Crowley, G., Bust, G. S., Reynolds, A., Azeem, I., Wilder, R., O'Hanlon, B. W., Psiaki, M. L., Powell, S., Humphreys, T. E., and Bhatti, J. A., "CASES: A Novel Low-Cost Ground-based DualFrequency GPS Software Receiver and Space Weather Monitor," *Proceedings of the ION GNSS Meeting*, Institute of Navigation, Portland, Oregon, 2011.

[34] Pany, T., Riedl, B., Winkel, J., Worz, T., and Schwikert, R., "Coherent Integration Time: The Longer, the Better," *Inside GNSS*, Vol. 4, No. 6, November/December 2009, pp. 52–61.