Kalman Filter-based INS Monitor to Detect GNSS Spoofers Capable of Tracking Aircraft Position

Çağatay Tanıl, Samer Khanafseh, Mathieu Joerger, Boris Pervan
Illinois Institute of Technology

Abstract – **In this work, we propose an innovation-based INS spoofing monitor that utilizes a tightly-coupled INS-GNSS integration in a Kalman filter. The performance of the monitor is evaluated when a spoofer tracks and estimates the aircraft position. To create the worst case spoofing conditions, we analytically derive a Kalman filter-based worst-case sequence of spoofed GNSS measurements. Utilizing this worst-case spoofing attack scenario during a Boeing 747 (B747) final approach, we prove that unless the spoofer's position-tracking devices have unrealistic accuracy and no-delay, the proposed INS monitor performance is highly effective in detecting spoofing attacks.**

I. INTRODUCTION

GNSS spoofing attack is a critical threat to positioning integrity, particularly in aircraft's final approach where the consequences are potentially catastrophic. In this paper, we propose a simple INS spoofing monitor and statistically validate its performance against worst-case spoofing attacks even if the spoofer has the ability to estimate the real-time position of the aircraft – for example, by means of remote tracking from the ground.

A spoofing attack happens when a counterfeit signal is deliberately broadcast to an aircraft, potentially resulting in incorrect position estimates. As a result, the trajectory of the target user can be manipulated through the fake broadcast signals [4]. Numerous anti-spoofing techniques have been developed and vulnerability of these existing methods have been discussed in [12, 13]. These include cryptographic authentication techniques employing modified GNSS navigation data [14–16], spoofing discrimination using spatial processing by antenna arrays and automatic gain control schemes [5, 17, 18], GNSS signal direction of arrival comparison [19] code and phase rate consistency checks [20], high-frequency antenna motion [7], and signal power monitoring techniques [21, 22]. Intuitive approaches to monitor for spoofing attacks using redundant sensors have also been proposed, however the first thorough description of their implementation and performance in terms of probability of false alarm and probability of missed detection was first introduced in [3].

The INS detector introduced in [2, 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. 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 [6].

Given this context, our previous work [3] illustrated how a spoofer can introduce false measurements slowly into the GNSS signal such that they corrupt the tightly coupled position solution while going unnoticed by the detector. It was also shown that if the spoofer knows the exact trajectory of an aircraft and has enough time for spoofing, he or she might eventually cause errors large enough to exceed hazard safety limits, again without triggering an alarm from the detector. However, it was acknowledged that in reality, the users 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 are assumed to be unknown to the spoofer, would enhance detection capability of the INS monitor.

In [2], 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 (approximately 10^9 to meet aircraft landing integrity requirements). In our latest work [1], we investigated the impact on spoofing detection due to an aircrafts response to control actions (actuated by the autopilot) due to spoofed GNSS signals. In response to the manipulated position state estimates, the aircraft autopilot commands an acceleration (force) to maneuver the aircraft to the spoofer's desired trajectory. As with the gust case, the controller response results in transient behavior immediately reflected by INS, but not on 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 on all our previous studies is that the spoofer knows that the aircraft uses INS to detect spoofing attacks, but has no real-time knowledge of the actual aircraft position during spoofing attack. In this paper, we first assume that the spoofer has the ability to estimate the real-time position of the aircraft, for example, by means of remote tracking from the ground. In addition, we assume that the spoofer have the knowledge of the exact INS and GNSS error models of the aircraft, and derive a worst-case fault profile that maximizes the integrity risk. Unlike the previous work, which used a batch estimator to derive the worst-case fault profile, we utilize the more realistic Kalman filter estimator and innovation-based cumulative test statistic in analytically deriving the worst-case fault vector. Then, we investigate the leveraging effect of the tracking sensor errors in making INS monitoring effective even if the spoofer has the ability to estimate the real-time position of the aircraft. We show that although the spoofer injects the worst-case spoofed measurements based on the sensed actual position of the aircraft, tracking sensor errors and lack of measuring angular states of the aircraft will be reflected as inconsistency in the test statistic and make the proposed INS monitor effective.

In this paper, we first define the proposed INS monitor that utilizes a Kalman filter-based cumulative test statistic. Next, we construct a stochastic performance evaluation model that stands for the state estimate error dynamics and the innovation propagation in the existence of a spoofing attack with real-time position tracking. To obtain the worst-case scenario within wide variety of threat space, we then introduce the analytical derivation for a Kalman filter-based worst-case fault. Finally, fusing the worst-case fault with the evaluation model, we perform covariance analysis simulations to quantify the performance of the monitor in terms of integrity risk for B747 landing approach.

II. INS AIRBORNE MONITOR

RAIM was originally developed to detect satellite faults by exploiting the extra redundancy in satellite measurements. The residual vector is defined as the difference between the predicted measurements and the actual measurements. In RAIM monitors, the test statistic is defined as the weighted norm of the residual vector. Under fault free conditions, the statistical behavior of the test statistic is governed by the measurement noise characteristics. For a given false alarm requirement, these characteristics are used to define a threshold for the RAIM monitor. Unlike conventional RAIM usage, detection concepts used in this work utilize the redundancy through INS measurements.

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 [23]. This work uses a tightly-coupled integration.

A. Tightly-coupled INS-GNSS Kalman Filter Estimator

The estimator in INS utilizes a kinematic model to predict aircraft motion as [8]

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

where $\boldsymbol{x}_n = [\delta\boldsymbol{r}, \delta\boldsymbol{v}, \delta\boldsymbol{E}]^T$ is 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 $\boldsymbol{u} = [\delta\mathbf{f}, \delta\boldsymbol{\omega}]^T$ contains the deviations in specific force $\delta\mathbf{f}$ and angular velocity $\delta\boldsymbol{\omega}$ relative to the inertial frame.

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

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

$\boldsymbol{\nu}_n$ 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

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

where $\boldsymbol{\eta}_b$ represents the driving white noise and $\boldsymbol{\tau}$ represents the autocorrelation time constants of biases.

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

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

Defining $\overline{\boldsymbol{w}} = \boldsymbol{G}_w\boldsymbol{w}$, 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, 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 (5).

Since the main focus of this work is to detect spoofing during landing approach, we assume a double-difference (DD) GNSS measurements. The actual GNSS code and carrier phase measurement equation linearized about a nominal position, is represented for the k^{th} time epoch as [9]

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

where $\boldsymbol{z}_k$ is the actual GNSS measurement vector containing carrier and code phase measurements after subtracting the nominal, $\boldsymbol{G}^*$ 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 variation on the position of the aircraft relative to reference station represented in navigation frame, $\boldsymbol{\nu}_{\rho\phi_k} \sim \mathcal{N}(0, \boldsymbol{V}_k)$ is the DD carrier and code measurement error vector.

In tightly coupled mechanism, raw INS and GNSS data are processed in a unified Kalman filter where the coupling between process model and spoofed measurement model can be obtained by first relating the state vector $\delta\boldsymbol{r}_k$ in (20) to the state vector $\boldsymbol{x}_k$ in the process model in (5) as

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

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

Using the relation in (7), the measurement in (20) is reformulated as

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

where $\boldsymbol{H}_k$ is the observation matrix of the augmented measurement model. It should be noted that, although the augmentation of multipath and cycle ambiguity states in (5) and (8) is not shown for the sake of simplicity in the equations. They are accounted for in the implementation and the results in Section IV.

Given the measurement model in (8) and 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.

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 at time epoch k, and optimally computed by the actual 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 augmented state estimate error covariance at time epoch k and 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 prior information on the state estimate error covariance at time k and 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 use an innovation-based INS monitor, which utilizes Kalman filter in an INS-GNSS integration. The innovation $\boldsymbol{\gamma}$ 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).

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

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

where $\boldsymbol{S}_n$ is innovation vector covariance matrix at time epoch n.

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

$$q_k < T^2 \tag{16}$$

Let n be the number of measurements, under fault free conditions, the test statistic q_k is centrally chi-square distributed with $k \times n$ degrees of freedom. For a given false alarm requirement, the threshold T2 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,

$$\lambda_k^2 = \sum_{i=1}^{k} \mathbb{E}[\boldsymbol{\gamma}_i]^T\boldsymbol{S}_i^{-1}\mathbb{E}[\boldsymbol{\gamma}_i] \tag{17}$$

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 Kalman filter-based 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. We also introduce an analytical derivation for a Kalman filter-based worst-case fault that maximize 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

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 GNSS measurement that the aircraft receives will be the spoofer's broadcast $\boldsymbol{z}_k^s$ which is expressed as

$$\boldsymbol{z}_k^s = \boldsymbol{H}_k\hat{\boldsymbol{x}}_k^s + \boldsymbol{\nu}_{\rho\phi_k} + \boldsymbol{f}_k \tag{18}$$

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

$$\hat{\boldsymbol{x}}_k^s = \boldsymbol{x}_k + \tilde{\boldsymbol{x}}_k^s \tag{19}$$

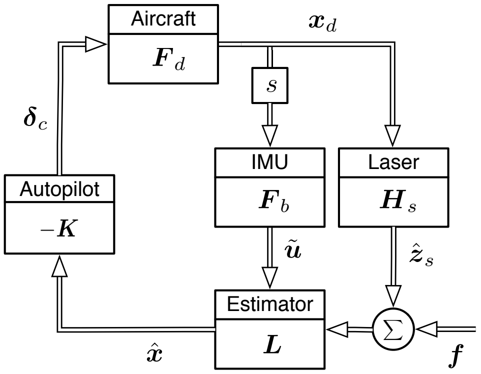

Fig. 1. An example closed loop model for an aircraft altitude hold system in the existence of a GNSS spoofing attack with laser position tracking from ground.

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

Substituting (19) into (18), the spoofed measurement becomes

$$\boldsymbol{z}_k^s = \boldsymbol{H}_k \boldsymbol{x}_k + \boldsymbol{\nu}_{\rho\phi_k} + \underbrace{\boldsymbol{H}_k \tilde{\boldsymbol{x}}_k^s + \boldsymbol{f}_k}_{\boldsymbol{f}_k'} \tag{20}$$

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

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 (20), that is

$$\hat{\boldsymbol{x}}_k = \overline{\boldsymbol{x}}_k + \boldsymbol{L}_k \big(\boldsymbol{z}_k^s - \boldsymbol{H}_k \overline{\boldsymbol{x}}_k\big) \tag{21}$$

Substituting (20) into (21) gives

$$\hat{\boldsymbol{x}}_k = \underbrace{\big(\boldsymbol{I} - \boldsymbol{L}_k \boldsymbol{H}_k\big)}_{\boldsymbol{L}_k^{'}} \overline{\boldsymbol{x}}_k + \boldsymbol{L}_k \boldsymbol{H}_k \boldsymbol{x}_k + \boldsymbol{L}_k \big(\boldsymbol{\nu}_{\rho\phi_k} + \boldsymbol{f}_k'\big) \tag{22}$$

Substituting time update equation (9) into (22),

$$\hat{\boldsymbol{x}}_k = \boldsymbol{L}_k^{'} \boldsymbol{\Phi}\, \hat{\boldsymbol{x}}_{k-1} + \boldsymbol{L}_k \boldsymbol{H}_k \boldsymbol{x}_k + \boldsymbol{L}_k^{'} \boldsymbol{\Gamma}\, \tilde{\boldsymbol{u}}_{k-1} + \boldsymbol{L}_k \big(\boldsymbol{\nu}_{\rho\phi_k} + \boldsymbol{f}_k'\big) \tag{23}$$

Let us define the state estimate error as $\tilde{\boldsymbol{x}}_k = \hat{\boldsymbol{x}}_k - \boldsymbol{x}_k$. Subtracting (5) from (23) gives the state estimate error dynamics as

$$\tilde{\boldsymbol{x}}_k = \boldsymbol{L}_k^{'} \boldsymbol{\Phi}\, \tilde{\boldsymbol{x}}_{k-1} - \boldsymbol{L}_k^{'} \overline{\boldsymbol{w}}_{k-1} + \boldsymbol{L}_k \big(\boldsymbol{\nu}_{\rho\phi_k} + \boldsymbol{f}_k'\big) \tag{24}$$

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 (20) as

$$\gamma_k = \boldsymbol{z}_k^s - \boldsymbol{H}_k \overline{\boldsymbol{x}}_k \tag{25}$$

Using (5) and (9), the current innovation vector γ_k in (25) can be expressed in terms of the previous state estimate error $\tilde{\boldsymbol{x}}_{k-1}$ as

$$\gamma_k = \boldsymbol{f}_k' + \boldsymbol{\nu}_{\rho\phi_k} - \boldsymbol{H}_k \big(\boldsymbol{\Phi}\, \tilde{\boldsymbol{x}}_{k-1} - \overline{\boldsymbol{w}}_{k-1}\big) \tag{26}$$

Augmenting the state estimate error model in (24) and the innovation model in (26) results in a performance evaluation model capturing the impact of the error in spoofer's tracking sensors and the fault on both the state estimate error and the innovation as

$$\begin{bmatrix} \tilde{\boldsymbol{x}}_k \\ \gamma_k \end{bmatrix} = \overbrace{\begin{bmatrix} \boldsymbol{L}_k^{'} \boldsymbol{\Phi} & 0 \\ -\boldsymbol{H}_k \boldsymbol{\Phi} & 0 \end{bmatrix}}^{\boldsymbol{\Phi}_{y_k}} \overbrace{\begin{bmatrix} \tilde{\boldsymbol{x}}_{k-1} \\ \gamma_{k-1} \end{bmatrix}}^{\boldsymbol{y}_{k-1}} + \underbrace{\begin{bmatrix} -\boldsymbol{L}_k^{'} & \boldsymbol{L}_k \\ \boldsymbol{H}_k & \boldsymbol{I} \end{bmatrix}}_{\boldsymbol{\Upsilon}_{y_k}} \underbrace{\begin{bmatrix} \overline{\boldsymbol{w}}_{k-1} \\ \boldsymbol{\nu}_{\rho\phi_k} \end{bmatrix}}_{\boldsymbol{w}_{y_k}} + \underbrace{\begin{bmatrix} \boldsymbol{L}_k \\ \boldsymbol{I} \end{bmatrix}}_{\boldsymbol{\Psi}_{y_k}} \boldsymbol{f}_k' \tag{27}$$

where $\boldsymbol{y}$ is defined as the state vector of the evaluation model including the state estimate error and the innovation. $\boldsymbol{\Phi}_y$, $\boldsymbol{\Upsilon}_y$, and $\boldsymbol{\Psi}_y$ are the state transition, noise coefficient, and fault input coefficient matrices of the evaluation model, respectively. Using (27), the mean $\mathbb{E}[\boldsymbol{y}_k]$ and covariance $\boldsymbol{Y}_k$ of the evaluation model state $\boldsymbol{y}$ can be propagated as

$$\mathbb{E}[\boldsymbol{y}_k] = \boldsymbol{\Phi}_{y_k} \mathbb{E}[\boldsymbol{y}_{k-1}] + \boldsymbol{\Psi}_{y_k} \boldsymbol{f}_{w_k}' \tag{28}$$

$$\boldsymbol{Y}_k = \boldsymbol{\Phi}_{y_k} \boldsymbol{Y}_{k-1} \boldsymbol{\Phi}_{y_k}^T + \boldsymbol{\Upsilon}_{y_k} \boldsymbol{W}_{y_k} \boldsymbol{\Upsilon}_{y_k}^T \tag{29}$$

where $\boldsymbol{W}_{y_k}$ is the covariance of $\boldsymbol{w}_{y_k}$.

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

$$I_{r_k} = \Pr\big(|\varepsilon_k| > l\,;\, q_k < T^2 \mid H_s\big) \tag{30}$$

where l is the vertical alert limit, and T^2 is pre-defined threshold for detection which is same as that in (16).

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 $\tilde{\boldsymbol{x}}_k$ using the row transformation vector $\boldsymbol{\tau}_\varepsilon$ as

$$\varepsilon_k = \boldsymbol{\tau}_\varepsilon \tilde{\boldsymbol{x}}_k \tag{31}$$

where ε_k is normally distributed.

Cumulative test statistic q_k in (15) is expressed in vector form as

$$q_k = \begin{bmatrix} \gamma_1^T & \cdots & \gamma_k^T \end{bmatrix} \underbrace{\begin{bmatrix} \boldsymbol{S}_1^{-1} & & \\ & \ddots & \\ & & \boldsymbol{S}_k^{-1} \end{bmatrix}}_{\boldsymbol{S}_{1|k}^{-1}} \underbrace{\begin{bmatrix} \gamma_1 \\ \vdots \\ \gamma_k \end{bmatrix}}_{\gamma_{1|k}} \tag{32}$$

where $\boldsymbol{S}_k$ is the innovation covariance obtained from $\boldsymbol{Y}_k$ in (29) as

$$\boldsymbol{S}_k = \boldsymbol{T}_\gamma \boldsymbol{Y}_k \boldsymbol{T}_\gamma^T \tag{33}$$

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 (17) is written as

$$\lambda_k^2 = \mathbb{E}[\boldsymbol{\gamma}_{1|k}^T]\, \boldsymbol{S}_{1|k}^{-1}\, \mathbb{E}[\boldsymbol{\gamma}_{1|k}] \tag{34}$$

Using the Kalman filter-based evaluation model in (27), it is proved that $\mathbb{E}[\tilde{\boldsymbol{x}}_i \boldsymbol{\gamma}_j^T] = 0$ for all $i \geq j$ in Appendix A. 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. Therefore, integrity risk I_{r_k} can be written as a multiplication of two probabilities as

$$I_{r_k} = \Pr\left(|\varepsilon_k| > l\right)\, \Pr\left(q_k < T^2\right) \tag{35}$$

C. Kalman Filter-based Worst-case Fault Derivation

In this work, since all GNSS measurements may be impacted by the spoofing attack, it is assumed that all GNSS measurements are faulty and that IMU is the fault-free source of redundancy in the INS monitor. If a spoofing attack is not detected instantaneously, it may impact INS error state estimates through the tightly coupled mechanism, which impacts subsequent detection capability. Therefore, a smart spoofer may select a fault profile $\boldsymbol{f}_{1|k}$ that has smaller faults at the beginning and gradually increases over time, thereby corrupting INS calibration without being detected.

A worst case fault derivation based on a batch estimator was previously introduced in [6]. In this work, we extend the methodology to analytically 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 or in other words, maximizing the integrity risk. To obtain the optimal direction and magnitude of the worst-case fault history vector $\boldsymbol{f}_{1|k}$, we utilize the Kalman filter-based evaluation model in (27) by conservatively assuming that the spoofer has the knowledge of exact error models for the aircraft's INS-GNSS system and account for his/her own position tracking sensor errors in the worst-case fault computation. (28) and (34) indicate that the fault history vector $\boldsymbol{f}_{1|k}$ affects the mean of $\tilde{\boldsymbol{x}}_k$ and the non-centrality 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 and provides an upper bound to the integrity risk I_{r_k} in (35) [6]. That is, the optimization problem for obtaining the worst-case fault can be formulated as

$$\underset{\boldsymbol{f}_{1|k}}{\text{maximize}} \quad \rho_k^2 = \frac{\mathbb{E}[\varepsilon_k]^2}{\lambda_k^2} \tag{36}$$

Recall that ε_k and λ^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 (28) and (27), the means of $\tilde{\boldsymbol{x}}_k$ and $\boldsymbol{\gamma}_k$ can be extracted as

$$\mathbb{E}[\tilde{\boldsymbol{x}}_k] = \underbrace{\boldsymbol{L}_k^{'}\boldsymbol{\Phi}}_{\boldsymbol{L}_k^{''}}\, \mathbb{E}[\tilde{\boldsymbol{x}}_{k-1}] + \boldsymbol{L}_k \boldsymbol{f}_k \tag{37}$$

$$\mathbb{E}[\boldsymbol{\gamma}_k] = -\boldsymbol{H}_k \boldsymbol{\Phi}\, \mathbb{E}[\tilde{\boldsymbol{x}}_{k-1}] + \boldsymbol{f}_k \tag{38}$$

Assuming fault-free initial condition as $\mathbb{E}[\tilde{\boldsymbol{x}}_0] = 0$, the particular solution to (37) is obtained as a function of $\boldsymbol{f}_{1|k}$ as

$$\mathbb{E}[\tilde{\boldsymbol{x}}_k] = \underbrace{\begin{bmatrix}\boldsymbol{A}_{1k} & \dots & \boldsymbol{A}_{kk}\end{bmatrix}}_{\boldsymbol{A}_k} \underbrace{\begin{bmatrix}\boldsymbol{f}_1 \\ \vdots \\ \boldsymbol{f}_k\end{bmatrix}}_{\boldsymbol{f}_{1|k}} \tag{39}$$

where

$$\boldsymbol{A}_{ik} = \begin{cases}\boldsymbol{L}_k^{''}\boldsymbol{L}_{k-1}^{''}\dots\boldsymbol{L}_{1+i}^{''}\boldsymbol{L}_i & \text{if } i < k \\ \boldsymbol{L}_i & \text{if } i = k\end{cases} \tag{40}$$

Substituting (39) into (38) gives the mean of innovation as a function of $\boldsymbol{f}_{1|k}$ as

$$\mathbb{E}[\boldsymbol{\gamma}_k] = \underbrace{\begin{bmatrix}-\boldsymbol{H}_k\boldsymbol{\Phi}\boldsymbol{A}_{k-1} & \boldsymbol{I}\end{bmatrix}}_{\boldsymbol{B}_k} \underbrace{\begin{bmatrix}\boldsymbol{f}_{1|k-1} \\ \boldsymbol{f}_k\end{bmatrix}}_{\boldsymbol{f}_{1|k}} \tag{41}$$

Substituting (41) into (17) gives the non-centrality parameter of the cumulative test statistic as

$$\lambda_k^2 = \sum_{i=1}^{k} \boldsymbol{f}_{1|i}^T \boldsymbol{B}_i^T \boldsymbol{S}_i^{-1} \boldsymbol{B}_i \boldsymbol{f}_{1|i} \tag{42}$$

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 measurement at each time epoch and $0 < i < k$. Then, (42) is equivalently expressed in block matrix form as

$$\lambda_k^2 = \boldsymbol{f}_{1|k}^T \begin{bmatrix}\overline{\boldsymbol{B}}_1^T & \dots & \overline{\boldsymbol{B}}_k^T\end{bmatrix} \underbrace{\begin{bmatrix}\boldsymbol{S}_1^{-1} & & \\ & \ddots & \\ & & \boldsymbol{S}_k^{-1}\end{bmatrix}}_{\boldsymbol{S}_{1|k}^{-1}} \underbrace{\begin{bmatrix}\overline{\boldsymbol{B}}_1 \\ \vdots \\ \overline{\boldsymbol{B}}_k\end{bmatrix}}_{\overline{\boldsymbol{B}}_{1|k}} \boldsymbol{f}_{1|k} \tag{43}$$

Substituting (39), (43) and (31) into (36) gives the failure mode slope ρ_k as a function of only the fault history vector $\boldsymbol{f}_{1|k}$ as

$$\rho_k^2 = \frac{\boldsymbol{f}_{1|k}^T \boldsymbol{A}_k^T \boldsymbol{\tau}_\varepsilon^T \boldsymbol{\tau}_\varepsilon \boldsymbol{A}_k \boldsymbol{f}_{1|k}}{\boldsymbol{f}_{1|k}^T \overline{\boldsymbol{B}}_{1|k}^T \boldsymbol{S}_{1|k}^{-1} \overline{\boldsymbol{B}}_{1|k} \boldsymbol{f}_{1|k}} \tag{44}$$

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

$$\breve{\boldsymbol{f}}_{1|k} = \left(\boldsymbol{S}_{1|k}^{-1/2}\overline{\boldsymbol{B}}_{1|k}\right)\boldsymbol{f}_{1|k} \tag{45}$$

The failure mode slope in (44) can be rewritten in terms of $\breve{\boldsymbol{f}}_{1|k}$ as

$$\rho_k^2 = \frac{\breve{\boldsymbol{f}}_{1|k}^T \boldsymbol{\kappa}_k^T \boldsymbol{\kappa}_k \breve{\boldsymbol{f}}_{1|k}}{\breve{\boldsymbol{f}}_{1|n}^T \breve{\boldsymbol{f}}_{1|k}} \tag{46}$$

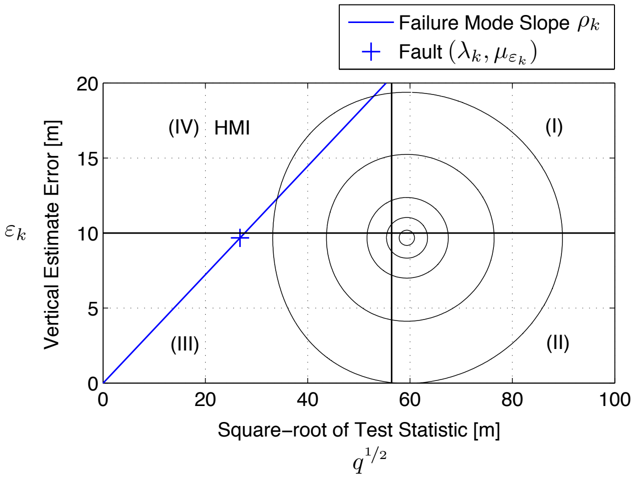

Fig. 2. The worst-case fault and failure mode slope for a 140 s approach flight of B747 with a GNSS sampling frequency of 2 Hz. The marker (+) on the failure mode slope corresponds to the worst-case fault for this scenario. The black curves are lines of constant joint probability density obtained using (35).

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

$$\boldsymbol{\kappa}_k = \boldsymbol{\tau}_\varepsilon \boldsymbol{A}_k \left(\boldsymbol{S}_{1|k}^{-1/2} \overline{\boldsymbol{B}}_{1|k}\right)^{-1} \tag{47}$$

From (46), it can be concluded that $\breve{\boldsymbol{f}}_{1|k}$ that maximizes 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

$$\boldsymbol{f}_{w_{1|k}} = \alpha_w \, \mathbf{f}_{w_{1|k}} \tag{48}$$

Using (45) and (47), the worst-case fault direction $\mathbf{f}_{w_{1|k}}$ is obtained as

$$\mathbf{f}_{w_{1|k}} = \left(\boldsymbol{S}_{1|k}^{-1/2} \overline{\boldsymbol{B}}_{1|k}\right)^{-1} \boldsymbol{\kappa}_k \tag{49}$$

The worst-case fault magnitude α_w is a scalar that is determined through iteration to maximize I_{r_k} in (35) along the worst-case direction $\mathbf{f}_{w_{1|k}}$ obtained in (49).

IV. Performance Analysis Results

To test the performance of the proposed INS spoofing monitor, a covariance analysis with a B747 flight on approach is simulated at trimmed flight conditions in Table I. The IMU sensor and GNSS receiver specifications are provided in Table II. 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 at fault free conditions and reached steady state prior to the spoofing attack and the monitor.

To investigate the performance of the INS monitor, we initially assumed a spoofing attack with perfect tracking sensors that estimates the exact aircraft position ($\tilde{\boldsymbol{x}}_k^s = 0$) and computed the worst-case fault profile that maximizes the integrity risk for a given spoofing attack period. An example worst-case fault and its failure mode slope for a 140 s B747 approach are illustrated in Fig. 2. The non-central chi distribution $q_k^{1/2}$ and the normal distribution ε_k are represented on the x-axis and y-axis, respectively. The x-y plane is divided into four quadrants by a typical vertical alert limit $l = 10$ m and a threshold $T = 56.4$ m computed using fault-free test statistic. The fourth quadrant refers to the area of hazardous misleading information (HMI), where undetected faults result in an unacceptably large estimation errors. The probability of being in the HMI area corresponds to the integrity risk in (35). Each point $(\lambda_k, \mu_{\varepsilon_k})$ on the x-y plane corresponds to a different fault, and for this scenario the worst-case fault is obtained at the marker ($\lambda_k = 26.8$ m, $\mu_{\varepsilon_k} = 9.7$ m) located on the worst-case fault failure mode slope (blue line). This worst-case fault results in a distribution in the oval shape contours of constant joint probability density (black curves). The integrity risk for the worst-case fault is computed as $I_r = 5.9 \times 10^{-6}$.

TABLE I
B747 Approach Trimmed Flight Conditions [11]

Flight Conditions	Value	Unit
Speed	63	m/s
Angle of Attack	8	deg
Flight Path Angle	−3	deg
Altitude	Sea Level	–

TABLE II
INS-GNSS Error Parameters [10]

Parameter	Value	Unit
Gyro angle random walk	0.001	$^\circ/\sqrt{\mathrm{h}}$
Gyro bias error	0.01	$^\circ$/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
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

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 seen in Fig. 3, if the spoofer has perfect position tracking sensors, increasing the attack period eventually causes high integrity risks of up to 1. The reason is that, increasing the spoofing time allows the spoofer to inject faults to the system more slowly (see Fig. 4), which reduces the monitors ability to detect spoofing attacks by corrupting the estimation of INS states. On the other hand, for limited attack periods, the integrity risk is considerably low. For example, at the GNSS sampling frequency of 2 Hz, 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. Fig. 3 also illustrates that at lower GNSS sampling rates, the worst-case spoofing attacks result in lower integrity risks for same attack periods.

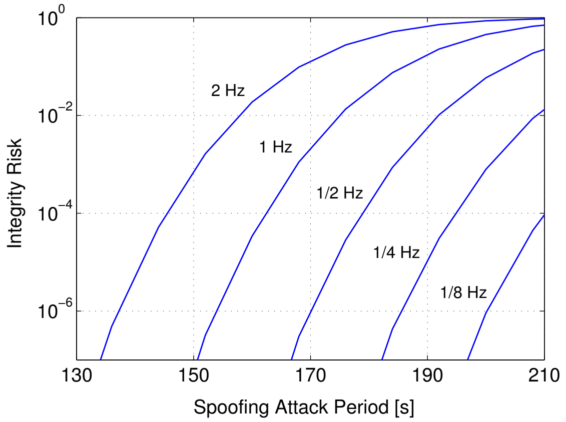

Fig. 3. The impact of spoofing attack period and GNSS sampling frequency on the integrity risk. The results are obtained for a B747 landing approach in the presence of a worst-case spoofing attack with a closed-loop position tracking using a sensor having a perfect accuracy and no-delay.

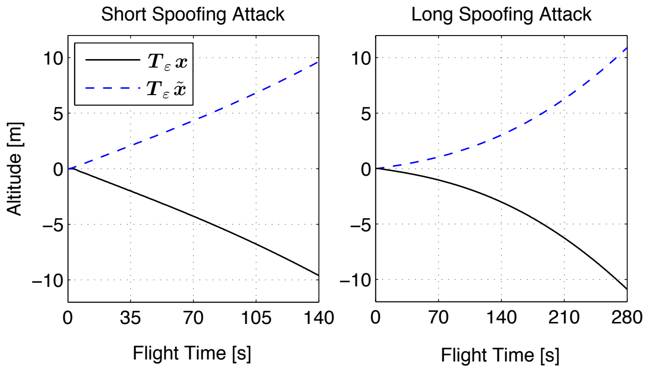

Fig. 4. The vertical components of aircraft position $\boldsymbol{x}$ and its estimate error $\tilde{\boldsymbol{x}}$ due to the worst-case fault profile computed for a closed-loop spoofing attack for 140 s (left) and 280 s (right) landing approach of a B747 with GNSS sampling rate of 2 Hz.

Previous results assumes that the spoofer is able to estimate the exact position of the aircraft. In order to be more realistic, the errors in position tracking must be accounted for. Therefore, we assume that the spoofer's position estimate error $\tilde{\boldsymbol{x}}_k$ is a zero-mean white noise $\tilde{\boldsymbol{x}}^s_k \sim \mathcal{N}(0, \hat{\boldsymbol{P}}^s_k)$. Utilizing deterministic noise profiles for the vertical component of $\tilde{\boldsymbol{x}}^s_k$, we illustrate the leveraging effect of the altitude tracking errors in detecting spoofing attacks. Fig. 5 shows that for a position tracking error of more than 4 mm (1-sigma), the integrity risk always remains below 10^{-9}, which is a typical safety requirement in aviation applications. The results are very promising because that level of tracking accuracy is unrealistic to be achieved with any combination of the existing high-grade position tracking systems (e.g., laser, radar, vision).

V. CONCLUSION

In this work, we developed a generalized statistical methodology to evaluate the performance of the INS monitor by deriving a Kalman filter-based evaluation model, where the

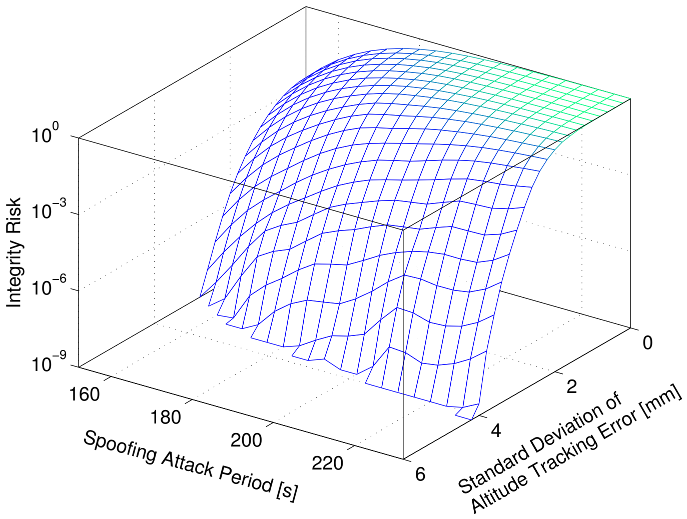

Fig. 5. The impact of altitude tracking error and attack period on the integrity risk in the presence of worst-case spoofing attacks with a GNSS sampling frequency of 2 Hz.

GNSS fault is fed into a tightly-coupled INS-GNSS integrated system. We also introduced a novel analytical derivation of a worst-case fault profile for spoofing attacks with aircraft position tracking. Utilizing this worst case fault profile, we performed a covariance analysis to quantify the detector performance in terms of integrity risk. The simulation results showed that, although we conservatively assumed the spoofer knows the exact INS-GNSS error models of the aircraft and has no-delay in his/her position tracking loop and broadcast, the proposed monitor provides a direct means to detect spoofing attacks unless the spoofer's tracking sensors has unrealistic high accuracy.

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. The authors would also like to thank Dr. Todd Humphreys of University of Texas at Austin for his advice about Appendix A.

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 enables us formulate integrity risk as in (35) instead of numerically more complicated form as in (30). In this section, we prove the statistical independency 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 (27) as

$$\tilde{\boldsymbol{x}}_k = \boldsymbol{L}_k^{'}\boldsymbol{\Phi}\,\tilde{\boldsymbol{x}}_{k-1} - \boldsymbol{L}_k^{'}\overline{\boldsymbol{w}}_{k-1} + \boldsymbol{L}_k\boldsymbol{\nu}_{\rho\phi_k} + \boldsymbol{L}_k\boldsymbol{f}_{w_k} \quad (50)$$

$$\boldsymbol{\gamma}_k = -\boldsymbol{H}_k\boldsymbol{\Phi}\,\tilde{\boldsymbol{x}}_{k-1} + \boldsymbol{H}_k\,\overline{\boldsymbol{w}}_{k-1} + \boldsymbol{\nu}_{\rho\phi_k} + \boldsymbol{f}_{w_k} \quad (51)$$

Using (50) and (51), covariance between the current state estimate error $\tilde{\boldsymbol{x}}_k$ and the innovation $\boldsymbol{\gamma}_k$ is obtained as

$$\mathbb{E}[\tilde{\boldsymbol{x}}_k\boldsymbol{\gamma}_k^T] = -\boldsymbol{L}_k^{'}\big(\boldsymbol{\Phi}\,\hat{\boldsymbol{P}}_{k-1}\boldsymbol{\Phi}^T + \overline{\boldsymbol{W}}_{k-1}\big)\boldsymbol{H}_k^T + \boldsymbol{L}_k\boldsymbol{V}_k \quad (52)$$

Recall $\overline{\boldsymbol{P}}_k = \boldsymbol{\Phi}\,\hat{\boldsymbol{P}}_{k-1}\boldsymbol{\Phi}^T + \overline{\boldsymbol{W}}_{k-1}$ from (13) and $\boldsymbol{L}_k^{'} = \boldsymbol{I} - \boldsymbol{L}_k\boldsymbol{H}_k$ from (22), and substitute them into (52)

$$\mathbb{E}[\tilde{\boldsymbol{x}}_k\boldsymbol{\gamma}_k^T] = \big(\boldsymbol{L}_k\boldsymbol{H}_k - \boldsymbol{I}\big)\overline{\boldsymbol{P}}_k\,\boldsymbol{H}_k^T + \boldsymbol{L}_k\boldsymbol{V}_k \quad (53)$$

Recall $\boldsymbol{L}_k = \hat{\boldsymbol{P}}_k\boldsymbol{H}_k^T\boldsymbol{V}_k^{-1}$ from (11) and substitute it into (53)

$$\mathbb{E}[\tilde{\boldsymbol{x}}_k\boldsymbol{\gamma}_k^T] = \big(\hat{\boldsymbol{P}}_k\boldsymbol{H}_k^T\boldsymbol{V}_k^{-1}\boldsymbol{H}_k - \boldsymbol{I}\big)\overline{\boldsymbol{P}}_k\,\boldsymbol{H}_k^T + \hat{\boldsymbol{P}}_k\boldsymbol{H}_k^T \quad (54)$$

Re-arranging (12) gives

$$\boldsymbol{H}_k^T\boldsymbol{V}_k^{-1}\boldsymbol{H}_k = \hat{\boldsymbol{P}}_k^{-1} - \overline{\boldsymbol{P}}_k^{-1} \quad (55)$$

Substituting (55) into (54) gives

$$\begin{aligned}\mathbb{E}[\tilde{\boldsymbol{x}}_k\boldsymbol{\gamma}_k^T] &= \big[\hat{\boldsymbol{P}}_k(\hat{\boldsymbol{P}}_k^{-1} - \overline{\boldsymbol{P}}_k^{-1}) - \boldsymbol{I}\big]\,\overline{\boldsymbol{P}}_k\,\boldsymbol{H}_k^T + \hat{\boldsymbol{P}}_k\,\boldsymbol{H}_k^T \\ &= -\hat{\boldsymbol{P}}_k^{-1}\,\boldsymbol{H}_k^T + \hat{\boldsymbol{P}}_k^{-1}\,\boldsymbol{H}_k^T = 0\end{aligned} \quad (56)$$

Eq. (56) proves that $\tilde{\boldsymbol{x}}_k$ and $\boldsymbol{\gamma}_k$ are statistically independent.

REFERENCES

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

[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] 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.

[4] 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.

[5] 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.

[6] 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.

[7] 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

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

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

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

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

[12] 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

[13] 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

[14] 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.

[15] 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.

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

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

[18] 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.

[19] 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.

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

[21] 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.

[22] 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.

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

[24] 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.