Detecting GNSS Spoofing using Temporal Behavior of Spoofed Signals

Birendra Kujur, Samer Khanafseh, and Boris Pervan, Illinois Institute of Technology

BIOGRAPHIES

Birendra Kujur is currently a PhD candidate in Mechanical and Aerospace Engineering at Illinois Institute of Technology. He received his Bachelor of Science in Mechanical Engineering from Purdue University in 2014. His research interests include multi-sensor navigation systems and navigation integrity monitoring. Currently, he focuses on detecting GNSS spoofing attacks and developing anti-spoofing solution.

Dr. Samer Khanafseh is currently a research associate professor at Illinois Institute of Technology (IIT), Chicago, and the principal of TruNav LLC. He received his MSc and PhD degrees in Aerospace Engineering from IIT in 2003 and 2008, respectively. Dr. Khanafseh has been involved in several aviation applications such as Autonomous Airborne Refueling (AAR) of unmanned air vehicles, autonomous shipboard landing for NUCAS and JPALS programs and Ground Based Augmentation System (GBAS). His research interests are focused on high accuracy and high integrity navigation algorithms, cycle ambiguity resolution, high integrity applications, fault monitoring and robust estimation techniques. He was the recipient of the 2011 Institute of Navigation Early Achievement Award for his outstanding contributions to the integrity of carrier phase navigation systems.

Dr. Boris Pervan is a Professor of Mechanical and Aerospace Engineering at IIT, where he conducts research on advanced navigation systems. Prior to joining the faculty at IIT, he was a spacecraft mission analyst at Hughes Aircraft Company (now Boeing) and a postdoctoral research associate at Stanford University. Prof. Pervan received his B.S. from the University of Notre Dame, M.S. from the California Institute of Technology, and Ph.D. from Stanford University. He is an Associate Fellow of the AIAA, a Fellow of the Institute of Navigation (ION), and Editor-in-Chief of the ION journal NAVIGATION. He was the recipient of the IIT Sigma Xi Excellence in University Research Award (2011, 2002), Ralph Barnett Mechanical and Aerospace Dept. Outstanding Teaching Award (2009, 2002), Mechanical and Aerospace Dept. Excellence in Research Award (2007), University Excellence in Teaching Award (2005), IEEE Aerospace and Electronic Systems Society M. Barry Carlton Award (1999), RTCA William E. Jackson Award (1996), Guggenheim Fellowship (Caltech 1987), and Albert J. Zahm Prize in Aeronautics (Notre Dame 1986).

ABSTRACT

In this paper, we propose a novel method to detect Global Navigation Satellite System (GNSS) spoofing using Inertial Navigation Systems (INS) based on inherent noise of spoofed signals. We showed in prior work [21] that a solution separation-based monitor provides detection capability for slowly growing faults. We also demonstrated how the monitor can enable fault exclusion by utilizing an INS-only solution that is not corrupted by prior calibration using spoofed GNSS signals. We proposed utilizing sequence of solution separation monitor windows which allow us to maintain continuous bounded protection level while switching from one window to the next. However, for very slowly growing faults that may be present longer than the run time of a solution separation monitor window, spoofing can go undetected thereby invalidating the fault free assumption required to switch from one window to another. To mount an effective attack of this type, a spoofer would need to closely track the motion of the target to generate the appropriate GNSS signal. It is undeniable, however, that the spoofer would not be able to precisely replicate an authentic GNSS signal because of inherent error in the tracking device, latency of tracking and spoofed signal broadcast, and external environment factors such as wind gusts. In this work, we evaluate the worst-case scenario from missed detection aspect, where a spoofer replicates the authentic GNSS signal with only additive errors due to uncertainty and latency of user's position. We model these tracking errors as additive white noise to the spoofed signal. We observe the changes in the stochastic nature of the Kalman filter position errors over

time—i.e., prior to and after a spoofing onset. We propose a cumulative position domain innovation monitor, which accumulates these tracking errors over time to detect the anomalous temporal structure of the spoofed measurements. We analytically show that accumulated errors result in spectral change of the test statistic with a shift in mean and increased variance. We provide an analytical method to determine the length of the monitor window that would ensure detection of a minimum tracking error with given probability of missed detection requirement. This allows us to choose the length of solution separation monitor windows where detection is ensured to maintain the fault free assumption required to switch from one window to another.

I. Introduction

The civil infrastructure of safety critical fields such as aviation, maritime, and terrestrial navigation rely on GNSS. This brings a major responsibility to ensure absolute GNSS integrity in the system. The civil GNSS signal structure is publicly known and vulnerable to spoofing attacks, which endangers public safety [1]. Spoofing attacks consist of feeding a predetermined faulty signal to the user which may be preceded with intentional jamming of the authentic radio-frequency signals. The fault can be injected to cause gradual position or time offsets. Potential detection techniques include signal processing techniques, cryptographic authentication [2], spoofing discrimination using spatial processing by antenna arrays, automatic gain control schemes [3], [4], GNSS signal direction of arrival comparison [5], code and phase rate consistency checks [6], high-frequency antenna motion [7], and signal power monitoring techniques [8]. 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 (IMU), barometric altimeters, and independent radar sensors to discriminate spoofing has also been proposed [9], [10].

The first stochastic description and quantification of the performance of an IMU-based GNSS spoofing monitor against worst-case faults was introduced by us [11]–[17]. We specifically investigated anti-spoofing solutions utilizing IMUs since essentially all modern vehicles are equipped with them, thereby requiring minimal additional cost or system modification. An IMU is naturally immune to external interference, which makes it an excellent resource to ensure navigation continuity. Additionally, when used in the navigation solution in various integration schemes with GNSS (such as uncoupled, loosely-, tightly-, or ultra-tightly coupled), the INS provides redundancy needed to resist spoofing attacks. In our prior work [14]–[17], we developed a chi-squared innovation sequence-based detector which monitored the accumulated time history of normalized Kalman filter (KF) innovations. The main advantages of KF innovation sequence monitor are that innovations are already computed by the KF, so 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 innovation sequence monitor against worst-case sequences of GNSS faults both analytically and experimentally [17], [18]. The worst-case fault here represents a spoofed GNSS signal profile that maximizes integrity risk. We also analyzed the sensitivity of the innovation sequence monitor against error modeling uncertainties in the INS/GNSS KF structure [19]. The innovation sequence monitor accounts for spoofing detection but does not provide direct exclusion since the INS is being re-calibrated with GNSS during spoofing monitoring. Also, the innovation sequence monitor assumes that the monitor start time was the same as the spoofing onset time and does not have a defined run time.

To address the aforementioned issues of fault exclusion, and monitor start and run time, we developed a solution separation-based monitor which provides better detection capability for slowly growing faults than innovation sequence monitor [21]. We also demonstrated how the solution separation monitor can enable fault exclusion by utilizing an INS-only solution that is not corrupted by prior calibration using spoofed GNSS signals. To address monitor start and run time, we then proposed a sequential window monitoring method which utilizes sequence of solution separation monitors to capture fault onset at any given time epoch. Also, the sequence of monitors allow us to maintain a continuous bounded protection level while switching from one window to the next. For slowly growing faults present longer than the run time of the monitor, spoofing can go undetected. This undetected spoofing will invalidate the fault free assumption required to switch from one window to the next. We need to ensure detection within each window to maintain the fault free assumption required for switching windows.

In this paper we propose a novel method to ensure detection for a window of solution separation monitor. We propose accumulating inherent errors in a spoofed signal due to spoofer's uncertainty of user position —i.e., position tracking error. Instead of observing the innovations where the position tracking errors might be diluted with other state

errors, we observe these errors directly in the position domain. We accumulate these tracking errors using position domain innovation to form a test statistic and derive its distribution. We also analytically derive the relationship between the magnitude of the tracking error and monitor run time required for detection given a probability of false alarm requirement. This in turn allows us to choose the run time of solution separation windows where detection is ensured for a minimum tracking error allowing us to switch from one window to another.

Section II provides the background of the tightly coupled INS/GNSS KF structure used for an en route aircraft and section III contains the background of innovation sequence and solution separation monitor with their limitations. We then introduce the cumulative position domain innovation monitor in section IV with the results for an en route example shown in section V. Finally we conclude this work in section VI while providing some derivations in appendices.

II. Kalman Filter State Model

In this work, we consider an example of an en route scenario where an aircraft utilizes a tightly-coupled INS/GNSS architecture and its position and velocity solution from the KF is used for navigation. En route scenarios are vulnerable to spoofing due to the absence of visual references for the pilot, possible unavailability of navigation error corrections from reference stations, and the time availability for spoofer to slowly deviate the aircraft.

Tightly-coupled INS/GNSS architecture

An INS provides the navigation solution as aircraft position vector $\bar{\mathbf{r}}$ with components x, y, z, velocity vector $\bar{\mathbf{v}}$ with components u, v, w, and attitude ϕ, θ, ψ (Euler angles), using IMU measurements. The aircraft states are,

$$\mathbf{x}_{A/C} = \begin{bmatrix} x & y & z & u & v & w & \phi & \theta & \psi \end{bmatrix}^T \tag{1}$$

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

The IMU measurement $\widetilde{u}$ 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 time-dependent component of bias b, and additive White-Gaussian noise (WGN) η_u as represented in (2). The constant bias is usually specified as bias repeatability and the additive WGN η_u is commonly derived from specifications of velocity random walk (VRW) of accelerometer and angular random walk (ARW) of gyroscope.

$$\widetilde{u} = u^* + b_c + b + \eta_u \tag{2}$$

The time dependent component of the bias b, is modeled as a first order Gauss-Markov random process (GMRP) with time constant τ_b and driving WGN ν_b. This driving WGN ν_b is derived from the specification of bias instability.

$$\dot{b} = -\frac{1}{\tau_b} b + \nu_b \tag{3}$$

The bias dynamics are included in the process model with 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 (4). Equations (1) and (4) show all the nominal states that are propagated to obtain the INS navigation solution.

$$\mathbf{x}_{bias} = \begin{bmatrix} b_{a_x} & b_{a_y} & b_{a_z} & b_{\omega_x} & b_{\omega_y} & b_{\omega_z} \end{bmatrix}^T \tag{4}$$

We assume that an en route aircraft utilizes only single frequency GNSS measurements without any differential corrections, but the idea is also applicable to dual frequency multi constellation GNSS, terminal and precision approach scenarios. Equation (5) shows a simplified GNSS measurement equation where the code measurement ρ for each satellite is composed of true range r, satellite and receiver clock biases dt_{sv} and dt_{rc}, code ionospheric delay I_ρ, code tropospheric delay T_ρ, code mulitpath m_ρ, and receiver code thermal WGN $\nu_{th_{(\rho)}}$. Similarly, the carrier

phase measurement $\lambda\phi$ for each satellite is composed of 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 mulitpath m_ϕ, carrier phase cycle integer ambiguity N_ϕ, and receiver carrier thermal WGN ν_{th_ϕ}. The code ionospheric delay I_ρ is of the same magnitude as carrier ionospheric delay I_ϕ and code tropospheric delay T_ρ is of the same magnitude as carrier tropospheric delay T_ϕ:

$$\begin{bmatrix}\rho\\ \lambda\phi\end{bmatrix} = \begin{bmatrix}r\\ r\end{bmatrix} + \begin{bmatrix}c\,(dt_{rc}-dt_{sv})\\ c\,(dt_{rc}-dt_{sv})\end{bmatrix} + \begin{bmatrix}I_\rho\\ -I_\phi\end{bmatrix} + \begin{bmatrix}T_\rho\\ T_\phi\end{bmatrix} + \begin{bmatrix}m_\rho\\ m_\phi\end{bmatrix} + \begin{bmatrix}0\\ \lambda N_\phi\end{bmatrix} + \begin{bmatrix}\nu_{th_{(\rho)}}\\ \nu_{th_{(\phi)}}\end{bmatrix} \tag{5}$$

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

All GNSS errors need to be accounted for in the measurement in order to be utilized in the KF. Satellite clock offsets cdt_{sv} have a correction model available from the navigation message. After applying the satellite clock offset correction, there are still residual errors due to satellite clock and ephemeris parameter uncertainty. These residual errors r_{sv} are modeled [22] as a first order GMRP with a time constant $\tau_{r_{sv}}$ of 5 hours subject to driving WGN $\nu_{r_{sv}}$ with a standard deviation of 1.8 m. Equation (6) represents the first order GMRP model for satellite clock and ephemeris residual errors.

$$\dot{r}_{sv} = -\frac{1}{\tau_{r_{sv}}} r_{sv} + \nu_{r_{sv}} \tag{6}$$

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 (7),

$$\begin{bmatrix}\dot{r}_{rc}\\ \ddot{r}_{rc}\end{bmatrix} = \begin{bmatrix}0 & 1\\ 0 & 0\end{bmatrix}\begin{bmatrix}r_{rc}\\ \dot{r}_{rc}\end{bmatrix} + \begin{bmatrix}w_{r_{rc}}\\ w_{\dot{r}_{rc}}\end{bmatrix} \tag{7}$$

where, $w_{r_{rc}}$ and $w_{\dot{r}_{rc}}$ are WGN for clock offset and clock offset drift rate, respectively. The variance of these WGN is obtained using typical Allan Variance coefficients of TCXO 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 modeled in [20] to have a standard deviation given by equation (8),

$$\sigma_i = \sqrt{\max\left[(\tfrac{cT_{iono}}{5})^2, (F_{pp}\tau_{vert})^2\right]} \tag{8}$$

where, F_{pp} is the obliquity factor and τ_{vert} is calculated given the geomagnetic latitude [20]. Since ionospheric delay is a slow changing error it is modeled as a first order GMRP with a time constant of 40 hours and driving WGN ν_{r_i} shown as,

$$\dot{r}_i = -\frac{1}{\tau_{r_i}} r_i + \nu_{r_i} \tag{9}$$

The troposheric delay is corrected with the correction model specified in [20] and the residual errors r_t in the zenith direction are modeled as a first order GMRP with a time constant of 20 hours and a standard deviation 0.09 $m(el)$ (meters) [23]. $m(el)$ is the mapping function of satellite elevation. Equation (10) shows the first order GMRP model of tropospheric residual error r_t,

$$\dot{r}_t = -\frac{1}{\tau_{r_t}} r_t + \nu_{r_t} \tag{10}$$

where, ν_{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 seconds and driving WGN ν_m [20] .

$$\dot{m} = -\frac{1}{\tau_m} m + \nu_m \tag{11}$$

The standard deviation for code multipath error is 5 m and for carrier multipath error we assume it to be 0.02 m [20] .

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

$$\mathbf{x}_{GNSS} = \begin{bmatrix} {r_{sv}}^{1:n} & r_{rc} & \dot{r}_{rc} & {r_i}^{1:n} & {r_t}^{1:n} & m_\rho^{1:n} & m_\phi^{1:n} & \lambda N_\phi^{1:n} \end{bmatrix}^T \tag{12}$$

where, n is the number of satellites.

The final state vector of the INS/GNSS system is

$$\mathbf{x} = \begin{bmatrix} \mathbf{x}_{A/C} & \mathbf{x}_{bias} & \mathbf{x}_{GNSS} \end{bmatrix}^T \tag{13}$$

The dynamics of the augmented system is perturbed to obtain the linear error-state ($\delta\mathbf{x}$) process model to be utilized in the KF. The error-state process model in discrete time can be represented as,

$$\delta\mathbf{x}_{k+1} = \Phi_k\, \delta\mathbf{x}_k + \Gamma_{w_k}\, \mathbf{w}_k \tag{14}$$

where, Φ is the state transition matrix, Γ_w is the process noise model, and $\mathbf{w}$ is the additive white noise with a respective process noise covariance $\mathbf{Q}$.

The error-state measurement model in discrete time is represented as,

$$\delta\mathbf{z}_k = \mathbf{H}_k\, \delta\mathbf{x}_k + \nu_k \tag{15}$$

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

III. Innovation sequence and solution separation monitors

The innovation sequence-based monitor is a chi-squared monitor which utilizes cumulative normalized innovations from a KF as the test statistic, and compares it against a threshold [17]. The innovation vector γ at time epoch k is defined as

$$\gamma_k = \delta\mathbf{z}_k - \mathbf{H}_k\, \delta\bar{\mathbf{x}}_k \tag{16}$$

where, $\delta\bar{\mathbf{x}}$ is the a priori error state vector.

A cumulative test statistic q_k is defined as the sum of squares of the normalized innovation vectors over time as

$$q_k = \sum_{i=1}^{k} \gamma_i^T\, \mathbf{S}_i^{-1}\, \gamma_i \tag{17}$$

where, $\mathbf{S}_i$ is the innovation vector covariance matrix at time epoch i.

For a given false alarm rate requirement under fault free scenario, the threshold T_k^2 is determined from the inverse chi-square cumulative distribution function (CDF). The monitor simply checks whether the test statistic q_k is smaller than a predefined threshold T_k^2 as

$$q_k \gtrless T_k^2 \tag{18}$$

Due to limitations of the innovation sequence monitor mentioned earlier in the paper, we proposed the sequential solution separation monitor. The solution separation monitor is based on the difference of position solution between a faulty full-set (INS and GNSS) KF solution $\hat{\mathbf{X}}_{KF_k}$ and a fault-free subset INS-only solution $\overline{\mathbf{X}}_{c_k}$. The test statistic at any time k is defined as,

$$q_k = \hat{\mathbf{X}}_{KF_k} - \overline{\mathbf{X}}_{c_k} \tag{19}$$

The covariance for the test statistic is given by [21],

$$\mathbf{P}_k = \overline{\mathbf{P}}_{c_k} - \hat{\mathbf{P}}_{KF_k} \tag{20}$$

where, $\hat{\mathbf{P}}_{KF_k}$ is the position error covariance for $\hat{\mathbf{X}}_{KF_k}$ and $\overline{\mathbf{P}}_{c_k}$ is the position error covariance for $\overline{\mathbf{X}}_{c_k}$. The threshold for the test statistic is obtained using the false alarm requirement and inverse CDF of the Gaussian distribution.

A major limitation of the solution separation monitor is the ever increasing protection level. Predefined alert limits do not allow for the protection levels to grow infinitely and an aircraft would need to maintain protection levels less than the alert limit. Thus, a solution separation monitor would have a fixed run time until the protection level

reaches a certain predetermined value. One way monitor run time can be determined is the time required for the protection level to reach a given maximum value. To maintain a bounded protection level we proposed in our prior work a sequence of solution separation monitor windows [24]. Fig. 1 illustrates the concept of sequential window monitors each with its own increasing protection level. To maintain a bounded protection level over time we switch from one monitor window to the next. Since we switch windows to maintain the bounded protection level, this requires fault free assumption for the prior window, or accounting for prior windows missed detection probabilities in the current computation of the protection level.

The increasing nature of protection level of solution separation monitor comes from the increasing nature of test statistic covariance, and causes the threshold to increase over time as well. For faults growing slower than the rate of threshold, spoofing will go undetected and thus invalidate the fault free assumption required to switch from one window to the next. Thus, we need a separate detection method which can ensure that for a given run time of solution separation window, there was no spoofing allowing us to switch from one window to the next. We analytically derive this monitor window length N in the next section which is the run time for each monitor window. We will observe that monitor run time will not be a function of some predetermined maximum protection level but will depend on the detection capability of the new monitor.

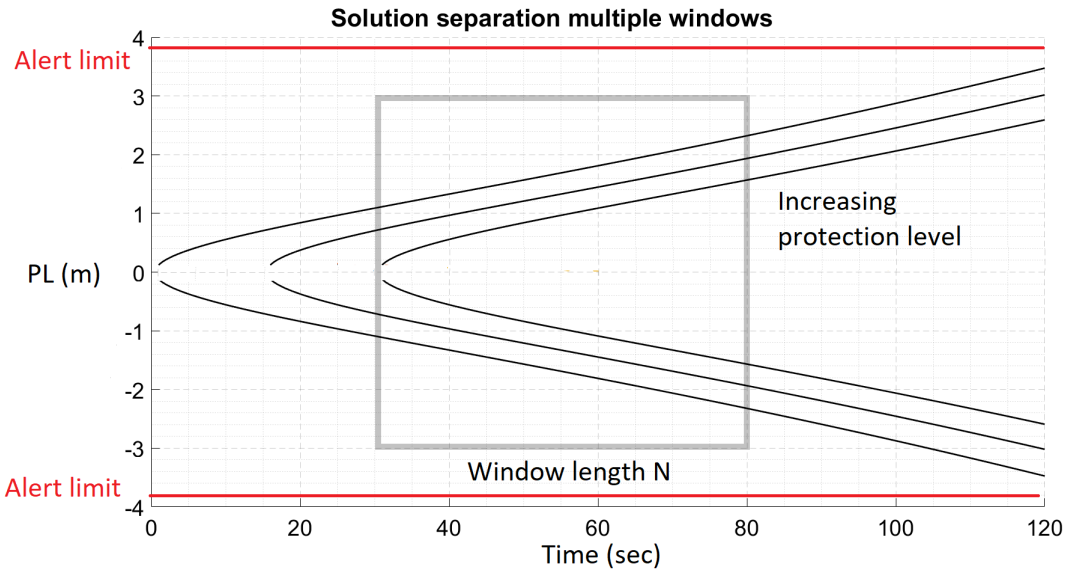

Fig. 1: Illustration of solution separation sequential monitor windows with increasing protection levels.

To formulate this new detection method, we look in detail at the mechanism of spoofing. In order to slowly divert an aircraft from its planned path, the spoofer would replicate an authentic signal and then send a higher power spoofed signal to the aircraft. Once the aircraft locks into the spoofed signal, the spoofer then would inject very small deviations and thus divert the aircraft over time. Although the attacker tries to broadcast a signal that mimics the authentic one in order to go unnoticed, it practically is infeasible to broadcast an exact replica. The reason being that the spoofer needs the aircraft's antenna exact location to construct the spoofed signal. Any uncertainty in aircraft antenna position would eventually appear as errors in the spoofed signal. Since the spoofer would have to use some sort of tracking device to locate the aircraft, we refer to these position uncertainties as tracking errors.

In this work, we aim to detect even spoofing scenarios that only include these tracking errors. Any additional fault that the spoofer injects would be even easier to detect. Therefore, our proposed detection method would detect spoofing even before spoofer injects any small deviations or faults to the spoofed signal. In other words, our detection methods would work even if the spoofer decides to send a spoofed signal which mimics the authentic signal for a long time given only small inherent noise in the signal.

IV. Cumulative position domain innovation monitor

In appendix C, we show how tracking error appears in spoofed measurements as an additive term.

$$\mathbf{z}_{k+1}^{s} = \mathbf{z}_{k+1} + \mathbf{H}_{k+1}\nu_t \tag{21}$$

where, $\mathbf{z}_{k+1}^{s}$ is the spoofed measurement vector $\mathbf{z}_k$ is the actual measurement vector, $\mathbf{H}_k$ is the observation matrix, and ν_t is the column vector with tracking error for all the position states.

We can observe these tracking errors in the innovation vector as it contains the difference between GNSS measurement and the predicted measurement of the process model with INS measurements. Since the innovation vector contains all the states, the position tracking errors would be diluted due to presence of errors from other states such as multipath. A better way to observe these tracking errors would be to directly observe the position errors by transforming the innovation vector in the position domain. In our prior work [24], we developed the position domain innovation monitor. In Appendix B, we define the position domain innovation ($\Delta\mathbf{x}$) which is the state error vector obtained after the innovation vector is transformed to the state domain. From the state error vector we extract a single position state error (say z position) for any time k as,

$$\Delta z_k = \mathbf{u}^T\mathbf{L}_k(\mathbf{z}_k - \mathbf{H}_k\bar{\mathbf{x}}_k) \tag{22}$$

where, $\bar{\mathbf{x}}_k$ is the a-priori state, $\mathbf{L}_k$ is the Kalman gain matrix and u^T is the single row vector that extracts the state error along the desired position direction.

This position domain innovation has the following distribution.

$$\Delta z_k \sim \mathcal{N}(0, \mathbf{u}^T\mathbf{L}_k(\mathbf{H}_k\overline{\mathbf{P}}_k\mathbf{H}_k^T + \mathbf{V}_k)\mathbf{L}_k^T\mathbf{u}) \tag{23}$$

where, $\mathbf{V}_k$ is the measurement error covariance.

We define scalar variance for Δz_k and as,

$$\sigma_{\Delta z_k}^2 \cong \mathbb{E}(\Delta z_k \Delta z_k{}^T) = \mathbf{u}^T\mathbf{L}_k(\mathbf{H}_k\overline{\mathbf{P}}_k\mathbf{H}_k^T + \mathbf{V}_k)\mathbf{L}_k^T\mathbf{u} \tag{24}$$

When a spoofer sends a spoofed signal mimicking the authentic signal with some inherent additive noise, this additive noise can be observed in the position domain innovation. In Appendix C, we show how tracking error affects the position domain innovation. We model these tracking errors as white Gaussian noise ν_t distributed as $\mathcal{N}(0, \sigma_t^2)$. These tracking errors affect the position domain innovation with no change in mean but increasing the variance. Note that superscript s is used to denote terms related to the spoofer. If we define Δz_k^s as the position domain innovation which includes the tracking error then,

$$\Delta z_k^s = \mathbf{u}^T\Delta\mathbf{x}_k + \mathbf{u}^T\mathbf{L}_k\mathbf{H}_k\nu_t \tag{25}$$

The distribution for this spoofed position domain innovation is,

$$\Delta z_k^s \sim \mathcal{N}(0, \mathbf{u}^T\mathbf{L}_k(\mathbf{H}_k\overline{\mathbf{P}}_k\mathbf{H}_k^T + \mathbf{V}_k)\mathbf{L}_k^T\mathbf{u} + \mathbf{u}^T\mathbf{L}_k\mathbf{H}_k\mathbf{R}_t\mathbf{H}_k^T\mathbf{L}_k^T\mathbf{u}) \tag{26}$$

where, $\mathbf{R}_t$ is the error covariance for the tracking error.

Also, if we define,

$$\sigma_{\Delta z_t}^2 \cong \mathbf{u}^T\mathbf{L}_k\mathbf{H}_k\mathbf{R}_t\mathbf{H}_k^T\mathbf{L}_k^T\mathbf{u} \tag{27}$$

then we can write the scalar variance of spoofed z position domain innovation as,

$$\sigma_{\Delta z_k^s}^2 = \sigma_{\Delta z_k}^2 + \sigma_{\Delta z_t}^2 \tag{28}$$

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

$$\Delta z_k \sim \mathcal{N}(0, \sigma_{\Delta z_k}^2) \tag{29}$$

$$\Delta z_k^s \sim \mathcal{N}(0, \sigma_{\Delta z_k}^2 + \sigma_{\Delta z_t}^2) \tag{30}$$

If we observe just the position domain innovation at each time epoch for detection, then for a small tracking errors this change in variance might not provide detection. We propose accumulating these errors over time for

detection and form the position domain innovations squared as a test statistic. For the period of accumulation N we define our test statistic as,

$$q_N = \sum_{k=1}^{N} \Delta z_k{}^2 \tag{31}$$

In Appendix A, we show that a scalar normal random variable squared follows a gamma distribution. A gamma distribution $Gamma(k,\theta)$ is defined by its shape parameter k and scale parameter θ. Utilizing this result from Appendix A, we can write the distribution of square of z position domain innovation as,

$$\Delta z_k{}^2 \sim Gamma\left(\frac{1}{2}, 2\sigma^2_{\Delta z_k}\right) \tag{32}$$

Similarly, for the spoofed case we will get,

$$(\Delta z^s_k)^2 \sim Gamma\left(\frac{1}{2}, 2\sigma^2_{\Delta z^s_k}\right) = Gamma\left(\frac{1}{2}, 2\left(\sigma^2_{\Delta z_k} + \sigma^2_{\Delta z_t}\right)\right) \tag{33}$$

Also, from summation property, the sum of gamma distributed random variables is also gamma distributed as shown in Appendix A. The assumptions made for this summation is that for a given period of time, the change in variance of the position domain innovation is negligible. Thus, the test statistic q_N has gamma distribution as,

$$\sum_{k=1}^{N} \Delta z_k{}^2 \sim Gamma\left(\sum_{k=1}^{N} \frac{1}{2}, 2\sigma^2_{\Delta z}\right) = Gamma\left(\frac{N}{2}, 2\sigma^2_{\Delta z}\right) \tag{34}$$

where, $\sigma^2_{\Delta z} = \sigma^2_{\Delta z_1} = \sigma^2_{\Delta z_2} = ... = \sigma^2_{\Delta z_k} = \mathbf{u}^T \mathbf{L}_k (\mathbf{H}_k \overline{\mathbf{P}}_k \mathbf{H}_k^T + \mathbf{V}_k) \mathbf{L}_k^T \mathbf{u}$.

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

$$T_N = F^{-1}\left(P_{FA} \;\middle|\; \frac{N}{2}, 2\sigma^2_{\Delta z}\right) \tag{35}$$

where, F^{-1} is the inverse CDF function of gamma distribution.

In the spoofed case where the tracking error is embedded in the test statistic, the distribution of test statistic changes to,

$$\sum_{k=1}^{N} (\Delta z^s_k)^2 \sim Gamma\left(\sum_{k=1}^{N} \frac{1}{2}, 2\left(\sigma^2_{\Delta z} + \sigma^2_{\Delta z_t}\right)\right) = Gamma\left(\frac{N}{2}, 2\left(\sigma^2_{\Delta z_k} + \sigma^2_{\Delta z_t}\right)\right) \tag{36}$$

where, $\sigma^2_{\Delta z_t} = \mathbf{u}^T \mathbf{L}_k \mathbf{H}_k \mathbf{R}_t \mathbf{H}_k^T \mathbf{L}_k^T \mathbf{u}$ and $\mathbf{R}_t$ is the covariance for the tracking error.

From (36) we can see that tracking error causes the scale parameter of the test statistic distribution to change. For a gamma distribution with shape parameter k and scale parameter θ, using moment generating function, we know that the mean and variance are $k\theta$ and $k\theta^2$, respectively. In order to understand how the tracking error helps with detection, we take the large N approximation for gamma distribution. For large values of N,

$$Gamma(k,\theta) \approx \mathcal{N}(k\theta, k\theta^2) \tag{37}$$

Thus, the distributions for spoof free and spoofed case can be approximated for large N as,

$$\sum_{k=1}^{N} \Delta z_k{}^2 \sim Gamma\left(\frac{N}{2}, 2\sigma^2_{\Delta z}\right) \approx \mathcal{N}\left(N\sigma^2_{\Delta z}, 2N\sigma^4_{\Delta z}\right) \tag{38}$$

$$\sum_{k=1}^{N} (\Delta z^s_k)^2 \sim Gamma\left(\frac{N}{2}, 2\left(\sigma^2_{\Delta z} + \sigma^2_{\Delta z_t}\right)\right) \approx \mathcal{N}\left(N\left(\sigma^2_{\Delta z} + \sigma^2_{\Delta z_t}\right), 2N\left(\sigma^2_{\Delta z} + \sigma^2_{\Delta z_t}\right)^2\right) \tag{39}$$

It is clear from the above two equations that the tracking error causes the mean of the test statistic q_N distribution to shift by $N\sigma^2_{\Delta z_t}$ and increases its variance by $2N\sigma^4_{\Delta z_t} + 4N\sigma^2_{\Delta z}\sigma^2_{\Delta z_t}$, which is illustrated in Fig. 2. Although the tracking error shifts the mean of the distribution and helps with detection, the increase in variance slightly increases the likelihood of missed detection. Thus, there is a trade-off between mean shift and increase in variance which

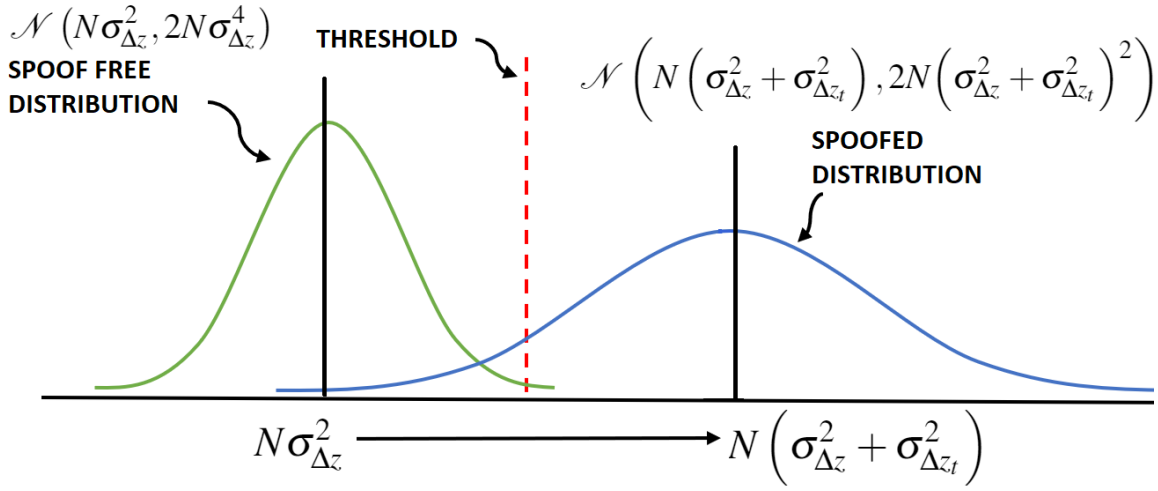

Fig. 2: Illustration of change in test statistic q_N distribution due to tracking error.

limits the minimum tracking error that can be detected. We will observe in the results section that the shift in mean eventually dominates the increase in variance with increasing N and $\sigma_{\Delta z_t}$.

Now given the above equations, we can determine the probability of missed detection as,

$$P_{MD} = \Phi\left(\frac{-\Phi^{-1}\left(\frac{P_{FA}}{2}\right)\sigma_{\Delta z}^2 - N\sigma_{\Delta z_t}^2}{\sqrt{2N}\left(\sigma_{\Delta z}^2+\sigma_{\Delta z_t}^2\right)}\right) \tag{40}$$

Recall in section III we introduced the motivation for this work as determining a new monitor which would ensure detection for a run time N of solution separation window. The developed cumulative position domain innovation monitor ensures detection with a missed detection rate P_{MD}, within run time N, given spoofer's tracking error magnitude exceeding σ_t. Thus, we propose running a cumulative position domain innovation monitor within each solution separation monitor window. The cumulative position domain innovation monitor would ensure detection with acceptable P_{MD}, thereby allowing to maintain the fault free assumption required to switch from one solution separation window to the next. Given that spoofer's tracking error is bound to exceed a magnitude of σ_t, equation (40) would allow to determine the required run time N such that spoofing is detected with a missed detection rate P_{MD}. With the run time N determined we can now ensure a corresponding bounded protection level. In the next section, we discuss the relationship between tracking error magnitude and monitor run time and an en route example result is shown.

V. Results

In Fig. 3 we illustrate the analytical relationship between monitor run time N, tracking error magnitude σ_t and probability of missed detection P_{MD}. The missed detection rate decreases with increasing the run time as more errors are accumulated over time and shift the mean of test statistic distribution as shown in equation (39). Similarly, increasing tracking error magnitude contributes to shift of mean of test statistic which reduces P_{MD}.

We perform en-route simulations for an aircraft utilizing a navigation grade IMU and single frequency GPS measurements. The spoofer tracks the aircraft with inherent tracking errors to generate and broadcast counterfeit spoofed signals. The spoofed signal are replica of the authentic signals with only additive zero mean white Gaussian noise. We chose a monitor run time of 150 seconds with GNSS frequency of 2 Hz (i.e. $N = 300$) and a false alarm rate requirement of 10^{-5}. Although, we can take credit for 3-dimensional tracking errors, we conservatively assume the error is one dimensional and ignore the other two in this analysis. Fig. 4 shows the performance of the cumulative position domain innovation monitor for different tracking error magnitudes. The monitor is able to detect spoofing for tracking error as small as 2 cm for the given monitor run time.

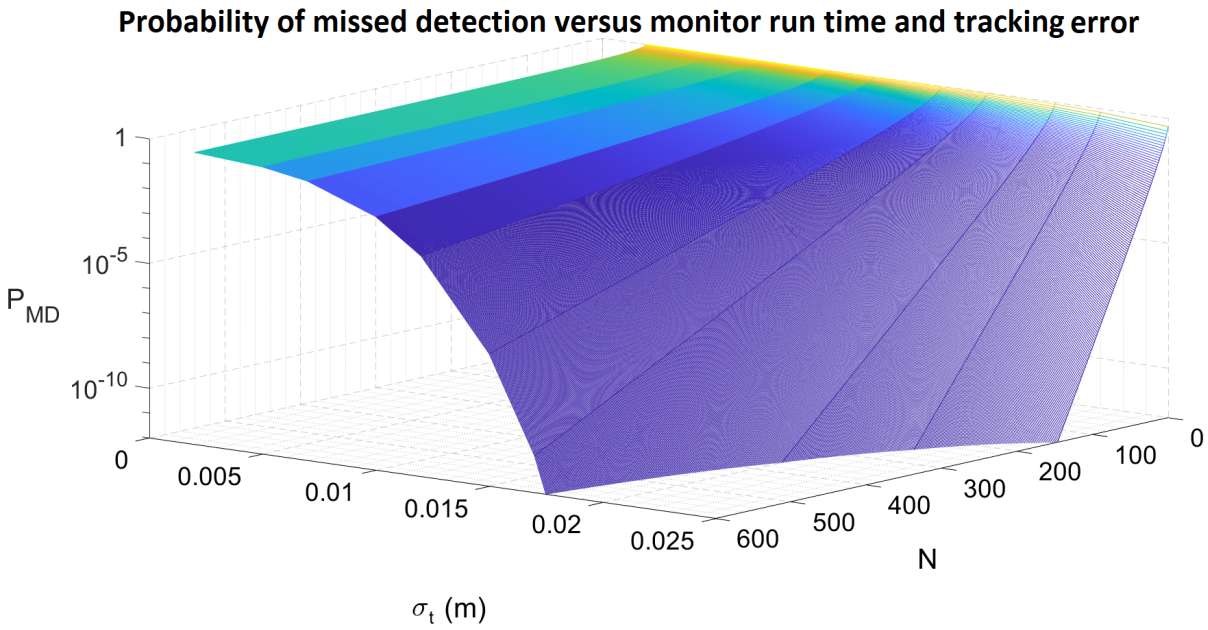

Fig. 3: Illustration of probability of missed detection P_{MD} for given tracking error σ_t and monitor run time N.

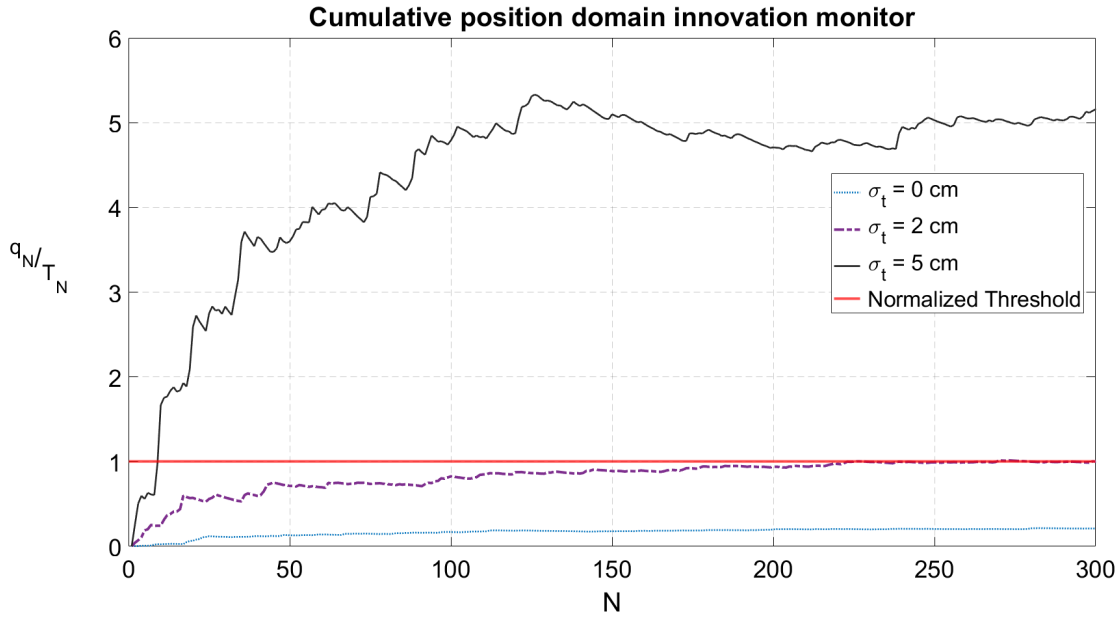

Fig. 4: Monitor performance for different tracking error magnitude.

More realistically, spoofer's tracking error would be more in the decimeter range due to multiple factors such as the long range of spoofer from the aircraft, inherent noise of tracking device, latency of tracking and signal broadcast, spoofer's uncertainty of aircraft lever arms, wind gusts etc. Even if the attacker can overcome most of these obstacles and assume a non-realistic 5cm tracking error can be achieved, the monitor detects the attack within a few seconds. Therefore, this monitor may also cover critical scenarios such as aircraft approach and landing where

aircraft time to alert or protection level is tighter. As a first step we modeled the spoofer tracking error as white Gaussian noise and aim to analyze the performance of the monitor for tracking errors modeled as colored noise in the future.

VI. Conclusion

In this work, we propose a cumulative position domain innovation monitor which accumulates tracking error in spoofer's signal for detection. We analytically derive equations to relate missed detection rate, tracking error magnitude and monitor run time. We also address the monitor run time for sequence of solution separation monitor windows by proposing that we run the cumulative position domain innovation monitor in conjunction to ensure detection and allow switching of windows. We analytically prove that even with centimeter level tracking error, the monitor can detect spoofing with low probability of missed detection.

VII. Appendix

A. Distribution of scalar normal random variable squared

Consider a scalar normal random variable X, which has the following distribution,

$$X \sim \mathcal{N}(0, \sigma^2) \tag{41}$$

The square of the normal random variable can be represented as another random variable Y and can be written as,

$$Y = X^2 \tag{42}$$

In order to determine the distribution of this new random variable Y, we first evaluate the cumulative distribution function (CDF) of Y and then take its derivative to get the probability density function (PDF). The CDF for the random variable Y evaluated at x can be written as the probability that Y will take a value less than or equal to x. This is shown below as,

$$F_Y(x) = F_{X^2}(x) = P(X^2 \leq x) = P(-\sqrt{x} \leq X \leq \sqrt{x}) \tag{43}$$

The above CDF equation can be written in terms of integral of PDF as,

$$P(-\sqrt{x} \leq X \leq \sqrt{x}) = \int_{-\sqrt{x}}^{\sqrt{x}} \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{t^2}{2\sigma^2}} dt \tag{44}$$

Now to obtain the PDF of X^2, we differentiate the CDF as,

$$f_{X^2}(x) = \frac{\mathrm{d}}{\mathrm{d}x} \int_{-\sqrt{x}}^{\sqrt{x}} \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{t^2}{2\sigma^2}} dt \tag{45}$$

For differentiating the CDF we use the Leibniz rule of differentiating an integral. If,

$$\Phi(x) = \int_{a(x)}^{b(x)} g(t,x) dt \tag{46}$$

then, its derivative with respect to x is given by,

$$\frac{\mathrm{d}}{\mathrm{d}x}\Phi(x) = \int_{a(x)}^{b(x)} \frac{\partial}{\partial x} g(t,x) dt + g(b(x),x)\frac{\mathrm{d}}{\mathrm{d}x}b(x) - g(a(x),x)\frac{\mathrm{d}}{\mathrm{d}x}a(x) \tag{47}$$

For our case,

$$\Phi(x) = \int_{-\sqrt{x}}^{\sqrt{x}} \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{t^2}{2\sigma^2}} dt \tag{48}$$

Thus, we get the derivative as,

$$f_{X^2}(x) = \int_{-\sqrt{x}}^{\sqrt{x}} \frac{\partial}{\partial x} \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{t^2}{2\sigma^2}} dt + \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{(\sqrt{x})^2}{2\sigma^2}} \frac{\mathrm{d}}{\mathrm{d}x}\sqrt{x} - \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{(-\sqrt{x})^2}{2\sigma^2}} \frac{\mathrm{d}}{\mathrm{d}x} - \sqrt{x} \tag{49}$$

The first term of the equation above becomes zero and we get,

$$f_{X^2}(x) = \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{x}{2\sigma^2}} \frac{1}{2\sqrt{x}} + \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{x}{2\sigma^2}} \frac{1}{2\sqrt{x}} \tag{50}$$

Simplifying further,

$$f_{X^2}(x) = \frac{1}{\sqrt{2\pi}\sigma} \frac{1}{\sqrt{x}} e^{-\frac{x}{2\sigma^2}} \tag{51}$$

We know that the PDF of a gamma distribution with shape parameter k and scale parameter θ is given by,

$$f(x) = \frac{1}{\Gamma(k)\,\theta^k} x^{k-1} e^{-\frac{x}{\theta}} \tag{52}$$

where, Γ is the Gamma function. We can rewrite the PDF of X^2 as the general form of PDF of gamma function as,

$$f_{X^2}(x) = \frac{1}{\sqrt{\pi}(2\sigma^2)^{\frac{1}{2}}} x^{\frac{1}{2}-1} e^{-\frac{x}{2\sigma^2}} \tag{53}$$

Using $\Gamma(\frac{1}{2}) = \sqrt{\pi}$, we get,

$$f_{X^2}(x) = \frac{1}{\Gamma(\frac{1}{2})(2\sigma^2)^{\frac{1}{2}}} x^{\frac{1}{2}-1} e^{-\frac{x}{2\sigma^2}} \tag{54}$$

Comparing the above equation to the general PDF of a gamma distribution, we can see that the PDF of X^2 is gamma distributed with shape parameter $k = \frac{1}{2}$ and scale parameter $\theta = 2\sigma^2$. As an illustration, if we consider a special case of standard normal variable i.e. $\sigma = 1$, we get the PDF as,

$$f_{X^2_{\sigma=1}}(x) = \frac{1}{\sqrt{2\pi}} x^{\frac{1}{2}-1} e^{-\frac{x}{2}} \tag{55}$$

The PDF of a chi-square distribution with degrees of freedom k is,

$$f(x) = \frac{1}{\Gamma(\frac{k}{2}) 2^{\frac{k}{2}}} x^{\frac{k}{2}-1} e^{-\frac{x}{2}} \tag{56}$$

If we substitute $k = 1$, we get the PDF of standard normal random variable squared. Thus, we can see that scalar standard normal random variable squared has a chi-squared distribution with a single degree of freedom. Also, this chi-squared distribution is a special case of gamma distribution with shape parameter $k = \frac{1}{2}$ and scale parameter $\theta = 2$.

If we take the cumulative sum of the normal random variables squared, the distribution of this sum can be evaluated using the summation property of random variables with gamma distribution. The summation property states that if the random variables $Y_i \sim Gamma(k_i, \theta)$ are independent then,

$$\sum_{i=1}^{N} Y_i \sim Gamma\left(\sum_{i=1}^{N} k_i, \theta\right) \tag{57}$$

B. Position domain innovation

In a Kalman filter structure the innovation at at time k is,

$$\gamma_k = \mathbf{z}_k - \mathbf{H}_k \bar{\mathbf{x}}_k \tag{58}$$

where, $\mathbf{z}_k$ is the measurement vector, $\mathbf{H}_k$ is the observation matrix and $\bar{\mathbf{x}}_k$ is the a-priori state. The state error vector of size $n \times 1$, where n is the number of states, can be written as,

$$\Delta\mathbf{x}_k = \mathbf{L}_k(\mathbf{z}_k - \mathbf{H}_k \bar{\mathbf{x}}_k) \tag{59}$$

where, $\mathbf{L}_k$ is the Kalman gain. In order to observe just one state error (say z position), we would use a single row vector u^T that extracts the desired position direction as,

$$\Delta z_k = \mathbf{u}^T \mathbf{L}_k(\mathbf{z}_k - \mathbf{H}_k \bar{\mathbf{x}}_k) = \mathbf{u}^T \mathbf{L}_k \gamma_k \tag{60}$$

Since, $\mathbb{E}(\gamma_k) = 0$, then $\mathbb{E}(\Delta z_k) = 0$. Also using the result that $\mathbb{E}(\gamma_{k+1}{\gamma_k}^T) = 0$, it can similarly be shown that $\mathbb{E}(\Delta z_{k+1}{\Delta z_k}^T) = 0$. The variance for the innovation vector γ_k is given by,

$$\mathbb{E}(\gamma_k{\gamma_k}^T) = \mathbf{H}_k\overline{\mathbf{P}}_k\mathbf{H}_k^T + \mathbf{V}_k \tag{61}$$

where, $\overline{\mathbf{P}}_k$ is the a-priori state error covariance and $\mathbf{V}_k$ is the measurement error covariance. Thus, the variance for Δz_k is,

$$\sigma^2_{\Delta z_k} \cong \mathbb{E}(\Delta z_k{\Delta z_k}^T) = \mathbf{u}^T\mathbf{L}_k(\mathbf{H}_k\overline{\mathbf{P}}_k\mathbf{H}_k^T + \mathbf{V}_k)\mathbf{L}_k^T\mathbf{u} \tag{62}$$

C. Effect of tracking error on position domain innovation

We define the user position uncertainty of the spoofer as the tracking error and assume that it is a zero mean Gaussian white noise and distributed as,

$$\nu_t \sim \mathcal{N}(0, \sigma_t^2) \tag{63}$$

We will use the subscript s for terms that are related to the spoofer or spoofed signal. At time k, the spoofer estimates the user position with tracking error given as,

$$\begin{bmatrix} x_k^s \\ y_k^s \\ z_k^s \end{bmatrix} = \begin{bmatrix} x_k \\ y_k \\ z_k \end{bmatrix} + \begin{bmatrix} \nu_{t_x} \\ \nu_{t_y} \\ \nu_{t_z} \end{bmatrix} \tag{64}$$

where, x_k, y_k, z_k are actual user position. We conservatively assume that the spoofer does not have any uncertainty in the user's velocity v_k and predicts the user future position at time $k+1$ as,

$$\begin{bmatrix} x_{k+1}^s \\ y_{k+1}^s \\ z_{k+1}^s \end{bmatrix} = \begin{bmatrix} x_k^s \\ x_k^s \\ x_k^s \end{bmatrix} + \begin{bmatrix} u_k \\ v_k \\ w_k \end{bmatrix} \Delta t \tag{65}$$

where, Δt is the time interval after which the user receives GPS signals. We also assume the worst case scenario where the spoofer has negligible uncertainty for all the other states of the Kalman filter as well as knowlegde of the Kalman filter structure. Thus, the spoofer creates the state vector $\mathbf{x}_{k+1}^s$ with all the other states to be transformed into range domain as,

$$\mathbf{z}_{k+1}^s = \mathbf{H}_{k+1}\mathbf{x}_{k+1}^s \tag{66}$$

The user then receives this spoofed measurement with receiver thermal noise ν_{th} as,

$$\mathbf{z}_{k+1}^s = \mathbf{H}_{k+1}\mathbf{x}_{k+1}^s + \nu_{th} \tag{67}$$

Expanding the above equation,

$$\mathbf{z}_{k+1}^s = \mathbf{H}_{k+1}\mathbf{x}_{k+1} + \mathbf{H}_{k+1}\nu_t + \nu_{th} \tag{68}$$

where, ν_t is the column vector with tracking error for all the position states. Rearranging the above equation we get,

$$\mathbf{z}_{k+1}^s = \mathbf{H}_{k+1}\mathbf{x}_{k+1} + \nu_{th} + \mathbf{H}_{k+1}\nu_t = \mathbf{z}_{k+1} + \mathbf{H}_{k+1}\nu_t \tag{69}$$

Now, the innovation vector due to spoofed measurements is given as,

$$\gamma_{k+1}^s = \mathbf{z}_{k+1}^s - \mathbf{H}_{k+1}\bar{\mathbf{x}}_{k+1} = \mathbf{z}_{k+1} + \mathbf{H}_{k+1}\nu_t - \mathbf{H}_{k+1}\bar{\mathbf{x}}_{k+1} \tag{70}$$

Rearranging the above equation we get,

$$\gamma_{k+1}^s = \mathbf{z}_{k+1} - \mathbf{H}_{k+1}\bar{\mathbf{x}}_{k+1} + \mathbf{H}_{k+1}\nu_t = \gamma_{k+1} + \mathbf{H}_{k+1}\nu_t \tag{71}$$

Thus, the position domain innovation can be written as,

$$\Delta\mathbf{x}_{k+1}^s = \mathbf{L}_{k+1}(\gamma_{k+1} + \mathbf{H}_{k+1}\nu_t) = \Delta\mathbf{x}_{k+1} + \mathbf{L}_{k+1}\mathbf{H}_{k+1}\nu_t \tag{72}$$

We can see that $\mathbb{E}(\Delta\mathbf{x}_{k+1}^s) = 0$ and the variance is given by,

$$\mathbb{E}(\Delta\mathbf{x}_{k+1}^s{\Delta\mathbf{x}_{k+1}^s}^T) = \mathbf{L}_{k+1}(\mathbf{H}_{k+1}\overline{\mathbf{P}}_{k+1}\mathbf{H}_{k+1}^T + \mathbf{V}_k)\mathbf{L}_{k+1}^T + \mathbf{L}_{k+1}\mathbf{H}_{k+1}\mathbf{R}_t\mathbf{H}_{k+1}^T\mathbf{L}_{k+1}^T \tag{73}$$

where, $\mathbf{R}_t$ is the covariance for the tracking errors, given as,

$$\mathbf{R}_t = \begin{bmatrix} \sigma_t^2 & 0 & 0 & \dots & 0 \\ 0 & \sigma_t^2 & & & \\ 0 & 0 & \sigma_t^2 & & \\ \vdots & & & \ddots & \vdots \\ 0 & & & \dots & 0 \end{bmatrix}_{n \times n} \tag{74}$$

and n is the number of states. Extracting z position error state using u^T and for simplicity taking the above equations for time k we get,

$$\Delta z_k^s = \mathbf{u}^T \Delta \mathbf{x}_k + \mathbf{u}^T \mathbf{L}_k \mathbf{H}_k \nu_t = \Delta z_k + \mathbf{u}^T \mathbf{L}_k \mathbf{H}_k \nu_t \tag{75}$$

The scalar variance is then given by,

$$\mathbb{E}(\Delta z_k^s \Delta z_k^{s\,T}) = \mathbf{u}^T \mathbf{L}_k (\mathbf{H}_k \overline{\mathbf{P}}_k \mathbf{H}_k^T + \mathbf{V}_k) \mathbf{L}_k^T \mathbf{u} + \mathbf{u}^T \mathbf{L}_k \mathbf{H}_k \mathbf{R}_t \mathbf{H}_k^T \mathbf{L}_k^T \mathbf{u} \tag{76}$$

If we define,

$$\sigma_{\Delta z_t}^2 \cong \mathbf{u}^T \mathbf{L}_k \mathbf{H}_k \mathbf{R}_t \mathbf{H}_k^T \mathbf{L}_k^T \mathbf{u} \tag{77}$$

then we can write the scalar variance of spoofed z position domain innovation as,

$$\sigma_{\Delta z_k^s}^2 = \sigma_{\Delta z_k}^2 + \sigma_{\Delta z_t}^2 \tag{78}$$

REFERENCES

[1] Humphreys T. E., Ledvina B. M., Psiaki M. L., and O'Hanlon B. W., "Assessing the spoofing threat: development of a portable GPS civilian spoofer," *Proceedings of the 21st International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2008), Savannah, GA*, September 2008, pp. 2314-2325.

[2] Wesson K. D., Rothlisberger M. P., and Humphreys T. E., "A proposed navigation message authentication implementation for civil GPS anti-spoofing," *Proceedings of the 24th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2011), Portland, OR*, September 2011, pp. 3129-3140.

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

[4] Nielsen J., Broumandan A., and Lachapelle G., "GNSS Spoofing Detection for Single Antenna Handheld Receivers," *NAVIGATION*, vol. 58, no. 9, , September, 2010, pp. 335–344.

[5] Meurer M., Konovaltsev A., Cuntz M., and Hättich C., "Robust joint multi-antenna spoofing detection and attitude estimation using direction assisted multiple hypotheses RAIM," *Proceedings of the 25th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2012)*, Nashville, TN, September 2012, pp. 3007-3016..

[6] Moshavi S., "Multi-user detection for DS-CDMA communications," *IEEE Communications Magazine*, vol. 34, no. 10, , October, 1996, pp. 124–135.

[7] Psiaki M. L., Powell S. P., and O'Hanlon B. W., "GNSS spoofing detection using high-frequency antenna motion and carrier-phase data," *Proceedings of the 26th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2013), Nashville, TN*, September 2013, pp. 2949-2991.

[8] Jafarnia-Jahromi A., Broumandan A., Nielsen J., and Lachapelle G., "GPS spoofer countermeasure effectiveness based on signal strength, noise power and C/N0 observables," *International Journal of Satellite Communications and Networking*, vol. 30, no. 4, July, 2012, pp. 181–191.

[9] Swaszek P. F., Hartnett R. J., and Seals K. C., "GNSS spoof detection using independent range information," *Proceedings of the 2016 International Technical Meeting of The Institute of Navigation, Monterey, California*, January 2016, pp. 739-747.

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

[11] Khanafseh S., et. al., "GPS Spoofing Detection Using RAIM with INS Coupling," *Proceedings of IEEE/ION PLANS 2014, Monterey, CA*, May 2014, pp. 1232-1239.

[12] Tanil C., Khanafseh S., and Pervan B., "Impact of Wind Gust on Detectability of GPS Spoofing Attack Using RAIM with INS Coupling," *Proceedings of the ION 2015 Pacific PNT Meeting, Honolulu, Hawaii* ,April 2015, pp. 674-686.

[13] Tanil C., Khanafseh S., and Pervan B., "GNSS spoofing attack detection using aircraft autopilot response to deceptive trajectory," *Proceedings of the 28th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2015), Tampa, Florida*, September 2015, pp. 3345-3357.

[14] Tanil C., Khanafseh S., Joerger M., and Pervan B., "Kalman filter-based Innovation monitor to detect GNSS spoofers capable of tracking aircraft position," *Proceedings of IEEE/ION PLANS 2016, Savannah, GA*, April 2016, pp. 1027-1034.

[15] Tanil C., Khanafseh S., and Pervan B., "An INS monitor against GNSS Spoofing Attacks during GBAS and SBAS- assisted Aircraft Landing Approaches," *Proceedings of the 29th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2016), Portland, Oregon*, September 2016, pp. 2981-2990.

[16] Tanil C., Khanafseh S., and Pervan B., "Detecting Global Navigation Satellite System spoofing using inertial sensing of aircraft disturbance," *Journal of Guidance, Control, and Dynamics*, vol. 40, no. 8, 2017, pp. 2006–2016.

[17] Tanil C., Khanafseh S., Joerger M. and Pervan B., "An Innovation monitor to Detect GNSS Spoofers Capable of Tracking Aircraft Position," *IEEE Transactions on Aerospace and Electronics*, vol. 54, no. 1, February 2018, pp. 131–143.

[18] Tanil C., Jimenez P. M., Raveloharison M., Kujur B., Khanafseh S., and Pervan B., "Experimental Validation of Innovation monitor against GNSS Spoofing," *Proceedings of the 31st International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2018), Miami, FL*, September 2018, pp. 2923-2937.

[19] Kujur B., Tanil C., Khanafseh S., and Pervan B., "Sensitivity of Innovation Monitors to Uncertainty in Error Modeling," *Proceedings of the 32nd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2019), Miami, FL*, September 2019, pp. 3266-3274.

[20] RTCA DO-316, Minimum Operational Performance Standards for Global Positioning System/ Aircraft-Bases Augmentation System Airborne Equipment.

[21] Kujur B., Khanafseh S., and Pervan B., "A Solution Separation Monitor using INS for Detecting GNSS Spoofing," *Proceedings of the 33rd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2020), St. Louis, MO*, September 2020, pp. 3210-3226..

[22] Gallon, E., Joerger, M., and Pervan B., "Frequency-Domain Modeling of Orbit and Clock Errors for Sequential Positioning," *Proceedings of the 33rd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2020), St. Louis, MO*, September 2020, pp. 1041-1053..

[23] Gallon, E., Joerger, M., and Pervan B., "Robust Modeling of GNSS Tropospheric Delay Dynamics," *IEEE Transactions on Aerospace and Electronic Systems*, doi: 10.1109/TAES.2021.3068441.

[24] Kujur B., Khanafseh S., and Pervan B., "Detecting GNSS Spoofing of ADS-B Equipped Aircraft using INS," *2020 IEEE/ION Position, Location and Navigation Symposium (PLANS), Portland, OR*, April 2020, pp. 548-554..