INVITED PAPER

GNSS Spoofing and Detection

The paper discusses numerous defense strategies ranging from special signal processing within a traditional GNSS receiver to employing advanced encryption-based techniques on GNSS measurements.

By Mark L. Psiaki, *Member IEEE*, and Todd E. Humphreys

ABSTRACT | Global navigation satellite signals can be spoofed by false signals, but special receivers can provide defenses against such attacks. The development of good spoofing defenses requires an understanding of the possible attack modes of a spoofer and the properties of those modes that can be exploited for defense purposes. Sets of attack methods and defense methods are described in detail. An attack/defense matrix is developed that documents which defense techniques are effective against the various attack techniques. Recommendations are generated to improve the offerings of commercial off-the-shelf receivers from the current situation, a complete lack of spoofing defenses, to a situation in which various levels of defense are present, some that add significant security for relatively little additional cost and others that add more security at costs that start to become appreciable.

KEYWORDS | GNSS; GPS; spoofing detection; spoofing

I. INTRODUCTION

Spoofing of Global Navigation Satellite System (GNSS) signals is the broadcast of false signals with the intent that the victim receiver will misinterpret them as authentic signals. The victim might deduce a false position fix, a false clock offset, or both. A coordinated sequence of false position or timing fixes could induce dangerous behavior by a user platform that believed the false fixes. For example, Global Positioning System (GPS) spoofing has been used to send a hovering drone into an unplanned dive [1] and to steer a yacht off course [2].

Spoofing defenses seek to detect an attack in order to warn the victim receiver that its navigation fix and clock offset are unreliable [3]. A second objective of defense is to recover a reliable navigation and timing solution.

Receivers employing receiver autonomous integrity monitoring (RAIM) at the pseudorange level already have a rudimentary defense against spoofing. An inconsistent set of five or more pseudoranges would allow the receiver to detect an unsophisticated spoofer that broadcasts one or more false signals with no attempt to achieve a believable consistency. In 2001, the Volpe report warned of the potential that a sophisticated, subtle form of spoofing might outflank this defense [4].

The GNSS community paid little attention to this threat in the open literature until such a spoofer was developed and successfully tested against a commercial off-the-shelf (COTS) receiver [5]. This combined receiver/spoofer exploits knowledge of the true GNSS signals and knowledge of its location relative to the victim. Its attack strategy captures each receiver channel by aligning its spoofed signal with the true signal for each visible satellite. It starts at low power and ramps its power until it captures the receiver's tracking loops. Afterwards, it smoothly drags the victim off to a false position/timing fix. The sequence of steps enabling capture and drag-off of a receiver's tracking points for a single tracking channel is illustrated in Fig. 1. This figure shows five successive snapshots of the spoofed and spoofed + true pseudorandom number (PRN) code autocorrelation function. This drag-off strategy avoids detection by the receiver tracking loops because they all maintain lock during the entire attack. It avoids detection using simple RAIM techniques because the drag-off falsehoods of each channel—the distances between the truth and spoofed humps in the bottom panel of Fig. 1—are consistent with a false position/timing fix that is prescribed by the spoofer.

Interest in GNSS spoofing has intensified with recent rumors of spoofing "in the wild," i.e., of actual malicious spoofing attacks. Iranian military forces captured a highly

Manuscript received October 15, 2015; revised January 8, 2016; accepted January 18, 2016. Date of publication April 1, 2016; date of current version May 18, 2016. The work of M. Psiaki was supported in part by the National Research Council through a Senior Research Associate appointment at the Air Force Research Lab Space Vehicles Directorate, Kirtland AFB, Albuquerque, NM. The work of T. Humphreys was supported by the National Science Foundation under Grant No. 1454474 and by the Data-supported Transportation Operations and Planning Center (D-STOP), a Tier 1 USDOT University Transportation Center.

M. L. Psiaki is with the Sibley School of Mechanical and Aerospace Engineering, Cornell University, Ithaca, NY 14853-7501 USA (e-mail: mlp4@cornell.edu).

T. E. Humphreys is with the Department of Aerospace Engineering and Engineering Mechanics, University of Texas, Austin, TX 78712-1221 USA.

Digital Object Identifier: 10.1109/JPROC.2016.2526658

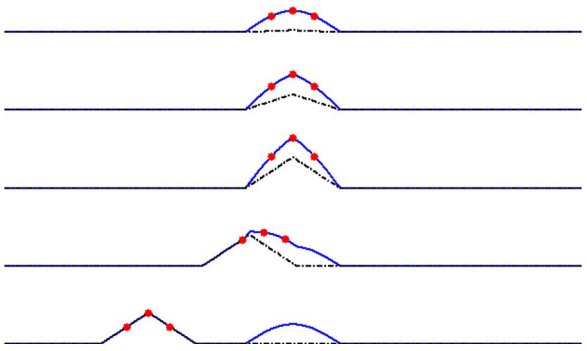

Fig. 1. *Receiver/spoofer attack sequence viewed from a victim receiver channel. Spoofer: black dash-dotted curve; sum of spoofer and truth: blue solid curve; receiver tracking points: red dots.*

classified CIA drone in December 2011. An Iranian engineer involved in the capture claimed that they spoofed the drone into landing in Iran when it thought it was landing at its base in Afghanistan [6]. There have been rumors of spoofing on the Korean peninsula. A scientific satellite has received spoofing-like GPS interference over Ukraine [7]. To date, there have been no confirmed malicious attacks using a coordinated receiver/spoofer like the one described in [5].

Live-signal spoofing attacks have been conducted in controlled tests. The drone attack of [1] and the yacht spoofing of [2] and [3] were all controlled experiments that were conducted to evaluate the threat and possible remedies. Similar tests have been run by the DLR in Germany [8].

Increased concern about GNSS spoofing is being caused by the availability of inexpensive programmable signal simulators that can be used to mount an attack. In June 2015, a fully functional software-defined GPS signal simulator was posted to github, a publicly accessible online software repository. The software can be downloaded and run on a number of general-purpose, low-cost COTS RF generation platforms. A researcher at the University of Bath in the U.K. has downloaded the software and has verified that it works effectively as a spoofer against a standard civil GPS receiver. As illustrated by this example, COTS GNSS signal simulation and record-and-replay devices [9] provide potential platforms for developing a spoofing capability for under $5k.

A variety of potential targets might interest malicious spoofers. In addition to military systems, such as surveillance drones, there are many potential civilian targets. Aircraft or ships could be sent off course while relying on GNSS in low-visibility conditions, perhaps causing an accident. Much civilian infrastructure relies partly or solely on GPS for precise timing. Cell phone towers, power grid monitors, and automated stock trading systems could be knocked offline or cheated. The U.S. Military uses encrypted signals that make properly secured receivers invulnerable to the spoofer of [5], but a technique known as meaconing could be used to mount a spoofing-like attack against such receivers.

Despite the heightened interest in GNSS spoofing since 2008, the authors know of no COTS civilian receiver that can defend against a state-of-the-art attack. Some manufacturers are looking into the problem, but real defenses remain unavailable for purchase. On the other hand, many promising authentication techniques have been developed and demonstrated in the research literature, e.g., [3], [8], and [10]–[16].

This paper makes two principal contributions to the subject of GNSS spoofing and detection. One is a survey of the many attack modes and defense techniques that are under consideration or development. Each is described in moderate detail. The second contribution is a relative assessment of the difficulties of mounting various types of attacks and defenses. Earlier surveys and assessments can be found in [17] and [18]. The authors have been involved in the development of red-team civilian GNSS spoofers and blue-team defenses since early 2008. They hope that this survey and assessment will offer a convenient reference for those endeavoring to secure their receivers and for those developing improved defense methods.

The remainder of this paper consists of four main sections plus a summary and conclusions. Section II presents a spoofer signal model, and it defines and explains a number of spoofer attack strategies. Section III describes a variety of defense techniques. Most of them address only the problem of spoofing detection. Section IV compares attack and defense strategies in a cross-referenced matrix analysis. This analysis indicates which defenses are effective against which attacks, and it attempts to rank the attack and defense strategies in order of increasing costliness. Section V discusses the current status of spoofing defense and suggests paths for developing COTS defenses. Section VI summarizes this paper's contributions and gives its conclusions.

II. GNSS SPOOFING ATTACK METHODS

A. Description of a Spoofing Attack

A spoofer must replicate the RF carrier, PRN/spreading code, and data bits of each open-service GNSS signal that it intends to spoof. A typical received GNSS signal takes the form

$$y(t) = \mathrm{Re}\left\{\sum_{i=1}^{N} A_i D_i[t-\tau_i(t)]C_i[t-\tau_i(t)]e^{j\left[\omega_c t-\phi_i(t)\right]}\right\} \quad (1)$$

where N is the number of constituent spreading-code-specific signals, A_i is the carrier amplitude of the ith signal, $D_i(t)$ is the ith signal's data bit stream, $C_i(t)$ is its

spreading code—often a BPSK PRN code or BOC/PRN code, $\tau_i(t)$ is the ith signal's code phase, ω_c is the nominal carrier frequency, and $\phi_i(t)$ is the ith beat carrier phase.

A spoofer sends a set of false signals that are similar

$$y_s(t) = \mathrm{Re}\left\{ \sum_{i=1}^{N_s} A_{si} \hat{D}_i[t-\tau_{si}(t)] C_i[t-\tau_{si}(t)] \times e^{j\left[\omega_c t - \phi_{si}(t)\right]} \right\}. \tag{2}$$

Nominally $N_s = N$, i.e., the number of spoofed signals equals the number of true signals. Each spoofed signal must have the same spreading code $C_i(t)$ as the corresponding true signal in order to deceive the receiver, and usually it broadcasts its best estimate of the same data bit stream $\hat{D}_i(t)$. The spoofed amplitudes, code phases, and carrier phases are, respectively, A_{si}, $\tau_{si}(t)$, and $\phi_{si}(t)$ for $i = 1, \ldots, N_s$. These quantities are likely to differ from their true counterparts for reasons that are specific to the type of attack that is being mounted, as will be discussed below.

During a spoofing attack, the total signal at the victim receiver antenna is

$$y_{\mathrm{tot}}(t) = y(t) + y_s(t) + \nu(t) \tag{3}$$

where $\nu(t)$ is received noise. In some cases, all of this noise is naturally generated. In other cases, the spoofer contributes a noise component in addition to its fake signals.

B. Self-Consistent Spoofer

Self-consistent spoofers design their attacks to defeat the legacy RAIM strategy that considers pseudorange residuals. They do this by synthesizing their false code phases $\tau_{s1}(t), \ldots, \tau_{sN_s}(t)$ in a way that induces a desired false position/timing fix at the victim receiver while maintaining small pseudorange residuals. The needed calculations to synthesize the false code phase time histories are straightforward. The spoofed beat carrier phases $\phi_{s1}(t), \ldots, \phi_{sN_s}(t)$ are typically designed to vary consistently with the spoofed code phases so that $\omega_c[\tau_{si}(t_b) - \tau_{si}(t_a)] = [\phi_{si}(t_b) - \phi_{si}(t_a)]$ for any two times t_a and t_b and for every spoofed signal i. Otherwise, the victim receiver might take warning from an unusual code/carrier divergence, or it might lose lock on the spoofed signal.

Any good GNSS signal simulator can produce a self-consistent ensemble of spoofing signals. A single-antenna receive-and-rebroadcast device, commonly called a meaconer, can do the same thing.

One of the challenges for a spoofer is to induce the victim receiver to lock onto the false signals. There are two main ways to achieve this goal. One is to start by jamming the victim in order to disrupt normal tracking and induce reacquisition. If the spoofed signals are significantly stronger than the true signals, i.e., $A_{si} \gg A_i$ for $i = 1, \ldots, N$, then the receiver will lock with high probability onto the false signals during reacquisition.

The other method of capturing the victim receiver tracking loops is to transmit the false signals so that they are code-phase- and Doppler-matched to the true signals at the location of the victim antenna. The spoofed power starts low and increases until it suffices to capture the tracking loops. Finally, the spoofer drags off the code and carrier phases in a self-consistent way. This is the attack strategy depicted in Fig. 1. By avoiding the need for jamming and reacquisition, this latter method has a better potential to avoid detection.

Stated mathematically, this second attack strategy starts with $A_{si} \approx 0$ and $\tau_{si}(t) \approx \tau_i(t)$ for $i = 1, \ldots, N$. It maintains each $\tau_{si}(t) = \tau_i(t)$ while it increases each A_{si} until $A_{si} > A_i$ by a sufficient amount to capture the victim receiver's tracking loops, as in the top three panels of Fig. 1. Finally, it drags the victim to a false position/timing fix by moving each $\tau_{si}(t)$ away from the corresponding $\tau_i(t)$ value in a coordinated manner, as in the bottom two panels of Fig. 1.

This second initialization method requires knowledge of the true A_i values and $\tau_i(t)$ time histories for $i = 1, \ldots, N$. Therefore, the spoofer must also be a receiver. Additionally, it must know its geometric relationship to the victim in order to extrapolate from its received amplitude and code phase values to those of the victim.

A receiver/spoofer may relax its requirement for code-phase/carrier-phase consistency during the initial drag-off. If each false A_{si} is only slightly larger than the true A_i, then any beating of the false $\phi_{si}(t)$ against the true $\phi_i(t)$ can lead to distortion of the tracking loop accumulations in the victim receiver. Unusually large variations of the detected amplitude and phase can occur. Such variations might allow an advanced receiver to detect the attack. If $\phi_{si}(t)$ is kept constant relative to the truth value $\phi_i(t)$ during the initial drag-off, i.e., if the spoofed carrier Doppler shift $-\dot{\phi}_{si}(t)$ is kept close to the true Doppler shift $-\dot{\phi}_i(t)$, then large amplitude and phase gyrations can be avoided. After $\tau_{si}(t)$ is sufficiently far from the true $\tau_i(t)$, as in the bottom panel of Fig. 1, $\phi_{si}(t)$ can start varying in a way that respects the usual code-phase/carrier-phase relationship.

Two known self-consistent receiver/spoofers have been built and tested, one by this paper's second author and his group [5] and another by Italian researchers [19]. The latter system uses a very expensive COTS signal simulator. It is likely that similar devices exist that have not been publicly acknowledged or whose publication has not yet been seen by the present authors.

One challenge in developing such a spoofer is the legality of over-the-air live signal testing. The legitimate developer—someone who only wants to stand up a credible "red-team" spoofer in order to evaluate "blue-team" spoofing defenses—needs to respect international sanctions against broadcasting in restricted GNSS bands. One option is to go through the difficult process of gaining official permission, as was done in White Sands, NM, USA, in June 2012 [1] and in Berchtesgaden, Germany [8]. Another option is to operate in international waters at low power and for scientific purposes, as in the yacht tests [2], [3]. It is legal anywhere to add spoofer signals into a coaxial antenna output cable via RF combiner. This method has proved useful for testing defenses that do not rely on special antenna properties, antenna motion, or multiple antennas.

C. Meaconing and Estimate-and-Replay Attacks

The spoofers described in Section II-B must recreate the transmitted spreading code $C_i(t)$ and the transmitted data bit stream $D_i(t)$, which are easy to synthesize if they are perfectly predictable. If either $C_i(t)$ or $D_i(t)$ is not fully predictable, then to mount its attack, the spoofer must synthesize approximate replicas of $C_i(t)$ and $D_i(t)$ "on the fly" based on noisy received versions of them.

The U.S. GPS includes military signals that have encrypted spreading codes, the legacy P(Y) code and the new M code. These codes can be predicted only with a secret encryption key. A secure military receiver has the necessary key, but a spoofer presumably does not.

Even if $C_i(t)$ is known, certain systems may include unpredictable low-rate bit transmissions in their $D_i(t)$ modulation. Another type of security-enhanced signal is one in which short segments of $C_i(t)$ are unpredictable. Proposed enhancements to civilian GNSS signals have such unpredictable features [13], [20]. For a spoofing attack to remain undetected, it might be necessary for the spoofer to transmit these features correctly.

One of the options for a spoofer in such situations is to perform meaconing. Meaconing records the true GNSS signals, as in (1), and replays the signals through a transmitter with enough gain to overwhelm the true signal at the victim antenna. A meaconer has the potential to spoof any GNSS signal, even an encrypted military signal.

The simplest meaconer/spoofer uses a single reception antenna. Its spoofed code phase time histories, $\tau_{si}(t)$ for $i = 1, \ldots, N$, are the true values for its reception antenna plus an additional time delay for its own processing and for the signal time of flight from its transmission antenna to the victim receiver antenna. In this situation, $\tau_{si}(t) > \tau_i(t)$ for $i = 1, \ldots, N$. The victim receiver's false position fix will be that of the spoofer's reception antenna. Its false clock fix will deduce a false time that will be earlier than true time, e.g., it might deduce a time of 8:59:59.999 when the time is actually 9:00:00.000.

A more sophisticated meaconer might use multiple receiver antennas and phased-array signal processing. Individual record-and-replay channels could point increased gain at individual GNSS satellites and could implement independent delay variations. Such a system could independently steer the relative delays of its false transmissions to construct $\tau_{si}(t)$ time histories that produce any conceivable false position fix. Such a meaconer must still obey $\tau_{si}(t) > \tau_i(t)$ for $i = 1, \ldots, N$. This constraint induces constraints on the relationship between the spoofed clock fix and the spoofed position fix.

If the unpredictable part of the signal lies only in the low-rate $D_i(t)$ bits, then it may be possible to accomplish spoofing without meaconing. Instead, a spoofer could use a Security Code Estimation and Replay (SCER) attack [21]: The spoofer estimates the unpredictable $D_i(t)$ bits, and it broadcasts them as soon as it has reliable estimates. Prior to broadcasting them, it can broadcast a random guess of these bits or its own poor best estimate. Alternatively, it could restrict itself to use only delays in its spoofed code phases, as with the meaconer, i.e., it could enforce $\tau_{si}(t) > \tau_i(t)$ for $i = 1, \ldots, N$. Its minimum delay could be chosen to ensure that it could transmit accurate estimates of all unpredictable $D_i(t)$ bits. Such a system allows the spoofer to use arbitrary relative delays between the different spoofed channels. Unlike the meaconer, it would not need to use a multielement receiver antenna with independently steerable gains in order to induce an arbitrary spoofed location.

An SCER attack is more difficult to mount against a fully encrypted spreading code or against encrypted short segments of spreading codes. It may require increased receiver antenna gain. It will certainly require much more signal processing in order to achieve a reasonable probability of correct chip estimation for chips that arrive at a fast rate. On the plus side, an SCER attack against a spreading code need not estimate each unknown chip with a very high probability of correctness. The SCER spoofer can compensate for a reduced probability of correct chips by increasing its output power—provided its probability of correct chip estimation is significantly greater than 50%.

D. Advanced Forms of Spoofing

Advanced forms of GNSS spoofing have been conceived in response to efforts to defend against spoofing. These advanced methods defeat various defense strategies that have been developed to deal with self-consistent spoofing.

One advanced technique is called nulling. The spoofer transmits two signals for each spoofed signal. One is the spoofed version that acts in concert with all other spoofed signals in order to induce a false position/timing fix. The other is the negative of the true signal. Thus, $N_s = 2N$. Suppose that the first N signals are the spoofed versions and that the last N are the nulling versions.

Then, $C_{i+N}(t) = C_i(t)$ and $\hat{D}_{i+N}(t) = D_i(t)$ for $i = 1, \ldots, N$. The last N signals must cancel the true signals at the receiver. Therefore, they must obey $A_{s[i+N]} = A_i$, $\tau_{s[i+N]}(t) = \tau_i(t)$, and $\phi_{s[i+N]}(t) = \phi_i(t) + \pi$ for $i = 1, \ldots, N$. Cancellation occurs because of the 180° (π radians) carrier phase shift.

Nulling erases all traces of the true signal from the total received signal $y_{\text{tot}}(t)$ of (3). Various defenses look for signs that there are two signals ostensibly from the same satellite. They may look for distinct signals that have sufficient spreads between their code phases $\tau_i(t)$ and $\tau_{si}(t)$ or between their carrier Doppler shifts $-\dot{\phi}_i(t)$ and $-\dot{\phi}_{si}(t)$. Alternatively, they may look for interfering signals that have similar code phases and carrier Doppler shifts. In either case, nulling will remove all telltale signs of duplicate signals. Spoofing defenses that depend on these signs will fail.

Nulling is difficult. It is straightforward to achieve adequate code-phase alignment between the true signal and the nulling signal, but exact carrier phase alignment and amplitude matching are more difficult. Exact nulling requires calibration of various physical parameters. These include the spoofer's antenna gain and phase patterns, its RF mixing signal phases, and its filter delays, both in its reception path and in its transmission path. The second author's group has studied this problem experimentally and has found the calibration challenges to be surmountable. A valuable aid to calibration can be a second spoofer reception antenna. This antenna is situated within the gain pattern of the spoofer's transmission antenna. It is used to conduct online testing of the nulling efficacy of the calibration parameters.

An exotic type of nulling attack uses only nulling signals, ones with twice the amplitudes of the corresponding true signals. It turns on each signal only during data bits $D_i(t)$ whose polarity it seeks to reverse. The spoofer induces a false position/timing fix by providing false satellite ephemerides and clock calibration data instead of false pseudoranges. An advantage of this type of nulling attack is that it requires half as many spoofing channels as does a general nulling attack.

As mentioned, a stealthy receiver/spoofer needs to know its geometry relative to the victim receiver in order to place each initial code phase $\tau_{si}(t)$ on top of the corresponding true code phase $\tau_i(t)$. It may be necessary for the spoofer to ensure that a high-pass-filtered version of each false beat carrier phase $\phi_{si}(t)$ is the same as a high-pass-filtered version of the corresponding true beat carrier phase $\phi_i(t)$. This matching may need to be maintained throughout the spoofing attack in order to defeat certain types of defenses. If so, then the spoofer must employ a high-bandwidth sensor of the relative motion between its transmission antenna and the victim receiver's antenna. This sensor's outputs will be needed in order to synthesize the correct high-bandwidth variations of each $\phi_{si}(t)$.

An advanced spoofer acting against a multiantenna victim receiver might use multiple independent spoofer transmission antennas and match each one to a corresponding receiver antenna. The relative geometry of each spoofer/victim antenna pair would need to be known. Also, the spoofer would need to be sufficiently close to the victim and have sufficiently narrow individual antenna gain patterns so that each victim antenna received only the signal from the intended spoofer antenna. Such a technique would enable the spoofer to control the differences between each satellite's spoofed beat carrier phase time history, each $\phi_{si}(t)$, as received at the different victim antennas. This type of spoofing would likely be practical only with a cooperative victim, such as a fishing boat whose crew was intentionally spoofing its GNSS tracker in order to poach undetected in restricted waters.

An expensive type of multiantenna spoofer might transmit only one spoofed signal from each antenna. Such a spoofer might deceive spoofing defenses that were based on signal direction of arrival. It might need to distribute its antennas about the victim so that the spoofed signal arrival directions would seem physically reasonable to the victim's detection system. As will be discussed in Section III, certain spoofing detection methods monitor the signal arrival directions. They declare a spoofing attack if all of the arrival directions are identical or if they are unrealistic in some other manner. The difficulty of mounting an attack from multiple directions would make this type of spoofer expensive and cumbersome. All the most advanced spoofing methods tend to involve increased costliness and complexity.

A stealthy spoofing attack should not attempt to alter the victim's position or timing fix too rapidly. Otherwise, the attack may be recognized by the unphysical nature of the changes. As an extreme example, one test-case spoofing attack against a cruising yacht ramped its speed up above 900 kn and its altitude down to 23 km below sea level. Furthermore, the yacht's spoofed course made landfall beneath Italy and again beneath Sicily [3]. The crew on the bridge easily detected the attack because the yacht could not cruise above 16 kn, and it was not properly equipped to burrow under land masses at any speed.

A victim receiver may be able to detect physical unrealism in seemingly subtle attacks. For example, a ship's magnetic compass reading, if combined with known possible levels of compass error, sea currents, and winds, can be used to restrict the believable GNSS-derived heading to a narrow range. If a spoofer tries to induce too great a heading falsehood, then the compass will enable the crew to detect the unreliability of the GNSS fix. An inertial measurement unit (IMU) can serve to further bound the possible rate of growth of a spoofer's false navigation fix. Suspicions will be raised by a rate of growth too high to be explained by typical IMU drift

levels. The same goes for growth in the spoofed receiver clock offset. Spoofing will be suspected if the clock offset grows too rapidly to be explained by the expected levels of clock drift for the receiver's given oscillator type.

The requirement of physical reasonableness forces the spoofer to be patient. Such patience was employed in the less dramatic yacht spoofing tests that are reported in [2]. The amount of patience required of the spoofer in building up a false position fix depends on the characteristics of the intended victim receiver and on any potential aiding that it might have from external sensors or *a priori* information.

E. Spoofing of a Cooperative Victim

The intended victim may have cause to aid the spoofer. This is the case when GNSS position is used to enforce compliance with laws, court orders, or company policy. For example, a fishing boat captain might want his GNSS receiver to falsely report that he had stayed out of restricted fishing grounds when he had been poaching. A criminal under house arrest with a GNSS ankle monitor might want the monitor to show him safely at home when he was fleeing to another country.

With a complicit victim, it becomes easier for the spoofer to mount certain types of attack scenarios listed above. It is very easy for the attacker to know its geometry relative to the victim antenna; it can be measured with a physical scale. Nulling of the true signal can be achieved simply by placing a metal can over the victim antenna—with the spoofer transmission antenna inside the can. A multi-transmission-antenna spoofer attack can be mounted with a small array of antennas near the victim. If the victim antenna output cables are accessible to the spoofer, then an equivalent attack can be mounted via direct electrical connection into those wires. The attacker would synthesize special differences between the spoofed signals sent to each array element wire.

In order to defend against a cooperative spoofer, the interested downstream user of the victim GNSS receiver must ensure that the receiver has various levels of physical security. These could include a tamper-resistant antenna and antenna output wire. If the spoofing defense employs multiple antennas, then an opaque tamper-resistant radome should cover the array in order to conceal the antennas' relative geometry and to prevent attachment of an individual spoofing antenna to each receiving antenna element.

III. SPOOFING DEFENSE TECHNIQUES

A spoofing defense is the detection of an attack followed by authenticated recovery of the true position/timing fix. Like most of the work and results in the literature, this section concentrates on various strategies for the detection part of the spoofing defense problem.

Much less work has been done on the problem of recovery after an attack. Work on the recovery phase has been conducted by the group that produced [8]. In addition, this paper's first author has demonstrated an offline ability to recover the true signals from wideband recordings of some of the attacks that are reported in [3]. Much more work needs to be done on the navigation recovery problem, and that subject will be left to future efforts. It should be noted, however, that it is impossible to recover GNSS navigation in two scenarios. One is an attack that includes nulling of the true signals. Its cancellation of the signals precludes their use. The other is an attack where the spoofer is very high-powered and effectively jams the true signals to the point where they are unrecoverable. They will be particularly hard to recover if the spoofing saturates the victim receiver's RF front end.

The present survey of spoofing defense methods does not deal with the legacy pseudorange-based RAIM defense. It is too weak against modern spoofers to justify a description.

All receiver-based spoofing detection strategies rely on one or the other of two methods, possibly on both. One method is to look for differences between the spoofed signals and the true signals, differences that can be detected by the intended victim receiver. Despite the public definition of civilian GNSS signals, there are usually noticeable differences of spoofer signals unless the spoofer is sophisticated and expensive. The other method is to look for interaction between the true and spoofed signals. Interaction is unavoidable for the spoofer except in two situations. One is a nulling attack. The other situation is a vastly overpowered attack. An overpowered attack, however, has an obvious difference from the expected power levels of true signals. Thus, good detection strategies are typically multipronged, e.g., combining power monitoring with some form of interaction monitoring.

A. Advanced Signal-Processing-Based Techniques for a Single-Antenna Receiver

There are several spoofing detection techniques that can be implemented entirely as advanced signal processing algorithms within an otherwise standard GNSS receiver. One set of techniques looks for distortions or disruptions that typically occur during signal drag-off. The simplest of these techniques looks for sudden unreasonable jumps in the received carrier amplitude A_i, beat carrier phase $\phi_i(t)$, or code phase $\tau_i(t)$. A quick increase in A_i or unusual jumps in $\phi_i(t)$ or $\tau_i(t)$ might occur at the onset of an attack.

Received power monitoring (RPM) looks at the total received power on an absolute scale. This requires looking at all the received A_i values and at the receiver RF front end's automatic gain control (AGC) setpoint [22]. The total power might suddenly increase at the

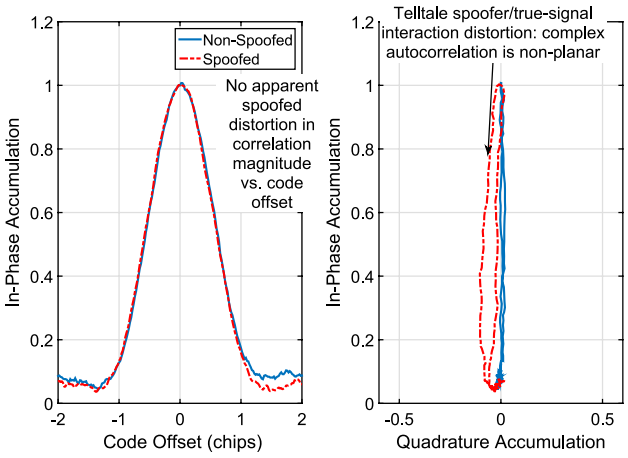

Fig. 2. *Two 2-D views of the 3-D unspoofed (blue) and spoofed (red) complex correlation function.*

onset of an attack if the spoofer required a substantial power advantage, $A_{si} \gg A_i$ for all $i = 1, \ldots, N$. Thus, a sudden power jump could indicate an attack, especially if the increase were more than 1 or 2 dB. A related method eliminates retrieval of the AGC setpoint in order to simplify the hardware [14], but it is vulnerable to an overpowered attack that includes noise-floor spoofing.

Another technique looks in detail at the complex correlation function from which a receiver synthesizes discriminators for its tracking loops. During the initial drag-off of a spoofing attack, misalignments between the true and spoofed code and carrier phases result in distorted autocorrelation functions. Two views of two complex correlation functions are depicted in Fig. 2 for nonspoofed (blue) and spoofed (red) signals. The nonspoofed complex in-phase magnitude plotted along its code offset axis is a rounded version of the triangular auto-correlation function that is typical of a BPSK PRN code; this is represented by the blue curve in the left-hand plot. The rounding is the result of filter distortion in the receiver RF front end. The in-phase (I)/quadrature (Q) view of this same curve in the right-hand plot shows that it lies along a single line in the (I, Q) plane, as expected. The interaction of a second spoofed signal with this signal will distort this picture. In the case of Fig. 2, the distortion lies mostly in the (I, Q) plane: Note how the red curve in the right-hand plot is clearly not restricted to a single line. The red curves in the two plots of Fig. 2 are taken from a specific instant of the drag-off portion of an actual live-signal spoofing attack that is reported in [3]. Had they been plotted at a different instant, the distortion would have been in the left-hand I (magnitude) versus code offset plot. The distorted left-hand plot might have looked similar to the blue curve on the fourth panel of Fig. 1.

It is possible to modify a typical GNSS receiver to look for such distortions of the correlation function [16]. The main requirement is to calculate additional complex base-band correlations between the receiver's signal replica and the received signal. These correlations would be calculated at an expanded set of delays along the code offset axis.

The detection method that looks at the complex correlation function has two unique drawbacks. First, natural multipath signals produce similar results. Before issuing an alarm, a spoofing detector would need to verify that the observed distortion was not explainable as mere multipath. The second problem is this method's poor performance if the spoofer greatly overpowers the true signal, i.e., if $A_{si} \gg A_i$. In this case, very little distortion occurs because, with reference to Fig. 1, the true signal is too much smaller than the black spoofed signal, and the blue total correlation curve looks nearly like a planar triangular function. Of course, the increased spoofer power needed to avoid distortion could be exploited by the RPM detection method in order to sound an alarm in this case.

Another challenge for this class of detection strategies is the transient nature of their applicability. The distortion shown in Fig. 2 occurs only during the initial drag-off. After drag-off is complete, the spoofed signal is too far from the true signal for distortion to be evident. This is the situation shown in the bottom panel of Fig. 1. Note that the horizontal axes in all five panels of Fig. 1 are analogous to the code offset axis in the left-hand panel of Fig. 2. Observable glitches also disappear after drag-off, and the spoofer is free to lower its power after drag-off. Thus, all of these methods could miss their opportunities to detect an attack if they failed to detect it during drag-off.

One signal-processing-based detection technique can work long after drag-off. This technique constantly attempts to reacquire all of its tracked signals. It performs a brute-force search for each signal over the entire range of possible code phases and carrier Doppler shifts. A brute-force acquisition search places a heavy signal processing load on a receiver. One reasonable strategy is to search sequentially for additional instances of the tracked signals, one signal at a time. If a second version of any received signal is detected, then a spoofing alarm is issued. Afterwards, the receiver reverts to an initial acquisition mode and detects all instances of all signals via brute-force search. The receiver then attempts to sort out the true signal versions from the spoofed ones in hopes of recovering its navigation functionality.

Even this last technique could be defeated by an overly powerful spoofer. Part of its effect could be to jam the true signals, making them undetectable during the reacquisition search. Of course, such a spoofer should be detectable by using the RPM method.

B. Encryption-Based Defenses

There are various means to use encryption in order to create unpredictable parts of the transmitted signals that are difficult for the spoofer to produce short of a meaconing attack. The strongest defense is a symmetric key encryption of the full spreading code $C_i(t)$. The transmitting GNSS satellite and the secure receiver both have copies of a secret key. This method is cumbersome to use because it requires a secure means of distributing keys to receivers.

Symmetric-key-encrypted GNSS signals can be used to detect spoofing in civil GNSS receivers without the need for access to the secret key [10], [11]. Instead of distributing keys to civilian receivers, the known relationship of an open-service civilian spreading code to an encrypted military code is exploited. In GPS, they are modulated in quadrature on the same carrier. The receiver uses its civilian code tracking system to record a noisy base-band version of the encrypted code. This is done at a potential victim receiver and at another receiver that is known to be secure from spoofing. The two noisy versions of the encrypted code are then cross-correlated to look for the correlation peak that would exist if the signals in the potential victim were authentic. If the correlation peak is high, then the signals are declared authentic; otherwise, a spoofing alarm is issued. This system can operate after the fact or nearly in real time if a high-bandwidth communications link is available between the receivers [11].

A delayed symmetric key encryption method can provide a defense for civilian receivers. It interleaves short segments of a symmetric-keyed Spread Spectrum Security Code (SSSC) with long segments of predictable spreading codes in $C_i(t)$ [20]. The receiver uses the known portions to track the signal, and it records the unknown portions. A short time after the unpredictable SSSC has been broadcast, a key arrives in the $D_i(t)$ data that can be used to generate the SSSC. The key is digitally signed so that it can be confidently traced to the relevant GNSS control segment. Once verified, the key is used to synthesize the unknown spreading code, and the receiver correlates this code portion with its recorded signal portion in order to verify signal authenticity. This system involves significant latency of its detections while it waits for the full digital signatures, perhaps seconds to minutes of latency.

An asymmetric private-key/public-key approach provides another means of using encryption to detect a spoofing attack against an open-service civilian system. In this approach, a subset of the broadcast data stream $D_i(t)$ contains an unpredictable digital signature generated using the control segment's private key. This signature signs the rest of the data in $D_i(t)$. The receiver knows where to expect these bits in the demodulated data stream. It collects the full number needed to check the signature, which it verifies using the known public key. This method is known as Navigation Message Authentication (NMA) [13], [20]. As with the SSSC defense, this method involves latency from seconds to minutes in order to verify the signal's authenticity. The amount of latency is driven by the need for a sufficiently long signature and limitations on the number of available bits in a typical $D_i(t)$ data stream.

Implementation of the delayed-symmetric-key SSSC method and the asymmetric private-key/public-key NMA method both require modifications to the satellite signals. This is difficult or impossible for existing GNSS satellites and expensive for future satellites, especially if it involves significant changes to the $D_i(t)$ data stream in order to enable the transmission of enough bits to support the technique.

By contrast, no signal changes are needed to implement the technique that uses cross-correlation of unknown encrypted military signals between two receivers. This method does require new infrastructure in order to be used in COTS systems. It needs a network of secure receivers to generate noisy "truth" versions of the encrypted codes. It also requires a secure communications network to bring the authentic and unverified versions of the encrypted codes to a common signal processing unit that can perform the needed correlation to check signal authenticity.

The NMA defense may require an additional technique in order to deal with an SCER-based attack in which the spoofer rapidly estimates the unpredictable bits of the $D_i(t)$ data stream. If the spoofer does not use enough latency in its attack, then the initial portions of its transmissions of unknown $D_i(t)$ bits will contain errors about half the time. A victim receiver can implement detection tests that look for this initial uncertainty of the unpredictable $D_i(t)$ bits [21]. If it sees enough unusual behavior at the initial portions of these bits, then it issues a spoofing alarm. The spoofer's only means of counteracting this defense is to use a longer latency in its code offset, which exposes it to detection by a timing consistency check.

C. Defenses Based on Drift Monitoring

This category of defense looks for unusual changes in the receiver position or clock fix. If the spoofer causes the receiver clock error to change too rapidly, then the victim receiver can detect that the rate of clock drift is larger than is reasonable for its class of oscillator. Depending on the class of oscillator, e.g., temperature-compensated crystal oscillator, ovenized crystal oscillator, Rubidium oscillator, Hydrogen maser, etc., the spoofer might find itself more and more constrained. Otherwise, the victim will notice the unusual drift and issue a spoofing alarm.

An IMU or some other motion sensor can be used to place similar constraints on reasonable rates of drift of a position fix. Even the rolling constraint of a vehicle and

the known maxima of its velocity, acceleration, and turn rate could be used to check for excessive drift. As with clock drift, the victim receiver will issue a spoofing alarm if an unrealistic motion profile is detected.

As noted in Section II-D, a patient spoofer could build up the victim's false clock offset and false position fix slowly and avoid being detected by a drift monitor. A slow build-up, however, might make it vulnerable to detection by other means.

This type of defense may be especially useful against a meaconer or against an SCER attack on an NMA signal. Both types of attack must respect the delayed spoofing constraint $\tau_{si}(t) > \tau_i(t)$ for all $i = 1, \ldots, N$. This delay induces one of two situations, possibly both: Either the victim receiver's time fix is earlier than actual true time, or the receiver's position fix is further away from the average satellite location, e.g., at a lower altitude in typical terrestrial scenarios. Therefore, it will be impossible for the spoofer to maintain both a low initial clock offset and a low initial position offset if there is a minimum amount by which the spoofed signals are delayed from the true signals. One or both of these quantities will exhibit an unreasonably large jump in the victim receiver, thereby giving it an opportunity to detect the attack.

D. Signal-Geometry-Based Defenses

Another class of spoofing defenses monitors the direction of arrival of the signals by considering the received beat carrier phase. The beat carrier phase can be modeled as

$$\frac{\lambda\phi_i}{2\pi} = \rho_0^i + (\hat{\boldsymbol{\rho}}^i)^T \Delta\boldsymbol{d} + c(\delta_r - \delta^i) + \frac{\lambda\beta^i}{2\pi} \qquad (4)$$

where λ is the signal's carrier wavelength, ρ_0^i is the nominal range to the ith satellite, $\hat{\boldsymbol{\rho}}^i$ is the unit vector that points from the satellite to the receiver, $\Delta\boldsymbol{d}$ is the displacement of the receiving antenna from the nominal receiver location, δ_r and δ^i are the respective receiver and satellite clock offsets, and β^i is the unknown carrier phase bias.

A receiver can use interferometry to measure the direction-of-arrival vector $\hat{\boldsymbol{\rho}}^i$ by using three or more antennas with different $\Delta\boldsymbol{d}$ offsets [8] or by using a single antenna that undergoes a known $\Delta d(t)$ motion profile [12]. If only two antennas are used, or if a 1-D $\Delta\boldsymbol{d}(t)$ profile is used, then it will be impossible to estimate all three components of $\hat{\boldsymbol{\rho}}^i$, but at least one component will be estimable [3], [12].

A well-designed receiver typically can measure ϕ_i to an accuracy of about 1/40th of a cycle. This allows a receiver to measure $\hat{\boldsymbol{\rho}}^i$ to an accuracy of about 3° using only a short baseline of $\Delta\boldsymbol{d} = 0.1$ m.

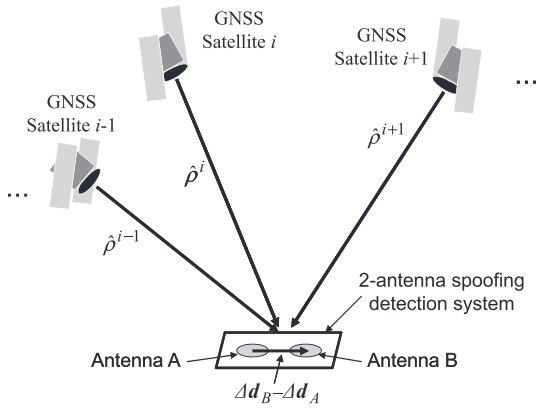

Fig. 3. *Typical signal arrival geometry for a nonspoofed case and a two-antenna-based spoofing detection system.*

In a nonspoofed case, the $\hat{\boldsymbol{\rho}}^i$ direction vectors are distributed about the sky, as depicted in Fig. 3. The simplest spoofer will broadcast all of its signals from the same direction. A typical geometry-based spoofing detection system tests whether the received ϕ_i phases at the multiple antennas are more consistent with the diversity of $\hat{\boldsymbol{\rho}}^i$ directions expected for authentic signals or with the uniformity of directions consistent with single-transmitter spoofing. The calculations for the nonspoofed hypothesis include an attitude determination algorithm [3], [8], [12]. One such system has demonstrated real-time spoofing detection aboard a cruising yacht [3].

Some methods do not directly estimate $\hat{\boldsymbol{\rho}}^i$ or any of its components. One such method uses an IMU on an aircraft [23]. In effect, motions induced by controls and winds produce a $\Delta\boldsymbol{d}(t)$ time history that can be sensed by the IMU but that is difficult for the spoofer to predict. If corresponding high-frequency variations consistent with each $\hat{\boldsymbol{\rho}}^i$ direction are absent from each $\phi_i(t)$, then a spoofing attack is indicated.

A related approach uses multiple feeds of a single patch antenna to make certain properties of each received signal sensitive to the corresponding direction vector $\hat{\boldsymbol{\rho}}^i$ [15]. If all signals display the same response, then uniformity of the $\hat{\boldsymbol{\rho}}^i$ directions has been detected, and a spoofing alarm is declared.

A spoofer that transmits from multiple directions is harder to detect using such methods. If its directional diversity does not equate to that of the true set of $\hat{\boldsymbol{\rho}}^i$ vectors, then it may be detectable. The research group that produced [8] has developed a capability to detect such attacks.

E. Multipronged Spoofing Defense Strategies

Many of the spoofing detection strategies have weaknesses that might be exploited by a sophisticated spoofer. In some cases, the strength of one strategy might offset the weakness of another. Thus, the simultaneous use of

two or three complementary strategies might provide a very powerful means to detect spoofing.

A spoofer may elect to use $A_{si} \gg A_i$ in order to avoid an obvious distortion of the complex correlation function during drag off, as shown in Fig. 2. If a spoofing defense examines the complex correlation at many code phases while implementing RPM, then it can detect the onset of the attack regardless of how much power the spoofer uses. If clock offset drift rate and position drift rate are also monitored, then the spoofer will be forced to perform a slow drag-off, thus giving the victim receiver more time to detect a distortion of the complex correlation function or too high a received power level.

Another useful combined strategy might employ the unpredictable data bits of NMA, monitoring of distortion of those bits, an IMU, and clock drift monitoring. The IMU and clock drift monitoring will force the spoofer to initiate its attack slowly in order to avoid detection by inducing unreasonably large drifts in the position or timing fixes. This limitation will prevent the build up of dangerous position or timing errors during the latency period of NMA-based spoofing detection. If the spoofer implements an SCER attack in order to estimate and replay the unpredictable NMA bits, then the victim will be able to detect the initial uncertainties of those bits because the clock drift monitoring will limit the spoofer's initial ability to use a delay that would allow reliable estimation of a bit prior to the start of its broadcast.

IV. SUMMARY COMPARISON OF ATTACK AND DEFENSE STRATEGIES

Not all defenses are equally good against all modes of attack and vice versa. Not all defenses or modes of attack are equally costly to implement. On the threat side, it seems obvious that a less expensive mode of attack—less expensive in terms of the required equipment and expertise—is also a more likely mode of attack. Thus, a receiver designer would like to use the least expensive techniques that defend against the greatest number of inexpensive attack modes. Depending on the needed security of the application and on the receiver cost budget, the designer may elect to defend against additional attack modes.

In order to provide guidance to receiver developers, an attempt has been made to rank the various attack modes and defense techniques discussed in this paper according to relative cost. For both attacks and defenses, "cost" is a subjective term that attempts to include all of: 1) the cost of developing or buying the hardware; 2) the expertise required to set it up and run it; and 3) and the complexity of operating it. Table 1 offers this summary ranking, with attack and detection techniques ordered by increasing cost from left to right (attack) and from top to bottom (detection). The matrix entries indicate either high, intermediate/case-dependent, or low detection probability for the corresponding attack/detection pair.

Some of the 13 detection techniques listed in Table 1 are multipronged methods, e.g., D2, D5, D7, and D9. This is not an exhaustive list of all sensible combinations. These combinations are representative of good complementary strategies.

Detection methods D2–D9 might be implementable by a firmware update with no extra hardware. They might be relatively inexpensive for retrofitting an existing system. Methods D3, D5, and D8 might require extra signal processing hardware in receivers that compute only the minimum number of correlation accumulations per tracking channel.

As an example of how to interpret Table 1, consider it from the perspective of a manufacturer of low-cost GNSS receivers who wishes to harden his receivers against spoofing. Owing to cost constraints, the manufacturer may only consider the top seven or so rows in the table. Among these, he wishes to find a detection technique, or combination thereof, that offers a useful probability of detection against the lowest-cost (highest likelihood) attacks—say, those in the table's first five columns. The manufacturer observes that technique D3, correlation function distortion monitoring, offers at least intermediate protection against all five of the lowest-cost attacks. If he can afford additional measures, the manufacturer may decide to combine D3 with D7 to improve resistance against attacks A2 and A3. A manufacturer of a high-quality receiver meant to operate in adversarial environments may instead decide to implement techniques D9 and D10 to achieve a high probability of detection for all attacks but A11, for which he could offer intermediate protection. Of course, the choice of D7 or D9 assumes that the SIS includes an NMA component.

The costliness of key distribution of current and future symmetric-key SSSC (D13) military spoofing defenses is well known. It has prompted consideration of alternative techniques for hardening military receivers against spoofing [24].

V. CURRENT STATUS AND PRACTICAL WAYS FORWARD

The salient feature of the current status of spoofing and defense is the complete lack of defenses in COTS receivers for civilian signals. It is a valid question to ask whether this needs to change given that there remains no conclusive evidence that "spoofing in the wild" has ever happened or ever will occur. It seems wise, however, to "lock the barn" even before any "horses are stolen"—provided that the lock's cost is not exorbitant.

Therefore, it is recommended that some low-cost spoofing defense methods be implemented in commercial products to provide a measure of security in the near to medium term. One obvious inexpensive method to

Table 1 Cost-Ranked Matrix of GNSS Spoofing Attack and Detection Techniques

Detection	Attack Techniques												
Techniques	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12	A13
D1	X	X	X	X	X	X	X	X	X	X	X	X	X
D2	∼	✓	X	X	∼	X	X	X	X	X	X	X	X
D3	∼	∼	∼	∼	∼	X	X	∼	∼	∼	∼	X	X
D4	∼	✓	∼	∼	∼	∼	∼	∼	∼	∼	∼	∼	∼
D5	✓	✓	✓	✓	✓	∼	∼	✓	✓	✓	✓	∼	∼
D6	X	✓	✓	X	X	✓	X	✓	✓	X	X	✓	X
D7	X	✓	✓	∼	X	✓	∼	✓	✓	∼	X	✓	∼
D8	X	✓	✓	∼	X	✓	∼	✓	✓	∼	X	✓	∼
D9	∼	✓	✓	✓	∼	✓	✓	✓	✓	✓	∼	✓	✓
D10	✓	✓	✓	✓	✓	✓	✓	✓	∼	∼	∼	∼	∼
D11	✓	✓	✓	✓	✓	✓	✓	X	∼	∼	∼	∼	∼
D12	X	✓	✓	∼	X	✓	∼	✓	✓	∼	X	✓	∼
D13	X	✓	✓	∼	X	✓	∼	✓	✓	∼	X	✓	∼

Detection probability matrix keys: ✓ – high, ∼ – intermediate or case-dependent, X – low

	Detection Techniques Key		Attack Techniques Key
D1	Pseudorange-based RAIM	A1	Meaconing, single RX ant., single TX ant.
D2	Observables and RPM	A2	Open-loop signal simulator
D3	Correlation function distortion monitoring	A3	RX/SP, single TX ant., no SCER
D4	Drift monitoring (clock offset, IMU/position)	A4	RX/SP, single TX ant., SCER
D5	Observables, RPM, distortion, and drift monitoring	A5	Meaconing, multi. RX ants., single TX ant.
D6	NMA*	A6	Nulling RX/SP, single TX ant., no SCER
D7	NMA* and SCER detection	A7	Nulling RX/SP, single TX ant., SCER
D8	Delayed symmetric-key SSSC*	A8	RX/SP, single TX ant., sensing of victim ant. motion
D9	NMA*, SCER detection, RPM, and drift monitoring	A9	RX/SP, multi. TX ants., no SCER
D10	Multiple RX antennas	A10	RX/SP, multi. TX ants., SCER
D11	Moving RX antenna	A11	Meaconing, multi. RX ants., multi. TX ants.
D12	Dual-RX keyless correlation of unknown SSSC codes	A12	Nulling RX/SP, multi. TX ants., no SCER
D13	Symmetric-key SSSC* [e.g., P(Y) equiv.]	A13	Nulling RX/SP, multi. TX ants., SCER

* Detection techniques requiring changes to the Signal In Space (SIS); TX: Transmitter; RX: Receiver; RX/SP: Receiver-Spoofer

implement is RPM. Clock drift monitoring and scanning for strange jumps in observables are close seconds to RPM. These defenses could be implemented with only minor receiver modifications.

The next most reasonable defense is to monitor the complex correlation function for distortions that are not explainable as simple multipath. This modification would also be done entirely in the receiver. It may be more expensive, however, because extra correlation channels may be required. This could involve extra silicon, weight, power, and cost in an upgraded receiver. A related upgrade would be to continuously look for additional correlation peaks of a given spreading code that are distant from a given tracked signal in code phase and in carrier Doppler shift. This involves many brute-force acquisition calculations. If they were run on a receiver's spare MIPS, perhaps one signal at a time, then the added receiver expense might not be too great. Using fast Fourier transform (FFT)-based acquisition methods might help some receivers to implement such a defense more efficiently.

A next level of defense is to include unpredictable NMA bits in the $D_i(t)$ data stream. This could be much more costly because it could involve upgrading the SIS, which means upgrading the GNSS satellites. The European Galileo system is considering NMA and seems to be leaning towards implementing it. This will be more of a challenge for the U.S. GPS because receiver manufacturers would want it on the L1 civilian signal. There are not enough spare bits in the legacy C/A navigation data stream to implement NMA. Therefore, NMA would have to be part of the new L1C signal. Programmatic and budgetary hurdles would need to be surmounted in order to reconfigure the L1C data stream to implement an NMA defense. Once implemented on the SIS, it should be relatively easy for receiver manufacturers to develop the necessary algorithms for implementing NMA on their products.

IMU-based approaches or multiantenna approaches could be implemented for receivers that are already part of tightly coupled GNSS/inertial systems or that already process data from multiple antennas. The addition of carrier-phase-based spoofing defenses would be a matter of adding algorithms. They could be implemented in receiver software that runs at the low-bandwidth navigation signal processing update rate.

A number of these defenses will remain vulnerable to a determined spoofer with a very large budget. For example, a high-end spoofer might employ the receiver/spoofer architecture with nulling and SCER. It might use multiple transmission antennas carried on multiple

platforms to create believable directions of arrival $\hat{\boldsymbol{\rho}}^i$. Receiver cross-correlation of military signals could defeat such a system if the SCER part of the attack did not attempt to spoof the secure military codes. Another effective defense would be NMA with SCER detection and clock drift monitoring. Most other defenses would fail against this attacker.

VI. SUMMARY AND CONCLUSION

This paper has reviewed the state of GNSS spoofing and defense technologies. It has reviewed a number of spoofing attack strategies that can be used to deceive a victim GNSS receiver about its position and its clock offset. All current COTS GNSS receivers are vulnerable to spoofing attacks that can be mounted using technology that has already been demonstrated in laboratory and field conditions. Advanced spoofing technology might pose defense challenges even to very sophisticated victim receivers.

There also exist a number of practical defense strategies, and this paper has described many of them. Some of these strategies involve special signal processing to look for telltale signal anomalies within a traditional GNSS receiver. Others involve advanced encryption-based techniques or techniques that rely on carrier-phase measurements and interferometric methods that are sensitive to differences between signal arrival directions for spoofed and nonspoofed situations. A number of the proposed defense technologies have been demonstrated in simulation, in laboratory hardware tests, and in the field.

There is a need for more research and development in the area of spoofing defenses, especially concerning the question of how to recover accurate navigation after the detection of an attack. More importantly, however, there is a need for receiver manufacturers to start implementing spoofing defenses, even rudimentary ones, in COTS products. ■

REFERENCES

[1] A. J. Kerns, D. P. Shepard, J. A. Bhatti, and T. E. Humphreys, "Unmanned aircraft capture and control via GPS spoofing," *J. Field Robot.*, vol. 31, no. 4, pp. 617–636, 2014.

[2] J. Bhatti and T. Humphreys, "Hostile control of ships via false GPS signals: Demonstration and detection," *Navigation*, 2016.

[3] M. L. Psiaki, *et al.*, "GNSS lies, GNSS truth: Spoofing detection with two-antenna differential carrier phase," *GPS World*, vol. 25, no. 11, pp. 36–44, Nov. 2014.

[4] Anon, "Vulnerability assessment of the transportation infrastructure relying on the global positioning system," J.A. Volpe National Transportation Systems Center, 2001.

[5] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon, and P. M. Kintner, Jr., "Assessing the spoofing threat: Development of a portable GPS civilian spoofer," in *Proc. ION GNSS*, Savannah, GA, USA, 2008, pp. 2314–2325.

[6] A. Rawnsley, "Iran's alleged drone hack: Tough, but possible," *Wired*, Dec. 2011. [Online]. Available: http://www.wired.com/dangerroom/2011/12/iran-drone-hack-gps.

[7] D. A. Divis, "Scientists document possible drone jamming," *Inside Unmanned Syst.*, p. 14, Sep. 2015.

[8] A. Konovaltsev, M. Cuntz, C. Haettich, and M. Meurer, "Autonomous spoofing detection and mitigation in a GNSS receiver with an adaptive antenna array," in *Proc. ION GNSS +*, Nashville, TN, USA, 2013, pp. 2937–2948.

[9] Anon, "Labsat 3 GPS Simulator," Racelogic, Oct. 2015. [Online]. Available: http://www.labsat.co.uk/index.php/en/products.

[10] P. Levin, D. De Lorenzo, P. Enge, and S. Lo, "Authenticating a signal based on an unknown component thereof," Patent 7,969,354 B2, Jun. 2011.

[11] B. W. O'Hanlon, M. L. Psiaki, J. A. Bhatti, D. P. Shepard, and T. E. Humphreys, "Real-time GPS spoofing detection via correlation of encrypted signals," *Navigation*, vol. 60, no. 4, pp. 267–278, 2013.

[12] M. L. Psiaki, S. P. Powell, and B. W. O'Hanlon, "GNSS spoofing detection using high-frequency antenna motion and carrier-phase data," in *Proc. ION GNSS +*, Nashville, TN, USA, 2013, pp. 2949–2991.

[13] A. J. Kerns, K. D. Wesson, and T. E. Humphreys, "A blueprint for civil GPS navigation message authentication," in *Proc. IEEE/ION PLANS Meeting*, Monterey, CA, USA, May 2014, pp. 262–269.

[14] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle, "Pre-despreading authenticity verification for GPS L1 C/A signals," *Navigation*, vol. 61, no. 1, pp. 1–11, 2014.

[15] E. McMilin *et al.*, "Field test validation of single-element antenna with anti-jam and spoof detection," in *Proc. ION GNSS +*, Tampa, FL, USA, 2015, pp. 3314–3324.

[16] E. G. Manfredini, B. Motella, and F. Dovis, "Signal quality monitoring for discrimination between spoofing and environmental effects, based on multidimensional ratio metric tests," in *Proc. ION GNSS +*, Tampa, FL, USA, 2015, pp. 3100–3106.

[17] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle, "GPS vulnerability to spoofing threats and a review of antispoofing techniques," *Int. J. Navig. Observ.*, vol. 2012, no. 127072, pp. 1–16, Jul. 2012.

[18] C. Günther, "A survey of spoofing and counter-measures," *Navigation*, vol. 61, no. 3, pp. 159–177, 2014.

[19] O. Pozzobon *et al.*, "Status of signal authentication activities within the GNSS authentication and user protection system simulator (GAUPSS) project," in *Proc. ION GNSS*, Nashville, TN, USA, 2012, pp. 2894–2900.

[20] L. Scott, "Anti-spoofing and authenticated signal architectures for civil navigation systems," in *Proc. ION GPS/GNSS*, Portland, OR, USA, 2003, pp. 1543–1552.

[21] T. E. Humphreys, "Detection strategy for cryptographic GNSS anti-spoofing," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 49, no. 2, pp. 1073–1090, Apr. 2013.

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

[23] C. Tanil, S. Khanafseh, and B. Pervan, "GNSS spoofing attack detection using aircraft autopilot response to deceptive trajectory," in *Proc. ION GNSS +*, Tampa, FL, USA, 2015, pp. 3345–3357.

[24] G. McGraw, B. Disselkoen, and G. Buesnel, "Robust open service GNSS receivers for military applications," in *Proc. ION GNSS +*, Nashville, TN, USA, 2013, pp. 2533–2541.

ABOUT THE AUTHORS

Mark L. Psiaki (Member, IEEE) received the B.A. degree in physics and the M.A. and Ph.D. degrees in mechanical and aerospace engineering from Princeton University, Princeton, NJ, USA, in 1979, 1984, and 1987, respectively.

He has been on the faculty of the Sibley School of Mechanical and Aerospace Engineering, Cornell University, Ithaca, NY, USA, since 1986 and currently holds the rank of Professor. He has spent two sabbatical leaves with the Aerospace Engineering Faculty of the Technion, Haifa, Israel, where he held appointments as a Lady Davis Visiting Associate Professor. Another sabbatical was spent as an NRC Senior Research Associate with the Air Force Research Lab, Kirtland AFB, NM, USA. He has conducted research in the areas of estimation and filtering, GPS/GNSS receivers, navigation and remote sensing using GNSS signals, GNSS security and integrity, spacecraft attitude and orbit determination, aerospace vehicle guidance, numerical trajectory optimization, and dynamic modeling of satellites, aircraft, and wheeled vehicles.

Prof. Psiaki is a Fellow of the Institute of Navigation. He has received six best paper awards for AIAA conferences along with the Institute of Navigation's Tycho Brahe Award and its Burka Award for the best paper in a volume of Navigation.

Todd E. Humphreys received the B.S. and M.S. degrees in electrical and computer engineering from Utah State University, Logan, UT, USA, in 2000 and 2003, respectively, and the Ph.D. degree in aerospace engineering from Cornell University, Ithaca, NY, USA, in 2008.

He is an Associate Professor with the Department of Aerospace Engineering and Engineering Mechanics, The University of Texas (UT) at Austin, Austin, TX, USA, and Director of the UT Radionavigation Laboratory. He specializes in the application of optimal detection and estimation techniques to problems in satellite navigation, autonomous systems, and signal processing. His recent focus has been on secure perception for autonomous systems, including navigation, timing, and collision avoidance, and on centimeter-accurate location for the mass market.

Dr. Humphreys received the University of Texas Regents' Outstanding Teaching Award in 2012, the National Science Foundation CAREER Award in 2015, and the Institute of Navigation Thurlow Award in 2015.