An INS Monitor to Detect GNSS Spoofers Capable of Tracking Vehicle Position

ÇAĞATAY TANIL
SAMER KHANAFSEH
MATHIEU JOERGER, Member, IEEE
BORIS PERVAN, Senior Member, IEEE
Illinois Institute of Technology, Chicago, IL USA

In this paper, we describe and evaluate a new monitor that uses inertial navigation system (INS) measurements to detect spoofing attacks on global navigation satellite system (GNSS) receivers. Spoofing detection is accomplished by monitoring the Kalman filter innovations in a tightly coupled INS/GNSS mechanization. Monitor performance is evaluated against worst case spoofing attacks, including spoofers capable of tracking vehicle position. There are two main contributions of this paper. The first is a mathematical framework to quantify post-monitor spoofing integrity risk. The second is an analytical expression of the worst case sequence of spoofed GNSS signals. We then apply these to an example spoofing attack on a Boeing 747 on final approach. The results show that GNSS spoofing is easily detected, with high integrity, unless the spoofer's position-tracking devices have unrealistic, near-perfect accuracy, and no delays.

Manuscript received July 12, 2016; revised February 22, 2017 and July 28, 2017; released for publication July 30, 2017. Date of publication August 15, 2017; date of current version February 7, 2018.

DOI. No. 10.1109/TAES.2017.2739924

Refereeing of this contribution was handled by G. X. Gao.

This work was supported by the Federal Aviation Administration.

Authors' addresses: Ç. Tanıl, S. Khanafseh, M. Joerger, and B. Pervan are with the Illinois Institute of Technology, Chicago, IL 60616 USA, E-mail: (ctanil@hawk.iit.edu; khansam1@iit.edu; joermat@iit.edu; pervan@iit.edu). *(Corresponding author: Çağatay Tanıl.)*

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 [1]. In this paper, we propose a novel inertial navigation system (INS) monitor and statistically validate its performance against worst case GNSS spoofing attacks, even when the spoofer has the ability to estimate the real-time position of the aircraft—for example, by means of remote tracking from the ground. Our specific application of interest is aircraft precision approach and landing, but the methods introduced here are also applicable to other GNSS positioning systems that are already tightly coupled with inertial sensors.

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 [1]. Numerous antispoofing techniques have been developed and vulnerability of these existing methods have been discussed in [2]–[5]. These include cryptographic authentication techniques employing modified GNSS navigation data [6]–[8], spoofing discrimination using spatial processing by antenna arrays and automatic gain control schemes [9]–[11], GNSS signal direction of arrival comparison [12], code and phase rate consistency checks [13], high-frequency antenna motion [14], and signal power monitoring techniques [15], [16]. Augmenting data from auxiliary sensors such as inertial measurement units (IMU) and independent radar sensors to discriminate the spoofing have also been proposed in [17]–[19]. 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 [20]–[23].

The INS detector introduced in [20]–[22] 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. Here, the redundancy required for detection is provided through INS measurements, unlike conventional usage of RAIM, where detection is provided through satellite redundancy [24]. 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 [25].

In [20], 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. Furthermore, 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 also 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 [21] and [22], 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 of specific gust disturbance profiles (e.g., 10^9 to meet aircraft landing integrity requirements). In [23], we investigated the impact on spoofing detection due to aircraft response to control actions (actuated by the autopilot) due to the spoofed GNSS signals. In response to the manipulated (spoofed) 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 the prior work [20]–[23] is that the spoofer does not have real-time knowledge of the actual aircraft position during spoofing attack. In [26], a closed-loop tracking and spoofing was demonstrated on a standard receiver of a small drone using example spoofing strategies including ramp and acceleration type fault profiles. In [27] and this paper, we consider spoofers capable of tracking and estimating the position of the target aircraft and implementing a Kalman-filter-based worst case fault profile that maximizes the integrity risk.

Beyond our recent work in [27], this paper builds a more comprehensive performance evaluation model that captures the aircraft controller dynamic response (actuated by either the pilot or autopilot) to a worst case spoofing attack, augmented with a Kalman-filter-based estimator and innovation-based INS detector dynamics. We also allow for a maximum level of awareness on the part of the spoofer by introducing a stochastic methodology for the spoofer to account for his/her own tracking sensor errors in his/her worst case fault derivation. Finally, using the worst case fault with the evaluation model, we perform covariance analysis to quantify the performance of the monitor in terms of integrity risk for a B747 landing approach. The simulation results show that even if a spoofer injects the worst case spoofed signal based on his/her sensed position of the aircraft, the spoofer's tracking sensor errors will be reflected as inconsistency in the innovations that are detectable by the INS monitor with low integrity risk.

After this introductory section, Section II-A constructs the GNSS measurement and INS kinematics models, and explains tightly coupled INS/GNSS integration scheme for Kalman filter estimator. Section II-B describes the proposed Kalman-filter-based INS airborne monitor against GNSS spoofing. In Sections III-A1 and III-A2, a closed-loop performance evaluation model is derived to capture the impact of GNSS faults on the controller, estimator, and detector. The monitor performance is evaluated against worst case spoofing attacks by first constructing a mathematical framework to quantify the postmonitor spoofing integrity risk in Section III-B, then deriving an analytical expression of the worst case sequence of spoofed GNSS signals in Sections III-C. Finally, in Section IV, the performance of the monitor is demonstrated with a spoofing attack to an example relative navigation aircraft landing application.

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 ultratightly coupled mode in which the INS directly aids the GNSS tracking loops [28]. This paper assumes a nominal tightly coupled integration because we expect it to be a widely used implementation for integrated GNSS-INS in aviation (providing superior performance to loosely coupled systems but without the excessive cost and complexity associated with ultratight systems). As such, the INS monitor described here operates continuously and can be implemented directly on top of any tightly coupled GNSS-INS system. However, the concepts introduced here are transferable to other types of integration as well.

A. Tightly Coupled INS/GNSS Kalman Filter Estimator

In this section, we describe a nominal INS/GNSS tightly coupled mechanization. It will be needed later for the performance evaluation of the monitor.

The estimator in INS utilizes a kinematic model to predict the aircraft motion as [29]

$$\dot{\boldsymbol{x}}_n = \boldsymbol{F}_n \boldsymbol{x}_n + \boldsymbol{G}_u \boldsymbol{u} \tag{1}$$

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

The 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 (1) as

$$\tilde{\boldsymbol{u}} = \boldsymbol{u} + \boldsymbol{b} + \boldsymbol{v}_n \tag{2}$$

where $\boldsymbol{v}_n$ is a 6×1 vector including accelerometer and gyroscope white noises, which are mutually 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

$$\dot{\boldsymbol{b}} = \boldsymbol{F}_b\, \boldsymbol{b} + \boldsymbol{\eta}_b \tag{3}$$

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 (2), we augment the bias dynamics in (3) with the INS model in (1), which yields a process model for the Kalman filter as

$$\begin{bmatrix} \dot{\boldsymbol{x}}_n \\ \dot{\boldsymbol{b}} \end{bmatrix} = \overbrace{\begin{bmatrix} \boldsymbol{F}_n & -\boldsymbol{G}_u \\ 0 & \boldsymbol{F}_b \end{bmatrix}}^{\boldsymbol{F}} \overbrace{\begin{bmatrix} \boldsymbol{x}_n \\ \boldsymbol{b} \end{bmatrix}}^{\boldsymbol{x}} + \overbrace{\begin{bmatrix} \boldsymbol{G}_u \\ 0 \end{bmatrix}}^{\boldsymbol{G}_u'} \tilde{\boldsymbol{u}} + \underbrace{\begin{bmatrix} -\boldsymbol{G}_u & 0 \\ 0 & \boldsymbol{I} \end{bmatrix}}_{\boldsymbol{G}_w} \underbrace{\begin{bmatrix} \boldsymbol{v}_n \\ \boldsymbol{\eta}_b \end{bmatrix}}_{\boldsymbol{w}}. \tag{4}$$

Defining $\overline{\boldsymbol{w}} = \boldsymbol{G}_w \boldsymbol{w}$, the discrete form of the process model in (4) is written as

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

where $\boldsymbol{\Phi}$ is the state transition matrix of the process model $\boldsymbol{F}$, $\boldsymbol{\Gamma}$ is the discrete form of $\boldsymbol{G}_u'$, $\overline{\boldsymbol{w}}_k \sim \mathcal{N}(0, \overline{\boldsymbol{W}}_k)$ is the augmented process noise, and $\overline{\boldsymbol{W}}_k$ is the covariance matrix of $\overline{\boldsymbol{w}}_k$. The IMU measurement $\tilde{\boldsymbol{u}}_k$ is a deterministic input to the process model in (5).

We next integrate the INS with differential GNSS ranging measurements. The actual GNSS code and carrier phase measurement equation linearized about a nominal position are expressed at the kth time epoch as [30]

$$\boldsymbol{z}_k = \boldsymbol{G}^*\, \delta \boldsymbol{r}_k + \boldsymbol{v}_{\rho\phi_k} \tag{6}$$

where $\boldsymbol{z}_k$ is the GNSS measurement vector containing differential carrier and code phase measurements, $\boldsymbol{G}^*$ is the observation matrix including line-of-sight information from the reference station to the satellites in the navigation frame, $\delta \boldsymbol{r}_k$ is the deviation on the position of the aircraft relative to the reference station represented in navigation frame, $\boldsymbol{v}_{\rho\phi_k} \sim \mathcal{N}(0, \boldsymbol{V}_k)$ includes the carrier and code measurement error vectors, and $\boldsymbol{V}_k$ is the covariance matrix of $\boldsymbol{v}_{\rho\phi_k}$.

In a tightly coupled mechanization, raw INS and GNSS data are processed in a unified Kalman filter where the coupling between the INS process model and GNSS measurement model can be obtained by first relating the state vector $\delta \boldsymbol{r}_k$ in (21) to the state vector $\boldsymbol{x}_k$ in the process model in (5) as

$$\boldsymbol{x}_k = \begin{bmatrix} \delta \boldsymbol{r}_k \\ \boldsymbol{x}_k' \end{bmatrix} \tag{7}$$

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

Using the relation in (7), the measurement in (21) is reformulated as

$$\boldsymbol{z}_k = \underbrace{\begin{bmatrix} \boldsymbol{G}_k^* & 0 \end{bmatrix}}_{\boldsymbol{H}_k} \underbrace{\begin{bmatrix} \delta \boldsymbol{r}_k \\ \boldsymbol{x}_k' \end{bmatrix}}_{\boldsymbol{x}_k} + \boldsymbol{v}_{\rho\phi_k} \tag{8}$$

where $\boldsymbol{H}_k$ is the observation matrix of the augmented measurement model. The state vector in (5) and (8) is augmented with GNSS multipath and cycle ambiguity states, which are not shown for simplicity. However, they are accounted for in the implementation used to obtain the results in Section IV.

Given the process model in (5), the Kalman filter time update is

$$\overline{\boldsymbol{x}}_k = \boldsymbol{\Phi}\, \hat{\boldsymbol{x}}_{k-1} + \boldsymbol{\Gamma}\, \tilde{\boldsymbol{u}}_{k-1} \tag{9}$$

where $\overline{\boldsymbol{x}}_k$ and $\hat{\boldsymbol{x}}_{k-1}$ are the *a priori* estimate of $\boldsymbol{x}$ at time epoch k and *a posteriori* estimate of $\boldsymbol{x}$ at $k-1$, respectively.

Using (6) and (9), the measurement update at time epoch k gives the *a posteriori* estimate $\hat{\boldsymbol{x}}_k$ as

$$\hat{\boldsymbol{x}}_k = \overline{\boldsymbol{x}}_k + \boldsymbol{L}_k\big(\boldsymbol{z}_k - \boldsymbol{H}_k\, \overline{\boldsymbol{x}}_k\big) \tag{10}$$

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

$$\boldsymbol{L}_k = \hat{\boldsymbol{P}}_k \boldsymbol{H}_k^T \boldsymbol{V}_k^{-1} \tag{11}$$

and $\hat{\boldsymbol{P}}_k$ is the postmeasurement state estimate error covariance matrix at time epoch k, which is obtained as

$$\hat{\boldsymbol{P}}_k = \Big(\overline{\boldsymbol{P}}_k^{-1} + \boldsymbol{H}_k^T \boldsymbol{V}_k^{-1} \boldsymbol{H}_k\Big)^{-1} \tag{12}$$

where $\overline{\boldsymbol{P}}_k$ is the premeasurement state estimate error covariance matrix at time k, computed as

$$\overline{\boldsymbol{P}}_k = \boldsymbol{\Phi}\, \hat{\boldsymbol{P}}_{k-1}\, \boldsymbol{\Phi}^T + \overline{\boldsymbol{W}}_{k-1} \tag{13}$$

B. Kalman-Filter-Based INS Monitor

We implement an innovation-based INS monitor, which utilizes the Kalman filter innovation vector from the INS/GNSS integration. The proposed detector in this paper are simple, efficient, and can directly be implemented on top of tightly coupled INS/GNSS integrations without requiring any modification to the existing navigation system. However, when building a new integrated navigation system, it is possible to construct the design such that both estimation accuracy and fault detection performance are maximized. Such flexibility would lead to a computationally more complex but optimal detector.

The innovation vector $\boldsymbol{\gamma}$ at time epoch k is defined as

$$\boldsymbol{\gamma}_k = \boldsymbol{z}_k - \boldsymbol{H}_k\, \overline{\boldsymbol{x}}_k \tag{14}$$

where the *a priori* estimate of $\boldsymbol{x}_k$ is obtained from the Kalman filter time update in (9).

A cumulative test statistic q at time epoch k is defined as the sum of squares of the normalized innovation vectors over time as

$$q_k = \sum_{i=1}^{k} \boldsymbol{\gamma}_i^T\, \boldsymbol{S}_i^{-1}\, \boldsymbol{\gamma}_i \tag{15}$$

where $\boldsymbol{S}_i$ is innovation vector covariance matrix at time epoch i and expressed using (8) and (14) as

$$\boldsymbol{S}_i = \boldsymbol{H}_i\, \overline{\boldsymbol{P}}_i\, \boldsymbol{H}_i^T + \boldsymbol{V}_i. \tag{16}$$

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

$$q_k \gtrless T_k^2. \tag{17}$$

Let n be the number of measurements for each GNSS measurement update; under fault free conditions, the test statistic q_k at the k^{th} GNSS measurement update is chi-square distributed with kn degrees of freedom. For a given false alarm requirement, the threshold T_k^2 is determined from the inverse chi-square cumulative distribution function. The INS monitor alarms for a fault if $q_k > T_k^2$. Under faulted conditions, q_k is noncentrally chi-square distributed with a noncentrality parameter λ_k^2

$$\lambda_k^2 = \sum_{i=1}^{k} \mathbb{E}[\boldsymbol{\gamma}_i]^T\, \boldsymbol{S}_i^{-1}\, \mathbb{E}[\boldsymbol{\gamma}_i] \tag{18}$$

which is used to evaluate the probability of missed detection. Note that due to cumulative nature of the test statistic, q_i per each test ($0 \le i \le k$) will be time correlated. Capturing this correlation in computing the threshold T_k in a repeated test scenario is difficult and being investigated in the literature. One of the recent studies [31] discusses the influence of the autocorrelations of monitor test statistics over time and their cross correlations across monitors on false alert and missed detection probabilities. For simplicity, this paper assumes a stationary process over the time interval of interest; the implications of the time correlation will be further investigated in the future work.

III. MONITOR PERFORMANCE EVALUATION

In this section, we derive an evaluation model for the performance of the proposed monitor by inputting the spoofed measurements into the estimator and detector. We then 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. We also introduce an analytical derivation for a Kalman-filter-based worst case fault that maximizes the integrity risk. The impact of the real-time position tracking and spoofing on the aircraft's compensation system and motion is described in the closed-loop block diagram in Fig. 1.

A. Evaluation Model for Spoofing Monitor Performance

The first part of this section constructs an analytical expression of spoofed measurements as a function of authentic signal, deliberate fault, and tracking noise. To quantify the impact of the spoofed measurements on aircraft response, the second part builds a Kalman-filter-based compensator, which is to be used to evaluate the monitor performance and derive the worst case fault sequence in the subsequent sections.

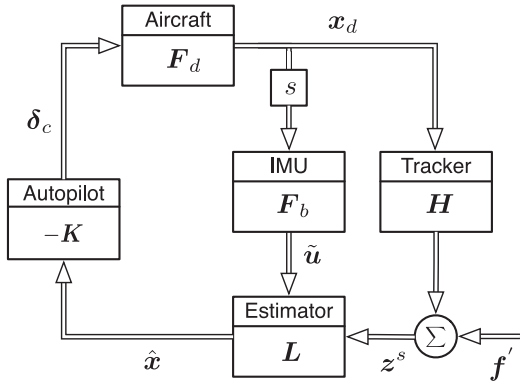

Fig. 1. INS monitor performance evaluation model capturing the closed-loop relation between the INS estimator (observer) and the altitude hold autopilot (controller) in presence of a GNSS spoofing attack with aircraft position tracking. The spoofer's deliberate resultant fault $\boldsymbol{f}'$ is the input of the model, which impacts the output of the Kalman estimator.

1) *Spoofed Measurements:* In a spoofing attack, the GNSS measurement that the aircraft receives will be the spoofer's broadcast $\boldsymbol{z}_k^s$, which is expressed as

$$\boldsymbol{z}_k^s = \boldsymbol{H}_k\, \hat{\boldsymbol{x}}_k^s + \boldsymbol{v}_{\rho\phi_k} + \boldsymbol{f}_k \tag{19}$$

where $\hat{\boldsymbol{x}}_k^s$ is the spoofer's estimate for the actual aircraft state $\boldsymbol{x}_k$ and $\boldsymbol{f}_k$ is a fault vector added by the spoofer.

The spoofer's estimate of the aircraft state vector $\hat{\boldsymbol{x}}_k^s$ can be expressed in terms of the actual state $\boldsymbol{x}_k$ as

$$\hat{\boldsymbol{x}}_k^s = \boldsymbol{x}_k + \tilde{\boldsymbol{x}}_k^s \tag{20}$$

where $\tilde{\boldsymbol{x}}_k^s$ is the estimate error influenced by the tracking sensor noise.

Substituting (20) into (19), the spoofed measurement becomes

$$\boldsymbol{z}_k^s = \boldsymbol{H}_k\, \boldsymbol{x}_k + \boldsymbol{v}_{\rho\phi_k} + \underbrace{\boldsymbol{H}_k\, \tilde{\boldsymbol{x}}_k^s + \boldsymbol{f}_k}_{\boldsymbol{f}_k'} \tag{21}$$

where $\boldsymbol{f}_k'$ is the resultant fault vector containing the position-tracking error.

It is assumed that the spoofer is capable of measuring aircraft position using an optical sensor, for example a laser ranging system. In this problem, the resulting estimation error $\tilde{\boldsymbol{x}}^s$ in (21) is modeled as white Gaussian noise. Filtering or smoothing the tracking noise will cause a phase shift between the spoofer's position estimate and the aircraft's actual dynamic response to the spoofing attack (actuated by autopilot), which will be reflected as an inconsistency between INS and GNSS measurements and may improve the detection capability of the monitor [23]. However, this phase shift will be low over the low frequencies at which large aircrafts fuselage vibrates. The phase shift becomes more significant at high frequencies.

Under a spoofing attack, the actual measurement $\boldsymbol{z}_k$ in the estimator's measurement update equation (10) is replaced with the spoofed measurement $\boldsymbol{z}_k^s$ in (21), that is

$$\hat{\boldsymbol{x}}_k = \overline{\boldsymbol{x}}_k + \boldsymbol{L}_k\big(\boldsymbol{z}_k^s - \boldsymbol{H}_k\, \overline{\boldsymbol{x}}_k\big). \tag{22}$$

Substituting (21) into (22) gives

$$\hat{\boldsymbol{x}}_k = \underbrace{\left(\boldsymbol{I} - \boldsymbol{L}_k \boldsymbol{H}_k\right)}_{\boldsymbol{L}_k'} \overline{\boldsymbol{x}}_k + \boldsymbol{L}_k \boldsymbol{H}_k \, \boldsymbol{x}_k + \boldsymbol{L}_k \left(\boldsymbol{v}_{\rho\phi_k} + \boldsymbol{f}_k' \right). \tag{23}$$

Substituting the time update equation (9) into (23) gives

$$\hat{\boldsymbol{x}}_k = \boldsymbol{L}_k' \boldsymbol{\Phi} \, \hat{\boldsymbol{x}}_{k-1} + \boldsymbol{L}_k \boldsymbol{H}_k \, \boldsymbol{x}_k + \boldsymbol{L}_k' \boldsymbol{\Gamma} \, \tilde{\boldsymbol{u}}_{k-1} + \boldsymbol{L}_k \left(\boldsymbol{v}_{\rho\phi_k} + \boldsymbol{f}_k' \right). \tag{24}$$

Let us define the state estimate error as $\tilde{\boldsymbol{x}}_k = \hat{\boldsymbol{x}}_k - \boldsymbol{x}_k$. Subtracting (5) from (24) gives the state estimate error dynamics as

$$\tilde{\boldsymbol{x}}_k = \boldsymbol{L}_k' \boldsymbol{\Phi} \, \tilde{\boldsymbol{x}}_{k-1} - \boldsymbol{L}_k' \overline{\boldsymbol{w}}_{k-1} + \boldsymbol{L}_k \left(\boldsymbol{v}_{\rho\phi_k} + \boldsymbol{f}_k' \right). \tag{25}$$

Similarly, the innovation vector under a spoofing attack is obtained by replacing the actual measurement $\boldsymbol{z}_k$ in (14) with the spoofed measurement $\boldsymbol{z}_k^s$ in (21) as

$$\boldsymbol{\gamma}_k = \boldsymbol{z}_k^s - \boldsymbol{H}_k \, \overline{\boldsymbol{x}}_k. \tag{26}$$

Using (5) and (9), the current innovation vector $\boldsymbol{\gamma}_k$ in (26) can be expressed in terms of the previous state estimate error $\tilde{\boldsymbol{x}}_{k-1}$ as

$$\boldsymbol{\gamma}_k = \boldsymbol{f}_k' + \boldsymbol{v}_{\rho\phi_k} - \boldsymbol{H}_k \left(\boldsymbol{\Phi} \, \tilde{\boldsymbol{x}}_{k-1} - \overline{\boldsymbol{w}}_{k-1} \right). \tag{27}$$

Augmenting the process model in (5) with the state estimate error model in (25) and the innovation model in (27) results in a performance evaluation model capturing the impact of the error in spoofer's tracking sensors and the fault on the actual state, the state estimate error, and the innovation

$$\begin{bmatrix} \boldsymbol{x}_k \\ \tilde{\boldsymbol{x}}_k \\ \boldsymbol{\gamma}_k \end{bmatrix} = \begin{bmatrix} \boldsymbol{\Phi} & 0 & 0 \\ 0 & \boldsymbol{L}_k' \boldsymbol{\Phi} & 0 \\ 0 & -\boldsymbol{H}_k \boldsymbol{\Phi} & 0 \end{bmatrix} \begin{bmatrix} \boldsymbol{x}_{k-1} \\ \tilde{\boldsymbol{x}}_{k-1} \\ \boldsymbol{\gamma}_{k-1} \end{bmatrix} + \begin{bmatrix} \boldsymbol{\Gamma} \\ 0 \\ 0 \end{bmatrix} \tilde{\boldsymbol{u}}_{k-1} + \begin{bmatrix} \boldsymbol{I} & 0 \\ -\boldsymbol{L}_k{}' & \boldsymbol{L}_k \\ \boldsymbol{H}_k & \boldsymbol{I} \end{bmatrix} \begin{bmatrix} \overline{\boldsymbol{w}}_{k-1} \\ \boldsymbol{v}_{\rho\phi_k} \end{bmatrix} + \begin{bmatrix} 0 \\ \boldsymbol{L}_k \\ \boldsymbol{I} \end{bmatrix} \boldsymbol{f}_k'. \tag{28}$$

In (28), the innovation $\boldsymbol{\gamma}_k$ is augmented into the states to simplify integrity risk evaluation, which will be explained in the following sections.

2) *Augmented Observer and Controller:* To include pilot/autopilot action, whose goal is to follow the prescribed final approach glidepath, we incorporate an altitude autopilot into the aircraft compensator model. Assuming that there is a spoofing attack during the landing approach, this altitude controller will respond to the spoofing attack by inducing control actions; the aircraft's response will be measured by the IMU. To quantify the impact of the motion induced by these control actions on the IMU measurements $\tilde{\boldsymbol{u}}$ in (28), we utilize a closed-loop compensation model (see Fig. 1) including an observer feedback based on the output of the Kalman filter estimator. Due to the presence of the spoofing fault in the estimator's output $\hat{\boldsymbol{x}}$, the altitude-hold autopilot generates a control input $\boldsymbol{\delta}_c$ (elevator and thrust) resulting in a correction maneuver (the black curve in Fig. 2).

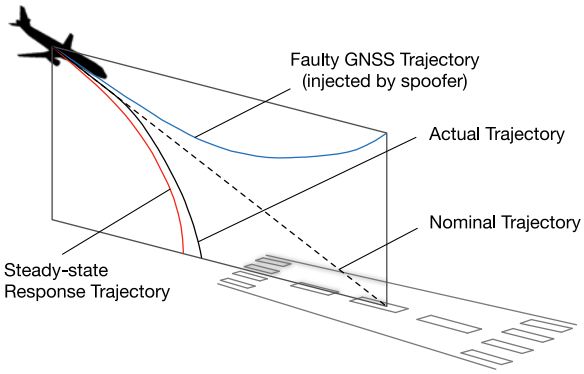

Fig. 2. Impact of the position fault and the consequent autopilot response to the spoofing attack on aircraft trajectory. The dotted line is the nominal or planned approach trajectory, the blue line represents the faulty positions injected by the spoofer, the red line is the steady-state trajectory that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

To capture the aircraft's response in this closed-loop system, we use an aircraft dynamic model as [32]

$$\dot{\boldsymbol{x}}_d = \boldsymbol{F}_d \, \boldsymbol{x}_d + \boldsymbol{G}_\delta \, \boldsymbol{\delta}_c \tag{29}$$

where $\boldsymbol{x}_d = [\delta u, \delta w, \delta q, \delta\theta, \delta h]^T$ is the aircraft longitudinal state vector containing deviation in forward speed u, down speed w, pitch rate q, pitch angle θ, and altitude h. $\boldsymbol{F}_d$ is the plant matrix, $\boldsymbol{G}_\delta$ is the input coefficient matrix, and $\boldsymbol{\delta}_c$ is the control input containing elevator deflection and thrust change.

The discrete form of (29) is

$$\boldsymbol{x}_{d_k} = \boldsymbol{\Phi}_d \, \boldsymbol{x}_{d_{k-1}} + \boldsymbol{\Gamma}_\delta \, \boldsymbol{\delta}_{c_{k-1}} \tag{30}$$

where $\boldsymbol{\Phi}_d$ and $\boldsymbol{\Gamma}_\delta$ are discrete forms of $\boldsymbol{F}_d$ and $\boldsymbol{G}_\delta$, respectively.

The control input $\boldsymbol{\delta}_{c_k}$ is generated based on the state estimate feedback as

$$\boldsymbol{\delta}_{c_k} = -\boldsymbol{K}_x \, \hat{\boldsymbol{x}}_k - \boldsymbol{K}_q \, \delta\hat{q}_k \tag{31}$$

where the first term represents state feedback of position, velocity and attitude, the second term adds pitch rate feedback, and $\boldsymbol{K}_x$ and $\boldsymbol{K}_q$ are controller gain matrices.

Since the conventional INS state vector $\boldsymbol{x}_k$ does not contain the pitch rate δq_k that is required for the controller, the control law in (31) is separated into two terms. Remember $\boldsymbol{u}_k = [\ldots, \delta q_k, \ldots]^T$ is the vector containing specific force and angular velocity, therefore the pitch rate estimate $\delta\hat{q}_k$ in (31) can be extracted as $\delta\hat{q}_k = \boldsymbol{T}_q \, \hat{\boldsymbol{u}}_k$. Using (2), $\hat{\boldsymbol{u}}_k$ is obtained in terms of the IMU measurement vector $\tilde{\boldsymbol{u}}_k$ as $\hat{\boldsymbol{u}}_k = \tilde{\boldsymbol{u}}_k - \hat{\boldsymbol{b}}_k$. Recall $\boldsymbol{x}_k = [\ldots, \boldsymbol{b}_k]^T$, therefore the bias estimate $\hat{\boldsymbol{b}}_k$ is extracted as $\hat{\boldsymbol{b}}_k = \boldsymbol{T}_b \, \hat{\boldsymbol{x}}_k$. Substituting these transformations into (31), the control input is rewritten as

$$\boldsymbol{\delta}_{c_k} = -\left(\boldsymbol{K}_x - \boldsymbol{K}_q \, \boldsymbol{T}_q \, \boldsymbol{T}_b\right)\hat{\boldsymbol{x}}_k - \boldsymbol{K}_q \, \boldsymbol{T}_q \tilde{\boldsymbol{u}}_k. \tag{32}$$

The main aim of introducing the aircraft dynamic model in (29) is to augment the controller and observer by coupling between the controller and observer. This coupling is

realized through the specific force and angular velocity $\boldsymbol{u}$ measured by IMU. $\boldsymbol{u}$ can be extracted from aircraft state derivative $\dot{\boldsymbol{x}}_d$ as $\boldsymbol{u} = \boldsymbol{T}_u\ \dot{\boldsymbol{x}}_d$. This can be reexpressed in discrete form by utilizing (29) as

$$\boldsymbol{u}_k = \boldsymbol{T}_u\big(\boldsymbol{F}_d\ \boldsymbol{x}_{d_k} + \boldsymbol{G}_\delta\ \boldsymbol{\delta}_{c_k}\big). \tag{33}$$

Substituting (33) with the transformations $\boldsymbol{b}_k = \boldsymbol{T}_b\ \boldsymbol{x}_k$ and $\boldsymbol{v}_{n_k} = \boldsymbol{T}_v\ \boldsymbol{w}_k$ into (2), we obtain the IMU measurement $\tilde{\boldsymbol{u}}_k$ as

$$\tilde{\boldsymbol{u}}_k = \boldsymbol{T}_u\big(\boldsymbol{F}_d\ \boldsymbol{x}_{d_k} + \boldsymbol{G}_\delta\ \boldsymbol{\delta}_{c_k}\big) + \boldsymbol{T}_b\ \boldsymbol{x} + \boldsymbol{T}_v\ \boldsymbol{w}_k \tag{34}$$

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

Using $\hat{\boldsymbol{x}}_k = \boldsymbol{x}_k + \tilde{\boldsymbol{x}}_k$, one can solve for $\tilde{\boldsymbol{u}}_k$ and $\boldsymbol{\delta}_{c_k}$ in (32) and (34) in terms of the actual INS state $\boldsymbol{x}_k$ and its estimate error $\tilde{\boldsymbol{x}}_k$, the aircraft state $\boldsymbol{x}_{d_k}$, and the process noise $\boldsymbol{w}_k$ as

$$\tilde{\boldsymbol{u}}_k = \boldsymbol{U}_x\ \boldsymbol{x}_k + \boldsymbol{U}_{\tilde{x}}\ \tilde{\boldsymbol{x}}_k + \boldsymbol{U}_d\ \boldsymbol{x}_{d_k} + \boldsymbol{U}_w\ \boldsymbol{w}_k \tag{35}$$

$$\boldsymbol{\delta}_{c_k} = \boldsymbol{\Delta}_x\ \boldsymbol{x}_k + \boldsymbol{\Delta}_{\tilde{x}}\ \tilde{\boldsymbol{x}}_k + \boldsymbol{\Delta}_d\ \boldsymbol{x}_{d_k} + \boldsymbol{\Delta}_w\ \boldsymbol{w}_k \tag{36}$$

where the coefficient matrices in (35) and (36) are derived in Appendix B.

Augmenting the aircraft model in (30) and the Kalman model in (28) with the substitutions in (35) and (36) yields a closed-loop evaluation model as

$$\begin{bmatrix} \boldsymbol{x}_k \\ \tilde{\boldsymbol{x}}_k \\ \boldsymbol{\gamma}_k \\ \boldsymbol{x}_{d_k} \end{bmatrix} = \overbrace{\begin{bmatrix} \boldsymbol{\Phi} + \boldsymbol{\Gamma}\ \boldsymbol{U}_x & \boldsymbol{\Gamma}\ \boldsymbol{U}_{\tilde{x}} & 0 & \boldsymbol{\Gamma}\ \boldsymbol{U}_d \\ 0 & \boldsymbol{L}_k^{'}\boldsymbol{\Phi} & 0 & 0 \\ 0 & -\boldsymbol{H}_k\boldsymbol{\Phi} & 0 & 0 \\ \boldsymbol{\Gamma}_\delta\ \boldsymbol{\Delta}_x & \boldsymbol{\Gamma}_\delta\ \boldsymbol{\Delta}_{\tilde{x}} & 0 & \boldsymbol{\Phi}_d + \boldsymbol{\Gamma}_\delta\ \boldsymbol{\Delta}_d \end{bmatrix}}^{\boldsymbol{\Phi}_{y_k}} \times \overbrace{\begin{bmatrix} \boldsymbol{x}_{k-1} \\ \tilde{\boldsymbol{x}}_{k-1} \\ \boldsymbol{\gamma}_{k-1} \\ \boldsymbol{x}_{d_{k-1}} \end{bmatrix}}^{\boldsymbol{y}_{k-1}} + \underbrace{\begin{bmatrix} \boldsymbol{I} & 0 & \boldsymbol{\Gamma}\ \boldsymbol{U}_w \\ -\boldsymbol{L}_k^{'} & \boldsymbol{L}_k & 0 \\ \boldsymbol{H}_k & \boldsymbol{I} & 0 \\ 0 & 0 & \boldsymbol{\Gamma}_\delta\ \boldsymbol{\Delta}_w \end{bmatrix}}_{\boldsymbol{\Upsilon}_{y_k}} \underbrace{\begin{bmatrix} \overline{\boldsymbol{w}}_{k-1} \\ \boldsymbol{v}_{\rho\phi_k} \\ \boldsymbol{w}_{k-1} \end{bmatrix}}_{\boldsymbol{w}_{y_k}} + \underbrace{\begin{bmatrix} 0 \\ \boldsymbol{L}_k \\ \boldsymbol{I} \\ 0 \end{bmatrix}}_{\boldsymbol{\Psi}_{y_k}} \boldsymbol{f}_k' \tag{37}$$

where $\boldsymbol{y}$ is defined as the augmented state vector of the closed-loop evaluation model. $\boldsymbol{\Phi}_y$, $\boldsymbol{\Upsilon}_y$, and $\boldsymbol{\Psi}_y$ are the augmented state transition, noise coefficient, and fault input coefficient matrices, respectively. Note that the first three rows of (37) represent the real-time airborne estimator and detector equations whereas the last row corresponds to the aircraft dynamic response to the fault and is augmented for the purpose of monitor performance evaluation. Note also that some elements of $\boldsymbol{x}_{d_k}$ and $\boldsymbol{x}_k$ are dependent and can be merged. However, to distinguish the airborne implementation from the performance evaluation (37) is deliberately written in nonminimal state form.

Using (37), the mean $\mathbb{E}[\boldsymbol{y}_k]$ and covariance $\boldsymbol{Y}_k$ of the closed-loop evaluation model state vector $\boldsymbol{y}$ can be propagated as

$$\mathbb{E}[\boldsymbol{y}_k] = \boldsymbol{\Phi}_{y_k}\ \mathbb{E}[\boldsymbol{y}_{k-1}] + \boldsymbol{\Psi}_{y_k}\ \boldsymbol{f}_{w_k}' \tag{38}$$

$$\boldsymbol{Y}_k = \boldsymbol{\Phi}_{y_k}\ \boldsymbol{Y}_{k-1}\ \boldsymbol{\Phi}_{y_k}^T + \boldsymbol{\Upsilon}_{y_k}\boldsymbol{W}_{y_k}\boldsymbol{\Upsilon}_{y_k}^T \tag{39}$$

where $\boldsymbol{W}_{y_k}$ is the covariance matrix of $\boldsymbol{w}_{y_k}$. Note that $\mathbb{E}[\boldsymbol{w}_{k-1}\ \overline{\boldsymbol{w}}_{k-1}^T] = \mathbb{E}[\boldsymbol{w}_{k-1}\ \boldsymbol{v}_{\rho\phi_k}^T] = 0$.

B. Spoofing Integrity Risk

In this paper, integrity risk is used as a metric to quantify the performance of the spoofing monitor. Integrity risk is defined as the probability that the state estimate error (e.g., altitude error) exceeds an alert limit without being detected (i.e., $q < T^2$). Given spoofing fault vector $\boldsymbol{f}_k'$, the integrity risk at time epoch k is expressed in terms of a cumulative test statistic q_k and the current altitude estimate error ε_k as

$$I_{r_k} = \Pr\big(\ |\varepsilon_k| > l\ ,\ q_k < T_k^2\big) \tag{40}$$

where l is the vertical alert limit, and T_k^2 is the predefined threshold for detection, which is the same as that in (17).

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

$$\varepsilon_k = \boldsymbol{T}_\varepsilon\ \tilde{\boldsymbol{x}}_k \tag{41}$$

where ε_k is normally distributed.

The cumulative test statistic q_k in (15) may be expressed in vector form as

$$q_k = \begin{bmatrix} \boldsymbol{\gamma}_1^T & \cdots & \boldsymbol{\gamma}_k^T \end{bmatrix} \underbrace{\begin{bmatrix} \boldsymbol{S}_1^{-1} & & \\ & \ddots & \\ & & \boldsymbol{S}_k^{-1} \end{bmatrix}}_{\boldsymbol{S}_{1:k}^{-1}} \underbrace{\begin{bmatrix} \boldsymbol{\gamma}_1 \\ \vdots \\ \boldsymbol{\gamma}_k \end{bmatrix}}_{\boldsymbol{\gamma}_{1:k}} \tag{42}$$

where $\boldsymbol{S}_k$ is the innovation covariance obtained from $\boldsymbol{Y}_k$ in (39) as

$$\boldsymbol{S}_k = \boldsymbol{T}_\gamma \boldsymbol{Y}_k \boldsymbol{T}_\gamma^T \tag{43}$$

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

Similarly, the noncentrality parameter λ^2 of the cumulative test statistic in (18) is

$$\lambda_k^2 = \mathbb{E}\big[\boldsymbol{\gamma}_{1:k}^T\big]\ \boldsymbol{S}_{1:k}^{-1}\ \mathbb{E}[\boldsymbol{\gamma}_{1:k}]. \tag{44}$$

Using the evaluation model (28), it is proved in Appendix A that $\mathbb{E}[\tilde{\boldsymbol{x}}_i\boldsymbol{\gamma}_j^T] = 0$ for all $i \geq j$. Therefore, the cumulative test statistic q_k obtained from the current and past innovations and the altitude error ε_k obtained from the current state estimate error will be statistically independent. As a result, integrity risk I_{r_k} can be written as a product of two probabilities

$$I_{r_k} = \Pr(\ |\varepsilon_k| > l\ )\ \Pr\big(\ q_k < T_k^2\ \big). \tag{45}$$

C. Kalman-Filter-Based Worst Case Fault Derivation

Because all GNSS measurements may be impacted by the spoofing attack, it is assumed that all GNSS measurements are faulty during the attack period and that the IMU

measurements are the fault-free sources of redundancy in the monitor. If a spoofing attack is not detected instantaneously, it may impact the INS error state estimates through the tightly coupled mechanism, which can degrade subsequent detection ability. Therefore, a smart spoofer may select a fault profile $\boldsymbol{f}_{1:k}$ with smaller faults at the beginning and gradually increasing over time, thereby corrupting INS calibration, leading to a lower probability of detection.

A worst case fault derivation based on a batch estimator was previously introduced in [25]. Here, we extend the theory to derive 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. To obtain the optimal direction and magnitude of the worst case fault history vector $\boldsymbol{f}_{1:k}$, we use the evaluation model in (37) and conservatively assume that the spoofer has knowledge of the exact error models for the aircraft's INS/GNSS system and his/her own position-tracking sensor.

Equations (38) and (44) indicate that the fault history vector $\boldsymbol{f}_{1:k}$ affects the mean of $\tilde{\boldsymbol{x}}_k$ and the noncentrality parameter λ_k^2 of the cumulative test statistic q_k. The ratio $\mathbb{E}[\varepsilon_k]^2/\lambda_k^2$ is called the failure mode slope ρ_k^2 , which maximizes the integrity risk [25]. The optimization problem for obtaining the worst case fault can be formulated as

$$\arg\max_{\boldsymbol{f}_{1:k}} \rho_k^2. \tag{46}$$

Recall that ε_k and λ_k^2 are functions of the state estimate error $\tilde{\boldsymbol{x}}_k$ and the innovation history vector $\boldsymbol{\gamma}_{1:k}$, respectively. Also, $\tilde{\boldsymbol{x}}_k$ and $\boldsymbol{\gamma}_k$ are both linear functions of $\boldsymbol{f}_{1:k}$. Using (38) and (37), the means of $\tilde{\boldsymbol{x}}_k$ and $\boldsymbol{\gamma}_k$ can be extracted as

$$\mathbb{E}[\tilde{\boldsymbol{x}}_k] = \underbrace{\boldsymbol{L}_k^{'}\,\boldsymbol{\Phi}}_{\boldsymbol{L}_k^{''}}\,\mathbb{E}[\tilde{\boldsymbol{x}}_{k-1}] + \boldsymbol{L}_k\,\boldsymbol{f}_k \tag{47}$$

$$\mathbb{E}[\boldsymbol{\gamma}_k] = -\boldsymbol{H}_k\,\boldsymbol{\Phi}\,\mathbb{E}[\tilde{\boldsymbol{x}}_{k-1}] + \boldsymbol{f}_k \tag{48}$$

since $\mathbb{E}[\boldsymbol{f}_k'] = \boldsymbol{f}_k$ with the assumption of $\tilde{\boldsymbol{x}}^s \sim \mathcal{N}(0, \boldsymbol{P}^s)$.

Given a fault-free initial condition as $\mathbb{E}[\tilde{\boldsymbol{x}}_0] = \mathbb{E}[\boldsymbol{\gamma}_0] = 0$, the particular solution to the difference equation (47) is obtained as a function of $\boldsymbol{f}_{1:k}$ as

$$\mathbb{E}[\tilde{\boldsymbol{x}}_k] = \underbrace{\begin{bmatrix}\boldsymbol{A}_{1k} & \dots & \boldsymbol{A}_{kk}\end{bmatrix}}_{\boldsymbol{A}_{1:k}} \underbrace{\begin{bmatrix}\boldsymbol{f}_1\\ \vdots\\ \boldsymbol{f}_k\end{bmatrix}}_{\boldsymbol{f}_{1:k}} \tag{49}$$

where

$$\boldsymbol{A}_{ik} = \begin{cases}\boldsymbol{L}_k^{''}\,\boldsymbol{L}_{k-1}^{''}\,\dots\boldsymbol{L}_{1+i}^{''}\,\boldsymbol{L}_i & \text{if } i < k\\ \boldsymbol{L}_i & \text{if } i = k.\end{cases} \tag{50}$$

Substituting (49) into (48) gives the mean of innovation as a function of $\boldsymbol{f}_{1:k}$ as

$$\mathbb{E}[\boldsymbol{\gamma}_k] = \underbrace{\begin{bmatrix}-\boldsymbol{H}_k\,\boldsymbol{\Phi}\,\boldsymbol{A}_{1:k-1} & \boldsymbol{I}\end{bmatrix}}_{\boldsymbol{B}_k} \underbrace{\begin{bmatrix}\boldsymbol{f}_{1:k-1}\\ [2pt]\boldsymbol{f}_k\end{bmatrix}}_{\boldsymbol{f}_{1:k}}. \tag{51}$$

Substituting (51) into (18) gives the noncentrality parameter of the cumulative test statistic as

$$\lambda_k^2 = \sum_{i=1}^{k} \boldsymbol{f}_{1:i}^T\,\boldsymbol{B}_i^T\,\boldsymbol{S}_i^{-1}\boldsymbol{B}_i\,\boldsymbol{f}_{1:i}. \tag{52}$$

Let $\overline{\boldsymbol{B}}_i = \begin{bmatrix}\boldsymbol{B}_i & \boldsymbol{0}_{n\times n(k-i)}\end{bmatrix}$ where n is the number of measurements at each time epoch and $0 < i < k$. Then, (52) is equivalently expressed in block matrix form as

$$\lambda_k^2 = \boldsymbol{f}_{1:k}^T \begin{bmatrix}\overline{\boldsymbol{B}}_1^T & \dots & \overline{\boldsymbol{B}}_k^T\end{bmatrix} \underbrace{\begin{bmatrix}\boldsymbol{S}_1^{-1} & & \\ & \ddots & \\ & & \boldsymbol{S}_k^{-1}\end{bmatrix}}_{\boldsymbol{S}_{1:k}^{-1}} \underbrace{\begin{bmatrix}\overline{\boldsymbol{B}}_1\\ \vdots\\ \overline{\boldsymbol{B}}_k\end{bmatrix}}_{\overline{\boldsymbol{B}}_{1:k}} \boldsymbol{f}_{1:k} \tag{53}$$

where $\overline{\boldsymbol{B}}_{1:k}$ is a lower block triangular matrix.

Substituting (41), (49), and (53) into (46) gives the failure mode slope ρ_k as a function of the fault history vector $\boldsymbol{f}_{1:k}$ as

$$\rho_k^2 = \frac{\boldsymbol{f}_{1:k}^T\,\boldsymbol{A}_{1:k}^T\,\boldsymbol{T}_\varepsilon^T\,\boldsymbol{T}_\varepsilon\,\boldsymbol{A}_{1:k}\,\boldsymbol{f}_{1:k}}{\boldsymbol{f}_{1:k}^T\,\overline{\boldsymbol{B}}_{1:k}^T\,\boldsymbol{S}_{1:k}^{-1}\,\overline{\boldsymbol{B}}_{1:k}\,\boldsymbol{f}_{1:k}}. \tag{54}$$

To determine the direction of vector $\boldsymbol{f}_{1:k}$ that maximizes ρ_k, a change of variable is performed by defining $\breve{\boldsymbol{f}}_{1:k}$ as

$$\breve{\boldsymbol{f}}_{1:k} = \left(\boldsymbol{S}_{1:k}^{-1/2}\,\overline{\boldsymbol{B}}_{1:k}\right)\boldsymbol{f}_{1:k}. \tag{55}$$

The failure mode slope in (54) can be rewritten in terms of $\breve{\boldsymbol{f}}_{1:k}$ as

$$\rho_k^2 = \frac{\breve{\boldsymbol{f}}_{1:k}^T\,\boldsymbol{\kappa}_k\,\boldsymbol{\kappa}_k^T\,\breve{\boldsymbol{f}}_{1:k}}{\breve{\boldsymbol{f}}_{1:k}^T\,\breve{\boldsymbol{f}}_{1:k}} \tag{56}$$

where $\boldsymbol{\kappa}_k$ is a column vector defined as

$$\boldsymbol{\kappa}_k = \left(\boldsymbol{S}_{1:k}^{-1/2}\,\overline{\boldsymbol{B}}_{1:k}\right)^{-T}\,\boldsymbol{A}_{1:k}^T\,\boldsymbol{T}_\varepsilon^T. \tag{57}$$

From (56), it can be concluded that $\breve{\boldsymbol{f}}_{1:k}$ that maximizes the fault mode slope ρ_k^2 must be in the direction of the vector $\boldsymbol{\kappa}_k$. Let us denote the worst case fault history vector $\boldsymbol{f}_{w_{1:k}}$ with a magnitude α_w and a direction $\mathbf{f}_{w_{1:k}}$ as

$$\boldsymbol{f}_{w_{1:k}} = \alpha_w\,\mathbf{f}_{w_{1:k}}. \tag{58}$$

Using (55) and (57), the worst case fault direction $\mathbf{f}_{w_{1:k}}$ is obtained as

$$\mathbf{f}_{w_{1:k}} = \overline{\boldsymbol{B}}_{1:k}^{-1}\,\boldsymbol{S}_{1:k}\,\overline{\boldsymbol{B}}_{1:k}^{-T}\,\boldsymbol{A}_{1:k}^T\,\boldsymbol{T}_\varepsilon^T. \tag{59}$$

So far, we analytically obtained the worst case fault vector direction $\mathbf{f}_{w_{1:k}}$ in (59) from a fully deterministic objective function in (46). The worst case fault magnitude α_w in (58) is a scalar that maximizes the integrity risk I_{r_k} in (45) along the worst case fault direction. Unlike the worst case fault direction optimization, the magnitude optimization has a stochastic objective function I_{r_k} in (45), which is influenced by the spoofer's position-tracking sensor noise. In Section III-B, we explained how to compute the joint probability $\Pr\left(|\varepsilon_k| > l, q_k < T_k^2\right)$ for a given vector $\boldsymbol{f}'$, which, as defined in (21), assumes a given deterministic spoofer's

TABLE I
IMU-GNSS Error Parameters [33]

Parameter	Value	Unit
Gyro angle random walk	0.001	$^\circ/\sqrt{\text{h}}$
Gyro bias error	0.01	$^\circ$/h
Gyro time constant	3600	s
Accelerometer velocity random walk	0.0006	$(\text{m/s})/\sqrt{\text{h}}$
Accelerometer bias error	$10^{-5}\,g$	m/s^2
Accelerometer bias time constant	3600	s
Multipath time constant	100	s
SD Carrier phase multipath noise	1	cm
SD Code phase multipath noise	30	cm
SD Carrier phase thermal noise	0.2	cm
SD Code phase thermal noise	50	cm

tracking error $\tilde{\boldsymbol{x}}^s$. To statistically account for variability in $\tilde{\boldsymbol{x}}^s$, we express the integrity risk in terms of probability density function $f(\tilde{\boldsymbol{x}}^s)$ as

$$I_{r_k}(\alpha) = \int_{\tilde{\boldsymbol{x}}^s} \cdots \int \Pr\left(|\varepsilon_k| > l,\ q_k < T^2; \alpha \mid \tilde{\boldsymbol{x}}^s\right) f(\tilde{\boldsymbol{x}}^s)\, \mathrm{d}\tilde{\boldsymbol{x}}^s. \tag{60}$$

To compute the integral in (60) in the simulation, we generate m number of samples $\tilde{\boldsymbol{x}}^s_1, \tilde{\boldsymbol{x}}^s_2, \ldots, \tilde{\boldsymbol{x}}^s_m$ from the normally distributed $\tilde{\boldsymbol{x}}^s \sim \mathcal{N}(0, \boldsymbol{P}^s)$ and compute the integrity risk for different values of the fault magnitude α

$$I_{r_k}(\alpha) = \frac{1}{m}\sum_{i=1}^{m} \Pr\left(|\varepsilon_k| > l,\ q_k < T^2; \alpha \mid \tilde{\boldsymbol{x}}^s_i\right). \tag{61}$$

The worst case value for the fault magnitude α_w is determined through a one-dimensional search to maximize $I_{r_k}(\alpha)$ in (61). Note that when computing integrity risk, it is customary to be interested in one element of the state vector, for which the integrity requirement is the most stringent. Recall that in aircraft approach and landing the vertical component of the relative position vector is the most critical one. The worst case fault vector direction $\mathbf{f}_{w_{1:k}}$ derived in (59) is already generalized to multidimensional hazard states when $\boldsymbol{T}_\varepsilon = \boldsymbol{I}$. The fault magnitude α obtained from 1-D search in (61) can be easily generalized to multidimensional hazard state by computing the joint probability in (61) for multivariate Gaussian distribution $\boldsymbol{x}_k$ instead of univariate Gaussian distribution ε_k with the cost of computational complexity.

IV. PERFORMANCE ANALYSIS RESULTS

To test the performance of the INS spoofing monitor, a covariance analysis with a B747 flight on approach is simulated at the standard trimmed flight conditions at Mach 0.198 [34]. The B747 aircraft dynamics are modeled with a generic altitude hold autopilot utilizing the longitudinal stability derivatives in [34] at standard sea-level conditions. The IMU sensor and GNSS receiver specifications are provided in Table I. Since the spoofer is assumed to have a limited range, the spoofing attack will be of limited duration. Therefore, we assume that the state estimator has been running under fault free conditions and has reached steady state before the spoofing attack starts.

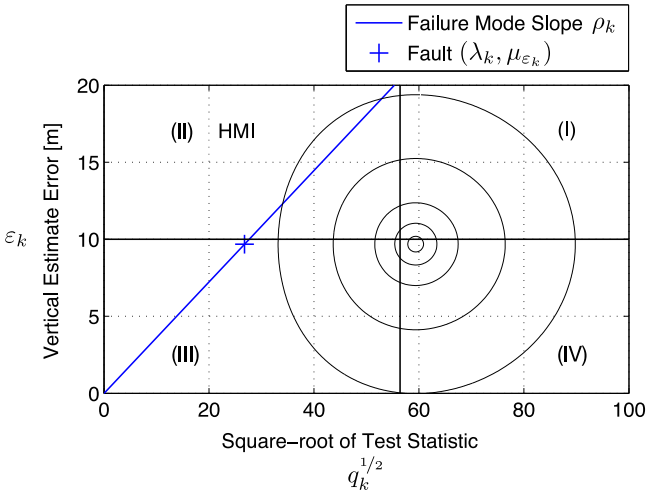

Fig. 3. Worst case fault and failure mode slope for a 140 s approach flight of B747 with a GNSS sampling frequency of 2 Hz. The marker (+) on the failure mode slope corresponds to the deterministic worst-case fault for this scenario, which is described by the noncentrality parameter $\lambda_k = 26.8$ of q_k and mean of vertical estimate error $\mu_{\varepsilon_k} = 9.7$ m. The black curves are lines of constant joint probability density obtained using (45).

To investigate the performance of the INS monitor, we initially assumed a spoofing attack with perfect tracking sensors, capable of tracking the exact aircraft position ($\tilde{\boldsymbol{x}}^s_k = 0$), and computed the worst case fault profile for a given spoofing attack period. An example worst case fault and its failure mode slope for a 140-s B747 approach is illustrated in Fig. 3. The test statistic $q_k^{1/2}$ and vertical position error ε_k are represented on the x-axis and y-axis, respectively. The x–y plane is divided into four quadrants by a vertical alert limit $l = 10$ m and a threshold $T_k = 56.4$, computed from the inverse cumulative chi-square distribution for a false alarm probability of 10^{-6}. The second quadrant refers to the area of hazardous misleading information (HMI), where undetected faults result in unacceptably large estimation errors. The probability of being in the HMI area corresponds to the integrity risk in (45). Each point $(\lambda_k, \mu_{\varepsilon_k})$ at or below failure mode slope line (blue line) on the x–y plane corresponds to a different fault, and for this scenario the worst case fault $\boldsymbol{f}_{w_{1:k}}$ is obtained at the marker ($\lambda_k = 26.8$, μ_{ε_k} =9.7 m) located on the worst case failure mode slope. This worst case fault results in a distribution represented as the oval shape contours of constant joint probability density (black curves). In this example, the integrity risk for the worst case fault is computed as $I_r = 5.9 \times 10^{-6}$.

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 130 to 210 s and computed the corresponding integrity risks. As can be seen in Fig. 4, if the spoofer has perfect position-tracking sensors, increasing the attack period eventually causes high integrity risks. The reason is that increasing the spoofing

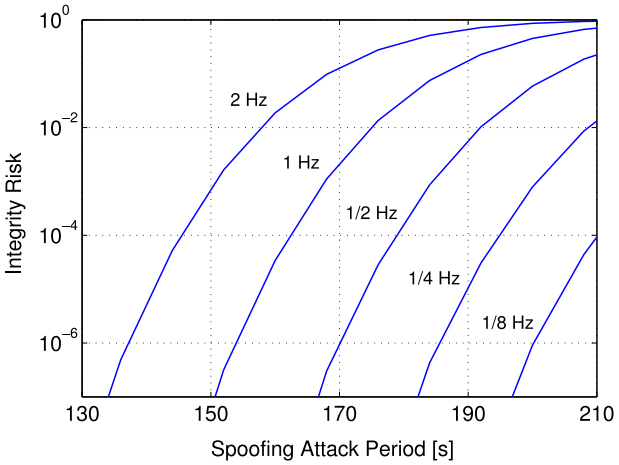

Fig. 4. Impact of spoofing attack period and GNSS sampling frequency on the integrity risk. The results are obtained for a B747 landing approach in the presence of a worst case spoofing attack with a closed-loop position tracking using a sensor having perfect accuracy and no delay.

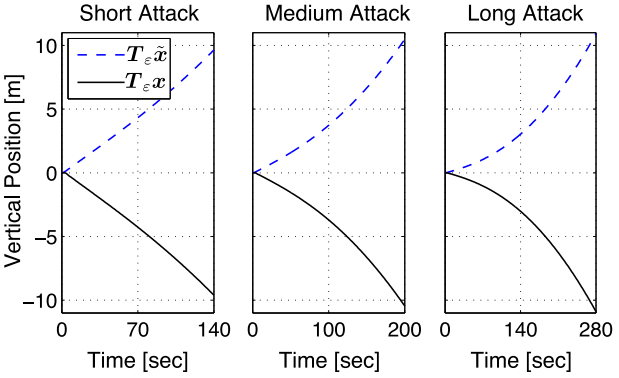

Fig. 5. Impact of the spoofing attack period on the vertical position components of aircraft true state $\boldsymbol{x}$ and its estimate error $\tilde{\boldsymbol{x}}$. In each plot where the worst case attack periods are ranging from 140 s (left), 200 s (middle), and 280 s (right), the consequent estimate error growth and the aircraft's altitude loss from nominal approach (due to the autopilot response to injected fault) are plotted. Note that the true state $\boldsymbol{x}$ and its estimate error $\tilde{\boldsymbol{x}}$ curves are nearly symmetric due to the autopilot's effort to hold the altitude estimate $\hat{\boldsymbol{x}}$ at the nominal during approach (i.e., $\hat{\boldsymbol{x}} = \boldsymbol{x} + \tilde{\boldsymbol{x}} = 0$).

time allows the spoofer to inject faults to the system in a less aggressive way (see Fig. 5), slowly corrupting the estimation of INS states and thereby reducing the monitor's ability to detect the spoofing attack. On the other hand, for limited attack periods, the integrity risk is considerably low. For example, at the GNSS sampling frequency of 2 Hz (see Fig. 4), the worst case attacks having a period shorter than 135 s results in integrity risks of less than 10^{-7} even though the spoofer tracks the aircraft position with zero error. The reason is that at higher GNSS rates the spoofer has more external input to corrupt INS calibration, which leads to a higher integrity risk. On the contrary, slowing the GNSS rate forces the spoofer to inject more aggressive faults in order to lead to the same hazard, which increases the likelihood of detection. It should also be noted that the growth in the integrity risk would plateau and no longer increase with sampling rate. The reason is that INS drifts

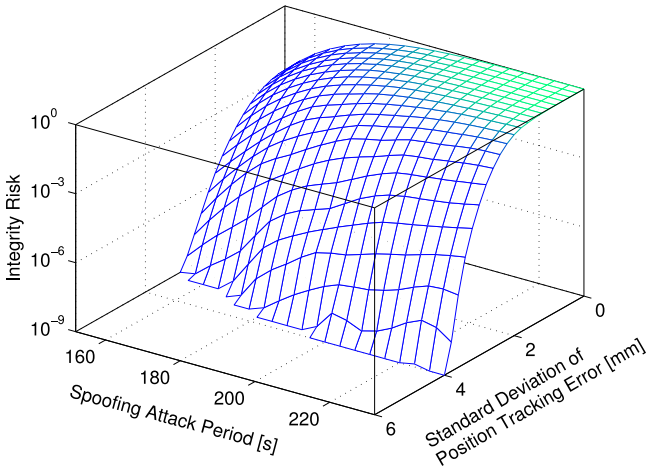

Fig. 6. Impact of altitude tracking error and attack period on the integrity risk in the presence of worst case spoofing attacks with a GNSS sampling frequency of 2 Hz.

less for shorter GNSS sampling intervals, which results in a smaller Kalman gain $\boldsymbol{L}_k$ in (10), thereby deweights GNSS measurements. Fig. 4 does not show the plateau due to unmanageable increase in the computational load in the covariance analysis at faster samples.

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 spoofer's position estimate error is a zero-mean white noise $\tilde{\boldsymbol{x}}_k^s \sim \mathcal{N}(0, \boldsymbol{P}_k^s)$ sequence. White noise is typical for laser tracking errors. Utilizing (61), we illustrate how the INS monitor leverages the spoofer's altitude tracking errors to detect spoofing attacks. Fig. 6 shows that for a position-tracking error of more than 4 mm (1-sigma), the integrity risk always remains below 10^{-9}, which is the most stringent safety requirement in aviation applications [35]. Even though 4 mm instantaneous error is very small in the position domain, the monitor integrates these errors over time. These accumulated errors have a considerable influence on the detection test statistic, which makes the monitor remarkably sensitive to the spoofing attacks. The results are very promising because such tracking accuracy by the spoofer is unrealistically high using any combination of existing high-grade position-tracking systems (e.g., laser, radar, vision).

Note that the simulation results are obtained by assuming that the summation of the test statistic in (15) is coincident with the beginning of the spoofing attack, that is defender's detector and spoofing attack begin simultaneously. If the attack begins at the a^{th} time epoch of the detector, the fault vector will be $\boldsymbol{f}_{1:k} = [\boldsymbol{0}_{1\times(a-1)}\ \boldsymbol{f}_{a:k}^T]^T$, which due to its initial zero elements will be different from the worst case fault $\boldsymbol{f}_{w_{1:k}}$ in (58); therefore resulting in a lower failure mode slope than the maximum slope in Fig. 3. For a perfect tracking scenario, that is $\boldsymbol{x}_i^s = 0$ for $a \le i \le k$ in (60), it is clear that the lower failure mode slope results in a lower integrity risk. However, in the existence of tracking errors $\boldsymbol{x}_i^s \neq 0$, it is hard to analytically prove that the

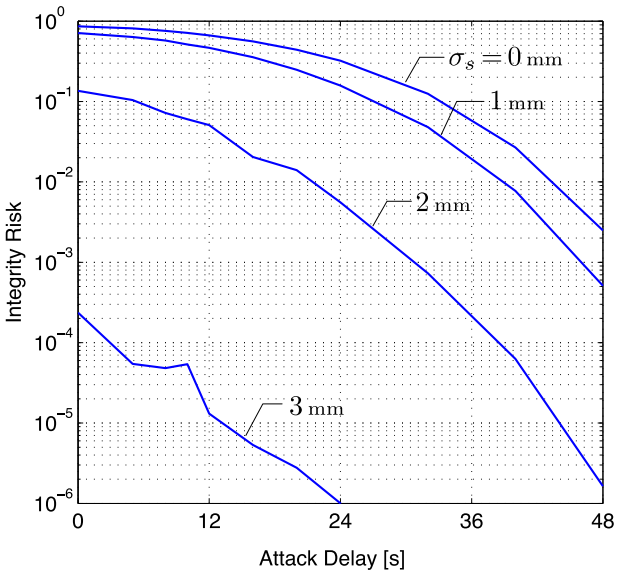

Fig. 7. Impact of attack delay on the integrity risk in the presence of worst case spoofing attacks with a GNSS sampling frequency of 2 Hz. Each curve represents worst case integrity risk using different standard deviations of tracking errors ranging from 0 to 3 mm.

integrity risk due to a worst case coincident attack is an upper bound to that due to a worst case late attack. Instead, the late attack scenarios are simulated using the worst case fault sequence $\boldsymbol{f}_{w_{a:k}}$, which is derived in Appendix C. Assuming that the airborne detector starts monitoring 200 s prior landing, the effect of the attack delay t_a is shown in Fig. 7 for different tracking error levels.

Fig. 7 shows that regardless of the magnitude of the tracking errors, increasing the attack delay results in a decrease in the integrity risk, which supports that the integrity risk surface obtained for worst case coincident attacks in Fig. 6 is an upper bound to a that for late attack scenarios. As can be seen in the figure, the integrity curves get distorted as the 1-sigma tracking errors σ_s increases. The reason is that the number of samples m in (61) to converge a solution increases as the standard deviation $\sigma_s = \mathbb{E}[\tilde{x}_i^s \tilde{x}_i^{s^T}]$ increases, as evident by (61). Due to computational capacity, the number of samples used in the simulations is restricted to 20 regardless of σ_s. Furthermore, if the attack begins prior to detector initialization, which was discussed in [36], the current solution may no longer be conservative, which will be addressed in the future work.

V. CONCLUSION

In this paper, we proposed a simple monitor that utilizes inertial sensors (IMU) to detect GNSS spoofing attacks. The monitor can be implemented into positioning systems using a tightly coupled INS/GNSS integration in a Kalman filter, which is common for precision relative navigation systems such as shipboard landing and autonomous airborne refueling. The performance of the monitor is evaluated in presence of spoofers capable of tracking and estimating aircraft position. A novel closed-form solution to the worst case GNSS fault is introduced. Utilizing this worst case fault in a B747 approach simulation, we showed that the proposed monitor provides an efficient means to detect spoofing attacks unless the spoofer's tracking sensors have unrealistic high accuracy and no delay. The simulation results also showed that the proposed monitor is capable of meeting the most stringent integrity requirements in aviation applications.

APPENDIX

A. STATISTICAL INDEPENDENCE BETWEEN CURRENT-TIME ESTIMATE ERROR AND INNOVATIONS

As discussed in Section III-B, the independence between current state estimate error and innovations in the Kalman-filter-based estimator allows us to formulate the integrity risk as in (45) instead of the more complicated joint probability form in (40). In this section, we prove the statistical independence between the current-time state estimate error $\tilde{\boldsymbol{x}}_k$ and innovation $\boldsymbol{\gamma}_k$.

The current state estimate error $\tilde{\boldsymbol{x}}_k$ and the innovation vector $\boldsymbol{\gamma}_k$ are extracted from the Kalman-filter-based evaluation model in (28) as

$$\tilde{\boldsymbol{x}}_k = \boldsymbol{L}_k^{'}\, \boldsymbol{\Phi}\, \tilde{\boldsymbol{x}}_{k-1} - \boldsymbol{L}_k^{'}\, \overline{\boldsymbol{w}}_{k-1} + \boldsymbol{L}_k\, \boldsymbol{v}_{\rho\phi_k} + \boldsymbol{L}_k\, \boldsymbol{f}_{w_k} \quad (62)$$

$$\boldsymbol{\gamma}_k = -\boldsymbol{H}_k\, \boldsymbol{\Phi}\, \tilde{\boldsymbol{x}}_{k-1} + \boldsymbol{H}_k\, \overline{\boldsymbol{w}}_{k-1} + \boldsymbol{v}_{\rho\phi_k} + \boldsymbol{f}_{w_k}. \quad (63)$$

Using (62) and (63), the covariance between $\tilde{\boldsymbol{x}}_k$ and $\boldsymbol{\gamma}_k$ is obtained as

$$\mathbb{E}\left[\tilde{\boldsymbol{x}}_k \boldsymbol{\gamma}_k^T\right] = -\boldsymbol{L}_k^{'}\left(\boldsymbol{\Phi}\, \hat{\boldsymbol{P}}_{k-1} \boldsymbol{\Phi}^T + \overline{\boldsymbol{W}}_{k-1}\right)\boldsymbol{H}_k^T + \boldsymbol{L}_k \boldsymbol{V}_k. \quad (64)$$

Recalling that $\overline{\boldsymbol{P}}_k = \boldsymbol{\Phi}\, \hat{\boldsymbol{P}}_{k-1} \boldsymbol{\Phi}^T + \overline{\boldsymbol{W}}_{k-1}$ from (13) and $\boldsymbol{L}_k^{'} = \boldsymbol{I} - \boldsymbol{L}_k \boldsymbol{H}_k$ from (23), and substituting them into (64)

$$\mathbb{E}\left[\tilde{\boldsymbol{x}}_k \boldsymbol{\gamma}_k^T\right] = \left(\boldsymbol{L}_k \boldsymbol{H}_k - \boldsymbol{I}\right)\overline{\boldsymbol{P}}_k\, \boldsymbol{H}_k^T + \boldsymbol{L}_k \boldsymbol{V}_k. \quad (65)$$

Substituting $\boldsymbol{L}_k = \hat{\boldsymbol{P}}_k \boldsymbol{H}_k^T \boldsymbol{V}_k^{-1}$ from (11) into (65) gives

$$\mathbb{E}\left[\tilde{\boldsymbol{x}}_k \boldsymbol{\gamma}_k^T\right] = \left(\hat{\boldsymbol{P}}_k \boldsymbol{H}_k^T \boldsymbol{V}_k^{-1} \boldsymbol{H}_k - \boldsymbol{I}\right)\overline{\boldsymbol{P}}_k\, \boldsymbol{H}_k^T + \hat{\boldsymbol{P}}_k \boldsymbol{H}_k^T. \quad (66)$$

Rearranging (12) gives

$$\boldsymbol{H}_k^T \boldsymbol{V}_k^{-1} \boldsymbol{H}_k = \hat{\boldsymbol{P}}_k^{-1} - \overline{\boldsymbol{P}}_k^{-1}. \quad (67)$$

Substituting (67) into (66) gives

$$\begin{aligned}\mathbb{E}\left[\tilde{\boldsymbol{x}}_k \boldsymbol{\gamma}_k^T\right] &= \left[\hat{\boldsymbol{P}}_k\left(\hat{\boldsymbol{P}}_k^{-1} - \overline{\boldsymbol{P}}_k^{-1}\right) - \boldsymbol{I}\right]\overline{\boldsymbol{P}}_k\, \boldsymbol{H}_k^T + \hat{\boldsymbol{P}}_k\, \boldsymbol{H}_k^T \\ &= -\hat{\boldsymbol{P}}_k^{-1}\, \boldsymbol{H}_k^T + \hat{\boldsymbol{P}}_k^{-1}\, \boldsymbol{H}_k^T = 0. \end{aligned} \quad (68)$$

Equation (68) proves that $\tilde{\boldsymbol{x}}_k$ and $\boldsymbol{\gamma}_k$ are statistically independent.

B. CLOSED-LOOP RELATION BETWEEN THE CONTROL INPUT AND IMU MEASUREMENT

This section provides the coefficients in the control input vector $\boldsymbol{\delta}_k$ and the IMU measurement vector $\tilde{\boldsymbol{u}}_k$ expressions in (35) and (36), respectively. These two expressions relate $\boldsymbol{\delta}_k$ and $\tilde{\boldsymbol{u}}_k$ in the closed-loop evaluation model described in Fig. 1.

The control input $\boldsymbol{\delta}_k$ is written in terms of the state estimate $\hat{\boldsymbol{x}}$ and the IMU measurement $\tilde{\boldsymbol{u}}_k$ in (32) as

$$\boldsymbol{\delta}_{c_k} = -\underbrace{\left(\boldsymbol{K}_x - \boldsymbol{K}_q\,\boldsymbol{T}_q\,\boldsymbol{T}_b\right)}_{\boldsymbol{K}'_x}\hat{\boldsymbol{x}}_k - \underbrace{\boldsymbol{K}_q\,\boldsymbol{T}_q}_{\boldsymbol{K}_{\tilde{u}}}\tilde{\boldsymbol{u}}_k \tag{69}$$

and the IMU measurement is written in terms of the true INS state $\boldsymbol{x}$, aircraft dynamic state $\boldsymbol{x}_d$, control input $\boldsymbol{\delta}_{c_k}$, and INS process noise $\boldsymbol{w}_k$ in (34) as

$$\tilde{\boldsymbol{u}}_k = \boldsymbol{T}_u\left(\boldsymbol{F}_d\,\boldsymbol{x}_{d_k} + \boldsymbol{G}_\delta\,\boldsymbol{\delta}_{c_k}\right) + \boldsymbol{T}_b\,\boldsymbol{x} + \boldsymbol{T}_v\,\boldsymbol{w}_k. \tag{70}$$

Solving the coupled equations (69) and (70) for $\boldsymbol{\delta}_k$ and $\tilde{\boldsymbol{u}}_k$ yields

$$\begin{aligned}\tilde{\boldsymbol{u}}_k &= \boldsymbol{U}_x\,\boldsymbol{x}_k + \boldsymbol{U}_{\tilde{x}}\,\tilde{\boldsymbol{x}}_k + \boldsymbol{U}_d\,\boldsymbol{x}_{d_k} + \boldsymbol{U}_w\,\boldsymbol{w}_k\\ \boldsymbol{\delta}_k &= \boldsymbol{\Delta}_x\,\boldsymbol{x}_k + \boldsymbol{\Delta}_{\tilde{x}}\,\tilde{\boldsymbol{x}}_k + \boldsymbol{\Delta}_d\,\boldsymbol{x}_{d_k} + \boldsymbol{\Delta}_w\,\boldsymbol{w}_k\end{aligned} \tag{71}$$

where the coefficients are

$$\begin{aligned}\boldsymbol{U}_x &= \left(\boldsymbol{I} + \boldsymbol{T}_u\boldsymbol{G}_\delta\boldsymbol{K}_{\tilde{u}}\right)^{-1}\left(\boldsymbol{T}_b - \boldsymbol{T}_u\,\boldsymbol{G}_\delta\,\boldsymbol{K}'_x\right)\\ \boldsymbol{U}_{\tilde{x}} &= -\left(\boldsymbol{I} + \boldsymbol{T}_u\boldsymbol{G}_\delta\boldsymbol{K}_{\tilde{u}}\right)^{-1}\boldsymbol{T}_u\,\boldsymbol{G}_\delta\,\boldsymbol{K}'_x\\ \boldsymbol{U}_d &= \left(\boldsymbol{I} + \boldsymbol{T}_u\boldsymbol{G}_\delta\boldsymbol{K}_{\tilde{u}}\right)^{-1}\boldsymbol{T}_u\,\boldsymbol{F}_d\\ \boldsymbol{U}_w &= \left(\boldsymbol{I} + \boldsymbol{T}_u\boldsymbol{G}_\delta\boldsymbol{K}_{\tilde{u}}\right)^{-1}\boldsymbol{T}_v\end{aligned} \tag{72}$$

and

$$\begin{aligned}\boldsymbol{\Delta}_x &= -\left(\boldsymbol{I} + \boldsymbol{K}_{\tilde{u}}\;\boldsymbol{T}_u\,\boldsymbol{G}_\delta\right)^{-1}\left(\boldsymbol{K}'_x + \boldsymbol{K}_{\tilde{u}}\,\boldsymbol{T}_b\right)\\ \boldsymbol{\Delta}_{\tilde{x}} &= -\left(\boldsymbol{I} + \boldsymbol{K}_{\tilde{u}}\;\boldsymbol{T}_u\,\boldsymbol{G}_\delta\right)^{-1}\boldsymbol{K}'_x\\ \boldsymbol{\Delta}_d &= -\left(\boldsymbol{I} + \boldsymbol{K}_{\tilde{u}}\;\boldsymbol{T}_u\,\boldsymbol{G}_\delta\right)^{-1}\boldsymbol{K}_{\tilde{u}}\,\boldsymbol{T}_u\,\boldsymbol{F}_d\\ \boldsymbol{\Delta}_w &= -\left(\boldsymbol{I} + \boldsymbol{K}_{\tilde{u}}\;\boldsymbol{T}_u\,\boldsymbol{G}_\delta\right)^{-1}\boldsymbol{K}_{\tilde{u}}\,\boldsymbol{T}_v.\end{aligned} \tag{73}$$

C. WORST CASE FAULT DERIVATION FOR LATE ATTACK SCENARIOS

This section derives the worst case fault for a spoofing attack that starts later than defender's monitor does. The derivation conservatively assumes that the spoofer has the exact knowledge of when the monitor is initialized. Let a late attack begin at the ath epoch of the monitor, then the fault history vector up to epoch k will be $\boldsymbol{f}_{1:k} = [\boldsymbol{0}_{1\times(a-1)}\;\boldsymbol{f}^T_{a:k}]^T$. Using the null hypothesis up to epoch a, the failure mode slope expression in (54) can be reduced to

$$\rho^2_k = \frac{\boldsymbol{f}^T_{a:k}\,\boldsymbol{A}^T_{a:k}\,\boldsymbol{T}^T_\varepsilon\,\boldsymbol{T}_\varepsilon\,\boldsymbol{A}_{a:k}\,\boldsymbol{f}_{a:k}}{\boldsymbol{f}^T_{a:k}\,\overline{\boldsymbol{B}}^T_{a:k}\,\boldsymbol{S}^{-1}_{1:k}\,\overline{\boldsymbol{B}}_{a:k}\,\boldsymbol{f}_{a:k}.} \tag{74}$$

Following the similar approach introduced from (55) to (61), the worst case fault direction $\mathbf{f}_{w_{a:k}}$ that maximizes the fault mode slope in (74) can be obtained as

$$\mathbf{f}_{w_{a:k}} = \left(\overline{\boldsymbol{B}}_{a:k}\,\boldsymbol{S}^{-1}_{1:k}\,\overline{\boldsymbol{B}}^T_{a:k}\right)^{-1}\boldsymbol{A}^T_{a:k}\,\boldsymbol{T}^T_\varepsilon. \tag{75}$$

Note that the structure of (75) is slightly different from that in (59), because unlike $\overline{\boldsymbol{B}}_{1:k}$ in (54) $\overline{\boldsymbol{B}}_{a:k}$ in (74) is not a square matrix, therefore its inverse is avoided in obtaining (75).

ACKNOWLEDGMENT

The authors would like to thank Dr. T. Humphreys of the University of Texas at Austin for his advice about Appendix A. The opinions expressed in this paper are the authors alone and do not necessarily represent those of any other organization or person.

REFERENCES

[1] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, and B. W. O'Hanlon
Assessing the spoofing threat: Development of a portable GPS civilian spoofer
In *Proc. IEEE/ION Position Location Navig. Symp.*, Savannah, GA, USA, 2008, pp. 2314–2325.

[2] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle
GPS vulnerability to spoofing threats and a review of antispoofing techniques
Int. J. Navig. Obsev., vol. 2012, May 2012, Art. no. 127072.

[3] C. Günther
A survey of spoofing and counter-measures
Int. J. Navig. Observ., vol. 61, no. 3, pp. 159–177, May 2014.

[4] M. L. Psiaki and T. E. Humphreys
GNSS spoofing and detection
Proc. IEEE, vol. 104, no. 6, pp. 1258–1270, Jun. 2016.

[5] A. Jovanovic, C. Botteron, and P. A. Farine
Multi-test detection and protection algorithm against spoofing attacks on GNSS receivers
In *Proc. IEEE/ION Position Location Navig. Symp.*, Nashville, TN, 2014, pp. 1258–1271.

[6] K. D. Wesson, M. P. Rothlisberger, and T. E. Humphreys
Practical cryptographic civil GPS signal authentication
Navig., J. Inst. Navig., vol. 59, no. 3, pp. 177–193, 2016.

[7] B. M. Ledvina, W. J. Bencze, B. Galusha, and I. Miller
An in-line spoofing module for legacy GPS receivers
In *Proc. ION GNSS+*, San Diego, CA, USA, 2010, pp. 698–712.

[8] G. W. Hein, F. Kneissl, J. A. Avila-Rodriguez, and S. Wallner
Authenticating GNSS: Proofs against spoofs part 2
GNSS Mag., vol. 2, no. 6, pp. 58–63, Sep./Oct. 2007.

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

[10] C. E. McDowell
GPS spoofer and repeater mitigation system using digital spatial nulling,"
U.S. Patent 7250903 B1, Jul. 31, 2007 [Online]. Available: http://www.google.com/patents/US7250903

[11] J. Nielsen, A. Broumandan, and G. Lachapelle
Spoofing detection and mitigation with a moving handheld receiver
GPS World, vol. 21, no. 9, pp. 27–33, Sep. 2010.

[12] M. Meurer, A. Konovaltsev, M. Cuntz, and C. Hättich
Robust joint multi-antenna spoofing detection and attitude estimation using direction assisted multiple hypotheses RAIM
In *Proc. ION GNSS+*, Nashville, TN, 2012, pp. 3007–3016.

[13] S. Moshavi
Multi-user detection for DS-CDMA communications
IEEE Commun. Mag., vol. 34, no. 10, pp. 124–135, Oct. 1996.

[14] M. L. Psiaki, S. P. Powell, and B. W. O'Hanlon
GNSS spoofing detection using high-frequency antenna motion and carrier-phase data
In *Proc. ION GNSS+*, Nashville, TN, USA, 2013, pp. 2949–2991.

[15] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle
GPS spoofer countermeasure effectiveness based on signal strength, noise power and C/N0 observables
Int. J. Satell. Commun. Netw., vol. 30, no. 4, pp. 181–191, Jul. 2012.

[16] H. Wen, P. Y. R. Huang, J. Dyer, A. Archinal, and J. Fagan
Countermeasures for GPS signal spoofing
In *Proc. ION GNSS+*, Long Beach, CA, USA, 2005, pp. 1285–1290.

[17] J. S. Warner and R. G. Johnston
GPS spoofing countermeasures
Homeland Secur. J., vol. 25, no. 2, pp. 19–27, Dec. 2003.

[18] P. F. Swaszek, K. C. Seals, S. A. Pratz, B. N. Arocho, and R. J. Hartnett
GNSS spoof detection using shipboard IMU measurements
In *Proc. ION GNSS+*, Tampa, FL, USA, 2014, pp. 745–758.

[19] P. F. Swaszek, R. J. Hartnett, and K. C. Seals
GNSS spoof detection using independent range information
In *Proc. ION Int. Tech. Meet.*, Monterey, CA, USA, 2016, pp. 739–747.

[20] S. Khanafseh, N. Roshan, S. Langel, F-C. Chan, M. Joerger, and B. Pervan
GNSS spoofing detection using RAIM with INS coupling
In *Proc. IEEE/ION Position Location Navig. Symp.*, Monterey, CA, USA, 2014, pp. 1232–1239.

[21] C. Tanil, S. Khanafseh, and B. Pervan
The impact of wind gust on detectability of GPS spoofing attack using RAIM with INS coupling
In *Proc. ION PNT*, Honolulu, HI, USA, 2015, pp. 674–686.

[22] C. Tanil, S. Khanafseh, and B. Pervan
Detecting global navigation satellite system spoofing using inertial sensing of aircraft disturbance
J. Guid., Control, Dyn., vol. 40, no. 8, pp. 2006–2016, 2017.

[23] C. Tanil, S. Khanafseh, and B. Pervan
GNSS spoofing attack detection using aircraft autopilot response to deceptive trajectory
In *Proc. ION GNSS+*, Tampa, FL, USA, 2015, pp. 3345–3357.

[24] B. W. Parkinson and P. Axelrad
Autonomous GNSS integrity monitoring using the pseudorange residual
Navigation, vol. 35, no. 2, pp. 255–274, May 1988.

[25] M. Joerger and B. Pervan
Kalman filter-based integrity monitoring against sensor faults
J. Guid., Control, Dyn., vol. 36, no. 2, pp. 349–361, Feb. 2013.

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

[27] C. Tanil, S. Khanafseh, M. Joerger, and B. Pervan
Kalman filter-based INS monitor to detect GNSS spoofers capable of tracking aircraft position
In *Proc. IEEE/ION Position Location Navig. Symp.*, Savannah, GA, USA, 2016, pp. 1027–1034.

[28] D. H. Titterton and J. L. Weston
Strapdown Inertial Navigation Technology. 3rd ed. Washington, DC, USA: AIAA, 2004.

[29] J. Farrell
Aided Navigation: GNSS With High Rate Sensors. New York, NY, USA: McGraw-Hill, Inc., 2008.

[30] P. Misra and P. Enge
Global Positioning System: Signals, Measurements and Performance, 2nd ed. Lincoln, MA, USA: Ganga–Jamuna Press, 2006.

[31] B. Pervan, S. Khanafseh, and J. Patel
Test statistic auto- and cross-correlation effects on monitor false alert and missed detection probabilities
In *Proc. ION Int. Techn. Meet.*, Monterey, CA, USA, 2017, pp. 562–590.

[32] T. R. Yechout, S. L. Morris, D. E. Bossert, and W. F. Hallgren
Introduction to Aircraft Flight Mechanics (AIAA Education Series). Washington, DC, USA: AIAA, 2003.

[33] R. G. Brown and P. Y. C. Hwang
Introduction to Random Signals and Applied Kalman Filtering, 3rd ed. New York, NY, USA: Wiley, 1997.

[34] R. K. Heffley and W. F. Jewell
Aircraft Handling Qualities Data. Washington, DC, USA: Nat. Aeron. Space Admin., 1972.

[35] *International Standards and Recommended Practices, Annex 10, Volume 1: Radio Navigation Aids*, 6th ed., Jul. 2004.

[36] J. Bhatti and T. E. Humphreys
Hostile control of ships via false GPS signals: Demonstration and detection
Navig., J. Inst. Navig., vol. 64, no. 1, pp. 51–66, Spring 2017.

Çağatay Tanıl received the B.S. and M.S. in mechanical engineering from Middle East Technical University, Ankara, Turkey, in 2006 and 2009, respectively. He is currently working toward the Ph.D. degree in mechanical and aerospace engineering at Illinois Institute of Technology, Chicago, IL, USA.

From 2006 to 2009, he was a Researcher in 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 was a Senior Research Engineer in Roketsan Missiles Industries, Ankara, Turkey, leading several work packages of guidance, control, and trajectory optimization of antiship cruise missiles. He is currently a Research Assistant in the Navigation and Guidance Laboratory, Chicago, IL, USA, focusing on antispoofing attack algorithms for aircraft precision landing.

Samer Khanafseh received the B.S. degree in Mechanical Engineering from Jordan University of Science and Technology, Irbid, Jordan, in 2000, and the M.S. and Ph.D. degrees in aerospace engineering from Illinois Institute of Technology (IIT), Chicago, IL USA, in 2003 and 2008, respectively.

He has been involved in several aviation applications such as autonomous airborne refueling of unmanned air vehicles, autonomous shipboard landing for NUCAS and JPALS programs and ground-based augmentation system. He is currently a Research Assistant Professor at Mechanical and Aerospace Engineering Department, IIT. His research interests include high-accuracy and high-integrity navigation algorithms for close proximity applications, cycle ambiguity resolution, high integrity applications, fault monitoring, and robust estimation techniques.

Dr. Khanafseh is a member of the Institute of Navigation. He received the 2011 Institute of Navigation Early Achievement Award for his outstanding contributions to the integrity of carrier phase navigation systems.

Mathieu Joerger (M'14) received the Diplome d'Ingenieur in mechatronics from the National Institute of Applied Sciences, Strasbourg, France, in 2002, and the M.S. and Ph.D. in mechanical and aerospace engineering from the Illinois Institute of Technology (IIT), in 2002 and 2009, respectively.

He is currently a Project Leader at IIT for multiconstellation advanced receiver autonomous integrity monitoring, for robust laser-based positioning, and for unmanned aircraft system sense and avoid. He is also a Research Assistant Professor, IIT. His research interests include autonomous ground vehicle navigation and control, integration of carrier phase GPS with laser-scanner observations, and augmentation of GPS with low-earth-orbiting Iridium satellites.

Dr. Joerger is a member of The American Institute of Aeronautics and Astronautics and the Institute of Navigation (ION). He received the 2009 ION Bradford Parkinson Award and the 2014 ION Early Achievement Award.

Boris Pervan (SM'15) received the B.S. degree from the University of Notre Dame, Notre Dame, IN, USA, in 1986, the M.S. degree from the California Institute of Technology, Pasadena, CA, USA, in 1987, and the Ph.D. degree from Stanford University, Stanford, CA, USA, in 1996, all in aerospace engineering.

From 1987 to 1990, he was a Systems Engineer in Hughes Space and Communications Group, responsible for mission analysis on commercial and government spacecraft programs. From 1996 to 1998, he was a Research Associate at Stanford University, serving as Project Leader for GPS Local Area Augmentation System Research and Development. He is currently a Professor of mechanical and aerospace engineering in the Illinois Institute of Technology, Chicago, IL, USA.

Prof. Pervan is an Associate Fellow of The American Institute of Aeronautics and Astronautics, a Fellow of the Institute of Navigation (ION), and the Editor-in-Chief of the ION journal *Navigation*. He received the Mechanical and Aerospace Department Excellence in Research Award (2007), IIT/Sigma Xi Excellence in University Research Award (2005), University Excellence in Teaching Award (2005), Ralph Barnett Mechanical and Aerospace Department Outstanding Teaching Award (2002, 2009), 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).