

A Solution Separation Monitor using INS for Detecting GNSS Spoofing

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 assistant professor at Illinois Institute of Technology (IIT), Chicago. 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 solution separation monitor to detect Global Navigation Satellite System (GNSS) spoofing using Inertial Navigation Systems (INS), which compares the position solution of a tightly coupled INS/GNSS to an INS-only position solution. In our prior work [11]–[17], we introduced an innovation sequence monitor that provided high integrity detection against slowly growing faults, but it lacked fault exclusion capability and assumed coincident monitor start at fault onset. In this work, we also prove that the solution separation monitor provides better detection capability compared to the innovation sequence monitor. The solution separation monitor enables direct fault exclusion after spoofing detection since the INS-only position solution is not corrupted by re-calibration using spoofed GNSS signals. We also address the monitor start and run time issue by proposing a sequential window monitoring method for which it is possible to explicitly quantify protection level for a given time frame of monitoring. For slowly growing faults which might remain undetected by the solution separation monitor we analyze the spoofer's tracking error as an aid to detection. Wind gusts cause rapid movement of aircraft which cannot be tracked in real time and hence can potentially help with detection. We model spoofer's tracking error based on empirical vertical velocity variation data of civil aircraft due to wind gusts. The solution separation monitor performance is shown to be enhanced with the presence of spoofer's tracking error even when the spoofer does not inject any fault profiles.

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. The civil GNSS signal structure is publicly known and vulnerable to spoofing attacks, which endangers public safety [1]. Spoofing attacks consist of intentional jamming of the authentic radio-frequency signals and feeding a predetermined faulty signal to the user. 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. This work is aimed at addressing the aforementioned issues of fault exclusion, and monitor start and run time.

II. EN ROUTE AIRCRAFT

In this work, we consider 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 absence of visual references for the pilot, possible unavailability of navigation error corrections from reference stations, and time availability for spoofer to slowly deviate the aircraft.

A. Tightly-coupled INS/GNSS architecture

An INS provides the navigation solution as states of aircraft position r_x, r_y, r_z , velocity v_x, v_y, v_z , and attitude ϕ, θ, ψ (Euler angles), using IMU measurements. The aircraft states are,

$$\mathbf{x}_{A/C} = [r_x \ r_y \ r_z \ v_x \ v_y \ v_z \ \phi \ \theta \ \psi]^T \quad (1)$$

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 \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 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 additive WGN η_u is commonly derived from specifications of velocity random walk (VRW) of accelerometer and angular random walk (ARW) of gyroscope.

$$\tilde{u} = u^* + b_c + b + \eta_u \quad (2)$$

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

$$\dot{b} = -\frac{1}{\tau_b}b + v_b \quad (3)$$

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.

$$\mathbf{x}_{bias} = [b_{a_x} \quad b_{a_y} \quad b_{a_z} \quad b_{\omega_x} \quad b_{\omega_y} \quad b_{\omega_z}]^T \quad (4)$$

We assume the en route aircraft utilizes only single frequency GNSS measurements without any differential corrections, which is typical of today’s RAIM environment. This work takes an en route example with single frequency measurements, but the idea is also applicable to dual frequency multi constellation GNSS, terminal and precision approach scenarios. Equation (5) shows the GNSS measurement equation. The code measurement ρ for each satellite is composed of true range p , 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 $v_{th(\rho)}$. Similarly, the carrier phase measurement $\lambda\phi$ for each satellite is composed of true range p , 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 $v_{th(\phi)}$. 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 :

$$\begin{bmatrix} \rho \\ \lambda\phi \end{bmatrix} = \begin{bmatrix} p \\ p \end{bmatrix} + \begin{bmatrix} c(dt_{rc} - dt_{sv}) \\ c(dt_{rc} - dt_{sv}) \end{bmatrix} + \begin{bmatrix} I_\rho \\ -I_\phi \end{bmatrix} + \begin{bmatrix} T_\rho \\ T_\phi \end{bmatrix} + \begin{bmatrix} m_\rho \\ m_\phi \end{bmatrix} + \begin{bmatrix} 0 \\ \lambda N_\phi \end{bmatrix} + \begin{bmatrix} v_{th(\rho)} \\ v_{th(\phi)} \end{bmatrix} \quad (5)$$

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

All the GNSS errors need to be accounted for in the measurement in order to be utilized in the KF. Satellite clock offsets cdt_{sv} are available from the navigation message. After satellite clock offset correction, there are still residual errors due to satellite clock and ephemeris parameter uncertainty. These residual errors r_{sv} can be modeled [20] as a first order GMRP with a time constant $\tau_{r_{sv}}$ of 2 hours subject to driving WGN $v_{r_{sv}}$. These errors are modeled to have a standard deviation of 2 m. Equation (6) represents the first order GMRP model for satellite clock and ephemeris residual errors.

$$\dot{r}_{sv} = -\frac{1}{\tau_{r_{sv}}}r_{sv} + v_{r_{sv}} \quad (6)$$

The receiver clock offset cdt_{rc} can be compensated by modeling the receiver clock with 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),

$$\begin{bmatrix} \dot{r}_{rc} \\ \dot{\dot{r}}_{rc} \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} r_{rc} \\ \dot{r}_{rc} \end{bmatrix} + \begin{bmatrix} w_{r_{rc}} \\ w_{\dot{r}_{rc}} \end{bmatrix} \quad (7)$$

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.

The ionospheric delay can be corrected using the ionospheric correction T_{iono} from the Klobachaur model and the residual errors r_i are modeled [20] to have a standard deviation given by equation (8),

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

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 can be modeled as a first order GMRP with a time constant of 2 hours and driving WGN v_{r_i} shown as,

$$\dot{r}_i = -\frac{1}{\tau_{r_i}} r_i + v_{r_i} \quad (9)$$

The tropospheric delay can be corrected with the correction model specified in [20] and the residual errors r_t can be modeled [20] as a first order GMRP with a time constant of 30 minutes. The standard deviation for this error is given as,

$$\sigma_t = 0.12 m(el) \quad (\text{meters}) \quad (10)$$

where, $m(el)$ is the mapping function of satellite elevation [20]. Equation (11) shows the first order GMRP model of tropospheric residual error r_t ,

$$\dot{r}_t = -\frac{1}{\tau_{r_t}} r_t + v_{r_t} \quad (11)$$

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

Being time correlated, the multipath is modeled as a first order GMRP with time constant τ_m of 25 seconds and driving WGN v_m [20] .

$$\dot{m} = -\frac{1}{\tau_m} m + v_m \quad (12)$$

The standard deviation for code multipath error is taken as 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:

$$\mathbf{x}_{GNSS} = [r_{sv}^{1:n} \ r_{rc} \ \dot{r}_{rc} \ r_i^{1:n} \ r_t^{1:n} \ m_{\rho}^{1:n} \ m_{\phi}^{1:n} \ \lambda N_{\phi}^{1:n}]^T \quad (13)$$

where, n is the number of satellites.

The final state vector of the INS/GNSS system is

$$\mathbf{x} = [\mathbf{x}_{A/C} \ \mathbf{x}_{bias} \ \mathbf{x}_{GNSS}]^T \quad (14)$$

This 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,

$$\delta \mathbf{x}_{k+1} = \Phi_k \delta \mathbf{x}_k + \Gamma_{w_k} \mathbf{w}_k \quad (15)$$

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

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

$$\delta \mathbf{z}_k = \mathbf{H}_k \delta \mathbf{x}_k + \mathbf{v}_k \quad (16)$$

where, \mathbf{H} is the observation matrix, and \mathbf{v} is the measurement noise with respective measurement noise covariance \mathbf{V}

B. Innovation Sequence Monitor

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. The innovation vector γ at time epoch k is defined as

$$\gamma_k = \delta \mathbf{z}_k - \mathbf{H}_k \delta \bar{\mathbf{x}}_k \quad (17)$$

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

$$(18)$$

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

The monitor simply checks whether the test statistic q_k is smaller than a predefined threshold T_k^2 as

$$q_k \geq T_k^2 \quad (19)$$

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 innovation monitor alarms for a fault if $q_k > T_k^2$.

One of the major limitations of the innovation sequence monitor is the incapability for fault exclusion since the aircraft has no fault-free solution to rely upon. Another unaddressed issue for this monitor is the start and run time. For all prior performance evaluations, it was assumed that the monitor start time and spoofing onset time are coincident. Also, no quantitative method exists to determine how long this monitor should run. To address these limitations specifically, we propose a solution separation monitor which we proved to have better detection capability than the innovation sequence monitor.

III. SOLUTION SEPARATION MONITOR WITH SEQUENTIAL WINDOW MONITORING

The solution separation monitor is based on the difference of position solution between faulty full-set (INS and GNSS) KF solution and fault-free subset INS-only solution. The test statistic at any time k is defined as,

$$q_k = \hat{\mathbf{X}}_{KF_k} - \bar{\mathbf{X}}_{c_k} \quad (20)$$

where, $\hat{\mathbf{X}}_{KF_k}$ is position solution obtained from the KF and $\bar{\mathbf{X}}_{c_k}$ is the position solution obtained from the INS-only coasting. The covariance for the test statistic is given by,

$$\mathbf{P}_k = \bar{\mathbf{P}}_{c_k} - \hat{\mathbf{P}}_{KF_k} \quad (21)$$

where, $\hat{\mathbf{P}}_{KF_k}$ is the position error covariance for $\hat{\mathbf{X}}_{KF_k}$ and $\bar{\mathbf{P}}_{c_k}$ is the position error covariance for $\bar{\mathbf{X}}_{c_k}$. The derivation for this covariance is shown in Appendix-B. The threshold for the test statistic can be obtained using the false alarm requirement and inverse CDF of the Gaussian distribution.

Appendix-A provides a proof that solution separation monitor performance is always better than the innovation sequence monitor. Additionally, the solution separation monitor allows for exclusion after spoofing is detected since the INS-only coasting solution is fault-free. The solution separation monitor is a snapshot monitor and relies primarily on the instantaneous error between the tightly coupled INS/GNSS KF position solution and INS-only coasting solution. The detectability of this monitor therefore gets degraded with time since the INS-only covariance $\bar{\mathbf{P}}_c$ drifts over time thereby causing the threshold to increase over time.

We address the monitor start and run time by proposing a sequential window monitoring method which utilizes consecutive fixed length monitoring windows. Fig. 1 illustrates the structure of the sequential window monitoring method. The idea is to run sequences of solution separation monitors each starting with the received GNSS signal frequency. This ensures that a fault is always captured by a monitor window and once detected can be used to exclude the fault in an optimal way. Each monitor window has its own INS-only solution and once spoofing is detected in a particular window, INS-only solution of the prior window can be used as the fault-free solution. Each window inherently provides a protection level (PL) in the form of INS-only covariance $\bar{\mathbf{P}}_c$ and hence sequence of solution separation monitors ensure PL at all times. This PL grows over time and eventually would reach some predefined alert limit (AL). The maximum time (t_{maxSS}) required for the PL to reach an AL can be used as the run time for monitor windows. Since each monitor would have its own PL approaching the alert limit over time,

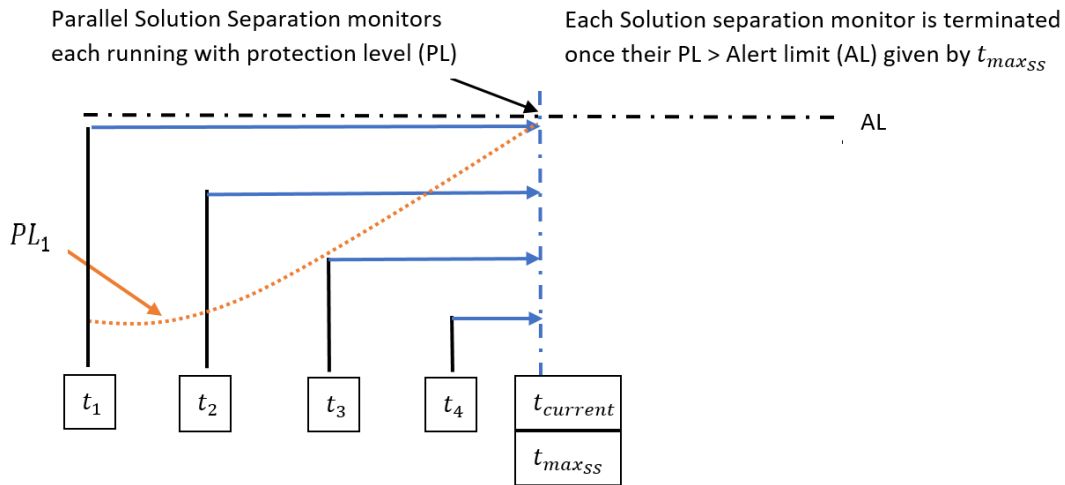


Fig. 1: Illustration of sequential window monitoring structure.

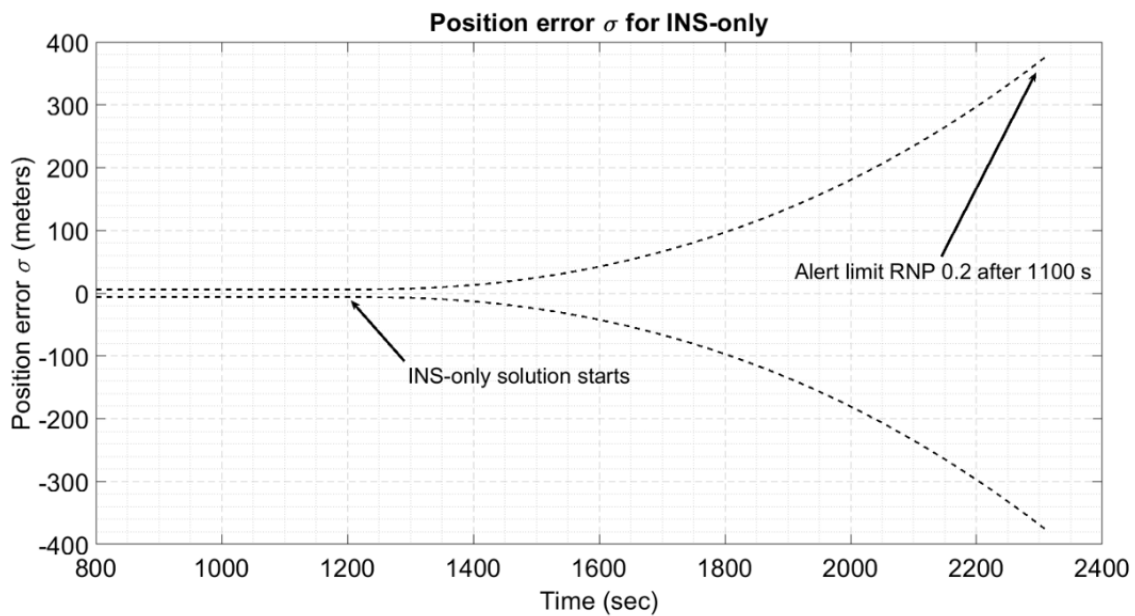


Fig. 2: Illustration of INS-only covariance (protection level) drift.

we can sequentially terminate each window if no spoofing is detected. Thus, the sequential window monitoring method addresses the issue of monitor start and run time. Since at any given instance of time there will be a set number of monitor windows running, the false alarm requirement allocation for each solution separation monitor will be equally divided among these set number of monitor windows to determine the threshold for each. This is conservative since the test statistic for different monitors will be correlated but it is easy to implement. For example, if at any time there are 5 windows running and the solution separation monitoring method has an overall false alarm allocation of 10^{-5} , each monitor window will have threshold computed using false alarm requirement of 0.2×10^{-5} . In a practical sense, the solution separation sequential window monitoring can be started as soon as an aircraft starts

using the GNSS signals for navigation.

Fig. 2 shows a typical INS-only covariance drift over time during an en route straight level flight (SLF) of an aircraft utilizing single frequency GNSS signals. The figure shows values of position error standard deviation for an aircraft with initial SLF of at least 20 minutes (1200 sec). At time $t = 1200$ seconds a solution separation window starts and the dotted curve represents the PL provided by that monitoring window. If an AL of RNP 0.2 is used (0.2 nmi), eventually the PL reaches that limit around 1100 seconds after window starts. At this point, this window can be terminated if no spoofing was detected. Thus for this specific AL, the monitor run time is evaluated to be 1100 seconds. Since, the solution separation monitor can provide PL only up until a certain time, there could be cases where the spoofer can inject fault profiles that grow very slowly over time and can go undetected by the solution separation monitor. In order to tackle these slow growing faults, we propose utilizing the spoofer's tracking errors to our advantage. One major contributing factor in spoofer's tracking error would be the random position variations of aircraft due to wind, which we can model. Before analyzing the impact of these position variations on spoofing detection, the next section gives an overview of the two spoofing scenarios that could occur and how sequential window monitoring is applied in each scenario. This will also allow us to determine more specifically how and in what situations tracking errors would enhance detection for the solution separation monitor.

IV. SPOOFING SCENARIOS

For an aircraft during SLF, a typical spoofing scenario is to deviate the aircraft and cause errors that exceed the alert limit. Recall, here we consider an aircraft using single frequency GNSS measurements which result in horizontal position error standard deviation ranging from 5 to 7 meters. A spoofer could use optical or laser tracking methods to determine the near exact location of the aircraft. This tracking is necessary since any sudden jump in consecutive GNSS signals could be detected by the aircraft. Due to instrument errors, latency issues, and lack of proximity

Case 1: No jamming before spoofing

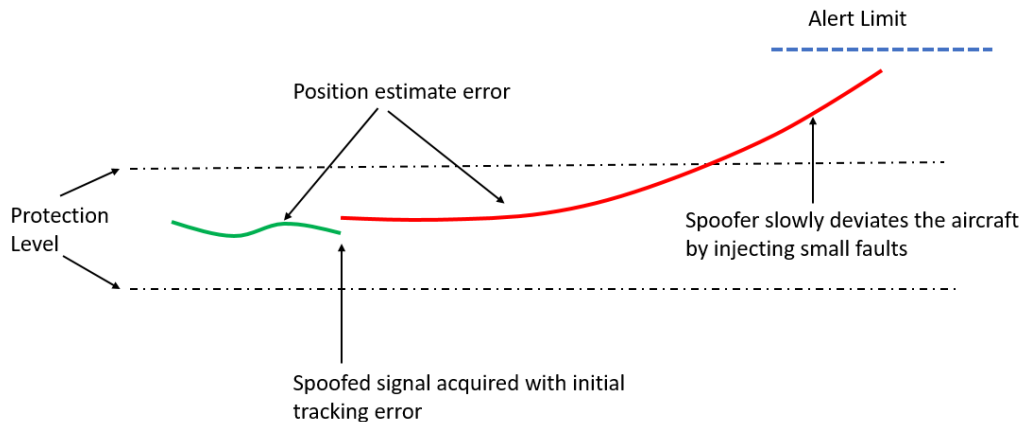


Fig. 3: Illustration of spoofing without jamming.

to aircraft, the spoofer will always have tracking error. Thus, if the spoofer wants the aircraft to lock on to the spoofed measurements without suspicion, a higher power spoofed signal needs to be broadcast without detectable discrepancies compared to the authentic signals. This can be achieved only if the spoofer has very small tracking errors.

In another scenario, where the tracking error is large enough such that spoofed GNSS signals can immediately be distinguished from the authentic signals, the spoofer can opt to jam the authentic signals first. This would cause the aircraft to use the INS-only position solution, whose covariance drifts over time. Once the covariance is large enough the spoofer can send the spoofed GNSS signals such that any tracking error is absorbed by the large position error covariance. There will be suspicion due to GNSS signals being jammed but since the aircraft INS needs to eventually incorporate GPS signal for correction, and as long as the re-acquired signals provide a position solution

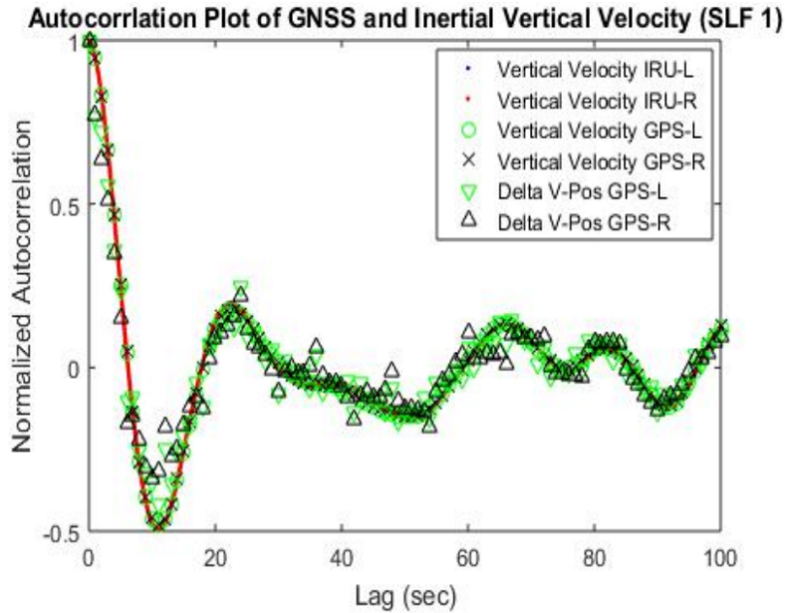


Fig. 5: Auto-correlation function for vertical velocity variation [21].

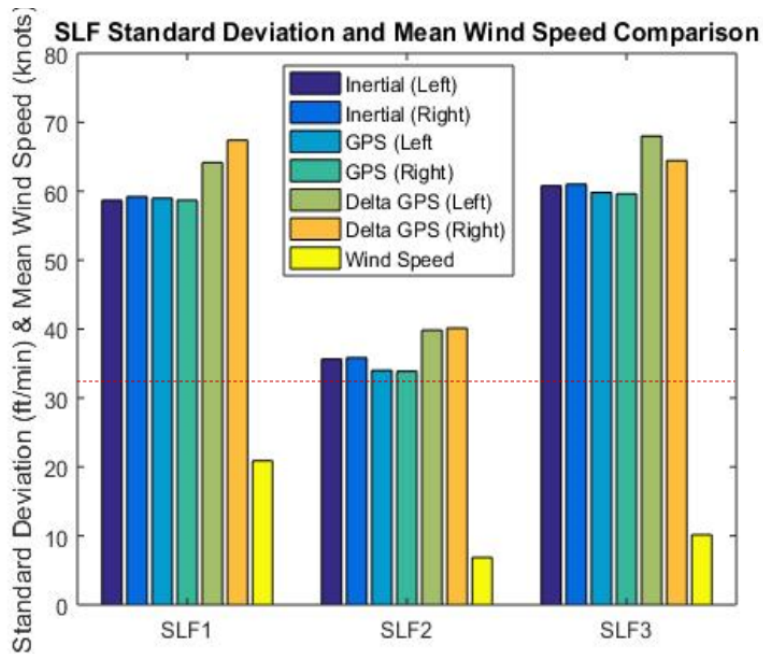


Fig. 6: Vertical velocity variation standard deviation [21].

where x_2 is the position variation, $\alpha = \sqrt{\beta^2 + \omega^2}$ and w is white Gaussian noise with spectral density $2\beta\sigma^2\delta(\tau)$, and σ is obtained from chosen values of Fig. 6. The values of parameters β and ω used for this model are $\frac{1}{15} \text{ sec}^{-1}$ and $\frac{2\pi}{23} \text{ rad/sec}$, respectively. The state x_2 obtained from this tracking error model represents the position variation due to gusts which we assume the spoofer is unable to track. Fig. 7 shows typical position variations over time for velocity variation standard deviation of 30 ft/min. These position variations, or tracking errors, are captured in the

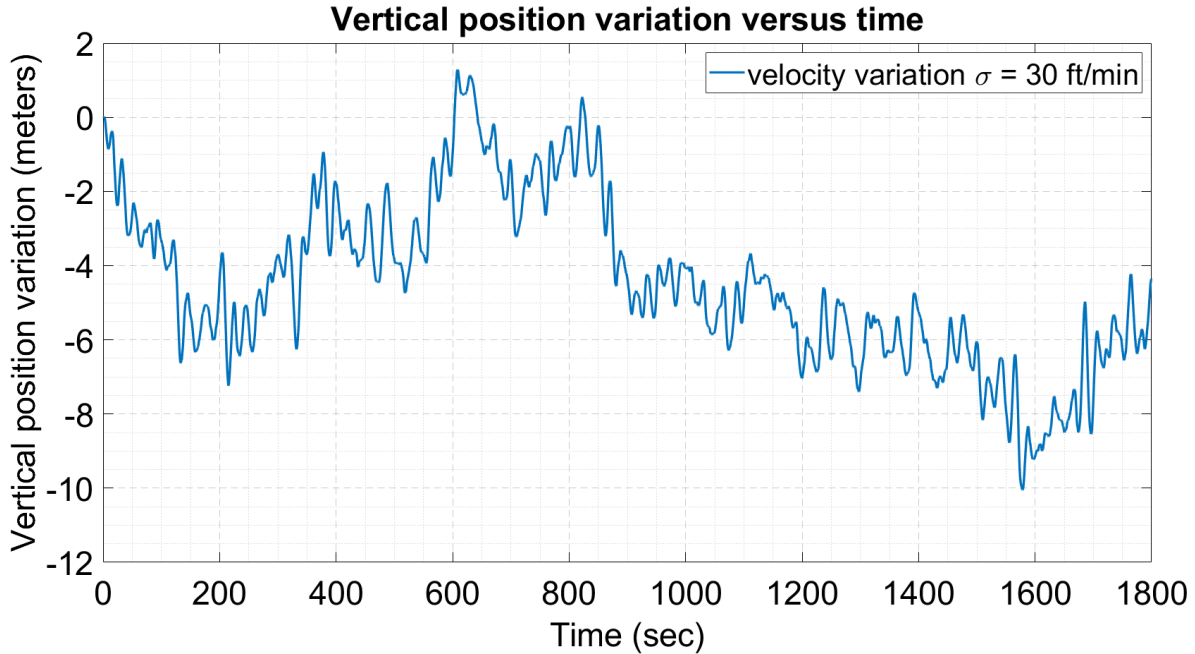


Fig. 7: Vertical position variation for velocity variation σ of 30 ft/min.

INS measurements since they represent actual aircraft movement. Meanwhile, since the spoofer cannot track these movements, they will not appear in the spoofed measurements. This creates a discrepancy between the INS and spoofed GNSS measurements. Note that even if the spoofer does not inject any additional fault profiles, these small discrepancies will appear when the two measurements are compared. Thus, we analyze the most stringent scenario when the spoofer does not inject any fault profile but just broadcast spoofed signal with these tracking errors.

VI. RESULTS

The analysis for tracking errors against spoofing detection was performed for both scenarios of when there is no jamming and when authentic GNSS signals are jammed before spoofing. Recall, when there is no jamming, we run the sequential window monitoring method and observe each sequential window, whereas when jamming occurs, we observe the solution separation monitor window that starts at the moment of jamming. Also, since the solution separation monitor is a snapshot monitor, it would detect spoofing if the tracking error is bigger than the threshold at any point of time during monitoring. Fig. 8 illustrates the discrepancy that occurs due to tracking error on the KF estimated position using the spoofed signals. This position variation is what the solution separation monitor would observe, and if this is greater than the threshold, spoofing is detected. We used Monte-Carlo simulations to get a statistical result for the monitor performance. We ran 100 Monte-Carlo simulations where the aircraft has been through an initial SLF period of 20 minutes. Spoofing occurs after the initial SLF period and we compute the missed detection rate of the monitor window that started at that time epoch. Note that spoofing here means presence of tracking errors in the GNSS signals and no additional fault profiles. For scenarios when there is jamming, we start jamming after the initial SLF period and varied the jamming period with increments of 5 seconds. After the jamming period, the aircraft receives the spoofed GNSS signals. Fig. 9 shows the probability of missed detection obtained from 100 Monte-Carlo simulations for different standard deviations of vertical velocity variation based on the range of standard deviations obtained from empirical data in Fig. 6. It can be observed from the results that jamming degrades the performance of the solution separation monitor. Also, with increased magnitude of gusts or vertical velocity variation, successful detection rate is higher. As a preliminary step in this paper, we used vertical tracking error only, and will consider the 3-dimensional error in future work.

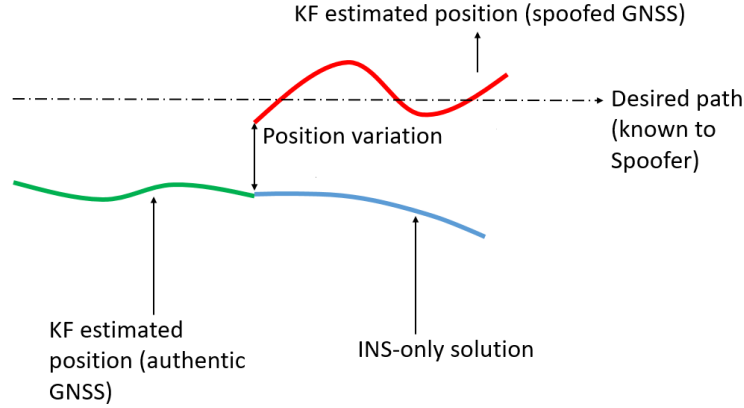


Fig. 8: Effect of tracking error on position estimation due to spoofed signals.

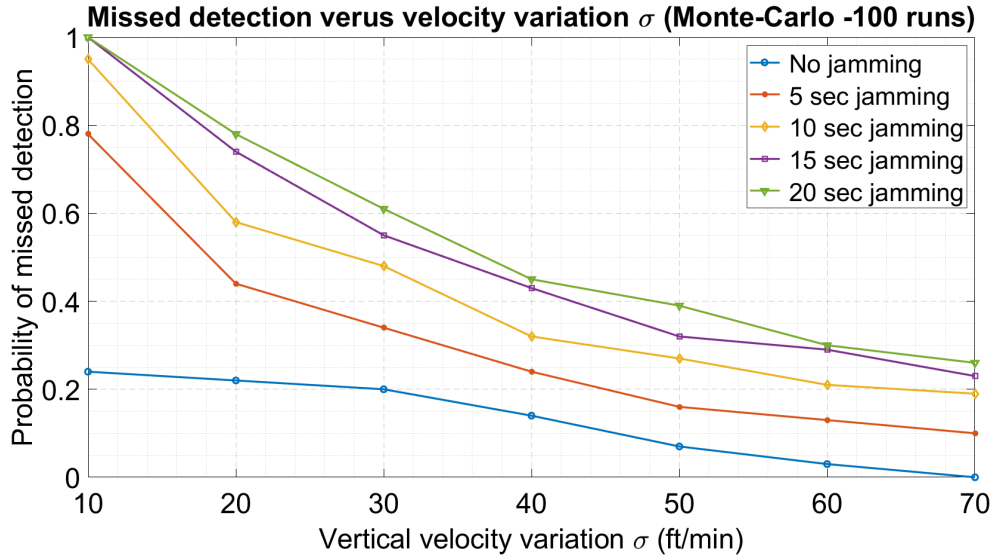


Fig. 9: Probability of missed detection for different vertical velocity variation standard deviation.

VII. CONCLUSION

In this work, we proposed a solution separation monitor that compares the KF INS/GNSS position solution against an INS-only position solution. The solution separation monitor provides a direct way for spoofing detection and exclusion since the INS-only solution does not include any faults. We analytically proved that the solution separation monitor offers better detection capability than the innovation sequence monitor used in previous work. We addressed the monitor start and run-time issue by proposing a sequential window monitoring method which runs consecutive solution separation monitoring windows. Lastly, to address very slowly growing faults that might go undetected by the solution separation monitor, we considered the spoofer's tracking error as an aid for detection. Using experimental data of vertical velocity variation due to wind gusts for civil aircraft, we generated a spoofer tracking error model. We then analyzed the performance of solution separation monitor against the spoofer's tracking error.

VIII. APPENDIX

A. Integrity risk comparison of solution separation and cumulative Chi-squared innovation sequence monitors

Consider a full-set position solution \mathbf{x}_o with fault vector \mathbf{f} and noise $v_o \sim N(0, \sigma_o^2)$ shown as,

$$\mathbf{x}_o = \mathbf{x} + \mathbf{f} + v_o \quad (25)$$

where, \mathbf{x} is the actual position. The fault-free subset solution is given by,

$$\mathbf{x}_i = \mathbf{x} + v_i \quad (26)$$

where, $v_i \sim N(0, \sigma_i^2)$ is the noise. The position estimate error in the faulty full-set is given as,

$$\mathbf{x}_o - \mathbf{x} = \mathbf{f} + v_o \quad (27)$$

The difference between the faulty full-set and fault-free subset position solution is the solution separation test statistic,

$$\mathbf{x}_o - \mathbf{x}_i = \mathbf{f} + v_o - v_i \quad (28)$$

Integrity risk for solution separation (SS) monitor can be written as probability of test statistic being less than the threshold and estimate error exceeding the alert limit,

$$P_{ss}(HMI) = P(x_o - \mathbf{x}_i < T_{ss}, \mathbf{x}_o - \mathbf{x} > \mathbf{L}) \quad (29)$$

where, T_{ss} is the threshold, HMI stands for hazardous misleading information and \mathbf{L} is the alert-limit. Substituting (27) and (28) in (29) we get,

$$P_{ss}(HMI) = P(\mathbf{f} + v_o - v_i < T_{ss}, \mathbf{f} + v_o > \mathbf{L}) \quad (30)$$

Defining $v_{\Delta i} = v_o - v_i$ and $\sigma_{\Delta i}^2 = \sigma_i^2 - \sigma_o^2$

$$P_{ss}(HMI) = P(\mathbf{f} + v_{\Delta i} < T_{ss}, \mathbf{f} + v_o > \mathbf{L}) \quad (31)$$

Re-writing in terms of Q- and cumulative distribution function,

$$P_{ss}(HMI) = \Phi\left(\frac{T_{ss} - \mathbf{f}}{\sigma_{\Delta i}}\right) Q\left(\frac{\mathbf{L} - \mathbf{f}}{\sigma_o}\right) \quad (32)$$

$$P_{ss}(HMI) = \Phi\left(\frac{T_{ss} - \mathbf{f}}{\sigma_{\Delta i}}\right) \Phi\left(\frac{\mathbf{f} - \mathbf{L}}{\sigma_o}\right) \quad (33)$$

Let β be defined as,

$$\beta = \frac{\mathbf{f}}{\sigma_{\Delta i}} \quad (34)$$

$$P_{ss}(HMI) = \Phi\left(\frac{T_{ss}}{\sigma_{\Delta i}} - \beta\right) \Phi\left(\frac{\beta \sigma_{\Delta i} - \mathbf{L}}{\sigma_o}\right) \quad (35)$$

where,

$$T_{ss} = -\Phi^{-1}\left(\frac{P_{FA}}{2}\right) \sigma_{\Delta i} \quad (36)$$

Now, to evaluate integrity risk of cumulative Chi-Squared innovation sequence monitor, first we define the fault slope g^2 which maximizes the integrity risk by maximizing the position estimate error with minimal fault, and can be written as,

$$g^2 = \left(\frac{\delta \mathbf{x}_f^2}{\gamma_f^2}\right) \quad (37)$$

where, $\delta \mathbf{x}_f$ is the position estimate error due to fault and γ_f^2 is the fault parameter in the test statistic. In [22], the following was shown for the solution separation monitor.

$$g^2 = \sigma_{\Delta i}^2 = \sigma_i^2 - \sigma_o^2 \quad (38)$$

For innovation sequence monitor, the fault parameter in the test statistic is the non-centrality parameter

$$\gamma_f^2 = \lambda_f^2 \quad (39)$$

The integrity risk for the Chi-squared (χ^2) innovation sequence monitor can be written as,

$$P_{\chi^2}(HMI) = P(\gamma^2 < T_{\chi^2})P(\delta x > \mathbf{L}) \quad (40)$$

where, δx is the estimate error with the noise and T_{χ^2} is the threshold determined from a Chi-square distribution

$$T_{\chi^2} = \chi^2(1 - P_{FA}, dof) \quad (41)$$

and

$$dof = nN \quad (42)$$

where, P_{FA} is the probability of false alarm, dof is the degrees of freedom for the Chi-squared distribution, n is the number of satellite vehicles and N is number of time epochs. Re-writing (40),

$$P_{\chi^2}(HMI) = \chi_{nc}^2(T_{\chi^2}, dof, \lambda^2)P(\delta x_f + v_o > \mathbf{L}) \quad (43)$$

Substituting (37) and (39) in (43) we get,

$$P_{\chi^2}(HMI) = \chi_{nc}^2(T_{\chi^2}, dof, \lambda^2)P(v_o > \mathbf{L} - g\lambda) \quad (44)$$

$$P_{\chi^2}(HMI) = \chi_{nc}^2(T_{\chi^2}, dof, \lambda^2)P(v_o < g\lambda - \mathbf{L}) \quad (45)$$

$$P_{\chi^2}(HMI) = \chi_{nc}^2(T_{\chi^2}, dof, \lambda^2)\Phi\left(\frac{g\lambda - \mathbf{L}}{\sigma_o}\right) \quad (46)$$

Substituting (38) in (46) we get,

$$P_{\chi^2}(HMI) = \chi_{nc}^2(T_{\chi^2}, dof, \lambda^2)\Phi\left(\frac{\lambda\sigma_{\Delta i} - \mathbf{L}}{\sigma_o}\right) \quad (47)$$

In order to compare the the integrity risk of solution separation and the innovation sequence monitor, let $\alpha = \lambda = \beta$, then using (35) and (47)

$$\frac{P_{\chi^2}(HMI)}{P_{ss}(HMI)} = \frac{\chi_{nc}^2((T_{\chi^2}, dof, \alpha^2)}{\Phi\left(\frac{T_{ss}}{\sigma_{\Delta i}} - \alpha\right)} \quad (48)$$

The threshold for the Solution separation monitor can be written as,

$$T_{ss} = k_{FA}\sigma_{\Delta i} \quad (49)$$

where k_{FA} is determined from given false alarm (FA) requirement and normal distribution CDF.

$$k_{FA} = -\Phi^{-1}\left(\frac{P_{FA}}{2}\right) \quad (50)$$

Thus, (48) can be re-written as,

$$\frac{P_{\chi^2}(HMI)}{P_{ss}(HMI)} = \frac{\chi_{nc}^2(\chi^2(1 - P_{FA}, nN), nN, \alpha^2)}{\Phi\left(-\Phi^{-1}\left(\frac{P_{FA}}{2}\right) - \alpha\right)} \quad (51)$$

Using parameters P_{FA}, n, N and variable α , the integrity risk of both Chi-square innovation sequence and solution separation monitor is shown in Fig. 10. The solution separation monitor is thus proven to always provide equal or better integrity risk than the innovation sequence monitor.

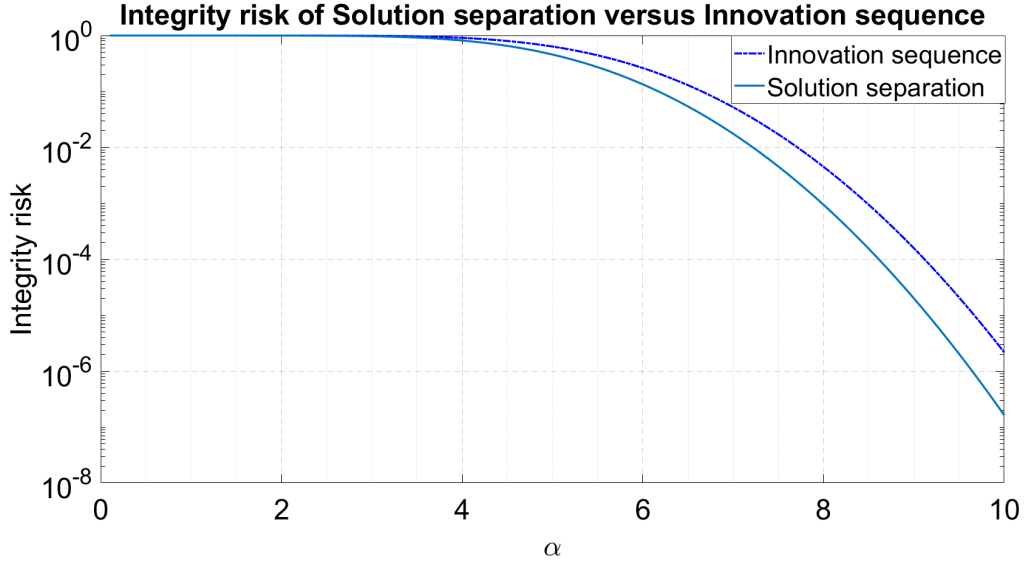


Fig. 10: Integrity risk comparison of solution separation and innovation sequence monitor.

B. Covariance of solution separation test statistic

Consider a solution separation monitor that starts at time epoch 1. The KF time and measurement update equation are,

$$\bar{\mathbf{x}}_1 = \Phi_1 \hat{\mathbf{x}}_0 \quad (52)$$

$$\hat{\mathbf{x}}_1 = \bar{\mathbf{x}}_1 + \mathbf{L}_1(\mathbf{z}_1 - \mathbf{H}_1 \bar{\mathbf{x}}_1) \quad (53)$$

where, for any time epoch k , $\bar{\mathbf{x}}_k$ and $\hat{\mathbf{x}}_k$ represent the states after time and measurement update in the KF, 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 time and measurement update error propagation equations can be shown as,

$$\bar{\mathbf{e}}_1 = \Phi_1 \hat{\mathbf{e}}_0 - \mathbf{w}_1 \quad (54)$$

$$\hat{\mathbf{e}}_1 = (\mathbf{I} - \mathbf{L}_1 \mathbf{H}_1) \bar{\mathbf{e}}_1 + \mathbf{L}_1 \mathbf{v}_1 \quad (55)$$

where, for any time epoch k , $\bar{\mathbf{e}}_k$ and $\hat{\mathbf{e}}_k$ represent the state estimate error after time and measurement update in the KF, 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 solution separation monitor a parallel INS-only coasting is initiated and the state propagation equation for this INS-only coasting is,

$$\bar{\mathbf{x}}_{c_1} = \Phi_1 \hat{\mathbf{x}}_0 \quad (56)$$

where, for any time epoch k , $\bar{\mathbf{x}}_{c_k}$ represents the state after time update in the 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 can be shown as,

$$\bar{\mathbf{e}}_{c_1} = \Phi_1 \hat{\mathbf{e}}_0 - \mathbf{w}_1 \quad (57)$$

where, for any time epoch k , $\bar{\mathbf{e}}_{c_k}$ represents the state estimate error after time update in INS-only coasting. Similarly for the second time epoch, we can write the time and measurement update equations in KF as,

$$\bar{\mathbf{x}}_2 = \Phi_2 \hat{\mathbf{x}}_1 \quad (58)$$

$$\hat{\mathbf{x}}_2 = \bar{\mathbf{x}}_2 + \mathbf{L}_2(\mathbf{z}_2 - \mathbf{H}_2 \bar{\mathbf{x}}_2) \quad (59)$$

and the propagation equation for the INS-only coasting as,

$$\bar{\mathbf{x}}_{c_2} = \Phi_2 \bar{\mathbf{x}}_{c_1} \quad (60)$$

The KF error propagation equations are

$$\bar{\mathbf{e}}_2 = \Phi_2 \hat{\mathbf{e}}_1 - \mathbf{w}_2 \quad (61)$$

$$\hat{\mathbf{e}}_2 = (\mathbf{I} - \mathbf{L}_2 \mathbf{H}_2) \bar{\mathbf{e}}_2 + \mathbf{L}_2 \mathbf{v}_2 \quad (62)$$

For INS-only coasting, the state estimate error propagation equation is,

$$\bar{\mathbf{e}}_{c_2} = \Phi_2 \bar{\mathbf{e}}_1 - \mathbf{w}_2 \quad (63)$$

Also, for any time epoch k the following notations of $\bar{\mathbf{P}}_k$ for $\mathbb{E}\{\bar{\mathbf{e}}_k \bar{\mathbf{e}}_k^T\}$, $\hat{\mathbf{P}}_k$ for $\mathbb{E}\{\hat{\mathbf{e}}_k \hat{\mathbf{e}}_k^T\}$, \mathbf{Q}_k for $\mathbb{E}\{\mathbf{w}_k \mathbf{w}_k^T\}$ and \mathbf{V}_k for $\mathbb{E}\{\mathbf{v}_k \mathbf{v}_k^T\}$ represent the covariances .

Since the test statistic at time k is defined as the difference between the position state estimate from the full set of INS/GNSS and the position state estimate from the subset of INS-only coasting as,

$$q_k = \hat{\mathbf{x}}_k - \bar{\mathbf{x}}_{c_k} \quad (64)$$

the covariance for the test statistic at time epoch k can be written as,

$$\mathbf{P}_{q_k} = \mathbb{E}\{q_k q_k^T\} \quad (65)$$

which can be expanded to,

$$\mathbf{P}_{q_k} = \mathbb{E}\{[\hat{\mathbf{x}}_k - \bar{\mathbf{x}}_{c_k}][\hat{\mathbf{x}}_k - \bar{\mathbf{x}}_{c_k}]^T\} \quad (66)$$

The covariance for the first time epoch is,

$$\mathbf{P}_{q_1} = \mathbb{E}\{[\hat{\mathbf{x}}_1 - \bar{\mathbf{x}}_{c_1}][\hat{\mathbf{x}}_1 - \bar{\mathbf{x}}_{c_1}]^T\} \quad (67)$$

which can be re-written as,

$$\mathbf{P}_{q_1} = \mathbb{E}\{[\hat{\mathbf{e}}_1 - \bar{\mathbf{e}}_{c_1}][\hat{\mathbf{e}}_1 - \bar{\mathbf{e}}_{c_1}]^T\} \quad (68)$$

The above equation can be further expanded as,

$$\mathbf{P}_{q_1} = \mathbb{E}\{\hat{\mathbf{e}}_1 \hat{\mathbf{e}}_1^T\} - \mathbb{E}\{\hat{\mathbf{e}}_1 \bar{\mathbf{e}}_{c_1}^T\} - \mathbb{E}\{\bar{\mathbf{e}}_{c_1} \hat{\mathbf{e}}_1^T\} + \mathbb{E}\{\bar{\mathbf{e}}_{c_1} \bar{\mathbf{e}}_{c_1}^T\} \quad (69)$$

$$\mathbf{P}_{q_1} = \hat{\mathbf{P}}_1 - \mathbb{E}\{\hat{\mathbf{e}}_1 \bar{\mathbf{e}}_{c_1}^T\} - \mathbb{E}\{\bar{\mathbf{e}}_{c_1} \hat{\mathbf{e}}_1^T\} + \bar{\mathbf{P}}_{c_1} \quad (70)$$

For the second and third term using (55),

$$\mathbb{E}\{\bar{\mathbf{e}}_{c_1} \hat{\mathbf{e}}_1^T\} = \mathbb{E}\{\hat{\mathbf{e}}_1 \bar{\mathbf{e}}_{c_1}^T\} = \mathbb{E}\{[(\mathbf{I} - \mathbf{L}_1 \mathbf{H}_1) \bar{\mathbf{e}}_1 + \mathbf{L}_1 \mathbf{v}_1] \bar{\mathbf{e}}_{c_1}^T\} \quad (71)$$

which after expanding the terms becomes,

$$\mathbb{E}\{\hat{\mathbf{e}}_1 \bar{\mathbf{e}}_{c_1}^T\} = (\mathbf{I} - \mathbf{L}_1 \mathbf{H}_1) \mathbb{E}\{\bar{\mathbf{e}}_1 \bar{\mathbf{e}}_{c_1}^T\} \quad (72)$$

From (54) and (57) we know that $\bar{\mathbf{e}}_1$ and $\bar{\mathbf{e}}_{c_1}$ are same for the first time epoch, hence,

$$\mathbb{E}\{\hat{\mathbf{e}}_1 \bar{\mathbf{e}}_{c_1}^T\} = (\mathbf{I} - \mathbf{L}_1 \mathbf{H}_1) \bar{\mathbf{P}}_1 \quad (73)$$

Also, from KF equations we know that for any time epoch k ,

$$\hat{\mathbf{P}}_k = (\mathbf{I} - \mathbf{L}_k \mathbf{H}_k) \bar{\mathbf{P}}_k \quad (74)$$

Thus, (70) becomes,

$$\mathbf{P}_{q_1} = \hat{\mathbf{P}}_1 - \hat{\mathbf{P}}_1 - \hat{\mathbf{P}}_1 + \bar{\mathbf{P}}_{c_1} = \bar{\mathbf{P}}_{c_1} - \hat{\mathbf{P}}_1 \quad (75)$$

Now the covariance for the second time epoch is,

$$\mathbf{P}_{q_2} = \mathbb{E}\{[\hat{\mathbf{x}}_2 - \bar{\mathbf{x}}_{c_2}][\hat{\mathbf{x}}_2 - \bar{\mathbf{x}}_{c_2}]^T\} \quad (76)$$

which can be re-written as,

$$\mathbf{P}_{q_2} = \mathbb{E}\{[\hat{\mathbf{e}}_2 - \bar{\mathbf{e}}_{c_2}][\hat{\mathbf{e}}_2 - \bar{\mathbf{e}}_{c_2}]^T\} \quad (77)$$

The above equation can be further expanded as,

$$\mathbf{P}_{q_2} = \mathbb{E}\{\hat{\mathbf{e}}_2\hat{\mathbf{e}}_2^T\} - \mathbb{E}\{\hat{\mathbf{e}}_2\bar{\mathbf{e}}_{c_2}^T\} - \mathbb{E}\{\bar{\mathbf{e}}_{c_2}\hat{\mathbf{e}}_2^T\} + \mathbb{E}\{\bar{\mathbf{e}}_{c_2}\bar{\mathbf{e}}_{c_2}^T\} \quad (78)$$

$$\mathbf{P}_{q_2} = \hat{\mathbf{P}}_2 - \mathbb{E}\{\hat{\mathbf{e}}_2\bar{\mathbf{e}}_{c_2}^T\} - \mathbb{E}\{\bar{\mathbf{e}}_{c_2}\hat{\mathbf{e}}_2^T\} + \bar{\mathbf{P}}_{c_2} \quad (79)$$

For the second and third term using (62), we can write

$$\mathbb{E}\{\bar{\mathbf{e}}_{c_2}\hat{\mathbf{e}}_2^T\} = \mathbb{E}\{\hat{\mathbf{e}}_2\bar{\mathbf{e}}_{c_2}^T\} = \mathbb{E}\{[(\mathbf{I} - \mathbf{L}_2\mathbf{H}_2)\bar{\mathbf{e}}_2 + \mathbf{L}_2\mathbf{v}_2]\bar{\mathbf{e}}_{c_2}^T\} \quad (80)$$

$$\mathbb{E}\{\hat{\mathbf{e}}_2\bar{\mathbf{e}}_{c_2}^T\} = (\mathbf{I} - \mathbf{L}_2\mathbf{H}_2)\mathbb{E}\{\bar{\mathbf{e}}_2\bar{\mathbf{e}}_{c_2}^T\} \quad (81)$$

Substituting (61) and (63) into (81) we get,

$$\mathbb{E}\{\hat{\mathbf{e}}_2\bar{\mathbf{e}}_{c_2}^T\} = (\mathbf{I} - \mathbf{L}_2\mathbf{H}_2)\mathbb{E}\{[\Phi_2\hat{\mathbf{e}}_1 - \mathbf{w}_2][\Phi_2\bar{\mathbf{e}}_1 - \mathbf{w}_2]^T\} \quad (82)$$

Expanding (82) again and using results from (72) and (74)

$$\mathbb{E}\{\hat{\mathbf{e}}_2\bar{\mathbf{e}}_{c_2}^T\} = (\mathbf{I} - \mathbf{L}_2\mathbf{H}_2)[\Phi_2\hat{\mathbf{P}}_1\Phi_2^T + \mathbf{Q}_2] \quad (83)$$

$$\mathbb{E}\{\hat{\mathbf{e}}_2\bar{\mathbf{e}}_{c_2}^T\} = (\mathbf{I} - \mathbf{L}_2\mathbf{H}_2)\bar{\mathbf{P}}_2 = \hat{\mathbf{P}}_2 \quad (84)$$

Substituting (84) into (79) we get,

$$\mathbf{P}_{q_2} = \bar{\mathbf{P}}_{c_2} - \hat{\mathbf{P}}_2 \quad (85)$$

Hence, from (75) and (85) we can write the general expression for the solution separation test statistic covariance for any time epoch k as,

$$\mathbf{P}_{q_k} = \bar{\mathbf{P}}_{c_k} - \hat{\mathbf{P}}_k \quad (86)$$

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] Harris M. and Kettering V., "GNSS vertical velocity variation due to aircraft motion," *RTCA SC-159 WG2/4*, 2019.
- [22] Joerger M., Chan F. C. and Pervan B., "Solution Separation Versus Residual-Based RAIM," *NAVIGATION*, vol. 61, no. 4, September 2014, pp. 273–291.