Received: 30 December 2022 | Revised: 8 September 2023 | Accepted: 15 September 2023

DOI: 10.33012/navi.629

ORIGINAL ARTICLE

Optimal INS Monitor for GNSS Spoofer Tracking Error Detection

Birendra Kujur | **Samer Khanafseh** | **Boris Pervan**

Mechanical, Materials and Aerospace Engineering Department, Illinois Institute of Technology, Illinois, USA

Correspondence
Birendra Kujur
10 W 32nd St., Chicago, IL, 60616.
Email: bkujur@hawk.iit.edu

Abstract

In this article, we describe a new method for detecting global navigation satellite system (GNSS) spoofing using an inertial navigation system. We specifically address the most difficult-to-detect scenario, in which a spoofer replicates the authentic GNSS signal with only additive errors due to the spoofer's uncertainty in knowledge of the target's position. We derive an optimal monitor to detect the anomalous temporal structure of the spoofed measurements caused by the spoofer's target tracking errors. This new monitor uses accumulated Kalman filter innovations projected into the position state domain. We demonstrate how the monitor window length can be set to achieve any required missed detection probability, and we evaluate the performance of the monitor for both white and colored tracking error. Finally, we present a complementary solution separation monitoring concept to detect rapid-onset spoofing and to achieve protection levels in real time.

Keywords

aircraft tracking error, GNSS, GNSS spoofing, INS, solution separation

1 | INTRODUCTION

The civil infrastructures behind safety-critical applications in aviation, maritime, and terrestrial navigation rely heavily on global navigation satellite systems (GNSSs). The civil GNSS signal structures are publicly known and vulnerable to spoofing attacks, which endangers public safety (Humphreys et al., 2008). In an attack, the spoofer feeds a counterfeit signal to the targeted user to cause faulty position or time estimates. Various spoofing attack methods and respective defense techniques have been summarized by Jafarnia-Jahromi et al. (2012b), Gunther (2014), Psiaki & Humphreys (2016), and Fernández-Hernández et al. (2019). Spoofing signals can be created in several ways, for example, by transmitting self-consistent synthetic GNSS signals using a GNSS simulator, by meaconing (i.e., recording authentic GNSS signals and rebroadcasting them with a delay), or by recording and replaying authentic signals with altered navigation data, among others. Spoofed signals can be sent to target receivers via a single transmit antenna or an array of multiple antennas, static or mobile, to mimic the satellite line-of-sight geometries. A spoofer may choose to initially send the counterfeit signals at a lower power than the authentic signals and then slowly increase the power to cause the

target receiver's tracking loops to transition from the authentic to the spoofed signals and to then slowly drag the user along a false trajectory. A spoofer can also opt to jam the GNSS signals before transmitting the spoofed signal. A more sophisticated spoofer could send two spoofed signals, where one of the spoofed signals would be in opposite phase to the authentic signals, causing cancellation. In this process, known as nulling, the target receiver would not even be able to detect multiple correlation peaks. Ideally, spoofing detection techniques should protect against all possible scenarios.

Potential detection techniques include signal-processing methods, such as power and distortion monitoring (Turner et al., 2020; Wesson et al., 2018), cryptographic authentication (Kerns, Wesson, et al., 2014; Wesson et al., 2011), correlation comparison with encrypted authentic signals (O'Hanlon et al., 2013), correlation peak comparison within a receiver (Rothmaier et al., 2021b), combining different observables (Broumandan et al., 2020; Rothmaier et al., 2021a), use of multiple receivers (Stenberg et al., 2020), spoofing discrimination using spatial processing by antenna arrays (Nielsen et al., 2014), GNSS signal direction of arrival comparison (Meurer et al., 2012), code and phase rate consistency checks (Moshavi, 1996), high-frequency antenna motion (Psiaki et al., 2013), automatic gain control schemes (Akos, 2012), and signal power monitoring techniques (Jafarnia-Jahromi et al., 2012a). Some of these methods are indeed effective, but they have various computational, logistical, and physical limitations. Augmenting data from auxiliary sensors such as inertial measurement units (IMUs), barometric altimeters, and independent radar sensors to discriminate spoofing has also been proposed (Kerns, Shepard, et al., 2014; Lo et al., 2017; Swaszek et al., 2016).

Our group introduced the first stochastic description and quantification of the performance of an IMU-based GNSS spoofing monitor against worst-case "faults" (i.e., spoofing inputs over time) (Khanafseh et al., 2014; Tanil, Khanafseh, et al., 2018; Tanil et al., 2015a, 2015b; Tanil, Khanafseh, et al., 2016; Tanil et al., 2017). We specifically investigated anti-spoofing solutions utilizing IMUs because essentially all modern aircraft are equipped with IMUs, thereby requiring minimal additional cost or system modification. An IMU is naturally immune to external interference, which makes it an excellent resource for ensuring navigation continuity. Additionally, when used in the navigation solution in various integration schemes with GNSS (uncoupled or loosely, tightly, or ultra-tightly coupled), the INS provides the redundancy needed to resist spoofing attacks. In our prior work (Tanil, Khanafseh, et al., 2018; Tanil et al., 2017), we developed a chi-squared innovation sequence detector to monitor the accumulated time history of normalized Kalman filter (KF) innovations. The two main advantages of this cumulative innovation (CI) sequence monitor are that innovations are already available in the KF, such that little additional computation is required for the monitor implementation, and that it provides detection capability against slowly growing faults. We evaluated the performance of the CI monitor against worst-case GNSS fault profiles both analytically and experimentally (Tanil, Jimenez, et al., 2018; Tanil, Khanafseh, et al., 2018). The worst-case fault here represents a spoofed GNSS signal profile that maximizes integrity risk. We also analyzed the sensitivity of the CI monitor against error modeling uncertainties in the INS/GNSS KF structure (Kujur et al., 2019).

However, post-detection *recovery* has not been addressed in previous work—the difficulty being that the KF is already corrupted once spoofing is detected. Moreover, previous performance evaluations assumed that the CI monitor started at spoofing onset and operated without a defined run time. Finally, the CI monitor did not provide the means to produce a protection level—i.e., a position-domain containment boundary corresponding to the maximum acceptable level of integrity

risk. To address these critical limitations, in this paper, we introduce a new type of CI monitor: a cumulative *position-domain* innovation (CPI) monitor that detects spoofing by accumulating the target position tracking error embedded in the spoofer's signal. We also present a complementary solution separation (SS) concept to produce protection levels and provide a means for post-detection recovery.

Section 2 provides useful background information on the original CI monitor. Section 3 introduces the new CPI monitor. An example application with quantitative results is presented in Section 4. In Section 5, we present the complementary SS monitor. Finally, we summarize our work in Section 6. We also provide relevant derivations in the appendices.

2 | KF STATE MODEL

We consider a vehicle employing INS and GNSS sensors integrated with a KF to estimate its position, velocity, and attitude. The dynamics of the INS/GNSS system, augmented as needed with sensor error state dynamics, are linearized to obtain the process model utilized in the KF:

$$\mathbf{x}_{k+1} = \mathbf{\Phi}_k \mathbf{x}_k + \mathbf{\Gamma}_{w_k} \mathbf{w}_k \tag{1}$$

where $\mathbf{x}_k$ is the state vector, $\mathbf{\Phi}_k$ is the state transition matrix, $\mathbf{\Gamma}_{w_k}$ is the process noise model matrix, and $\mathbf{w}_k$ is the additive white process noise with a respective covariance matrix $\mathbf{Q}_k$. The measurement model is as follows:

$$\mathbf{z}_k = \mathbf{H}_k \mathbf{x}_k + \boldsymbol{\nu}_k \tag{2}$$

where $\mathbf{H}_k$ is the observation matrix and $\boldsymbol{\nu}_k$ is the measurement noise with a respective covariance matrix $\mathbf{V}_k$.

The innovation vector γ_k at time epoch k is defined as follows:

$$\gamma_k = \mathbf{z}_k - \mathbf{H}_k \bar{\mathbf{x}}_k \tag{3}$$

where $\bar{\mathbf{x}}$ is the state vector estimate prior to the measurement update at time epoch k. The CI detector is a chi-squared monitor that utilizes the cumulative normalized innovations from a KF as the test statistic and compares this test statistic against a threshold. A cumulative test statistic q_N at time epoch N is the sum of squares of the normalized innovation vectors over time, given as follows:

$$q_N = \sum_{k=1}^{N} \gamma_k^T \mathbf{S}_k^{-1} \gamma_k \tag{4}$$

where $\mathbf{S}_k = \mathbf{H}_k \bar{\mathbf{P}}_k \mathbf{H}_k^T + \mathbf{V}_k$ is the innovation vector covariance matrix at time epoch k and $\bar{\mathbf{P}}_k$ is the estimate error covariance matrix prior to the measurement update at time epoch k. The monitor simply checks whether the test statistic q_N is smaller than a predefined threshold T_N^2. For a given false alarm requirement under fault-free conditions, the threshold T_N is determined from the inverse chi-squared cumulative distribution function (CDF) with N degrees of freedom. The monitor produces an alarm if $q_N > T_N$.

One of the major limitations of the CI monitor is that it does not offer a means for post-detection recovery because there is no fault-free source upon which to rely. Another unaddressed issue concerns the monitor start and run times. In all

prior performance evaluations, it was assumed that the monitor start time (conveniently) coincided with the spoofing onset time, and no guidance was provided to determine how long the monitor should run before resetting. In the next section, we introduce the CPI monitor and show that it directly addresses the run time issue and also provides superior detection performance relative to the CI monitor for *any* run time. The start time and recovery are addressed afterward.

3 | CPI MONITOR

3.1 | Spoofer's Tracking Error

The initial objective of a smart spoofer is to cause the target receiver to lose lock of the authentic GNSS signals and lock onto the counterfeit signals without being detected. This initial lock transition is crucial because any abrupt changes during the process would be easily detectable, sabotaging the spoofer's plan. The best way for a spoofer to cause the target to switch the counterfeit signal without being detected is to initially replicate the authentic signals at lower power and then slowly increase the power to cause the target receiver to transition. If successful, the spoofer would then attempt to inject small but accumulating position and/or time offsets in an attempt to slowly pull the target away along the desired spoofed trajectory while remaining undetected.

To deliver a replica of the authentic signal to the target, the spoofer would need to know the position of the target's GNSS antenna during the attempted takeover. Consequently, the spoofer would need to track the target in real time. Any tracking errors would ultimately be embedded in the replica signal and appear to the target as additional "noise" in the received GNSS signals. As tracking errors are inevitable, detecting the presence of such unusual noise would expose active spoofing. This is true even during the initial takeover phase when the spoofer has not yet injected any additional offsets to the spoofed signals. In the remainder of this paper, we address this case specifically, as any additional offsets to the spoofing profile are irrelevant to the monitor. The spoofer's uncertainty of the target position will simply be referred to as "tracking error" in the remainder of the paper. In Appendix C, we show that the tracking error appears in the spoofed measurements as an additive term, and the measurement equation can be represented as follows:

$$\mathbf{z}_k^s = \mathbf{z}_k + \mathbf{H}_k \boldsymbol{\nu}_k^t \tag{5}$$

where $\mathbf{z}_k^s$ is the spoofed measurement vector, $\mathbf{z}_k$ is the "true" (unspoofed) measurement vector, $\mathbf{H}_k$ is the observation matrix that maps the tracking error to the range domain, and $\boldsymbol{\nu}_k^t$ is an $n \times 1$ column vector of tracking error, with n being the number of states. The superscript s indicates "spoofed."

We can observe these tracking errors in the KF innovation vector because it extracts the difference between the GNSS measurements and the predicted measurements of the process model from the INS. We will see later that even small deviations over time are readily observable when the INS is used because of the precision of GNSS carrier phase measurements.

Because the innovation vector $\boldsymbol{\gamma}_k$ in Equation (3) is constructed from the entire measurement vector $\mathbf{z}_k$ and the entire state vector $\bar{\mathbf{x}}_k$, the effect of the position tracking errors, our proxy for spoofing, will not be the only contributor to $\boldsymbol{\gamma}_k$. A more direct way to observe the effect of the tracking errors would be to project the innovation vector into the position domain.

3.2 | Neyman–Pearson Optimal and Sufficient Test Statistic

We desire to find a test statistic to maximize the probability of detection for a given false alarm rate. The Neyman–Pearson lemma (Neyman & Pearson, 1933) provides the solution to this problem: given two mutually exclusive hypotheses H_0 and H_1, which for some observation x have conditional probability densities $p_0(x\,|\,H_0)$ and $p_1(x\,|\,H_1)$, the likelihood ratio is the optimal test statistic. The likelihood ratio is defined as follows:

$$\Lambda(x)=\frac{p_1(x\,|\,H_1)}{p_0(x\,|\,H_0)} \tag{6}$$

Our two hypotheses are the fault-free case, which has no tracking error, and the spoofed case, in which the tracking error appears in the innovation vector. As a starting point, we model the tracking error v_k^t as white Gaussian noise (WGN) distributed as $\mathcal{N}(0,\sigma_t^2)$, where σ_t^2 is the *unknown* variance of the tracking error.

We consider the innovation vector distributions with and without the tracking error for our likelihood ratio test. The fault-free innovation vector distribution at any time k is given as $H_0:\boldsymbol{\gamma}_k\sim\mathcal{N}(0,\mathbf{S}_k)$, whereas the spoofed innovation vector distribution, as shown in Appendix C, is given as $H_1:\boldsymbol{\gamma}_k\sim\mathcal{N}(0,\mathbf{S}_k+\mathbf{H}_k\mathbf{R}\mathbf{H}_k^T)$, where $\mathbf{R}=\mathbf{u}\mathbf{u}^T\sigma_t$ and $\mathbf{u}$ is a unit vector in an arbitrary spatial direction in which the tracking error exists. The innovation vectors are mutually independent over time under H_0. In principle, the vectors can also be modeled as independent under H_1 given that a "high-quality" IMU is being utilized because $\bar{\mathbf{x}}_k$ in Equation (2) would be relatively unaffected by the spoofer's tracking error if a high-quality IMU were used. (Note: We refer to IMUs with specifications equivalent to or better than the navigation-grade IMU listed in Appendix F as "high-quality" and IMUs with specifications equivalent to or lesser than the automotive-grade IMU listed in Appendix F as "low-quality/grade.") We accept this assumption as true in the following derivation of the optimal test statistic, and in Appendix D, we show that this assumption is valid even for small tracking errors and "low-grade" IMUs.

Using Equation (6) and given an arbitrary threshold $\lambda(N)$ for independent innovations $\boldsymbol{\gamma}_k(k=1,\ldots,N)$, the likelihood ratio test can be expressed as follows (Kay, 1998):

$$\Lambda(\boldsymbol{\gamma}_1,\boldsymbol{\gamma}_2,\ldots,\boldsymbol{\gamma}_N)=C_1(N)\frac{\exp\left(-\frac{1}{2}\sum_{k=1}^{N}\boldsymbol{\gamma}_k^T\left(\mathbf{S}_k+\mathbf{H}_k\mathbf{R}\mathbf{H}_k^T\right)^{-1}\boldsymbol{\gamma}_k\right)}{\exp\left(-\frac{1}{2}\sum_{k=1}^{N}\boldsymbol{\gamma}_k^T\mathbf{S}_k^{-1}\boldsymbol{\gamma}_k\right)}\underset{H_0}{\overset{H_1}{\gtrless}}\lambda(N) \tag{7}$$

where:

$$C_1(N)=\prod_{k=1}^{N}\left(\frac{|\mathbf{S}_k|}{|\mathbf{S}_k+\mathbf{H}_k\mathbf{R}\mathbf{H}_k^T|}\right)^{k/2} \tag{8}$$

captures the terms that do not depend on $\boldsymbol{\gamma}_k(k=1,\ldots,N)$. Taking the natural log of both sides and collecting all of the constant terms on the right, we obtain the following:

$$\sum_{k=1}^{N}\left[\boldsymbol{\gamma}_k^T\mathbf{S}_k^{-1}\boldsymbol{\gamma}_k-\boldsymbol{\gamma}_k^T\left(\mathbf{S}_k+\mathbf{H}_k\mathbf{R}\mathbf{H}_k^T\right)^{-1}\boldsymbol{\gamma}_k\right]\underset{H_0}{\overset{H_1}{\gtrless}}2\left[\ln\lambda(N)-\ln C_1(N)\right] \tag{9}$$

Moreover, because the matrices $\mathbf{S}_k$ and $\mathbf{S}_k + \mathbf{H}_k\mathbf{R}\mathbf{H}_k^T$ are non-singular, we can write the following (Miller, 1981):

$$\left(\mathbf{S}_k + \mathbf{H}_k\mathbf{R}\mathbf{H}_k^T\right)^{-1} = \mathbf{S}_k^{-1} - \frac{\mathbf{S}_k^{-1}\mathbf{H}_k\mathbf{R}\mathbf{H}_k^T\mathbf{S}_k^{-1}}{\mathrm{tr}\left(\mathbf{H}_k\mathbf{R}\mathbf{H}_k^T\mathbf{S}_k^{-1}\right)} \tag{10}$$

Substituting Equation (10) into Equation (9), we obtain the following relation:

$$\sum_{k=1}^{N}\boldsymbol{\gamma}_k^T\left[\mathbf{S}_k^{-1} - \mathbf{S}_k^{-1} + \frac{\mathbf{S}_k^{-1}\mathbf{H}_k\mathbf{R}\mathbf{H}_k^T\mathbf{S}_k^{-1}}{\mathrm{tr}\left(\mathbf{H}_k\mathbf{R}\mathbf{H}_k^T\mathbf{S}_k^{-1}\right)}\right]\boldsymbol{\gamma}_k \underset{H_0}{\overset{H_1}{\gtrless}} C_2(N) \tag{11}$$

where the constant on the right side is as follows:

$$C_2(N) = 2\left[\ln\lambda(N) - \ln C_1(N)\right] \tag{12}$$

For short periods of time, matrices $\mathbf{H}$ and $\mathbf{S}$ can be assumed to be time-invariant; thus, the term $\mathrm{tr}\left(\mathbf{H}_k\mathbf{R}\mathbf{H}_k^T\mathbf{S}_k^{-1}\right)$ can be moved to the right side of Equation (11). Equation (11) then reduces as follows:

$$\sum_{k=1}^{N}\boldsymbol{\gamma}_k^T\left[\mathbf{S}^{-1}\mathbf{H}\mathbf{R}\mathbf{H}^T\mathbf{S}^{-1}\right]\boldsymbol{\gamma}_k \underset{H_0}{\overset{H_1}{\gtrless}} C_3(N) \tag{13}$$

where:

$$C_3(N) = C_2(N)\ \mathrm{tr}(\mathbf{H}\mathbf{R}\mathbf{H}^T\mathbf{S}^{-1}) \tag{14}$$

Recalling that $\mathbf{R} = \mathbf{u}\mathbf{u}^T\sigma_t$, we substitute this term into Equation (13) to obtain the following:

$$\sum_{k=1}^{N}\boldsymbol{\gamma}_k^T\left[\mathbf{S}^{-1}\mathbf{H}\mathbf{u}\mathbf{u}^T\sigma_t\mathbf{H}^T\mathbf{S}^{-1}\right]\boldsymbol{\gamma}_k \underset{H_0}{\overset{H_1}{\gtrless}} C_3(N) \tag{15}$$

Rearranging the terms of Equation (15) and noting that $\mathbf{S}^{-1}$ is symmetric, we can now write the following relation:

$$\sum_{k=1}^{N}\left(\mathbf{u}^T\mathbf{H}^T\mathbf{S}^{-1}\boldsymbol{\gamma}_k\right)^T\left(\mathbf{u}^T\mathbf{H}^T\mathbf{S}^{-1}\boldsymbol{\gamma}_k\right) \underset{H_0}{\overset{H_1}{\gtrless}} C_4(N) \tag{16}$$

where we have defined $C_4(N) = C_3(N)/\sigma_t$.

Finally, we introduce the following *scalar* projection of the innovation vector:

$$\gamma_k^u = \mathbf{u}^T\mathbf{H}^T\mathbf{S}^{-1}\boldsymbol{\gamma}_k \tag{17}$$

which is a weighted projection of the innovation vector into the position-domain direction $\mathbf{u}$, the tracking error direction under consideration. Therefore, the optimal test statistic is given as follows:

$$q_N^u = \sum_{k=1}^{N}(\gamma_k^u)^2 \tag{18}$$

which we call the CPI. We note that q_N^u does not require a knowledge of σ_t.

3.3 | Position-Domain Innovation

Under spoof-free conditions, the scalar position-domain innovation in Equation (17) is distributed as follows:

$$\gamma_k^u \sim \mathcal{N}(0, \mathbf{u}^T\mathbf{H}^T\mathbf{S}^{-1}\mathbf{H}\mathbf{u}) \tag{19}$$

To simplify the notation, we define the variance as follows:

$$\sigma^2_{\gamma_k^u} = \mathbf{u}^T\mathbf{H}^T\mathbf{S}^{-1}\mathbf{H}\mathbf{u} \tag{20}$$

When the spoofer sends a signal mimicking the authentic signal with some inherent additive tracking error, the latter can be observed in the position-domain innovation. In Appendix C, we show that the innovation for the spoofed case with tracking error for an arbitrary spatial direction $\mathbf{u}$ is given by the following:

$$\boldsymbol{\gamma}_k^s = \boldsymbol{\gamma}_k + \mathbf{H}\mathbf{u}\nu_k^t \tag{21}$$

Substituting Equation (21) for $\boldsymbol{\gamma}_k$ in Equation (17), we obtain the spoofed position-domain innovation:

$$\gamma_k^{us} = \mathbf{u}^T\mathbf{H}^T\mathbf{S}^{-1}(\boldsymbol{\gamma}_k + \mathbf{H}\nu_k^t) = \gamma_k^u + \mathbf{u}^T\mathbf{H}^T\mathbf{S}^{-1}\mathbf{H}\mathbf{u}\nu_k^t \tag{22}$$

The mean of γ_k^{us} is again zero, but the variance is now as follows:

$$\mathbb{E}\left[(\gamma_k^{us})^2\right] = \mathbf{u}^T\mathbf{H}^T\mathbf{S}^{-1}\mathbf{H}\mathbf{u} + (\mathbf{u}^T\mathbf{H}^T\mathbf{S}^{-1}\mathbf{H}\mathbf{u})\left(\mathbf{u}^T\mathbf{H}^T\mathbf{S}^{-1}\mathbf{H}\mathbf{u}\right)^T\sigma_t^2 \tag{23}$$

This can be written more compactly using Equation (20):

$$\mathbb{E}\left[(\gamma_k^{us})^2\right] = \sigma^2_{\gamma_k^{us}} = \sigma^2_{\gamma_k^u} + \sigma^4_{\gamma_k^u}\sigma_t^2 \tag{24}$$

Thus, under spoofed conditions, the position-domain innovation has the following distribution:

$$\gamma_k^{us} \sim \mathcal{N}(0, \sigma^2_{\gamma_k^u} + \sigma^4_{\gamma_k^u}\sigma_t^2) \tag{25}$$

For notational simplicity, we also define the following:

$$\sigma^2_{\Delta\gamma_k^{us}} = \sigma^4_{\gamma_k^u}\sigma_t^2 \tag{26}$$

The tracking error affects the position-domain innovation by increasing its variance without changing the mean (which remains zero).

Now, we can write the position-domain innovation before and after spoofing, respectively, as follows:

$$\gamma_k^u \sim \mathcal{N}\left(0, \sigma^2_{\gamma_k^u}\right) \tag{27}$$

$$\gamma_k^{us} \sim \mathcal{N}\left(0, \sigma^2_{\gamma_k^u} + \sigma^2_{\Delta\gamma_k^{us}}\right) \tag{28}$$

When normalized by $\sigma_{\gamma_k^u}$, the position-domain innovation is distributed in the unspoofed case as follows:

$$\frac{\gamma_k^u}{\sigma_{\gamma_k^u}} \sim \mathcal{N}(0,1) \tag{29}$$

In the spoofed case, the position-domain innovation is distributed as follows:

$$\frac{\gamma_k^{us}}{\sigma_{\gamma_k^u}} \sim \mathcal{N}\left(0, 1+\sigma^2_{\Delta\gamma_k^{us}}/\sigma^2_{\gamma_k^u}\right) \tag{30}$$

3.4 | Sum of Squares of Normalized Position-Domain Innovations

The square of a scalar normal random variable distributed as $\mathcal{N}(0,\sigma^2)$ follows the Gamma distribution $\Gamma\left(\frac{1}{2}, 2\sigma^2\right)$ (Mathai & Provost, 1992). The Gamma distribution $\Gamma(\alpha,\theta)$ is defined by its shape parameter α and scale parameter θ. Therefore, we can write the distribution of the square of the normalized position-domain innovation in the unspoofed case as follows:

$$\left(\frac{\gamma_k^u}{\sigma_{\gamma_k^u}}\right)^2 \sim \Gamma\left(\frac{1}{2}, 2\right) \tag{31}$$

In the spoofed case, we obtain the following:

$$\left(\frac{\gamma_k^{us}}{\sigma_{\gamma_k^u}}\right)^2 \sim \Gamma\left(\frac{1}{2}, 2\left(1+\sigma^2_{\Delta\gamma_k^{us}}/\sigma^2_{\gamma_k^u}\right)\right) \tag{32}$$

For a period of accumulation N, following the results in Sections 3.2 and 3.3, we define our optimal CPI test statistic (in the unspoofed case) as follows:

$$q_N^u = \sum_{k=1}^{N}\left(\frac{\gamma_k^u}{\sigma_{\gamma_k^u}}\right)^2 \tag{33}$$

We note that the sum of independent Gamma-distributed random variables is also Gamma-distributed (Mathai & Provost, 1992). We assume that the change in variance of the position-domain innovations is negligible over the accumulation period, i.e., $\sigma_{\gamma^u} = \sigma_{\gamma_1^u} = \sigma_{\gamma_2^u} = \ldots = \sigma_{\gamma_N^u}$ and $\sigma_{\Delta\gamma^{us}} = \sigma_{\Delta\gamma_1^{us}} = \sigma_{\Delta\gamma_2^{us}} = \ldots = \sigma_{\Delta\gamma_N^{us}}$. The test statistic in the unspoofed case q_N is then Gamma-distributed as follows:

$$q_N^u \sim \Gamma\left(\sum_{k=1}^{N}\frac{1}{2}, 2\right) = \Gamma\left(\frac{N}{2}, 2\right) \tag{34}$$

For a given probability of false alarm P_{FA}, we can determine the threshold as follows:

$$T_N = F_\Gamma^{-1}\left(P_{FA}\middle|\frac{N}{2}, 2\right) \tag{35}$$

where F_Γ^{-1} is the inverse CDF of the Gamma distribution.

In the spoofed case, with the tracking error embedded in the test statistic, we have the following:

$$q_N^{us} = \sum_{k=1}^{N}\left(\frac{\gamma_k^{us}}{\sigma_{\gamma^u}}\right)^2 \sim \Gamma\left(\sum_{k=1}^{N}\frac{1}{2}, 2\left(1+\frac{\sigma^2_{\Delta\gamma^{us}}}{\sigma^2_{\gamma^u}}\right)\right) \tag{36}$$

By defining the ratio $\Omega = (\sigma_{\Delta\gamma^{us}} / \sigma_{\gamma^u})^2$, we can rewrite the above equation as follows:

$$q_N^{us} \sim \mathbb{\Gamma}\left(\frac{N}{2}, 2\left(1+\Omega\right)\right) \tag{37}$$

From Equations (34) and (37), we can see that tracking error causes the scale parameter of the test statistic distribution to change but does not affect the shape parameter, which remains the same as in the unspoofed distribution. The probability of missed detection (i.e., of not detecting the tracking error) is as follows:

$$P_{MD} = \gamma\left(\frac{N}{2}, \frac{T_N}{2(1+\Omega)}\right) \Big/ \Gamma\left(\frac{N}{2}\right) \tag{38}$$

where T_N is the threshold, as defined in Equation (35), $\gamma(a, b)$ is the lower incomplete Gamma function:

$$\gamma(a, b) = \int_0^b t^{a-1} e^{-t} dt \tag{39}$$

and $\Gamma(a)$ is the Gamma function: $\Gamma(a) = \gamma(a, \infty)$.

3.5 | Gaussian Approximation

For a Gamma distribution with shape parameter α and scale parameter θ, the mean and variance are $\alpha\theta$ and $\alpha\theta^2$, respectively. To determine how the tracking error helps with detection, we take the large-N approximation for a Gamma distribution:

$$\mathbb{\Gamma}(\alpha, \theta) \approx \mathcal{N}(\alpha\theta, \alpha\theta^2) \tag{40}$$

Thus, the distributions of q_N^u and q_N^{us} can be approximated for large N, respectively, as follows:

$$q_N^u \sim \mathcal{N}\left(N, 2N\right) \tag{41}$$

$$q_N^{us} \sim \mathcal{N}\left(N\left(1+\Omega\right), 2N\left(1+\Omega\right)^2\right) \tag{42}$$

We now introduce a modified test statistic:

$$\tilde{q}_N^{(\cdot)} = \frac{q_N^{(\cdot)} - N}{\sqrt{2N}} \tag{43}$$

The unspoofed distribution of this new test statistic is as follows:

$$\tilde{q}_N^u \sim \mathcal{N}(0, 1) \tag{44}$$

The spoofed test statistic distribution is given as the following:

$$\tilde{q}_N^{us} \sim \mathcal{N}\left(\sqrt{\frac{N}{2}}\Omega, (1+\Omega)^2\right) \tag{45}$$

It is clear from the preceding two equations that the accumulated tracking error causes the mean of the test statistic distribution to grow as N increases while the variance of the distribution remains independent of N.

3.6 | Tracking Error as Colored Noise

In the development thus far, for clarity, we have assumed that the tracking error is WGN. However, it is possible that the tracking sensor error could be time-correlated or even that the spoofer would choose to filter the tracking sensor output to try to smooth out the errors to lower the possibility of detection.

To analyze the performance of the CPI monitor, we need to determine the distribution of the test statistic in the case of colored tracking error. We model the tracking error as a zero-mean first-order Gauss–Markov random process (GMRP) with time constant τ_t and variance σ_t^2. To the spoofer's advantage, we ignore any time delays that might be incurred in the filtering process.

Although the CPI monitor operates sequentially in time, to analyze the monitor performance, it is more convenient to use a batch method for quadratic forms of random variables, as described by Mathai & Provost (1992). Let X be an $N\times 1$ random vector distributed as $X\sim\mathcal{N}(0,\Sigma)$ and A be an arbitrary $N\times N$ symmetric matrix. Then, the quadratic form $Q(X)=X^TAX$ can be expressed as a linear combination of independent central chi-squared variables Y:

$$Q(X)=X^TAX=\sum_{j=1}^{N}\lambda_j Y_j^2 \tag{46}$$

where $\lambda_1,\lambda_2,\lambda_3,...,\lambda_N$ are the eigenvalues of $\Sigma^{1/2}A\Sigma^{1/2}$, $Z=\Sigma^{-1/2}X$, $Y=P^TZ$, and P is the orthonormal matrix of eigenvectors of $\Sigma^{1/2}A\Sigma^{1/2}$.

We can now express the cumulative position-domain innovation from time 1 to N in terms of X, with Σ defined as follows:

$$\Sigma=\mathbf{I}\sigma^2_{\gamma^u}+\begin{bmatrix} 1 & e^{\frac{-\Delta t}{\tau_t}} & \cdots & e^{\frac{-(N-1)\Delta t}{\tau_t}} \\ e^{\frac{-\Delta t}{\tau_t}} & 1 & \ddots & \vdots \\ \vdots & \ddots & 1 & e^{\frac{-\Delta t}{\tau_t}} \\ e^{\frac{-(N-1)\Delta t}{\tau_t}} & \cdots & e^{\frac{-\Delta t}{\tau_t}} & 1 \end{bmatrix}\sigma^2_{\Delta\gamma^{us}} \tag{47}$$

and matrix $\mathbf{A}$ defined as follows:

$$\mathbf{A}=\mathbf{I}/\sigma^2_{\gamma^u} \tag{48}$$

making $Q(X)$ the sum of the squares of the normalized position-domain innovations, which is our CPI test statistic defined in Equation (36). For authentic signals, only the first term in Equation (47) exists because the innovations under normal conditions are white (and $\sigma^2_{\Delta\gamma^{us}}=0$). In the case of spoofing, $Q(X)$ includes colored noise, and in light of Equation (46), it will have a generalized chi-squared distribution, whose CDF can be evaluated using the method described by Das & Geisler (2016).

4 | QUANTITATIVE RESULTS

We first performed en route simulations of an aircraft utilizing a navigation-grade IMU (Appendix F) and single-frequency Global Positioning System (GPS) measurements. The aircraft level flight was simulated to start from 41°50'10" N, 87°37'30" W with a cruising speed of 454 knots at an altitude of 40,000 ft. The GNSS measurements were generated using the GPS constellation (SC-159, 2020). The error models for the GPS measurements are defined in Appendix A, and the IMUs are listed in Appendix F. The spoofer tracks the aircraft, with errors, to generate and broadcast counterfeit spoofed signals. The simulated spoofed signals are exact replicas of the authentic signals with either additive zero-mean WGN or zero-mean colored noise modeled as a first-order GMRP. In this example, we used a maximum monitor run time of 180 s, a GPS update frequency of 2 Hz (i.e., $N \leq 360$), and a false alarm requirement of 10^{-5}. Although tracking errors would exist in all three spatial dimensions, we conservatively assumed that the errors are only in the vertical direction and ignore any errors in the other two directions in the analysis. Figure 1 (left) shows the results of the simulation run with the tracking error modeled as WGN with standard deviation $\sigma_t = 2$ cm. The superior performance of the CPI monitor relative to the CI monitor is plainly evident in this simple example. Figure 1 (right) also illustrates the performance of the CPI monitor for WGN tracking errors with larger magnitudes.

The results of the direct simulations are instructive; however, such simulations are an unfeasible means for computing missed detection probabilities. Instead, we turn to Equation (38) to quantify the analytical relationship between monitor run time N, WGN tracking error standard deviation σ_t, and probability of missed detection P_{MD}. The results, for the same en route aircraft scenario, in Figure 2 show that the missed detection probability decreases with increasing run time as more tracking errors are accumulated over time and shift the mean of the test statistic distribution, as predicted in Equation (42). Similarly, an increasing tracking error magnitude (standard deviation) contributes to a shift in the mean of the test statistic, which reduces P_{MD}. Figure 3 shows two-dimensional cuts of Figure 2 for different tracking error variances and monitor run times.

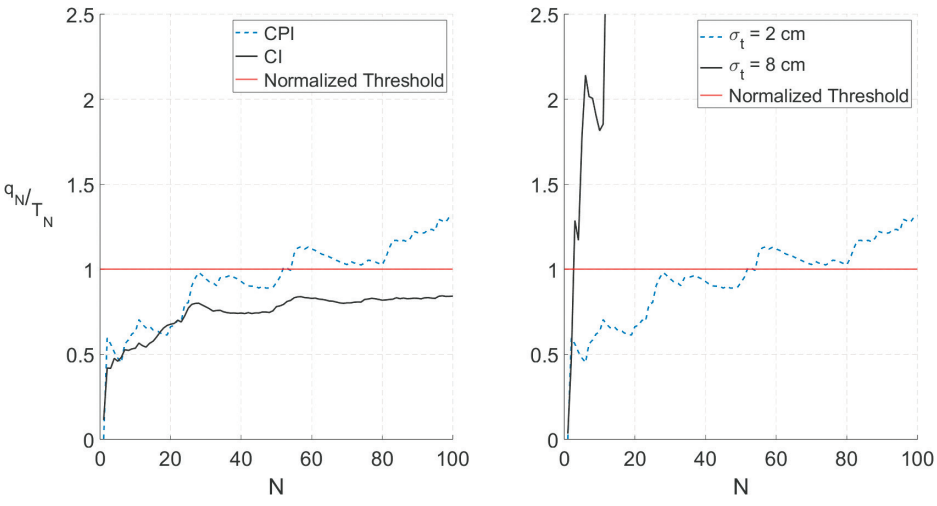

FIGURE 1 Performance of the CPI monitor versus the CI monitor for $\sigma_t = 2$ cm (left) and for two different tracking error magnitudes (right)

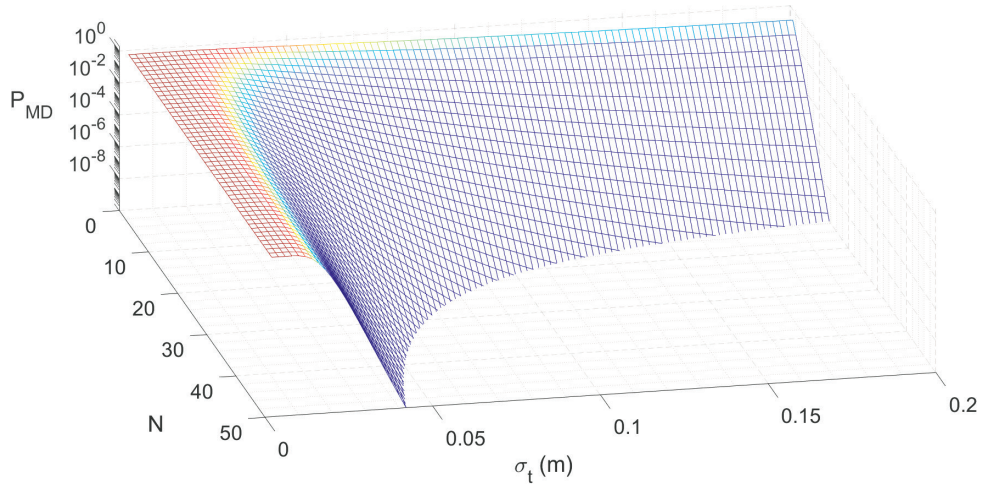

FIGURE 2 CPI probability of missed detection P_{MD} versus tracking error σ_t and monitor run time N

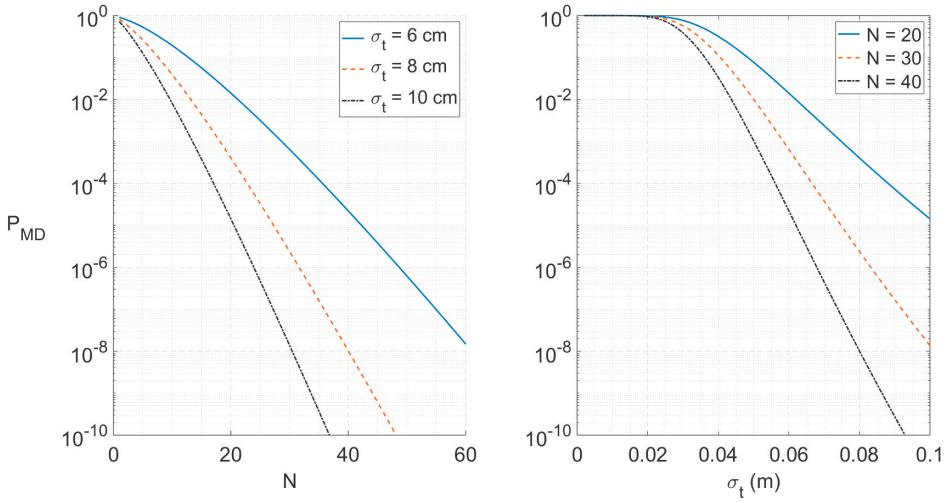

FIGURE 3 CPI probability cuts of missed detection P_{MD} versus monitor run time N and tracking error σ_t

For comparison, we computed the missed detection probabilities for different grades of IMUs. Figure 4 shows the variation in the probability of missed detection as a function of monitor run time N for different IMU grades. The WGN tracking error standard deviation for this example was 10 cm. The figure shows that, even with a relatively low-grade (automotive) IMU, the degradation in monitor performance is negligible.

The sensitivity of the CPI monitor to tracking error can be attributed to the precision of GPS carrier phase measurements and the IMU's accelerometer quality, specifically the velocity random walk (VRW). If tracking errors are smaller in magnitude than the relative position errors obtainable from time-differenced carrier phase measurements, the monitor threshold will be too loose to reliably detect a tracking error. Similarly, if the VRW is large, then the position estimate drift prior to the GPS measurement update will be greater than the impact of the tracking error on the measurement itself. Figure 5 illustrates this case by comparing the performance of the CPI monitor in a low-tracking-error scenario, $\sigma_t = 2$ cm, for different IMU grades against a "lousy" IMU with a VRW 100 times greater than

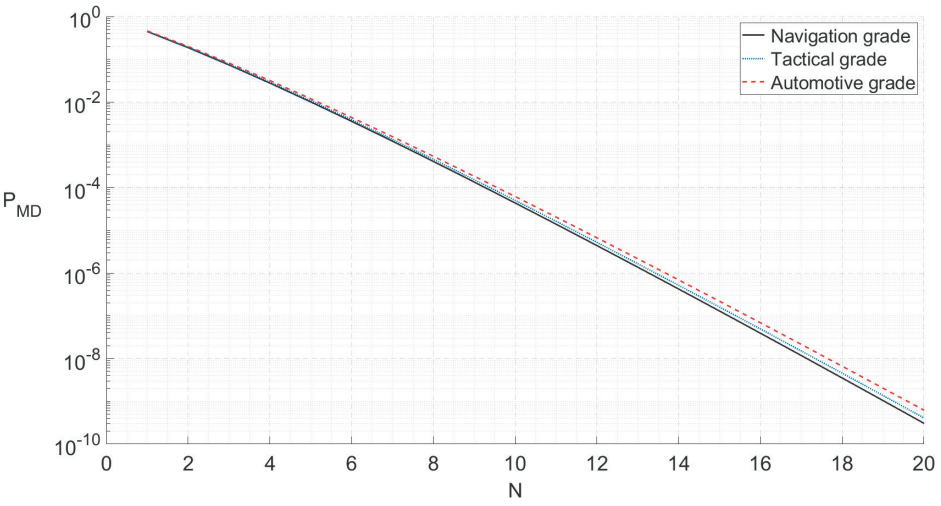

FIGURE 4 Probability of missed detection P_{MD} versus monitor run time (N) for different IMU grades, with $\sigma_t = 10$ cm

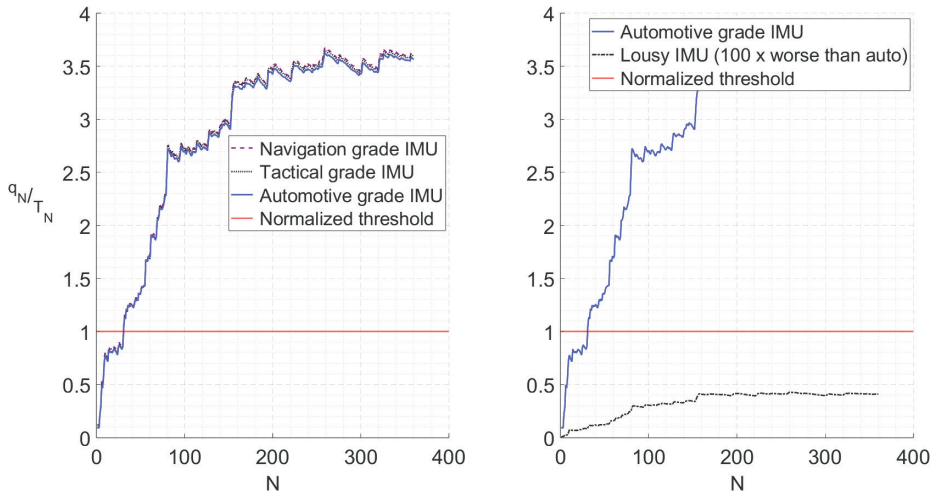

FIGURE 5 CPI monitor performance with $\sigma_t = 2$ cm for navigation-, tactical-, and automotive-grade IMUs (left) and automotive versus "lousy" IMUs (right)

that of an automotive-grade IMU. The reason that the automotive-grade IMU performs so well is that the accelerometer noise parameters are comparable to those of higher-grade IMUs. The latter are designed primarily to improve gyroscope bias stability, which is a critical performance parameter for controlling drift over longer time periods—significantly longer than those relevant to the spoofing monitor.

We now turn our attention to quantifying the performance of the monitor in the presence of time-correlated (colored) tracking error, coming either from the sensor itself or as a result of filtering of white sensor output by the spoofer. Figure 7 presents example tracking errors over time with the same standard deviation, but different time constants, including WGN. Using the method described in Section 3.6, we obtain the performance results in Figure 6, which show that time-correlated tracking error would help the spoofer remain undetected for longer, with larger filter time constants leading to a higher probability of missed detection.

We also evaluated the monitor performance for different start times during a standard 24-h period (SC-159, 2020) to evaluate the monitor sensitivity to different

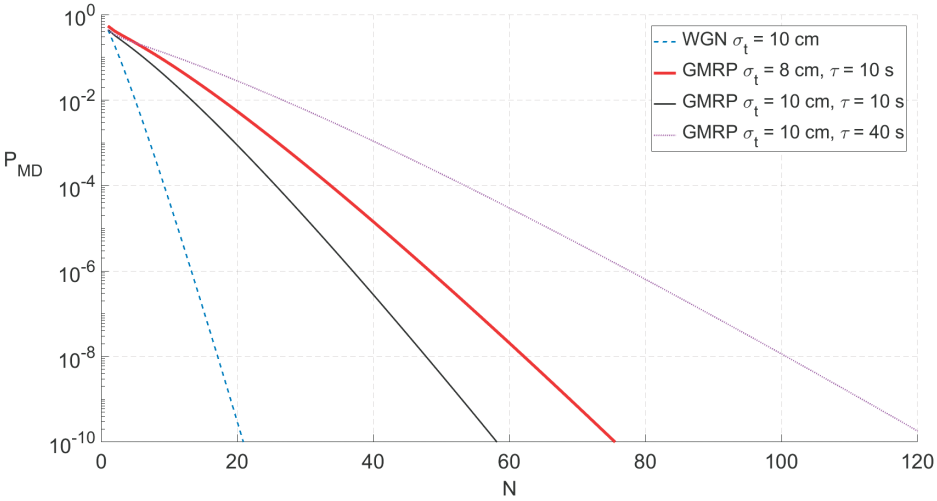

FIGURE 6 Probability of missed detection P_{MD} versus monitor run time N for WGN and colored noise tracking error
The sample interval is 2 Hz; thus, $N = 1$ corresponds to 0.5 s.

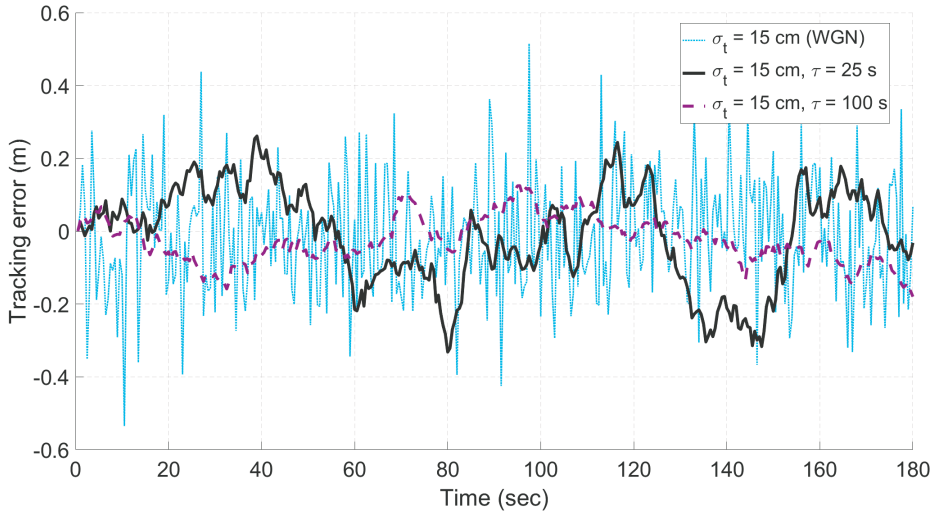

FIGURE 7 Illustration of tracking error versus time for white and colored noise processes

satellite geometries. Figure 8 shows the probability of missed detection versus monitor run time for tracking error modeled as WGN with a standard deviation of 10 cm, with 24 curves representing the performance results at 1-h intervals. It is evident that the monitor is effective over the entire day, although there is obviously some variation in performance with satellite geometry.

These results demonstrate that if a CPI monitor is implemented, the conjecture that INS-based spoofing detection is vulnerable to slowly deviating counterfeit signals can be largely dismissed. The results show that the spoofer's target tracking error should be easily detectable as long as the duration of spoofing lasts exceeds a minimum time defined by the variance and time constant of the tracking error. For the example application considered, Figure 6 shows that even for tracking error standard deviations as small as 10 cm and correlation time constants as large as 40 s, the probability of missed detection is negligible after less than 1 min. We have also experimentally validated the INS monitor, as reported by Kujur et al. (2023), using real GNSS and INS data.

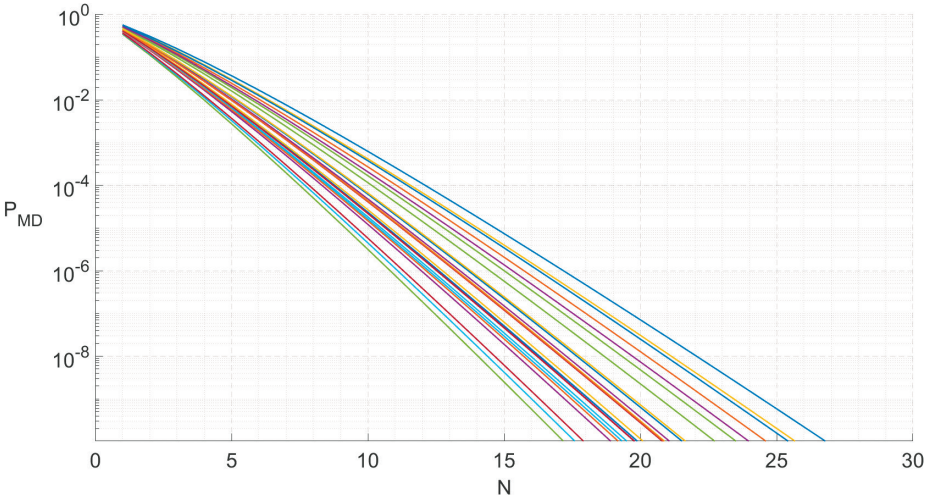

FIGURE 8 Probability of missed detection (P_{MD}) versus monitor run time (N) for different satellite geometries

The CPI monitor has the notable limitation that P_{MD}—or equivalently, a position-domain protection level—is difficult, if not impossible, to establish in real time. Thus, the CPI monitor performance must be evaluated in advance by simulation over a wide variety of satellite geometries and tracking error characteristics—for example, by following a more extensive version of the evaluation presented in this paper for the specific GNSS/INS integration and application considered. In the following section, we introduce a complementary SS monitor concept to ensure the detection of faster-onset spoofing, provide the means to produce protection levels in real time, and allow the navigation function to default to INS-only coasting to preserve continuity (at lower accuracy levels as the INS drifts over time).

5 | SS MONITOR WITH SEQUENTIAL WINDOWS

The SS monitor measures the difference in position solutions between the potentially spoofed integrated INS/GNSS KF output $\hat{\mathbf{x}}_{KF_k}$ and an ostensibly clean "coasting" INS-only solution $\bar{\mathbf{x}}_{C_k}$. The test statistic at any time k is defined as follows:

$$q_{SS_k} = \mathbf{u}^T(\hat{\mathbf{x}}_{KF_k} - \bar{\mathbf{x}}_{C_k}) \tag{49}$$

The variance for the test statistic is given by the following:

$$\sigma^2_{SS_k} = \mathbf{u}^T(\bar{\mathbf{P}}_{C_k} - \hat{\mathbf{P}}_{KF_k})\mathbf{u} \tag{50}$$

where $\hat{\mathbf{P}}_{KF_k}$ and $\bar{\mathbf{P}}_{C_k}$ are the estimate error covariance matrices for $\hat{\mathbf{x}}_{KF_k}$ and $\bar{\mathbf{x}}_{C_k}$, respectively. The derivation of Equation (50) is provided in Appendix E. The detection threshold for the test statistic can be obtained given a desired false alert requirement and inverse CDF of $\mathcal{N}(0, \sigma^2_{SS_k})$. After a detection, if the INS coasting solution is known to be unaffected by earlier spoofing, navigation can continue by switching from $\hat{\mathbf{x}}_{KF_k}$ to $\bar{\mathbf{x}}_{C_k}$.

Because the SS monitor observes the instantaneous error between the tightly coupled INS/GNSS KF position solution and INS-only coasting solution and because the coasting covariance $\bar{\mathbf{P}}_c$ drifts over time, the detection threshold must

continually increase to maintain a constant false alert probability. Thus, as the coasting window length increases, the SS spoofing detection performance will degrade, allowing slowly growing faults to go undetected. While this is obviously not a desirable performance characteristic, it is precisely over these increasing time windows that the CPI monitor will perform the best. Therefore, given the complementary nature of the two monitors, it is natural to consider running them in parallel, where the CPI monitor would detect slowly growing spoofing profiles and the SS would detect more rapidly growing faults.

For the CPI monitor, a minimum window length N_{min} is required to achieve a desired P_{MD_+}. Here, the subscript "+" designates the missed detection (integrity risk) requirement allocation for spoofing attacks lasting *longer* than N_{min}. The CPI monitor threshold would be obtained by using the false alert (continuity risk) allocation for the monitor, P_{FA_+}. For shorter attack windows, the SS monitor would provide the means for detection with the allocated missed detection and false alert probabilities, P_{MD_-} and P_{FA_-}. Obviously, the sum of the two missed detection probabilities must be smaller than the total integrity risk allocated to undetected spoofing. The same is true for the sum of the two false alert probabilities relative to the total continuity risk allocated to spoofing monitoring.

The SS monitor can provide a protection level for spoofing in the spatial direction $\mathbf{u}$ as follows:

$$PL_k^u = k_{FA_-}\sigma_{SS_k} + k_{MD_-}\sigma_{C_k} \tag{51}$$

where:

$$\sigma_{C_k}^2 = \mathbf{u}^T \bar{\mathbf{P}}_{C_k} \mathbf{u} \tag{52}$$

and the multipliers k_{FA_-} and k_{MD_-} are determined from the SS false alert and missed detection requirement probability allocations. The SS detection threshold is $k_{FA_-}\sigma_{SS_k}$. The protection level will increase with the SS window length because of the growth in σ_{C_k} over time.

The minimum run length N_{min} for the CPI monitor sets the upper limit on the SS monitor time window. The combined monitor system is implemented using consecutive fixed-length windows of length N_{min} (Figure 9) with an SS monitor initialized at the beginning of each window and terminated at the end of each window. A new SS monitor window is opened at each new GNSS measurement epoch and closed N_{min} epochs later. Figure 9 illustrates this idea, showing the (conceptual) protection level. Because each window has its own INS-only solution (from the SS monitor), if spoofing is detected in a particular window at time t_d, the final INS/GNSS KF solution and associated PL from a prior window closed (without detection) any time before t_d can be safely used to initialize subsequent fault-free coasting.

At any given time point, a set number of monitor windows will be running, and the false alert requirement allocation for each monitor can be equally divided among these monitor windows to determine the thresholds for each. This approach is conservative, as the test statistics for the different monitors will be correlated, but it is easy to implement.

The maximum protection level produced by any SS monitor will occur at the end of the window, $k = N_{min}$, because the INS coasting errors, σ_{C_k}, will be the largest at that point.

The value of N_{min} is determined by the CPI monitor performance. For the same example GPS/INS implementation and satellite geometry considered in Figure 6, Figure 10 shows the values of N_{min} for different tracking error magnitudes with

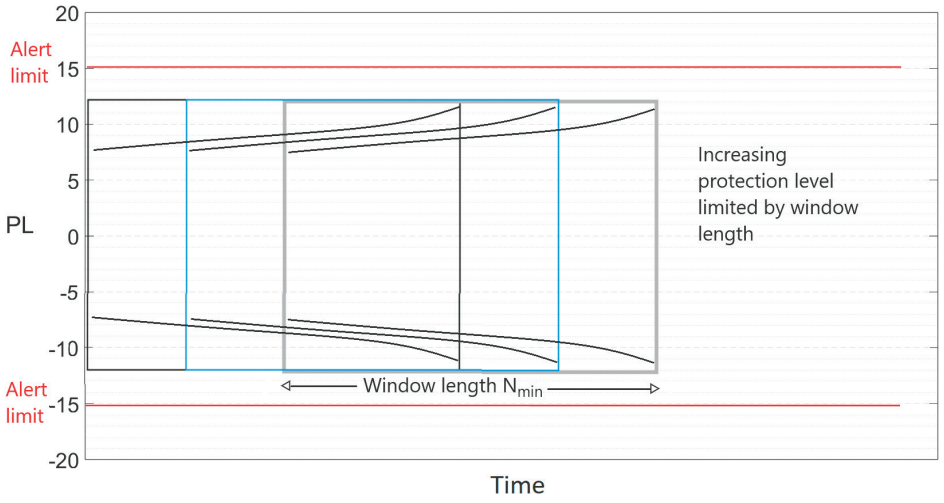

FIGURE 9 Illustration of SS sequential monitor windows with increasing protection level (PL)

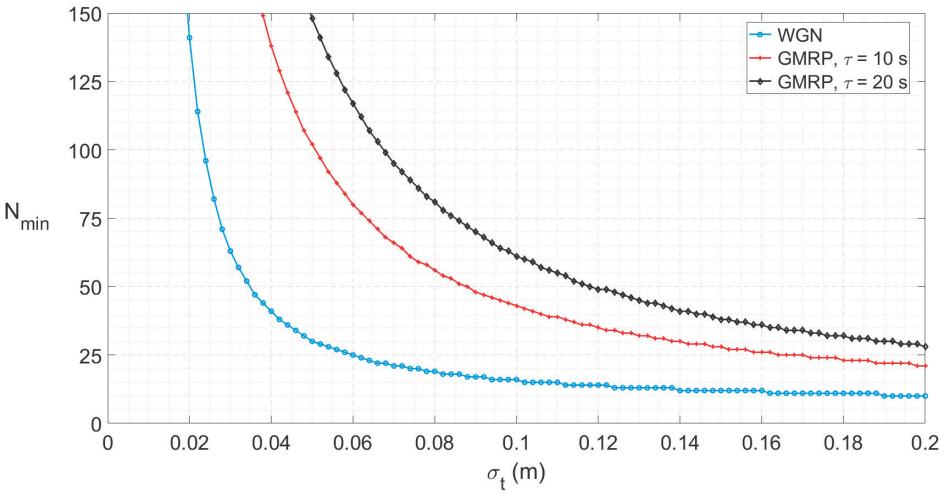

FIGURE 10 Minimum detection window (N_{min}) versus tracking error magnitude for an example satellite geometry

the missed detection requirement set to 10^{-7}. As in Figure 6, it is clear that colored tracking error takes longer to detect than white noise. Using these values of N_{min}, we can now determine the maximum protection levels. Figure 11 shows the results for a false alarm requirement of 10^{-5} and missed detection requirement of 10^{-6}, based on Equation (51). Again, it is clear that the WGN tracking error allows for tighter protection levels compared with colored noise. The large SS protection levels at small values of tracking error σ_t are due to correspondingly large values of N_{min}, which, in turn, lead to large coasting errors σ_{C_k} (with $k = N_{min}$). For colored noise, a shorter time constant provides a tighter protection level. Moreover, it can be seen that for a decimeter-level tracking error magnitude, the maximum protection level converges regardless of whether the tracking error is time-correlated.

When implemented together, the CPI and SS monitors address all of the limitations of the original CI monitor reported by Tanil et al. (2017), Tanil, Khanafseh, et al. (2018), Tanil, Jimenez, et al. (2018), and Kujur et al. (2019). The CPI monitor performs better than the CI monitor because its test statistic is optimized to

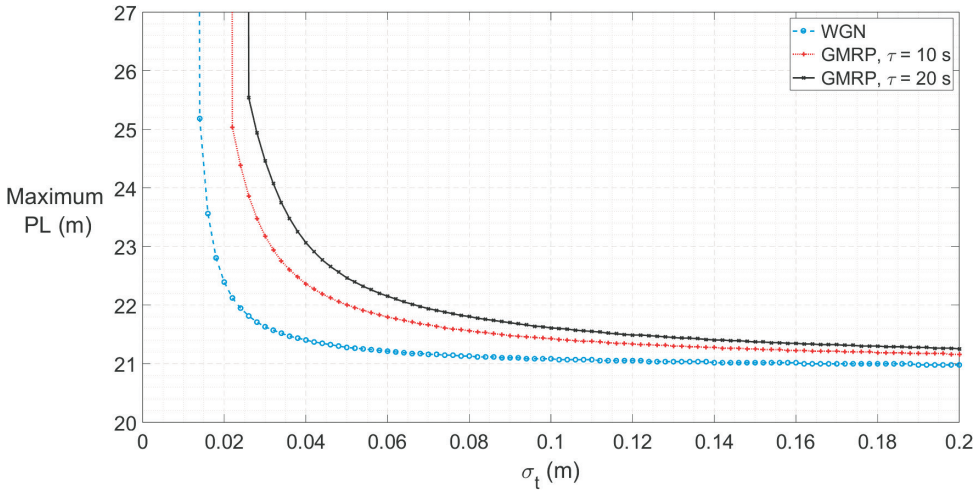

FIGURE 11 Maximum protection level (PL) versus tracking error magnitude for an example satellite geometry

detect tracking error. The addition of the SS monitor provides a means for detecting short-duration spoofing and for excluding the spoofed solution after detection. The sequential implementation of the monitors ensures that the performance is independent of the spoofing onset time.

6 | CONCLUSIONS

In this work, we introduced an optimal CPI monitor to detect spoofing by accumulating tracking error embedded in the spoofer's signal. We derived relationships between missed detection probability, tracking error magnitude, and monitor run time. We showed that even with decimeter-level tracking error, the monitor can detect spoofing with a low probability of missed detection in less than 1 min. We evaluated the performance of the CPI monitor for both white and time-correlated (colored) tracking error. To compute protection levels and detect short-duration spoofing, we proposed a complementary SS monitor to be implemented in sequential, overlapping windows to compare the integrated INS/GNSS position solution against an INS-only coasting solution. The INS-only coasting element also provides the capability to maintain positioning continuity after detection, albeit at lower accuracy, as the INS drifts.

REFERENCES

Akos, D. M. (2012). Who's afraid of the spoofer? GPS/GNSS spoofing detection via automatic gain control (AGC). *NAVIGATION*, *59*(4), 281–290. https://doi.org/10.1002/navi.19

Broumandan, A., Kennedy, S., & Schleppe, J. (2020). Demonstration of a multi-layer spoofing detection implemented in a high precision GNSS receiver. *Proc. of the 2020 IEEE/ION Position, Location and Navigation Symposium (PLANS),* Portland, OR, 538–547. https://doi.org/10.1109/PLANS46316.2020.9109842

Das, A., & Geisler, W. S. (2016). A method to integrate and classify normal distributions. *Journal of Vision*, *21*(10), 1. https://doi.org/10.1167/jov.21.10.1

Fernández-Hernández, I., Walter, T., Alexander, K., Clark, B., Châtre, E., Hegarty, C., Appel, M., & Meurer, M. (2019). Increasing international civil aviation resilience: A proposal for nomenclature, categorization and treatment of new interference threats. *Proc. of the 2019 International Technical Meeting of the Institute of Navigation,* Reston, VA, 389–407. https://doi.org/10.33012/2019.16699

Gallon, E., Joerger, M., & Pervan, B. (2020). Frequency-domain modeling of orbit and clock errors for sequential positioning. *Proc. of the 33rd International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+ 2020),* 1041–1053. https://doi.org/10.33012/2020.17542

Gallon, E., Joerger, M., & Pervan, B. (2021). Robust modeling of GNSS tropospheric delay dynamics. *IEEE Transactions on Aerospace and Electronic Systems*, *57*(5), 2992–3003. https://doi.org/10.1109/TAES.2021.3068441

Gunther, C. (2014). A survey of spoofing and counter-measures. *NAVIGATION*, *61*(3), 159–177. https://doi.org/10.1002/navi.65

Humphreys, T. E., Ledvina, B. M., Psiaki, M. L., O'Hanlon, B. W., & Kintner Jr., P. M. (2008). Assessing the spoofing threat: development of a portable GPS civilian spoofer. *Proc. of the 21st International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS 2008),* Savannah, GA, 2314–2325. https://www.ion.org/publications/abstract.cfm?articleID=8132

Jafarnia-Jahromi, A., Broumandan, A., Nielsen, J., & Lachapelle, G. (2012a). GPS spoofer countermeasure effectiveness based on signal strength, noise power, and C/N_0 measurements. *International Journal of Satellite, Communications and Networking*, *30*(4), 181–191. https://doi.org/10.1002/sat.1012

Jafarnia-Jahromi, A., Broumandan, A., Nielsen, J., & Lachapelle, G. (2012b). GPS vulnerability to spoofing threats and a review of antispoofing techniques. *International Journal of Navigation and Observation*, *2012*(127072), 1–16. https://doi.org/10.1155/2012/127072

Kay, M. S. (1998). *Fundamentals of statistical signal processing: detection theory, volume 2*. Prentice-Hall PTR. https://books.google.com/books?id=vA9LAQAAIAAJ

Kerns, A. J., Shepard, D. P., Bhatti, J. A., & Humpherys, T. E. (2014). Unmanned aircraft capture and control via GPS spoofing. *Journal of Field Robotics*, *31*(4), 617–636. https://doi.org/10.1002/rob.21513

Kerns, A. J., Wesson, K. D., & Humphreys, T. E. (2014). A blueprint for civil GPS navigation message authentication. *Proc. of the 2014 IEEE/ION Position, Location and Navigation Symposium (PLANS),* Monterey, CA, 262–269. https://doi.org/10.1109/PLANS.2014.6851385

Khanafseh, S., Roshan, N., Langel, S., Chan, F., Joerger, M., & Pervan, B. (2014). GPS spoofing detection using RAIM with INS coupling. *Proc. of the 2014 IEEE/ION Position, Location and Navigation Symposium (PLANS),* Monterey, CA, 1232–1239. https://doi.org/10.1109/PLANS.2014.6851498

Kujur, B., Khanafseh, S., & Pervan, B. (2023). Experimental validation of optimal INS monitor against GNSS spoofer tracking error detection. *Proc. of the 2023 IEEE/ION Position, Location and Navigation Symposium (PLANS),* Monterey, CA, 592–596. https://doi.org/10.1109/PLANS53410.2023.10140096

Kujur, B., Tanil, C., Khanafseh, S., & Pervan, B. (2019). Sensitivity of innovation monitors to uncertainty in error modeling. *Proc. of the 32nd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2019),* Miami, FL, 3266–3274. https://doi.org/10.33012/2019.17066

Lo, S., Chen, Y., Reid, T., Perkins, A., Walter, T., & Enge, P. (2017). Keynote: the benefits of low cost accelerometers for GNSS anti-spoofing. *Proc. of the ION 2017 Pacific PNT Meeting,* Honolulu, HI, 775–796. https://doi.org/10.33012/2017.15109

Mathai, A. M., & Provost, S. B. (1992). *Quadratic forms in random variables: Theory and applications*. Marcel Dekker. https://www.researchgate.net/publication/224817325_Quadratic_Forms_in_Random_Variables_Theory_and_Applications

Meurer, M., Konovaltsev, A., Cuntz, M., & Hattich, C. (2012). Robust joint multi-antenna spoofing detection and attitude estimation using direction assisted multiple hypotheses RAIM. *Proc. of the 25th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS 2012),* Nashville, TN, 3007–3016. https://www.ion.org/publications/abstract.cfm?articleID=10480

Miller, K. S. (1981). On the inverse of the sum of matrices. *Mathematics Magazine*, *54*(2), 67–72. https://doi.org/10.2307/2690437

Misra, P., & Enge, P. (2012). *Global Positioning System: Signals, measurements, and performance*. Ganga-Jamuna Press. https://www.google.com/books/edition/Global_Positioning_System/pv5MAQAAIAAJ?hl=en

Moshavi, S. (1996). Multi-user detection for DS-CDMA communications. *IEEE Communications Magazine*, *34*(10), 124–136. https://doi.org/10.1109/35.544334

Neyman, J., & Pearson, E. S. (1933). IX. On the problem of the most efficient tests of statistical hypotheses. *Philosophical Transactions of the Royal Society of London. Series A, Containing Papers of a Mathematical or Physical Character*, *231*(694–706), 289–337. https://doi.org/10.1098/rsta.1933.0009

Nielsen, J., Broumandan, A., & Lachapelle, G. (2014). GNSS spoofing detection for single antenna handheld receivers. *NAVIGATION*, *58*(4), 335–344. https://doi.org/10.1002/j.2161-4296.2011.tb02590.x

O'Hanlon, B. W., Psiaki, M. L., Bhatti, J. A., Shepard, D. P., & Humphreys, T. E. (2013). Real-time GPS spoofing detection via correlation of encrypted signals. *NAVIGATION*, *60*(4), 267–278. https://www.ion.org/publications/abstract.cfm?articleID=102607

Psiaki, M. L., & Humphreys, T. E. (2016). GNSS spoofing and detection. *Proc. of the IEEE*, *104*(6), 1258–1270. https://doi.org/10.1109/JPROC.2016.2526658

Psiaki, M. L., Powell, S. P., & O'Hanlon, B. W. (2013). GNSS spoofing detection using high-frequency antenna motion and carrier-phase data. *Proc. of the 26th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+ 2013),* Nashville, TN, 2949–2991. https://www.ion.org/publications/abstract.cfm?articleID=11137

Rothmaier, F., Chen, Y., Lo, S., & Walter, T. (2021b). GNSS spoofing mitigation in the position domain. *Proc. of the 2021 International Technical Meeting of the Institute of Navigation,* 42–55. https://doi.org/10.33012/2021.17824

Rothmaier, F., Chen, Y.-H., Lo, S., & Walter, T. (2021a). A framework for GNSS spoofing detection through combinations of metrics. *IEEE Transactions on Aerospace and Electronic Systems*, *57*(6), 3633–3647. https://doi.org/10.1109/TAES.2021.3082673

SC-159. (2009). *RTCA DO-316, Performance standards for global positioning system/ aircraft based augmentation system airborne equipment* (Tech. Rep.). RTCA. https://my.rtca.org/productdetails?id=a1B36000001IcgOEAS

SC-159. (2020). *RTCA DO-229, Minimum operational performance standards (MOPS) for global positioning system/satellite-based augmentation system airborne equipment* (Tech. Rep.). RTCA. https://my.rtca.org/productdetails?id=a1B1R0000092uanUAA

Stenberg, N., Axell, E., Rantakokko, J., & Hendeby, G. (2020). GNSS spoofing mitigation using multiple receivers. *Proc. of the 2020 IEEE/ION Position, Location and Navigation Symposium (PLANS),* Portland, OR, 555–565. https://doi.org/10.1109/PLANS46316.2020.9109958

Swaszek, P. F., Hartnett, R. J., & Seals, K. C. (2016). GNSS spoof detection using independent range information. *Proc. of the 2016 International Technical Meeting of the Institute of Navigation,* Monterey, CA, 739–747. https://doi.org/10.33012/2016.13457

Tanil, C., Jimenez, P. M., Raveloharison, M., Kujur, B., Khanafseh, S., & Pervan, B. (2018). Experimental validation of INS monitor against GNSS spoofing. *Proc. of the 31st International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+),* Miami, FL, 3266–3274. https://doi.org/10.33012/2018.15902

Tanil, C., Khanafseh, S., Joerger, M., & Pervan, B. (2018). An INS monitor to detect GNSS spoofers capable of tracking vehicle position. *IEEE Transactions on Aerospace and Electronic Systems*, *54*(1), 131–143. https://doi.org/10.1109/TAES.2017.2739924

Tanil, C., Khanafseh, S., & Pervan, B. (2015a). GNSS spoofing attack detection using aircraft autopilot response to deceptive trajectory. *Proc. of the 28th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+ 2015)*, Tampa, FL, 3345–3357. https://www.ion.org/publications/abstract.cfm?articleID=12888

Tanil, C., Khanafseh, S., & Pervan, B. (2015b). Impact of wind gusts on detectability of GPS spoofing attacks using RAIM with INS coupling. *Proc. of the ION 2015 Pacific PNT Meeting,* Honolulu, HI, 674–686. https://www.ion.org/publications/abstract.cfm?articleID=12756

Tanil, C., Khanafseh, S., & Pervan, B. (2016). An INS monitor against GNSS spoofing attacks during GBAS and SBAS-assisted aircraft landing approaches. *Proc. of the 29th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+ 2016),* Portland, OR, 2981–2990. https://doi.org/10.33012/2016.14779

Tanil, C., Khanafseh, S., & Pervan, B. (2017). Detecting Global Navigation Satellite System spoofing using inertial sensing of aircraft disturbance. *Journal of Guidance, Control, and Dynamics*, *40*(8), 2006–2016. https://doi.org/10.2514/1.G002547

Turner, M., Wimbush, S., Enneking, C., & Konovaltsev, A. (2020). Spoofing detection by distortion of the correlation function. *Proc. of the 2020 IEEE/ION Position, Location and Navigation Symposium (PLANS),* Portland, OR, 566–574. https://doi.org/10.1109/PLANS46316.2020.9110173

Walter, T., Datta-Barua, S., Blanch, J., & Enge, P. (2004). The effects of large ionospheric gradients on single frequency airborne smoothing filters for WAAS and LAAS. *Proc. of the 2004 National Technical Meeting of the Institute of Navigation,* San Diego, CA, 103–109. https://www.ion.org/publications/abstract.cfm?articleID=5486

Wesson, K. D., Gross, J. N., Humphreys, T. E., & Evans, B. L. (2018). GNSS signal authentication via power and distortion monitoring. *IEEE Transactions on Aerospace and Electronic Systems*, *54*(2), 739–754. https://doi.org/10.1109/TAES.2017.2765258

Wesson, K. D., Rothlisberger, M. P., & Humphreys, T. (2011). A proposed navigation message authentication implementation for civil GPS anti-spoofing. *Proc. of the 24th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS 2011),* Portland, OR, 3129–3140. https://www.ion.org/publications/abstract.cfm?articleID=9870

How to cite this article: Kujur, B., Khanafseh, S., & Pervan, B. (2024). Optimal INS monitor for GNSS spoofer tracking error detection. *NAVIGATION, 71*(1). https://doi.org/10.33012/navi.629

APPENDIX

A | TIGHTLY COUPLED INS/GNSS ARCHITECTURE

Using IMU measurements, an INS provides a navigation state vector, which includes the aircraft position vector $\mathbf{r}$ with components x, y, z, velocity vector $\mathbf{v}$ with components u, v, w, and attitude ϕ, θ, ψ (Euler angles):

$$\mathbf{x}_{A/C} = \begin{bmatrix} x & y & z & u & v & w & \phi & \theta & \psi \end{bmatrix}^T \tag{A1}$$

An IMU consists of tri-axis accelerometers and gyroscopes to provide measurements of acceleration and body angular rate. In an INS, the IMU acceleration measurements are integrated once to obtain the velocity and then integrated again to obtain the position, whereas attitude is obtained by integrating angular rate measurements. These measurements have errors (biases and noise), causing the state estimate error to drift over time. In a tightly coupled INS/GNSS architecture, a KF uses raw GNSS code and carrier phase measurements to estimate and correct the error in the drifting INS states to provide an integrated navigation solution.

An individual (scalar) IMU measurement $\tilde{u}$ has errors such as time-dependent biases and noise. Therefore, it is modeled as a "true" measurement u^*, corrupted with a constant bias b_c, a slowly varying time-dependent bias-like component b, and additive WGN η_u, as represented in Equation (A2). The constant bias is usually specified as bias repeatability, and the additive WGN η_u is commonly derived from specifications on the VRW for an accelerometer and angular random walk for a gyroscope:

$$\tilde{u} = u^* + b_c + b + \eta_u \tag{A2}$$

The time-dependent component of the bias b is modeled as a first-order GMRP with time constant τ_b and driving WGN ν_b. The driving WGN is derived from the IMU "bias instability" specifications:

$$\dot{b} = -\frac{1}{\tau_b} b + \nu_b \tag{A3}$$

The bias dynamics are included in the process model by augmentation of bias states $\mathbf{x}_{bias}$ to the aircraft states. Thus, for three different IMU axes, the bias states for both acceleration and angular rate measurements are shown in Equation (A4). Equations (A1) and (A4) show all of the nominal states that are propagated to obtain the INS navigation solution:

$$\mathbf{x}_{bias} = \begin{bmatrix} b_{a_x} & b_{a_y} & b_{a_z} & b_{\omega_x} & b_{\omega_y} & b_{\omega_z} \end{bmatrix}^T \tag{A4}$$

We assume that an en route aircraft utilizes single-frequency GPS measurements without any differential corrections; however, this concept is also applicable to dual-frequency multi-constellation GNSS, terminal, and precision approach scenarios. Equation (A5) shows a simplified GPS measurement model in which the code measurement ρ for each satellite is composed of the true range r, satellite and receiver clock biases dt_{sv} and dt_{rc}, code ionospheric delay I_ρ, code tropospheric delay T_ρ, code multipath m_ρ, and receiver code thermal WGN $\nu_{th_{(\rho)}}$. Similarly, the carrier phase measurement $\lambda\phi$ for each satellite is composed of the true range r, satellite and receiver clock bias dt_{sv} and dt_{rc}, carrier ionospheric

delay I_ϕ, carrier tropospheric delay T_ϕ, carrier phase multipath m_ϕ, carrier phase cycle integer ambiguity N_ϕ, and receiver carrier thermal WGN v_{th_ϕ}. The code ionospheric delay I_ρ is of the same magnitude as the carrier ionospheric delay I_ϕ, and the code tropospheric delay T_ρ is of the same magnitude as the carrier tropospheric delay T_ϕ:

$$\begin{bmatrix}\rho\\ \lambda\phi\end{bmatrix}=\begin{bmatrix}r\\ r\end{bmatrix}+\begin{bmatrix}c\,(dt_{rc}-dt_{sv})\\ c\,(dt_{rc}-dt_{sv})\end{bmatrix}+\begin{bmatrix}I_\rho\\ -I_\phi\end{bmatrix}+\begin{bmatrix}T_\rho\\ T_\phi\end{bmatrix}+\begin{bmatrix}m_\rho\\ m_\phi\end{bmatrix}+\begin{bmatrix}0\\ \lambda N_\phi\end{bmatrix}+\begin{bmatrix}v_{th_{(\rho)}}\\ v_{th_{(\phi)}}\end{bmatrix} \tag{A5}$$

where c is the speed of light in vacuum and λ is the carrier wavelength.

All GPS errors must be included in the measurement in order to be utilized in the KF. The satellite clock offset cdt_{sv} is corrected based on the clock parameters broadcast in the navigation message. After the satellite clock offset correction has been applied, there are still residual errors caused by satellite clock and orbit ephemeris parameter uncertainty. These residual errors r_{sv} are modeled (Gallon et al., 2020) as a first-order GMRP with a time constant $\tau_{r_{sv}}$ of 5 h subject to driving WGN $v_{r_{sv}}$ with a standard deviation of 1.8 m. Equation (A6) represents the first-order GMRP model for satellite clock and ephemeris residual errors:

$$\dot{r}_{sv}=-\frac{1}{\tau_{r_{sv}}}r_{sv}+v_{r_{sv}} \tag{A6}$$

The receiver clock offset cdt_{rc} is compensated by a constant clock offset drift rate model. The clock offset state r_{rc} is modeled to drift with a constant rate $\dot{r}_{rc}$ over time, as shown by Equation (A7):

$$\begin{bmatrix}\dot{r}_{rc}\\ \ddot{r}_{rc}\end{bmatrix}=\begin{bmatrix}0 & 1\\ 0 & 0\end{bmatrix}\begin{bmatrix}r_{rc}\\ \dot{r}_{rc}\end{bmatrix}+\begin{bmatrix}w_{r_{rc}}\\ w_{\dot{r}_{rc}}\end{bmatrix} \tag{A7}$$

where $w_{r_{rc}}$ and $w_{\dot{r}_{rc}}$ are WGN inputs to the clock offset and clock offset drift rate, respectively. The variances of these WGN inputs are obtained using typical Allan variance coefficients of temperature-compensated crystal oscillator timing standards. The white phase noise (h_0) and frequency random walk noise (h_2) coefficients used are 2×10^{-19} and 2×10^{-20}, respectively.

For ionospheric delay, we use the ionospheric correction T_{iono} from the Klobachaur model, which results in residual errors r_i, as modeled by SC-159 (2009), with a standard deviation given by Equation (A8):

$$\sigma_i=\sqrt{\max\left[\left(\frac{cT_{iono}}{5}\right)^2,(F_{pp}\tau_{vert})^2\right]} \tag{A8}$$

where F_{pp} is the obliquity factor and τ_{vert} is calculated given the geomagnetic latitude (SC-159, 2009). Because the ionospheric delay is a slowly changing error, it is modeled as a first-order GMRP with a time constant of 40 h (Appendix B) and driving WGN v_{r_i} as follows:

$$\dot{r}_i=-\frac{1}{\tau_{r_i}}r_i+v_{r_i} \tag{A9}$$

The troposheric delay is corrected with the correction model specified in SC-159 (2009), and the residual errors r_t in the zenith direction are modeled as a first-order GMRP with a time constant of 20 h and a standard deviation of 0.09 m (Gallon

et al., 2021). The zenith error is converted to a slant ranging error using the elevation-dependent mapping function reported in SC-159 (2009). Equation (A10) shows the first-order GMRP model of the tropospheric residual error r_t:

$$\dot{r}_t = -\frac{1}{\tau_{r_t}} r_t + v_{r_t} \tag{A10}$$

where v_{r_t} is the driving WGN for zenith tropospheric residual errors.

Being time-correlated, the multipath is modeled as a first-order GMRP with a time constant τ_m of 25 s and driving WGN v_m (SC-159, 2009):

$$\dot{m} = -\frac{1}{\tau_m} m + v_m \tag{A11}$$

The standard deviation for code multipath error is 5 m (SC-159, 2009), and for carrier multipath error. we assume the standard deviation to be 0.02 m (Misra & Enge, 2012). The receiver code thermal noise standard deviation is taken to be 0.36 m (SC-159, 2009), and the carrier thermal noise standard deviation is assumed to be 3 mm (Misra & Enge, 2012).

Constant carrier phase cycle integer ambiguities, along with all of the above-mentioned residual error states, are included in the GNSS measurement error states:

$$\mathbf{x}_{GNSS} = \begin{bmatrix} r_{sv}^{1:n} & r_{rc} & \dot{r}_{rc} & r_i^{1:n} & r_t & m_\rho^{1:n} & m_\phi^{1:n} & \lambda N_\phi^{1:n} \end{bmatrix}^T \tag{A12}$$

where n is the number of satellites in view. The final state vector of the INS/GNSS system is as follows:

$$\mathbf{x} = \begin{bmatrix} \mathbf{x}_{A/C} & \mathbf{x}_{bias} & \mathbf{x}_{GNSS} \end{bmatrix}^T \tag{A13}$$

B | IONOSPHERIC RESIDUAL ERROR MODEL

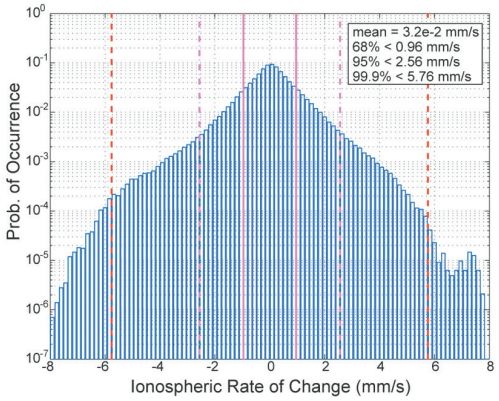

FIGURE B1 Histogram of rates of total electron content change for a quiet solar maximum day (Walter et al., 2004)

Figure B1 shows a histogram of the ionospheric rate based on 24 h of data from Walter et al. (2004). The data are boundable by a Gaussian distribution with a mean of 3.2×10^{-2} mm/s and a standard deviation of 0.96 mm/s. We model the

ionospheric residuals using a first-order GMRP such that the obtained rate matches this Gaussian distribution.

After utilizing Equation (A8) from SC-159 (2009) to obtain the standard deviation for the first-order GMRP, it was determined that the time constant that produces the best approximation of the ionospheric rate distribution in Figure B1 is approximately 40 h.

C | EFFECT OF TRACKING ERROR ON COVARIANCE OF INNOVATIONS

We define the spoofer's uncertainty in the target's position as the tracking error v^t and use the superscript s for terms that are otherwise related to the spoofer or spoofed signal. At time k, the spoofer estimates the user position with tracking error, given as follows:

$$\begin{bmatrix} x^s \\ y^s \\ z^s \end{bmatrix}_k = \begin{bmatrix} x \\ y \\ z \end{bmatrix}_k + \begin{bmatrix} v_x^t \\ v_y^t \\ v_z^t \end{bmatrix}_k \tag{C14}$$

where x_k, y_k, *and* z_k give the true user position. We conservatively assume that there is no latency in the spoofer's tracking and counterfeit signal generation and neglect additive errors due to thermal noise and multipath in the counterfeit signal transmission. We also concede to the spoofer the ability to replicate the true signal-in-space errors seen by the target—namely, satellite orbit and clock errors and atmospheric effects. We also ignore the contribution of the deliberate deviations added by the spoofer to the counterfeit signal. Relaxing any of these conservative assumptions and concessions would only make the spoofing easier to detect at the target and the analysis less complicated. We ignore these effects in what follows and concern ourselves only with the impacts of tracking error in a single, arbitrary spatial direction.

The spoofer projects the counterfeit state vector $\mathbf{x}_k^{us}$ into the range domain:

$$\mathbf{z}_k^{us} = \mathbf{H}_k \mathbf{x}_k^{us} = \mathbf{H}_k \mathbf{x}_k + \mathbf{H}_k \mathbf{u} v_k^t \tag{C15}$$

where $v_k^t \sim \mathcal{N}(0, \sigma_t^2)$ is the tracking error along the spatial direction corresponding to the unit vector $\mathbf{u}$ in the state space. This vector can be re-expressed in terms of the "true" range vector, $\mathbf{z}_k$, as follows:

$$\mathbf{z}_k^{us} = \mathbf{z}_k + \mathbf{H}_k \mathbf{u} v_k^t \tag{C16}$$

The contribution of the tracking error to the innovations is then given by the following:

$$\gamma_k^{us} = \mathbf{z}_k^{us} - \mathbf{H}_k \bar{\mathbf{x}}_k = \mathbf{z}_k + \mathbf{H}_k \mathbf{u} v_k^t - \mathbf{H}_k \bar{\mathbf{x}}_k \tag{C17}$$

Rearranging, we have the following relation:

$$\gamma_k^{us} = \mathbf{z}_k - \mathbf{H}_k \bar{\mathbf{x}}_k + \mathbf{H}_k \mathbf{u} v_k^t = \gamma_k + \mathbf{H}_k \mathbf{u} v_k^t \tag{C18}$$

The covariance of the innovation vector with the presence of tracking error can be written as follows:

$$\mathbb{E}\left[(\gamma_k^{us})^2\right] = \mathbf{S}_k + \mathbf{H}_k \mathbf{u}\mathbf{u}^T \mathbf{H}_k^T \sigma_t^2 \tag{C19}$$

D | EFFECT OF TRACKING ERROR ON TIME CORRELATION OF INNOVATIONS

The derivation of the Neyman–Pearson optimal test statistic relies on the assumption that the random variables forming the test statistic—the position-domain innovation in our case—are time-independent. To verify the independence of innovations over time, we generate sample auto-correlation functions (ACFs) and estimate the associated time constants. In the absence of tracking error, independence is guaranteed as long as the nominal error models in the KF are accurate. However, we also need to verify whether the assumption is valid if WGN tracking error is present. Figure D2 shows a sample ACF of carrier phase innovations for the case of WGN tracking error with $\sigma_t = 10$ cm using a navigation-grade IMU. The time constant (measured at the $1/e$ point) of the sample ACF was 0.21 s, which is less than the sample interval of 0.5 s, thus confirming that the innovations are white.

We expect that a lower-quality IMU would have a greater contribution toward the time correlation of innovations because the Kalman gain would give a higher weight to the GNSS measurements than in the high-quality IMU case. Consequently, the tracking error will affect the post-measurement states $\hat{\mathbf{x}}$ to a greater degree as well as the subsequent "predicted" measurement $\mathbf{H}\bar{\mathbf{x}}$ used to generate the innovations. To confirm that the innovations are still white, even for lower-grade IMUs, we evaluate sample ACFs of the carrier phase innovations for navigation-, tactical-, and automotive-grade IMUs. Figure D2 shows the results for the case of WGN tracking error with $\sigma_t = 10$ cm. It is clear from the figure that even for an automotive-grade IMU, the innovations still remain white, with a time constant of 0.24 s.

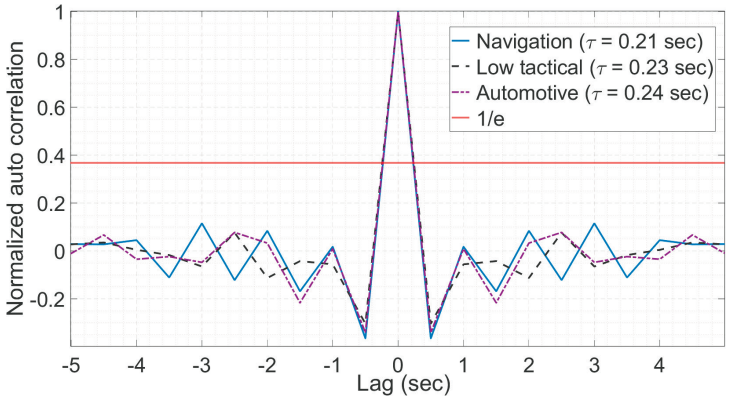

FIGURE D2 Normalized ACF plots of the carrier phase innovations for different IMU grades with WGN tracking error ($\sigma_t = 10$ cm)

E | COVARIANCE OF SS TEST STATISTIC

Let us consider an SS monitor that starts at time epoch 1. The KF time and measurement update equations are as follows:

$$\bar{\mathbf{x}}_1 = \Phi_1 \hat{\mathbf{x}}_0 \tag{E20}$$

$$\hat{\mathbf{x}}_1 = \bar{\mathbf{x}}_1 + \mathbf{L}_1(\mathbf{z}_1 - \mathbf{H}_1\bar{\mathbf{x}}_1) \tag{E21}$$

where, for any time epoch k, $\bar{\mathbf{x}}_k$ and $\hat{\mathbf{x}}_k$ represent the states after the KF time and measurement updates, respectively. Φ_k is the state transition matrix, $\mathbf{L}_k$ is the Kalman gain, $\mathbf{z}_k$ is the GNSS measurement, and $\mathbf{H}_k$ is the observation matrix. The associated estimation equations can be determined as follows:

$$\bar{\mathbf{e}}_1 = \Phi_1 \hat{\mathbf{e}}_0 - \mathbf{w}_1 \tag{E22}$$

$$\hat{\mathbf{e}}_1 = (\mathbf{I} - \mathbf{L}_1 \mathbf{H}_1)\bar{\mathbf{e}}_1 + \mathbf{L}_1 \mathbf{v}_1 \tag{E23}$$

where, for any time epoch k, $\bar{\mathbf{e}}_k$ and $\hat{\mathbf{e}}_k$ represent the state estimate error after the KF time and measurement updates, respectively. $\mathbf{I}$ is the identity matrix, $\mathbf{w}_k$ is the process noise vector, and $\mathbf{v}_k$ is the measurement noise vector. For the SS monitor, parallel INS-only coasting is initiated with the state propagation equation:

$$\bar{\mathbf{x}}_{c_1} = \Phi_1 \hat{\mathbf{x}}_0 \tag{E24}$$

where, for any time epoch k, $\bar{\mathbf{x}}_{c_k}$ represents the state after the time update in INS-only coasting. Here, we also assume that the state transition matrix does not differ from that of the KF. The time update error propagation for the first time epoch of INS-only coasting is given as follows:

$$\bar{\mathbf{e}}_{c_1} = \Phi_1 \hat{\mathbf{e}}_0 - \mathbf{w}_1 \tag{E25}$$

where, for any time epoch k, $\bar{\mathbf{e}}_{c_k}$ represents the state estimate error after the time update during INS-only coasting.

Similarly, for the second time epoch, we can write the KF time and measurement update equations as follows:

$$\bar{\mathbf{x}}_2 = \Phi_2 \hat{\mathbf{x}}_1 \tag{E26}$$

$$\hat{\mathbf{x}}_2 = \bar{\mathbf{x}}_2 + \mathbf{L}_2(\mathbf{z}_2 - \mathbf{H}_2 \bar{\mathbf{x}}_2) \tag{E27}$$

We can write the propagation equation for INS-only coasting as follows:

$$\bar{\mathbf{x}}_{c_2} = \Phi_2 \bar{\mathbf{x}}_{c_1} \tag{E28}$$

The associated KF error propagation equations are as follows:

$$\bar{\mathbf{e}}_2 = \Phi_2 \hat{\mathbf{e}}_1 - \mathbf{w}_2 \tag{E29}$$

$$\hat{\mathbf{e}}_2 = (\mathbf{I} - \mathbf{L}_2 \mathbf{H}_2)\bar{\mathbf{e}}_2 + \mathbf{L}_2 \mathbf{v}_2 \tag{E30}$$

For INS-only coasting, the state estimate error propagation equation is given by the following:

$$\bar{\mathbf{e}}_{c_2} = \Phi_2 \bar{\mathbf{e}}_1 - \mathbf{w}_2 \tag{E31}$$

We now define the following covariance matrices: $\bar{\mathbf{P}}_k = \mathbb{E}\{\bar{\mathbf{e}}_k \bar{\mathbf{e}}_k^T\}$, $\hat{\mathbf{P}}_k = \mathbb{E}\{\hat{\mathbf{e}}_k \hat{\mathbf{e}}_k^T\}$, $\mathbf{Q}_k = \mathbb{E}\{\mathbf{w}_k \mathbf{w}_k^T\}$, and $\mathbf{V}_k = \mathbb{E}\{\mathbf{v}_k \mathbf{v}_k^T\}$.

The test statistic for the SS monitor at time k is defined as follows:

$$q_{SS_k} = \mathbf{u}^T \mathbf{q}_{SS_k} \tag{E32}$$

where:

$$\mathbf{q}_{SS_k} = \hat{\mathbf{x}}_{KF_k} - \overline{\mathbf{x}}_{c_k} \tag{E33}$$

which has the following covariance matrix:

$$\mathbf{P}_{q_k} = \mathbb{E}\{\mathbf{q}_{SS_k}\mathbf{q}_{SS_k}^T\} = \mathbb{E}\{[\hat{\mathbf{x}}_k - \overline{\mathbf{x}}_{c_k}][\hat{\mathbf{x}}_k - \overline{\mathbf{x}}_{c_k}]^T\} \tag{E34}$$

The covariance for the first time epoch is as follows:

$$\mathbf{P}_{q_1} = \mathbb{E}\{[\hat{\mathbf{x}}_1 - \overline{\mathbf{x}}_{c_1}][\hat{\mathbf{x}}_1 - \overline{\mathbf{x}}_{c_1}]^T\} = \mathbb{E}\{[\hat{\mathbf{e}}_1 - \overline{\mathbf{e}}_{c_1}][\hat{\mathbf{e}}_1 - \overline{\mathbf{e}}_{c_1}]^T\} \tag{E35}$$

The above equation can be further expanded:

$$\mathbf{P}_{q_1} = \mathbb{E}\{\hat{\mathbf{e}}_1\hat{\mathbf{e}}_1^T\} - \mathbb{E}\{\hat{\mathbf{e}}_1\overline{\mathbf{e}}_{c_1}^T\} - \mathbb{E}\{\overline{\mathbf{e}}_{c_1}\hat{\mathbf{e}}_1^T\} + \mathbb{E}\{\overline{\mathbf{e}}_{c_1}\overline{\mathbf{e}}_{c_1}^T\} = \hat{\mathbf{P}}_1 - \mathbb{E}\{\hat{\mathbf{e}}_1\overline{\mathbf{e}}_{c_1}^T\} - \mathbb{E}\{\overline{\mathbf{e}}_{c_1}\hat{\mathbf{e}}_1^T\} + \overline{\mathbf{P}}_{c_1} \tag{E36}$$

For the second and third terms, we use Equation (E23):

$$\mathbb{E}\{\hat{\mathbf{e}}_1\overline{\mathbf{e}}_{c_1}^T\} = \mathbb{E}\{[(\mathbf{I} - \mathbf{L}_1\mathbf{H}_1)\overline{\mathbf{e}}_1 + \mathbf{L}_1\mathbf{v}_1]\overline{\mathbf{e}}_{c_1}^T\} = (\mathbf{I} - \mathbf{L}_1\mathbf{H}_1)\mathbb{E}\{\overline{\mathbf{e}}_1\overline{\mathbf{e}}_{c_1}^T\} \tag{E37}$$

From Equations (E22) and (E25), we know that $\overline{\mathbf{e}}_1$ and $\overline{\mathbf{e}}_{c_1}$ are the same for the first time epoch; hence, we have the following:

$$\mathbb{E}\{\hat{\mathbf{e}}_1\overline{\mathbf{e}}_{c_1}^T\} = (\mathbf{I} - \mathbf{L}_1\mathbf{H}_1)\overline{\mathbf{P}}_1 \tag{E38}$$

Similarly, we have the following relation:

$$\mathbb{E}\{\overline{\mathbf{e}}_{c_1}^T\hat{\mathbf{e}}_1\} = \overline{\mathbf{P}}_1(\mathbf{I} - \mathbf{L}_1\mathbf{H}_1)^T \tag{E39}$$

Moreover, from the KF equations, we have the following expression for any time epoch k:

$$\hat{\mathbf{P}}_k = (\mathbf{I} - \mathbf{L}_k\mathbf{H}_k)\overline{\mathbf{P}}_k \tag{E40}$$

Thus, Equation (E36) takes the following form:

$$\mathbf{P}_{q_1} = \hat{\mathbf{P}}_1 - \hat{\mathbf{P}}_1 - \hat{\mathbf{P}}_1 + \overline{\mathbf{P}}_{c_1} = \overline{\mathbf{P}}_{c_1} - \hat{\mathbf{P}}_1 \tag{E41}$$

Now, the covariance for the second time epoch is as follows:

$$\mathbf{P}_{q_2} = \mathbb{E}\{[\hat{\mathbf{x}}_2 - \overline{\mathbf{x}}_{c_2}][\hat{\mathbf{x}}_2 - \overline{\mathbf{x}}_{c_2}]^T\} = \mathbb{E}\{[\hat{\mathbf{e}}_2 - \overline{\mathbf{e}}_{c_2}][\hat{\mathbf{e}}_2 - \overline{\mathbf{e}}_{c_2}]^T\} \tag{E42}$$

As before, this expression can be further expanded:

$$\mathbf{P}_{q_2} = \mathbb{E}\{\hat{\mathbf{e}}_2\hat{\mathbf{e}}_2^T\} - \mathbb{E}\{\hat{\mathbf{e}}_2\overline{\mathbf{e}}_{c_2}^T\} - \mathbb{E}\{\overline{\mathbf{e}}_{c_2}\hat{\mathbf{e}}_2^T\} + \mathbb{E}\{\overline{\mathbf{e}}_{c_2}\overline{\mathbf{e}}_{c_2}^T\} = \hat{\mathbf{P}}_2 - \mathbb{E}\{\hat{\mathbf{e}}_2\overline{\mathbf{e}}_{c_2}^T\} - \mathbb{E}\{\overline{\mathbf{e}}_{c_2}\hat{\mathbf{e}}_2^T\} + \overline{\mathbf{P}}_{c_2} \tag{E43}$$

For the second and third terms, we use Equation (E30):

$$\mathbb{E}\{\hat{\mathbf{e}}_2\bar{\mathbf{e}}_{c_2}^T\} = \mathbb{E}\{[(\mathbf{I}-\mathbf{L}_2\mathbf{H}_2)\bar{\mathbf{e}}_2 + \mathbf{L}_2\mathbf{v}_2]\bar{\mathbf{e}}_{c_2}^T\} = (\mathbf{I}-\mathbf{L}_2\mathbf{H}_2)\mathbb{E}\{\bar{\mathbf{e}}_2\bar{\mathbf{e}}_{c_2}^T\} \tag{E44}$$

Substituting Equations (E29) and (E31) into Equation (E44), we obtain the following:

$$\mathbb{E}\{\hat{\mathbf{e}}_2\bar{\mathbf{e}}_{c_2}^T\} = (\mathbf{I}-\mathbf{L}_2\mathbf{H}_2)\mathbb{E}\{[\Phi_2\hat{\mathbf{e}}_1 - \mathbf{w}_2][\Phi_2\bar{\mathbf{e}}_1 - \mathbf{w}_2]^T\} \tag{E45}$$

By expanding Equation (E45) and using results from Equations (E37) and (E40), we obtain the following relation:

$$\mathbb{E}\{\hat{\mathbf{e}}_2\bar{\mathbf{e}}_{c_2}^T\} = (\mathbf{I}-\mathbf{L}_2\mathbf{H}_2)[\Phi_2\hat{\mathbf{P}}_1\Phi_2^T + \mathbf{Q}_2] = (\mathbf{I}-\mathbf{L}_2\mathbf{H}_2)\bar{\mathbf{P}}_2 = \hat{\mathbf{P}}_2 \tag{E46}$$

Substituting Equation (E46) into Equation (E43) gives the following:

$$\mathbf{P}_{q_2} = \bar{\mathbf{P}}_{c_2} - \hat{\mathbf{P}}_2 \tag{E47}$$

Hence, following Equations (E41) and (E47), we can write a general expression for the SS test statistic covariance for any time epoch k:

$$\mathbf{P}_{q_k} = \bar{\mathbf{P}}_{c_k} - \hat{\mathbf{P}}_k \tag{E48}$$

F | SPECIFICATIONS FOR IMU GRADES

TABLE F1
Specifications for Different IMU Grades

Parameter	Navigation	Low tactical	Automotive	Unit
Velocity random walk	1.43×10^{-2}	7×10^{-2}	0.18	m/s/$\sqrt{\text{h}}$
Accelerometer bias instability	1×10^{-2}	4×10^{-2}	4×10^{-2}	mg
Accelerometer bias repeatability	2.5×10^{-2}	0.75	1.5	mg
Accelerometer bias time constant	3600	3600	3600	s
Angular random walk	1×10^{-3}	0.15	0.2	deg/$\sqrt{\text{h}}$
Gyroscope bias instability	3.5×10^{-3}	0.3	7	deg/h
Gyroscope bias repeatability	3×10^{-3}	4	120	deg/h
Gyroscope time constant	3600	3600	3600	s