GNSS Spoofing Detection Using High-Frequency Antenna Motion and Carrier-Phase Data

by Mark L. Psiaki, Steven P. Powell, and Brady W. O'Hanlon
Cornell University, Ithaca, N.Y. 14853-7501, U.S.A.

BIOGRAPHIES

Mark L. Psiaki is a Professor of Mechanical and Aerospace Engineering. He received a B.A. in Physics and M.A. and Ph.D. degrees in Mechanical and Aerospace Engineering from Princeton University. His research interests are in the areas of GNSS technology and applications, spacecraft attitude and orbit determination, and general estimation, filtering, and detection.

Steven P. Powell is a Senior Engineer with the GPS and Ionospheric Studies Research Group in the Department of Electrical and Computer Engineering at Cornell University. He has M.S. and B.S. degrees in Electrical Engineering from Cornell University. He has been involved with the design, fabrication, testing, and launch activities of many scientific experiments that have flown on high altitude balloons, sounding rockets, and small satellites. He has designed ground-based and space-based custom GPS receiving systems primarily for scientific applications.

Brady W. O'Hanlon is a graduate student in the School of Electrical and Computer Engineering. He received a B.S. in Electrical and Computer Engineering from Cornell University. His interests are in the areas of GNSS technology and applications, GNSS security, and space weather.

ABSTRACT

A method is developed that processes Global Navigation Satellite System (GNSS) beat carrier phase measurements from a single moving antenna in order to determine whether the GNSS signals are being spoofed. This technique allows a specially equipped GNSS receiver to detect sophisticated spoofing that cannot be detected using receiver autonomous integrity monitoring techniques. It works for both encrypted military signals and for unencrypted civilian signals. It does not require changes to the signal structure of unencrypted civilian GNSS signals. The method uses a short segment of beat carrier-phase time histories that are collected while the receiver's single antenna is undergoing a known, high-frequency motion profile, typically one pre-programmed into an antenna articulation system. The antenna also can be moving in an unknown way at lower frequencies, as might be the case if it were mounted on a ground vehicle, a ship, an airplane, or a spacecraft. The spoofing detection algorithm correlates high-pass-filtered versions of the known motion component with high-pass-filtered versions of the carrier phase variations. True signals produce a specific correlation pattern, and spoofed signals produce a recognizably different correlation pattern if the spoofer transmits its false signals from a single antenna. The most pronounced difference is that non-spoofed signals display variations between the beat carrier phase responses of multiple signals, but all signals' responses are identical in the spoofed case. These differing correlation characteristics are used to develop a hypothesis test in order to detect a spoofing attack or the lack thereof. For moving-base receivers, there is no need for prior knowledge of the vehicle's attitude. Instead, the detection calculations also provide a rough attitude measurement. Several versions of this spoofing detection system have been designed and tested. Some have been tested only with truth-model data, but one has been tested with actual live-signal data from the Global Positioning System (GPS) C/A code on the L1 frequency. The live-data tests correctly identified spoofing attacks in the 4 cases out of 8 trials that had actual attacks. These detections used worst-case false-alarm probabilities of 10^{-6}, and their worst-case probabilities of missed detection were no greater than $1.6x10^{-6}$. The ranges of antenna motion used to detect spoofing in these trials were between 4 and 6 cm, i.e., on the order of a quarter-cycle of the GPS L1 carrier wavelength.

INTRODUCTION

The U.S. government has been aware of the vulnerability of unencrypted civilian GNSS signals to spoofing at least since the Department of Transportation released its Volpe report in 2001 [1]. A spoofer intentionally broadcasts signals that look like true signals to User Equipment receivers (UE). These false signals can fool a receiver into an incorrect determination of its position, receiver clock time, or both [2,3,4].

Spoofing of civilian GNSS signals is straightforward because their full characteristics are publicly available, e.g., Ref. 5 gives full information about the GPS civilian signals. It is relatively easy to synthesize false signals with the same characteristics [3,4]. Encrypted military signals, such as the GPS P(Y) and M codes, are much harder to spoof. One must break their encryptions or use

Copyright © 2013 by Mark L. Psiaki, Steven P. Powell, and Brady W. O'Hanlon. All rights reserved.

a meaconing-type attack, an attack which involves reception and rebroadcast of actual encrypted signals.

Spoofing of GPS receivers has been in the news recently. In December 2011, Iran captured a highly classified stealth drone that belonged to the U.S. government. An Iranian engineer claimed that they spoofed the drone's GPS in a way which fooled it into thinking that it was landing at its home base in Afghanistan. In reality, it was descending into the hands of waiting Iranian military personnel [6]. It remains unclear how much of the Iranian claims are true, but their claims are not outlandish and have to be taken seriously.

In June 2012, a group led by Todd Humphreys of UT Austin spoofed a small helicopter Uninhabited Air Vehicle (UAV) using live, on-air spoofing signals as part of a specially authorized test at White Sands Missile Range, NM. The UT Austin team caused the UAV to execute unintended maneuvers by spoofing its GPS-derived position and velocity. One of the untended maneuvers involved a near landing when the UAV had been commanded to hover about 20 m above the ground [7].

Existing anti-spoofing technology known as Receiver Autonomous Integrity Monitoring (RAIM) [8] will not suffice to detect sophisticated spoofing attacks like the one described in Refs. 3 and 4. Therefore, a number of recent and on-going efforts have sought to develop advanced spoofing detection methods that can alert a user to a sophisticated attack. These methods include advanced RAIM algorithms that operate at the correlator/discriminator/tracking-loop level [9,10,11], algorithms that cross-correlate the unknown encrypted parts of a signal between a potential victim receiver and a secure receiver [12,13,14,15], Navigation Message Authentication (NMA) that relies on proposed insertions of encrypted authentication elements within the low-bandwidth navigation message [16,17], multiple-antenna techniques [18,19,20,21,22], and moving-antenna techniques [21,22,23,24].

Reference 25 also describes a multiple-antenna technique, but it does not perform spoofing detection. Rather, it is a technique to mitigate spoofing by attenuating it without the need to formally detect it. Such techniques are not directly comparable to the detection methods under development here.

Each of the newer techniques has strengths and weaknesses. Advanced RAIM methods require only modest changes to receiver software and hardware, but they may only be able to detect spoofing at the onset of an attack. If an advanced RAIM algorithm misses the attack during this short window, then it may go undetected. The cross-correlation techniques can detect spoofing rapidly at any time during an attack, perhaps in as little as 0.2 seconds, but they rely on a high bandwidth communications link between the defended receiver and a secure receiver. NMA introduces encryption-level security into the civilian GNSS community, but it requires changes to GNSS message structures that are difficult to bring about. It may require additional signal processing in order ensure against estimation-and-replay by the spoofer of the NMA message components [26]. NMA techniques may be slow, requiring 10 seconds or more in order to detect an attack. A UAV may already be in the hands of an enemy by the time such a method discovered the attack. Multiple-antenna methods can be made reliable and fast if implemented well, but they require a significant amount of additional hardware and signal processing. The multi-receiver cross-correlation technique and the NMA technique share an additional drawback: they offer no protection against a meaconing-type receive-and-replay attack. Even an encrypted military signal is vulnerable to a meaconing attack.

The moving antenna technique can be implemented using simple hardware and algorithms, but the method of Refs. 23 and 24 requires long observation intervals, and it does not develop a clearly defined hypothesis test. Furthermore, its reliance on signal amplitude variations as an indication of spoofing may prove unreliable. A spoofer could easily create time-dependent amplitude variations between its false signals, and this particular moving-antenna detection method might interpret these variations as indicating a non-spoofed situation.

The present approach is a moving-antenna approach that is somewhat similar to that of Refs. 21 and 22, but that differs markedly from that of Refs. 23 and 24. Rather than relying on signal amplitude as in Refs. 23 and 24, it relies on signal carrier phase, as suggested in and for one of the modes of operation in Ref. 18 and in Refs. 21 and 22. Contrary to the method of Refs. 21 and 22, however, the present method does not need explicit or implicit knowledge of exact position or attitude. Those references check for inconsistencies between individual observables, such as carrier phase, on a satellite-by-satellite basis, and they propose to use any such inconsistencies to develop spoofing tests. They are not clear about how to obtain the needed accurate position knowledge of the spoofed receiver during a spoofing attack. Also, they offer no specifics about hypothesis test statistics, threshold values, and probabilities of false alarm and missed detection.

The methods developed in this paper have no such drawbacks. They need not know anything about vehicle attitude *a priori*, and their spoofing detection tests can function properly even if the receiver's position solution has been badly spoofed. They use comparisons between multiple carrier-phase signals to develop explicit spoofing detection tests that have clearly defined detection thresholds, probabilities of false alarm, and probabilities of missed detection. The embodiments discussed here do not require an Inertial Measurement Unit (IMU) to sense antenna motion, contrary to the moving-antenna system proposed in Refs. 21 and 22. Instead, motion is implemented and sensed using a special-purpose mechanical antenna deflection system. This motion need not be known relative to inertial space. Rather, it can be measured relative to a platform of unknown attitude, position, velocity, and acceleration. The only requirement is that the articulation system be able to measure virtually all of the high-frequency content of the motion. On the other hand, the new techniques proposed here could be aided by inertial sensing if it were available. A high-frequency dithering motion of the platform that carried the GNSS antenna, if coupled with inertial sensing, could constitute the principal motion/sensing system that is necessary to this method's GNSS spoofing detection approach.

The idea for this approach grew out of previous work by one of the authors on a single-antenna GNSS attitude determination system [27,28]. That system uses a GPS antenna mounted off-axis on a turntable in order to sense 3-axis attitude based on the signals from 2 or more GPS satellites. The rotation of the turntable gives rise to sinusoidal variations of the received beat carrier phase on each signal, with the frequency of the variations equal to the turntable rotation frequency. The amplitude and phase of each signal's turntable-correlated phase variations give the direction vector to the given GPS spacecraft measured in turntable coordinates.

A similar principle is used here to detect spoofing. It operates by correlating beat carrier phase time variations with known high-frequency components of the receiver antenna's position time history. In the non-spoofed case, this method has the side benefit of yielding attitude information, as in Refs. 27 and 28. The antenna motion, however, need not be circular in order to detect spoofing, nor does its amplitude need to be large enough to provide good attitude accuracy.

This paper's new GNSS spoofing detection method has some similarities to multi-antenna methods such as the one described in Ref. 20. They both rely on carrier phase measurements, and they both rely in geometrical differences between the line-of-sight (LOS) vectors to actual GNSS satellites for non-spoofed signals and the LOS vector to a spoofer. There are two important differences between the present method and carrier-phase-based multi-antenna methods. First, the use of a single antenna removes the need to resolve carrier-phase biases, and possibly integer ambiguities, between different antennas. This difference allows the present method to use simpler signal processing and to detect spoofing using shorter data intervals. Second, the present method does not always need to determine the full 3-axis attitude of the UE. Depending on the type of antenna motion that it uses, it may only determine 2-axes worth of attitude information. In some cases, however, it may estimate the full 3-axis attitude as a by-product of its spoofing detection calculations.

Note that this paper's new method, like the multi-antenna method of Ref. 20, is effective against spoofing of both open-source civilian and encrypted military GNSS signals. Thus, it could detect a meaconing attack against a U.S. Military SAASM GPS receiver.

This paper makes 3 principal contributions. First, it describes a new spoofing detection system based on correlation of beat carrier phase time variations with known high-frequency antenna motions. Second, it develops precise spoofing detection hypothesis tests for this system, complete with analyses of false-alarm and missed-detection probabilities. A number of distinct spoofing detection tests are developed for various scenarios in which decreasing amounts of *a priori* information are available to the detector. The third contribution is an evaluation of the new system. This evaluation involves tests using truth-model data and tests using actual live data. Live data for the non-spoofed null hypothesis is easy to collect by simply observing GPS L1 signals in typical outdoors environments. Live data for spoofed cases presents a challenge. One set of tests was conducted in an anechoic chamber using a re-radiated GPS signal from an outside antenna. The single re-radiating antenna inside the chamber provided exactly the same signal-in-space geometrical characteristics as are provided by a sophisticated spoofer along the lines of Refs. 3 and 4. The other set of live spoofed-case tests was conducted in conjunction with the recent spoofing attack test at White Sands Missile Range in New Mexico that is described in Ref. 7. This test was conducted under the auspices the U.S. Air Force 746 Test Squadron as a service to the Department of Homeland Security and with the approval of the FCC.

The body of this paper is divided into 9 main sections plus conclusions. The second section describes the multi-antenna spoofing detection system hardware architecture and its data flows. The third section develops the carrier-phase signal models that are used to derive spoofing detection hypothesis tests. The fourth through sixth sections develop three different versions of the spoofing detection hypothesis tests that apply for the case of uni-axial antenna articulation motion. The fourth section deals with the case of a known attitude of the articulations relative to the GNSS reference frame. The fifth section deals with the case of unknown attitude. The sixth section deals with unknown attitude and an unknown amplitude scaling factor. These sections also develop the calculations needed to derive detection thresholds as functions of false-alarm probabilities and to determine the resultant probabilities of missed detection. The seventh section address the issue of possible uncertainty in the time phasing of the articulations. The eighth section discusses enhancements that would be needed for general 3D antenna motion. The ninth section presents tests of the new method, both on truth-model data and on live-signal data. The tenth section discusses some characteristics of the new spoofing detection method along with possible enhancements, and it makes further comparisons to IMU-based detection methods. The final section provides a summary of the paper and presents its conclusions.

II. SYSTEM ARCHITECTURE

A. Antenna Hardware and Geometry

The hardware and geometry for this spoofing detection method are shown in Figs. 1 and 2 for one possible version of this system. Figure 1 shows the system in a non-spoofed scenario with 3 of the GNSS satellites whose signals are being tracked, satellites *j*-1, *j*, and *j*+1. Figure 2 shows the same system in which a spoofer is sending false versions of the signals from these same satellites. The spoofer has a single transmission antenna. Satellite *j*-1, *j*, and *j*+1 may be visible to the receiver antenna, but the spoofer has "hijacked" the receiver's tracking loops for these signals so that only the false spoofed versions of these signals are known to the receiver.

The receiver antenna of the potential spoofing victim is mounted in a way that allows its phase center to move with respect to its mounting base. In Figs. 1 and 2, this motion system is depicted as an open kinematic chain consisting of three links with ball joints that allow 6-degree-of-freedom motion. This is just one example of how a system can be configured in order to allow antenna motion relative to its mounting base. It is normally not necessary to allow for full 6-degree-of-freedom motion. The system can work well with just one translational degree of motion, such as a piston-like up-and-down motion that could be provided by a solenoid which operated along the z_a antenna articulation axis.

Yet another possible configuration is to mount the antenna on a cantilevered beam that points along the z_a axis and that allows for single-degree-of-freedom vibratory motion along the x_a or y_a axis, as shown in a photograph of the first prototype system, Fig. 3. A string connects to the left-hand side of the small metal ground plane below the patch antenna. It is used to excite the articulation motions. The thin beam extending below the antenna is cantilevered off of the barrel in the lower right of the figure. The antenna articulation motion is a 1-dimensional damped oscillation from left to right across Fig. 3's field of view, as indicated by the double-ended arrow. Although not present in the first prototype system, it is desirable to include a sensing system that measures the antenna motion. It would measure articulations relative to the mounting base.

Let the articulation time history vector relative to the (x_a,y_a,z_a) UE-fixed coordinate system be defined as

$$\boldsymbol{b}_a(t) = \begin{bmatrix} x_a(t) \\ y_a(t) \\ z_a(t) \end{bmatrix} \tag{1}$$

If the articulation system is designed to give single-degree-of-freedom motion along the known fixed unit direction vector $\hat{\boldsymbol{b}}_a$, then the full articulation vector can be written as

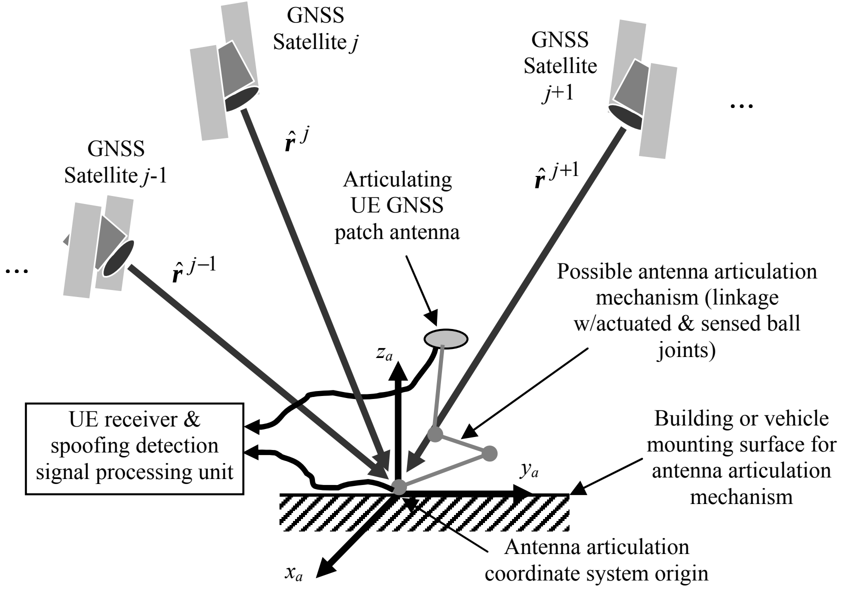
GNSS Satellite *j*
GNSS Satellite *j*+1
...
$\hat{\boldsymbol{r}}^{j}$
GNSS Satellite *j*-1
Articulating UE GNSS patch antenna
$\hat{\boldsymbol{r}}^{j+1}$
...
$\hat{\boldsymbol{r}}^{j-1}$
Possible antenna articulation mechanism (linkage w/actuated & sensed ball joints)
z_a
UE receiver & spoofing detection signal processing unit
Building or vehicle mounting surface for antenna articulation mechanism
y_a
Antenna articulation coordinate system origin
x_a

Fig. 1. Antenna articulation system geometry relative to base mount and GNSS satellites for spoofing detection system, non-spoofed case.

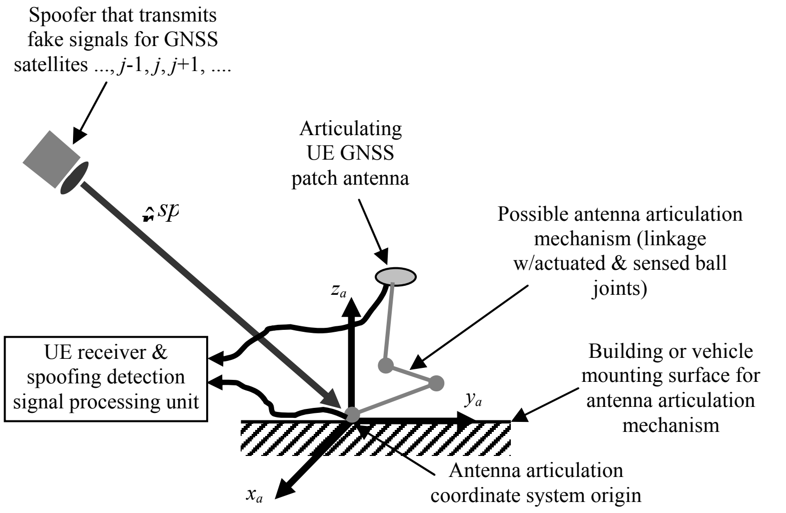
Spoofer that transmits fake signals for GNSS satellites ..., *j*-1, *j*, *j*+1, ...
Articulating UE GNSS patch antenna
$\hat{\boldsymbol{r}}^{sp}$
Possible antenna articulation mechanism (linkage w/actuated & sensed ball joints)
z_a
UE receiver & spoofing detection signal processing unit
Building or vehicle mounting surface for antenna articulation mechanism
y_a
Antenna articulation coordinate system origin
x_a

Fig. 2. Antenna articulation system geometry relative to base mount and GNSS spoofer for spoofing detection system, spoofed case.

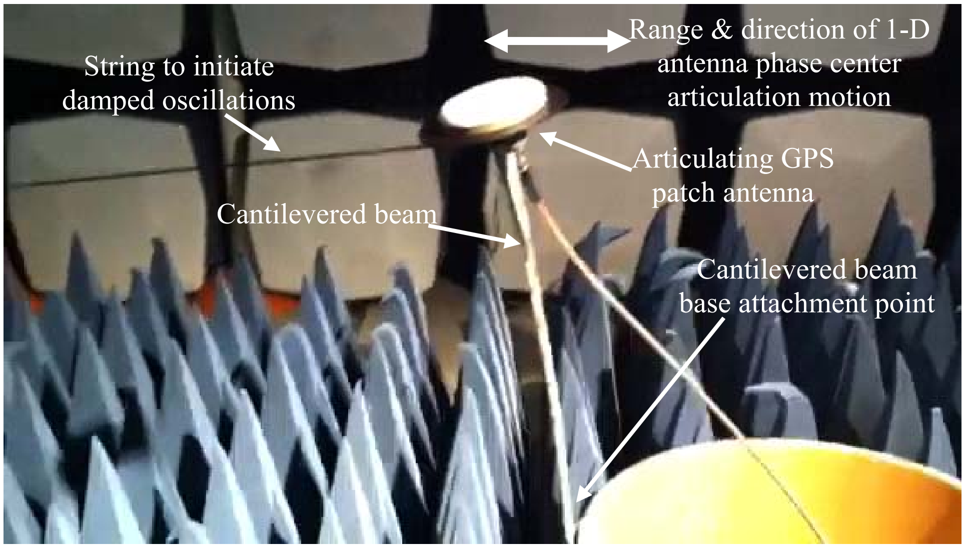
String to initiate damped oscillations
Range & direction of 1-D antenna phase center articulation motion
Articulating GPS patch antenna
Cantilevered beam
Cantilevered beam base attachment point

Fig. 3. Antenna articulation system for first prototype spoofing detector tests: a cantilevered beam that allows single-degree-of-freedom antenna phase center vibration along a horizontal axis.

$$\boldsymbol{b}_a(t) = \rho_a(t)\hat{\boldsymbol{b}}_a \tag{2}$$

where $\rho_a(t)$ is the antenna phase center deflection time history measured along the $\hat{\boldsymbol{b}}_a$ axis.

Note that the base of the antenna articulation system is mounted directly to the UE. If the UE is statically mounted on a building, as for a power grid monitor, a cell phone tower, or a financial institution, then the (x_a,y_a,z_a) UE-fixed coordinate system will also be Earth-fixed. It would be possible to calibrate/survey this coordinate system so that $\boldsymbol{b}_a(t)$ could be known in Earth-fixed coordinates.

If the UE is mounted to a moving vehicle, such as an airplane, a ship, or a wheeled vehicle, then (x_a,y_a,z_a) coordinate system will translate and rotate in the general case. It is assumed that the rotations and translations of this coordinate system occur in a lower-frequency domain as compared to the higher-frequency $\boldsymbol{b}_a(t)$ antenna articulations. It should be possible to articulate $\boldsymbol{b}_a(t)$ at a frequency of 8-16 Hz or possibly even a bit higher. Therefore, the maximum allowable frequency for significant UE rotational and translational motions is probably about 1-5 Hz, which is a reasonable upper limit for many applications.

Figure 1 includes the unit direction vectors from the GNSS spacecraft to the UE. They are $\hat{\boldsymbol{r}}^{j-1}$, $\hat{\boldsymbol{r}}^{j}$, and $\hat{\boldsymbol{r}}^{j+1}$ for, respectively, the GNSS satellites j-1, j, and j+1. These vectors point from the phase centers of the respective GNSS spacecraft antennas to the origin of the (x_a,y_a,z_a) UE-fixed coordinate system. It is assumed that these unit direction vectors are known to the spoofing detection algorithm. In the non-spoofed case, these vectors are typically computed as part of the standard pseudorange-based navigation solution [29]. In the case of spoofing, the spoofed pseudoranges can be used to compute a spoofed navigation solution and the corresponding spoofed values of the unit direction vectors $\hat{\boldsymbol{r}}^{j-1}$, $\hat{\boldsymbol{r}}^{j}$, and $\hat{\boldsymbol{r}}^{j+1}$. Even though these vectors are typically incorrect during a spoofing attack, perhaps wildly incorrect, they will be used in the spoofing detection calculations as though they were correct. Any believable spoofed scenario will be precluded from using a false set of $\hat{\boldsymbol{r}}^{j-1}$, $\hat{\boldsymbol{r}}^{j}$, and $\hat{\boldsymbol{r}}^{j+1}$ vectors that can deceive the spoofing detector's hypothesis test, as will be demonstrated in Subsection X.B. Note: the corresponding dimensional satellite-to-receiver vectors are $\boldsymbol{r}^{j-1}$, $\boldsymbol{r}^{j}$, and $\boldsymbol{r}^{j+1}$ in both the non-spoofed and spoofed cases.

The spoofed case in Fig. 2 replaces the presumed known unit direction vectors $\hat{\boldsymbol{r}}^{j-1}$, $\hat{\boldsymbol{r}}^{j}$, and $\hat{\boldsymbol{r}}^{j+1}$ with the unknown unit direction vector $\hat{\boldsymbol{r}}^{sp}$. This vector points from the spoofer's transmission antenna to the UE. In the spoofed case, the spoofing detector will, in effect, estimate one or more components of $\hat{\boldsymbol{r}}^{sp}$ as measured in its (x_a,y_a,z_a) antenna articulation coordinate system.

This paper's methods rely on the assumption that the spoofing signals come from a single spoofer transmission antenna. A spoofer that used more than one transmission antenna with significantly different $\hat{\boldsymbol{r}}^{sp}$ vectors would likely not be detectable using this paper's methods. Enhanced versions of its methods would be needed. Fortunately, successful implementation of a multi-transmitter spoofing attack would be very difficult technically, and the needed hardware would be much more costly than the spoofer hardware used in Refs. 3 and 4. Much of the difficulty in mounting a multi-transmitter spoofing attack lies in the need to precisely phase-align the false RF signals from the different transmitters.

It is important that the spoofer not know the antenna articulation time history $\boldsymbol{b}_a(t)$, at least not in a timely enough manner to spoof the effects of this motion on the received beat carrier-phase signals. One way to keep this knowledge from the spoofer is to cover the entire antenna articulation system with a radome. It must be opaque to visible light but transparent to GNSS RF signals. The radome need not be large because antenna articulation motions on the order of 4-6 cm peak-to-peak are typically sufficient for reliable spoofing detection, and they can occur along a single axis. Another possible method to avoid spoofing of the $\boldsymbol{b}_a(t)$ carrier-phase effects is to make the $\boldsymbol{b}_a(t)$ motions be of too high a frequency for the spoofer to sense and respond in a timely manner. On a UAV, concealment of $\boldsymbol{b}_a(t)$ can be achieved by masking the location of the GNSS antenna. This approach will be especially effective if the antenna is mounted far away from the UAV center of mass and if the $\boldsymbol{b}_a(t)$ motions are caused by high-frequency dithering commands to the UAV attitude.

B. Signal Processing Hardware and Connectivity

Much of the spoofing detection signal processing is carried out using standard GNSS receiver functions, as per Ref. 29. Figure 4 shows the signal processing block diagram for an example receiver channel and its relationship to the other elements of the spoofing detection system. All except 6 blocks, the three left-most blocks ("RF front-end", "Receiver clock", and "Antenna articulation sensor"), the two right-most blocks in the bottom row ("Mid-point sampler" and "Spoofing detection hypothesis test"), and the top-right block ("Navigation solution") are standard processing blocks in a single tracking channel of a digital GNSS receiver. A new function of each tracking channel is to synthesize a special beat carrier-phase measurement for input to the spoofing detection test. This is done using the "Mid-point sampler" block just to the right of center at the bottom of the figure and using the summation junction to the right of this block. A receiver uses L such channels to track L signals. It provides L carrier-phase time histories to the "Spoofing detection hypothesis test" block in the bottom right-hand corner of the figure.

The 3 blocks labeled "RF front end", "Receiver clock", and "Navigation solution" are also standard blocks. They are common to all receiver channels. They provide inputs to or accept outputs from each channel.

The 2 blocks "Antenna articulation sensor" and "Spoofing detection hypothesis test" are new blocks needed for spoofing detection. They are also common to all channels.

The RF signal from the patch antenna on the left-hand side of the figure first passes through an RF front-end. This RF front-end mixes the signal so that the nominal carrier frequency is down-translated to the intermediate frequency (IF) ω_{IF}. The RF front-end uses an ADC to digitally sample this IF signal, and sends the result into the receiver's high-sample-rate digital signal processing hardware. The signal first gets mixed to baseband, both in-phase and quadrature, as it moves from left to right across the center of the figure. Next, the signal is mixed with the prompt replica of the pseudo random number (PRN) code that is particular to the satellite being tracked. The base-band mixing signal is provided by the Phase-Lock Loop (PLL) feedback in the lower central portion of the figure. Its estimate of the carrier Doppler shift for the k^{th} accumulation interval is ω_{PLLk}. The prompt PRN code replica is provided by the Delay-Lock Loop (DLL) feedback in the upper central portion of the figure. Its estimate of the PRN code's Doppler-shifted chipping rate is f_{chipk}. These two tracking loops rely on the prompt in-phase and quadrature accumulations, I_{pk} and Q_{pk} for the k^{th} accumulation interval, which are computed by the accumulate-and-dump registers just to the right of the figure's center. The DLL discriminator also uses in-phase and prompt early-minus-late accumulations I_{emlk} and Q_{emlk} or related accumulations, but the signal processing paths for computing these standard accumulations is omitted from the figure.

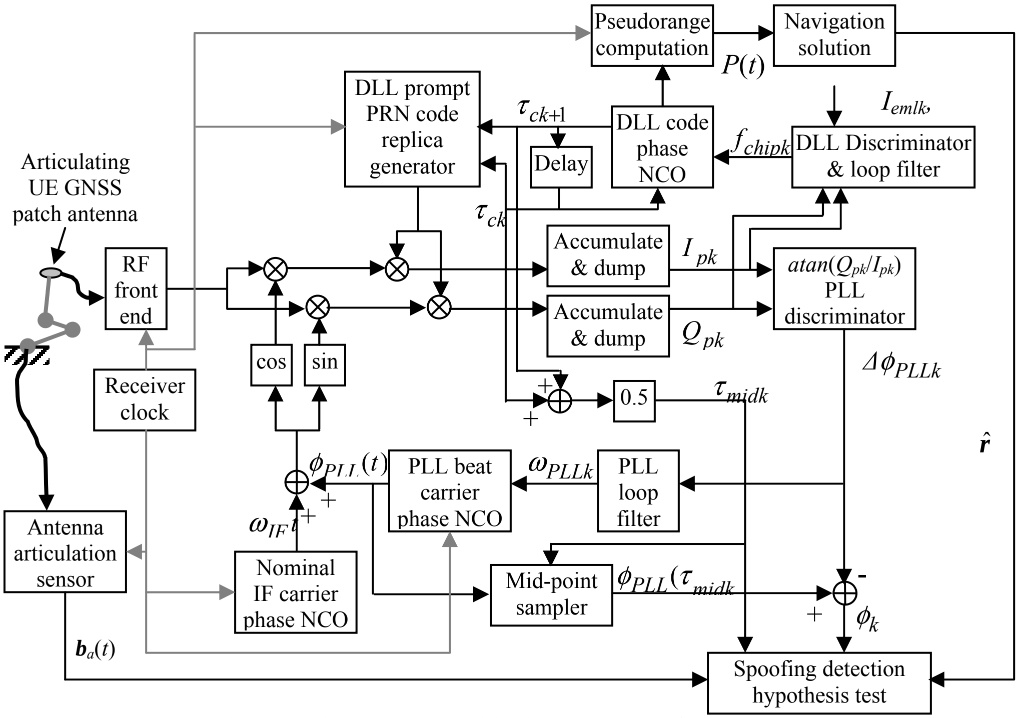

Fig. 4. Example signal processing block diagram of a single-satellite receiver channel that provides inputs to the spoofing detector.

The following quantities are the important outputs of the standard signal tracking hardware part of Fig. 4: The PLL (negative) beat carrier phase time history $\phi_{PLL}(t)$, the mid-point time of the k^{th} accumulation interval $\tau_{midk} = 0.5(\tau_{ck} + \tau_{ck+1})$, and the PLL phase error discriminator value for this interval $\Delta\phi_{PLLk}$. The beat carrier phase is termed "negative" because it has the opposite sign of the usual beat carrier phase definition in the GPS literature [29]. It equals the time integral of the received carrier Doppler shift, and it increase as the range from the GNSS satellite to the receiver decreases. Note that the start and stop times for the k^{th} accumulation interval are τ_{ck} and τ_{ck+1}, as dictated by the DLL.

The summation junction in the lower right-hand corner of Fig. 4 synthesizes the following wideband estimate of the (negative) beat carrier phase at the accumulation interval's mid-point:

$$\phi_k = \phi_{PLL}(\tau_{midk}) - \Delta\phi_{PLLk} \qquad (3)$$

This modified carrier-phase observable differs in two significant respects from the standard beat carrier phase measurement produced by most receivers, that is, from $\phi_{PLL}(\tau_{midk})$. First, the measurement noise samples for different accumulation periods are white rather than colored. Second, ϕ_k does not attenuate the effects of high-frequency components of $\boldsymbol{b}_a(t)$ that lie outside the PLL bandwidth; $\phi_{PLL}(\tau_{midk})$ includes only attenuated versions of these components. These distinctives of the ϕ_k observable are important to the proper functioning of the spoofing detection tests. Note, however, that the noise power in ϕ_k is larger than in $\phi_{PLL}(\tau_{midk})$. This drawback is insignificant in comparison to the advantage of having a wide-band beat carrier phase measurement corrupted by white noise rather than colored noise.

Note that some receivers may use slightly different signal processing strategies that could impact the needed summation in Eq. (3). In particular, the $-\Delta\phi_{PLLk}$ term on the right-hand side of Eq. (3) must be replaced by $+\Delta\phi_{PLLk}$ in some cases in order to properly form the wideband (negative) beat carrier phase. This will be the case if the RF front-end uses high-side mixing while the receiver uses the absolute value of the resulting intermediate frequency as its ω_{IF}. Alternatively, a negation of the quadrature baseband mixing signal used to form Q_{pk} would create the need for this same sign change in the ϕ_k formula.

The spoofing detection block in the bottom right-hand corner of Fig. 4 takes four types of inputs: the antenna articulation time history $\boldsymbol{b}_a(t)$, the accumulation mid-point time τ_{midk} for each tracking channel, the wideband (negative) beat carrier phase ϕ_k for each tracking channel, and the unit direction vector that points from each tracked GNSS satellite $\hat{\boldsymbol{r}}$. Suppose that there are L tracked GNSS satellites labeled $j = 1, ..., L$. Suppose, also, that for satellite j the spoofing detection test uses data from N_j accumulations. Then the spoofing detection receiver must implement L parallel DLL/PLL/wideband-beat-carrier-phase signal processing channels as per Fig. 4. The resulting outputs of these L channels that will be used in the spoofing detection block will be τ_{midk}^j and ϕ_k^j for $k = 1, ..., N_j$ and $j = 1, ..., L$. Also used will be $\boldsymbol{b}_a(\tau_{midk}^j)$ for $k = 1, ..., N_j$ and $j = 1, ..., L$ along with $\hat{\boldsymbol{r}}^j$ for $j = 1, ..., L$. This set of inputs implies that the spoofing detection interval is short enough to approximate each unit direction vector $\hat{\boldsymbol{r}}^j$ as being constant. The calculations implemented in the spoofing detection block are the subject of Sections III-VIII.

III. CARRIER PHASE MODEL FOR SPOOFING DETECTION

Two models of the negative beat carrier phase observable ϕ_k^j are needed in order to do spoofing detection. The first model covers the non-spoofed case, and the second model covers the spoofed case.

A. Non-Spoofed Carrier Phase Model and Cycle-Slip Repair

The non-spoofed carrier phase model starts with a standard model from the GPS literature [29]:

$$\phi_k^j = -\frac{2\pi}{\lambda}\sqrt{[\boldsymbol{r}_k^j + A_k^{\mathrm{T}}\boldsymbol{b}_a(\tau_{midk}^j)]^{\mathrm{T}}[\boldsymbol{r}_k^j + A_k^{\mathrm{T}}\boldsymbol{b}_a(\tau_{midk}^j)]} - \omega_c(\delta t_{Rk} - \delta t_k^j - \tau_{ionok}^j + \tau_{tropok}^j) + \beta^j + n_{\phi k}^j \qquad (4)$$

where λ is the carrier wavelength, ω_c is the nominal carrier frequency in rad/sec (= $2\pi c/\lambda$, with c being the speed of light), A_k is the 3-by-3 direction cosines matrix for the transformation from the reference coordinate system in which the $\boldsymbol{r}_k^j$ vector is known to the (x_a,y_a,z_a) UE-fixed coordinate system in which $\boldsymbol{b}_a(t)$ is known, δt_{Rk} is the receiver clock error, δt_k^j is the transmitter clock error for satellite j, τ_{ionok}^j is the ionospheric phase advance term, τ_{tropok}^j is the neutral atmosphere delay term, β^j is the carrier phase bias, and $n_{\phi k}^j$ is the random component of the carrier phase noise. The leading negative sign on the right-hand side of Eq. (4) is what makes ϕ_k^j a negative beat carrier phase rather than a standard beat carrier phase. The k subscripts on $\boldsymbol{r}_k^j$, A_k, δt_{Rk}, δt_k^j, τ_{ionok}^j, τ_{tropok}^j, and $n_{\phi k}^j$ indicate that they all vary with the time of applicability τ_{midk}^j. Note that ω_c equals $2\pi 1575.42\text{x}10^6$ rad/sec for the GPS L1 signal.

The carrier phase bias term β^j contains both the integer-ambiguity component and the lesser-known fractional cycle component [30]. It does not have a k subscript because it will be constant in a well-designed receiver. In the current application, however, an insufficient PLL bandwidth coupled with a higher bandwidth antenna motion $\boldsymbol{b}_a(t)$ can give rise to half- or full-cycle slips that violate this constancy assumption.

Therefore, it may be necessary to do some extra processing to a given ϕ_k^j vs. τ_{midk}^j beat carrier phase time history for $k = 1, ..., N_j$ in order to remove cycle slips and thereby ensure the required constancy of the bias. This amounts to a phase unwrapping operation. The needed operation starts with a detrending of ϕ_k^j vs. τ_{midk}^j, perhaps by subtracting a linear or quadratic fit of this curve from ϕ_k^j. Suppose that this detrended phase time history is $\delta\phi_{dtk}^j$ vs. τ_{midk}^j.

The following pseudocode performs the necessary phase unwrapping in the case of half-cycle ambiguities:

```
1. Initialize the first sample of the unwrapping increment time history: $\delta\phi_{uwk}^j = 0$ for $k = 1$.
2. Initialize $k = 2$.
3. Set $\delta\phi_{uwk}^j = \pi\, round[\frac{1}{\pi}(\delta\phi_{dtk-1}^j + \delta\phi_{uwk-1}^j - \delta\phi_{dtk}^j)]$.
4. Replace $\phi_k^j$ by $\phi_k^j + \delta\phi_{uwk}^j$.
5. Replace $k$ by $k+1$.
6. If $k \leq N_j$ go to Step 2; otherwise, stop.
```

The *round*() function is the standard function that rounds its argument to the nearest integer.

If the tracked channel is a dataless pilot channel, such as the CL code on the GPS L2 signal, then any carrier-phase slips will be full cycles rather than half cycles. In this case, the 2-quadrant *atan*(Q_{pk}/I_{pk}) phase discriminator in Fig. 4 should be replaced with the 4-quadrant *atan2*(Q_{pk},I_{pk}) discriminator, and the two π terms in Step 3 of the above pseudocode should be replaced by 2π terms.

The magnitude of $\boldsymbol{b}_a(t)$ is typically much smaller than the magnitude $\boldsymbol{r}_k^j$ in Eq. (4), centimeters vs. 20,000 km. Therefore, the following approximation of Eq. (4) to first-order in $\boldsymbol{b}_a$ is sufficiently accurate:

$$\begin{aligned}\phi_k^j &\cong -\frac{2\pi}{\lambda}[\sqrt{(\boldsymbol{r}_k^j)^{\mathrm{T}}\boldsymbol{r}_k^j} + (\hat{\boldsymbol{r}}_k^j)^{\mathrm{T}} A_k^{\mathrm{T}} \boldsymbol{b}_a(\tau_{midk}^j)] \\ &\quad - \omega_c(\delta t_{Rk} - \delta t_k^j - \tau_{ionok}^j + \tau_{tropok}^j) + \beta^j + n_{\phi k}^j \qquad (5)\end{aligned}$$

An additional approximation is reasonable, that of a constant $\hat{\boldsymbol{r}}^j$. The actual variations of elements of the $\hat{\boldsymbol{r}}_k^j$ unit direction vector from their mean values over a typical spoofing detection interval of 0.5 sec or less are on the order of 6x10^{-5} even for a supersonic aircraft traveling at Mach 3 in the opposite direction of GNSS Satellite *j*'s ground track. The components of $\boldsymbol{b}_a(t)$ typically are on the order of 10 cm or less. Therefore, $\hat{\boldsymbol{r}}_k^j$ can be approximated by the constant $\hat{\boldsymbol{r}}^j$ value that equals the $\hat{\boldsymbol{r}}_k^j$ vector which applies at the mid-point of a given spoofing detection interval. Thus, the new approximate (negative) beat carrier phase equation becomes:

$$\begin{aligned}\phi_k^j &\cong -\frac{2\pi}{\lambda}[\sqrt{(\boldsymbol{r}_k^j)^{\mathrm{T}}\boldsymbol{r}_k^j} + (\hat{\boldsymbol{r}}^j)^{\mathrm{T}} A_k^{\mathrm{T}} \boldsymbol{b}_a(\tau_{midk}^j)] \\ &\quad - \omega_c(\delta t_{Rk} - \delta t_k^j - \tau_{ionok}^j + \tau_{tropok}^j) + \beta^j + n_{\phi k}^j \qquad (6)\end{aligned}$$

Another simplification uses a quadratic polynomial in time in order to approximate all of the terms other than the $(\hat{\boldsymbol{r}}^j)^{\mathrm{T}} A_k^{\mathrm{T}} \boldsymbol{b}_a(\tau_{midk}^j)$ spoofing detection term and the $n_{\phi k}^j$ noise term. This involves the following approximation for the low-frequency behavior of the (negative) beat carrier phase:

$$\begin{aligned}\phi_{lf}^j(\tau_{midk}^j) &= -\frac{2\pi}{\lambda}\sqrt{(\boldsymbol{r}_k^j)^{\mathrm{T}}\boldsymbol{r}_k^j} \\ &\quad - \omega_c(\delta t_{Rk} - \delta t_k^j - \tau_{ionok}^j + \tau_{tropok}^j) + \beta^j \\ &\cong \beta_0^j + \beta_1^j(\tau_{midk}^j - \tau_{mid1}^j) + \tfrac{1}{2}\beta_2^j(\tau_{midk}^j - \tau_{mid1}^j)^2 \qquad (7)\end{aligned}$$

where β_0^j, β_1^j, and β_2^j are constant polynomial coefficients.

This approximation leads to the following non-spoofed carrier phase model

$$\begin{aligned}\phi_k^j &\cong -\frac{2\pi}{\lambda}(\hat{\boldsymbol{r}}^j)^{\mathrm{T}} A_k^{\mathrm{T}} \boldsymbol{b}_a(\tau_{midk}^j) \\ &\quad + \beta_0^j + \beta_1^j(\tau_{midk}^j - \tau_{mid1}^j) + \tfrac{1}{2}\beta_2^j(\tau_{midk}^j - \tau_{mid1}^j)^2 + n_{\phi k}^j \\ &\qquad (8)\end{aligned}$$

Yet another simplification approximates the coordinate transformation matrix A_k as being constant over the spoofing detection interval. This leads to a dropping of its k subscript so that the carrier phase model becomes:

$$\begin{aligned}\phi_k^j &\cong -\frac{2\pi}{\lambda}(\hat{\boldsymbol{r}}^j)^{\mathrm{T}} A^{\mathrm{T}} \boldsymbol{b}_a(\tau_{midk}^j) \\ &\quad + \beta_0^j + \beta_1^j(\tau_{midk}^j - \tau_{mid1}^j) + \tfrac{1}{2}\beta_2^j(\tau_{midk}^j - \tau_{mid1}^j)^2 + n_{\phi k}^j \\ &\qquad (9)\end{aligned}$$

One last simplification of the carrier-phase model can be made in the special case of uni-axial motion in $\boldsymbol{b}_a(t)$, as defined in Eq. (2). This takes place along the known unit vector direction $\hat{\boldsymbol{b}}_a$ in antenna articulation coordinates and along the typically unknown vector direction $\hat{\boldsymbol{r}}_a = A^{\mathrm{T}}\hat{\boldsymbol{b}}_a$ in reference coordinates. The beat carrier-phase model in this case becomes:

$$\begin{aligned}\phi_k^j &\cong -\frac{2\pi}{\lambda}(\hat{\boldsymbol{r}}^j)^{\mathrm{T}} \hat{\boldsymbol{r}}_a \rho_a(\tau_{midk}^j) \\ &\quad + \beta_0^j + \beta_1^j(\tau_{midk}^j - \tau_{mid1}^j) + \tfrac{1}{2}\beta_2^j(\tau_{midk}^j - \tau_{mid1}^j)^2 + n_{\phi k}^j \\ &\qquad (10)\end{aligned}$$

with the antenna deflection amplitude time history $\rho_a(t)$ known.

Carrier Phase Noise Model. The carrier phase noise term $n_{\phi k}^{j}$ is modeled as being Gaussian white noise. Its statistics are

$$E\{n_{\phi k}^{j}\}=0 \quad \text{and} \quad E\{n_{\phi k}^{j}n_{\phi l}^{j}\}=\begin{cases}(\sigma^{j})^{2} & \text{if } k=l\\ 0 & \text{if } k\neq l\end{cases} \quad \text{with}$$

$$(\sigma^{j})^{2}=\frac{1}{2(C/N_{0})^{j}\,\Delta\tau_{cavg}^{j}} \tag{11}$$

where $(C/N_0)^j$ is the carrier-to-noise ratio of the received signal for GNSS Satellite j in absolute Hz units and where $\Delta\tau_{cavg}^{j}$ = $mean(\tau_{ck+1}$ - $\tau_{ck})$ is the average accumulation interval in the Satellite j tracking system, as depicted in Fig. 4, given in seconds. The units of σ^j in Eq. (11) are radians. Note that the phase noise terms for different GNSS satellites are assumed to be uncorrelated.

B. Spoofed Carrier Phase Model

The spoofed carrier phase model starts with a modified version of Eq. (4) that includes both the effects of the spoofer's signal design and the relative geometry between the spoofer and the intended victim. The spoofer is assumed to know the relative geometry between it and the origin of the (x_a,y_a,z_a) UE-fixed coordinate system. It is assumed not to know the $\boldsymbol{b}_a(t)$ antenna articulation motions. As per the attack mode described in Refs. 3 and 4, the spoofer is presumed to have compensated for the known part of the relative geometry so that the signal looks to the victim like a real GNSS signal.

The spoofed beat carrier phase model that corresponds to this type of attack is

$$\begin{aligned}\phi_{k}^{j} \;=\; & -\frac{2\pi}{\lambda}\{\sqrt{(\boldsymbol{r}_{k}^{j})^{\mathrm{T}}\boldsymbol{r}_{k}^{j}}-\sqrt{(\boldsymbol{r}_{k}^{sp})^{\mathrm{T}}\boldsymbol{r}_{k}^{sp}}\\ & +\sqrt{[\boldsymbol{r}_{k}^{sp}+A_{k}^{\mathrm{T}}\boldsymbol{b}_{a}(\tau_{midk}^{j})]^{\mathrm{T}}[\boldsymbol{r}_{k}^{sp}+A_{k}^{\mathrm{T}}\boldsymbol{b}_{a}(\tau_{midk}^{j})]}\}\\ & -\omega_{c}(\delta t_{Rk}+\delta t_{Rspk}-\delta t_{k}^{j}-\tau_{ionok}^{j}+\tau_{tropok}^{j})\\ & +\beta^{j}+n_{\phi k}^{j}\end{aligned} \tag{12}$$

The first two terms in the braced expression on the right-hand side of Eq. (12) are generated by the spoofer as part of its false signal. The third term in that expression is the term due to the geometry of the spoofer/victim relative antenna location. The spoofer synthesizes the second of its terms with the goal of canceling the effects of the third term. Were it not for the $\boldsymbol{b}_a(t)$ antenna articulations, this cancellation would be perfect.

The spoofer also synthesizes the terms δt_{Rspk}, δt_{k}^{j}, τ_{ionok}^{j}, and τ_{tropok}^{j} in Eq. (12). These terms represent, respectively, the spoofed increment to the victim receiver clock error, the spoofed GNSS satellite clock error, the spoofed ionospheric carrier phase advance, and the spoofed ionospheric delay.

After a set of approximations similar to those used to go from Eq. (4) to Eqs. (6), (8), and (9) for the non-spoofed case, a reasonable approximation of the spoofed carrier-phase model in Eq. (12) takes the form:

$$\begin{aligned}\phi_{k}^{j} \;\cong\; & -\frac{2\pi}{\lambda}(\hat{\boldsymbol{r}}^{sp})^{\mathrm{T}}A^{\mathrm{T}}\boldsymbol{b}_{a}(\tau_{midk}^{j})\\ & +\beta_{0}^{j}+\beta_{1}^{j}(\tau_{midk}^{j}-\tau_{mid1}^{j})+\tfrac{1}{2}\beta_{2}^{j}(\tau_{midk}^{j}-\tau_{mid1}^{j})^{2}+n_{\phi k}^{j}\end{aligned} \tag{13}$$

This chain of approximations includes a linearization in terms of $\boldsymbol{b}_a(t)$ of the nonlinear 3rd term on the right-hand side of Eq. (12). This linearization is reasonable because the magnitude of $\boldsymbol{b}_a(t)$ is normally much smaller than the magnitude of $\boldsymbol{r}_{k}^{sp}$, less than 10 cm vs. 10s of meters or more. The approximation also involves replacing the time-varying unit-direction vector $\hat{\boldsymbol{r}}_{k}^{sp}$ with the constant mid-point direction $\hat{\boldsymbol{r}}^{sp}$. This approximation is reasonable because a spoofer typically maintains a relative geometry to the victim that does not vary very rapidly with time; otherwise, it might have trouble spoofing the victim. If either of these approximations were to break down, either because the spoofer was very close to the victim or because it changed geometry very rapidly, then Eq. (13) should and could be modified appropriately.

The approximation in Eq. (13) involves a modified low-frequency polynomial approximation for the non-articulation terms in the beat carrier phase model of Eq. (12). This approximation takes the form

$$\begin{aligned}\phi_{lf}^{j}(\tau_{midk}^{j}) \quad & -\frac{2\pi}{\lambda}\sqrt{(\boldsymbol{r}_{k}^{j})^{\mathrm{T}}\boldsymbol{r}_{k}^{j}}\\ & -\omega_{c}(\delta t_{Rk}+\delta t_{Rspk}-\delta t_{k}^{j}-\tau_{ionok}^{j}+\tau_{tropok}^{j})+\beta^{j}\\ & \cong\beta_{0}^{j}+\beta_{1}^{j}(\tau_{midk}^{j}-\tau_{mid1}^{j})+\tfrac{1}{2}\beta_{2}^{j}(\tau_{midk}^{j}-\tau_{mid1}^{j})^{2}\end{aligned} \tag{14}$$

with β_{0}^{j}, β_{1}^{j}, and β_{2}^{j} again being constant polynomial coefficients. The only differences between this low-frequency approximation and that of Eq. (7) are the presence of the spoofed receiver clock error increment δt_{Rspk} and the fact that most of the terms in this model are spoofed quantities rather than true quantities.

The salient feature of the spoofed carrier phase model in Eq. (13) is the first term on its right-hand side. In comparing this model to the non-spoofed model in Eq. (9), a single difference stands out: The non-spoofed satellite-to-receiver direction vector $\hat{\boldsymbol{r}}^{j}$ in Eq. (9) is replaced by the spoofer-to-receiver direction vector $\hat{\boldsymbol{r}}^{sp}$. The most important aspect of this replacement is that this direction is the same for all satellites j = 1, ..., L for the spoofed case, but different for the non-spoofed case. This fact implies that all signals' beat carrier phase time histories, ϕ_k^j vs. τ_{midk}^j for k = 1, ..., N_j and j = 1, ..., L, will display identical $\boldsymbol{b}_a(t)$ effects in the spoofed case but different $\boldsymbol{b}_a(t)$ effects in the non-spoofed case. This is the central principal upon which this paper's spoofing detection tests are based.

Similar to the non-spoofed case, a modified form of Eq. (13) can be developed for the special case of rectilinear antenna articulation motion, as defined in Eq. (2). It takes the form

$$\begin{aligned}\phi_k^j \;&\cong -\frac{2\pi}{\lambda}(\hat{\boldsymbol{r}}^{sp})^{\mathrm{T}}\hat{\boldsymbol{r}}_a\,\rho_a(\tau_{midk}^j)\\ &+\beta_0^j+\beta_1^j(\tau_{midk}^j-\tau_{mid1}^j)+\tfrac{1}{2}\beta_2^j(\tau_{midk}^j-\tau_{mid1}^j)^2+n_{\phi k}^j\end{aligned} \tag{15}$$

Recall that $\hat{\boldsymbol{r}}_a = A^{\mathrm{T}}\hat{\boldsymbol{b}}_a$ is the articulation unit direction vector in reference coordinates and that $\rho_a(t)$ is the articulation magnitude. The former quantity is often unknown, but the latter is usually known exactly.

IV. SPOOFING DETECTION HYPOTHESIS TESTS WITH UNI-AXIAL ANTENNA ARTICULATIONS AND KNOWN ATTITUDE

A. Restriction to Uni-axial Antenna Articulations

The spoofing detection test and analyses of the present section and of Sections V and VI deal with the special case of uni-axial antenna articulation motion as defined in the antenna coordinate system, i.e., as in Eq. (2). Therefore, Eq. (10) models the beat carrier phase in the non-spoofed case, and Eq. (15) is the spoofed-case model. This restriction to uni-axial motion is not necessary to the method. It is adopted here for two reasons: First, it simplifies the resulting spoofing detection statistic calculations and the analyses of their false-alarm and missed-detection probabilities. Second, it simplifies the design of the articulation hardware. Section VIII outlines methods to modify the detection statistic calculations and the corresponding probability analyses for a general 3-dimensional $\boldsymbol{b}_a(t)$ antenna articulation time history.

B. High-Pass Filtering via Linear Least-Squares Estimation

High-pass filtering of the carrier-phase measurements can be used to remove the low-frequency effects of unknown UE motion and unknown UE receiver clock drift. This high-pass filtering amounts to least-squares estimation of the unknown polynomial coefficients β_0^j, β_1^j, and β_2^j in Eq. (10) or Eq. (15). The same calculations can be used to isolate the uni-axial antenna motion effects into a single equation per GNSS signal.

The needed filtering calculations for the j^{th} GNSS signal start with the following over-determined system of linear equations

$$\begin{bmatrix}\phi_1^j\\ \phi_2^j\\ \phi_3^j\\ \vdots\\ \phi_{N_j}^j\end{bmatrix}=\begin{bmatrix}1 & 0 & 0 & -\frac{2\pi}{\lambda}\rho_a(\tau_{mid1}^j)\\ 1 & (\tau_{mid2}^j-\tau_{mid1}^j) & \frac{1}{2}(\tau_{mid2}^j-\tau_{mid1}^j)^2 & -\frac{2\pi}{\lambda}\rho_a(\tau_{mid2}^j)\\ 1 & (\tau_{mid3}^j-\tau_{mid1}^j) & \frac{1}{2}(\tau_{mid3}^j-\tau_{mid1}^j)^2 & -\frac{2\pi}{\lambda}\rho_a(\tau_{mid3}^j)\\ \vdots & \vdots & \vdots & \vdots\\ 1 & (\tau_{midN_j}^j-\tau_{mid1}^j) & \frac{1}{2}(\tau_{midN_j}^j-\tau_{mid1}^j)^2 & -\frac{2\pi}{\lambda}\rho_a(\tau_{midN_j}^j)\end{bmatrix}\begin{bmatrix}\beta_0^j\\ \beta_1^j\\ \beta_2^j\\ (\hat{\boldsymbol{r}}^x)^{\mathrm{T}}\hat{\boldsymbol{r}}_a\end{bmatrix}+\begin{bmatrix}n_{\phi1}^j\\ n_{\phi2}^j\\ n_{\phi3}^j\\ \vdots\\ n_{\phi N_j}^j\end{bmatrix} \tag{16}$$

This same set of equations is repeated once for each satellite j = 1, …, L. In the non-spoofed case, the unit direction vector $\hat{\boldsymbol{r}}^x$ in Eq. (16) is $\hat{\boldsymbol{r}}^j$, but it equals $\hat{\boldsymbol{r}}^{sp}$ in the spoofed case.

The high-pass filter works by computing the orthogonal/upper-triangular (QR) factorization [31] of a normalized version of the N_j-by-4 coefficient matrix on the right-hand side of Eq. (16). This factorization takes the form:

$$Q^j\begin{bmatrix}R_{11}^j & R_{12}^j & R_{13}^j & R_{14}^j\\ 0 & R_{22}^j & R_{23}^j & R_{24}^j\\ 0 & 0 & R_{33}^j & R_{34}^j\\ 0 & 0 & 0 & R_{44}^j\\ 0 & 0 & 0 & 0\\ \vdots & \vdots & \vdots & \vdots\end{bmatrix}=\frac{1}{\sigma^j}\begin{bmatrix}1 & 0 & 0 & -\frac{2\pi}{\lambda}\rho_a(\tau_{mid1}^j)\\ 1 & (\tau_{mid2}^j-\tau_{mid1}^j) & \frac{1}{2}(\tau_{mid2}^j-\tau_{mid1}^j)^2 & -\frac{2\pi}{\lambda}\rho_a(\tau_{mid2}^j)\\ 1 & (\tau_{mid3}^j-\tau_{mid1}^j) & \frac{1}{2}(\tau_{mid3}^j-\tau_{mid1}^j)^2 & -\frac{2\pi}{\lambda}\rho_a(\tau_{mid3}^j)\\ \vdots & \vdots & \vdots & \vdots\\ 1 & (\tau_{midN_j}^j-\tau_{mid1}^j) & \frac{1}{2}(\tau_{midN_j}^j-\tau_{mid1}^j)^2 & -\frac{2\pi}{\lambda}\rho_a(\tau_{midN_j}^j)\end{bmatrix} \tag{17}$$

The N_j-by-N_j orthonormal matrix Q^j and the R_{11}^j, R_{12}^j, R_{13}^j, …, R_{44}^j elements of the corresponding upper-triangular matrix are computed as the QR factorization algorithm's outputs, and the matrix on the right-hand side of Eq. (17) is the input [31].

The high-pass filter operations also compute the transformed, normalized beat carrier phase time history, and they are used to define the corresponding noise time history:

$$\begin{bmatrix} z_1^j \\ z_2^j \\ z_3^j \\ z_4^j \\ \vdots \\ z_{N_j}^j \end{bmatrix} = \frac{1}{\sigma^j}(Q^j)^{\mathrm{T}} \begin{bmatrix} \phi_1^j \\ \phi_2^j \\ \phi_3^j \\ \vdots \\ \phi_{N_j}^j \end{bmatrix} \quad \text{and}$$

$$\begin{bmatrix} n_1^j \\ n_2^j \\ n_3^j \\ n_4^j \\ \vdots \\ n_{N_j}^j \end{bmatrix} = \frac{1}{\sigma^j}(Q^j)^{\mathrm{T}} \begin{bmatrix} n_{\phi 1}^j \\ n_{\phi 2}^j \\ n_{\phi 3}^j \\ \vdots \\ n_{\phi N_j}^j \end{bmatrix} \tag{18}$$

The orthogonal nature of Q^j and the $1/\sigma^j$ normalization factor cause the transformed, normalized Gaussian noise vector $[n_1^j; \ldots; n_{N_j}^j]$ to have an identity covariance matrix. Note that this vector has a mean of zero.

The important output of these high-pass filtering operations is a single equation for each GNSS signal that contains all the information about whether or not it has been spoofed. This equation is the 4th scalar equation in the transformed, normalized version of Eq. (16). It takes the form:

$$z_4^j = R_{44}^j[(\hat{\boldsymbol{r}}^x)^{\mathrm{T}}\hat{\boldsymbol{r}}_a] + n_4^j \tag{19}$$

where n_4^j is a zero-mean, unit-variance Gaussian random scalar. The 1st through 3rd equations in the transformed system do not affect any of the spoofing detection tests because their effects can be integrated out of any standard Neyman-Pearson test [32] under the diffuse prior assumption about the polynomial coefficients β_0^j, β_1^j, and β_2^j. The resulting integrals are identical under the non-spoofed and spoofed hypotheses. Equations 5 through N_j are identical under the non-spoofed and spoofed hypothesis. Therefore, neither do they contribute to the optimal Neyman-Pearson detection statistic. They serve only to isolate the residual error terms $z_5^j, \ldots, z_{N_j}^j$. The data in Eq. (19) for $j = 1, \ldots, L$ will form the basis for the spoofing detection tests of this section and of Sections V and VI.

C. Spoofing Detection Hypothesis Test for Fixed-Base UE with Known Attitude

The optimal Neyman-Pearson test statistic is based on the ratio of the probability densities of the carrier-phase data given the two hypotheses, the H_0 hypothesis of no spoofing and the H_1 hypothesis of spoofing. Stated in terms of the high-pass-filtered result in Eq. (19), the two relevant probability densities are:

$$p(z_4^1,\ldots,z_4^L \mid H_0) = w\exp(-\tfrac{1}{2}\sum_{j=1}^{L}\{R_{44}^j[(\hat{\boldsymbol{r}}^j)^{\mathrm{T}}\hat{\boldsymbol{r}}_a] - z_4^j\}^2) \tag{20a}$$

$$p(z_4^1,\ldots,z_4^L \mid \hat{\boldsymbol{r}}^{sp}, H_1) = w\exp(-\tfrac{1}{2}\sum_{j=1}^{L}\{R_{44}^j[(\hat{\boldsymbol{r}}^{sp})^{\mathrm{T}}\hat{\boldsymbol{r}}_a] - z_4^j\}^2) \tag{20b}$$

In the fixed-location case with a known attitude, $\hat{\boldsymbol{r}}_a$ is known as are $\hat{\boldsymbol{r}}^1$ through $\hat{\boldsymbol{r}}^L$. The dot product quantity $(\hat{\boldsymbol{r}}^{sp})^{\mathrm{T}}\hat{\boldsymbol{r}}_a$ is the only unknown quantity. In an optimal detection test, this unknown quantity would be integrated out of the probability density expression in Eq. (20b). A simpler sub-optimal approach, however, is to use the value of $(\hat{\boldsymbol{r}}^{sp})^{\mathrm{T}}\hat{\boldsymbol{r}}_a$ that maximizes the probability density in Eq. (20b), i.e., to use the maximum-likelihood estimate of $(\hat{\boldsymbol{r}}^{sp})^{\mathrm{T}}\hat{\boldsymbol{r}}_a$ under the spoofed assumption. This maximum-likelihood estimate also minimizes the negative natural logarithm of the spoofed likelihood function. If this unknown dot product is defined to be $\eta = (\hat{\boldsymbol{r}}^{sp})^{\mathrm{T}}\hat{\boldsymbol{r}}_a$, then the negative-log-likelihood cost function for estimating it is:

$$\begin{aligned} J_{sp}(\eta) &= -\ln[p(z_4^1,\ldots,z_4^L \mid \hat{\boldsymbol{r}}^{sp}, H_1)] + \ln[w] \\ &= \tfrac{1}{2}\sum_{j=1}^{L}(R_{44}^j\eta - z_4^j)^2 \end{aligned} \tag{21}$$

Note that this cost definition cancels the constant negative natural logarithm of the normalizing probability density constant *w* without affecting any subsequent results.

The optimal value of this dot product under the spoofing assumption can be computed by first solving for its unconstrained minimizing value. Standard linear least-squares techniques yield:

$$\eta_{uopt} = \frac{\sum_{j=1}^{L} R_{44}^j z_4^j}{\sum_{j=1}^{L}(R_{44}^j)^2} \tag{22}$$

Afterwards, the constraints $-1 \leq \eta \leq 1$ are enforced to produce the final solution:

$$\eta_{opt} = \begin{cases} -1 & \text{if } \eta_{uopt} < -1 \\ \eta_{uopt} & \text{if } -1 \leq \eta_{uopt} \leq 1 \\ 1 & \text{if } 1 < \eta_{uopt} \end{cases} \tag{23}$$

This constraint arises from the fact that the η dot product is defined between two unit direction vectors.

Given the dot product estimate in Eq. (23), the associated spoofing detection statistic can be defined in terms of the difference between the negative logarithms of the spoofed and non-spoofed probability density functions in, respectively, Eqs. (20b) and (20a). The former quantity is $J_{sp}(\eta_{opt})$. The latter quantity is

$$J_{nonsp} = -\ln[p(z_4^1,\ldots,z_4^L \mid H_0)] + \ln[w]$$
$$= \tfrac{1}{2}\sum_{j=1}^{L} \{R_{44}^j[(\hat{\boldsymbol{r}}^j)^{\mathrm{T}}\hat{\boldsymbol{r}}_a] - z_4^j\}^2 \qquad (24)$$

This latter quantity is defined using the cost-function-like notation "J" even though it contains no unknown quantities that need to be determined via maximum-likelihood optimization. This notation has been adopted because spoofing detection tests for later cases will involve unknown quantities for the non-spoofed H_0 hypothesis in addition to the unknown dot product η for the spoofed H_1 hypothesis.

Given these values, the spoofing detection hypothesis test statistic is

$$\gamma = J_{sp}(\eta_{opt}) - J_{nonsp} \qquad (25)$$

The corresponding spoofing detection test takes the form: Accept the non-spoofed hypothesis H_0 if $\gamma \geq \gamma_{th}$; otherwise, accept the spoofed hypothesis H_1. The quantity γ_{th} is the detection threshold. Its value is determined based on a desired false-alarm probability, as described in the next subsection. Under the reasonable assumption that the use of η_{opt} in $p(z_4^1,\ldots,z_4^L \mid \hat{\boldsymbol{r}}^{sp},H_1)$ yields nearly the same detection performance as would integration of the η uncertainty out of $p(z_4^1,\ldots,z_4^L \mid \hat{\boldsymbol{r}}^{sp},H_1)$, this detection test is nearly optimal. This is true because there is a monotonic relationship between γ and the optimal hypothesis test ratio $p(z_4^1,\ldots,z_4^L \mid H_0) / p(z_4^1,\ldots,z_4^L \mid \hat{\boldsymbol{r}}^{sp},H_1)$.

Before conducting a rigorous analysis, it is worthwhile to note that this detection test makes sense intuitively. If the signals from GNSS satellites $j = 1, \ldots, L$ are not being spoofed, then the non-spoofed carrier-phase model in Eq. (10) should fit the data well. The corresponding weighted sum of squared residual errors, J_{nonsp} in Eq. (24), should be small. The spoofed carrier-phase model in Eq. (15), however, should not fit the data well, and the associated optimized weighted sum of squared residuals, $J_{sp}(\eta_{opt})$, should be large. Therefore, Eq. (25) should produce a large, positive value of the spoofing detection statistic γ. This value will exceed any reasonable choice of γ_{th}, and the lack of spoofing will be correctly identified. In the case of spoofing, however, it is J_{nonsp} that should be large due to the poor fit of the non-spoofed model in Eq. (10), and $J_{sp}(\eta_{opt})$ should be small due to the good fit of the spoofed model in Eq. (15). The resulting γ from Eq. (25) will likely be negative and lie below any reasonable γ_{th} threshold value. The threshold test will successfully detect a spoofing attack in this case.

D. Approximation of Non-Spoofed and Spoofed Probability Density Functions of Spoofing Detection Statistic

Design of the spoofing detection threshold and analysis of the detection power starts with derivation of two probability density functions. One is the probability density function for the detection statistic γ under the non-spoofed hypothesis, $p(\gamma|H_0)$. The other is the γ probability density function under the spoofed hypothesis, $p(\gamma|\eta,H_1)$. The random variability of γ which gives rise to its probability density function in each of these cases derives from the detection statistic's dependence on the zero-mean, identity-covariance L-by-1 Gaussian random vector $\boldsymbol{\nu} = [\, n_4^1 ;\ n_4^2 ;\ n_4^3 ; \ldots ;\ n_4^L \,]$

Analysis of the non-spoofed density function $p(\gamma|H_0)$ yields the result that γ can be expressed as the sum of two uncorrelated random terms:

$$\gamma = -\tfrac{1}{2}\chi_1^2 + y_{nonsp} \qquad (26)$$

where χ_1^2 is a sample from a chi-squared distribution of degree 1 and where y_{nonsp} is a Gaussian random variable with mean and variance:

$$\bar{y}_{nonsp} = \tfrac{1}{2}\sum_{j=1}^{L} \{R_{44}^j[(\hat{\boldsymbol{r}}^j)^{\mathrm{T}}\hat{\boldsymbol{r}}_a]\}^2 - \tfrac{1}{2}\frac{\{\sum_{j=1}^{L} (R_{44}^j)^2[(\hat{\boldsymbol{r}}^j)^{\mathrm{T}}\hat{\boldsymbol{r}}_a]\}^2}{\sum_{j=1}^{L} (R_{44}^j)^2} \qquad (27a)$$

$$\sigma_{ynonsp}^2 = \sum_{j=1}^{L} \{R_{44}^j[(\hat{\boldsymbol{r}}^j)^{\mathrm{T}}\hat{\boldsymbol{r}}_a]\}^2 - \frac{\{\sum_{j=1}^{L} (R_{44}^j)^2[(\hat{\boldsymbol{r}}^j)^{\mathrm{T}}\hat{\boldsymbol{r}}_a]\}^2}{\sum_{j=1}^{L} (R_{44}^j)^2} \qquad (27b)$$

The derivation that leads to Eqs. (26)-(27a) is based on an analysis of the ways in which J_{sp} and J_{nonsp} depend on $\boldsymbol{\nu}$ and on $(\hat{\boldsymbol{r}}^1)^{\mathrm{T}}\hat{\boldsymbol{r}}_a, \ldots, (\hat{\boldsymbol{r}}^L)^{\mathrm{T}}\hat{\boldsymbol{r}}_a$ in the non-spoofed case. It assumes that the optimal estimate η_{opt} from Eq. (23) is based on the middle condition. This is the typical situation, and the expected errors from this assumption are small when the first or third conditions of Eq. (23) apply. Therefore, this is a reasonable simplifying assumption. This simplifying assumption is used in the analysis of every test statistic that is developed in the present paper.

An additional feature of the analysis leading to Eqs. (26)-(27a) involves a special transformation of the Gaussian random vector $\boldsymbol{\nu}$. It is transformed orthogonally into a new vector whose first component is parallel to the unit-norm L-by-1 vector $\boldsymbol{q}_{R44} = [\, R_{44}^1 ;\ \ldots;$

$R_{44}^L]/\sqrt{(R_{44}^1)^2+\ldots+(R_{44}^L)^2}$. The remaining (L-1) components are orthogonal to this vector. The first component of this transformed random vector gives rise to the χ_1^2 term in Eq. (26), and the last (L-1) components give rise to the randomness in the Gaussian term y_{nonsp}.

One final approximation leads to a model of $p(\gamma|H_0)$. This approximation assumes that the randomness in y_{nonsp} dominates the randomness in χ_1^2 in determining the variability of γ for the non-spoofed case. This is reasonable because the variance σ_{ynonsp}^2 is typically much larger than the variance of the term $-\frac{1}{2}\chi_1^2$, which equals 0.5. This approximation leads to

$$\begin{aligned} p(\gamma\,|\,H_0) &\cong N[\gamma;(-\tfrac{1}{2}+\bar{y}_{nonsp}),(\tfrac{1}{2}+\sigma_{ynonsp}^2)^{0.5}] \\ &= N[\gamma;\bar{\gamma}_{nonsp},\sigma_{\gamma nonsp}] \end{aligned} \tag{28}$$

where $N(x;\bar{x},\sigma_x)$ denotes the usual scalar Gaussian distribution:

$$N(x;\bar{x},\sigma_x)=\frac{1}{\sqrt{2\pi}\sigma_x}e^{-(x-\bar{x})^2/(2\sigma_x^2)} \tag{29}$$

and where the mean and standard deviation of the non-spoofed detection statistic are

$$\bar{\gamma}_{nonsp}=-\tfrac{1}{2}+\bar{y}_{nonsp} \tag{30a}$$

$$\sigma_{\gamma nonsp}=\sqrt{\tfrac{1}{2}+\sigma_{ynonsp}^2} \tag{30b}$$

An analysis of the spoofed density function $p(\gamma|\eta,H_1)$ yields the following expression for γ:

$$\gamma=-\tfrac{1}{2}\chi_{nc1}^2+y_{sp} \tag{31}$$

where χ_{nc1}^2 is a sample from a non-central chi-squared distribution of degree 1 and where y_{sp} is a Gaussian random variable. These two random quantities are uncorrelated. The non-centrality parameter of χ_{nc1}^2 is

$$\lambda_{nc}=\frac{\{\sum_{j=1}^{L}(R_{44}^j)^2[\eta-(\hat{\boldsymbol{r}}^j)^{\mathrm{T}}\hat{\boldsymbol{r}}_a]\}^2}{\sum_{j=1}^{L}(R_{44}^j)^2} \tag{32}$$

so that χ_{nc1}^2 is the square of the sum of a zero-mean, unit-variance Gaussian random variable and the constant $\sqrt{\lambda_{nc}}$. The mean and variance of y_{sp} are

$$\begin{aligned} \bar{y}_{sp} &= -\tfrac{1}{2}\sum_{j=1}^{L}\{R_{44}^j[\eta-(\hat{\boldsymbol{r}}^j)^{\mathrm{T}}\hat{\boldsymbol{r}}_a]\}^2 \\ &\quad +\tfrac{1}{2}\frac{\{\sum_{j=1}^{L}(R_{44}^j)^2[\eta-(\hat{\boldsymbol{r}}^j)^{\mathrm{T}}\hat{\boldsymbol{r}}_a]\}^2}{\sum_{j=1}^{L}(R_{44}^j)^2} \end{aligned} \tag{33a}$$

$$\begin{aligned} \sigma_{ysp}^2 &= \sum_{j=1}^{L}\{R_{44}^j[\eta-(\hat{\boldsymbol{r}}^j)^{\mathrm{T}}\hat{\boldsymbol{r}}_a]\}^2 \\ &\quad -\frac{\{\sum_{j=1}^{L}(R_{44}^j)^2[\eta-(\hat{\boldsymbol{r}}^j)^{\mathrm{T}}\hat{\boldsymbol{r}}_a]\}^2}{\sum_{j=1}^{L}(R_{44}^j)^2} \end{aligned} \tag{33b}$$

The analysis that yields Eqs. (31)-(33b) involves the same orthonormal transformation as was used in the non-spoofed case, the one that transforms the Gaussian random vector $\boldsymbol{\nu}$ into a first component parallel to the unit direction vector $\boldsymbol{q}_{R44}$ and the remaining (L-1) components perpendicular to it.

The final form of $p(\gamma|\eta,H_1)$ approximates the randomness in the spoofed version of γ as being dominated by the Gaussian term y_{sp}, similar to the approximation used in the non-spoofed case. Again, This is reasonable because the variance σ_{ysp}^2 is typically much larger than the variance of $-\frac{1}{2}\chi_{nc1}^2$, which equals 0.5+λ_{nc}. The resulting $p(\gamma|\eta,H_1)$ approximation is the Gaussian:

$$\begin{aligned} &p(\gamma\,|\,\eta,H_1) \\ &\quad\cong N[\gamma;(-\tfrac{1}{2}-\tfrac{1}{2}\lambda_{nc}+\bar{y}_{sp}),(\tfrac{1}{2}+\lambda_{nc}+\sigma_{ysp}^2)^{0.5}] \\ &\quad\cong N[\gamma;\bar{\gamma}_{sp}(\eta),\sigma_{\gamma sp}(\eta)] \end{aligned} \tag{34}$$

and where the mean and standard deviation of the non-spoofed detection statistic are

$$\begin{aligned} \bar{\gamma}_{sp}(\eta) &= -\tfrac{1}{2}-\tfrac{1}{2}\lambda_{nc}+\bar{y}_{sp} \\ &= -\tfrac{1}{2}-\tfrac{1}{2}\sum_{j=1}^{L}\{R_{44}^j[\eta-(\hat{\boldsymbol{r}}^j)^{\mathrm{T}}\hat{\boldsymbol{r}}_a]\}^2 \end{aligned} \tag{35a}$$

$$\begin{aligned} \sigma_{\gamma sp}(\eta) &= \sqrt{\tfrac{1}{2}+\lambda_{nc}+\sigma_{ysp}^2} \\ &= \sqrt{\tfrac{1}{2}+\sum_{j=1}^{L}\{R_{44}^j[\eta-(\hat{\boldsymbol{r}}^j)^{\mathrm{T}}\hat{\boldsymbol{r}}_a]\}^2} \end{aligned} \tag{35b}$$

E. Design of Spoofing Detection Threshold and Analysis of Detection Probability

Given the approximation of $p(\gamma|H_0)$, the spoofing detection threshold γ_{th} can be computed as a function of the desired false-alarm probability α. It is determined by solving the following implicit equation for γ_{th}:

$$\begin{aligned} \alpha &= \int_{-\infty}^{\gamma_{th}} p(\gamma\,|\,H_0)d\gamma \\ &= \frac{1}{\sqrt{2\pi}\sigma_{\gamma nonsp}}\int_{-\infty}^{\gamma_{th}} e^{-(\gamma-\bar{\gamma}_{nonsp})^2/(2\sigma_{\gamma nonsp}^2)}d\gamma \end{aligned} \tag{36}$$

Standard software functions exist that can solve this equation for γ_{th}, e.g., MATLAB's "norminv" function.

Given the spoofing detection threshold γ_{th} and the spoofed probability density function approximation $p(\gamma|\eta,H_1)$, the probability of a missed spoofing detection can be calculated as follows:

$$P_{MD} = \int_{\gamma_{th}}^{\infty} p(\gamma\,|\,\eta,H_1)d\gamma$$
$$= \frac{1}{\sqrt{2\pi}\,\sigma_{\gamma sp}(\eta)} \int_{\gamma_{th}}^{\infty} e^{-[\gamma-\bar{\gamma}_{sp}(\eta)]^2/[2\sigma_{\gamma sp}^2(\eta)]} d\gamma \qquad (37)$$

Again, standard software functions, such as MATLAB's "normcdf" function, can be used to compute this probability.

Note how the spoofed mean and standard deviation, $\bar{\gamma}_{sp}(\eta)$ of Eq. (35a) and $\sigma_{\gamma sp}(\eta)$ of Eq. (35b), both depend on the actual spoofed value of the vector dot product η = $(\hat{\boldsymbol{r}}^{sp})^{\mathrm{T}}\hat{\boldsymbol{r}}_a$. This value is never actually known. One could use its estimate from Eq. (23) in order to carry out the calculations in Eqs. (35a), (35b), and (37). Alternatively, one could postulate an *a priori* distribution for η and integrate out the dependence of P_{MD} on this unknown quantity. A preferred approach, however, is to use its worst-case value to compute a worst-case P_{MD}. This value, designated as η_{wc}, is the value that maximizes P_{MD} as computed using Eqs. (35a), (35b), and (37). In typical situations, η_{wc} is the η value that maximizes $\bar{\gamma}_{sp}(\eta)$ in Eq. (35a). This value is

$$\eta_{wc} = \frac{\sum_{j=1}^{L} (R_{44}^j)^2 [(\hat{\boldsymbol{r}}^j)^{\mathrm{T}}\hat{\boldsymbol{r}}_a]}{\sum_{j=1}^{L} (R_{44}^j)^2} \qquad (38)$$

This is the value which minimizes the sum on the extreme right-hand side of Eq. (35a). This maximization of $\bar{\gamma}_{sp}(\eta)$ tends to push more of the area under the $p(\gamma|\eta,H_1)$ vs. γ curve above the detection threshold γ_{th}, thereby increasing P_{MD}. Given this worst-case value, it can be used to define the worst-case mean and standard deviation of γ under the spoofed assumption along with the worst-case probability of missed detection:

$$\bar{\gamma}_{spwc} = -\tfrac{1}{2} - \tfrac{1}{2}\sum_{j=1}^{L} \{R_{44}^j[\eta_{wc} - (\hat{\boldsymbol{r}}^j)^{\mathrm{T}}\hat{\boldsymbol{r}}_a]\}^2 \qquad (39a)$$

$$\sigma_{\gamma spwc} = \sqrt{\tfrac{1}{2} + \sum_{j=1}^{L} \{R_{44}^j[\eta_{wc} - (\hat{\boldsymbol{r}}^j)^{\mathrm{T}}\hat{\boldsymbol{r}}_a]\}^2} \qquad (39b)$$

$$P_{MDwc} = \frac{1}{\sqrt{2\pi}\,\sigma_{\gamma spwc}} \int_{\gamma_{th}}^{\infty} e^{-(\gamma-\bar{\gamma}_{spwc})^2/(2\sigma_{\gamma spwc}^2)} d\gamma \qquad (39c)$$

V. SPOOFING DETECTION HYPOTHESIS TEST FOR MOVING-BASE UE WITH UNKNOWN ATTITUDE

The spoofing detection test of the previous section can be adapted to the situation of an unknown receiver attitude by explicitly considering the possible orientations of the unknown articulation direction vector $\hat{\boldsymbol{r}}_a$. In the spoofed case, the lack of *a priori* knowledge of $\hat{\boldsymbol{r}}_a$ adds no further complication because the lack of knowledge of the direction to the spoofer, $\hat{\boldsymbol{r}}^{sp}$, renders the dot product η = $(\hat{\boldsymbol{r}}^{sp})^{\mathrm{T}}\hat{\boldsymbol{r}}_a$ unknown regardless of whether $\hat{\boldsymbol{r}}_a$ is known or not. In the unspoofed case, however, lack of knowledge of $\hat{\boldsymbol{r}}_a$ has a significant impact.

A. Spoofing Detection Hypothesis Test, Unknown Attitude

The optimal Neyman-Pearson spoofing detection test would multiply $p(z_4^1,...,z_4^L\,|\,\hat{\boldsymbol{r}}_a,H_0)$ from Eq. (20a) by an *a priori* probability distribution for $\hat{\boldsymbol{r}}_a$ and compute the integral over all possible unit-normalized $\hat{\boldsymbol{r}}_a$ values. A more practical approach, however, is to compute the maximum-likelihood estimate of $\hat{\boldsymbol{r}}_a$ and to use it in $p(z_4^1,...,z_4^L\,|\,\hat{\boldsymbol{r}}_a,H_0)$. The maximum-likelihood estimate is the solution to the following minimization problem:

$$\text{find:} \qquad \hat{\boldsymbol{r}}_a \qquad (40a)$$

$$\text{to minimize:} \quad J_{nonsp}(\hat{\boldsymbol{r}}_a) = \tfrac{1}{2}\sum_{j=1}^{L} \{R_{44}^j[(\hat{\boldsymbol{r}}^j)^{\mathrm{T}}\hat{\boldsymbol{r}}_a] - z_4^j\}^2 \qquad (40b)$$

$$\text{subject to:} \quad (\hat{\boldsymbol{r}}_a)^{\mathrm{T}}\hat{\boldsymbol{r}}_a = 1 \qquad (40c)$$

This takes the form of a quadratically-constrained quadratic program. Its minimization of $J_{nonsp}(\hat{\boldsymbol{r}}_a)$ is the equivalent of maximizing $p(z_4^1,...,z_4^L\,|\,\hat{\boldsymbol{r}}_a,H_0)$ because the former function equals a constant plus the negative natural logarithm of the latter.

The constrained optimal estimation problem in Eqs. (40a)-(40c) can be solved using a singular value decomposition coupled with a Lagrange-multiplier/constraint calculation [31]. The computation begins with the singular value decomposition

$$U\begin{bmatrix} \sigma_a & 0 & 0 \\ 0 & \sigma_b & 0 \\ 0 & 0 & \sigma_c \\ 0 & 0 & 0 \\ \vdots & \vdots & \vdots \\ 0 & 0 & 0 \end{bmatrix} V^{\mathrm{T}} = B = \begin{bmatrix} R_{44}^1(\hat{\boldsymbol{r}}^1)^{\mathrm{T}} \\ R_{44}^2(\hat{\boldsymbol{r}}^2)^{\mathrm{T}} \\ R_{44}^3(\hat{\boldsymbol{r}}^3)^{\mathrm{T}} \\ \vdots \\ R_{44}^L(\hat{\boldsymbol{r}}^L)^{\mathrm{T}} \end{bmatrix} \qquad (41)$$

where U is an L-by-L orthonormal matrix, V is a 3-by-3 orthonormal matrix, and $\sigma_a \geq \sigma_b \geq \sigma_c \geq 0$ are the three non-negative singular values, in decreasing order, of the

L-by-3 matrix B that is defined by the expression on the extreme right-hand side of Eq. (41). The B matrix is the input to the singular-value matrix factorization calculations [31], and U, V, σ_a, σ_b, and σ_c are its outputs. Note that the singular values σ_a, σ_b, and σ_c do not represent standard deviations.

Next, the U matrix is used to transform the non-homogeneous terms from the squared-error cost function in Eq. (40b):

$$\begin{bmatrix} z_a \\ z_b \\ z_c \\ \boldsymbol{z}_r \end{bmatrix} = U^{\mathrm{T}} \begin{bmatrix} z_4^1 \\ z_4^2 \\ z_4^3 \\ \vdots \\ z_4^L \end{bmatrix} \tag{42}$$

where z_a, z_b, and z_c are scalars and $\boldsymbol{z}_r$ is a vector of residuals.

Next, one defines the transformed unit direction vector of the antenna articulations:

$$\begin{bmatrix} \breve{r}_a \\ \breve{r}_b \\ \breve{r}_c \end{bmatrix} = \breve{\boldsymbol{r}} = V^{\mathrm{T}} \hat{\boldsymbol{r}}_a \tag{43}$$

The singular-value decomposition and the vector transformations in Eqs. (42) and (43) can be used to pose an equivalent optimal estimation problem in terms of the unknown components of $\breve{\boldsymbol{r}}$:

$$\text{find:} \qquad \breve{\boldsymbol{r}} = [\,\breve{r}_a\,;\breve{r}_b\,;\breve{r}_c\,] \tag{44a}$$

$$\text{to minimize:} \quad J'_{nonsp}(\breve{\boldsymbol{r}}) = \tfrac{1}{2}(\sigma_a\breve{r}_a - z_a)^2 + \tfrac{1}{2}(\sigma_b\breve{r}_b - z_b)^2 + \tfrac{1}{2}(\sigma_c\breve{r}_c - z_c)^2 + \tfrac{1}{2}\boldsymbol{z}_r^{\mathrm{T}}\boldsymbol{z}_r \tag{44b}$$

$$\text{subject to:} \quad \breve{r}_a^2 + \breve{r}_b^2 + \breve{r}_c^2 = 1 \tag{44c}$$

This optimization problem can be solved by first adjoining the unit-norm constraint in Eq. (44c) to the cost function in Eq. (44b) using the undetermined Lagrange multiplier $\mu/2$. Next, one takes the first derivatives of the resulting Lagrangian with respect to the elements of $\breve{\boldsymbol{r}}$ and one solves the resulting equations to yield:

$$\breve{r}_a = \frac{\sigma_a z_a}{\mu + \sigma_a^2}, \quad \breve{r}_b = \frac{\sigma_b z_b}{\mu + \sigma_b^2}, \quad \text{and} \quad \breve{r}_c = \frac{\sigma_c z_c}{\mu + \sigma_c^2} \tag{45}$$

These results are then substituted into the equality constraint in Eq. (44c) to yield a single equation in the single unknown μ:

$$\frac{\sigma_a^2 z_a^2}{(\mu + \sigma_a^2)^2} + \frac{\sigma_b^2 z_b^2}{(\mu + \sigma_b^2)^2} + \frac{\sigma_c^2 z_c^2}{(\mu + \sigma_c^2)^2} = 1 \tag{46}$$

This equation can be transformed into a 6th-order polynomial in μ via multiplication by the product of all the denominator factors in Eq. (46):

$$\begin{aligned} 0 = {} & (\mu + \sigma_a^2)^2(\mu + \sigma_b^2)^2(\mu + \sigma_c^2)^2 \\ & - \sigma_a^2 z_a^2(\mu + \sigma_b^2)^2(\mu + \sigma_c^2)^2 \\ & - \sigma_b^2 z_b^2(\mu + \sigma_a^2)^2(\mu + \sigma_c^2)^2 \\ & - \sigma_c^2 z_c^2(\mu + \sigma_a^2)^2(\mu + \sigma_b^2)^2 \end{aligned} \tag{47}$$

The polynomial in Eq. (47) is solved using standard numerical techniques. The solution procedure will normally yield 6 possible values of μ. The correct value must be real. Typically, it is the minimum real value that is no smaller than $-\sigma_c^2$, which guarantees that the minimum is global. Special cases might arise in which a smaller value of μ yields the optimum if $\sigma_c^2 z_c^2 = 0$. A detailed discussion of this special case is beyond the scope of this paper. The interested reader can refer to the discussion of Fig. 2 in Ref. 33 for treatment of the same special case in a similar optimization problem. Given the globally-optimizing value of μ, it can be substituted into Eq. (45) to determine the elements of $\breve{\boldsymbol{r}}_{opt}$, and Eq. (43) can be inverted to determine $\hat{\boldsymbol{r}}_{aopt} = V\breve{\boldsymbol{r}}_{opt}$. This value of $\hat{\boldsymbol{r}}_{aopt}$ is guaranteed to satisfy the unit normalization constraint in Eq. (40c) by virtue of the unit normalization constraint on $\breve{\boldsymbol{r}}_{opt}$ in Eq. (44c) and by virtue of the orthogonality of the V matrix.

Given this non-spoofed $\hat{\boldsymbol{r}}_{aopt}$ estimate and a spoofed-case η_{opt} estimate computed as per Eqs. (22) and (23), the spoofing detection hypothesis test statistic for this scenario is

$$\gamma = J_{sp}(\eta_{opt}) - J_{nonsp}(\hat{\boldsymbol{r}}_{aopt}) \tag{48}$$

As in Section IV.C, the spoofing detection test takes the form: Accept the non-spoofed hypothesis H_0 if $\gamma \geq \gamma_{th}$; otherwise, accept the spoofed hypothesis H_1. This makes sense because one would expect $J_{nonsp}(\hat{\boldsymbol{r}}_{aopt})$ to be small, $J_{sp}(\eta_{opt})$ to be large, and γ to be a positive number if there were no spoofing. Conversely, one would expect $J_{nonsp}(\hat{\boldsymbol{r}}_{aopt})$ to be large, $J_{sp}(\eta_{opt})$ to be small, and γ to be a negative number if a spoofing attack were in progress. This is not an optimal Neyman-Pearson test because of the use of optimal estimates for the unknown values of η and $\hat{\boldsymbol{r}}_a$ rather than integration over their possible ranges, but experience shows that this type of test is likely to have good detection power.

B. Approximation of Non-Spoofed and Spoofed Probability Density Functions of Spoofing Detection Statistic, Unknown Attitude

The spoofing detection threshold design begins with a derivation of the probability distribution of the detection statistic under the assumption of no spoofing, $p(\gamma|\hat{\mathbf{r}}_a,H_0)$. This analysis must account for the effects of the zero-mean, identity-covariance Gaussian random vector $\boldsymbol{\nu}$ as it propagates through the two optimizations involved in computing γ, the η_{opt} calculation and the $\hat{\mathbf{r}}_{aopt}$ calculation. The important new aspect of this analysis for the moving-base/unknown-attitude test is the effect of the optimal estimation of $\hat{\mathbf{r}}_{aopt}$ on this propagation.

Analysis of the non-spoofed case yields the following approximation for the spoofing detection statistic:

$$\gamma \cong \frac{1}{2}\mathbf{g}_{nonsp}^{\mathrm{T}}(\hat{\mathbf{r}}_a)\mathbf{g}_{nonsp}(\hat{\mathbf{r}}_a)+\mathbf{g}_{nonsp}^{\mathrm{T}}(\hat{\mathbf{r}}_a)\boldsymbol{\nu} + \frac{1}{2}\boldsymbol{\nu}^{\mathrm{T}}[H_{nonsp}(\hat{\mathbf{r}}_a)-\mathbf{q}_{R44}\mathbf{q}_{R44}^{\mathrm{T}}]\boldsymbol{\nu} \tag{49}$$

where the L-by-1 vector $\mathbf{g}_{nonsp}(\hat{\mathbf{r}}_a)$ and the L-by-L symmetric matrix $H_{nonsp}(\hat{\mathbf{r}}_a)$ are

$$\mathbf{g}_{nonsp}(\hat{\mathbf{r}}_a)=(I-\mathbf{q}_{R44}\mathbf{q}_{R44}^{\mathrm{T}})B\hat{\mathbf{r}}_a \tag{50a}$$

$$H_{nonsp}(\hat{\mathbf{r}}_a)=[B\ 0]\begin{bmatrix} B^{\mathrm{T}}B & \hat{\mathbf{r}}_a \\ \hat{\mathbf{r}}_a^{\mathrm{T}} & 0\end{bmatrix}^{-1}\begin{bmatrix} B^{\mathrm{T}} \\ 0\end{bmatrix} \tag{50b}$$

The formula for γ in Eq. (49) is exact to second order in the noise vector $\boldsymbol{\nu}$. It can be derived by approximating the first-order optimality necessary conditions for the solution to the problem in Eqs. (40a)-(40c). This particular approximation is carried out to first order in $\boldsymbol{\nu}$ starting with recognition that the non-homogeneous vector $[z_4^1$; ...; $z_4^L]$ is equal to $B\hat{\mathbf{r}}_a+\boldsymbol{\nu}$ in the non-spoofed case. The resulting derivation is straightforward, but somewhat lengthy.

Note that the $H_{nonsp}(\hat{\mathbf{r}}_a)$ matrix in Eq. (50b) is a projection matrix. Two of its eigenvalues equal 1, and the rest equal 0; it projects onto a 2-dimensional subspace.

The dominant random term in Eq. (49) is $\mathbf{g}_{nonsp}^{\mathrm{T}}(\hat{\mathbf{r}}_a)\boldsymbol{\nu}$. Its variance is typically much larger than that of the quadratic term $\frac{1}{2}\boldsymbol{\nu}^{\mathrm{T}}[H_{nonsp}(\hat{\mathbf{r}}_a)-\mathbf{q}_{R44}\mathbf{q}_{R44}^{\mathrm{T}}]\boldsymbol{\nu}$. It is also typically much larger than the variance of the neglected higher-order terms in $\boldsymbol{\nu}$.

The dominance of the randomness in $\mathbf{g}_{nonsp}^{\mathrm{T}}(\hat{\mathbf{r}}_a)\boldsymbol{\nu}$ implies that a Gaussian approximation of γ is reasonable for this non-spoofed case. Thus

$$p(\gamma\,|\,\hat{\mathbf{r}}_a,H_0)\cong N[\gamma;\bar{\gamma}_{nonsp}(\hat{\mathbf{r}}_a),\sigma_{\gamma nonsp}(\hat{\mathbf{r}}_a)] \tag{51}$$

where the mean and standard deviation of this approximation are:

$$\bar{\gamma}_{nonsp}(\hat{\mathbf{r}}_a)=\frac{1}{2}\mathbf{g}_{nonsp}^{\mathrm{T}}(\hat{\mathbf{r}}_a)\mathbf{g}_{nonsp}(\hat{\mathbf{r}}_a) + \frac{1}{2}trace[H_{nonsp}(\hat{\mathbf{r}}_a)-\mathbf{q}_{R44}\mathbf{q}_{R44}^{\mathrm{T}}] \tag{52a}$$

$$\sigma_{\gamma nonsp}(\hat{\mathbf{r}}_a)=\Big[\mathbf{g}_{nonsp}^{\mathrm{T}}(\hat{\mathbf{r}}_a)\mathbf{g}_{nonsp}(\hat{\mathbf{r}}_a) + \frac{1}{2}trace\{[H_{nonsp}(\hat{\mathbf{r}}_a)-\mathbf{q}_{R44}\mathbf{q}_{R44}^{\mathrm{T}}] \bullet[H_{nonsp}(\hat{\mathbf{r}}_a)-\mathbf{q}_{R44}\mathbf{q}_{R44}^{\mathrm{T}}]\}\Big]^{1/2} \tag{52b}$$

The *trace*() function is the usual sum of the diagonal elements of its square matrix argument.

Analysis of the spoofed case yields a detection statistic approximation that is somewhat similar to that from the non-spoofed case:

$$\gamma \cong -\frac{1}{2}\mathbf{g}_{sp}^{\mathrm{T}}(\eta)\mathbf{g}_{sp}(\eta)+\mathbf{g}_{sp}^{\mathrm{T}}(\eta)\boldsymbol{\nu} + \frac{1}{2}\boldsymbol{\nu}^{\mathrm{T}}[H_{sp}(\eta)-\mathbf{q}_{R44}\mathbf{q}_{R44}^{\mathrm{T}}]\boldsymbol{\nu} \tag{53}$$

where the L-by-1 residuals vector $\mathbf{g}_{sp}(\eta)$ and the L-by-L symmetric matrix $H_{sp}(\eta)$ are

$$\mathbf{g}_{sp}(\eta)=B\tilde{\mathbf{r}}_a(\eta)-\begin{bmatrix} R_{44}^1\eta \\ R_{44}^2\eta \\ R_{44}^3\eta \\ \vdots \\ R_{44}^L\eta\end{bmatrix} \tag{54a}$$

$$H_{sp}(\eta)=[B\ 0]\begin{bmatrix} \{B^{\mathrm{T}}B+\tilde{\mu}(\eta)I\} & \tilde{\mathbf{r}}_a(\eta) \\ \tilde{\mathbf{r}}_a^{\mathrm{T}}(\eta) & 0\end{bmatrix}^{-1}\begin{bmatrix} B^{\mathrm{T}} \\ 0\end{bmatrix} \tag{54b}$$

The 3-by-1 unit direction vector $\tilde{\mathbf{r}}_a(\eta)$ in these formulas is the solution to an auxiliary articulation direction estimation problem that takes the form of Eqs. (40a)-(40c), except with z_4^j replaced by $R_{44}^j\eta$ for all GNSS satellites j = 1, ..., L. The scalar Lagrange multiplier $\tilde{\mu}(\eta)$ is the value that solves Eq. (47) in the process of solving for $\tilde{\mathbf{r}}_a(\eta)$.

The approximation in Eq. (53) is valid to second order in the noise vector $\boldsymbol{\nu}$. It can be derived by approximating the first-order optimality necessary conditions for the solution to the problem in Eqs. (40a)-(40c). This latter approximation is carried out to first order in $\boldsymbol{\nu}$ by recognizing that the non-homogeneous vector $[z_4^1$, ..., $z_4^L]^{\mathrm{T}}$ is equal to $[R_{44}^1\eta$,..., $R_{44}^L\eta]^{\mathrm{T}}+\boldsymbol{\nu}$ in the spoofed case. The resulting derivation is lengthy and somewhat tricky.

One difficult part of the derivation relies on the equation:

$$\boldsymbol{g}_{sp}^{\mathrm{T}}(\eta)B\Delta\hat{\boldsymbol{r}}_a = \tfrac{1}{2}\tilde{\mu}(\eta)\Delta\hat{\boldsymbol{r}}_a^{\mathrm{T}}\Delta\hat{\boldsymbol{r}}_a \qquad (55)$$

in order to recognize that a seemingly first-order term in the unit-vector perturbation $\Delta\hat{\boldsymbol{r}}_a$ = $\hat{\boldsymbol{r}}_a$ - $\tilde{\boldsymbol{r}}_a(\eta)$ is actually second-order in this small quantity. This substitution is crucial to the proof that a first-order approximation of how $\Delta\hat{\boldsymbol{r}}_a$ depends on $\boldsymbol{\nu}$ can be used to achieve a second-order approximation of how the optimized $J_{nonsp}(\hat{\boldsymbol{r}}_a)$ depends on $\boldsymbol{\nu}$. Equation (55) can be derived by considering the first-order necessary conditions that are obeyed by $\tilde{\boldsymbol{r}}_a(\eta)$ and $\tilde{\mu}(\eta)$ and by recognizing that the unit normalization constraint on the perturbed solution $\tilde{\boldsymbol{r}}_a(\eta)+\Delta\hat{\boldsymbol{r}}_a$ can be manipulated into the form 0 = $\tilde{\boldsymbol{r}}_a^{\mathrm{T}}(\eta)\Delta\hat{\boldsymbol{r}}_a + \tfrac{1}{2}\Delta\hat{\boldsymbol{r}}_a^{\mathrm{T}}\Delta\hat{\boldsymbol{r}}_a$.

Similar to the non-spoofed case, the term $\boldsymbol{g}_{sp}^{\mathrm{T}}(\eta)\boldsymbol{\nu}$ on the right-hand side of Eq. (53) is usually the dominant source of random variations. That is, its variance is much larger than those of the quadratic term $\frac{1}{2}\boldsymbol{\nu}^{\mathrm{T}}[H_{sp}(\eta)-\boldsymbol{q}_{R44}\boldsymbol{q}_{R44}^{\mathrm{T}}]\boldsymbol{\nu}$ and the neglected higher-order $\boldsymbol{\nu}$ terms. Therefore, a Gaussian approximation of the spoofing detection statistic is reasonable in this spoofed case:

$$p(\gamma\,|\,\eta,H_1) \cong N[\gamma;\bar{\gamma}_{sp}(\eta),\sigma_{\gamma sp}(\eta)] \qquad (56)$$

with the mean and standard deviation:

$$\bar{\gamma}_{sp}(\eta) = -\frac{1}{2}\boldsymbol{g}_{sp}^{\mathrm{T}}(\eta)\boldsymbol{g}_{sp}(\eta) + \frac{1}{2}trace[H_{sp}(\eta)-\boldsymbol{q}_{R44}\boldsymbol{q}_{R44}^{\mathrm{T}}] \qquad (57a)$$

$$\sigma_{\gamma sp}(\eta) = \Big[\boldsymbol{g}_{sp}^{\mathrm{T}}(\eta)\boldsymbol{g}_{sp}(\eta) + \frac{1}{2}trace\{[H_{sp}(\eta)-\boldsymbol{q}_{R44}\boldsymbol{q}_{R44}^{\mathrm{T}}] \bullet [H_{sp}(\eta)-\boldsymbol{q}_{R44}\boldsymbol{q}_{R44}^{\mathrm{T}}]\}\Big]^{1/2} \qquad (57b)$$

C. Design of Worst-Case Spoofing Detection Threshold and Analysis of Worst-Case Detection Probability, Unknown Attitude

One might be tempted to compute the spoofing detection threshold γ_{th} using $p(\gamma\,|\,\hat{\boldsymbol{r}}_a,H_0)$ in Eq. (51) along with the desired false-alarm rate α, similar to what is done in Eq. (36) for the known-attitude case. This is impractical, however, because the mean and standard deviation that define $p(\gamma\,|\,\hat{\boldsymbol{r}}_a,H_0)$ are functions of the unknown true antenna articulation direction $\hat{\boldsymbol{r}}_a$. One might try using the estimated value of this vector, $\hat{\boldsymbol{r}}_{aopt}$, but a safer approach is to use a worst-case direction.

The worst-case value of the articulation direction $\hat{\boldsymbol{r}}_a$ can be defined as follows: It is the direction which gives the highest possible false-alarm probability for the designed spoofing detection threshold value γ_{th}. Suppose that the worst-case direction is denoted as $\hat{\boldsymbol{r}}_{awc}$. This direction and the corresponding spoofing detection threshold γ_{th} can be computed simultaneously for a given worst-case false-alarm probability α_{wc}.

The first step is to compute the transformed detection threshold that would produce the false-alarm probability α_{wc} if $p(\gamma|H_0)$ were a Gaussian with zero mean and unit variance. Call this value κ_{wc}. It is the solution of

$$\alpha_{wc} = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\kappa_{wc}} e^{-\gamma_{nd}^2/2}d\gamma_{nd} \qquad (58)$$

This value is a measure of the offset of the spoofing detection threshold from the mean of $p(\gamma\,|\,\hat{\boldsymbol{r}}_a,H_0)$ measured in units of standard deviations of $p(\gamma\,|\,\hat{\boldsymbol{r}}_a,H_0)$. This κ_{wc} is normally a negative number because α_{wc} is normally much less than 0.5.

The transformed detection threshold is used to define an optimization problem that can be solved in order to determine the worst-case antenna articulation direction vector and the corresponding worst-case spoofing detection threshold. The optimization problem is:

find: $\hat{\boldsymbol{r}}_a$ (59a)

to minimize: $J_{\gamma th}(\hat{\boldsymbol{r}}_a) = \bar{\gamma}_{nonsp}(\hat{\boldsymbol{r}}_a) + \kappa_{wc}\sigma_{\gamma nonsp}(\hat{\boldsymbol{r}}_a)$ (59b)

subject to: $\hat{\boldsymbol{r}}_a^{\mathrm{T}}\hat{\boldsymbol{r}}_a = 1$ (59c)

The antenna articulation direction that minimizes the cost function in Eq. (59b) is $\hat{\boldsymbol{r}}_{awc}$, the one that produces the highest probability of false alarm for the given spoofing detection test. The corresponding worst-case spoofing detection threshold is equal to the value of the minimum cost: γ_{th} = $J_{\gamma th}(\hat{\boldsymbol{r}}_{awc})$. Given that $J_{\gamma th}(\hat{\boldsymbol{r}}_a) \geq J_{\gamma th}(\hat{\boldsymbol{r}}_{awc})$ for any other articulation direction $\hat{\boldsymbol{r}}_a$, the corresponding false alarm probability for the direction $\hat{\boldsymbol{r}}_a$ is

$$\alpha(\hat{\boldsymbol{r}}_a) = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\kappa(\hat{\boldsymbol{r}}_a)} e^{-\gamma_{nd}^2/2}d\gamma_{nd} \leq \alpha_{wc} \qquad (60)$$

where $\kappa(\hat{\boldsymbol{r}}_a)$ = $[\gamma_{th}-\bar{\gamma}_{nonsp}(\hat{\boldsymbol{r}}_a)]/\sigma_{\gamma nonsp}(\hat{\boldsymbol{r}}_a)$. The inequality $\gamma_{th} = J_{\gamma th}(\hat{\boldsymbol{r}}_{awc}) \leq J_{\gamma th}(\hat{\boldsymbol{r}}_a)$ can be manipulated algebraically and then combined with the definition of $\kappa(\hat{\boldsymbol{r}}_a)$ to prove that $\kappa(\hat{\boldsymbol{r}}_a)$ ≤ κ_{wc}. This latter inequality leads directly to the inequality in Eq. (60). Thus, α_{wc} truly is the worst-case false-alarm probability.

Solution of the constrained nonlinear optimization problem in Eqs. (59a)-(59c) can be carried out using a suitable numerical method. In the tests of Section IX, Newton's method [31] has been used with enhancements to ensure global convergence and to enforce the normalization constraint. The method starts with a guess of $\hat{\boldsymbol{r}}_{awc}$ that satisfies the constraint, and it computes increments that continue to satisfy this constraint while decreasing the cost. The increments are computed by developing a second-order expansion of the cost function variations that applies in the 2-dimensional local null space of the normalization constraint [31]. Global convergence is enforced by using a quadratic trust-region step size restriction when solving for the increment in the null-space of the constraint [31,34].

It is important to start the numerical solution of the optimization problem in Eqs. (59a)-(59c) in with a reasonable first guess of $\hat{\boldsymbol{r}}_{awc}$. Otherwise, the iterative numerical solution procedure can take too much computation time or it can even fail to converge to the global minimum. The first guess algorithm recognizes that the $\boldsymbol{g}_{nonsp}^{\mathrm{T}}(\hat{\boldsymbol{r}}_a)\boldsymbol{g}_{nonsp}(\hat{\boldsymbol{r}}_a)$ terms are the dominant terms in the formulas for $\bar{\gamma}_{nonsp}(\hat{\boldsymbol{r}}_a)$ and $\sigma_{\gamma nonsp}(\hat{\boldsymbol{r}}_a)$ in Eqs. (52a) and (52b). Therefore, it finds the values of $\hat{\boldsymbol{r}}_a$ that maximize or minimize $\boldsymbol{g}_{nonsp}^{\mathrm{T}}(\hat{\boldsymbol{r}}_a)\boldsymbol{g}_{nonsp}(\hat{\boldsymbol{r}}_a)$. Consistent with the formula for $\boldsymbol{g}_{nonsp}(\hat{\boldsymbol{r}}_a)$ in Eq. (50a), these values of $\hat{\boldsymbol{r}}_a$ and the associated extrema of $\boldsymbol{g}_{nonsp}^{\mathrm{T}}(\hat{\boldsymbol{r}}_a)\boldsymbol{g}_{nonsp}(\hat{\boldsymbol{r}}_a)$ can be found by computing the singular value decomposition of the L-by-3 matrix $(I-\boldsymbol{q}_{R44}\boldsymbol{q}_{R44}^{\mathrm{T}})B$. The minimum and maximum values of $\boldsymbol{g}_{nonsp}^{\mathrm{T}}(\hat{\boldsymbol{r}}_a)\boldsymbol{g}_{nonsp}(\hat{\boldsymbol{r}}_a)$ are then used in truncated versions of Eqs. (52a) and (52b) to compute the approximations $\bar{\gamma}_{nonsp}(\hat{\boldsymbol{r}}_a) \cong 0.5\boldsymbol{g}_{nonsp}^{\mathrm{T}}(\hat{\boldsymbol{r}}_a)\boldsymbol{g}_{nonsp}(\hat{\boldsymbol{r}}_a)$ and $\sigma_{\gamma nonsp}(\hat{\boldsymbol{r}}_a) \cong [\boldsymbol{g}_{nonsp}^{\mathrm{T}}(\hat{\boldsymbol{r}}_a)\boldsymbol{g}_{nonsp}(\hat{\boldsymbol{r}}_a)]^{0.5}$. These approximations, in turn, are used to compute corresponding approximations of $J_{\gamma th}(\hat{\boldsymbol{r}}_a)$ from Eq. (59b). For the approximation of $J_{\gamma th}(\hat{\boldsymbol{r}}_a)$ that is the smallest, the corresponding value of $\hat{\boldsymbol{r}}_a$ from the singular decomposition of $(I-\boldsymbol{q}_{R44}\boldsymbol{q}_{R44}^{\mathrm{T}})B$ is used as the first guess of $\hat{\boldsymbol{r}}_{awc}$.

Given the spoofing detection threshold γ_{th} from the worst-case analysis, the final analysis problem is to compute the probability of a missed detection. This calculation involves $p(\gamma \,|\, \eta, H_1)$. Unfortunately, this probability density function depends on the unknown true value of the spoofed-case dot product η. As in the case of a known articulation direction vector, the case of Section IV, a worst-case value of η is computed and used in order to remove the η dependence. The worst-case value of η is the one that produces the largest possible value of P_{MD}.

The worst-case value of η is the solution to the following optimization problem:

find: $\quad \eta$ (61a)

to minimize: $\quad J_{PMD}(\eta) = \dfrac{\gamma_{th} - \bar{\gamma}_{sp}(\eta)}{\sigma_{\gamma sp}(\eta)}$ (61b)

subject to: $\quad -1 \le \eta \le 1$ (61c)

This is a relatively simple constrained 1-dimensional nonlinear optimization problem. It is solved using Newton's method with enhancements to enforce the inequality constraints, if one or the other of them is active, and to ensure global convergence [31,34].

It is helpful to start the numerical solution of the problem in Eqs. (61a)-(61c) with a good first guess of the solution η_{wc}. A good first guess comes from recognizing that, in a well-designed spoofing detection test, the $\boldsymbol{g}_{sp}^{\mathrm{T}}(\eta)\boldsymbol{g}_{sp}(\eta)$ terms are the dominant terms in the formulas for $\bar{\gamma}_{sp}(\eta)$ and $\sigma_{\gamma sp}(\eta)$ in Eqs. (57a) and (57b). Also, the term $-\bar{\gamma}_{sp}(\eta)/\sigma_{\gamma sp}(\eta)$ in Eq. (61b) contains the dominant η dependence of $J_{PMD}(\eta)$. Under these two assumptions, a reasonable first guess of η_{wc} is

$$\eta_{wc} = \frac{\boldsymbol{q}_{R44}^{\mathrm{T}} B \hat{\boldsymbol{r}}_{amineig}}{\sqrt{\sum\limits_{j=1}^{L} (R_{44}^{j})^2}} \tag{62}$$

where $\hat{\boldsymbol{r}}_{amineig}$ is a unit-normalized eigenvector of the 3-by-3 symmetric matrix

$$B^{\mathrm{T}}(I - \boldsymbol{q}_{R44}\boldsymbol{q}_{R44}^{\mathrm{T}})B \tag{63}$$

It is the eigenvector associated with the minimum eigenvalue. It is straightforward to prove that this combination of η minimizes $\boldsymbol{g}_{sp}^{\mathrm{T}}(\eta)\boldsymbol{g}_{sp}(\eta)$ with $\boldsymbol{g}_{sp}(\eta)$ defined in Eq. (54a). The proof involves the recognition that the unit-vector $\tilde{\boldsymbol{r}}_a(\eta_{wc}) = \hat{\boldsymbol{r}}_{amineig}$, where the function $\tilde{\boldsymbol{r}}_a(\eta)$ is defined in connection with Eq. (54a). One can show that this first guess of η_{wc} is guaranteed to respect the inequality constraints in Eq. (61c) because it amounts to a weighted average of the unit-vector dot products $(\hat{\boldsymbol{r}}^{j})^{\mathrm{T}}\hat{\boldsymbol{r}}_{amineig}$ for j = 1, ..., L, each of which obeys the constraints.

Given the value η_{wc} that solves the optimization problem in Eqs. (61a)-(61c), the worst-case probability of missed detection is

$$\begin{aligned} P_{MDwc} &= \frac{1}{\sqrt{2\pi}\,\sigma_{\gamma sp}(\eta_{wc})}\int_{\gamma_{th}}^{\infty} e^{-[\gamma-\bar{\gamma}_{sp}(\eta_{wc})]^2/[2\sigma_{\gamma sp}^2(\eta_{wc})]}d\gamma \\ &= \frac{1}{\sqrt{2\pi}}\int_{J_{PMD}(\eta_{wc})}^{\infty} e^{-\gamma_{nd}^2/2}d\gamma_{nd} \end{aligned} \tag{64}$$

The transformation from the first integral to the second integral is carried out by the change of dummy integration variable from γ to $\gamma_{nd} = [\gamma - \bar{\gamma}_{sp}(\eta_{wc})]/\sigma_{\gamma sp}(\eta_{wc})$. For any other actual η value, the probability of missed detection is

$$P_{MD}(\eta) = \frac{1}{\sqrt{2\pi}}\int_{J_{PMD}(\eta)}^{\infty} e^{-\gamma_{nd}^2/2}d\gamma_{nd} \le P_{MDwc} \tag{65}$$

The inequality at the end of Eq. (65) is true because the lower limit in this integral will be no smaller than the lower limit in the corresponding integral of Eq. (64) by virtue of η_{wc} being the value that minimizes $J_{PMD}(\eta)$.

These false-alarm and missed-detection probability calculations need to be re-evaluated from time to time. They must be re-computed each time there is a change in the set of available GNSS signals and each time there are significant changes in any of the following quantities: the duration of the spoofing detection batch interval, the interval's antenna articulation time history $\rho_a(t)$, the direction vectors to the GNSS spacecraft, $\hat{\boldsymbol{r}}^j$ for $j = 1, ..., L$, or the carrier-to-noise ratios of the GNSS signals. Although their derivations are long and complex, these calculations involve only matrix-matrix, matrix-vector, and nonlinear optimization calculations for low-dimensional problems. Therefore, they can be executed very rapidly on typical processors, and they can be implemented in a practical real-time system.

VI. SPOOFING DETECTION HYPOTHESIS TEST FOR MOVING-BASE UE WITH UNKNOWN ATTITUDE AND UNKNOWN ARTICULATION AMPLITUDE

A third version of the spoofing detection test with uni-axial antenna articulation allows for the possibility that the amplitude of the motion is also unknown. This could happen if a system such as that shown in Fig. 3 were excited by an initial impulse of uncertain amplitude. It also could happen with an antenna mounted on a UAV where the antenna articulations were caused by rapid controller-induced attitude motions and where the gain of the transfer function from the control inputs to the antenna motions was uncertain. In this case, it is necessary to estimate both the direction of antenna articulation and an articulation amplitude scaling factor. It is assumed that there is a known minimum antenna articulation amplitude. Otherwise, the spoofing detection test could be very weak due to having an articulation amplitude that was too small.

A. Spoofing Detection Hypothesis Test, Unknown Attitude and Unknown Amplitude Scaling

As with the previous two tests, a test statistic based on optimal estimates of unknown parameters is used in place of a truly optimal Neyman-Pearson test. This approach is used because it is easier to implement and because it typically involves only a small degradation of detection power for a given false-alarm probability.

For the non-spoofed case, the spoofing detection calculation must estimate the product of the unknown articulation direction $\hat{\boldsymbol{r}}_a$ and an articulation amplitude scaling factor a. This scaling factor is defined so that the nominal articulation amplitude time history in the $\hat{\boldsymbol{r}}_a$ direction is $\rho_a(t)$ while the true time history is $a\rho_a(t)$. Supposed that one defines the un-normalized vector $\boldsymbol{r}_a = a\hat{\boldsymbol{r}}_a$. Suppose also, without loss of generality, that $\rho_a(t)$ and a are defined to set the known lower bound for a equal to 1. Then the following optimization problem is solved to estimate the direction/amplitude product vector $\boldsymbol{r}_a$:

$$\text{find:} \qquad \boldsymbol{r}_a \tag{66a}$$

$$\text{to minimize:} \quad J_{nonsp}(\boldsymbol{r}_a) = \frac{1}{2}\sum_{j=1}^{L}\{R_{44}^j[(\hat{\boldsymbol{r}}^j)^{\mathrm{T}}\boldsymbol{r}_a] - z_4^j\}^2 \tag{66b}$$

$$\text{subject to:} \quad \boldsymbol{r}_a^{\mathrm{T}}\boldsymbol{r}_a \geq 1 \tag{66c}$$

where R_{44}^j and z_4^j for $j = 1, ..., L$ are computed as defined in Eqs. (17) and (18). The cost function in Eq. (66b) is identical to the non-spoofed cost function in the previous spoofing detection calculation, the one in Eq. (40b).

The optimization problem in Eqs. (66a)-(66c) can be solved in almost an identical manner to the solution of the equality-constrained problem for $\hat{\boldsymbol{r}}_a$ in Eqs. (40a)-(40c). The only difference is that the initial trial solution assumes that the inequality constraint in Eq. (66c) is inactive. The constraint can be ignored in this case, and μ can be set equal to 0 in Eq. (45) to determine the components of $\breve{\boldsymbol{r}}_{opt}$ that are used to compute the initial trial solution $\boldsymbol{r}_{aopt} = V\breve{\boldsymbol{r}}_{opt}$. If this trial value of $\boldsymbol{r}_{aopt}$ satisfies the inequality in Eq. (66c), then the solution procedure is done. If this candidate $\boldsymbol{r}_{aopt}$ violates Eq. (66c), however, then Eq. (47) is used to determine the Kuhn-Tucker multiplier μ. A negative value of μ that satisfies Eq. (47) must be used for the final solution in order to satisfy the Kuhn-Tucker first-order optimality conditions [31,34].

For the spoofed case, the original unknown dot product between unit vectors $\eta = (\hat{\boldsymbol{r}}^{sp})^{\mathrm{T}}\hat{\boldsymbol{r}}_a$ is redefined to become the product of the unknown amplitude scaling factor and the unknown dot product: $\eta = a(\hat{\boldsymbol{r}}^{sp})^{\mathrm{T}}\hat{\boldsymbol{r}}_a = (\hat{\boldsymbol{r}}^{sp})^{\mathrm{T}}\boldsymbol{r}_a$. The practical effect of this re-definition of η is that it is no longer constrained to lie in the range $-1 \leq \eta \leq 1$ because of the possibility that $a > 1$. Therefore, the spoofed-case estimation problem becomes that of finding η to minimize the cost function in Eq. (21) subject to no constraints on η. The minimizing value is just the unconstrained minimum η_{uopt} from Eq. (22).

Given the $\boldsymbol{r}_{aopt}$ solution to the problem in Eqs. (66a)-(66c) and the η_{uopt} estimate from Eq. (22), this case uses the spoofing detection hypothesis test statistic

$$\gamma = J_{sp}(\eta_{uopt}) - J_{nonsp}(\boldsymbol{r}_{aopt}) \tag{67}$$

The spoofing detection test has the same form is in the previous two cases: Accept the non-spoofed hypothesis H_0 if $\gamma \geq \gamma_{th}$; otherwise, accept the spoofed hypothesis H_1. Again, this is sensible because $J_{nonsp}(\boldsymbol{r}_{aopt})$ should be small, $J_{sp}(\eta_{uopt})$ should be large, and γ should be a positive number without spoofing. The quantity $J_{nonsp}(\boldsymbol{r}_{aopt})$ should be large, $J_{sp}(\eta_{uopt})$ should be small, and γ should be a negative number during a spoofing attack.

B. Approximation of Non-Spoofed and Spoofed Probability Density Functions of Spoofing Detection Statistic, Unknown Attitude and Unknown Amplitude Scaling

As in the analyses of the previous spoofing detection statistics, design of the detection threshold and analysis of the probability of missed detection begin with the determination of $p(\gamma|\boldsymbol{r}_a,H_0)$, the non-spoofed probability density of the detection statistic. This analysis quantifies the impact of the random vector $\boldsymbol{\nu}$ on γ as propagated through the η_{uopt} and $\boldsymbol{r}_{aopt}$ calculations. That quantification is similar to Eq. (49) for the known-amplitude case. It is approximated to 2nd order in $\boldsymbol{\nu}$ as follows:

$$\gamma \cong \frac{1}{2}\boldsymbol{g}_{nonsp}^{\mathrm{T}}(\boldsymbol{r}_a)\boldsymbol{g}_{nonsp}(\boldsymbol{r}_a) + \boldsymbol{g}_{nonsp}^{\mathrm{T}}(\boldsymbol{r}_a)\boldsymbol{\nu} + \frac{1}{2}\boldsymbol{\nu}^{\mathrm{T}}(H_{nonsp}^{'} - \boldsymbol{q}_{R44}\boldsymbol{q}_{R44}^{\mathrm{T}})\boldsymbol{\nu} - \frac{1}{2}\bar{\hat{\nu}}^2(\boldsymbol{r}_a) \tag{68}$$

where the function $\boldsymbol{g}_{nonsp}(\boldsymbol{r}_a)$ is the same as in Eq. (50a) and where the L-by-L symmetric matrix $H_{nonsp}^{'} = B(B^{\mathrm{T}}B)^{-1}B^{\mathrm{T}}$ is a projection matrix. The scalar random variable $\bar{\hat{\nu}}(\boldsymbol{r}_a)$ accounts for the fact that the noise vector $\boldsymbol{\nu}$ may cause the $\boldsymbol{r}_{aopt}$ calculation to produce a negative Kuhn-Tucker multiplier μ even though $\mu = 0$ would suffice in the absence of noise because the true $\boldsymbol{r}_a$ respects the inequality in Eq. (66c). This scalar random variable is correlated with the random vector $\boldsymbol{\nu}$, as is a related zero-mean, unit-variance scalar Gaussian random variable $\hat{\nu}(\boldsymbol{r}_a)$. These two distributions and their relationships to each other and to $\boldsymbol{\nu}$ are characterized by the following formulas:

$$\bar{\hat{\nu}}(\boldsymbol{r}_a) = \begin{cases} \hat{\nu}(\boldsymbol{r}_a) - \hat{\nu}_{\max}(\boldsymbol{r}_a) & \text{if } \hat{\nu}(\boldsymbol{r}_a) < \hat{\nu}_{\max}(\boldsymbol{r}_a) \\ 0 & \text{if } \hat{\nu}_{\max}(\boldsymbol{r}_a) \leq \hat{\nu}(\boldsymbol{r}_a) \end{cases} \tag{69}$$

where

$$\hat{\nu}(\boldsymbol{r}_a) = \hat{\boldsymbol{q}}^{\mathrm{T}}(\boldsymbol{r}_a)\boldsymbol{\nu} \tag{70a}$$

$$\hat{\nu}_{\max}(\boldsymbol{r}_a) = \frac{1 - \boldsymbol{r}_a^{\mathrm{T}}\boldsymbol{r}_a}{2\sqrt{\boldsymbol{r}_a^{\mathrm{T}}(B^{\mathrm{T}}B)^{-1}\boldsymbol{r}_a}} \tag{70b}$$

with $\hat{\boldsymbol{q}}(\boldsymbol{r}_a)$ being the following unit-normalized L-by-1 vector:

$$\hat{\boldsymbol{q}}(\boldsymbol{r}_a) = \frac{B(B^{\mathrm{T}}B)^{-1}\boldsymbol{r}_a}{\sqrt{\boldsymbol{r}_a^{\mathrm{T}}(B^{\mathrm{T}}B)^{-1}\boldsymbol{r}_a}} \tag{71}$$

If $\boldsymbol{r}_a^{\mathrm{T}}\boldsymbol{r}_a >> 1$, then $\hat{\nu}_{\max}(\boldsymbol{r}_a) << 0$, and the contribution of $\bar{\hat{\nu}}(\boldsymbol{r}_a)$ to the randomness in γ becomes negligible, as one would expect.

The derivation of the approximation in Eq. (68) is similar to the derivation of the approximation in Eq. (49) for the known-amplitude case. The terms $\frac{1}{2}\boldsymbol{\nu}^{\mathrm{T}}H_{nonsp}^{'}\boldsymbol{\nu} - \frac{1}{2}\bar{\hat{\nu}}^2(\boldsymbol{r}_a)$ in Eq. (68) constitute the modified form of the term $\frac{1}{2}\boldsymbol{\nu}^{\mathrm{T}}H_{nonsp}(\hat{\boldsymbol{r}}_a)\boldsymbol{\nu}$ in Eq. (49) when the equality constraint in Eq. (40c) is replaced by the inequality constraint in Eq. (66c). This replacement leads to a negativity constraint on the Kuhn-Tucker multiplier μ associated with the Eqs. (66a)-(66c) optimal solution, and this constraint is what modifies the original $\frac{1}{2}\boldsymbol{\nu}^{\mathrm{T}}H_{nonsp}(\hat{\boldsymbol{r}}_a)\boldsymbol{\nu}$ term. There was no sign constraint on the corresponding Lagrange multiplier for the Eqs. (40a)-(40c) optimum.

Similar to the known-amplitude case, the dominant random term in Eq. (68) is $\boldsymbol{g}_{nonsp}^{\mathrm{T}}(\boldsymbol{r}_a)\boldsymbol{\nu}$. Normally its variance is significantly larger than the variance of the quadratic terms $\frac{1}{2}\boldsymbol{\nu}^{\mathrm{T}}[H_{nonsp}^{'} - \boldsymbol{q}_{R44}\boldsymbol{q}_{R44}^{\mathrm{T}}]\boldsymbol{\nu}$ and $-\frac{1}{2}\bar{\hat{\nu}}^2(\boldsymbol{r}_a)$. This variance is also normally a lot larger than the variance of the neglected higher order $\boldsymbol{\nu}$ terms. Therefore, it is reasonable to approximate the probability density function of γ in the non-spoofed case by a Gaussian:

$$p(\gamma|\boldsymbol{r}_a,H_0) \cong N[\gamma;\bar{\gamma}_{nonsp}^{'}(\boldsymbol{r}_a),\sigma_{\gamma nonsp}^{'}(\boldsymbol{r}_a)] \tag{72}$$

where the mean and standard deviation of this approximation are:

$$\bar{\gamma}_{nonsp}^{'}(\boldsymbol{r}_a) = \frac{1}{2}\boldsymbol{g}_{nonsp}^{\mathrm{T}}(\boldsymbol{r}_a)\boldsymbol{g}_{nonsp}(\boldsymbol{r}_a) + \frac{1}{2}trace[H_{nonsp}^{'} - \boldsymbol{q}_{R44}\boldsymbol{q}_{R44}^{\mathrm{T}}] - \frac{1}{2}\xi_{ns}(\boldsymbol{r}_a) \tag{73a}$$

$$\sigma_{\gamma nonsp}^{'}(\boldsymbol{r}_a) = \Big[\boldsymbol{g}_{nonsp}^{\mathrm{T}}(\boldsymbol{r}_a)\boldsymbol{g}_{nonsp}(\boldsymbol{r}_a) \quad \frac{1}{2}trace\{[H_{nonsp}^{'} - \boldsymbol{q}_{R44}\boldsymbol{q}_{R44}^{\mathrm{T}}] \bullet [H_{nonsp}^{'} - \boldsymbol{q}_{R44}\boldsymbol{q}_{R44}^{\mathrm{T}}]\} + \psi_{ns}(\boldsymbol{r}_a)\Big]^{1/2} \tag{73b}$$

where

$$\xi_{ns}(\boldsymbol{r}_a) = E\{\bar{\hat{\nu}}^2(\boldsymbol{r}_a)\} = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\hat{\nu}_{\max}(\boldsymbol{r}_a)}[\hat{\nu} - \hat{\nu}_{\max}(\boldsymbol{r}_a)]^2 e^{-\hat{\nu}^2/2}d\hat{\nu}$$

$$= \frac{\hat{\nu}_{\max}(\boldsymbol{r}_a) e^{-\hat{\nu}_{\max}^2(\boldsymbol{r}_a)/2}}{\sqrt{2\pi}}$$

$$+ [1 + \hat{\nu}_{\max}^2(\boldsymbol{r}_a)] \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\hat{\nu}_{\max}(\boldsymbol{r}_a)} e^{-\hat{\nu}^2/2} d\hat{\nu} \tag{74a}$$

$$\begin{aligned}
\psi_{ns}(\boldsymbol{r}_a) = & -E\{[\boldsymbol{g}_{nonsp}^{\mathrm{T}}(\boldsymbol{r}_a)\boldsymbol{\nu}][\hat{\bar{\nu}}^2(\boldsymbol{r}_a) - \xi_{ns}(\boldsymbol{r}_a)]\} \\
& -\frac{1}{2}E\{[\boldsymbol{\nu}^{\mathrm{T}}(H'_{nonsp} - \boldsymbol{q}_{R44}\boldsymbol{q}_{R44}^{\mathrm{T}})\boldsymbol{\nu} \\
& \qquad - trace(H'_{nonsp} - \boldsymbol{q}_{R44}\boldsymbol{q}_{R44}^{\mathrm{T}})] \\
& \qquad [\hat{\bar{\nu}}^2(\boldsymbol{r}_a) - \xi_{ns}(\boldsymbol{r}_a)]\} \\
& + \frac{1}{4}E\{\hat{\bar{\nu}}^4(\boldsymbol{r}_a)\} - \frac{1}{4}\xi_{ns}^2(\boldsymbol{r}_a)
\end{aligned} \tag{74b}$$

with

$$\begin{aligned}
& E\{[\boldsymbol{g}_{nonsp}^{\mathrm{T}}(\boldsymbol{r}_a)\boldsymbol{\nu}][\hat{\bar{\nu}}^2(\boldsymbol{r}_a) - \xi_{ns}(\boldsymbol{r}_a)]\} \\
& = \boldsymbol{g}_{nonsp}^{\mathrm{T}}(\boldsymbol{r}_a)\hat{\boldsymbol{q}}(\boldsymbol{r}_a)E\{\hat{\nu}(\boldsymbol{r}_a)[\hat{\bar{\nu}}^2(\boldsymbol{r}_a) - \xi_{ns}(\boldsymbol{r}_a)]\} \\
& = \boldsymbol{g}_{nonsp}^{\mathrm{T}}(\boldsymbol{r}_a)\hat{\boldsymbol{q}}(\boldsymbol{r}_a) \\
& \quad \bullet \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\hat{\nu}_{\max}(\boldsymbol{r}_a)} \hat{\nu}[\hat{\nu} - \hat{\nu}_{\max}(\boldsymbol{r}_a)]^2 e^{-\hat{\nu}^2/2} d\hat{\nu} \\
& = \boldsymbol{g}_{nonsp}^{\mathrm{T}}(\boldsymbol{r}_a)\hat{\boldsymbol{q}}(\boldsymbol{r}_a) \left(\frac{-2e^{-\hat{\nu}_{\max}^2(\boldsymbol{r}_a)/2}}{\sqrt{2\pi}} \right. \\
& \qquad \left. - 2\hat{\nu}_{\max}(\boldsymbol{r}_a) \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\hat{\nu}_{\max}(\boldsymbol{r}_a)} e^{-\hat{\nu}^2/2} d\hat{\nu} \right)
\end{aligned} \tag{75a}$$

$$\begin{aligned}
& E\{[\boldsymbol{\nu}^{\mathrm{T}}(H'_{nonsp} - \boldsymbol{q}_{R44}\boldsymbol{q}_{R44}^{\mathrm{T}})\boldsymbol{\nu} \\
& \qquad - trace(H'_{nonsp} - \boldsymbol{q}_{R44}\boldsymbol{q}_{R44}^{\mathrm{T}})] \\
& \quad \bullet [\hat{\bar{\nu}}^2(\boldsymbol{r}_a) - \xi_{ns}(\boldsymbol{r}_a)]\} \\
& = \hat{\boldsymbol{q}}^{\mathrm{T}}(\boldsymbol{r}_a)(H'_{nonsp} - \boldsymbol{q}_{R44}\boldsymbol{q}_{R44}^{\mathrm{T}})\hat{\boldsymbol{q}}(\boldsymbol{r}_a) \\
& \quad \bullet E\{\hat{\nu}^2(\boldsymbol{r}_a)[\hat{\bar{\nu}}^2(\boldsymbol{r}_a) - \xi_{ns}(\boldsymbol{r}_a)]\} \\
& = \hat{\boldsymbol{q}}^{\mathrm{T}}(\boldsymbol{r}_a)(H'_{nonsp} - \boldsymbol{q}_{R44}\boldsymbol{q}_{R44}^{\mathrm{T}})\hat{\boldsymbol{q}}(\boldsymbol{r}_a) \\
& \quad \bullet \{\frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\hat{\nu}_{\max}(\boldsymbol{r}_a)} \hat{\nu}^2[\hat{\nu} - \hat{\nu}_{\max}(\boldsymbol{r}_a)]^2 e^{-\hat{\nu}^2/2} d\hat{\nu} \\
& \quad - \xi_{ns}(\boldsymbol{r}_a)\} \\
& = \hat{\boldsymbol{q}}^{\mathrm{T}}(\boldsymbol{r}_a)(H'_{nonsp} - \boldsymbol{q}_{R44}\boldsymbol{q}_{R44}^{\mathrm{T}})\hat{\boldsymbol{q}}(\boldsymbol{r}_a) \\
& \quad \bullet \left(2\frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\hat{\nu}_{\max}(\boldsymbol{r}_a)} e^{-\hat{\nu}^2/2} d\hat{\nu} \right)
\end{aligned} \tag{75b}$$

$$\begin{aligned}
E\{\hat{\bar{\nu}}^4(\boldsymbol{r}_a)\} & = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\hat{\nu}_{\max}(\boldsymbol{r}_a)} [\hat{\nu} - \hat{\nu}_{\max}(\boldsymbol{r}_a)]^4 e^{-\hat{\nu}^2/2} d\hat{\nu} \\
& = \frac{[\hat{\nu}_{\max}^3(\boldsymbol{r}_a) + 5\hat{\nu}_{\max}(\boldsymbol{r}_a)]e^{-\hat{\nu}_{\max}^2(\boldsymbol{r}_a)/2}}{\sqrt{2\pi}} \\
& \quad + [\hat{\nu}_{\max}^4(\boldsymbol{r}_a) + 6\hat{\nu}_{\max}^2(\boldsymbol{r}_a) + 3] \\
& \quad \bullet \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\hat{\nu}_{\max}(\boldsymbol{r}_a)} e^{-\hat{\nu}^2/2} d\hat{\nu}
\end{aligned} \tag{75c}$$

Note that the same probability integral appears in the final versions of the right-hand sides of Eqs. (74a) and (75a)-(75c). It is the cumulative probability for a scalar zero-mean, unit-variance Gaussian distribution between negative infinity and $\hat{\nu}_{\max}(\boldsymbol{r}_a)$. Any good statistical functions software package should contain a standard function that computes this integral.

For the spoofed case, the approximate model of the dependence of γ on $\boldsymbol{\nu}$ is derived in a manner similar to the analysis that produced the corresponding known-amplitude model in Eq. (53). It involves consideration of the optimized non-spoofed and spoofed cost functions, as per Eqs. (66a)-(66c) and as per Eq. (22) when the actual data obeys the spoofed model. The approximate model for the detection statistic, valid to second order in $\boldsymbol{\nu}$, is

$$\begin{aligned}
\gamma \cong & -\frac{1}{2}\breve{\boldsymbol{g}}_{sp}^{\mathrm{T}}(\eta)\breve{\boldsymbol{g}}_{sp}(\eta) + \breve{\boldsymbol{g}}_{sp}^{\mathrm{T}}(\eta)\boldsymbol{\nu} \\
& + \frac{1}{2}\boldsymbol{\nu}^{\mathrm{T}}[H'_{sp}(\eta) - \boldsymbol{q}_{R44}\boldsymbol{q}_{R44}^{\mathrm{T}}]\boldsymbol{\nu} - \frac{1}{2}\breve{\bar{\nu}}^2(\eta)\zeta(\eta)
\end{aligned} \tag{76}$$

where the L-by-1 residuals vector $\breve{\boldsymbol{g}}_{sp}(\eta)$ and the L-by-L symmetric matrix $H'_{sp}(\eta)$ are

$$\breve{\boldsymbol{g}}_{sp}(\eta) = B\breve{\boldsymbol{r}}_a(\eta) - \begin{bmatrix} R_{44}^1\eta \\ R_{44}^2\eta \\ R_{44}^3\eta \\ \vdots \\ R_{44}^L\eta \end{bmatrix} \tag{77a}$$

$$H'_{sp}(\eta) = B[B^{\mathrm{T}}B + \breve{\mu}(\eta)I]^{-1}B^{\mathrm{T}} \tag{77b}$$

The 3-by-1 vector $\breve{\boldsymbol{r}}_a(\eta)$ in these formulas is the solution to an auxiliary articulation-direction/articulation-scaling-factor estimation problem that takes the form of Eqs. (66a)-(66c), except with z_4^j replaced by $R_{44}^j\eta$ for all GNSS satellites j = 1, ..., L. The scalar Kuhn-Tucker multiplier $\breve{\mu}(\eta)$ is the associated value that is determined when solving for $\breve{\boldsymbol{r}}_a(\eta)$. It is determined using Eq. (47) if the inequality constraint in Eq. (66c) is active, and it is non-positive in this case, but $\breve{\mu}(\eta)$ = 0 if the inequality constraint is inactive, i.e., if $\breve{\boldsymbol{r}}_a^{\mathrm{T}}(\eta)\breve{\boldsymbol{r}}_a(\eta) > 1$.

The scalar random variable $\bar{\breve{\nu}}(\eta)$ accounts for the effects of the inequality constraint and its variations of activity or inactivity, depending on the specific values of $\boldsymbol{\nu}$ and η. It is defined as follows:

$$\bar{\breve{\nu}}(\eta) = \begin{cases} \breve{\nu}(\eta) & \text{if } \breve{\mu}(\eta) < 0 \text{ and } \breve{\nu}(\eta) < \breve{\nu}_{\mathrm{maxc}}(\eta) \\ \breve{\nu}_{\mathrm{maxc}}(\eta) & \text{if } \breve{\mu}(\eta) < 0 \text{ and } \breve{\nu}_{\mathrm{maxc}}(\eta) \le \breve{\nu}(\eta) \\ \breve{\nu}(\eta) - \breve{\nu}_{\mathrm{maxu}}(\eta) & \text{if } \breve{\mu}(\eta) = 0 \text{ and } \breve{\nu}(\eta) < \breve{\nu}_{\mathrm{maxu}}(\eta) \\ 0 & \text{if } \breve{\mu}(\eta) = 0 \text{ and } \breve{\nu}_{\mathrm{maxu}}(\eta) \le \breve{\nu}(\eta) \end{cases} \tag{78}$$

where

$$\breve{\nu}(\eta) = \breve{\boldsymbol{q}}^{\mathrm{T}}(\eta)\boldsymbol{\nu} \tag{79a}$$

$$\breve{\nu}_{\mathrm{maxc}}(\eta) = -\left(\frac{\breve{\boldsymbol{r}}_a^{\mathrm{T}}(\eta)[B^{\mathrm{T}}B + \breve{\mu}(\eta)I]^{-1}\breve{\boldsymbol{r}}_a(\eta)}{\sqrt{\breve{\boldsymbol{r}}_a^{\mathrm{T}}(\eta)[B^{\mathrm{T}}B + \breve{\mu}(\eta)I]^{-1}B^{\mathrm{T}}B[B^{\mathrm{T}}B + \breve{\mu}(\eta)I]^{-1}\breve{\boldsymbol{r}}_a(\eta)}} \right)\breve{\mu}(\eta) \tag{79b}$$

$$\breve{\nu}_{\mathrm{maxu}}(\eta) = \frac{1 - \breve{\boldsymbol{r}}_a^{\mathrm{T}}(\eta)\breve{\boldsymbol{r}}_a(\eta)}{2\sqrt{\breve{\boldsymbol{r}}_a^{\mathrm{T}}(\eta)(B^{\mathrm{T}}B)^{-1}\breve{\boldsymbol{r}}_a(\eta)}} \tag{79c}$$

with the unit-normalized L-by-1 vector $\breve{\boldsymbol{q}}(\eta)$ being defined as:

$$\breve{\boldsymbol{q}}(\eta) = \frac{B[B^{\mathrm{T}}B + \breve{\mu}(\eta)I]^{-1}\breve{\boldsymbol{r}}_a(\eta)}{\sqrt{\breve{\boldsymbol{r}}_a^{\mathrm{T}}(\eta)[B^{\mathrm{T}}B + \breve{\mu}(\eta)I]^{-1}B^{\mathrm{T}}B[B^{\mathrm{T}}B + \breve{\mu}(\eta)I]^{-1}\breve{\boldsymbol{r}}_a(\eta)}} \tag{80}$$

The two upper-most conditions in Eq. (78) deal with the active constraint case, in which $\breve{\boldsymbol{r}}_a^{\mathrm{T}}(\eta)\breve{\boldsymbol{r}}_a(\eta) = 1$. The two lower-most conditions cover the inactive constraint case, i.e., the case when $\breve{\boldsymbol{r}}_a^{\mathrm{T}}(\eta)\breve{\boldsymbol{r}}_a(\eta) > 1$.

The coefficient of function that multiplies $\bar{\breve{\nu}}^2(\eta)$ in Eq. (76) is

$$\zeta(\eta) = \frac{\breve{\boldsymbol{r}}_a^{\mathrm{T}}(\eta)[B^{\mathrm{T}}B + \breve{\mu}(\eta)I]^{-1}B^{\mathrm{T}}B[B^{\mathrm{T}}B + \breve{\mu}(\eta)I]^{-1}\breve{\boldsymbol{r}}_a(\eta)}{\breve{\boldsymbol{r}}_a^{\mathrm{T}}(\eta)[B^{\mathrm{T}}B + \breve{\mu}(\eta)I]^{-1}\breve{\boldsymbol{r}}_a(\eta)} \tag{81}$$

When $\breve{\mu}(\eta)$ = 0, i.e., in the inactive constraint case, this coefficient equals 1.

As for all preceding models of all preceding detection statistics, the model in Eq. (76) is dominated by the term $\breve{\boldsymbol{g}}_{sp}^{\mathrm{T}}(\eta)\boldsymbol{\nu}$. Its variance is typically much larger than that of $\frac{1}{2}\boldsymbol{\nu}^{\mathrm{T}}[H_{sp}^{'}(\eta) - \boldsymbol{q}_{R44}\boldsymbol{q}_{R44}^{\mathrm{T}}]\boldsymbol{\nu}$, of $-\frac{1}{2}\bar{\breve{\nu}}^2(\eta)\zeta(\eta)$, or of the neglected higher-order terms in $\boldsymbol{\nu}$. Given that this dominant term is Gaussian, the following Gaussian distribution is a reasonable approximation of the detection statistic probability density function in the spoofed case:

$$p(\gamma \mid \eta, H_1) \cong N[\gamma; \bar{\gamma}_{sp}^{'}(\eta), \sigma_{\gamma sp}^{'}(\eta)] \tag{82}$$

with the mean and standard deviation:

$$\bar{\gamma}_{sp}^{'}(\eta) = -\frac{1}{2}\breve{\boldsymbol{g}}_{sp}^{\mathrm{T}}(\eta)\breve{\boldsymbol{g}}_{sp}(\eta) + \frac{1}{2}\mathit{trace}[H_{sp}^{'}(\eta) - \boldsymbol{q}_{R44}\boldsymbol{q}_{R44}^{\mathrm{T}}] - \frac{1}{2}\xi_{sp}(\eta) \tag{83a}$$

$$\sigma_{\gamma sp}^{'}(\eta) = \Big[\breve{\boldsymbol{g}}_{sp}^{\mathrm{T}}(\eta)\breve{\boldsymbol{g}}_{sp}(\eta) + \frac{1}{2}\mathit{trace}\{[H_{sp}^{'}(\eta) - \boldsymbol{q}_{R44}\boldsymbol{q}_{R44}^{\mathrm{T}}] \bullet [H_{sp}^{'}(\eta) - \boldsymbol{q}_{R44}\boldsymbol{q}_{R44}^{\mathrm{T}}]\} + \psi_{sp}(\eta)\Big]^{1/2} \tag{83b}$$

where

$$\xi_{sp}(\eta) = \zeta(\eta)E\{\bar{\breve{\nu}}^2(\eta)\} \tag{84a}$$

$$\begin{aligned} \psi_{sp}(\eta) = {} & -E\{[\breve{\boldsymbol{g}}_{sp}^{\mathrm{T}}(\eta)\boldsymbol{\nu}][\bar{\breve{\nu}}^2(\eta)\zeta(\eta) - \xi_{sp}(\eta)]\} \\ & -\frac{1}{2}E\{[\boldsymbol{\nu}^{\mathrm{T}}(H_{sp}^{'}\{\eta\} - \boldsymbol{q}_{R44}\boldsymbol{q}_{R44}^{\mathrm{T}})\boldsymbol{\nu} \\ & \qquad - \mathit{trace}(H_{sp}^{'}\{\eta\} - \boldsymbol{q}_{R44}\boldsymbol{q}_{R44}^{\mathrm{T}})] \\ & \qquad \bullet [\bar{\breve{\nu}}^2(\eta)\zeta(\eta) - \xi_{sp}(\eta)]\} \\ & +\frac{1}{4}\zeta^2(\eta)E\{\bar{\breve{\nu}}^4(\eta)\} - \frac{1}{4}\xi_{sp}^2(\eta) \end{aligned} \tag{84b}$$

The calculations that determine the scalar quantities $\xi_{sp}(\eta)$ and $\psi_{sp}(\eta)$ differ depending on whether the constrained non-spoofed optimization applies, $\breve{\boldsymbol{r}}_a^{\mathrm{T}}(\eta)\breve{\boldsymbol{r}}_a(\eta) = 1$ and $\breve{\mu}(\eta)$ < 0, or the unconstrained optimization applies, $\breve{\boldsymbol{r}}_a^{\mathrm{T}}(\eta)\breve{\boldsymbol{r}}_a(\eta) \ge 1$ and $\breve{\mu}(\eta)$ = 0. In the constrained case, these quantities are computed using the following formulas for various of their components:

$$\begin{aligned} E\{\bar{\breve{\nu}}^2(\eta)\} & = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\breve{\nu}_{\mathrm{maxc}}(\eta)} \breve{\nu}^2 e^{-\breve{\nu}^2/2} d\breve{\nu} + \frac{\breve{\nu}_{\mathrm{maxc}}^2(\eta)}{\sqrt{2\pi}}\int_{\breve{\nu}_{\mathrm{maxc}}(\eta)}^{\infty} e^{-\breve{\nu}^2/2} d\breve{\nu} \\ & = \breve{\nu}_{\mathrm{maxc}}^2(\eta) - \frac{\breve{\nu}_{\mathrm{maxc}}(\eta)e^{-\breve{\nu}_{\mathrm{maxc}}^2(\eta)/2}}{\sqrt{2\pi}} + \frac{[1 - \breve{\nu}_{\mathrm{maxc}}^2(\eta)]}{\sqrt{2\pi}}\int_{-\infty}^{\breve{\nu}_{\mathrm{maxc}}(\eta)} e^{-\breve{\nu}^2/2} d\breve{\nu} \end{aligned} \tag{85a}$$

$$\begin{aligned} & E\{[\breve{\boldsymbol{g}}_{sp}^{\mathrm{T}}(\eta)\boldsymbol{\nu}][\bar{\breve{\nu}}^2(\eta)\zeta(\eta) - \xi_{sp}(\eta)]\} \\ & \quad = \breve{\boldsymbol{g}}_{sp}^{\mathrm{T}}(\eta)\breve{\boldsymbol{q}}(\eta)E\{\breve{\nu}(\eta)[\bar{\breve{\nu}}^2(\eta)\zeta(\eta) - \xi_{sp}(\eta)]\} \\ & \quad = \breve{\boldsymbol{g}}_{sp}^{\mathrm{T}}(\eta)\breve{\boldsymbol{q}}(\eta)\left(\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\breve{\nu}_{\mathrm{maxc}}(\eta)} \breve{\nu}^3 e^{-\breve{\nu}^2/2} d\breve{\nu}\right. \end{aligned}$$

$$+\frac{\breve{\nu}^2_{\rm maxc}(\eta)}{\sqrt{2\pi}}\int_{\breve{\nu}_{\rm maxc}(\eta)}^{\infty}\breve{\nu}e^{-\breve{\nu}^2/2}d\breve{\nu}\Bigg)\zeta(\eta)$$

$$=\breve{\boldsymbol{g}}_{sp}^{\rm T}(\eta)\breve{\boldsymbol{q}}(\eta)\left(-\frac{2e^{-\breve{\nu}^2_{\rm maxc}(\eta)/2}}{\sqrt{2\pi}}\right)\zeta(\eta) \qquad (85b)$$

$$E\{[\boldsymbol{\nu}^{\rm T}(H'_{sp}\{\eta\}-\boldsymbol{q}_{R44}\boldsymbol{q}_{R44}^{\rm T})\boldsymbol{\nu}$$

$$-trace(H'_{sp}\{\eta\}-\boldsymbol{q}_{R44}\boldsymbol{q}_{R44}^{\rm T})]$$

$$\bullet[\bar{\breve{\nu}}^2(\eta)\zeta(\eta)-\xi_{sp}(\eta)]\}$$

$$=\breve{\boldsymbol{q}}^{\rm T}(\eta)(H'_{sp}\{\eta\}-\boldsymbol{q}_{R44}\boldsymbol{q}_{R44}^{\rm T})\breve{\boldsymbol{q}}(\eta)$$

$$E\{\breve{\nu}^2(\eta)[\bar{\breve{\nu}}^2(\eta)\zeta(\eta)-\xi_{sp}(\eta)]\}$$

$$=\breve{\boldsymbol{q}}^{\rm T}(\eta)(H'_{sp}\{\eta\}-\boldsymbol{q}_{R44}\boldsymbol{q}_{R44}^{\rm T})\breve{\boldsymbol{q}}(\eta)\times$$

$$\{\Bigg(\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\breve{\nu}_{\rm maxc}(\eta)}\breve{\nu}^4e^{-\breve{\nu}^2/2}d\breve{\nu}$$

$$+\frac{\breve{\nu}^2_{\rm maxc}(\eta)}{\sqrt{2\pi}}\int_{\breve{\nu}_{\rm maxc}(\eta)}^{\infty}\breve{\nu}^2e^{-\breve{\nu}^2/2}d\breve{\nu}\Bigg)\zeta(\eta)$$

$$-\xi_{sp}(\eta)\}$$

$$=\breve{\boldsymbol{q}}^{\rm T}(\eta)(H'_{sp}\{\eta\}-\boldsymbol{q}_{R44}\boldsymbol{q}_{R44}^{\rm T})\breve{\boldsymbol{q}}(\eta)$$

$$\bullet\Bigg(-\frac{2\breve{\nu}_{\rm maxc}(\eta)e^{-\breve{\nu}^2_{\rm maxc}(\eta)/2}}{\sqrt{2\pi}}$$

$$+\frac{2}{\sqrt{2\pi}}\int_{-\infty}^{\breve{\nu}_{\rm maxc}(\eta)}e^{-\breve{\nu}^2/2}d\breve{\nu}\Bigg)\zeta(\eta) \qquad (85c)$$

$$E\{\bar{\breve{\nu}}^4(\eta)\}=\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\breve{\nu}_{\rm maxc}(\eta)}\breve{\nu}^4e^{-\breve{\nu}^2/2}d\breve{\nu}$$

$$+\frac{\breve{\nu}^4_{\rm maxc}(\eta)}{\sqrt{2\pi}}\int_{\breve{\nu}_{\rm maxc}(\eta)}^{\infty}e^{-\breve{\nu}^2/2}d\breve{\nu}$$

$$=\breve{\nu}^4_{\rm maxc}(\eta)-\frac{[\breve{\nu}^3_{\rm maxc}(\eta)+3\breve{\nu}_{\rm maxc}(\eta)]e^{-\breve{\nu}^2_{\rm maxc}(\eta)/2}}{\sqrt{2\pi}}$$

$$+\frac{[3-\breve{\nu}^4_{\rm maxc}(\eta)]}{\sqrt{2\pi}}\int_{-\infty}^{\breve{\nu}_{\rm maxc}(\eta)}e^{-\breve{\nu}^2/2}d\breve{\nu} \qquad (85d)$$

In the unconstrained case, on the other hand, the following alternate formulas apply for the needed components of $\xi_{sp}(\eta)$ and $\psi_{sp}(\eta)$:

$$E\{\bar{\breve{\nu}}^2(\eta)\}=\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\breve{\nu}_{\rm maxu}(\eta)}[\breve{\nu}-\breve{\nu}_{\rm maxu}(\eta)]^2e^{-\breve{\nu}^2/2}d\breve{\nu}$$

$$=\frac{\breve{\nu}_{\rm maxu}(\eta)e^{-\breve{\nu}^2_{\rm maxu}(\eta)/2}}{\sqrt{2\pi}}$$

$$+[1+\breve{\nu}^2_{\rm maxu}(\eta)]\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\breve{\nu}_{\rm maxu}(\eta)}e^{-\breve{\nu}^2/2}d\breve{\nu}$$

$$(86a)$$

$$E\{[\breve{\boldsymbol{g}}_{sp}^{\rm T}(\eta)\boldsymbol{\nu}][\bar{\breve{\nu}}^2(\eta)\zeta(\eta)-\xi_{sp}(\eta)]\}$$

$$=\breve{\boldsymbol{g}}_{sp}^{\rm T}(\eta)\breve{\boldsymbol{q}}(\eta)E\{\breve{\nu}(\eta)[\bar{\breve{\nu}}^2(\eta)\zeta(\eta)-\xi_{sp}(\eta)]\}$$

$$=\breve{\boldsymbol{g}}_{sp}^{\rm T}(\eta)\breve{\boldsymbol{q}}(\eta)\zeta(\eta)$$

$$\bullet\left(\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\breve{\nu}_{\rm maxu}(\eta)}\breve{\nu}[\breve{\nu}-\breve{\nu}_{\rm maxu}(\eta)]^2e^{-\hat{\nu}^2/2}d\breve{\nu}\right)$$

$$=\breve{\boldsymbol{g}}_{sp}^{\rm T}(\eta)\breve{\boldsymbol{q}}(\eta)\zeta(\eta)\Bigg(\frac{-2e^{-\breve{\nu}^2_{\rm maxu}(\eta)/2}}{\sqrt{2\pi}}$$

$$-2\breve{\nu}_{\rm maxu}(\eta)\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\breve{\nu}_{\rm maxu}(\eta)}e^{-\breve{\nu}^2/2}d\breve{\nu}\Bigg)$$

$$(86b)$$

$$E\{[\boldsymbol{\nu}^{\rm T}(H'_{sp}\{\eta\}-\boldsymbol{q}_{R44}\boldsymbol{q}_{R44}^{\rm T})\boldsymbol{\nu}$$

$$-trace(H'_{sp}\{\eta\}-\boldsymbol{q}_{R44}\boldsymbol{q}_{R44}^{\rm T})]$$

$$\bullet[\bar{\breve{\nu}}^2(\eta)\zeta(\eta)-\xi_{sp}(\eta)]\}$$

$$=\breve{\boldsymbol{q}}^{\rm T}(\eta)(H'_{sp}\{\eta\}-\boldsymbol{q}_{R44}\boldsymbol{q}_{R44}^{\rm T})\breve{\boldsymbol{q}}(\eta)$$

$$\bullet E\{\breve{\nu}^2(\eta)[\bar{\breve{\nu}}^2(\eta)\zeta(\eta)-\xi_{sp}(\eta)]\}$$

$$=\breve{\boldsymbol{q}}^{\rm T}(\eta)(H'_{sp}\{\eta\}-\boldsymbol{q}_{R44}\boldsymbol{q}_{R44}^{\rm T})\breve{\boldsymbol{q}}(\eta)\times$$

$$\{\left(\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\breve{\nu}_{\rm maxu}(\eta)}\breve{\nu}^2[\breve{\nu}-\breve{\nu}_{\rm maxu}(\eta)]^2e^{-\breve{\nu}^2/2}d\breve{\nu}\right)\zeta(\eta)$$

$$-\xi_{sp}(\eta)\}$$

$$=\breve{\boldsymbol{q}}^{\rm T}(\eta)(H'_{sp}\{\eta\}-\boldsymbol{q}_{R44}\boldsymbol{q}_{R44}^{\rm T})\breve{\boldsymbol{q}}(\eta)$$

$$\bullet\left(2\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\breve{\nu}_{\rm maxu}(\eta)}e^{-\breve{\nu}^2/2}d\breve{\nu}\right)\zeta(\eta) \qquad (86c)$$

$$E\{\bar{\breve{\nu}}^4(\eta)\}=\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\breve{\nu}_{\rm maxu}(\eta)}[\breve{\nu}-\breve{\nu}_{\rm maxu}(\eta)]^4e^{-\breve{\nu}^2/2}d\breve{\nu}$$

$$=\frac{[\breve{\nu}^3_{\rm maxu}(\eta)+5\breve{\nu}_{\rm maxu}(\eta)]e^{-\breve{\nu}^2_{\rm maxu}(\eta)/2}}{\sqrt{2\pi}}$$

$$+[\breve{\nu}^4_{\rm maxu}(\eta)+6\breve{\nu}^2_{\rm maxu}(\eta)+3]$$

$$\bullet\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\breve{\nu}_{\rm maxu}(\eta)}e^{-\hat{\nu}^2/2}d\hat{\nu} \qquad (86d)$$

C. Design of Worst-Case Spoofing Detection Threshold and Analysis of Worst-Case Detection Probability, Unknown Attitude and Unknown Amplitude Scaling

Given the Gaussian $p(\gamma\,|\,\boldsymbol{r}_a,H_0)$ probability density function defined by Eqs. (72)-(75c), it is possible to compute a spoofing detection threshold value γ_{th} that achieves a worst-case probability of missed detection α_{wc}. The approach taken here is similar to what is done in Subsection V.C for the known-amplitude case.

The first step of the threshold calculation computes κ_{wc} from α_{wc} using Eq. (58). The second step solves an optimization problem to find the worst-case product of the antenna articulation direction vector and scaling amplitude $\boldsymbol{r}_a$ that produces the lowest threshold for the target false-alarm probability. This problem is

$$\text{find:} \quad \boldsymbol{r}_a \tag{87a}$$

$$\text{to minimize:} \quad J'_{\gamma th}(\boldsymbol{r}_a) = \bar{\gamma}'_{nonsp}(\boldsymbol{r}_a) + \kappa_{wc}\sigma'_{\gamma nonsp}(\boldsymbol{r}_a) \tag{87b}$$

$$\text{subject to:} \quad \boldsymbol{r}_a^{\mathrm{T}}\boldsymbol{r}_a \geq 1 \tag{87c}$$

The antenna articulation-direction/scaling product that minimizes the cost function in Eq. (87b) is $\boldsymbol{r}_{awc}$. It yields the highest probability of false alarm for the given spoofing detection test. The corresponding worst-case spoofing detection threshold is equal to the value of the minimum cost: $\gamma_{th} = J'_{\gamma th}(\boldsymbol{r}_{awc})$. As in Subsection V.C, it is easy to show that $\alpha(\boldsymbol{r}_a) \leq \alpha_{wc}$, i.e., that the spoofing detection false-alarm probability for any actual true value of $\boldsymbol{r}_a$ is no greater than α_{wc}.

The optimization problem in Eqs. (87a)-(87c) can be solved using a numerical method. Newton's method [31] will serve if it has been enhanced to ensure global convergence and enforce the inequality constraint in Eq. (87c). Such an approach has been used for the tests of Section IX. It is similar to the one used to solve the problem in Eqs. (59a)-(59c) for the known-amplitude case. In addition, it uses the same procedure to generate its first guess of $\boldsymbol{r}_{awc}$ as is used to generate the first guess of the $\hat{\boldsymbol{r}}_{awc}$ solution to the problem in Eqs. (59a)-(59c). Thus, the first guess obeys $\boldsymbol{r}_{awc}^{\mathrm{T}}\boldsymbol{r}_{awc} = 1$. This makes sense because this is the lowest possible amplitude, and the lowest possible amplitude is likely to give the highest probability of generating a false alarm.

Also similar to the known-amplitude case, a worst-case probability of missed detection is calculated by computing the corresponding worst true value of η = $a(\hat{\boldsymbol{r}}^{sp})^{\mathrm{T}}\hat{\boldsymbol{r}}_a$ = $(\hat{\boldsymbol{r}}^{sp})^{\mathrm{T}}\boldsymbol{r}_a$. The worst-case value is the solution to the following optimization problem:

$$\text{find:} \quad \eta \tag{88a}$$

$$\text{to minimize:} \quad J'_{PMD}(\eta) = \frac{\gamma_{th} - \bar{\gamma}'_{sp}(\eta)}{\sigma'_{\gamma sp}(\eta)} \tag{88b}$$

This 1-dimensional nonlinear optimization problem is solved using a numerical technique similar to the one that is used to solve the corresponding problem for the known-amplitude worst-case probability of missed detection, the problem in Eqs. (61a)-(61c). The algorithm for solving the present problem is somewhat simpler due to the lack of any inequality constraints here. The similarity of the problems and cost functions in Eqs. (61a)-(61c) allows the same procedure to be used in order to generate the initial guess of η_{wc}, as per Eqs. (62) and (63). This guess produces a corresponding value of $\breve{\boldsymbol{r}}_a(\eta_{wc})$ that obeys $\breve{\boldsymbol{r}}_a^{\mathrm{T}}(\eta_{wc})\breve{\boldsymbol{r}}_a(\eta_{wc}) = 1$. This makes sense because the worst-case probability of missed detection would tend to correspond to the lowest possible amplitude of antenna articulation.

The optimal η_{wc} that solves the problem in Eqs. (88a) and (88b) can be used to compute the worst-case probability of missed detection

$$\begin{aligned} P_{MDwc} &= \frac{1}{\sqrt{2\pi}\sigma'_{\gamma sp}(\eta_{wc})} \int_{\gamma_{th}}^{\infty} e^{-[\gamma - \bar{\gamma}'_{sp}(\eta_{wc})]^2/[2\{\sigma'_{\gamma sp}(\eta_{wc})\}^2]} d\gamma \\ &= \frac{1}{\sqrt{2\pi}} \int_{J'_{PMD}(\eta_{wc})}^{\infty} e^{-\gamma_{nd}^2/2} d\gamma_{nd} \end{aligned} \tag{89}$$

By an analysis similar to that which produced Eq. (65) in the known-amplitude case, it is straightforward to show that the probability of missed detection for any other true value of η will be no greater than this worst-case probability.

VII. SPOOFING DETECTION HYPOTHESIS TEST FOR MOVING-BASE UE WITH UNKNOWN ARTICULATION TIME PHASING

A fourth version of the spoofing detection test with uni-axial antenna articulation allows for uncertainty in the time phasing of the $\rho_a(t)$ antenna articulation time history. Such uncertainty can be present when a system like that shown in Fig. 3 is excited by an initial impulse of uncertain time of application. This type of uncertainty also can occur for an antenna mounted on a UAV if rapid controller-induced attitude maneuvers are used to induce the high-frequency antenna motion. Any uncertainty of the transfer-function lag between the control inputs and the attitude response will translate into a time phasing uncertainty. In such cases, it is necessary to estimate a time offset of the articulations, Δt_0, in addition to other quantities. This time offset is defined so that the nominal articulation time history $\rho_a(t)$ becomes $\rho_a(t - \Delta t_0)$ after correcting for the time phasing error.

A. Estimation of Time Phasing via Outer Optimization

There are various possible approaches to dealing with Δt_0 uncertainty. The approach adopted here is to estimate Δt_0 in an outer nonlinear optimization calculation that does not explicitly estimate other quantities needed to form a spoofing detection statistic. The outer numerical optimization problem is posed by exploiting the following fact of 1-dimensional antenna articulations: All of the articulation-induced carrier phase time histories for all channels are multiples of $\rho_a(t - \Delta t_0)$ regardless of whether or not a spoofing attack is in progress. Given this knowledge, one can solve the over-determined least-squares estimation problem in Eq. (16) for each GNSS satellite $j = 1, ..., L$ and then form a Δt_0 optimization cost function that is a weighted sum of the residuals from each of the least-squares problems. Each of these L solutions treats the value of the scalar $(\hat{\boldsymbol{r}}^x)^{\mathrm{T}}\hat{\boldsymbol{r}}_a$ in Eq. (16) as a different independent unknown so that the value determined for the j^{th} signal need not be related in any particular way to the values determined for the other L-1 signals.

The minimum costs of these L linear least-squares optimizations are combined with a cost that introduces *a priori* Δt_0 knowledge to yield a Δt_0 estimation cost function of the form:

$$J_{phs}(\Delta t_0) = \frac{1}{2}\left(\frac{\Delta t_0}{\sigma_{\Delta t0ap}}\right)^2 + \frac{1}{2}\sum_{j=1}^{L}(\boldsymbol{f}^j)^{\mathrm{T}}\{I - \hat{\boldsymbol{d}}^j(\Delta t_0)[\hat{\boldsymbol{d}}^j(\Delta t_0)]^{\mathrm{T}}\}\boldsymbol{f}^j \qquad (90)$$

where

$$\boldsymbol{f}^j = \frac{1}{\sigma^j}P^j\begin{bmatrix}\phi_1^j\\ \phi_2^j\\ \phi_3^j\\ \vdots\\ \phi_{N_j}^j\end{bmatrix} \qquad (91a)$$

$$\hat{\boldsymbol{d}}^j(\Delta t_0) = \frac{\boldsymbol{d}^j(\Delta t_0)}{\sqrt{[\boldsymbol{d}^j(\Delta t_0)]^{\mathrm{T}}\boldsymbol{d}^j(\Delta t_0)}} \qquad (91b)$$

with

$$P^j = I - D^j[(D^j)^{\mathrm{T}}D^j]^{-1}(D^j)^{\mathrm{T}} \qquad (92a)$$

$$\boldsymbol{d}^j(\Delta t_0) = P^j\begin{bmatrix}\rho_a(\tau_{mid1}^j - \Delta t_0)\\ \rho_a(\tau_{mid2}^j - \Delta t_0)\\ \rho_a(\tau_{mid3}^j - \Delta t_0)\\ \vdots\\ \rho_a(\tau_{midN_j}^j - \Delta t_0)\end{bmatrix} \qquad (92b)$$

$$D^j = \begin{bmatrix}1 & 0 & 0\\ 1 & (\tau_{mid2}^j - \tau_{mid1}^j) & \frac{1}{2}(\tau_{mid2}^j - \tau_{mid1}^j)^2\\ 1 & (\tau_{mid3}^j - \tau_{mid1}^j) & \frac{1}{2}(\tau_{mid3}^j - \tau_{mid1}^j)^2\\ \vdots & \vdots & \vdots\\ 1 & (\tau_{midN_j}^j - \tau_{mid1}^j) & \frac{1}{2}(\tau_{midN_j}^j - \tau_{mid1}^j)^2\end{bmatrix} \qquad (92c)$$

The cost function $J_{phs}(\Delta t_0)$ in Eq. (90) is a negative log-likelihood cost function, and its $\sigma_{\Delta t0ap}$ parameter is the standard deviation of the *a priori* uncertainty about how much Δt_0 might differ from 0. The N_j-by-1 vector $\boldsymbol{f}^j$ contains the high-pass-filtered carrier phase time history for the j^{th} GNSS signal normalized by its measurement error standard deviation. The N_j-by-1 vector $\hat{\boldsymbol{d}}^j(\Delta t_0)$ is a unit-normalized version of the high-pass-filtered time history $\rho_a(t - \Delta t_0)$ sampled at the midpoints of the accumulation intervals of the j^{th} signal. The N_j-by-N_j matrix P^j is a projection matrix that performs the high-pass filtering for the j^{th} signal, as is evident by its definition in terms of the N_j-by-3 matrix D^j. P^j projects signal time histories orthogonal to the constant, linear, and quadratic time histories in the columns of D^j.

The cost function in Eq. (90) can be optimized to determine Δt_{0opt} by using standard numerical techniques, such as Newton's method [31]. Given that this involves unconstrained optimization of a scalar, the implementation is straightforward.

A useful auxiliary quantity is the Cramer-Rao lower bound [35] on the uncertainty in Δt_{0opt}. It takes the form:

$$\sigma_{\Delta t0opt}^2 \cong \frac{1}{\left(\left.\frac{\partial^2 J_{phs}}{\partial \Delta t_0^2}\right|_{\Delta t_{0opt}}\right)} \qquad (93)$$

B. Spoofing Detection Statistic with Timing Uncertainty

Given the estimate Δt_{0opt} that minimizes the cost function in Eq. (90), any of the three spoofing detection tests of Sections IV-VI can be implemented by replacing $\rho_a(t)$ in Eqs. (16) and (17) by $\rho_a(t - \Delta t_0)$. All of the subsequent spoofing detection calculations can then be carried out by using the resulting values of R_{44}^j and z_4^j for $j = 1, ..., L$. The ensuing calculations will yield a spoofing detection statistic γ that can be used to develop a powerful detection test.

C. Design of Spoofing Detection Threshold and Analysis of False-Alarm Probability

One might try to use the corresponding pair of $p(\gamma|H_0)$ and $p(\gamma|H_1)$ probability density functions from Sections IV-VI directly in the design of the spoofing detection threshold and the analysis of the probability of missed detection for an uncertain Δt_0 case. One could substitute $\rho_a(t - \Delta t_0)$ for $\rho_a(t)$ in any given analysis. This approach, however, is not exactly right when working with an uncertain Δt_0 and its estimate Δt_{0opt}. Complications occur because an additional source of γ variability arises from the impact of measurement noise on the Δt_{0opt} estimate.

One could do an exact or approximate analysis of the impact of this Δt_{0opt} variability on $p(\gamma|H_0)$ and $p(\gamma|H_1)$. Perhaps a reasonable analysis would use a linear approximation of the effect of the noise vector $\boldsymbol{\nu}$ on the errors in Δt_{0opt}. Such an analysis might be rather complicated.

This case of uncertain Δt_0 is not considered to be a very important one because it is not a preferred mode of operation. This case is considered here mostly because it is helpful to the processing of experimental data from the initial prototype spoofing detection system, where timing uncertainty was present because the prototype articulation system lacked a $\rho_a(t)$ sensor.

In an operational system, the need to estimate Δt_{0opt} opens up the possibility of a new type of spoofing attack, one that also simulates the expected non-spoofed carrier-phase effects of $\rho_a(t)$. The spoofer might have an idea about the types of $\rho_a(t)$ time histories, but knowledge of the exact timing could be made virtually inaccessible to a spoofer. Armed with the right $\rho_a(t)$ but the wrong Δt_0, however, a spoofer might avoid detection by fooling the detection system into choosing a value of Δt_{0opt} that aligned with the spoofed version of $\rho_a(t)$. Therefore, a system that needs to estimate Δt_0 is undesirable and should be avoided.

Because this case is considered mostly in support of initial prototype experiments, it has not been deemed worthwhile to do a full analysis of the impacts of Δt_{0opt} uncertainty. Instead, the threshold calculations of the relevant previous section have been carried out three different times using the following three different candidate antenna articulation time histories: $\rho_a(t - \Delta t_{0opt})$, $\rho_a(t - \Delta t_{0opt} - 2\sigma_{\Delta t0opt})$, and $\rho_a(t - \Delta t_{0opt} + 2\sigma_{\Delta t0opt})$. Let the corresponding three spoofing detection thresholds be called γ_{tha}, γ_{thb}, and γ_{thc}. The final detection threshold was then chosen to be $\gamma_{th} = \min(\gamma_{tha},\gamma_{thb},\gamma_{thc})$, which is consistent with the philosophy of taking a worst-case approach.

The worst-case probability of missed detection was calculated in a similar ad hoc manner. Suppose that the corresponding spoofed means and standard deviations for the above three time offsets have been calculated using the relevant equations from Section IV, V, or VI and suppose that the resulting values are, respectively, $\bar{\gamma}_{spa}$, $\bar{\gamma}_{spb}$, $\bar{\gamma}_{spc}$, $\sigma_{\gamma spa}$, $\sigma_{\gamma spb}$, and $\sigma_{\gamma spc}$. Then the worst-case probability of false alarm is approximated as:

$$P_{MDwc} = \frac{1}{\sqrt{2\pi}} \int_{J_{PMDwc}}^{\infty} e^{-\gamma_{nd}^2/2} d\gamma_{nd} \tag{94}$$

where

$$J_{PMDwc} = \min\left[\left(\frac{\gamma_{th} - \bar{\gamma}_{spa}}{\sigma_{\gamma spa}}\right), \left(\frac{\gamma_{th} - \bar{\gamma}_{spb}}{\sigma_{\gamma spb}}\right), \left(\frac{\gamma_{th} - \bar{\gamma}_{spc}}{\sigma_{\gamma spc}}\right)\right] \tag{95}$$

VIII. SPOOFING DETECTION WITH 2- AND 3-DIMENSIONAL ANTENNA ARTICULATIONS

The present section develops a spoofing hypothesis test in the case of general 2-D or 3-D articulation motion of the antenna. This differs from the tests in Sections IV-VI, which deal with the case of uni-axial motion defined in Eq. (2). The general case is more complicated, both in terms of hardware implementation of the articulations and in terms of the spoofing detection calculations and analyses. The general case offers benefits as well. One benefit is an improved ability to discern when only a subset of signals are being spoofed. Another benefit is an improved spoofing detection power with fewer signals. As useful by-product is a coarse 3-axis attitude solution. For these reasons, a designer might want to implement a 2-D or 3-D articulation system.

The present section develops the rudiments of a spoofing detection test for this situation in the case of an unknown attitude but a known articulation amplitude. Analysis strategies for statistical design of the detection threshold and computation of the missed-detection probability are suggested but not fully developed. Generalizations to other interesting cases are omitted, e.g., known attitude or unknown attitude plus unknown amplitude scaling.

A. High-Pass Filtering via Linear Least-Squares Estimation

A modified form of carrier-phase measurement high-pass filtering is needed to remove the low-frequency effects of unknown UE motion and clock drift. The high-pass filter calculations solve a modified version of the least-squares problem in Eq. (16). Instead of including the unknown vector dot product $(\hat{\boldsymbol{r}}^x)^{\mathrm{T}}\hat{\boldsymbol{r}}_a$, the modified problem includes the unknown vector $\hat{\boldsymbol{b}}^x = A\hat{\boldsymbol{r}}^x$, where the unit direction vector $\hat{\boldsymbol{r}}^x$ is $\hat{\boldsymbol{r}}^j$ in the unspoofed case and $\hat{\boldsymbol{r}}^{sp}$ in the spoofed case. Thus, $\hat{\boldsymbol{b}}^x$ is the unit direction vector from the signal source to the receiver as measured in the same coordinate system that is used to define the antenna articulation time history $\boldsymbol{b}_a(t)$.

Using the newly defined $\hat{\boldsymbol{b}}^x$ direction vector in either Eq. (9) or Eq. (13), the carrier-phase time history model for the j^{th} GNSS satellite becomes:

$$\begin{bmatrix}\phi_1^j\\ \phi_2^j\\ \phi_3^j\\ \vdots\\ \phi_{N_j}^j\end{bmatrix}=\begin{bmatrix}1 & 0 & 0 & -\frac{2\pi}{\lambda}\boldsymbol{b}_a^{\mathrm{T}}(\tau_{mid1}^j)\\ 1 & (\tau_{mid2}^j-\tau_{mid1}^j) & \frac{1}{2}(\tau_{mid2}^j-\tau_{mid1}^j)^2 & -\frac{2\pi}{\lambda}\boldsymbol{b}_a^{\mathrm{T}}(\tau_{mid2}^j)\\ 1 & (\tau_{mid3}^j-\tau_{mid1}^j) & \frac{1}{2}(\tau_{mid3}^j-\tau_{mid1}^j)^2 & -\frac{2\pi}{\lambda}\boldsymbol{b}_a^{\mathrm{T}}(\tau_{mid3}^j)\\ \vdots & \vdots & \vdots & \vdots\\ 1 & (\tau_{midN_j}^j-\tau_{mid1}^j) & \frac{1}{2}(\tau_{midN_j}^j-\tau_{mid1}^j)^2 & -\frac{2\pi}{\lambda}\boldsymbol{b}_a^{\mathrm{T}}(\tau_{midN_j}^j)\end{bmatrix}\begin{bmatrix}\beta_0^j\\ \beta_1^j\\ \beta_2^j\\ \hat{\boldsymbol{b}}^x\end{bmatrix}+\begin{bmatrix}n_{\phi 1}^j\\ n_{\phi 2}^j\\ n_{\phi 3}^j\\ \vdots\\ n_{\phi N_j}^j\end{bmatrix} \tag{96}$$

One such system of equations applies for each satellite j = 1, ..., L.

As for the uni-axial case, high-pass filtering in this case starts with a QR factorization [31] of a re-scaled version of the coefficient matrix on the right-hand side of Eq. (96):

$$Q^j\begin{bmatrix}R_{11}^j & R_{12}^j & R_{13}^j & R_{14}^j & R_{15}^j & R_{16}^j\\ 0 & R_{22}^j & R_{23}^j & R_{24}^j & R_{25}^j & R_{26}^j\\ 0 & 0 & R_{33}^j & R_{34}^j & R_{35}^j & R_{36}^j\\ 0 & 0 & 0 & R_{44}^j & R_{45}^j & R_{46}^j\\ 0 & 0 & 0 & 0 & R_{55}^j & R_{56}^j\\ 0 & 0 & 0 & 0 & 0 & R_{66}^j\\ 0 & 0 & 0 & 0 & 0 & 0\\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots\end{bmatrix}=\frac{1}{\sigma^j}\begin{bmatrix}1 & 0 & 0 & -\frac{2\pi}{\lambda}\boldsymbol{b}_a^{\mathrm{T}}(\tau_{mid1}^j)\\ 1 & (\tau_{mid2}^j-\tau_{mid1}^j) & \frac{1}{2}(\tau_{mid2}^j-\tau_{mid1}^j)^2 & -\frac{2\pi}{\lambda}\boldsymbol{b}_a^{\mathrm{T}}(\tau_{mid2}^j)\\ 1 & (\tau_{mid3}^j-\tau_{mid1}^j) & \frac{1}{2}(\tau_{mid3}^j-\tau_{mid1}^j)^2 & -\frac{2\pi}{\lambda}\boldsymbol{b}_a^{\mathrm{T}}(\tau_{mid3}^j)\\ \vdots & \vdots & \vdots & \vdots\\ 1 & (\tau_{midN_j}^j-\tau_{mid1}^j) & \frac{1}{2}(\tau_{midN_j}^j-\tau_{mid1}^j)^2 & -\frac{2\pi}{\lambda}\boldsymbol{b}_a^{\mathrm{T}}(\tau_{midN_j}^j)\end{bmatrix} \tag{97}$$

where the N_j-by-6 matrix on the right-hand side of this equation is the input to the QR factorization. The N_j-by-N_j orthonormal matrix Q^j along with the R_{11}^j, R_{12}^j, R_{13}^j, …, R_{66}^j elements of the corresponding upper-triangular matrix are the factorization's outputs. The corresponding operations on the carrier-phase time history and the phase noise time history are still defined by Eq. (18), even though the actual Q^j as computed in Eq. (97) will differ from what would have been computed had Eq. (17) been used for a uni-axial antenna articulation case. The actual values of some of the R_{mn}^j coefficients will also differ, especially for $n \geq 4$.

It is helpful to collect the R_{mn}^j and z_m^j terms for all m and n in the range 4 to 6 into a single matrix vector pair:

$$R_{3D}^j=\begin{bmatrix}R_{44}^j & R_{45}^j & R_{46}^j\\ 0 & R_{55}^j & R_{56}^j\\ 0 & 0 & R_{66}^j\end{bmatrix} \quad\text{and}\quad \boldsymbol{z}_{3D}^j=\begin{bmatrix}z_4^j\\ z_5^j\\ z_6^j\end{bmatrix} \tag{98}$$

These terms define the 4th-6th rows of the transformed version of Eq. (96), the version that results from multiplication of the equation on both sides by $(Q^j)^{\mathrm{T}}/\sigma^j$. These 3 transformed equations are the only ones that are relevant to spoofing detection with general 3-D antenna articulation motion. The 1st-3rd transformed equations serve only to determine the estimates of the auxiliary low-pass-filter parameters β_0^j, β_1^j, and β_2^j. They produce no effects on any sensible spoofing detection statistic, regardless of whether these three parameters are removed from the problem via optimization or via integration over all possibilities. All equations beyond the 6th produce only residual errors that are the same for the unspoofed and spoofed cases. Therefore, they do not affect any sensible spoofing detection test either.

B. Calculation of a Spoofing Detection Statistic based on Attitude Estimation

If one assumes that the attitude A is unknown, then a sensible spoofing detection test estimates the 3-by-3 orthonormal A matrix for the non-spoofed case, and it estimates $\hat{\boldsymbol{b}}^{sp} = A\hat{\boldsymbol{r}}^{sp}$ for the spoofed case. The non-spoofed optimal attitude estimation problem takes the form:

$$\text{find:} \quad A \tag{99a}$$

$$\text{to minimize:} \quad J_{nonsp3D}(A)=\tfrac{1}{2}\sum_{j=1}^{L}[R_{3D}^j A\hat{\boldsymbol{r}}^j-\boldsymbol{z}_{3D}^j]^{\mathrm{T}} \bullet[R_{3D}^j A\hat{\boldsymbol{r}}^j-\boldsymbol{z}_{3D}^j] \tag{99b}$$

$$\text{subject to:} \quad A^{\mathrm{T}}A=I \tag{99c}$$

The problem in Eqs. (99a)-(99c) constitutes a batch maximum likelihood attitude estimation problem because $J_{nonsp3D}(A)$ is the negative natural logarithm of the probability density $p(\boldsymbol{z}_{3D}^1,...,\boldsymbol{z}_{3D}^L|A,H_0)/w$, where w is its normalization constant. The constraint in Eq. (99c) is a symmetric 3-by-3 matrix constraint. Thus, it has only 6 independent elements. The remaining unconstrained elements of A are its 3 independent attitude parameters, e.g., roll, pitch, and yaw.

A helpful tool for solving the problem in Eq. (99a)-(99c) is the attitude quaternion $\boldsymbol{q}$. It is a unit-normalized 4-element vector that can parameterize the attitude. It can be used to compute the direction cosines matrix $A = A(\boldsymbol{q})$

[36]. Using this parameterization, the attitude estimation problem becomes

$$\text{find:}\quad \boldsymbol{q} \tag{100a}$$

$$\text{to minimize:}\quad J'_{nonsp3D}(\boldsymbol{q}) = \tfrac{1}{2}\sum_{j=1}^{L}[R_{3D}^{j}A(\boldsymbol{q})\hat{\boldsymbol{r}}^{j} - \boldsymbol{z}_{3D}^{j}]^{\mathrm{T}} \bullet [R_{3D}^{j}A(\boldsymbol{q})\hat{\boldsymbol{r}}^{j} - \boldsymbol{z}_{3D}^{j}] \tag{100b}$$

$$\text{subject to:}\quad \boldsymbol{q}^{\mathrm{T}}\boldsymbol{q} = 1 \tag{100c}$$

This transformation reduces the problem to one of nonlinear constrained optimization involving 4 unknowns and a single scalar equality constraint.

A constrained implementation of Newton's method could be used to solve the problem in Eqs. (100a)-(100c) [31]. It would be helpful to start the Newton procedure with a good first guess. A reasonable first guess could be determined by solving a related problem

$$\text{find:}\quad \boldsymbol{q} \tag{101a}$$

$$\text{to minimize:}\quad J''_{nonsp3D}(\boldsymbol{q}) = \tfrac{1}{2}\sum_{j=1}^{L} w^{j}[\hat{\boldsymbol{b}}_{opt}^{j} - A(\boldsymbol{q})\hat{\boldsymbol{r}}^{j}]^{\mathrm{T}} \bullet [\hat{\boldsymbol{b}}_{opt}^{j} - A(\boldsymbol{q})\hat{\boldsymbol{r}}^{j}] \tag{101b}$$

$$\text{subject to:}\quad \boldsymbol{q}^{\mathrm{T}}\boldsymbol{q} = 1 \tag{101c}$$

where each 3-by-1 unit-direction vector $\hat{\boldsymbol{b}}_{opt}^{j}$ for j = 1, ..., L is the solution to the following estimation problem:

$$\text{find:}\quad \hat{\boldsymbol{b}}^{j} \tag{102a}$$

$$\text{to minimize:}\quad J_{j3D}(\hat{\boldsymbol{b}}^{j}) = \tfrac{1}{2}[R_{3D}^{j}\hat{\boldsymbol{b}}^{j} - \boldsymbol{z}_{3D}^{j}]^{\mathrm{T}} \bullet [R_{3D}^{j}\hat{\boldsymbol{b}}^{j} - \boldsymbol{z}_{3D}^{j}] \tag{102b}$$

$$\text{subject to:}\quad (\hat{\boldsymbol{b}}^{j})^{\mathrm{T}}\hat{\boldsymbol{b}}^{j} = 1 \tag{102c}$$

Thus, the suggested first-guess procedure involves solving L problems of the type defined in Eqs. (102a)-(102c) followed by solution of the problem in Eqs. (101a)-(101c).

This multi-step approach to generating a first guess for the problem in Eqs. (100a)-(100c) may seem complicated, but the extra effort can be worthwhile. The L $\hat{\boldsymbol{b}}_{opt}^{j}$ solutions each can be computed in closed form by using a singular value decomposition of the 3-by-3 R_{3D}^{j} matrix followed by solution of a 6th-order polynomial for the Lagrange multiplier associated with the constraint in Eq. (102c). This is essentially the same set of operations that are implemented in Eqs. (41)-(47) in order to solve the $\hat{\boldsymbol{r}}_{a}$ estimation problem in Eqs. (40a)-(40c). Of course, each of these problems must have a unique solution in order to be useful for setting up the problem in Eqs. (101a)-(101c). The problem in Eqs. (101a)-(101c) also can be solved in closed form by computing the eigenvalues and associated eigenvectors of a 4-by-4 symmetric matrix. The problem in Eqs. (101a)-(101c) is the classic Wahba problem of attitude determination [37]. The eigenvalue-based solution method is known as the q-method [36]. The positive weights w^{j} for j = 1, ..., L in Eq. (101b) should be chosen to be roughly proportional to the inverse variance of the directional accuracy of the corresponding $\hat{\boldsymbol{b}}_{opt}^{j}$ estimate from Eqs. (102a)-(102c). This can be computed from the inverse of the Hessian of the Lagrangian function associated with the optimal solution to Eqs. (102a)-(102c) after projection of that Hessian into the 2-dimensional tangent space of the normalization constraint.

Consider now the spoofed case with general $\boldsymbol{b}_{a}(t)$ antenna articulation motion. In this situation, the full attitude is not observable because the signals all come from a single unknown direction. Therefore, the relevant free parameter in the model is $\hat{\boldsymbol{b}}^{sp}$. A useful detection statistic can be developed if one estimates this quantity by solving the following problem

$$\text{find:}\quad \hat{\boldsymbol{b}}^{sp} \tag{103a}$$

$$\text{to minimize:}\quad J_{sp3D}(\hat{\boldsymbol{b}}^{sp}) = \tfrac{1}{2}\sum_{j=1}^{L}[R_{3D}^{j}\hat{\boldsymbol{b}}^{sp} - \boldsymbol{z}_{3D}^{j}]^{\mathrm{T}} \bullet [R_{3D}^{j}\hat{\boldsymbol{b}}^{sp} - \boldsymbol{z}_{3D}^{j}] \tag{103b}$$

$$\text{subject to:}\quad (\hat{\boldsymbol{b}}^{sp})^{\mathrm{T}}\hat{\boldsymbol{b}}^{sp} = 1 \tag{103c}$$

This problem can be solved in closed form using the following singular decomposition

$$U_{3D}\begin{bmatrix} \sigma_{3Da} & 0 & 0 \\ 0 & \sigma_{3Db} & 0 \\ 0 & 0 & \sigma_{3Dc} \\ 0 & 0 & 0 \\ \vdots & \vdots & \vdots \\ 0 & 0 & 0 \end{bmatrix} V_{3D}^{\mathrm{T}} = \begin{bmatrix} R_{3D}^{1} \\ R_{3D}^{2} \\ R_{3D}^{3} \\ \vdots \\ R_{3D}^{L} \end{bmatrix} \tag{104}$$

and using the following transformation of non-homogeneous terms.

$$\begin{bmatrix} z_{3Da} \\ z_{3Db} \\ z_{3Dc} \\ \boldsymbol{z}_{3Dr} \end{bmatrix} = U_{3D}^{\mathrm{T}}\begin{bmatrix} \boldsymbol{z}_{3D}^{1} \\ \boldsymbol{z}_{3D}^{2} \\ \boldsymbol{z}_{3D}^{3} \\ \vdots \\ \boldsymbol{z}_{3D}^{L} \end{bmatrix} \tag{105}$$

One performs analogous operations to those in Eqs. (43)-(47) that solve the similar problem in Eqs. (40a)-(40c). Suppose that the resulting solution is called $\hat{\boldsymbol{b}}_{opt}^{sp}$.

Note: the case of planar articulation presents special challenges to these optimization problems. It is the case of purely 2-dimensional $\boldsymbol{b}_a(t)$ motion. Its challenges are the possibility of there being two globally optimum solutions for the attitude A in Eqs. (99a)-(99c) and the certainty of there being two globally optimal solutions for the spoofing direction $\hat{\boldsymbol{b}}^{sp}$ in Eqs. (103a)-(103c). The solution pairs will map to each other via reflections through the plane of the $\boldsymbol{b}_a(t)$ motion. This happens because all of the 3-by-3 matrices R^j_{3D} are rank 2. This condition causes each of the $\hat{\boldsymbol{b}}^j$ optimization problems in Eqs. (102a)-(102c) to have 2 globally optimal solutions, and it causes σ_{3Dc} in Eq. (104) to be 0, giving rise to the two $\hat{\boldsymbol{b}}^{sp}$ solutions. If there are $L = 3$ or more signals and if their $\hat{\boldsymbol{r}}^j$ vectors are not all coplanar, which is the case for non-infinite Geometric Dilution of Precision (GDOP), then the ambiguities of the $\hat{\boldsymbol{b}}^j_{opt}$ vectors should be resolvable by the following technique: One chooses the $\hat{\boldsymbol{b}}^j_{opt}$ vectors that approximately match the dot products of all pairs of $\hat{\boldsymbol{b}}^j_{opt}$ vectors with the corresponding $\hat{\boldsymbol{r}}^j$ dot products and that approximately match the scalar triple products of all trios of $\hat{\boldsymbol{b}}^j_{opt}$ vectors with corresponding $\hat{\boldsymbol{r}}^j$ scalar triple products. These disambiguated $\hat{\boldsymbol{b}}^j_{opt}$ vectors can be used in the approximate $\boldsymbol{q}$ optimization problem in Eqs. (101a)-(101c) in order to generate a first guess for the exact problem in Eqs. (100a)-(100c). The solution to this latter problem should be unique in this case. Unfortunately, there is no similar method to resolve the $\hat{\boldsymbol{b}}^{sp}$ ambiguity. Fortunately, the ambiguity likely does not need resolution because the global minimum Eq.-(103b) costs of the true and false $\hat{\boldsymbol{b}}^{sp}$ values will be the same and will yield identical values for the spoofing detection statistic γ.

There is another possible way to resolve the ambiguities caused by 2-dimensional $\boldsymbol{b}_a(t)$ articulations. It relies on a consideration of the gain pattern of the receiver's GPS antenna. Typical gain patterns are hemispherical or narrower. Normally, only one of the two global solutions for any given $\hat{\boldsymbol{b}}^j_{opt}$ or for $\hat{\boldsymbol{b}}^{sp}$ will correspond to a signal reception direction that lies in a reasonable region of the antenna's gain pattern. Note, however, that this may not be the case for a poor combination of $\boldsymbol{b}_a(t)$ motion and gain pattern. Therefore, it may behoove the system designer to consider this issue when designing the articulation system.

Given the optimal solution A_{opt} to the attitude determination problem in Eqs. (99a)-(99c), or equivalently, the $\boldsymbol{q}_{opt}$ solution of Eqs. (100a)-(100c), and given the solution $\hat{\boldsymbol{b}}^{sp}_{opt}$ to the spoofer direction determination problem in Eqs. (103a)-(103c), a sensible spoofing detection statistic is:

$$\begin{aligned}\gamma &= J_{sp3D}(\hat{\boldsymbol{b}}^{sp}_{opt}) - J_{nonsp3D}(A_{opt}) \\ &= J_{sp3D}(\hat{\boldsymbol{b}}^{sp}_{opt}) - J'_{nonsp3D}(\boldsymbol{q}_{opt}) \qquad (106)\end{aligned}$$

A sensible spoofing detection test selects a threshold value γ_{th} and determines that no spoofing has occurred if $\gamma \geq \gamma_{th}$. A spoofing attack is declared, however, if $\gamma < \gamma_{th}$. As in all other tests defined in this paper, this test makes sense because $J_{sp3D}(\hat{\boldsymbol{b}}^{sp}_{opt})$ will tend to be large in the non-spoofed case due to the poor fit of its underlying spoofed signal model to the non-spoofed data. The cost $J_{nonsp3D}(A_{opt})$, or the equivalent quantity $J'_{nonsp3D}(\boldsymbol{q}_{opt})$, will tend to be small due to the reasonableness of its model. Therefore, γ will tend to be a large positive number in the absence of spoofing. Under a spoofing attack, however, $J_{sp3D}(\hat{\boldsymbol{b}}^{sp}_{opt})$ will be small due to a good fit between its model and the carrier-phase data, while $J_{nonsp3D}(A_{opt})$ and the equivalent $J'_{nonsp3D}(\boldsymbol{q}_{opt})$ will tend to be large, and γ will tend to be a negative number of large magnitude. A value of γ_{th} in the vicinity of 0 should suffice to detect spoofing attacks with a low probability of false alarm and a low probability of missed detection. This test will not be an optimal Neyman-Pearson test due to its use of the optimized values A_{opt} and $\hat{\boldsymbol{b}}^{sp}_{opt}$ instead of integration over all possible values. This test is likely to be nearly as powerful as the optimal test, however, due to the efficacy of optimization as a proxy for integration.

Although the specifics of the detection statistic calculation change for 2D and 3D antenna motion, the basic spoofing detection principle remains the same. During a spoofing attack, there is no geometric diversity of the direction of arrival of the L signals. Therefore, to within measurement error, all of the carrier phase variations caused by the $\boldsymbol{b}_a(t)$ motion will be identical for all L satellites. When there is no spoofing, however, the L different satellites will, in general, exhibit L distinct carrier-phase responses to the $\boldsymbol{b}_a(t)$ motion. Successful spoofing detection is a matter of distinguishing between these two situations. The difference of carrier-phase-model fits between the spoofed and non-spoofed assumptions, as embodied in Eq. (106) and in similar equations throughout this paper, represents a good mechanization for comparing the relative sameness vs. diversity of the carrier phase responses to $\boldsymbol{b}_a(t)$.

C. Design of Spoofing Detection Threshold and Analysis of Probabilities, Unknown Attitude and General 3D Articulation

The spoofing detection test for the case of general 3D antenna articulations requires some design and analysis.

The spoofing detection threshold γ_{th} must be chosen to give a particular false-alarm probability, and the resulting probability of missed detection must be analyzed. For the sake of brevity, the required analyses are not carried out here. Instead, general approaches are defined that could be used to carry out the analyses.

The first step in the design and analysis is to characterize the non-spoofed and spoofed probability density functions for the detection statistic γ, $p(\gamma|A,H_0)$ and $p(\gamma|\hat{\boldsymbol{b}}^{sp},H_1)$. A good first step in deriving these functions is to express γ as a function of the ($3L$)-by-1 dimensional noise vector $\boldsymbol{\nu}_{3D} = [n_4^1;\ n_5^1;\ n_6^1;\ n_4^2;\ n_5^2;\ n_6^2;\ n_4^3;\ n_5^3;\ n_6^3;\ ...\ ;\ n_4^L;\ n_5^L;\ n_6^L]$. The noise terms n_4^j, n_5^j, and n_6^j are the ones calculated in the alternate version of Eq. (18) that is associated with the high-pass-filter QR factorization for the 3D problem given in Eq. (97). This first step will probably require approximation to yield a result that is valid only to second order in $\boldsymbol{\nu}_{3D}$. The resulting equations will be 3D analogs of Eqs. (49) and (53) that look somewhat similar. The main differences will lie in the terms that are quadratic forms in $\boldsymbol{\nu}_{3D}$. In Eqs. (49) and (53), the quadratic form in $\boldsymbol{\nu}$ involves a symmetric weighting matrix that is the difference between a projection matrix onto a 2D subspace, or nearly so, and a projection matrix onto a 1D subspace. In the new equations, the matrix difference will be between a projection matrix onto a 3D subspace, or nearly so, and a projection matrix onto a 2D subspace, or nearly so.

The most important feature of the resulting γ formulas in terms of $\boldsymbol{\nu}_{3D}$ is that they will still be dominated by Gaussian terms. Therefore, Gaussian approximations can be developed for $p(\gamma|A,H_0)$ and $p(\gamma|\hat{\boldsymbol{b}}^{sp},H_1)$.

Given $p(\gamma|A,H_0)$, the design of γ_{th} will proceed similarly to the design used in Subsection V.C. Given a worst-case probability of false alarm α_{wc}, a corresponding worst-case attitude A_{wc} will be estimated, and the corresponding threshold γ_{th} will be determined using α_{wc} and $p(\gamma|A_{wc},H_0)$ in a standard calculation. Note that the optimization problem used to determine A_{wc} will be somewhat more complicated than the corresponding problems for the case of 1D antenna articulation motion. It may be advisable to solve for an equivalent worst-case true attitude quaternion $\boldsymbol{q}_{wc}$ and then use that to compute $A_{wc} = A(\boldsymbol{q}_{wc})$. Such an approach will reduce the dimensionality of the worst-case optimization problem from 9 to 4 while reducing the number of nonlinear equality constraints from 6 to 1.

Given γ_{th} and $p(\gamma|\hat{\boldsymbol{b}}^{sp},H_1)$, a worst-case false-alarm probability will be computable, similar to what has been done in Subsection V.C for the unknown attitude case with 1D articulation motion. This will involve an optimization problem to determine the worst-case spoofing direction vector $\hat{\boldsymbol{b}}_{wc}^{sp}$. It will be an equality-constrained optimization that enforces $(\hat{\boldsymbol{b}}_{wc}^{sp})^{\mathrm{T}}\hat{\boldsymbol{b}}_{wc}^{sp} = 1$.

IX. SPOOFING DETECTION RESULTS USING DATA FROM TRUTH-MODEL SIMULATIONS AND FROM LIVE-SIGNAL TESTS

The spoofing detection techniques of Sections IV-VI have been tested using truth-model simulation data. The technique of Section VI, coupled with the time phasing estimation of Section VII, has also been tested using live-signal data. All of these tests involve simple 1-dimensional $\boldsymbol{b}_a(t)$ articulation motion. No tests have yet been implement for general 3D antenna articulation. All of the tests have worked with the GPS L1 C/A-code signal, which has a nominal carrier frequency of $f_{L1} = 1575.42\text{x}10^6$ Hz and a nominal wavelength of $\lambda_{L1} = c/f_{L1} = 0.190294$ m. All of these tests exhibit very good detection power and small probabilities of false alarm when using peak-to-peak antenna deflections in the range 4-6 cm and detection intervals in the range 0.125 to 0.5 sec. Representative test results are described in this section.

A. Design of Monte-Carlo Truth-Model Simulation Tests

Two truth-model simulations have been developed, one to simulate the non-spoofed beat carrier phase time histories, as modeled by Eq. (10), and another to simulate the spoofed beat carrier phase histories, as per Eq. (15). Each simulation has used truth values of the quadratic polynomial low-pass filter nuisance parameters β_0^j, β_1^j, and β_2^j for GPS satellites j = 1, ..., L. It also has used a truth articulation direction $\hat{\boldsymbol{r}}_a$ and a truth articulation amplitude time history $\rho_a(t)$. The non-spoofed simulations have used truth directions from the satellites to the defended receiver $\hat{\boldsymbol{r}}^j$ for j = 1, ..., L, but the spoofed simulations have used only a truth value for the spoofer-to-receiver unit direction vector $\hat{\boldsymbol{r}}^{sp}$. Each simulation has generated simulated carrier phase measurements ϕ_k^j at the truth sample times τ_{midk}^j for k = 1, ..., N_j and j = 1, ..., L. Each such measurement has been corrupted by zero-mean Gaussian discrete-time white noise $n_{\phi k}^j$ sampled using a random number generator. The standard deviation σ^j of the jth satellite signal's noise sequence has been dictated by its carrier-to-noise ratio C/N_0, as modeled in Eq. (11).

For each spoofing detection test, the test calculations have been supplied with the following data from the truth-model simulation: ϕ_k^j and τ_{midk}^j for k = 1, ..., N_j and j = 1, ..., L, $\rho_{anom}(t)$, $\hat{\boldsymbol{r}}^j$ for j = 1, ..., L, and σ^j for j = 1, ..., L. In all non-spoofed cases, the supplied $\hat{\boldsymbol{r}}^j$ direction vectors have equaled the truth vectors that have been used in the corresponding truth-model simulation. In all spoofed cases, the supplied $\hat{\boldsymbol{r}}^j$ direction vectors are a reasonable fictitious set that the spoofer has led the victim receiver to believe as being the directions from actual satellites.

Additional data supplied to the spoofing detection test have varied with the test. In the case of the known-attitude/known-amplitude tests of Section IV, the articulation direction vector $\hat{\boldsymbol{r}}_a$ also has been supplied to the detection test calculations, the same one as has been used in the truth-model simulation. For both the known-attitude/known-amplitude test of Section IV and the unknown-attitude/known-amplitude test of Section V, the supplied nominal articulation amplitude time history $\rho_{anom}(t)$ has equaled the truth $\rho_a(t)$ that has been used in the simulation. For the unknown-attitude/unknown-amplitude test of Section VI, however, the supplied value of $\rho_{anom}(t)$ has equaled $\rho_a(t)/a$, where $\rho_a(t)$ is the truth time history and the value $a \geq 1$ is the truth amplitude rescaling factor. In no spoofed case has the spoofer direction $\hat{\boldsymbol{r}}^{sp}$ been supplied to the spoofing detection calculations.

In each test scenario, the truth-model simulation has been run in a Monte-Carlo mode: Thousands of trials have been run with the same input parameters but with different random number seeds to generate different white-noise sequences $n_{\phi k}^j$ for $k = 1, ..., N_j$ and $j = 1, ..., L$. A spoofing detection statistic has been computed for each set of simulated data, and histograms of the statistic have been plotted. Also plotted have been the spoofing detection threshold and the predicted theoretical probability density functions of the spoofing detection statistic for the non-spoofed and spoofed conditions. These plots characterize the power of the test and the accuracy of the Gaussian approximations used to design and analyze the various detection scenarios.

The tests that have been run have concentrated on cases that use $L = 6$ GPS satellite signals with a distribution of $\hat{\boldsymbol{r}}^j$ direction vectors that yields a GDOP of 3.5. The modeled carrier-to-noise ratios range from 38.2 dB-Hz to 44.0 dB-Hz. These are somewhat conservative assumptions about the number of available satellites, their geometric dilution of precision, and their signal strengths. This conservatism translates into less detection power for a given false-alarm probability than would be available in spoofing detection tests that had more satellites, a better GDOP, or stronger signals.

Additional common features of the simulation cases have been the form of the $\rho_a(t)$ articulation time history, the duration of the detection data batch, and the sample rate. $\rho_a(t)$ is always an 8 Hz sine wave, and the detection covers one full period of its oscillation. Thus, the total detection interval is 0.125 sec. The accumulation period $\Delta\tau_{cavg}^j = 0.001$ sec has been used so that each satellite contributes $N_j = 125$ carrier-phase measurements to each detection test.

The decision to use one full period of a sine wave, starting at zero phase and ending at a phase of 2π, guarantees a significant residual signal component after the high-pass filtering associated with the QR factorization in Eq. (17). This is true because a full period of a sine wave cannot be fit well by the quadratic polynomial that is parameterized by its β_0^j, β_1^j, and β_2^j coefficients. The presence of significant residual articulation signal after high-pass filtering is important to achieving a good detection power.

The peak-to-peak $\rho_a(t)$ deflections have been varied from 4.76 cm to 5.85 cm. The lower number is exactly a quarter of a carrier wavelength. The higher number is about 31% of a wavelength. As per Eq. (11), $C/N_0 = 38.2$ dB-Hz at a 1000 Hz accumulation frequency translates into a carrier phase measurement error standard deviation of $\sigma^j = 0.275$ rad (0.0438 cycles). This standard deviation is no greater than 17.5% of the phase effect of the peak-to-peak antenna motion. Therefore, the articulation motion should be clearly discernable in the data.

Several truth values have been used for the articulation direction vector $\hat{\boldsymbol{r}}_a$ and for the spoofer direction vector $\hat{\boldsymbol{r}}^{sp}$. In some cases, random values have been chosen for these directions. In other cases, worst-case values have been chosen as the truth values. That is, the truth $\hat{\boldsymbol{r}}_a$ sometimes has been chosen to equal the solution to the worst-case direction problem in Eqs. (59a)-(59c) for the situation of known amplitude and unknown attitude. Similarly, $\hat{\boldsymbol{r}}^{sp}$ sometimes has been chosen so that $\eta = (\hat{\boldsymbol{r}}^{sp})^{\mathrm{T}}\hat{\boldsymbol{r}}_a$ equals the solution to the worst-case dot product problem in Eqs. (61a)-(61c).

B. Monte-Carlo Simulation Test Results

The Monte-Carlo simulation results for a typical spoofing detection test are shown in Fig. 5. It shows γ detection statistic histograms for 10000 Monte-Carlo simulations of a non-spoofed case and 10000 other Monte-Carlo simulations of the corresponding spoofed case for an unknown-attitude/known-amplitude spoofing detection test. This is the test developed in Section V. Also shown are the spoofing detection threshold for a worst-case false alarm probability of $\alpha_{wc} = 10^{-5}$ along with the theoretical non-spoofed and spoofed probability density functions for

γ. Note that the non-spoofed and spoofed cases both use the same $\rho_a(t)$ articulation time history and the same values of $\hat{\boldsymbol r}^j$ for $j = 1, ..., L$ for all of their tests. The peak-to-peak antenna deflections in $\rho_a(t)$ are 4.76 cm, i.e., exactly a quarter of the nominal L1 wavelength. All 10000 non-spoofed cases use the same truth value of $\hat{\boldsymbol r}_a$, and all 10000 spoofed cases use the same truth value of $\eta = (\hat{\boldsymbol r}^{sp})^{\mathrm T}\hat{\boldsymbol r}_a$.

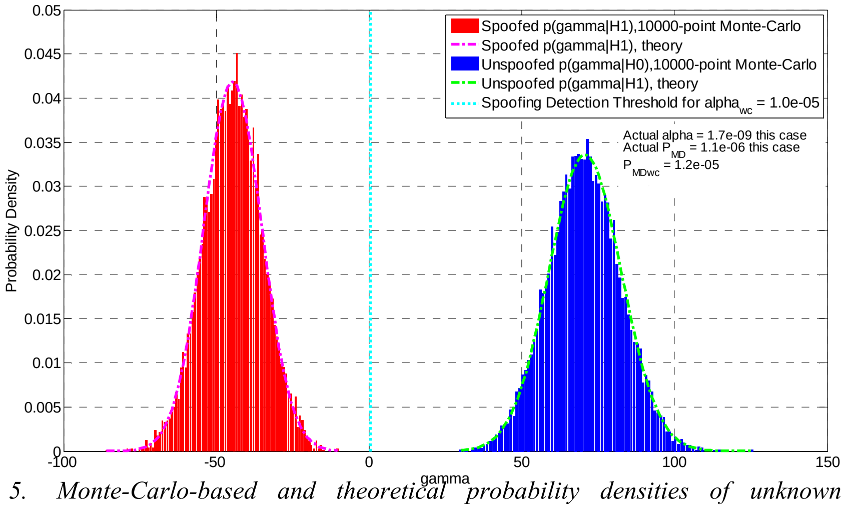

Fig. 5. *Monte-Carlo-based and theoretical probability densities of unknown-attitude/known-amplitude 1D-articulation spoofing detection tests and comparison to worst-case detection threshold.*

It is clear from Fig. 5 that the spoofing detection test correctly classified all 10000 non-spoofed cases and all 10000 spoofed cases. It is also clear that the theoretical and Monte-Carlo probability density functions are in good agreement. This agreement confirms the reasonableness of the Gaussian approximations of $p(\gamma\,|\,\hat{\boldsymbol r}_a, H_0)$ and $p(\gamma\,|\,\eta, H_1)$.

The truth values of $\hat{\boldsymbol r}_a$ and η that have been used to generate the data in Fig. 5 are not the worst-case values for the given situation. This is evidenced by two facts: The actual probability of false alarm is $\alpha = 1.7\text{x}10^{-9} < \alpha_{wc} = 10^{-5}$, and the actual probability of missed detection is $P_{MD} = 1.1\text{x}10^{-6} < P_{MDwc} = 1.2\text{x}10^{-5}$. Even if $\hat{\boldsymbol r}_a$ and η had taken on their worst-case values, the resulting detection test still would have been very powerful.

Another typical case is shown in Fig. 6. This case is similar in many respects to that of Fig. 5, except for three points: First, it is for the unknown-attitude/unknown-amplitude case. Second, its truth values of $\boldsymbol r_a = a\,\hat{\boldsymbol r}_a$ and of $\eta = a\,(\hat{\boldsymbol r}^{sp})^{\mathrm T}\hat{\boldsymbol r}_a$ are the worst-case values for the given parameters of this problem. Third, the $\rho_a(t)$ articulation time history has a slightly larger peak-to-peak deflection, 5.77 cm, which is 30.3% of the nominal L1 carrier wavelength. Note that the worst-case value of a is 1, i.e., the smallest possible value, so that $\boldsymbol r_a = \hat{\boldsymbol r}_a$.

The results for the unknown-attitude/unknown-amplitude test in Fig. 6 are very good, and they are comparable to those in Fig. 5. The probability of false alarm is only $\alpha = \alpha_{wc} = 10^{-7}$, and the probability of missed detection is only $P_{MD} = P_{MDwc} = 1.6\text{x}10^{-7}$. Note that the improved worst-case values for Fig. 6's results vs. those of Fig. 5 are likely due to the slightly larger amplitude of the antenna articulations.

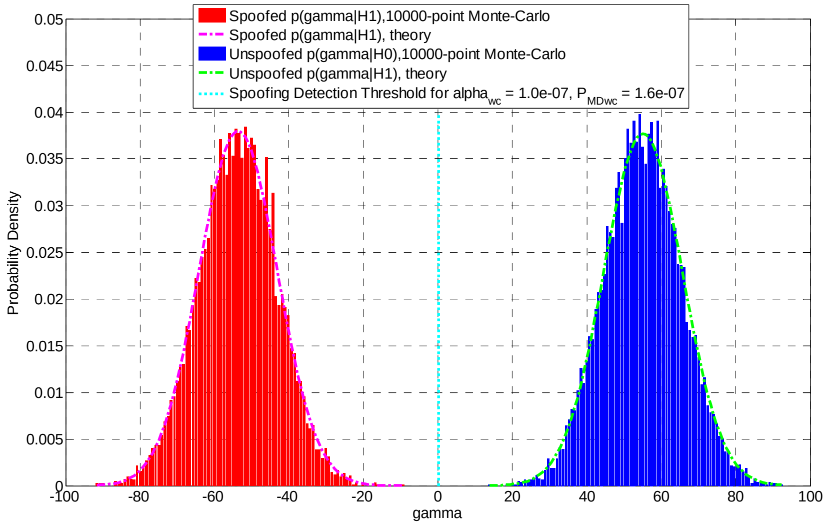

Fig. 6. *Unknown-attitude/Unknown-amplitude 1D-articulation spoofing detection test results from Monte-Carlo simulation and theoretical analyses.*

All of the other Monte-Carlo tests have produced similar good results. The largest values of α_{wc} and P_{MDwc} have been, respectively, $3.0\text{x}10^{-5}$ and $2.8\text{x}10^{-5}$. These both occurred on the smallest-amplitude case, a case with unknown-attitude/unknown-amplitude and with a $\rho_{anom}(t)$ peak-to-peak articulation of only 4.52 cm. Even these largest probabilities are very small. They are characteristic of reliable tests. All of the tests used peak-to-peak antenna motion of less than 6 cm and a detection interval of 0.125 seconds. These are very powerful tests for a compact system, and they detect spoofing attacks quickly.

C. Test Scenarios that use Live Data

Three sets of test have been conducted using live data. All of these tests have been conducted using the prototype articulation system shown in Fig. 3. Therefore, it has been necessary to use the unknown-attitude/unknown-amplitude spoofing detection test of Section VI along with the Δt_0 time phasing estimation pre-processing calculations that are described in Section VII.

Two of the test sets included spoofing or spoofing-like signals. A spoofing-like signal has been generated for one set of tests by receiving GPS signals using an outdoor antenna, amplifying them, and re-radiating them indoors in an anechoic chamber. Although not true spoofing, this configuration has the same signal-in-space geometry that is exploited by the present spoofing detection techniques: All of the signals come from the common direction $\hat{\boldsymbol{r}}^{sp}$. In this case, the direction points from the re-radiating antenna to the defended receiver's articulating antenna, which is also inside the anechoic chamber. The particular anechoic chamber that has been used is a NASA facility in Wallops Island, Virginia. This facility has permission to re-radiate GPS signals inside the chamber because it provides sufficient shielding to prevent RF energy from radiating outside of the chamber. The tests in this facility were conducted on April 26, 2012.

A true spoofing signal has been generated using an advanced version of the spoofer described in Refs. 3 and 4. It was authorized to broadcast live spoofing signals on the night of June 19-20, 2012 at White Sands Missile Range, NM (WSMR). These broadcasts were conducted as part of a special series of GPS integrity tests that had been arranged by the Department of Homeland Security. The prototype spoofing detection system was brought to WSMR and tested against some of the spoofing attacks that were initiated that night. It was located in the region where the spoofer was targeting victims so that the spoofed signals would look realistic. The prototype system was also tested that same night during quite times when the spoofer was turned off.

The third set of tests were for a typical non-spoofed case in Ithaca, NY. This test was conducted on top of a tall building on the campus of Cornell University on May 3, 2012. Thus, there were two independent sets of data under spoofing or spoofing-like conditions and two other independent sets of data under non-spoofed conditions.

Purely for the sake of ease of implementation, the prototype system did all of its GPS signal processing and spoofing detection calculations in a post-processing mode. The antenna motion was activated by using an attached string to cause an initial deflection of the cantilevered-beam antenna mount. Prior to initiating motion, a GPS digital storage receiver started operation to record the entire L1 signal bandwidth. The stored RF data were later processed on a work station using a C-language software GPS receiver in order to produce the raw beat carrier phase observables ϕ_k^j for $k = 1, \ldots, N_j$ and $j = 1, \ldots, L$. The software receiver also produced raw signal accumulations, which were used in order to deduce each carrier-to-noise ratio $(C/N_0)^j$ for purposes of computing carrier-phase measurement standard deviation σ^j, as in Eq. (11). All of the beat carrier phase measurements used a nominal accumulation interval of $\Delta\tau_{cavg}^j = 0.01$ sec. That is, carrier phase was sampled at 100 Hz.

After generation by the software receiver, the raw ϕ_k^j measurements were input to the spoofing detection signal processing calculations. These calculations included the cycle-slip repair described in Subsection III.A, the high-pass filtering calculations in Eqs. (17) and (18) of Section IV.B, the Δt_0 estimation calculations of Subsection VII.A, and the spoofing detection calculations of Section VI.

An additional auxiliary estimation problem had to be solved prior to performing the spoofing detection calculations: The shape of the $\rho_{anom}(t)$ articulation profile had to be estimated. It was known *a priori* from the vibration theory of linear structures that a good approximation of this profile would be a decaying sinusoid of the form

$$\rho_{anom}(t-\Delta t_0) = \rho_{a0} e^{-\zeta\omega_n(t-\Delta t_0)} \sin[(t-\Delta t_0)\omega_n\sqrt{1-\zeta^2}] \qquad (107)$$

where ρ_{a0} is the initial amplitude, ζ is the damping ratio, ω_n is the undamped natural frequency, and Δt_0 is the time phasing variable defined in Section VII. Unfortunately, these quantities were not known ahead of time. In order to do spoofing detection, it was necessary to have good estimates of ζ and ω_n along with a coarse estimate of Δt_0 and a lower bound for ρ_{a0}.

Therefore, a pre-processing estimation problem has been solved to determine ζ, ω_n, and Δt_0. It minimizes the following modified version of the Δt_0 estimation cost function from Eq. (90):

$$J_{shape}(\zeta,\omega_n,\Delta t_0) = \frac{1}{2}\left(\frac{\Delta t_0}{\sigma_{\Delta t0ap}}\right)^2 + \frac{1}{2}\sum_{j=1}^{L}(\boldsymbol{f}^j)^{\mathrm{T}}\{I - \hat{\boldsymbol{d}}^j(\Delta t_0;\zeta,\omega_n)[\hat{\boldsymbol{d}}^j(\Delta t_0;\zeta,\omega_n)]^{\mathrm{T}}\}\boldsymbol{f}^j \qquad (108)$$

where $\hat{\boldsymbol{d}}^{j}(\Delta t_0;\zeta,\omega_n)$ is the same function that is defined by Eqs. (91b) & (92b), but with $\rho_a(t\text{–}\Delta t_0)$ in Eq. (92b) replaced by $\rho_{anom}(t\text{–}\Delta t_0)$ from Eq. (107). Note that this cost function does not depend on the unknown articulation amplitude ρ_{a0} because the $\hat{\boldsymbol{d}}^{j}(\Delta t_0;\zeta,\omega_n)$ normalization calculations in Eq. (91b) remove the dependence on ρ_{a0}. The corresponding $\hat{\boldsymbol{d}}^{j}(\Delta t_0;\zeta,\omega_n)$ $[\hat{\boldsymbol{d}}^{j}(\Delta t_0;\zeta,\omega_n)]^{\mathrm{T}}$ term in Eq. (108) effectively estimates the phase time history scaling quantities $-\frac{2\pi}{\lambda}(\hat{\boldsymbol{r}}^{j})^{\mathrm{T}}\hat{\boldsymbol{r}}_a\rho_{a0}$ for j = 1, …, L as independent unknowns and removes them from the problem. The minimization of $J_{shape}(\zeta,\omega_n,\Delta t_0)$ starts with reasonable first guesses of ζ, ω_n, and Δt_0 as determined by operator inspection of the corresponding ϕ_k^j vs. τ_{midk}^j time histories, and it iterates to compute improved estimates using Newton's method.

Typical detrended carrier-phase data used in the estimation of ζ, ω_n, and Δt_0 appear in Fig. 7. These data come from one of the non-spoofed detection tests conducted at WSMR. The initial string pull starts at t = 0.3 sec. The release of the string and the start of the damped oscillations occur as t = 2.2 sec. It is obvious that the subsequent carrier phase oscillations during the interval from t = 2.2 sec to t = 4 sec are modeled reasonably well by the decaying sinusoid in Eq. (107). In one curve fitting scenario, all of the data from t = 2.35 sec to t = 3.63 sec were used, which constitutes 3 full cycles of the decaying oscillations. The resulting estimates of the damping ratio and the undamped natural frequency are ζ = 0.0581 and ω_n = 14.8405 rad/sec. This gives a damped period of 0.4241 sec. The damping ratios and undamped natural frequencies estimated for all the various data sets of the prototype system span the ranges ζ = 0.0137 to 0.1164 and ω_n = 10.9982 to 15.2119 rad/sec. The lower frequency cases in the range ω_n = 10.9982 to 11.9545 rad/sec occurred in the April and May tests in Wallops Island and Ithaca. The higher frequency cases in the range ω_n = 14.7732 to 15.2119 rad/sec all occurred at WSMR. This frequency jump was the result of a change in the cantilever beam conditions that caused a slight stiffening of its effective spring constant. The highest damping ratios, in the range ζ = 0.0751 to 0.1164, correspond to WSMR cases that use only the last one or two oscillation periods before the oscillations stop altogether, e.g., between t = 3 and t = 3.85 sec in Fig. 7. The larger effective damping ratios for lower amplitude oscillations presumably are due to the presence of nonlinear static friction in the system. This indicates that spoofing detection tests conducted using the later oscillations of the prototype system might not perform exactly as modeled because the nonlinear friction effects become more important, and they are not modeled as well by the decaying sinusoidal time history in Eq. (107).

The carrier phase time histories in Fig. 7 serve to illustrate this paper's means of spoofing detection. It is obvious from this figure that all of the L = 8 satellite signals exhibit similar decaying sinusoid time histories with the same phase, except for a possible sign change. This is exactly what is predicted by the 1-dimensional non-spoofed carrier phase model in Eq. (10). Presumably the differing signs and amplitudes of the signals are explainable in terms of the differing values of $(\hat{\boldsymbol{r}}^{j})^{\mathrm{T}}\hat{\boldsymbol{r}}_a$ for some reasonable estimate of $\hat{\boldsymbol{r}}_a$. In all of the spoofed cases, however, the detrended decaying sinusoids for the different signals all have the same amplitude and sign because the $(\hat{\boldsymbol{r}}^{sp})^{\mathrm{T}}\hat{\boldsymbol{r}}_a$ term in Eq. (15) is the same for all signals. This situation is shown in Fig. 8 for a spoofed case recorded at WSMR.

The task of the spoofing detection calculation is to test whether sameness is the best model or whether a better model is one of differences. The former explanation indicates spoofing, but the latter indicates no spoofing. In the latter case, however, these differences must be explainable in terms of differing $(\hat{\boldsymbol{r}}^{j})^{\mathrm{T}}\hat{\boldsymbol{r}}_a$ values for differing signal indices j and for some reasonable $\hat{\boldsymbol{r}}_a$ estimate. The other carrier-phase-based spoofing detection tests that have been proposed, e.g., those of Refs. 21 and 22, give no indication that one can detect GNSS spoofing by

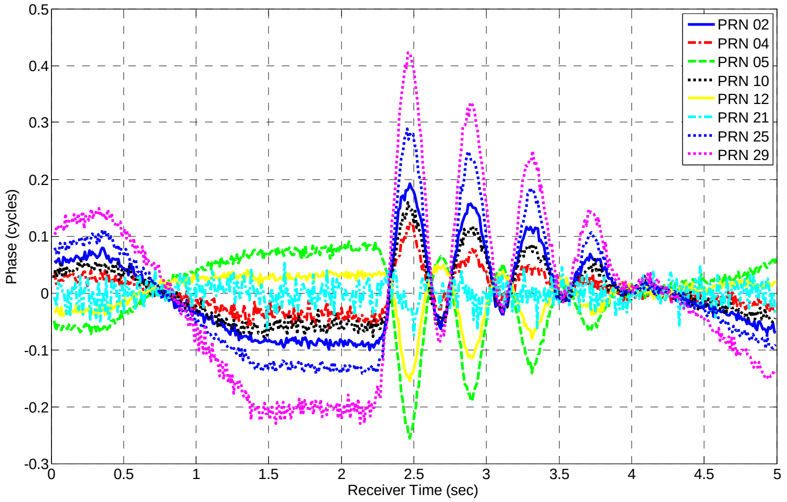

Fig. 7. Detrended carrier-phase data for multiple satellites for a typical non-spoofed case using the prototype 1-dimensional antenna articulation system.

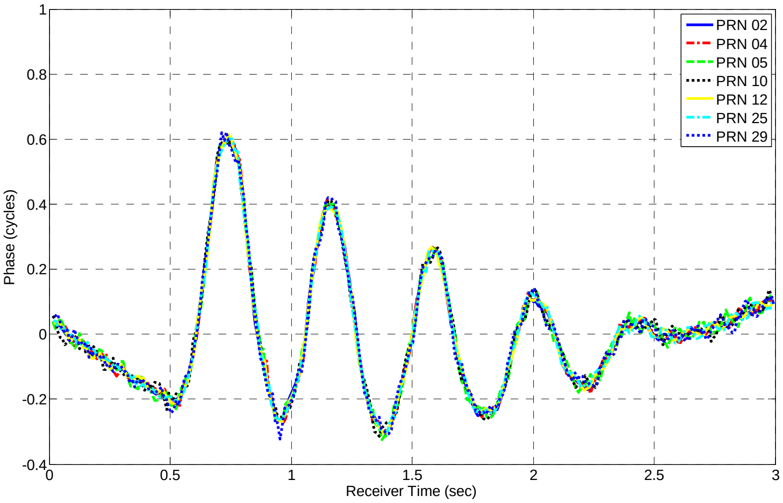

Fig. 8. Multiple satellites' detrended carrier-phase data for a typical spoofed case using the prototype 1-dimensional antenna articulation system.

exploiting the obvious difference between the diversity of carrier phase time histories in Fig. 7 and the uniformity in Fig. 8, especially if the diversity in Fig. 7 correlates well with the known antenna motions.

D. Results of Live-Data Tests

The live-data spoofing detection tests have all proved successful. A total of 4 non-spoofed cases and 4 spoofed cases have been analyzed, and the correct decision about the presence of spoofing has been reached in every case. All cases have used the worst-case probability of false alarm value α_{wc} = 10^{-6}, and the largest worst-case probability of missed detection has been P_{MDwc} = 1.6x10^{-6}.

Peak-to-peak antenna deflections in the non-spoofed cases, where they could be directly estimated, have ranged from 4.01 cm (21% of λ_{L1}) to 13.55 cm (71% of λ_{L1}). The spoofed-case amplitudes have been appraised as having been commensurate based on the known consistency of the initial impulses, and the corresponding η dot-product/amplitude estimates have been consistent with this range of peak-to-peak amplitudes. The tests with the largest peak-to-peak articulation amplitudes used data from the start of an articulation time history, e.g., the first full oscillation periods in Figs. 7 and 8. The tests with the smallest amplitudes used one of the last full oscillations, e.g., the oscillation starting at t = 3.43 sec in Fig. 7 and the one starting at t = 2.11 sec in Fig. 8. A test using one of the later oscillations has been run for each of the 8 cases, and the non-spoofed later oscillation peak-to-peak amplitude estimates range from 4.01 cm 5.9 cm. The corresponding minimum peak-to-peak deflections, as determined by the $a \geq 1$ amplitude constraint and the $\rho_{anom}(t)$ time histories, ranged from 2.86 cm to 4.21 cm. Thus, the system can work effectively with small antenna deflections.

Each test used approximately one period of the decaying sinusoidal $\rho_{anom}(t)$, yielding detection intervals ranging from 0.39 sec to 0.57 sec. The simulation test results of Subsection IX.B imply that shorter intervals would have sufficed had the articulation system been designed to vibrate at a higher frequency.

The number of satellites available for the tests ranged from L = 6 to 9, and the corresponding GDOP values ranged from 1.77 to 4.90. The carrier-to-noise ratios ranged from C/N_0 = 30.6 to 51.3 dB-Hz, with the mean values over all the satellites in a given test ranging from $(C/N_0)_{avg}$ = 39.3 to 47.3 dB-Hz. The power of the test is expected to increase with increasing L, with increasing $(C/N_0)_{avg}$, and with increasing minimum peak-to-peak antenna deflection, and to decrease with increasing GDOP. In fact, the weakest test, the one with P_{MDwc} = 1.6x10^{-6}, had the minimum number of satellites of any of the cases, L = 6 satellites, and it had the second highest GDOP, 4.35. Its $(C/N_0)_{avg}$ was 44.3 dB-Hz. It also had almost the smallest minimum peak-to-peak deflection constraint as defined by its $\rho_{anom}(t)$. The other case with L = 6 satellites had almost the same $(C/N_0)_{avg}$, 44.2 dB-Hz, a larger minimum peak-to-peak deflection, 3.99 cm, and a lower GDOP, 3.86. The larger minimum deflection and the lower GDOP explain its lower P_{MDwc}. The other case with slightly higher GDOP, 4.90, had a larger number of satellites, L = 7, a larger $(C/N_0)_{avg}$, 47.3, and a larger minimum peak-to-peak deflection, 4.21 cm. These differences explain its decreased P_{MDwc}.

The detection results for a typical non-spoofed case are shown in Fig. 9. The test was made at WSMR when the spoofer was not broadcasting. This case corresponds to the weakest detection of all 8 cases, both spoofed and non-spoofed, the one that yielded P_{MDwc} = 1.6x10^{-6}. The spoofing detection statistic γ is plotted along the horizontal axis. The vertical black dashed line shows the actual computed value of γ from the GPS data. The vertical dash-dotted magenta lines show the worst-case threshold values γ_{th} as computed for the following three different estimates of Δt_0: t_{0opt}, $\Delta t_{0opt}+2\sigma_{\Delta t0opt}$, and Δt_{0opt}-$2\sigma_{\Delta t0opt}$, as per the analysis described in Subsection VII.C. The left-most of these three vertical lines constitutes the detection threshold. Given that the three candidate thresholds lie virtually on top of each other, the choice of the lowest is somewhat immaterial. The vertical dashed black line lies very far to the right of the three vertical dash-dotted magenta lines. Therefore, this detection is clearly successful in ruling out a spoofing attack.

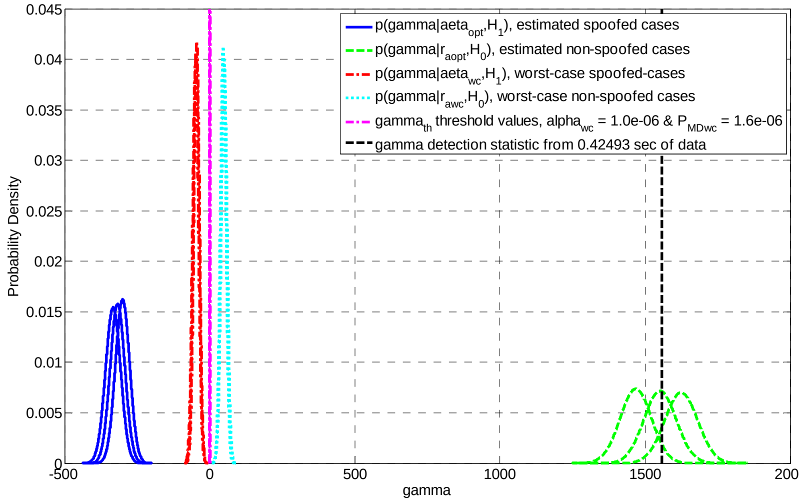

Fig. 9. Spoofing detection statistic, threshold, and related probability density functions for a typical non-spoofed case with live data.

Figure 9 also plots various relevant probability density functions. Consistent with the analysis of Subsection VII.C, these are plotted in triplets, one for each of the elements of the triplet of candidate Δt_0 estimates: t_{0opt}, $\Delta t_{0opt}+2\sigma_{\Delta t0opt}$, and $\Delta t_{0opt}-2\sigma_{\Delta t0opt}$. The three dotted cyan probability density functions represent the worst-case non-spoofed situation, and the three dash-dotted red probability functions represent the corresponding worst-case spoofed situations. Obviously, there is sufficient separation between these sets of probability density functions to yield a powerful detection test, as evidenced by the ability to draw the dash-dotted magenta detection thresholds in a way that clearly separates the red and cyan distributions. Further confirmation of good detection power is provided by the low worst-case probabilities of false alarm and missed-detection.

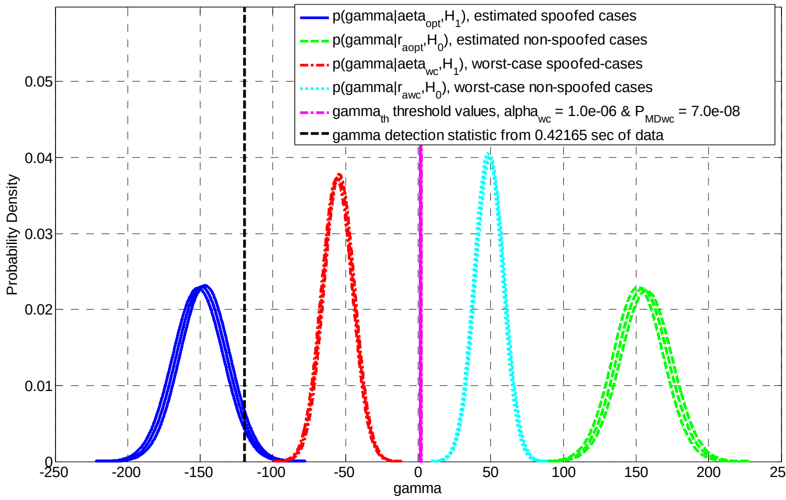

Fig. 10. Performance of a typical spoofed case with live data: spoofing detection statistic, threshold, and related probability density functions.

The three dashed green curves are the non-spoofed $p(\gamma|\mathbf{r}_a,H_0)$ probability density functions using the estimated value of $\mathbf{r}_a$ in place of the worst-case value. The solid blue curves are the spoofed $p(\gamma|\eta,H_1)$ probability density functions using the estimated value of η in place of the worst-case value. Of course, the $\mathbf{r}_a$ estimate used to generate the dashed green curves has much more meaning than does the η estimate used to generate the solid blue curves because this is a non-spoofed case. The important point of these latter probability density plots is that the actual γ, the vertical dashed black line, is believable as a sample from all three of the dashed green probability density functions. This fact indicates that the signal models used to generate the hypothesis test calculations are reasonable.

Figure 10 plots detection results for a typical spoofed case. All of the definitions and line/curve colors are the same in Fig. 10 as in Fig. 9. The only major difference is that the vertical dashed black line plotted at the calculated detection value γ now lies far to the left of the 3 dash-dotted magenta vertical lines, the three candidate γ_{th} detection threshold values. The fact that $\gamma < \gamma_{th}$ by a wide margin indicates a very reliable detection of the spoofing attack. The worst-case spoofed and non-spoofed probability density functions are widely separated, allowing the selection of a γ_{th} threshold value that yields both a low worst-case probability of false alarm and a low worst-case probability of missed detection. The overlap between the vertical dashed black detection statistic and the solid blue probability density functions indicates the reasonableness of the spoofed hypothesis that γ is a sample from one of these 3 $p(\gamma|\eta_{opt},H_1)$ distributions. Note that this case has L = 6 GPS signals, $(C/N_0)_{avg}$, = 44.2 dB-Hz, GDOP = 3.86, and a minimum peak-to-peak antenna articulation of 3.99 cm.

In summary, the live-data tests of this system indicate excellent performance. The correct situation of spoofing or non-spoofing has been identified unambiguously in all cases considered. Furthermore, small antenna motions, in the range 4-6 cm peak-to-peak, and short data batches, 0.57 sec or less, yield very powerful spoofing detection tests.

X. DISCUSSION OF SYSTEM PROPERTIES, POTENTIAL ENHANCEMENTS, AND MERITS RELATIVE TO IMU-BASED METHODS

A. Non-Detectable Spoofing Cases

There exist special cases in which some or all of this paper's spoofing detection methods would not work. The basic method relies on geometric diversity of the terms $-\frac{2\pi}{\lambda}(\hat{\boldsymbol{r}}^j)^{\mathrm{T}} A_k^{\mathrm{T}} \boldsymbol{b}_a(\tau_{midk}^j)$ in Eq. (8) for j = 1, …, L for the non-spoofed case as compared to lack of diversity in the term $-\frac{2\pi}{\lambda}(\hat{\boldsymbol{r}}^{sp})^{\mathrm{T}} A^{\mathrm{T}} \boldsymbol{b}_a(\tau_{midk}^j)$ in the spoofed case, Eq. (13). In perverse situations, however, the vectors $\hat{\boldsymbol{r}}^j$ may not have sufficient diversity. Of course, if L = 1, if there is only one available signal, then there is no diversity, and this method fails. Even if L = 2 GNSS satellites, however, the one-dimensional version of this system lacks sufficient diversity. Recall that $\boldsymbol{b}_a(t)$ = $\hat{\boldsymbol{b}}_a \rho_a(t)$ when the articulations are 1-dimensional. In this case, it is possible to find a vector $\hat{\boldsymbol{r}}_a$ = $A^{\mathrm{T}}\hat{\boldsymbol{b}}_a$ that solves the non-spoofed estimation problem in Eqs. (40a)-(40c) to yield a low cost even during a spoofing attack. This solution will satisfy $(\hat{\boldsymbol{r}}^1)^{\mathrm{T}}\hat{\boldsymbol{r}}_a = (\hat{\boldsymbol{r}}^2)^{\mathrm{T}}\hat{\boldsymbol{r}}_a$ by lying in the plane exactly between $\hat{\boldsymbol{r}}^1$ and $\hat{\boldsymbol{r}}^2$. In fact, poor spoofing detection power will occur in any case where there exists the possibility of finding an $\hat{\boldsymbol{r}}_a$ such that all values of $(\hat{\boldsymbol{r}}^j)^{\mathrm{T}}\hat{\boldsymbol{r}}_a$ for j = 1, …, L are equal or nearly so. It is easy to show, however, that any such case yields a very high GDOP, an infinite GDOP if $(\hat{\boldsymbol{r}}^j)^{\mathrm{T}}\hat{\boldsymbol{r}}_a$ for j = 1, …, L can be exactly equal for some choice of $\hat{\boldsymbol{r}}_a$. A very large GDOP, however, would preclude the spoofer from fooling the victim into confidently computing a false position/time solution. Therefore, it is unlikely that a near-infinite GDOP case would occur in practice. Even if a spoofer were to mount such an attack, this paper's spoofing detection algorithm would realize that it was incapable of discerning whether or not an attack was occurring: It would not be able to achieve both a low false-alarm probability and a low probability of missed detection.

B. Advantages of 2D and 3D Antenna Articulations

There are a two important advantages to using a version of this spoofing detection method that employs 2D or full 3D antenna articulations $\boldsymbol{b}_a(t)$. One advantage occurs in the case of a low number of signals. As mentioned in the preceding subsection, spoofing detection will be impossible using this paper's 1-dimensional techniques if L = 2 available GNSS signals or if GDOP is infinite or very large. In the case of 2-dimensional or 3-dimensional antenna articulations, however, it becomes much easier to detect spoofing in these situations.

The enhanced spoofing detection occurs because the detection calculations can estimate individual $\hat{\boldsymbol{b}}^j$ unit direction vectors by solving the problem in Eqs. (102a)-(102c). Without spoofing, the relative directions between the estimated $\hat{\boldsymbol{b}}_{opt}^j$ vectors should be the same as the relative directions between the corresponding known $\hat{\boldsymbol{r}}^j$ vectors, to within the estimation accuracies of the $\hat{\boldsymbol{b}}_{opt}^j$ vectors. The sameness of the relative directions can be explored by comparing dot products between various pairs ($\hat{\boldsymbol{b}}_{opt}^j, \hat{\boldsymbol{b}}_{opt}^l$) the corresponding pairs ($\hat{\boldsymbol{r}}^j, \hat{\boldsymbol{r}}^l$) and by comparing scalar triple products between non-coplanar trios ($\hat{\boldsymbol{b}}_{opt}^j, \hat{\boldsymbol{b}}_{opt}^l, \hat{\boldsymbol{b}}_{opt}^m$) and the corresponding trios ($\hat{\boldsymbol{r}}^j, \hat{\boldsymbol{r}}^l, \hat{\boldsymbol{r}}^m$). These dot products and scalar triple products are directly comparable because they are independent of the unknown coordinate frame rotation that distinguishes $\hat{\boldsymbol{b}}^j$ from its corresponding $\hat{\boldsymbol{r}}^j$. Any significant difference in dot products or scalar triple products indicates a spoofing attack. Using this approach, an attack should be detectable even when L = 2 vectors if $\hat{\boldsymbol{r}}^1$ and $\hat{\boldsymbol{r}}^2$ differ sufficiently in their directions.

The use of 2D and 3D $\boldsymbol{b}_a(t)$ articulations also can help address the problem of partial spoofing, i.e., of spoofing only some signals. In that case, the spoofer would almost certainly have to broadcast its signal from an $\hat{\boldsymbol{r}}^{sp}$ direction which differed from one or more of the spoofed $\hat{\boldsymbol{r}}^j$ directions that the spoofer had implied to the victim. The victim's solution of Eqs. (102a)-(102c) would generate a corresponding $\hat{\boldsymbol{b}}_{opt}^j$ that would equal $A\hat{\boldsymbol{r}}^{sp}$ instead of $A\hat{\boldsymbol{r}}^j$. This difference of directions would be detected in dot-product or scalar-triple-product comparisons that involved $\hat{\boldsymbol{b}}_{opt}^j$ on one side of the calculations and $\hat{\boldsymbol{r}}^j$ on the other side.

C. Impact of Multipath Errors

In theory, carrier-phase multipath has the potential to impact this paper's spoofing detection in a negative manner. It is a well known fact that carrier-phase multipath errors can be on the order of 0.5 cm or more and that they can negatively impact the closely related technology of GNSS-based attitude determination [38]. No explicit analysis has been made of the potential impact of multipath on this system. There is, however, strong experimental evidence that the impacts are manageable.

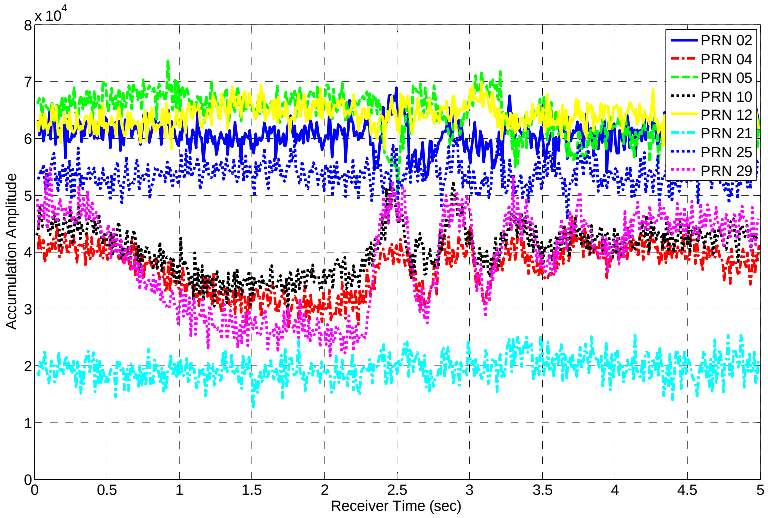

Fig. 11. Experimental evidence of carrier-phase multipath: correlation of accumulation amplitude variations with antenna articulation variations.

In two of the three live-data tests of this system, significant carrier-phase multipath effects have been evident. The two tests in question are the non-spoofed tests in Ithaca, NY and the spoofed and non-spoofed tests at WSMR. The indications of strong carrier-phase multipath consisted of strong variations of the received signal power that were highly correlated with the decaying sinusoidal antenna articulation motions. Such variations are depicted in Fig. 11. This figure plots the amplitude time histories of the GPS receiver's $[I_{pk}; Q_{pk}]$ prompt accumulation vectors that correspond to the detrended carrier phase time histories in Fig. 7. It is clear from the figure that PRNs 04, 10, and 29, the dash-dotted red curve, the dotted black curve, and the dotted magenta curve, all show significant exponential decays that correlate closely with the exponentially decaying carrier phase time histories of Fig. 7. The largest zero-to-peak amplitude variations of the dotted magenta curve equal 30% of its nominal level.

The most reasonable explanation for the amplitude variations in Fig. 11 is that of alternating constructive and destructive interference between the direct signal and a significant multipath signal. One might postulate that variations in antenna gain pattern could have caused these fluctuations. The actual rotations of the antenna gain pattern were small, however, and it is not believable that the resulting gain fluctuations along any fixed line-of-sight could have been large enough to cause that oscillations observed in Fig. 11.

The following fact further supports the multipath explanation for the oscillations in Fig. 11: The anechoic chamber data taken at NASA Wallops displayed no such amplitude oscillations. This is exactly what one would expect if the oscillations were caused by multipath because an anechoic chamber has very low multipath.

One would expect that the corresponding multipath-induced carrier-phase variations would be commensurate in a relative sense. Thus, the peak carrier phase multipath errors for the dotted magenta curve, PRN 29, might be as large as 0.3 rad = 0.048 cycles at the start of the antenna oscillations. Fortunately, this level of multipath error is significantly smaller than the beat carrier phase variations that were caused by the antenna motion. As per Fig. 7, these were about 0.6 cycles peak-to-peak for PRN 29 at the outset of the antenna vibrations.

None of the spoofing detection tests suffered any discernible ill effects from the apparent presence of significant multipath error. All of them produced reasonable detection statistics, as evidenced in Figs. 9 and 10 and in similar figures for other cases.

The only apparent effect of multipath was an error in estimated antenna articulation direction $\hat{\boldsymbol{r}}_{aopt} = \boldsymbol{r}_{aopt}/\left\|\boldsymbol{r}_{aopt}\right\|$. For a non-spoofed test in Ithaca, NY. The prototype antenna articulation system of Fig. 3 had been set up to produce an $\hat{\boldsymbol{r}}_a$ articulation direction that was horizontal. The estimated $\hat{\boldsymbol{r}}_{aopt}$, however, was tilted about 8 deg away from horizontal. This apparent tilt may have been the result of carrier-phase multipath. Fortunately, it did not adversely impact the detection technique's ability to rule out the possibility of a spoofing attack.

D. Possible Improvements to Detect Advanced Spoofing Attacks

This paper's new spoofing detection technique and its associated hypothesis tests make specific assumptions about the spoofer. These assumptions could be violated. Likely violations should be considered in order to develop enhancements to the basic system described here.

Two possible violations to the assumptions of the preceding analysis seem obvious. One is that the spoofer might not spoof all of the GNSS signals. In that case, the spoofed signals would all have identical detrended carrier-phase time history responses to the antenna articulation $\boldsymbol{b}_a(t)$, as in Fig. 8, but the non-spoofed signals would have different responses. This situation has already been observed in one of the spoofed cases from

WSMR. In that case, one signal could not be spoofed because the receiver/spoofer of Refs. 3 and 4 could not receive that particular low-elevation signal in order to know how to spoof it. The fact that this signal was not being spoofed was obvious, partly because it was much weaker than the spoofed signals, but mostly because its detrended carrier phase time history diverged from that of all the other signals. Its signal was not used in the spoofing detection calculation because of this difference.

The obvious upgrade needed to the present spoofing detection system in response to a mixture of spoofed and non-spoofed signals is to allow for multiple spoofed hypotheses in which only certain subsets of the signals are spoofed. Essentially, that upgrade has been implemented "by hand", in the WSMR test noted above. It should not be very difficult to implement some sort of combinatorial analysis of the different possibilities for sets of spoofed and non-spoofed signals and to apply that analysis as an outer loop wrapped around this paper's basic spoofing detection calculations.

Note, however, that spoofing of only a subset of the GNSS signals presents a problem to the spoofer as well. Unless the spoofer is very clever, subset spoofing will lead to pseudorange inconsistencies that are easily detectable by standard RAIM methods. It is not clear how a clever spoofer could spoof only a small subset of the signals, avoid RAIM detection, and still cause the victim to compute an erroneous position or time. If the spoofer were to spoof most of the signals, then the number of combinations of potentially spoofed signals that would need to be analyzed by this paper's techniques would not be very large, and the detection would not be difficult. Of course, this discussion presumes that the present system would be implemented in conjunction with a traditional RAIM detection method based on checking for pseudorange consistency.

A second possible violation of this paper's spoofing detection assumptions is the possibility of the spoofer generating high-frequency dynamic carrier phase variations on the spoofed signals, variations that differ for each GNSS signal and that have frequency content which can pass through the high-pass filter calculations implemented in Eqs. (17) and (18). In effect, the spoofer would vary each if its spoofed $\boldsymbol{r}_k^j$ satellite-to-victim-receiver vectors in Eq. (12) in a high-frequency manner that sought to confuse the spoofing detection calculations. The result would be a modified version of the spoofed carrier-phase model in Eq. (13):

$$\begin{aligned}\phi_k^j \; &\cong -\frac{2\pi}{\lambda}(\hat{\boldsymbol{r}}^{sp})^{\mathrm{T}} A^{\mathrm{T}} \boldsymbol{b}_a(\tau_{midk}^j) + \Delta\phi_{sp}^j(\tau_{midk}^j) \\ &\qquad + \beta_0^j + \beta_1^j(\tau_{midk}^j - \tau_{mid1}^j) \\ &\qquad \tfrac{1}{2}\beta_2^j(\tau_{midk}^j - \tau_{mid1}^j)^2 + n_{\phi k}^j \end{aligned} \qquad (109)$$

where the new component $\Delta\phi_{sp}^j(\tau_{midk}^j)$ would be the high-frequency term. The spoofer's best strategy for avoiding detection would be to make this term equal the difference between the non-spoofed carrier phase in Eq. (9) and the simple spoofed phase in Eq. (13):

$$\Delta\phi_{sp}^j(\tau_{midk}^j) \;=\; -\frac{2\pi}{\lambda}[(\hat{\boldsymbol{r}}^j)^{\mathrm{T}} - (\hat{\boldsymbol{r}}^{sp})^{\mathrm{T}}]A^{\mathrm{T}}\boldsymbol{b}_a(\tau_{midk}^j) \qquad (110)$$

This strategy could be implemented perfectly only if the spoofer knew the antenna articulation motion in the reference coordinates, $A^{\mathrm{T}}\boldsymbol{b}_a(\tau_{midk}^j)$. If the spoofing detection system placed an optically opaque radome over the entire antenna and articulation system, then the spoofer would be prevented from obtaining this information.

In the absence of knowledge of $A^{\mathrm{T}}\boldsymbol{b}_a(\tau_{midk}^j)$, the spoofer would have to guess suitable $\Delta\phi_{sp}^j(\tau_{midk}^j)$ time histories that might serve to confuse the spoofing detection system. If it knew *a priori* the frequency, amplitude, and direction of a sinusoidal $\boldsymbol{b}_a(t)$ articulation time history, then it might try to guess at the time history's phasing and thereby have a chance of accurately reproducing $A^{\mathrm{T}}\boldsymbol{b}_a(\tau_{midk}^j)$. A good choice of $\boldsymbol{b}_a(t)$ for the spoofing detection system, one that randomized its motions at least to the extent of randomizing the phase of sinusoidal oscillations, would neutralize the effectiveness of any attempt to defeat its detection strategy by mimicking $A^{\mathrm{T}}\boldsymbol{b}_a(\tau_{midk}^j)$.

Nevertheless, an improved spoofing detection test might want to consider the possibility of high-frequency $\Delta\phi_{sp}^j(\tau_{midk}^j)$ signals being generated by a spoofer. If the detection system is able to conceal the true $\boldsymbol{b}_a(t)$ from the spoofer, through physical covering and through randomization of the motion, then the principle effect of any $\Delta\phi_{sp}^j(\tau_{midk}^j)$ will be to spread out the spoofed-case probability distribution for the spoofing detection statistic, $p(\gamma|H_1)$. That is, the red/magenta probability distributions in Figs. 5 and 6 and the red and blue probability distributions in Figs. 9 and 10 will be wider. This situation will lead to larger probabilities of missed detection. A careful consideration of possible spoofer strategies for choosing $\Delta\phi_{sp}^j(\tau_{midk}^j)$, especially worst-case strategies, could be used to generate spoofing detection tests that still had reasonably low probabilities of false alarm and missed detection. It is likely that all such tests will still involve consideration of the non-spoofed carrier-phase model in Eq. (10) or similar equations and the posing and solution of non-spoofed estimation problems, as in Eqs. (40a)-(40c) and (66a)-(66c). Although the spoofed carrier phase model will have to be augmented, as in the change from Eq. (13) to Eq. (109), the spoofed-case model will still involve the unknown spoofer direction $\hat{\boldsymbol{r}}^{sp}$ and the unknown vector dot product $(\hat{\boldsymbol{r}}^{sp})^{\mathrm{T}} A^{\mathrm{T}} \hat{\boldsymbol{b}}_a$ or some related quantity. The spoofing detection statistic will probably still involve some sort of optimization in order to account for the parameterized effect on the spoofed carrier phases of the unknown spoofer direction.

The main difference for the detector in the case of spoofer-generated $\Delta\phi_{sp}^{j}(\tau_{midk}^{j})$ signals is that the carrier-phase-sameness paradigm for the spoofed case, as illustrated in Fig. 8, will no longer apply. There will still be a portion of the spoofed carrier-phase variations that is the same for all spoofed signals. It will still be correlated to the antenna articulation motions $\boldsymbol{b}_a(t)$, but there will be another component that varies between signals. The spoofing detection will rely on the fact that these differences will not be correlated to the $\boldsymbol{b}_a(t)$ variations, in distinction to the differences that exist in the non-spoofed case. Straightforward enhancements to the present methods can be used to mechanize the posing and answering of the one important question: Do the correlations between the measured beat carrier-phase variations and the known $\boldsymbol{b}_a(t)$ variations indicate real GNSS signals or a spoofing attack?

E. Merits in Comparison to Existing IMU-Aided Spoofing Detection Approaches

The system developed in the present paper has some similarities to IMU-based methods, such as those described in Refs. 21 and 22, but it has several advantages over such methods. First, it can be implemented in a fixed-base installation by adding a device to create the required $\boldsymbol{b}_a(t)$ motions and to sense them, e.g., a solenoid and a linear encoder.

A second improvement is a difference from IMU-based methods' presumption that some sort of navigation filter, perhaps an extended Kalman filter, is estimating the vehicle position and attitude. IMU-based spoofing detection methods rely on this navigation filter's estimated direction cosines matrix A. The present method forms its own independent estimate of A or of $\hat{\boldsymbol{r}}_a = A^{\mathrm{T}}\hat{\boldsymbol{b}}_a$ in a globally convergent manner. There is no possibility that failure or inaccuracy of a full navigation filter could deteriorate its performance.

A third advantage of the new detection approach lies in the design of its test statistic. IMU-based approaches tend to rely on a general residuals test in the navigation filter. In the present context, this amounts to considering only whether a cost such as $J_{nonsp}(\hat{\boldsymbol{r}}_a)$ in Eq. (40b) is small enough. The present method also seeks to exploit the fact of sameness in the $\boldsymbol{b}_a(t)$-correlated parts of the carrier phase variations during a spoofing attack. Minimization of the cost function in Eq. (21) represents an example of this approach. By considering both $J_{nonsp}(\hat{\boldsymbol{r}}_{aopt})$ from Eq. (40b) and $J_{sp}(\eta_{opt})$ from Eq. (21), the spoofing detection power of any given test can be increased relative to a test that considers only the residual errors relative to a non-spoofed signal model. Also, there appears to be little or no literature for the IMU-based approaches that discusses how to design a spoofing detection threshold for a given probability of false alarm, how to compute the corresponding probability of missed detection, or how much motion and time are needed to achieve reasonably low probabilities of false alarm and missed detection.

Another advantage of the present system is that it could be used on an UAV without the need for any inertial measurements. Rather than using an IMU to infer antenna motions $\boldsymbol{b}_a(t)$, a system based on the new approach could use high-frequency dithering of one or more UAV control inputs in order to create a suitable $\boldsymbol{b}_a(t)$. Given known control input dithering signals, $\boldsymbol{b}_a(t)$ could be inferred from the transfer functions of a dynamic model of the UAV. This could be especially effective if the GNSS antenna were mounted near a wing tip and if the aileron input were the dithered control. Alternatively, the antenna could be mounted on the tail, and the elevator could be dithered. It is likely that an unknown scaling factor a would have to multiply a known nominal $\boldsymbol{b}_{anom}(t)$ in order to model the true $\boldsymbol{b}_a(t)$, but this type of re-scaling approach is already covered in Section VI.

Yet another advantage over IMU-based methods concerns the particular carrier phase measurement that gets used. A tightly coupled GPS/IMU system feeds the GPS observables, including pseudorange and possibly beat carrier phase, into the Kalman filter. This is the type of system envisioned in Refs. 21 and 22. Unfortunately, the beat carrier phase used is usually that produced by the carrier NCO. The special processing of I_{pk} and Q_{pk} accumulations associated with Fig. 4 and Eq. (3) is not used. Therefore, the finite bandwidth of the PLL can degrade the ability of this system to discern the high-frequency carrier-phase variations, the ones whose differences between the non-spoofed and spoofed cases are central to spoofing detection. In addition, the ability to detect and remove cycle slips, as outlined in Subsection III.A, can be important to the success of carrier-phase-based spoofing detection when high-frequency antenna motions are used. Thus, it is unclear that a tightly coupled GPS/IMU system could be relied on to produce the most useful beat carrier phase information for purposes of spoofing detection.

An ultra-tightly-coupled GPS/IMU system should have none of these difficulties due to its use of the raw I_{pk} and Q_{pk} accumulations as its Kalman filter observables. The processing suggested in Refs. 21 and 22 and similar proposals, however, does not envision using an ultra-tightly-coupled GPS/IMU system for spoofing detection.

One more advantage of the present method is its reduced susceptibility to a very sophisticated spoofing attack. In theory, a sophisticated spoofer could aim a high-bandwidth relative position sensor at a victim UAV's GNSS antenna. It could sense the high-frequency component of the actual antenna motions and use that data to synthesize the equivalent of the $\Delta\phi_{sp}^{j}(\tau_{midk}^{j})$ spoofing signal given in Eq. (110). It would only need to synthesize the correct $\Delta\phi_{sp}^{j}(\tau_{midk}^{j})$ in the bandwidth that was above the effective drift bandwidth of the IMU. Below that bandwidth, it could spoof the signal at will. Such an attack would go completely undetected by any IMU-based single-antenna system. If the present approach were used with concealed $\boldsymbol{b}_a(t)$ motions, as under an optically opaque radome, then this new approach would not have the same vulnerability.

Of course, if an IMU were present on a UAV, its outputs could be used to aid in the determination of the high-frequency components of $\boldsymbol{b}_a(t)$. Such an approach would not need to run the IMU data through a full navigation filter in order to do GNSS spoofing detection. The high-pass pre-filtering calculations of Eqs. (17) and (18) and the attitude estimation calculations in, for example, Eqs. (40a)-(40c) or (99a)-(99c) would obviate the need for data from a full navigation solution.

XI. SUMMARY AND CONCLUSIONS

This paper has developed, analyzed, and investigated a new method to detect spoofing of GNSS signals. It relies on measurements of the beat carrier phase of multiple GNSS signals and on the impact on these measurements that is caused by intentional high-frequency antenna motion. Dithering motion of a victim receiver's antenna could be implemented by a solenoid, a cantilevered beam, or dithering of the controls of a UAV. After detrending of the beat carrier phase variations using a high-pass filter, they can be matched to models of their expected dependence on the known antenna motion. The model for the non-spoofed case shows differing effects of the antenna motion on the signals, but the spoofed case yields identical effects due to spoofing geometry in which all of the false signals originate from a single spoofer transmission antenna. Spoofing detection hypothesis tests have been developed by comparing the two models' ability to fit the measured data. Some of these tests involve auxiliary estimation of attitude or attitude-like parameters of the user system in lieu of *a priori* attitude information. Precise detection tests have been developed with spoofing detection thresholds that respect upper limits on probabilities of false alarm or on worst-case probabilities of false alarm. These tests also allow analysis to determine probabilities of missed detection or worst-case probabilities of missed detection.

The new GNSS spoofing detection techniques have been tested both with Monte-Carlo simulations and with live data. One set of live-data tests evaluated the new techniques against a new sophisticated type of receiver/spoofer, one that mimics all visible signals in a way which foils standard receiver autonomous integrity monitoring techniques. These tests were part of a specially authorized event run at the White Sands Missile Range in New Mexico under the auspices of the Department of Homeland Security. The new spoofing detection methods consistently yield false alarm probabilities and missed detection probabilities on the order of 10^{-5} or lower when working with typical numbers of GPS signals available at typical patch-antenna signal strengths. The needed antenna articulation peak-to-peak deflections are modest, on the order of 4-6 cm. The tests at White Sands Missile Range constitute the first known demonstration of practical detection of live-signal spoofing attacks mounted against a civilian GNSS receiver by a dangerous new generation of receiver/spoofers.

ACKNOWLEDGEMENTS

The authors thank the following people and organizations for their contributions to this effort: The NASA Wallops Flight Facility provided access to their anechoic chamber. Robert Miceli helped with data collection at that facility. Dr. John Merrill and the Department of Homeland Security arranged the live-signal spoofing tests. The U.S. Air Force 746 Test Squadron hosted the live-signal spoofing tests at White Sands Missile Range. Prof. Todd Humphreys and members of his UT Austin Radionavigation Laboratory provided live-signal spoofing broadcasts from their latest receiver/spoofer.

REFERENCES

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

[2] Scott, L., "Location Assurance," *GPS World*, Vol. 18, No. 7, July 2007, pp. 14-18.

[3] Humphreys, T.E., Ledvina, B.M., Psiaki, M.L., O'Hanlon, B., and Kintner, P.M., Jr., "Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer," *Proc. ION GNSS 2008*, Sept. 16-19, 2008, Savannah, GA.

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

[5] Anon., "Global Positioning System Wing (GPSW) Systems Engineering & Integration," Interface Specification IS-GPS-200, Revision E (IS-GPS-200E), Science Applications International Corporation, El Segundo, CA, June 2010.

[6] Rawnsley, A., "Iran's Alleged Drone Hack: Tough, but Possible," *Wired*, available online at http://www.wired.com/dangerroom/2011/12/iran-drone-hack-gps/, Dec. 2011.

[7] Warwick, G., "Civil UAVs Need GPS Anti-Spoofing, But Who Pays," Aviation Week & Space Technology, available online at http://www.aviationweek.com/Blogs.aspx?plckBlogId=Blog:27ec4a53-dcc8-42d0-bd3a-01329aef79a7&plckPostId=Blog%3A27ec4a53-dcc8-42d0-bd3a-01329aef79a7Post%3A4861b58f-7472-47a7-8da7-8bb968fc3af3, July 2012.

[8] Brown, R.G., "Receiver Autonomous Integrity Monitoring," in *Global Positioning System: Theory and Applications, Vol. II*, B.W. Parkinson and J.J. Spilker, Jr., eds., American Institute of Aeronautics and Astronautics, (Washington, 1996), pp. 143-165.

[9] Dovis, F., Chen, X., Cavaleri, A., Ali, K., and Pini, M., "Detection of Spoofing Threats by Means of Signal Parameters Estimation," *Proc. ION GNSS 2011*, Sept. 20-23, 2011, Portland, OR, pp. 416-421.

[10] Pini, M., Fantino, M., Cavaleri, A., Ugazio, S., and Lo Presti, L., "Signal Quality Monitoring Applied to Spoofing Detection," *Proc. ION GNSS 2011*, Sept. 20-23, 2011, Portland, OR, pp. 1888-1896.

[11] Wesson, K.D., Shepard, D.P., Bhatti, J.A., and Humphreys, T.E., "An Evaluation of the Vestigial Signal Defense for Civil GPS Anti-Spoofing," *Proc. ION GNSS 2011*, Sept. 20-23, 2011, Portland, OR, pp. 2646-2656.

[12] Lo, S., De Lorenzo, D., Enge, P., Akos, D., and Bradley, P., "Signal Authentication, A Secure Civil GNSS for Today," *Inside GNSS*, Vol. 4, No. 5, Sept./Oct. 2009, pp. 30-39.

[13] Levin, P., De Lorenzo, D.S., Enge, P.K., and Lo, S.C., "Authenticating a Signal Based on an Unknown Component Thereof," U.S. Patent No. 7,969,354 B2, June 2011.

[14] Psiaki, M.L., O'Hanlon, B.W., Bhatti, J.A., Shepard, D.P., and Humphreys, T.E., "Civilian GPS Spoofing Detection based on Dual-Receiver Correlation of Military Signals," *Proc. ION GNSS 2011*, Sept. 20-23, 2011, Portland, OR, pp. 2619-2645.

[15] Psiaki, M.L., O'Hanlon, B.W., Bhatti, J.A., Shepard, D.P., and Humphreys, T.E., "GPS Spoofing Detection via Dual-Receiver Correlation of Military Signals," to appear in the *IEEE Transactions on Aerospace and Electronic* Systems.

[16] Scott, L., "Anti-Spoofing and Authenticated Signal Architectures for Civil Navigation Systems," *Proc. ION GPS/GNSS 2003*, Sept. 9-11, 2003, Portland, OR, pp. 1543-1552.

[17] Wesson, K., Rothlisberger, M., and Humphreys, T., "Practical Cryptographic Civil GPS Signal Authentication," to appear in *Navigation* (Currently available online at http://radionavlab.ae.utexas.edu/images/stories/files/papers/nma.pdf).

[18] Hartman, R.G., "Spoofing Detection System for a Satellite Positioning System," U.S. Patent No. 5,557,284, Sept. 1996.

[19] 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, March/April 2009, pp. 40–46.

[20] Meurer, M., Konovaltsev, A., Cuntz, M., and Rippl, M., "Robust Joint Multi-Antenna Spoofing Detection and Attitude Estimation by Direction Assisted Multiple Hypotheses RAIM," *Proc. ION GNSS 2012*, Sept. 18-21, 2012, Nashville, TN.

[21] Strachan, V.F., "Signal Inconsistency Detection of Spoofing," U.S. Patent No. 7,450,060 B2, Nov. 2008.

[22] Strachan, V.F., "Signal Inconsistency Detection of Spoofing," U.S. Patent No. 7,564,401 B1, July 2009.

[23] Nielsen, J., Broumandan, A., and Lachapelle, G., "GNSS Spoofing Detection for Single Antenna Handheld Receivers," Navigation, Vol. 58, No. 4, Winter 2011, pp. 335-344.

[24] Nielsen, J., Broumandan, A., and Lachapelle, G., "Method and System for Detecting GNSS Spoofing Signals," U.S. Patent No. 7,952,519 B1, May 2011.

[25] Daneshmand, S., Jafarnia-Jahromi, A., Broumandan, A., and Lachapelle, G. "Low Complexity Spoofing Mitigation," *GPS World*, Vol. 22, No. 12, Dec. 2012, pp. 44-46.

[26] Humphreys, T.E., "Detection Strategy for Cryptographic GNSS Anti-Spoofing," to appear in *IEEE Transactions on Aerospace and Electronic Systems* (Currently available online at http://radionavlab.ae.utexas.edu/images/stories/files/papers/ds.pdf).

[27] Psiaki, M.L., "Attitude Sensing Using a Global-Positioning-System Antenna on a Turntable," *Journal of Guidance, Control, and Dynamics*, Vol. 24, No. 3, May-June 2001, pp. 474-481.

[28] Jung, H., Psiaki, M.L., Scott, W.J., and Boitnott, C.L., "Attitude Sensing Using a GPS Antenna on a Turntable, Experimental Tests," *Navigation*, Vol. 51, No. 3, Fall 2004, pp. 221-229.

[29] Misra, P., and Enge, P. *Global Positioning System, Signals, Measurements, and Performance, 2nd Ed.*, Ganga-Jamuna Press, (Lincoln, MA, 2006), pp. 199-213, 238-241, 467-498.

[30] Psiaki, M.L., and Mohiuddin, S., "Modeling, Analysis, and Simulation of GPS Carrier Phase for Spacecraft Relative Navigation," *Journal of Guidance, Control, and Dynamics*, Vol. 30, No. 6, Nov.-Dec. 2007, pp. 1628-1639.

[31] Gill, P.E., Murray, W., and Wright, M.H., *Practical Optimization*, Academic Press, (New York, 1981), pp. 37-40, 71-82, 105-115, 167-175, 233-251.

[32] Poor, H.V., *An Introduction to Signal Detection and Estimation*, Springer-Verlag, (New York, 1988), pp. 7-195.

[33] Psiaki, M.L., and Hinks, J.C., "Numerical Solution of a Generalized Wahba Problem for a Spinning Spacecraft," *Journal of Guidance, Control, and Dynamics*, Vol. 35, No. 3, May-June 2012, pp. 764-773.

[34] Fletcher, R., *Practical Methods of Optimization*, J. Wiley & Sons, (New York, 1987), pp. 95-107, 195-201.

[35] Bar-Shalom, Y., Li, X.-R., and Kirubarajan, T., *Estimation with Applications to Tracking and Navigation*, J. Wiley & Sons, (New York, 2001), pp. 109-113.

[36] Wertz, J.R. ed., *Spacecraft Attitude Determination and Control*, D. Reidel Pub. Co., (Boston, 1978), pp. 414-416, 426-428.

[37] Wahba, G., "A Least Squares Estimate of Satellite Attitude," *SIAM Review*, Vol. 7, No. 3, 1965, p. 409.

[38] Cohen, C.E., "Attitude Determination," in *Global Positioning System: Theory and Applications, Vol. II*, B. W. Parkinson and J. J. Spilker, Jr., eds., American Institute of Aeronautics and Astronautics, (Washington, 1996), pp. 519-538.