An INS Monitor against GNSS Spoofing Attacks during GBAS and SBAS-assisted Aircraft Landing Approaches

Cagatay Tanil, Samer Khanafseh, Boris Pervan
Illinois Institute of Technology

BIOGRAPHY

Çağatay Tanıl received his B.S. and M.S. in Mechanical Engineering from Middle East Technical University (METU), Turkey, in 2006 and 2009, respectively. From 2006 to 2009, he worked as a researcher at Tubitak-SAGE (Defense Industries Research and Development Institute), Ankara-Turkey, responsible for dynamic modeling and simulation of guided missiles and torpedoes. From 2010 to 2013, he worked as a senior research engineer at Roketsan Missiles Industries, Ankara-Turkey, leaded several work packages of guidance, control, and trajectory optimization of anti-ship cruise missiles. He is currently a Ph.D. candidate in Mechanical and Aerospace Engineering at Illinois Institute of Technology (IIT) and Research Assistant in Navigation and Guidance Lab, focused on anti-spoofing attack algorithms for aircraft precision landing.

Dr. Khanafseh is currently a Research Assistant Professor at Mechanical and Aerospace Engineering Department at IIT. He received his M.S. 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 for close proximity applications, 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 was the recipient of the IIT Sigma Xi Excellence in University Research Award, Ralph Barnett Mechanical and Aerospace Dept. Outstanding Teaching Award, Mechanical and Aerospace Dept. Excellence in Research Award, IIT University Excellence in Teaching Award, IEEE Aerospace and Electronic Systems Society M. Barry Carlton Award, RTCA William E. Jackson Award, Guggenheim Fellowship (Caltech), and the Albert J. Zahm Prize in Aeronautics (Notre Dame). 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.

ABSTRACT

In this paper, we propose a simple monitor that utilizes Inertial Navigation System (INS) to detect spoofing attacks on Global Navigation Satellite System (GNSS). It is an innovation-based monitor that can be implemented into positioning systems using a loosely-coupled INS-GNSS integration in a Kalman filter, which is consistent with both Ground-Based and Space-Based Augmentation Systems (GBAS and SBAS). The main contribution of this paper is the development of a framework that integrates the monitor (detector) and estimator, which provides a fully stochastic integrity risk analysis. The performance of the monitor is evaluated in presence of a spoofer capable of tracking and estimating the aircraft position, and computing the worst-case sequence of GNSS fault. Utilizing this worst-case fault, we simulated GBAS-assisted final approach of Boeing 747. The simulation results demonstrate that unless the spoofers position-tracking devices have unrealistic accuracy, the proposed monitor efficiently detects spoofing attacks and meets the most stringent integrity requirements in aviation applications.

I. INTRODUCTION

A Global Navigation Satellite System (GNSS) spoofing attack can be a critical threat to positioning integrity, particularly during an aircraft's final approach where the consequences are potentially catastrophic. In this paper, we propose a novel Inertial Navigation System (INS) spoofing monitor and statistically validate its performance against worst-case spoofing attacks, even when the spoofer has the ability to estimate the real-time position of the aircraft. Our specific application of interest is aircraft landing approaches assisted by Ground-Based and Space-Based Augmentation Systems (GBAS and SBAS), but the methods introduced here are also applicable to other GNSS positioning systems.

GNSS spoofing is a process whereby an external agent tries to control the position output of a GNSS receiver by

deliberately broadcasting a counterfeit signal. The spoofed signal mimics the original GNSS signal with higher power and thus may go unnoticed by measurement screening techniques used within the receiver. As a result, the trajectory of the target user can be controlled through the fake broadcast signals [12]. Numerous anti-spoofing techniques have been developed and vulnerability of these existing methods have been discussed in [18, 19]. These include cryptographic authentication techniques employing modified GNSS navigation data [20–22], spoofing discrimination using spatial processing by antenna arrays and automatic gain control schemes [23–25], GNSS signal direction of arrival comparison [26], code and phase rate consistency checks [27], high-frequency antenna motion [13], and signal power monitoring techniques [28, 29]. Augmenting data from auxiliary sensors such as Inertial Measurement Units (IMU) and independent radar sensors to discriminate the spoofing have also been proposed in [31–33]. The first thorough description of the performance of IMU-based monitoring against worst-case spoofing attacks in terms of integrity risk was first introduced by us in [1–6].

The INS detector introduced in [1–3] monitors discrepancies between GNSS spoofed measurements and INS measurements. The basis for the detector is a tightly coupled integration of GNSS measurements and INS kinematic models using a weighted least squares batch estimator. Receiver Autonomous Integrity Monitoring (RAIM) concepts are implemented using the time history of estimator residuals for spoofing detection. The redundancy required for detection is provided through INS measurements, unlike conventional usage of RAIM, where detection is provided through satellite redundancy [11]. Using the residual-based detector it is possible to analytically determine the worst-case sequence of spoofed GNSS measurements – that is, the spoofed GNSS signal profile that maximizes integrity risk [7].

In [1], we illustrated how a spoofer can inject faults slowly into the GNSS measurements such that they corrupt the tightly coupled solution while going unnoticed by the INS detector. It was also shown that if the spoofer knows the exact trajectory of an aircraft, he or she might eventually cause errors large enough to exceed hazard safety limits, again without triggering an alarm from the INS detector. However, it was acknowledged that in reality, the user's actual trajectory would always deviate from a prescribed path (e.g., a straight line final approach) due to natural disturbances such as wind gusts and aircraft autopilot response to control actions. Deviations from the nominal trajectory due to these disturbances, which were assumed to be unknown to the spoofer, would enhance detection capability of the INS monitor.

In [2, 3], we generalized the spoofing integrity analysis by deriving the statistical dynamic response of an aircraft to a well-established vertical wind gust power spectrum. The main contribution of that work was the development of a rigorous methodology to compute upper bounds on the integrity risk resulting from a worst-case spoofing attack – without needing to simulate individual aircraft approaches with an unmanageably large number specific gust disturbance profiles (e.g., 10^9 to meet aircraft landing integrity requirements [34]). In [4], we investigated the impact on spoofing detection due to aircraft's response to control actions (actuated by the autopilot) due to the spoofed GNSS signals. In response to the manipulated position state estimates, the aircraft autopilot commands accelerations (forces) to maneuver the aircraft to the spoofer's desired trajectory. As with the wind gust case, the controller response results in transient behavior immediately sensed by the INS, but absent in the spoofed signal. We showed that even without exposure to wind gusts, autopilot reactions to the spoofer's input significantly enhance INS detection of the spoofing attack.

One assumption made in [1–4] is that the spoofer knows that the aircraft may use INS to detect spoofing attacks, but has no real-time knowledge of the actual aircraft position during spoofing attack. In [5, 6], we considered spoofers capable of 1) tracking and estimating the position of the target aircraft and, 2) deriving a worst-case fault profile that maximizes the integrity risk. Unlike the prior work, which used a batch estimator to derive the worst-case fault profile, we utilize the more realistic Kalman filter estimator in deriving the worst-case fault profile. In [6], we also introduced a stochastic methodology for the spoofer to account for his/her own tracking sensor errors in his/her worst-case fault derivation, which accounts for a maximum level of awareness on the part of the spoofer. The covariance analysis results demonstrated that unless the position-tracking devices have unrealistic accuracy, the proposed INS monitor is effective in detecting worst-case spoofing attacks with low integrity risk.

In the prior work [1–6], both the differential code and carrier measurements were assumed available for use directly in the airborne Kalman filter estimator, which is common for precision relative navigation systems such as shipboard landing [8] and autonomous airborne refueling [9]. On the other hand, in this current work we assume only the differential carrier-smoothed code measurements are available at the aircraft, which is consistent with both GBAS and SBAS avionics implementations. In this configuration, instead of the code and carrier measurements, GBAS position solution obtained from a GNSS-only weighted least squares estimation is fed into a Kalman filter in a loosely-coupled INS-GNSS integration scheme. In this work, the proposed monitor and the Kalman filter-based worst-case fault derivation are extended for the loosely-coupled INS-GNSS integration. Utilizing this worst-case fault, we simulate a GBAS-assisted landing approaches of B747 and investigate the minimum accuracy levels of the spoofer's position tracking to achieve unacceptably large integrity risks. The simulation results show that even when the spoofer have the full knowledge of the GBAS system to take into account in his/her spoofed measurement computation, the monitor performance is still efficient in detecting worst-case spoofing attacks with low integrity risk unless the spoofer has unrealistic position tracking accuracy.

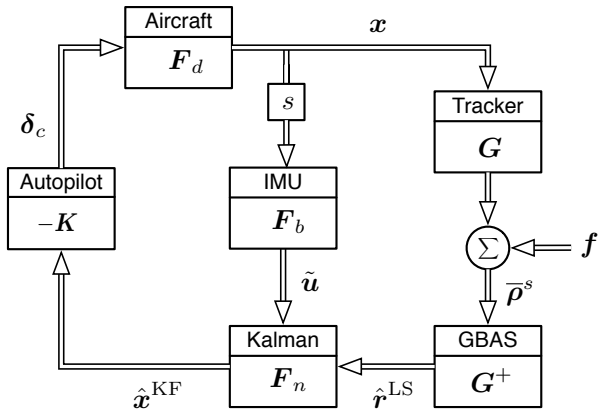

Fig. 1. The performance evaluation model for the INS spoofing monitor utilizing a loosely-coupled integration of INS and GNSS. This model captures the closed-loop relation between the Kalman filter (KF), GBAS weighted least-squares (LS) estimator, and the altitude hold autopilot (controller) in presence of a spoofer capable of tracking aircraft position and injecting a fault $\boldsymbol{f}$ through GNSS signals $\overline{\boldsymbol{\rho}}$.

II. INS AIRBORNE MONITOR

GNSS and INS can be coupled using a variety of integration schemes. These can range from the simple loosely coupled integration, to the complex ultra-tightly coupled mode in which the INS directly aids the GNSS tracking loops [30]. Unlike the prior work [1–6] assumed a tightly-coupled INS-GNSS integration in a Kalman filter, to be consistent with the GBAS and SBAS-assisted landing approaches, this work assumes a loosely-coupled integration where the GBAS position solution (obtained from a weighted least squares estimator using differential carrier-smoothed code $\overline{\boldsymbol{\rho}}$) is directly fed to a Kalman filter that calibrates INS (Fig. 1).

A. GBAS-assisted Weighted Least Squares Estimator

The GBAS measurement equation linearized about a nominal position, is represented for the k^{th} time epoch as

$$\overline{\boldsymbol{\rho}}_k = \underbrace{\begin{bmatrix}\boldsymbol{e}_k^T & 1\end{bmatrix}}_{\boldsymbol{G}_k} \begin{bmatrix}\boldsymbol{r}_k \\ ct_k\end{bmatrix} + \boldsymbol{\epsilon}_k \tag{1}$$

where $\overline{\boldsymbol{\rho}}_k$ is the differentially corrected carrier-smoothed code measurement vector, $\boldsymbol{e}_k$ is the line of sight matrix, $\boldsymbol{r}_k$ is the deviation on the position of the aircraft relative to the reference station, t_k is the receiver clock error relative to the receiver of the reference station, c is the speed of light, $\boldsymbol{\epsilon}_k \sim \mathcal{N}(0, \boldsymbol{V}_k)$ is a vector containing the errors in $\overline{\boldsymbol{\rho}}_k$.

Utilizing the measurement model in (1), the weighted least squares estimate $\hat{\boldsymbol{r}}_k^{\mathrm{LS}}$ of the position is obtained by

$$\hat{\boldsymbol{r}}_k^{\mathrm{LS}} = \boldsymbol{T}_r \boldsymbol{G}_k^+ \overline{\boldsymbol{\rho}}_k \tag{2}$$

where $\boldsymbol{T}_r$ is the transformation matrix that extracts the position $\boldsymbol{r}_k$ from the augmented GNSS state vector $[\boldsymbol{r}_k, ct_k]^T$ and $\boldsymbol{G}_k^+$ is the weighted pseudo-inverse matrix of $\boldsymbol{G}_k$

$$\boldsymbol{G}_k^+ = \left(\boldsymbol{G}_k^T \boldsymbol{V}_k^{-1} \boldsymbol{G}_k\right)^{-1} \boldsymbol{G}_k^T \boldsymbol{V}_k^{-1} \tag{3}$$

Defining $\hat{\boldsymbol{r}}_k^{\mathrm{LS}} = \boldsymbol{r}_k + \tilde{\boldsymbol{r}}_k^{\mathrm{LS}}$ and substituting (1) into (2), we can obtain the least squares estimation error $\tilde{\boldsymbol{r}}_k^{\mathrm{LS}}$ as

$$\tilde{\boldsymbol{r}}_k^{\mathrm{LS}} = \boldsymbol{T}_r \boldsymbol{G}_k^+ \boldsymbol{\epsilon}_k \tag{4}$$

B. Loosely-coupled Kalman Filter Estimator

Discrete form of the INS process model is obtained in Appendix A as

$$\boldsymbol{x}_k = \boldsymbol{\Phi}\, \boldsymbol{x}_{k-1} + \boldsymbol{\Gamma}\, \tilde{\boldsymbol{u}}_{k-1} + \overline{\boldsymbol{w}}_{k-1} \tag{5}$$

where $\boldsymbol{x} = [\boldsymbol{r}, \boldsymbol{v}, \boldsymbol{E}, \boldsymbol{b}]^T$ is referred to as the INS state vector including deviations in position vector $\boldsymbol{r}$, velocity vector $\boldsymbol{v}$, attitude vector $\boldsymbol{E}$, and IMU bias vector $\boldsymbol{b}$. $\boldsymbol{\Phi}$ is the state transition matrix of the process model, and $\boldsymbol{\Gamma}$ is the discrete input coefficient matrix. $\tilde{\boldsymbol{u}}$ is the IMU measurement vector, and $\overline{\boldsymbol{w}}_k \sim \mathcal{N}(0, \overline{\boldsymbol{W}}_k)$ is the INS process noise vector.

A Kalman filter in a loosely-coupled integration utilizes the GNSS position solution as a measurement to calibrate INS error states. In this work, GBAS provides the GNSS position solution $\hat{\boldsymbol{r}}_k^{\mathrm{LS}}$ obtained from the weighted least squares estimator in (2). The measurement model of the Kalman filter in the loosely-coupled architecture has the typical form

$$\hat{\boldsymbol{r}}_k^{\mathrm{LS}} = \begin{bmatrix}\boldsymbol{I} & 0\end{bmatrix} \begin{bmatrix}\boldsymbol{r}_k \\ \boldsymbol{x}'_k\end{bmatrix} + \tilde{\boldsymbol{r}}_k^{\mathrm{LS}} \tag{6}$$

where $\boldsymbol{x}'_k$ refers to all the states in $\boldsymbol{x}_k$ except $\boldsymbol{r}_k$.

The main assumption in a Kalman filter is that the measurements are uncorrelated over time. On the other hand, $\hat{\boldsymbol{r}}_k^{\mathrm{LS}}$ in (6) are time-correlated. The reason is that the GBAS measurement noise $\boldsymbol{\epsilon}$ in (1) is time-correlated due to the prior hatch (smoothing) filtering. Assuming time constant of the hatch filter is larger than that of the multipath ($\tau_h > \tau_m$), the time correlation of the measurement noise $\boldsymbol{\epsilon}$ can be captured with a first-order Gauss Markov process driven with a white noise $\boldsymbol{\kappa} \sim \mathcal{N}(0, \boldsymbol{K})$ as

$$\underbrace{\begin{bmatrix}\epsilon_k^1 \\ \vdots \\ \epsilon_k^n\end{bmatrix}}_{\boldsymbol{\epsilon}_k} = \underbrace{\begin{bmatrix} e^{-\frac{\Delta t}{\tau_h}} & & 0 \\ & \ddots & \\ 0 & & e^{-\frac{\Delta t}{\tau_h}} \end{bmatrix}}_{\boldsymbol{\Phi}_h} \underbrace{\begin{bmatrix}\epsilon_{k-1}^1 \\ \vdots \\ \epsilon_{k-1}^n\end{bmatrix}}_{\boldsymbol{\epsilon}_{k-1}} + \underbrace{\begin{bmatrix}\kappa_{k-1}^1 \\ \vdots \\ \kappa_{k-1}^n\end{bmatrix}}_{\boldsymbol{\kappa}_{k-1}} \tag{7}$$

where Δt and τ_h are the GNSS receiver sampling time and the hatch filter time constant, respectively. The components of $\boldsymbol{\epsilon}$ and $\boldsymbol{\kappa}$ superscripted from 1 to n are the errors corresponding to the measurements obtained from different satellites.

The measurement error covariance $\boldsymbol{V}_k$ is a diagonal matrix obtained from the hatch filter at steady-state. The error models to construct $\boldsymbol{V}_k$ are defined as a function of elevation of each satellite in GBAS [35]. Incorparating this steady-state value of $\boldsymbol{V}_k$ in the process model (7), the driving noise covariance matrix $\boldsymbol{K}_k$ is obtained as

$$\boldsymbol{K}_k = (\boldsymbol{I} - \boldsymbol{\Phi}_h^2)\, \boldsymbol{V}_k \tag{8}$$

To capture the correlation in Kalman filter equations, we first obtain a zero-noise measurement model by substituting

(4) into (6) and augmenting the colored noise $\boldsymbol{\epsilon}_k$ into the state vector as [38]

$$\hat{\boldsymbol{r}}_k^{\mathrm{LS}} = \underbrace{\begin{bmatrix}\boldsymbol{I} & 0 & \boldsymbol{T}_r\boldsymbol{G}_k^{+}\end{bmatrix}}_{\boldsymbol{H}_k} \underbrace{\begin{bmatrix}\boldsymbol{r}_k \\ \boldsymbol{x}'_k \\ \boldsymbol{\epsilon}_k\end{bmatrix}}_{\mathbf{x}_k} \tag{9}$$

Then, we also augment the Gauss Markov process model for $\boldsymbol{\epsilon}$ in (7) with the INS process model in (5) as

$$\begin{bmatrix}\boldsymbol{x}_{n_k} \\ \boldsymbol{\epsilon}_k\end{bmatrix} = \underbrace{\begin{bmatrix}\boldsymbol{\Phi} & 0 \\ 0 & \boldsymbol{\Phi}_h\end{bmatrix}}_{\boldsymbol{\Phi}_{\mathrm{x}}} \underbrace{\begin{bmatrix}\boldsymbol{x}_{k-1} \\ \boldsymbol{\epsilon}_{k-1}\end{bmatrix}}_{\mathbf{x}_{k-1}} + \underbrace{\begin{bmatrix}\boldsymbol{\Gamma} \\ 0\end{bmatrix}}_{\boldsymbol{\Gamma}_{\mathrm{x}}} \tilde{\boldsymbol{u}}_{k-1} + \underbrace{\begin{bmatrix}\overline{\boldsymbol{w}}_{k-1} \\ \boldsymbol{\kappa}_{k-1}\end{bmatrix}}_{\boldsymbol{w}_{\mathrm{x}_k}} \tag{10}$$

where $\overline{\boldsymbol{w}}_{\mathrm{x}_k} \sim \mathcal{N}(0, \boldsymbol{W}_{\mathrm{x}})$.

Given the augmented process model in (10), the Kalman filter time update is

$$\overline{\mathbf{x}}_k^{\mathrm{KF}} = \boldsymbol{\Phi}_{\mathrm{x}}\hat{\mathbf{x}}_{k-1}^{\mathrm{KF}} + \boldsymbol{\Gamma}_{\mathrm{x}}\tilde{\boldsymbol{u}}_{k-1} \tag{11}$$

where $\overline{\mathbf{x}}_k^{\mathrm{KF}}$ is the a priori estimate of $\mathbf{x}$ at time epoch k.

The measurement update at time epoch k gives the a posteriori estimate $\hat{\mathbf{x}}_k$ as

$$\hat{\mathbf{x}}_k^{\mathrm{KF}} = \overline{\mathbf{x}}_k^{\mathrm{KF}} + \boldsymbol{L}_k\left(\hat{\boldsymbol{r}}_k^{\mathrm{LS}} - \boldsymbol{H}_k\overline{\mathbf{x}}_k^{\mathrm{KF}}\right) \tag{12}$$

where $\boldsymbol{L}_k$ is the Kalman gain at time epoch k, and optimally computed by the aircraft estimator as

$$\boldsymbol{L}_k = \overline{\boldsymbol{P}}_{\mathrm{x}_k}\boldsymbol{H}_k^T(\boldsymbol{H}_k\overline{\boldsymbol{P}}_{\mathrm{x}_k}\boldsymbol{H}_k^T)^{-1} \tag{13}$$

and $\overline{\boldsymbol{P}}_{\mathrm{x}_k}$ is the pre-measurement estimate error covariance of $\mathbf{x}_k$ and is obtained as

$$\overline{\boldsymbol{P}}_{\mathrm{x}_k} = \boldsymbol{\Phi}_{\mathrm{x}}\hat{\boldsymbol{P}}_{\mathrm{x}_{k-1}}\boldsymbol{\Phi}_{\mathrm{x}}^T + \boldsymbol{W}_{\mathrm{x}_{k-1}} \tag{14}$$

and $\hat{\boldsymbol{P}}_{\mathrm{x}_k}$ is the post-measurement estimate error covariance of $\mathbf{x}_k$ and computed as

$$\hat{\boldsymbol{P}}_{\mathrm{x}_k} = (\boldsymbol{I} - \boldsymbol{L}_k\boldsymbol{H}_k)\overline{\boldsymbol{P}}_{\mathrm{x}_k} \tag{15}$$

C. Kalman Filter-based INS Monitor

We use an innovation-based INS monitor, which utilizes Kalman filter in a loosely-coupled INS-GNSS integration. The innovation vector $\boldsymbol{\gamma}$ at time epoch k is defined as

$$\boldsymbol{\gamma}_k = \hat{\boldsymbol{r}}_k^{\mathrm{LS}} - \boldsymbol{H}_k\overline{\mathbf{x}}_k^{\mathrm{KF}} \tag{16}$$

Cumulative test statistic q at time epoch k is defined as the sum of weighted norm of the innovation vectors as

$$q_k = \sum_{i=1}^{k}\boldsymbol{\gamma}_i^T\boldsymbol{S}_i^{-1}\boldsymbol{\gamma}_i \tag{17}$$

where $\boldsymbol{S}_i$ is innovation vector covariance matrix

$$\boldsymbol{S}_i = \boldsymbol{H}_i\overline{\boldsymbol{P}}_{\mathrm{x}_i}\boldsymbol{H}_i^T \tag{18}$$

The proposed INS monitor checks whether the test statistic q_k is smaller than a pre-defined threshold T^2 as

$$q_k < T^2 \tag{19}$$

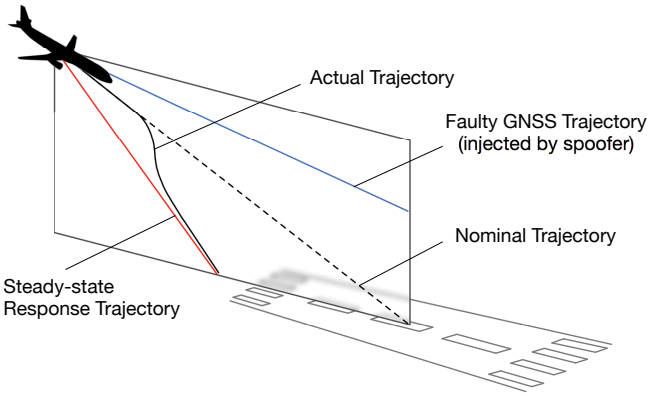

Fig. 2. Impact of the position fault and the consequent autopilot response to the spoofing attack on aircraft trajectory. The dotted line is the nominal or planned approach trajectory, the blue line represents the faulty positions injected by the spoofer, the red line is the steady- state trajectory that the aircraft will maneuver and reach to after responding to the spoofed signal, and the black curve is the actual flight path deviated from the nominal due to autopilots response to the spoofing attack. Note that the blue and red trajectories are symmetric about the nominal approach line.

Under fault free conditions, the test statistic q_k is centrally chi-square distributed with $3k$ degrees of freedom. For a given false alarm requirement, the threshold T^2 is determined from the inverse cumulative chi-square distribution. The INS monitor alarms for a fault if $q_k > T^2$. Under faulted conditions, q_k is non-centrally chi-square distributed with a non-centrality parameter λ_k^2,

$$\lambda_k^2 = \sum_{i=1}^{k}\mathbb{E}[\boldsymbol{\gamma}_i]^T\boldsymbol{S}_i^{-1}\mathbb{E}[\boldsymbol{\gamma}_i] \tag{20}$$

which is used to evaluate the performance of the monitor by computing the probability of missed detection.

III. MONITOR PERFORMANCE EVALUATION

In this section, we derive an evaluation model for the performance of the proposed monitor by fusing the spoofed measurements into the loosely-coupled Kalman filter estimator and detector derived in the previous section. Using this evaluation model, we derive a methodology to quantify the performance of the INS monitor in terms of integrity risk under worst-case spoofing attacks with aircraft position tracking.

A. Evaluation Model for Spoofing Monitor Performance

To quantify the impact of the spoofing attack with position tracking on the proposed monitor performance, we construct a Kalman filter-based estimation error model capturing the impact of the spoofed measurements that contain the spoofer's tracking sensor errors and fault.

In a spoofing attack, the spoofer broadcasts raw code and carrier signals, which mimics the actual GNSS signals with an additional fault

$$\begin{bmatrix}\boldsymbol{\rho}_k^s \\ \lambda\boldsymbol{\phi}_k^s\end{bmatrix} = \begin{bmatrix}\boldsymbol{\rho}_k \\ \lambda\boldsymbol{\phi}_k\end{bmatrix} + \begin{bmatrix}\boldsymbol{I} \\ \boldsymbol{I}\end{bmatrix}\underbrace{(\boldsymbol{f}_k + \boldsymbol{e}_k^T\tilde{\boldsymbol{r}}_k^s)}_{\boldsymbol{f}'} \tag{21}$$

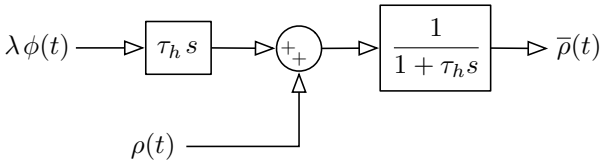

Fig. 3. Block diagram of the continuous carrier-smoothing system (hatch filter). The inputs $\rho(t)$ and $\lambda\phi(t)$ are the code and carrier measurements, respectively. The output of the filter $\overline{\rho}(t)$ is the carrier-smoothed code measurement. τ_h and λ are the filter time constant and L1 carrier wavelength, respectively.

where $\boldsymbol{\rho}_k^s$ and $\boldsymbol{\phi}_k^s$ are the spoofed code and carrier signals, $\boldsymbol{\rho}_k$ and $\boldsymbol{\phi}_k$ are the original code and carrier signals, and $\boldsymbol{f}_k'$ is the resultant fault vector containing the spoofer's position tracking estimation error $\tilde{\boldsymbol{r}}_k^s = \hat{\boldsymbol{r}}_k^s - \boldsymbol{r}_k$ and the computed fault $\boldsymbol{f}_k$.

Equation (21) assumes that the spoofer preserves the consistency in the code and carrier signals by using the same fault for both the code and carrier signals. Otherwise, the spoofing attack detected by the Code Carrier Divergence (CCD) airborne monitors in [10]. Also, the spoofer's position estimation error $\tilde{\boldsymbol{r}}^s$ in (21) is modeled as a white Gaussian noise additive to the computed fault $\boldsymbol{f}_k$, which is a conservative assumption. The reason is that, filtering or smoothing the tracking noise will automatically cause a delay between the spoofer's position estimate and the aircraft's actual dynamic response to the spoofing attack (actuated by autopilot), which will be eventually reflected as an inconsistency between INS and GNSS measurements and improve the detection capability of the monitor [4].

It can be shown that the resultant fault $\boldsymbol{f}_k'$ term in (21) will not be smoothed out by the airborne hatch filter (Fig. 3) since it is the same for the spoofed code and carrier signals. Therefore, the spoofed carrier-smoothed code $\overline{\boldsymbol{\rho}}_k^s$ (output of the filter) can be expressed as

$$\overline{\boldsymbol{\rho}}_k^s = \overline{\boldsymbol{\rho}}_k + \boldsymbol{f}_k' \tag{22}$$

where $\overline{\boldsymbol{\rho}}_k$ is the original carrier-smoothed code for the spoof-free case.

Substituting (1) into (22) gives the spoofed carrier-smoothed code measurement

$$\overline{\boldsymbol{\rho}}_k^s = \underbrace{\begin{bmatrix}\boldsymbol{e}_k^T & 1\end{bmatrix}}_{\boldsymbol{G}_k}\begin{bmatrix}\boldsymbol{r}_k \\ ct_k\end{bmatrix} + \boldsymbol{\epsilon}_k + \boldsymbol{f}_k' \tag{23}$$

Replacing the actual measurement $\overline{\boldsymbol{\rho}}_k$ in (1) with the spoofed measurement $\overline{\boldsymbol{\rho}}_k^s$ in (23) and re-deriving the equations from (2) to (9) yield a spoofed measurement model for the Kalman filter estimator as

$$\hat{\boldsymbol{r}}_k^{\mathrm{LS}} = \boldsymbol{H}_k\mathbf{x}_k + \underbrace{\boldsymbol{T}_r\boldsymbol{G}_k^{+}\boldsymbol{f}_k'}_{\boldsymbol{f}_k''} \tag{24}$$

Substituting (24) in (12) gives the Kalman filter measurement update as a function of the fault as

$$\hat{\mathbf{x}}_k^{\mathrm{KF}} = \underbrace{\left(\boldsymbol{I} - \boldsymbol{L}_k\boldsymbol{H}_k\right)}_{\boldsymbol{L}_k'}\overline{\mathbf{x}}_k^{\mathrm{KF}} + \boldsymbol{L}_k\boldsymbol{H}_k\mathbf{x}_k + \boldsymbol{L}_k\boldsymbol{f}_k'' \tag{25}$$

Substituting the Kalman filter time update equation (11) into (25)

$$\hat{\mathbf{x}}_k^{\mathrm{KF}} = \boldsymbol{L}_k'\boldsymbol{\Phi}_{\mathrm{x}}\hat{\mathbf{x}}_{k-1}^{\mathrm{KF}} + \boldsymbol{L}_k\boldsymbol{H}_k\mathbf{x}_k^{\mathrm{KF}} + \boldsymbol{L}_k'\boldsymbol{\Gamma}_{\mathrm{x}}\tilde{\boldsymbol{u}}_{k-1} + \boldsymbol{L}_k\boldsymbol{f}_k'' \tag{26}$$

Let us define the state estimate error as $\tilde{\mathbf{x}}_k^{\mathrm{KF}} = \hat{\mathbf{x}}_k^{\mathrm{KF}} - \mathbf{x}_k$. Subtracting the INS process model (10) from (26) gives the state estimate error dynamics as

$$\tilde{\mathbf{x}}_k^{\mathrm{KF}} = \boldsymbol{L}_k'\boldsymbol{\Phi}_{\mathrm{x}}\tilde{\mathbf{x}}_{k-1}^{\mathrm{KF}} - \boldsymbol{L}_k'\boldsymbol{w}_{\mathrm{x}_{k-1}} + \boldsymbol{L}_k\boldsymbol{f}_k'' \tag{27}$$

Similarly, the innovation vector under a spoofing attack is obtained by substituting (24) into (16) as

$$\boldsymbol{\gamma}_k = \boldsymbol{f}_k'' - \boldsymbol{H}_k\left(\boldsymbol{\Phi}_{\mathrm{x}}\tilde{\mathbf{x}}_{k-1} - \boldsymbol{w}_{\mathrm{x}_{k-1}}\right) \tag{28}$$

Augmenting the state estimate error model in (27), and the innovation model in (28) results in a performance evaluation model capturing the impact of the error in spoofer's tracking sensors and the fault on the state estimate error, and the innovation:

$$\begin{bmatrix}\tilde{\mathbf{x}}_k^{\mathrm{KF}} \\ \boldsymbol{\gamma}_k\end{bmatrix} = \overbrace{\begin{bmatrix}\boldsymbol{L}_k'\boldsymbol{\Phi}_{\mathrm{x}} & 0 \\ -\boldsymbol{H}_k\boldsymbol{\Phi}_{\mathrm{x}} & 0\end{bmatrix}}^{\boldsymbol{\Phi}_{y_k}}\overbrace{\begin{bmatrix}\tilde{\mathbf{x}}_{k-1}^{\mathrm{KF}} \\ \boldsymbol{\gamma}_{k-1}\end{bmatrix}}^{\boldsymbol{y}_{k-1}} + \overbrace{\begin{bmatrix}-\boldsymbol{L}_k' \\ \boldsymbol{H}_k\end{bmatrix}}^{\boldsymbol{\Upsilon}_{y_k}}\boldsymbol{w}_{\mathrm{x}_{k-1}} + \underbrace{\begin{bmatrix}\boldsymbol{L}_k \\ \boldsymbol{I}\end{bmatrix}}_{\boldsymbol{\Psi}_{y_k}}\boldsymbol{f}_k'' \tag{29}$$

where $\boldsymbol{y}$ is defined as the augmented state vector of the evaluation model capturing the estimate error and innovation dynamics. $\boldsymbol{\Phi}_y$, $\boldsymbol{\Upsilon}_y$, and $\boldsymbol{\Psi}_y$ are the augmented state transition, noise coefficient, and fault input coefficient matrices, respectively.

Using (29), the mean $\mathbb{E}[\boldsymbol{y}_k]$ and covariance $\boldsymbol{Y}_k$ of the evaluation model state vector $\boldsymbol{y}$ can be propagated as

$$\mathbb{E}[\boldsymbol{y}_k] = \boldsymbol{\Phi}_{y_k}\mathbb{E}[\boldsymbol{y}_{k-1}] + \boldsymbol{\Psi}_{y_k}\boldsymbol{f}_{w_k}'' \tag{30}$$

$$\boldsymbol{Y}_k = \boldsymbol{\Phi}_{y_k}\boldsymbol{Y}_{k-1}\boldsymbol{\Phi}_{y_k}^T + \boldsymbol{\Upsilon}_{y_k}\boldsymbol{W}_{\mathrm{x}}\boldsymbol{\Upsilon}_{y_k}^T \tag{31}$$

B. Spoofing Integrity Risk

In this work, integrity risk is used as a metric to quantify the performance of the spoofing monitor. Integrity risk is defined as the probability that the aircraft state estimate error (e.g., altitude error) exceeds an alert limit without being detected (i.e. $q < T^2$). Given spoofing hypothesis H_s, integrity risk at time epoch k is expressed in terms of a cumulative test statistic q_k and the altitude estimate error ε_k as

$$I_{r_k} = \Pr\left(|\varepsilon_k| > l, q_k < T^2 \mid H_s\right) \tag{32}$$

where l is the vertical alert limit, and T^2 is pre-defined threshold for detection which is the same as that in (19).

Since the error in altitude is the most critical in landing approach and vertical requirements are usually the most stringent, it is convenient to evaluate the performance with respect to vertical direction only. The error associated with the altitude ε_k can be extracted from $\tilde{\mathbf{x}}_k$ using the row transformation vector $\boldsymbol{T}_\varepsilon$ as

$$\varepsilon_k = \boldsymbol{T}_\varepsilon \tilde{\mathbf{x}}_k \tag{33}$$

where ε_k is normally distributed.

Cumulative test statistic q_k in (17) is expressed in vector form as

$$q_k = \begin{bmatrix}\boldsymbol{\gamma}_1^T & \dots & \boldsymbol{\gamma}_k^T\end{bmatrix} \underbrace{\begin{bmatrix}\boldsymbol{S}_1^{-1} & & \\ & \ddots & \\ & & \boldsymbol{S}_k^{-1}\end{bmatrix}}_{\boldsymbol{S}_{1:k}^{-1}} \underbrace{\begin{bmatrix}\boldsymbol{\gamma}_1 \\ \vdots \\ \boldsymbol{\gamma}_k\end{bmatrix}}_{\boldsymbol{\gamma}_{1:k}} \tag{34}$$

where $\boldsymbol{S}_k$ is the innovation covariance obtained from $\boldsymbol{Y}_k$ in (31) as

$$\boldsymbol{S}_k = \boldsymbol{T}_\gamma \boldsymbol{Y}_k \boldsymbol{T}_\gamma^T \tag{35}$$

where $\boldsymbol{T}_\gamma$ extracts the rows of $\boldsymbol{y}_k$ corresponding to $\boldsymbol{\gamma}_k$.

Similarly, non-centrality parameter λ^2 of the cumulative test statistic in (20) is

$$\lambda_k^2 = \mathbb{E}[\boldsymbol{\gamma}_{1:k}^T]\, \boldsymbol{S}_{1:k}^{-1}\, \mathbb{E}[\boldsymbol{\gamma}_{1:k}] \tag{36}$$

Using the Kalman filter-based evaluation model in (29), it is proved in [5] that $\mathbb{E}[\tilde{\mathbf{x}}_i \boldsymbol{\gamma}_j^T] = 0$ for all $i \geq j$. Therefore, the cumulative test statistic q_k obtained from innovations and the altitude error ε_k obtained from the current state estimate error will be statistically independent. As a result, the integrity risk I_{r_k} can be written as a product of two probabilities as

$$I_{r_k} = \Pr\left(|\varepsilon_k| > l\right) \Pr\left(q_k < T^2\right) \tag{37}$$

C. Kalman Filter-based Worst-case Fault Derivation

A worst-case fault derivation based on a Kalman filter estimator using tightly-coupled INS-GNSS integration was first introduced by the authors in [5, 6]. This derivation provides an analytical solution to the worst-case fault profile that maximizes the Kalman filter estimate error associated with the most hazardous state ε_k while minimizing the cumulative test statistic q_k or in other words, maximizing the integrity risk.

In this work, we incorporate the same methodology to obtain a worst-case fault solution for the GBAS systems utilizing loosely-coupled INS-GNSS integration in a Kalman filter. The worst case fault history vector $\boldsymbol{f}''_{w_{1:k}}$ that maximizes the failure mode slope $\mathbb{E}[\varepsilon_k]^2/\lambda_k^2$ was derived in [5] as

$$\boldsymbol{f}''_{w_{1:k}} = \alpha\, \overline{\boldsymbol{B}}_{1:k}^{-1} \boldsymbol{S}_{1:k} \overline{\boldsymbol{B}}_{1:k}^{-T} \boldsymbol{A}_k^T \boldsymbol{T}_\varepsilon^T \tag{38}$$

where $\boldsymbol{A}_k$ and $\overline{\boldsymbol{B}}_{1:k}$ are the constant matrices defined in [5] as functions of the deterministic Kalman filter parameters as

$$\begin{aligned} \boldsymbol{A}_k &= \begin{bmatrix}\boldsymbol{A}_{1k} & \dots & \boldsymbol{A}_{kk}\end{bmatrix} \\ \boldsymbol{A}_{ik} &= \begin{cases} \boldsymbol{L}_k^{'} \boldsymbol{\Phi}_{\mathrm{x}} \boldsymbol{L}_{k-1}^{'} \boldsymbol{\Phi}_{\mathrm{x}} \dots \boldsymbol{L}_{1+i}^{'} \boldsymbol{\Phi}_{\mathrm{x}} \boldsymbol{L}_i & \text{if } i < k \\ \boldsymbol{L}_i & \text{if } i = k \end{cases} \end{aligned} \tag{39}$$

and

$$\begin{aligned} \overline{\boldsymbol{B}}_{1:k} &= \begin{bmatrix}\overline{\boldsymbol{B}}_1^T & \dots & \overline{\boldsymbol{B}}_k^T\end{bmatrix}^T \\ \overline{\boldsymbol{B}}_i &= \begin{bmatrix}-\boldsymbol{H}_k \boldsymbol{\Phi}_{\mathrm{x}} \boldsymbol{A}_{k-1} & \boldsymbol{I}_{n\times n} & \boldsymbol{0}_{n\times n(k-i)}\end{bmatrix} \end{aligned} \tag{40}$$

where $\boldsymbol{H}_i$, $\boldsymbol{\Phi}_{\mathrm{x}}$, $\boldsymbol{L}_i^{'}$, and $\boldsymbol{L}_i$ for $i = 1, 2, .., k$ can be extracted using the evaluation model in (29), and n is the number of Kalman filter measurements at each time epoch ($n = 3$ in the loosely-coupled integration).

The magnitude α in (38) is a scalar that is determined to maximize the integrity risk I_{r_k} in (37), which is influenced by the spoofer's position tracking sensor noise $\tilde{\boldsymbol{r}}^s$. In Sections III-A and III-B, we explained how to compute the joint probability $\Pr\left(|\varepsilon_k| > l, q_k < T^2\right)$ for a given deterministic error $\tilde{\boldsymbol{r}}^s$. To statistically account for $\tilde{\boldsymbol{r}}^s$ in the worst-case fault derivation, we generate m number of samples $\tilde{\boldsymbol{r}}_1^s, \tilde{\boldsymbol{r}}_2^s, \dots, \tilde{\boldsymbol{r}}_m^s$ from the normally distributed white error $\tilde{\boldsymbol{r}}^s \sim \mathcal{N}(0, \boldsymbol{P}^s)$ and compute the integrity risk for different values of α as defined in [6]:

$$I_{r_k}(\alpha) = \frac{1}{m} \sum_{i=1}^{m} \Pr\left(|\varepsilon_k| > l; \alpha \mid \tilde{\boldsymbol{r}}_i^s\right) \Pr\left(q_k < T^2; \alpha \mid \tilde{\boldsymbol{r}}_i^s\right) \tag{41}$$

The worst-case value for the fault magnitude α is determined through one dimensional search to maximize $I_{r_k}(\alpha)$ in (41).

IV. PERFORMANCE ANALYSIS RESULTS

To test the performance of the proposed INS spoofing monitor, a covariance analysis with a B747 flight on GBAS-assisted approach is simulated at the standard trimmed flight conditions at 131 knots [17]. The aviation-grade IMU sensor specifications and the parameters for the GBAS error model defined in Appendix B are provided in Table I and Table II, respectively. We assume that the airborne estimator has been running at fault free conditions and has reached steady state before the spoofing attack starts.

To quantify the impact of the spoofing attack period on the integrity risk, we obtained the worst-case fault profiles for different attack periods ranging from 152 to 232 s and computed the corresponding integrity risks assuming the spoofer has perfect position tracking sensors (i.e., $\tilde{\boldsymbol{r}}_k^s = 0$). As seen in Fig. 4, increasing the attack period causes higher integrity risks. The reason is that, increasing the spoofing time allows the spoofer to inject faults to the system in a less aggressive way, slowly corrupting the estimation of INS states

TABLE I
AVIATION-GRADE IMU ERROR PARAMETERS [16]

Parameter	Value	Unit
Gyro angle random walk	0.001	deg/$\sqrt{\text{h}}$
Gyro bias error	0.01	deg/h
Gyro time constant	3600	s
Accelerometer white noise	$10^{-5}g$	m/s^2
Accelerometer bias error	$10^{-5}g$	m/s^2
Accelerometer bias time constant	3600	s

TABLE II
GBAS ERROR MODEL PARAMETERS [36]

Parameter	Value	Unit
Carrier-smoothing time constant	100	s
Radius of Earth	6378.1363	km
Ionospheric shell height	350	km
Tropospheric scale height	7.3	km
Ionospheric vertical gradient	4	mm/km
Airborne receiver noise (AAD-B)	15	cm
Number of ground antenna	4	-
Number of satellites in view	6	-
Satellite elevations	$31^{o} \leq \theta \leq 63^{o}$	deg

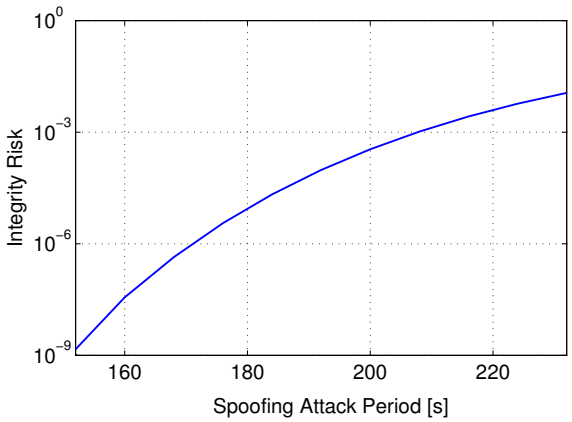

Fig. 4. The impact of spoofing attack period on the integrity risk. The results are obtained for B747 GBAS-assisted approaches in the presence of worst-case spoofing attacks when the spoofer is capable of tracking the aircraft position with perfect accuracy.

and thereby reducing the monitors ability to detect the spoofing attack. On the other hand, even though we conservatively assumed that the spoofer tracks the aircraft position with zero-error, the worst-case spoofing fault for a standard B747 approach of 150 s results in an integrity risk of less than 10^{-9}, which satisfies the most stringent safety requirement in aviation [34].

The results so far assume that the spoofer is able to estimate the exact position of the aircraft. In a more realistic scenario, the errors in position tracking must be accounted for. Therefore, we assume that the spoofers position estimate error is a zero-mean white noise $\tilde{\boldsymbol{r}}_k^s$ sequence. White noise is typical for laser tracking errors. Utilizing (41), we illustrate how the INS monitor leverages the spoofers altitude tracking errors to detect spoofing attacks. Fig. 5 shows that for a position tracking error of more than 6 cm (1-σ), the integrity risk always remains below 10^{-9} for spoofing attacks having a period of up to 200 s. This 200 s attack period is conservative since the standard B747 approach is 150 s and the spoofer have a limited range. The results are promising because such tracking accuracy is high considering existing high-grade position tracking systems (e.g., laser, radar, vision). Also, maintaining this high tracking accuracy during whole approach of the aircraft is unrealistic

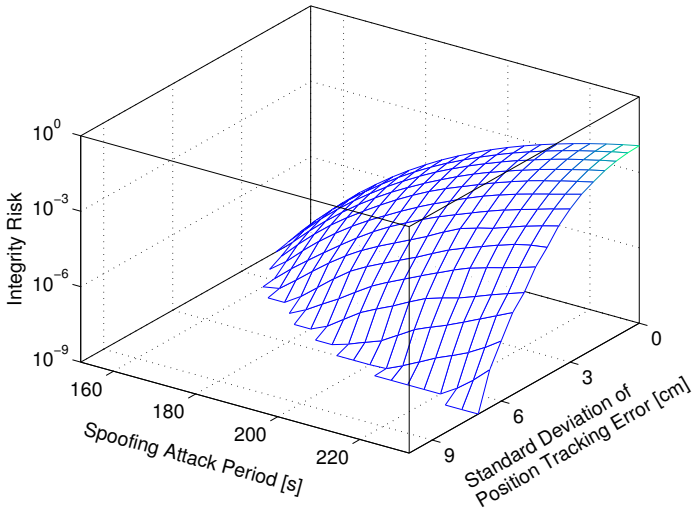

Fig. 5. The influence of spoofer's tracking errors on detection performance of the monitor using loosely-coupled INS/GNSS integration in terms of the integrity risk.

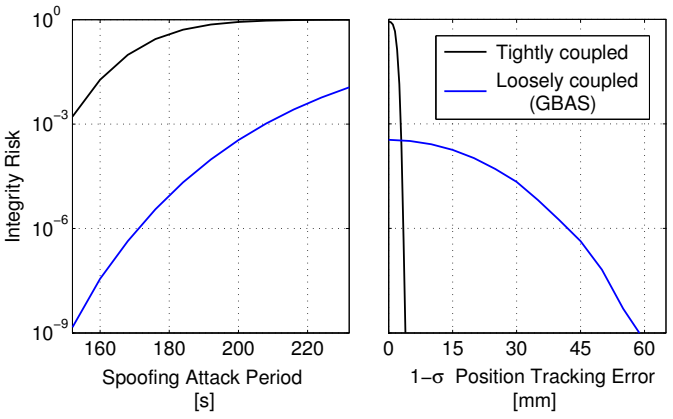

Fig. 6. Comparison of performance of the INS monitors for the tightly and loosely-coupled systems. The integrity risk are given as a function of spoofing attack period in the presence of worst-case spoofing attacks with perfect tracking (left). The monitor sensitivity to the spoofer's tracking error for an example approach of 200 s is also given in terms of the integrity risk (right). The integrity risk values for the tightly-coupled systems (black curves) are obtained from the prior work in [5] and [6].

due to uncertainties in the lever arm from the GNSS antenna location to the spoofer's measuring point on the aircraft.

The covariance analysis so far demonstrates the performance of the INS monitor using loosely-coupled systems (i.e., GBAS). The monitor performance for tightly-coupled systems (i.e., shipboard landing and autonomous airborne refueling) was shown in the prior work [5,6]. Fig. 6 compares detection capability of the monitor implemented with the loosely and tightly-coupled systems. The left plot shows the integrity risk values as a function of the spoofing attack period in presence of worst-case spoofing attacks with perfect position tracking. The plot shows that the loosely coupled INS/GNSS integration results in a better integrity than the tightly-coupled integration

does. The reason is that the tightly-coupled integration scheme gives the spoofer better opportunity to fuse the GNSS spoofing fault into the system and thereby corrupt the IMU biases. On the other hand, in a more realistic scenario where the spoofer has position tracking errors, the right plot illustrates that the monitor with the tightly-coupled systems is more sensitive to the spoofer's tracking errors than that with the loosely-coupled systems. For example, for the same spoofing attack period (200 s), the tracking error (1-σ) resulting in a 10^{-9} integrity risk is 4 mm in the tightly-coupled systems, whereas it is 60 mm in the loosely-coupled systems.

V. CONCLUSION

This work proposed a monitor to detect spoofing attacks during GBAS and SBAS-assisted aircraft final approaches. It is an innovation-based monitor using loosely-coupled IMU sensors and GNSS receivers. To evaluate the performance of the monitor, we first established a stochastic spoofing integrity analysis methodology, then obtained the worst-case spoofing fault that maximizes the integrity risk. The B747 simulation results show that even when the spoofer achieves the worst-case scenario by closed-loop tracking of the aircraft position, the monitor is still highly effective in detecting spoofing attacks during GBAS-assisted approaches with low integrity risk. Also, different INS/GNSS integration schemes were evaluated by quantifying trade-offs between the loosely and tightly-coupled navigation systems. It was found that the tightly-coupled INS/GNSS monitor is more sensitive to the spoofer's tracking errors.

ACKNOWLEDGMENT

The authors gratefully acknowledge the FAA for supporting this research. However, the opinions expressed in this paper are the authors alone and do not necessarily represent those of any other organization or person.

Appendix A
INS KINEMATIC MODEL

The estimator in INS utilizes a kinematic model to predict the aircraft motion as [14]

$$\dot{\boldsymbol{x}}_n = \boldsymbol{F}_n\,\boldsymbol{x}_n + \boldsymbol{G}_u\,\boldsymbol{u} \tag{42}$$

where $\boldsymbol{x}_n = [\boldsymbol{r}, \boldsymbol{v}, \boldsymbol{E}]^T$ is referred to as the INS state vector including deviations in position vector $\boldsymbol{r}$, velocity vector $\boldsymbol{v}$, and attitude vector $\boldsymbol{E}$ of the aircraft. $\boldsymbol{F}_n$ is plant matrix of the kinematic model, $\boldsymbol{G}_u$ is input coefficient matrix, and $\boldsymbol{u} = [\mathbf{f}, \boldsymbol{\omega}]^T$ contains the deviations in specific force $\mathbf{f}$ and angular velocity $\boldsymbol{\omega}$ relative to the inertial frame.

IMU measures the deviations in specific force and angular velocity, and the IMU measurement $\tilde{\boldsymbol{u}}$ is expressed in terms of $\boldsymbol{u}$ in (42) as

$$\tilde{\boldsymbol{u}} = \boldsymbol{u} + \boldsymbol{b} + \boldsymbol{\nu}_n \tag{43}$$

$\boldsymbol{\nu}_n$ is a 6×1 vector including accelerometer and gyroscope white noises, which are uncorrelated and zero-mean and $\boldsymbol{b}$ is a 6×1 IMU bias vector that is modeled as a first order Gauss Markov process as

$$\dot{\boldsymbol{b}} = \boldsymbol{F}_b\,\boldsymbol{b} + \boldsymbol{\eta}_b \tag{44}$$

where $\boldsymbol{\eta}_b$ represents the bias driving white noise and $\boldsymbol{F}_b$ is a diagonal bias dynamic matrix, the elements of which are the negative inverses of the bias time constants of the sensors.

Using (43), we augment the bias dynamics in (44) with the INS model in (42), which yields a process model for the Kalman filter as

$$\begin{bmatrix} \dot{\boldsymbol{x}}_n \\ \dot{\boldsymbol{b}} \end{bmatrix} = \underbrace{\begin{bmatrix} \boldsymbol{F}_n & -\boldsymbol{G}_u \\ 0 & \boldsymbol{F}_b \end{bmatrix}}_{\boldsymbol{F}} \underbrace{\begin{bmatrix} \boldsymbol{x}_n \\ \boldsymbol{b} \end{bmatrix}}_{\boldsymbol{x}} + \underbrace{\begin{bmatrix} \boldsymbol{G}_u \\ 0 \end{bmatrix}}_{\boldsymbol{G}_u^{'}} \tilde{\boldsymbol{u}} + \underbrace{\begin{bmatrix} -\boldsymbol{G}_u & 0 \\ 0 & \boldsymbol{I} \end{bmatrix}}_{\boldsymbol{G}_w} \underbrace{\begin{bmatrix} \boldsymbol{\nu}_n \\ \boldsymbol{\eta}_b \end{bmatrix}}_{\boldsymbol{w}} \tag{45}$$

Defining $\overline{\boldsymbol{w}} = \boldsymbol{G}_w \boldsymbol{w}$, discrete form of the process model in (45) is written as:

$$\boldsymbol{x}_k = \boldsymbol{\Phi}\,\boldsymbol{x}_{k-1} + \boldsymbol{\Gamma}\,\tilde{\boldsymbol{u}}_{k-1} + \overline{\boldsymbol{w}}_{k-1} \tag{46}$$

where $\boldsymbol{\Phi}$ is the state transition matrix of the process model, and $\boldsymbol{\Gamma}$ is the discrete form of $\boldsymbol{G}_u^{'}$. $\overline{\boldsymbol{w}}_k \sim \mathcal{N}(0, \overline{\boldsymbol{W}}_k)$. The IMU measurement $\tilde{\boldsymbol{u}}_k$ can be treated as a deterministic input to the process model in (46).

Appendix B
GBAS ERROR MODELS

In this section, standard error models for GBAS differential processing are given based on Ground Accuracy Designator-C (GAD-C) and Airborne Accuracy Designator-B (AAD-B). The total GBAS measurement error vector $\boldsymbol{\epsilon}$ in (1) has a diagonal covariance matrix

$$\boldsymbol{V} = \begin{bmatrix} \sigma^2(\theta_1) & & \\ & \ddots & \\ & & \sigma^2(\theta_n) \end{bmatrix} \tag{47}$$

where $\sigma(\theta_j)$ is the standard deviation of the total GBAS measurement error corresponding to j^{th} satellite, θ is the elevation angle, n is the total number of satellites.

σ is a function of elevation angle of satellites and composed of airborne σ_a, ground station σ_g, tropospheric σ_t, and ionospheric σ_i standard deviations [35]

$$\sigma(\theta) = \sqrt{\sigma_a^2 + \sigma_g^2 + \sigma_t^2 + \sigma_i^2} \tag{48}$$

where σ_a contains airborne receiver noise σ_n and multipath σ_m components [36]

$$\sigma_a = \sqrt{\sigma_n^2 + \sigma_m^2} \tag{49}$$

and σ_m is modeled as [35]

$$\sigma_m(\theta) = 0.13 + 0.53\,\mathrm{e}^{-\theta/10^{\circ}} \tag{50}$$

The residual tropospheric error for the airborne equipment σ_t is computed as [35]

$$\sigma_t(\theta) = \sigma_N\,h_0 \frac{10^{-6}}{\sqrt{0.002 + \sin^2\theta}} (1 - \mathrm{e}^{-\Delta h/h_0}) \tag{51}$$

where σ_N is the refractivity uncertainty transmitted by ground subsystem, h_0 is the tropospheric scale height, and Δh is the height of the aircraft above the GBAS reference point.

The ionospheric error model is given as [35]

$$\sigma_i(\theta) = F_p \, \sigma_{\nabla i} \, (x_a + 2 \, \tau_h \, v_a) \tag{52}$$

where $\sigma_{\nabla i}$ is the standard deviation for the nominal ionospheric vertical spatial gradient, x_a is the slant range distance between current aircraft location and the ground station, v_a is the horizontal aircraft velocity, and F_p is the vertical-to-slant obliquity factor defined as [35]

$$F_p = \frac{1}{\sqrt{1 - \left(\dfrac{R_e \cos\theta}{R_e + h_I} \right)^2}} \tag{53}$$

where h_I is the ionospheric shell height.

The total ground station error is composed of the ground reference receiver errors $\sigma_{g,r}$ and the signal-in-space errors $\sigma_{g,s}$ as [37]

$$\sigma_g(\theta) = \sqrt{\frac{\sigma_{g,r}^2}{M} + \sigma_{g,s}^2} \tag{54}$$

where M is the number of reference station antennas.

The total ground reference receiver error including noise and multipath is modeled as [37]

$$\sigma_{g,r}(\theta) = \begin{cases} 0.15 + 0.84 \, \mathrm{e}^{\theta / 15.5^\circ}, & \theta \geq 35^\circ \\ 0.24, & \theta < 35^\circ \end{cases} \tag{55}$$

and the ground signal-in-space errors are modeled as [37]

$$\sigma_{g,s}(\theta) = \sqrt{0.04^2 + 0.01^2 \, F_p} \tag{56}$$

REFERENCES

[1] Khanafseh, S., Roshan, N., Langel, S., Chan, F., Joerger, M., Pervan, B., GPS Spoofing Detection Using RAIM with INS Coupling, ION PLANS Conference, Monterey, CA, May 2014.

[2] Tanil, C., Khanafseh, S., Pervan, B., The Impact of Wind Gust on Detectability of GPS Spoofing Attack Using RAIM with INS Coupling, IEEE/ION PNT Conference, Honolulu, HI, April 2015.

[3] Tanil, C., Khanafseh, S., Pervan, B., Detecting GNSS Spoofing Attacks Using Inertial Sensing of Aircraft Disturbance Response, submitted to the Journal of Navigation on March 2016.

[4] Tanil, C., Khanafseh, S., Pervan, B. GNSS Spoofing Attack Detection using Aircraft Autopilot Response to Deceptive Trajectory, ION GNSS+ Conference, Tampa, FL, September 2015.

[5] Tanil, C., Khanafseh, S., Joerger, M., Pervan, B. Kalman Filter-based INS Monitor to Detect GNSS Spoofers Capable of Attacking Aircraft Position, ION PLANS Conference, Savannah, GA, April 2016.

[6] Tanil, C., Khanafseh, S., Joerger, M., Pervan, B., An INS Monitor to Detect GNSS Spoofers Capable of Tracking Vehicle Position, submitted to the IEEE Transactions on Aerospace and Electronics on July 2016.

[7] Joerger, M., B. Pervan, Kalman Filter-Based Integrity Monitoring Against Sensor Faults, Journal of Guidance, Control, and Dynamics, Vol. 36, No. 2 (2013), pp. 349-361.

[8] Steven Langel, Samer Khanafseh, Fang-C. Chan, and Boris Pervan, Tightly Coupled GPS/INS Integration for Differential Carrier Phase Navigation Systems Using Decentralized Estimation, in Proceedings of IEEE/ION PLANS 2010, Palm Springs, CA, May 2010.

[9] Khanafseh, S. and Pervan, B. "Autonomous Airborne Refueling of Unmanned Air Vehicles Using the Global Positioning System," Journal of Aircraft, Vol. 44, No. 5, Sep.-Oct. 2007

[10] Simili, D., V., and Pervan, B., Code-Carrier Divergence Monitoring for the GPS Local Area Augmentation System, 2006 IEEE/ION Position, Location, And Navigation Symposium, 2006, pp. 483-493. doi: 10.1109/PLANS.2006.1650636

[11] Parkinson, B. W., and Axelrad, P., Autonomous GNSS Integrity Monitoring Using the Pseudorange Residual, NAVIGATION, Washington, DC, Vol. 35, No. 2, 1988, pp. 225-274.

[12] Humphreys, T. E., Ledvina, B. M., Psiaki, M. L., O'Hanlon, B. W., Kintner, P. M. Jr., Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer, ION GNSS Conference, Savannah, GA, September 2008.

[13] Mark L. Psiaki, Steven P. Powell, and Brady W. OHanlon, 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

[14] Farrell, J. (2008). Aided navigation: GNSS with high rate sensors. McGraw-Hill, Inc.

[15] Misra, P., Enge, P. (2006). Global Positioning System: Signals, Measurements and Performance Second Edition. Lincoln, MA: Ganga-Jamuna Press.

[16] Brown, R. G., P. Y. C Hwang, Introduction to Random Signals and Applied Kalman Filtering. 3rd Ed. New York: John Wiley Sons, 1997.

[17] Heffley, R. K., Jewell, W. F. (1972). Aircraft Handling Qualities Data.

[18] Ali Jafarnia-Jahromi, Ali Broumandan, John Nielsen, and Grard Lachapelle, GPS Vulnerability to Spoofing Threats and a Review of Antispoofing Techniques, International Journal of Navigation and Observation, vol. 2012, Article ID 127072, 16 pages, 2012. doi:10.1155/2012/127072

[19] Jovanovic, A.; Botteron, C.; Farine, P.-A., "Multi-test detection and protection algorithm against spoofing attacks on GNSS receivers," in Position, Location and Navigation Symposium - PLANS 2014, 2014 IEEE/ION , vol., no., pp.1258-1271, 5-8 May 2014

[20] Wesson, K. D., Rothlisberger, M. P., Humphreys, T. E., "A Proposed Navigation Message Authentication Implementation for Civil GNSS 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.

[21] Ledvina, M. Brent and Bencze, J. William and Galusha, Brian and Miller, Issac, An In-Line Spoofing Module for Legacy GPS Receivers, in Proceedings of the US Institute of Navigation International Technical Meeting, 2010, pp. 698-712.

[22] G. W. Hein, F. Kneissl, J. A. Avila-Rodriguez, and S. Wallner, Authenticating GNSS: Proofs Against Spoofs Part 2, GNSS magazine, pp. 5863, 2007

[23] Akos, Dennis M., Whos Afraid of the Spoofer? GPS/GNSS Spoofing Detection via Automatic Gain Control (AGC), NAVIGATION, Journal of The Institute of Navigation, Vol. 59, No. 4, Winter 2012, pp. 281-290.

[24] C. E. McDowell, GPS Spoofer and Repeater Mitigation System using Digital Spatial NullingUS Patent 7250903 B1, 2007.

[25] J. Nielsen, A. Broumandan, and G. Lachapelle, Spoofing detection and mitigation with a moving handheld receiver, GPS World, vol. 21, no. 9, pp. 2733, 2010.

[26] Meurer, Michael, Konovaltsev, Andriy, Cuntz, Manuel, HŁttich, Christian, "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.

[27] S. Moshavi, Multi-user detection for DS-CDMA communications, IEEE Communications Magazine, vol. 34, no. 10, pp. 124135, 1996.

[28] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle, 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, pp. 181191, 2012.

[29] H. Wen, P. Y. R. Huang, J. Dyer, A. Archinal, and J. Fagan, Countermeasures for GPS signal spoofing, in Proceedings of the 18th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS '05), pp. 12851290, Long Beach, Calif, USA, September 2005.

[30] D.H Titterton, J.L. Weston, Strapdown Inertial Navigation Technology, The American Institute of Aeronautics and Astronautics, 2004.

[31] J. S. Warner and R. G. Johnston, GPS spoofing countermeasures, Homeland Security Journal, Dec. 2003.

[32] P. F. Swaszek, K. C. Seals, S. A. Pratz, B. N. Arocho, and R. J. Hartnett,

GNSS spoof detection using shipboard IMU measurements, Proc. ION GNSS+ 2014, Tampa FL, Sept. 2014.
[33] P. F. Swaszek, R. J. Hartnett, K. C. Seals, "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.
[34] International Civil Aviation Organization. International Standards and Recommended Practices, Annex 10, volume I: Radio Navigation Aids. New Zealand, sixth edition, July 2006.
[35] RTCA DO-253C. Minimum Operational Performance Standards for the Local Area Augmentation System (LAAS), December 2008.
[36] RTCA DO-245A. Minimum Aviation System Performance Standards for the Local Area Augmentation System (LAAS), December 2004.
[37] McGraw, Gary A., Murphy, Tim, Brenner, Mats, Pullen, Sam, Van Dierendonck, A. J., "Development of the LAAS Accuracy Models," Proceedings of the 13th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GPS 2000), Salt Lake City, UT, September 2000, pp. 1212-1223.
[38] Crassidis, John L., and John L. Junkins. Optimal estimation of dynamic systems. CRC press, 2011.