

# GNSS Spoofing Attack Detection using Aircraft Autopilot Response to Deceptive Trajectory

Çağatay Tanıl, Samer Khanafseh, Boris Pervan  
*Illinois Institute of Technology*

## BIOGRAPHY

Çağatay Tanıl obtained his B.S. and M.S. in Mechanical Engineering from Middle East Technical University (METU), Turkey, in 2006 and 2009. He is currently a Ph.D. Candidate in Aerospace Engineering at Illinois Institute of Technology (IIT) and Research Assistant in Navigation and Guidance Lab. Prior to doctorate studies at IIT, he worked as a senior design engineer at several defense/aerospace companies (Roketsan Missiles Industries, TAI Turkish Aerospace Industries, Tubitak-SAGE Defense Industries Research and Development Institute) in Turkey from 2006 to 2013. He has been involved in flight mechanics, guidance, navigation and control, optimization, modeling and simulation, and path planning for autonomous systems in aerospace applications. He is currently focused on anti-spoofing attack algorithms for aircrafts.

Dr. Khanafseh is currently a Research Assistant Professor at Mechanical and Aerospace Engineering Department at IIT. He received his M.S. and PhD degrees in Aerospace Engineering from IIT, in 2003 and 2008, respectively. Dr. Khanafseh has been involved in several aviation applications such as Autonomous Airborne Refueling (AAR) of unmanned air vehicles, autonomous shipboard landing for NUCAS and JPALS programs and Ground Based Augmentation System (GBAS). He published 13 journal articles and more than 30 conference papers. His research interests are focused on high accuracy and high integrity navigation algorithms for close proximity applications, cycle ambiguity resolution, high integrity applications, fault monitoring and robust estimation techniques. He was the recipient of the 2011 Institute of Navigation Early Achievement Award for his outstanding contributions to the integrity of carrier phase navigation systems

Dr. Boris Pervan is a Professor of Mechanical and Aerospace Engineering at IIT, where he conducts research on advanced navigation systems. Prior to joining the faculty at IIT, he was a spacecraft mission analyst at Hughes Aircraft Company (now Boeing) and a postdoctoral research associate at Stanford University. Prof. Pervan received his B.S. from the University of Notre Dame, M.S. from the California Institute of Technology, and Ph.D. from Stanford University. He was the recipient of the IIT Sigma Xi Excellence in University Research Award, Ralph Barnett Mechanical and Aerospace Dept. Outstanding Teaching Award, Mechanical and Aerospace Dept. Excellence in Research Award, IIT University Excellence in Teaching Award, IEEE Aerospace

and Electronic Systems Society M. Barry Carlton Award, RTCA William E. Jackson Award, Guggenheim Fellowship (Caltech), and the Albert J. Zahm Prize in Aeronautics (Notre Dame). He is an Associate Fellow of the AIAA, a Fellow of the Institute of Navigation (ION), and Editor-in-Chief of the ION Journal Navigation.

## ABSTRACT

In this work, we propose an innovation-based spoofing monitor that utilizes a tightly-coupled INS-GNSS integration in a Kalman filter and investigate the impact on spoofing detection due to an aircraft's dynamic response to control actions (actuated by the pilot or autopilot) during a spoofing attack. To evaluate the performance of the proposed monitor, we generalize the spoofing integrity analysis by deriving a rigorous statistical methodology capturing the aircraft compensator dynamics in estimation and detection. We prove that for INS-RAIM-equipped aircrafts, aircraft controller response to a spoofed GNSS signal improves the detection capability of the aircrafts. The reason is that the autopilot response will be instantaneously sensed by the inertial sensors, but not reflected in the spoofed GNSS signal. The impact of a generic altitude hold autopilot on the detection of the worst-case spoofing attacks is demonstrated using a standard approach of Boeing 747 (B747). We show that even without exposure to other disturbances such as wind gusts, control reactions to the spoofers deceptive input significantly enhance INS RAIM detection of the spoofing attack although we conservatively select B747 as the least maneuverable aircraft.

## I. INTRODUCTION

Vulnerability of GNSS users to signal spoofing is a critical threat to positioning integrity, especially in aviation applications where the consequences are potentially catastrophic. Spoofing may even become a more serious risk to aviation in the near future with the rollout of the GNSS-based Next Generation Air Traffic Control (ATC) system, and the corresponding reduction in reliance on ground-based radar systems by ATC. In the previous work [3], we showed that the presence of nominal gust disturbances on aircraft enables the detection of malicious spoofing attacks via tightly-coupled GNSS-INS RAIM. In the current work, we further prove that aircraft controller response (actuated by either the pilot or autopilot) provides a significant, additional countermeasure against GNSS spoofing attacks.

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 [5]. Numerous anti-spoofing techniques have been developed, including employing modified GNSS navigation data [6], using antenna arrays and automatic gain control schemes [7], high-frequency antenna motion [8], or signal power analysis techniques. Intuitive approaches to monitor spoofing attacks using redundant sensors have also been proposed, however the first thorough description of their implementation and quantitative measures of performance, in terms of probability of false alarm and probability of missed detection, was introduced in our previous work in [4] and [3].

The GNSS-INS RAIM detector introduced in [4] and [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. 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. 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 [1].

Given this context, in our previous work [4] we 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 RAIM detector. It was also shown that if the spoofer knows the exact trajectory of an aircraft, he or she might eventually cause errors large enough to exceed hazard safety limits, again without triggering an alarm from the RAIM detector. However, it was acknowledged that in reality, the users actual trajectory would always deviate somewhat from a prescribed path (e.g., a straight line final approach) due to natural disturbances such as wind gusts and aircraft dynamic response to control actions. Deviations from the nominal trajectory due to these disturbances, which are initially assumed to be unknown to the spoofer, would enhance detection capability of the INS RAIM monitor.

As a case study in [4], in the presence of simple sinusoidal deviations from a nominal straight trajectory, it was concluded that the monitor was effective, for the cases tested at least, in detecting spoofing attacks with quantifiably low integrity risk. In the subsequent work [3], we generalized the spoofing integrity analysis by deriving the statistical dynamic response of an aircraft to a well-established vertical wind gust power spectrum (the Dryden Gust Turbulence model). 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 this current paper, we investigate how the INS RAIM spoofing detection is impacted by an aircrafts dynamic response to control actions (actuated by the pilot or autopilot) during a spoofing attack. In response to the manipulated position state estimates, the aircraft autopilot commands an acceleration (force) to maneuver the aircraft to the spoofer desired trajectory. (Note that the spoofer desired aircraft trajectory is not the spoofed trajectory itself, but the trajectory that the spoofer wishes the aircraft to follow; that is, if the intent is to make the aircraft drift eastward, then anticipating the aircrafts control response to follow its original prescribed path, the spoofer would inject a westward drift in the spoofed signal.) As with the gust case, the controller response would also result in transient behavior which is immediately reflected in the inertial sensors, but not in the spoofed signal.

To investigate and quantify the impact of controller response on INS RAIM spoofing detection, we augment the aircraft dynamic model with a standard autopilot control system to generate specific forces and angular velocities for input to the INS kinematic model. The INS kinematic model is tightly coupled to the GNSS measurement model in a Kalman filter estimator, for bias estimation and covariance analysis, subject to the worst-case fault profile. The impact of controller dynamics on INS RAIM detection of spoofing is demonstrated using the longitudinal stability characteristics of B747 in landing approach. We show that control reactions to the spoofer deceptive position signals significantly enhance to spoofing attack detection.

## II. GNSS-INS AIRBORNE RAIM 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, RAIM detection concepts used in this work utilize the redundancy through INS measurements.

GNSS and inertial navigation systems 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 [4]. This work uses tightly-coupled integration since the worst-case fault vector in [4] is derived for tightly-coupled formulation.

Within the various disturbances on the aircraft motion, aircraft controller's (autopilot, guidance) response to false GNSS measurements has a significant impact that improves monitor sensitivity to position-domain discrepancies due to spoofing attack. The previous study in [4] proved that if the spoofer have the exact trajectory information of the aircraft, it

is impossible to detect a spoofing with the worst-case fault. On the other hand, in INS-RAIM-equipped aircrafts, the autopilot response to spoofing attack provides a direct means to detect spoofing attacks. The reason is that the control deflections commanded by the autopilot will induce slight maneuvers which are instantaneously reflected in INS measurements, but not in the spoofed GNSS signal. This increases position discrepancy between INS and GNSS measurements.

#### A. Kalman Filter-based RAIM Monitor

We assume an innovation-based RAIM monitor, which utilizes Kalman filter in an INS-GNSS integration. The Kalman filter is based on a discrete augmented dynamic model obtained from linearized INS kinematics, IMU error model and cycle ambiguity dynamics can be expressed in vector form as

$$\mathbf{x}_{k+1}^a = \Phi^a \mathbf{x}_k^a + \Gamma_w^a \mathbf{w}_k \quad (1)$$

where  $\mathbf{x}^a = [\delta \mathbf{r}, \delta \mathbf{v}, \delta \mathbf{E}, \mathbf{b}, \mathbf{N}]^T$  is the augmented state vector including deviations in position  $\mathbf{r}$ , velocity  $\mathbf{v}$ , attitude  $\mathbf{E}$ ; and bias  $\mathbf{b}$  and cycle ambiguity  $\mathbf{N}$ .  $\Phi^a$  is the augmented state transition matrix. The second term in right hand side of (1) stands for the noise due to IMU sensors where  $\mathbf{w} \sim \mathcal{N}(0, \mathbf{W})$  is the noise vector containing white and bias driving noises, and  $\Gamma_w^a$  is the noise coefficient matrix. More details about the derivation of INS mechanization will be introduced in Section III-A and Appendix C.

In addition to the dynamic model in (1), the double-difference (DD) carrier and code GNSS measurement equation can be defined as a function of augmented state vector  $\mathbf{x}^a$  as

$$\mathbf{z}_k = \mathbf{H}_k^a \mathbf{x}_k^a + \boldsymbol{\nu}_{\rho\phi_k} + \mathbf{f}_k \quad (2)$$

where  $\mathbf{z}$  includes carrier and code measurements after correcting with the nominal terms.  $\mathbf{H}^a$  is the augmented observation matrix containing line of sight information and zeros.  $\boldsymbol{\nu}_{\rho\phi} \sim (0, \mathbf{V})$  is the DD carrier and code measurement error vector and  $\mathbf{f}$  denotes fault vector due to spoofing attack. More details about measurement model are given in Section III-B and Appendix D.

Using (1) and (2), the innovation vector  $\boldsymbol{\gamma}$  at time epoch  $k$  is defined as

$$\boldsymbol{\gamma}_k = \mathbf{z}_k - \mathbf{H}_k^a \bar{\mathbf{x}}_k^a \quad (3)$$

where  $\bar{\mathbf{x}}_k^a$  is the a priori estimate of  $\mathbf{x}^a$  at time epoch  $k$  and can be obtained from the Kalman time update equation as

$$\bar{\mathbf{x}}_k^a = \Phi^a \hat{\mathbf{x}}_{k-1}^a \quad (4)$$

where  $\hat{\mathbf{x}}_k^a$  is the a posteriori estimate of  $\mathbf{x}^a$  at time epoch  $k$ .

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

$$q_k = \sum_{n=1}^k \boldsymbol{\gamma}_n^T \mathbf{S}_n^{-1} \boldsymbol{\gamma}_n \quad (5)$$

where  $\mathbf{S}_n$  is innovation covariance at time epoch  $n$ .

RAIM monitor of the actual system checks whether test statistics  $q_k$  is smaller than a pre-defined threshold  $T^2$  as

$$q_k < T^2 \quad (6)$$

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. Under faulted conditions,  $q_k$  is non-centrally chi-square distributed with a non-centrality parameter  $\lambda_k^2$  as

$$\lambda_k^2 = \sum_{n=1}^k \boldsymbol{\mu}_{\gamma_n}^T \mathbf{S}_n^{-1} \boldsymbol{\mu}_{\gamma_n} \quad (7)$$

where  $\boldsymbol{\mu}_{\gamma}$  is the mean of the innovation.

For a given false alarm requirement, the threshold  $T^2$  is determined from the inverse cumulative chi-square distribution. RAIM alarms for a fault if  $q_k$  is bigger than  $T^2$ .

#### B. Monitor Performance Evaluation

A wide variety of possible spoofing scenarios may exist, but when using RAIM monitor, it is not necessary to define a threat space because the worst-case spoofing attack can be determined by finding the profile that maximizes the integrity risk [1]. This profile takes into account the impact of spoofed signals on the test statistic and the user position estimate error simultaneously.

State estimation error  $\boldsymbol{\varepsilon}$  at time epoch  $k$  is defined as

$$\boldsymbol{\varepsilon}_k = \hat{\mathbf{x}}_k^a - \mathbf{x}_k^a \quad (8)$$

where  $\hat{\mathbf{x}}_k^a$  is the augmented state estimate which can be obtained using Kalman measurement update as

$$\hat{\mathbf{x}}_k^a = \bar{\mathbf{x}}_k^a + \mathbf{L}_k (\mathbf{z}_k - \mathbf{H}_k^a \bar{\mathbf{x}}_k^a) \quad (9)$$

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

$$\mathbf{L}_k = \hat{\mathbf{P}}_k^a \mathbf{H}_k^{aT} \mathbf{V}_k^{-1} \quad (10)$$

where  $\hat{\mathbf{P}}_k^a$  is the augmented state estimate error covariance at time epoch  $k$  and is obtained as

$$\hat{\mathbf{P}}_k^a = (\bar{\mathbf{P}}_k^{a-1} + \mathbf{H}_k^{aT} \mathbf{V}_k^{-1} \mathbf{H}_k^a)^{-1} \quad (11)$$

where  $\bar{\mathbf{P}}_k$  is the prior information on state estimate error covariance at time  $k$  and computed as

$$\bar{\mathbf{P}}_k^a = \Phi^a \bar{\mathbf{P}}_{k-1}^a \Phi^{aT} + \Gamma_w^a \mathbf{W}_{k-1} \Gamma_w^{aT} \quad (12)$$

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 [4]. The error associated with the altitude is related to  $\boldsymbol{\varepsilon}_k$  in (8) as

$$\boldsymbol{\varepsilon}_k = \mathbf{T}_v \boldsymbol{\varepsilon}_k \quad (13)$$

where  $\mathbf{T}_v$  extracts the row in  $\boldsymbol{\varepsilon}$  corresponding to altitude.

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 INS is the source of redundancy in RAIM. 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

that has smaller faults at the beginning, but increases over time. The worst case fault profile is one that is injected slowly into the GNSS measurements, thereby corrupting INS calibration without being detected.

Integrity risk is a metric to evaluate the performance of the RAIM monitor and is defined as the probability that the position error  $\varepsilon$  exceeds an alert limit  $l$  without being detected (i.e.  $q < T^2$ ). It has been shown in [2] that  $\varepsilon$  and  $q$  are statistically independent. Therefore, integrity risk  $I_r$  can be written as a multiplication of two probabilities as

$$I_r = P\{|\varepsilon| > l\} P\{q < T^2\} \quad (14)$$

The worst case fault vector that maximizes the integrity risk was derived in [1] based on batch estimator. In a batch estimator, we assume a batch measurement model

$$\mathbf{z}_b = \mathbf{H}_b \mathbf{x}_b + \boldsymbol{\nu}_b + \mathbf{f}_b \quad (15)$$

where  $\mathbf{x}_b = [x_1, x_2, \dots]^T$ ,  $\mathbf{z}_b = [z_1, z_2, \dots]^T$  and  $\mathbf{H}_b$  is the overall observation matrix of the actual system containing the INS and GNSS information. Similarly,  $\boldsymbol{\nu}_b$  is the noise vector including both GNSS and IMU process noise. Note that the subscript  $b$  is used to refer to the batch form. Details of the batch formulation was given in the previous work [3].

Based on the batch model in (15), the worst case fault vector that maximizes the integrity risk was derived in [1] as

$$\mathbf{f}_{w_b} = \alpha \mathbf{A} \mathbf{M}_A \mathbf{M}_A^T \mathbf{M}_X^T \quad (16)$$

where  $\mathbf{M}_A$ ,  $\mathbf{M}_X$  and  $\mathbf{A}$  are defined and analytically optimized as a function of  $\mathbf{H}_b$  and  $\mathbf{V}_b$ .  $\alpha$  is a scalar that is determined through iteration to maximize  $I_r$ . The fault vector in (16) represents the most dangerous fault profile that a spoofer can inject into the GNSS measurements which is a threat for aviation users. In this work, although Kalman filter is used in the monitor performance evaluation, we use the worst-case fault  $\mathbf{f}_w$  derived based on batch estimator. In the future, we will extend the derivation of the worst-case fault for the Kalman filter estimator.

As discussed in the introduction, autopilot response to spoofing may assist the detection of the fault. To evaluate RAIM performance, we will first need to introduce the aircraft dynamics with an autopilot in a feedback loop and obtain the aircraft controller's response to spoofing, then integrate it with a Kalman filter-based estimator using tightly-coupled INS-GNSS integration.

### III. RAIM PERFORMANCE EVALUATION MODEL

In this section, we derive a closed loop performance evaluation model by integrating the aircraft controller dynamics with a tightly coupled INS-GNSS mechanism. Afterwards, we derive a methodology to evaluate the performance of the RAIM in terms of integrity risk by utilizing this closed loop model.

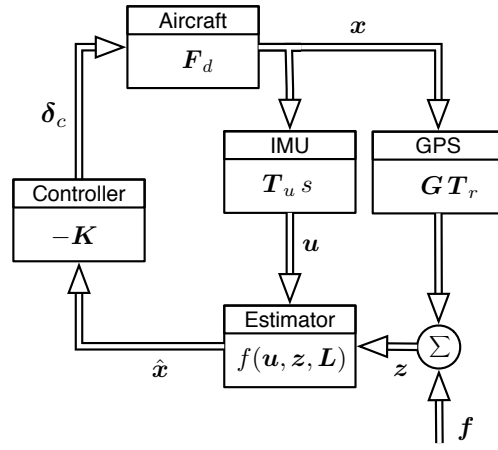


Fig. 1. Feedback Control System with a Tightly Coupled INS-GNSS Estimator and Altitude Hold Autopilot

#### A. Estimator and Controller Mechanization for Altitude Hold

To capture the effect of autopilot on tracking the final approach glideslope, we augment 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 that will be measured by the IMU. To quantify the impact of the aircraft's autopilot response on RAIM spoofing monitor performance, we utilize a closed loop compensation model including a control feedback obtained from a Kalman filter-based estimator.

The block diagram in Fig. 1 illustrates a closed-loop control system with a tightly-coupled INS-GNSS estimator. In this block diagram, true aircraft (A/C) state  $\mathbf{x}$  is fed to IMU and GNSS sensors which generate measurements for state estimation. Note that the fault  $\mathbf{f}$  is also added to the system through the GNSS measurements. Using the output  $\hat{\mathbf{x}}$  of the estimator, altitude-hold autopilot produces a control input  $\delta_c$  (elevator and thrust) resulting in maneuver commands to the aircraft.

In this section, we construct a combined estimator-controller mechanization equation. To capture aircraft's response in this closed loop mechanism, we use an aircraft dynamic model, state-space representation of which is given in Appendix B as

$$\dot{\mathbf{x}}_d = \mathbf{F}_d \mathbf{x}_d + \mathbf{G}_\delta \delta_c \quad (17)$$

where  $\mathbf{x}_d = [\delta u, \delta w, \delta q, \delta \theta, \delta h]^T$  is aircraft state containing deviation in forward speed  $u$ , down speed  $w$ , pitch rate  $q$ , pitch angle  $\theta$ , and altitude  $h$ .  $\mathbf{F}_d$  is the plant matrix,  $\mathbf{G}_\delta$  is input coefficient matrix, and  $\delta_c$  is the control input containing elevator deflection and thrust change, and it is generated based on INS state estimate feedback  $\hat{\mathbf{x}}_n$  as

$$\delta_c = -\mathbf{K} \hat{\mathbf{x}}_n \quad (18)$$

where  $\mathbf{K}$  is the autopilot gain matrix.

On the other hand, the estimator in INS utilizes a kinematic model to predict aircraft motion, which is defined in

Appendix C as

$$\dot{\mathbf{x}}_n = \mathbf{F}_n \mathbf{x}_n + \mathbf{G}_u \mathbf{u} \quad (19)$$

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

All the states except  $\delta q$  in the aircraft state vector  $\mathbf{x}_d$  can be extracted from the INS state vector  $\mathbf{x}_n$  by using proper row eliminations and navigation-to-body frame transformations. Before we define a transformation between them, for analysis purposes, we augment  $\delta q$  into  $\mathbf{x}_n$  to account for angular rate information which  $\mathbf{x}_d$  includes but  $\mathbf{x}_n$  does not. The modified INS state  $\mathbf{x}'_n$  becomes

$$\mathbf{x}'_n = \begin{bmatrix} \mathbf{x}_n \\ \delta q \end{bmatrix} \quad (20)$$

Now, we can define a direct conversion between  $\mathbf{x}_d$  and  $\mathbf{x}'_n$  as

$$\mathbf{x}_d = \mathbf{T}_x \mathbf{x}'_n \quad (21)$$

where  $\mathbf{T}_x$  extracts aircraft states  $\mathbf{x}_d$  from augmented INS states  $\mathbf{x}'_n$  by applying a combination of rotation from navigation to stability frame and row elimination.

Pitch rate dynamics is extracted from the aircraft model in (17) as

$$\dot{q} = \mathbf{T}_q (\mathbf{F}_d \mathbf{x}_d + \mathbf{G}_\delta \delta_c) \quad (22)$$

where  $\mathbf{T}_q$  extracts the row corresponding to pitch rate  $q$  in the aircraft model.

To account for the pitch rate dynamics in the INS mechanization, we augment (22) into INS model in (19) as

$$\begin{bmatrix} \dot{\mathbf{x}}_n \\ \delta \dot{q} \end{bmatrix} = \begin{bmatrix} \mathbf{F}'_n & 0 \\ \mathbf{T}_q \mathbf{F}_d \mathbf{T}_x & 0 \end{bmatrix} \begin{bmatrix} \mathbf{x}'_n \\ \delta q \end{bmatrix} + \begin{bmatrix} \mathbf{G}'_u \\ 0 \end{bmatrix} \mathbf{u} + \begin{bmatrix} 0 \\ \mathbf{T}_q \mathbf{G}_\delta \end{bmatrix} \delta_c \quad (23)$$

where  $\mathbf{F}'_n$  and  $\mathbf{G}'_u$  are the plant and input coefficient matrix of modified INS kinematic model, respectively. Since the aircraft sensors do not provide angular acceleration information ( $\delta \dot{q}$ ), there is a side process in the INS system that differentiates angular velocity information provided by IMU. This is the reason that we have the second row in (23).

Recall that the main aim of introducing an INS kinematic model in (19) and an aircraft dynamic model in (17) is to construct a mechanization equation for the state feedback control system by defining the coupling between these two models. This coupling could be attained through the specific force and angular velocity measurements captured in input vector  $\mathbf{u}$  in (19).  $\mathbf{u}$  can be defined as a combination of

variations due to the aircraft controller's response to spoofing and IMU sensor errors as

$$\mathbf{u} = \mathbf{T}_u \dot{\mathbf{x}}_d + \mathbf{b} + \boldsymbol{\nu}_n \quad (24)$$

where  $\mathbf{T}_u$  extracts specific force and angular velocity terms from aircraft state derivative and converts them to body frame.  $\boldsymbol{\nu}_n$  is a  $6 \times 1$  vector including accelerometer and gyroscope white noises, which are uncorrelated and zero-mean and  $\mathbf{b}$  is a  $6 \times 1$  IMU bias vector that is modeled as a first order Gauss Markov process as

$$\dot{\mathbf{b}} = -\boldsymbol{\tau}^{-1} \mathbf{b} + \boldsymbol{\eta}_b \quad (25)$$

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

Using (17), (18), (21) and (24), the modified INS kinematic model in (23), can be reformulated in terms of only the modified INS state  $\mathbf{x}'_n$ , its estimate  $\hat{\mathbf{x}}'_n$ , and sensor errors as

$$\dot{\mathbf{x}}'_n = (\mathbf{F}'_n + \mathbf{G}'_u \mathbf{T}_u \mathbf{F}_d \mathbf{T}_x) \mathbf{x}'_n - (\mathbf{G}'_u \mathbf{T}_u \mathbf{G}_\delta \mathbf{K} + \mathbf{G}'_\delta \mathbf{K}) \hat{\mathbf{x}}'_n + \mathbf{G}'_u \mathbf{b} + \mathbf{G}'_u \boldsymbol{\nu}_n \quad (26)$$

Augmenting the bias dynamics in (25) with the modified INS model in (26) yields a mechanization equation for actual closed loop control system of the aircraft as

$$\begin{bmatrix} \dot{\mathbf{x}}'_n \\ \dot{\mathbf{b}} \end{bmatrix} = \underbrace{\begin{bmatrix} \mathbf{F}'_n + \mathbf{G}'_u \mathbf{T}_u \mathbf{F}_d \mathbf{T}_x & \mathbf{G}'_u \\ 0 & -\boldsymbol{\tau}^{-1} \end{bmatrix}}_{\mathbf{F}} \underbrace{\begin{bmatrix} \mathbf{x}'_n \\ \mathbf{b} \end{bmatrix}}_{\mathbf{x}} - \underbrace{\begin{bmatrix} \mathbf{G}'_u \mathbf{T}_u \mathbf{G}_\delta \mathbf{K} + \mathbf{G}'_\delta \mathbf{K} & 0 \\ 0 & 0 \end{bmatrix}}_{\mathbf{G}_c} \underbrace{\begin{bmatrix} \hat{\mathbf{x}}'_n \\ \hat{\mathbf{b}} \end{bmatrix}}_{\hat{\mathbf{x}}} + \underbrace{\begin{bmatrix} \mathbf{G}'_u & 0 \\ 0 & \mathbf{I} \end{bmatrix}}_{\mathbf{G}_w} \underbrace{\begin{bmatrix} \boldsymbol{\nu}_n \\ \boldsymbol{\eta}_b \end{bmatrix}}_{\mathbf{w}} \quad (27)$$

where  $\mathbf{x}$  and  $\hat{\mathbf{x}}$  are the bias augmented INS state and state estimate vectors, respectively.  $\mathbf{F}$ ,  $\mathbf{G}_c$ , and  $\mathbf{G}_w$  are the dynamic, control input coefficient, and noise coefficient matrices of augmented closed loop system, respectively.

Discrete form of the closed loop model in (27) is expressed as

$$\mathbf{x}_{k+1} = \boldsymbol{\Phi} \mathbf{x}_k - \boldsymbol{\Gamma} \hat{\mathbf{x}}_k + \boldsymbol{\Gamma}_w \mathbf{w}_k \quad (28)$$

where  $\boldsymbol{\Phi}$  is the state transition matrix of the overall closed loop system.  $\boldsymbol{\Gamma}$  and  $\boldsymbol{\Gamma}_w$  are discrete forms of  $\mathbf{G}_c$  and  $\mathbf{G}_w$ , respectively. For analysis purpose, we assume that INS and control actuation system have the same sampling rates in discretization. So far, we obtained an overall closed loop dynamic model in (28). Fusing this model with the measurement model in Kalman filter will be introduced in the next section.

## B. Tightly Coupled INS-GNSS Integration

To perform a covariance analysis for performance evaluation of the RAIM monitor under GNSS spoofing attacks, GNSS measurement model should be first integrated with the closed loop dynamic model.

Since the main focus of this work is to detect spoofing during landing phase of the flight, we assumed a DD GNSS measurements. The faulted GNSS code and carrier phase measurement equation linearized about a nominal position (Appendix D), can be represented for the  $k^{th}$  time epoch as

$$\mathbf{z}_k = \mathbf{G}^* \delta \mathbf{r}_k + \mathbf{D} \mathbf{N} + \boldsymbol{\nu}_{\rho\phi_k} + \mathbf{f}_k \quad (29)$$

where  $\mathbf{z}$  is the measurement vector containing carrier and code phase measurements after subtracting the nominal,  $\mathbf{G}^*$  is the observation matrix including line-of-sight information from the reference station to the satellites in the navigation frame.  $\delta \mathbf{r}$  is the variation on the position of the aircraft relative to reference station represented in navigation frame.  $\mathbf{N}$  and  $\mathbf{D}$  are the cycle ambiguity state vector and its constant coefficient matrix, respectively and  $\boldsymbol{\nu}_{\rho\phi}$  is the DD carrier and code measurement error vector.  $\mathbf{f}_k$  is the resultant fault vector.

By using GNSS-aided INS navigation system, INS error drift is bounded, which allows INS to be used as a consistency check against GNSS spoofing attacks. In tightly coupled mechanism, raw INS and GNSS data are processed in a unified filter [10]. In the tightly coupled integration, coupling between dynamic model and GNSS measurement model can be obtained by first relating the state vector  $\delta \mathbf{r}$  in GNSS measurement model in (29) to the state vector  $\mathbf{x}$  used in the closed loop dynamic model in (28) as

$$\mathbf{x} = \begin{bmatrix} \delta \mathbf{r} \\ \mathbf{x}' \end{bmatrix} \quad (30)$$

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

Using the relation in (30) and augmenting cycle ambiguity state into  $\mathbf{x}$ , measurement equation in (29) can be reformulated as

$$\mathbf{z}_k = \underbrace{\begin{bmatrix} \mathbf{G}_k^* & 0 & \mathbf{D} \end{bmatrix}}_{\mathbf{H}_k} \underbrace{\begin{bmatrix} \delta \mathbf{r}_k \\ \mathbf{x}'_k \\ \mathbf{N} \end{bmatrix}}_{\mathbf{x}_k^N} + \boldsymbol{\nu}_{\rho\phi_k} + \mathbf{f}_k \quad (31)$$

where  $\mathbf{H}$  and  $\mathbf{x}^N$  are the observation matrix and the state vector of the augmented measurement model, respectively. It should be noted that, although the augmentation of multipath states in (31) is not shown for the sake of simplicity in equations, we take multi path states into account in the implementation, results of which is demonstrated in Section IV.

In the existence of the worst-case spoofing attack, measurement  $\mathbf{z}$  received by the aircraft at time epoch  $k$  can be defined as a function of worst-case fault as

$$\mathbf{z}_k = \mathbf{f}_{w_k} + \boldsymbol{\nu}_{\rho\phi_k} \quad (32)$$

where  $\mathbf{f}_w$  is the worst-case fault vector that the spoofer computes. It should be mentioned that  $\mathbf{H}_k \mathbf{x}_k^N$  term disappears in (32) since the spoofer assumes a nominal flight – zero deviation from nominal trajectory  $\mathbf{x}_k^N = 0$ .

In order for (31) to equal to (32), the relation between resultant fault  $\mathbf{f}_k$  and worst-case fault  $\mathbf{f}_{w_k}$  injected by the

spoofer must be

$$\mathbf{f}_k = \mathbf{f}_{w_k} - \mathbf{H}_k \mathbf{x}_k^N \quad (33)$$

The difference between the worst-case fault that spoofer assumes, and the resultant fault vector shown in (33) will have an impact on detector, which will be explained in Section III-C in detail.

To be consistent with the measurement model in (31), the cycle ambiguity state must also be augmented into the dynamic model in (28) as

$$\begin{bmatrix} \mathbf{x}_{k+1} \\ \mathbf{N}_{k+1} \end{bmatrix} = \underbrace{\begin{bmatrix} \Phi & 0 \\ 0 & \mathbf{I} \end{bmatrix}}_{\Phi^N} \underbrace{\begin{bmatrix} \mathbf{x}_k \\ \mathbf{N}_k \end{bmatrix}}_{\mathbf{x}_k^N} - \underbrace{\begin{bmatrix} \Gamma & 0 \\ 0 & 0 \end{bmatrix}}_{\Gamma^N} \underbrace{\begin{bmatrix} \hat{\mathbf{x}}_k \\ \hat{\mathbf{N}}_k \end{bmatrix}}_{\hat{\mathbf{x}}_k^N} + \underbrace{\begin{bmatrix} \Gamma_w \\ 0 \end{bmatrix}}_{\Gamma_w^N} \mathbf{w}_k \quad (34)$$

where  $\Phi^N$  and  $\Gamma^N$  are the state transition and state estimate coefficient matrices of the augmented closed loop dynamic system. Superscript N implies cycle ambiguity augmentation.

So far, we derived an augmented measurement model in (31) with a closed loop dynamic model in (34) and their short forms can be written as

$$\mathbf{z}_k = \mathbf{H}_k \mathbf{x}_k^N + \boldsymbol{\nu}_{\rho\phi_k} + \mathbf{f}_k \quad (35)$$

$$\mathbf{x}_{k+1}^N = \Phi^N \mathbf{x}_k^N - \Gamma^N \hat{\mathbf{x}}_k^N + \Gamma_w^N \mathbf{w}_k \quad (36)$$

A Kalman filter based on equations (35) and (36), has a time update as

$$\bar{\mathbf{x}}_{k+1}^N = \underbrace{(\Phi^N - \Gamma^N)}_{\Upsilon} \hat{\mathbf{x}}_k^N \quad (37)$$

where  $\bar{\mathbf{x}}_{k+1}^N$  is the a priori estimate of  $\mathbf{x}^N$  at time epoch  $k + 1$ .  $\Upsilon$  is defined for simplicity, which is a function of state transition matrix and the state estimate coefficient matrix of closed loop dynamics.

Measurement update at time epoch  $k + 1$  gives the a posteriori estimate  $\hat{\mathbf{x}}_{k+1}^N$  as

$$\hat{\mathbf{x}}_{k+1}^N = \bar{\mathbf{x}}_{k+1}^N + \mathbf{L}_{k+1} (\mathbf{z}_{k+1} - \mathbf{H}_{k+1} \bar{\mathbf{x}}_{k+1}^N) \quad (38)$$

where  $\mathbf{L}_{k+1}$  is the Kalman gain at time epoch  $k + 1$ , and optimally computed as in (10). The only difference between  $\mathbf{L}$  in (38) and that in (10) is that the one in (38) has extra zero due to the augmentation of the pitch rate state  $\delta q$ . However, this does not affect the estimator.

Substituting (32) into (38) gives

$$\hat{\mathbf{x}}_{k+1}^N = (\mathbf{I} - \mathbf{L}_{k+1} \mathbf{H}_{k+1}) \bar{\mathbf{x}}_{k+1}^N + \mathbf{L}_{k+1} (\mathbf{f}_{w_{k+1}} + \boldsymbol{\nu}_{\rho\phi_{k+1}}) \quad (39)$$

Substituting time update equation (37) into measurement update equation (39) results in

$$\hat{\mathbf{x}}_{k+1}^N = (\mathbf{I} - \mathbf{L}_{k+1} \mathbf{H}_{k+1}) \Upsilon \hat{\mathbf{x}}_k^N + \mathbf{L}_{k+1} (\mathbf{f}_{w_{k+1}} + \boldsymbol{\nu}_{\rho\phi_{k+1}}) \quad (40)$$

Subtracting (36) from (40) and defining the state estimate error  $\tilde{\mathbf{x}}_k^N$  as  $\hat{\mathbf{x}}_k^N - \mathbf{x}_k^N$  gives the state estimate error dynamics as

$$\begin{aligned} \tilde{\mathbf{x}}_{k+1}^N = & (\Phi^N - \mathbf{L}_{k+1} \mathbf{H}_{k+1} \Upsilon) \tilde{\mathbf{x}}_k^N - \mathbf{L}_{k+1} \mathbf{H}_{k+1} \Upsilon \mathbf{x}_k^N \\ & + \mathbf{L}_{k+1} (\mathbf{f}_{w_{k+1}} + \nu_{\rho\phi_{k+1}}) - \Gamma_w^N \mathbf{w}_k \end{aligned} \quad (41)$$

Dynamic model in (36) can also be written in terms of only the true state  $\mathbf{x}$  and the state estimate error  $\tilde{\mathbf{x}}$  by using the relation  $\hat{\mathbf{x}} = \mathbf{x} + \tilde{\mathbf{x}}$  as

$$\mathbf{x}_{k+1}^N = \Upsilon \mathbf{x}_k^N - \Gamma^N \tilde{\mathbf{x}}_k^N + \Gamma_w^N \mathbf{w}_k \quad (42)$$

Combining (42) with the estimator error dynamics in (41), we obtain two coupled equations that describe the overall dynamic behavior of the system as

$$\begin{aligned} \begin{bmatrix} \mathbf{x}_k^N \\ \tilde{\mathbf{x}}_k^N \end{bmatrix} = & \begin{bmatrix} \Upsilon & -\Gamma^N \\ -\mathbf{L}_k \mathbf{H}_k \Upsilon & \Phi^N - \mathbf{L}_k \mathbf{H}_k \Upsilon \end{bmatrix} \begin{bmatrix} \mathbf{x}_{k-1}^N \\ \tilde{\mathbf{x}}_{k-1}^N \end{bmatrix} \\ & + \begin{bmatrix} \Gamma_w^N & 0 \\ -\Gamma_w^N & \mathbf{L}_k \end{bmatrix} \begin{bmatrix} \mathbf{w}_{k-1} \\ \nu_{\rho\phi_k} \end{bmatrix} + \begin{bmatrix} 0 \\ \mathbf{L}_k \end{bmatrix} \mathbf{f}_{w_k} \end{aligned} \quad (43)$$

Although state estimate error is not a function of true state in most of the applications [14], it can be seen that there is two-way coupling between the state  $\mathbf{x}_k^N$  and its estimate error  $\tilde{\mathbf{x}}_k^N$  in (43). The reason is that the resultant fault in the system is a function of actual state as in (33).

Using (43), we aim to obtain the time history of the true state  $\mathbf{x}^N$  which represents the deviations from nominal trajectory due to autopilot's response to the fault in the GNSS measurements. In the closed loop dynamics given in (28), since the current state is a function of previous state estimate which is a random variable, true state will also be a random variable.

Let us define

$$\mathbf{X}_k = \mathbb{E}\{\mathbf{x}_k^N \mathbf{x}_k^{N^T}\} \quad (44)$$

$$\hat{\mathbf{P}}_k = \mathbb{E}\{\tilde{\mathbf{x}}_k^N \tilde{\mathbf{x}}_k^{N^T}\} \quad (45)$$

where  $\mathbf{X}_k$  and  $\hat{\mathbf{P}}_k$  are true state covariance and state estimate error covariance at time epoch  $k$ , respectively such that  $\mathbf{x}_k^N \sim \mathcal{N}(\hat{\mathbf{x}}_k^N, \hat{\mathbf{P}}_k)$ .

### C. RAIM Formulation for Fault Detection Performance

In this section, we formulate the monitor in terms of the estimator derived for evaluation purpose in the previous section, and derive the integrity risk equations to quantify the monitor performance.

Fig. 2 explains the impact of the autopilot response on the aircraft trajectory under spoofing attack. The black dotted line in Fig. 2 is the nominal or planned trajectory. The blue line represents the spoofing trajectory and  $\delta r_f$  refers to position discrepancy from the nominal due to fault. The black curved trajectory is the actual flight path deviated from the nominal trajectory due to autopilot's response to spoofing attack. This

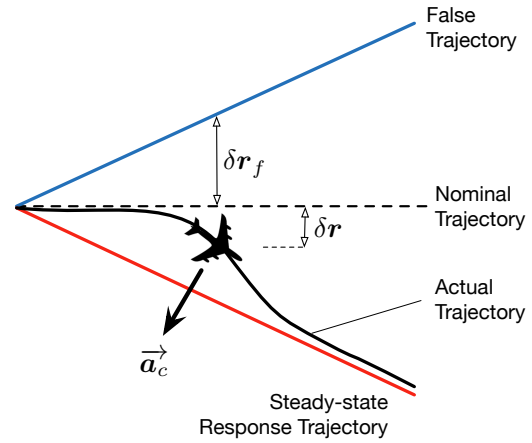


Fig. 2. Impact of the Position Fault and the Consequent Autopilot Response to Spoofing Attack on Aircraft's Trajectory

deviation is denoted by  $\delta r$ . The red trajectory is the steady-state trajectory the aircraft will maneuver and reach to after responding to the spoofed signal. Knowing the nominal path of the aircraft, a smart spoofer may inject the worst-case fault leading to a hazardous situation without being detected by the aircraft monitor [1]. On the other hand, in the existence of autopilot – and assuming the spoofer cannot predict the response of the autopilot – the resultant fault in the system will be different than the worst-case fault assumed by the spoofer. This increases the detectability of the fault since the actual fault is not the worst case fault anymore, which has a direct impact in the residual.

In this work, we assume a worst-case fault  $\mathbf{f}_w$  derived based on a batch estimator, which maximizes integrity risk [1]. In the future work, we will derive worst-case fault based on Kalman filter estimator. Remember that the worst-case fault is computed using nominal trajectory values since it is assumed that the spoofer have knowledge of the nominal trajectory only.

Based on (3) and (43), the innovation vector  $\gamma_k$  is

$$\gamma_k = z_k - \mathbf{H}_k \bar{\mathbf{x}}_k^N \quad (46)$$

Substituting (32) into (46) results in

$$\gamma_k = \mathbf{f}_{w_k} + \nu_{\rho\phi_k} - \mathbf{H}_k \bar{\mathbf{x}}_k^N \quad (47)$$

Using (36) and (37), the innovation vector in (47) can be expressed in terms of true state  $\mathbf{x}_{k-1}$  and state estimate error  $\tilde{\mathbf{x}}_{k-1}$  as

$$\gamma_k = \mathbf{f}_{w_k} + \nu_{\rho\phi_k} - \mathbf{H}_k (\mathbf{x}_k^N + \Phi^N \tilde{\mathbf{x}}_{k-1}^N - \Gamma_w^N \mathbf{w}_{k-1}) \quad (48)$$

The new formulation of the innovation vector in (48) captures the autopilot's response to spoofing attack. Therefore, we can quantify the effect of the controller on the detection capability of RAIM. In order to capture the correlation between  $\gamma_k$  and  $\tilde{\mathbf{x}}_k$ , we augment (48) into (43), which results in a complete model containing system dynamics and innovation

as

$$\begin{aligned}
\begin{bmatrix} \mathbf{x}_k^N \\ \tilde{\mathbf{x}}_k^N \\ \gamma_k \end{bmatrix} &= \underbrace{\begin{bmatrix} \mathbf{\Upsilon} & -\mathbf{\Gamma}^N & 0 \\ -\mathbf{L}_k \mathbf{H}_k \mathbf{\Upsilon} & \mathbf{\Phi}^N - \mathbf{L}_k \mathbf{H}_k \mathbf{\Upsilon} & 0 \\ -\mathbf{H}_k \mathbf{\Upsilon} & -\mathbf{H}_k \mathbf{\Upsilon} & 0 \end{bmatrix}}_{\mathbf{\Phi}_{y_k}} \underbrace{\begin{bmatrix} \mathbf{x}_{k-1}^N \\ \tilde{\mathbf{x}}_{k-1}^N \\ \gamma_{k-1} \end{bmatrix}}_{\mathbf{y}_{k-1}} \\
&+ \underbrace{\begin{bmatrix} \mathbf{\Gamma}_w^N & 0 \\ -\mathbf{\Gamma}_w^N & \mathbf{L}_k \\ 0 & \mathbf{I} \end{bmatrix}}_{\mathbf{\Gamma}_{y_k}} \underbrace{\begin{bmatrix} \mathbf{w}_{k-1} \\ \nu_{\rho\phi_k} \end{bmatrix}}_{\mathbf{v}_{y_k}} + \underbrace{\begin{bmatrix} 0 \\ \mathbf{L}_k \\ \mathbf{I} \end{bmatrix}}_{\mathbf{\Gamma}_{f_k}} \mathbf{f}_{w_k}
\end{aligned} \quad (49)$$

where  $\mathbf{y}$  is defined as the state vector of the complete model including true state, state estimate error, and innovation.  $\mathbf{\Phi}_y$ ,  $\mathbf{\Gamma}_y$ , and  $\mathbf{\Gamma}_f$  are the state transition, noise coefficient, and fault input coefficient matrices of the complete system, respectively. Using (49), the mean and covariance of the complete model state  $\mathbf{y}$  can be propagated as

$$\boldsymbol{\mu}_{y_k} = \mathbf{\Phi}_{y_k} \boldsymbol{\mu}_{y_{k-1}} + \mathbf{\Gamma}_{f_k} \mathbf{f}_{w_k} \quad (50)$$

$$\mathbf{Y}_k = \mathbf{\Phi}_{y_k} \mathbf{Y}_{k-1} \mathbf{\Phi}_{y_k}^T + \mathbf{\Gamma}_{y_k} \mathbf{V}_{y_k} \mathbf{\Gamma}_{y_k}^T \quad (51)$$

where  $\boldsymbol{\mu}_{y_k}$  and  $\mathbf{Y}_k$  are the mean and covariance of  $\mathbf{y}_k$ , respectively, and  $\mathbf{V}_{y_k}$  is the covariance of  $\mathbf{v}_{y_k}$ .

In Kalman Filter innovation-based RAIM, it was proven that the test statistics obtained from the weighted norm of the innovation using (5) and state estimate error are independent [2]. Therefore, the integrity risk is obtained as a product of the two probabilities as in (14). However, in our case, since the fault is fed into the aircraft by autopilot controller input through a closed-loop mechanism, the state estimate error  $\tilde{\mathbf{x}}_k$  and test statistic  $q_k$  are no longer independent. Computing the integrity risk with correlated gaussian distribution  $\tilde{\mathbf{x}}_k$  and chi-square distribution  $q_k$  is difficult. Therefore, we compute a bound on the integrity risk by first whitening the innovation by its covariance matrix as

$$\bar{\gamma}_k = \mathbf{S}_k^{-1/2} \gamma_k \quad (52)$$

where  $\bar{\gamma}_k$  is the whitened innovation vector which is a Gaussian and identically distributed in  $n$ -space (i.e.  $\mathbb{E}\{\bar{\gamma}_k \bar{\gamma}_k^T\} = \mathbf{I}_{n \times n}$ ) and  $\mathbf{S}_k$  is the innovation covariance obtained from  $\mathbf{Y}$  in (51) as

$$\mathbf{S}_k = \mathbf{T}_\gamma \mathbf{Y}_k \mathbf{T}_\gamma^T \quad (53)$$

where  $\mathbf{T}_\gamma$  and  $\mathbf{T}_{\tilde{\mathbf{x}}}$  extracts the rows of  $\mathbf{y}_k$  corresponding to  $\gamma_k$  and  $\tilde{\mathbf{x}}_k^N$ , respectively.

Re-expressing the test statistic in (5) in terms of  $\bar{\gamma}_k$  gives

$$q_k = \sum_{n=1}^k \bar{\gamma}_n^T \bar{\gamma}_n \quad (54)$$

Defining a cumulative innovation vector  $\bar{\gamma}_{1|k} = [\bar{\gamma}_1, \bar{\gamma}_2, \dots, \bar{\gamma}_k]^T$  containing all whitened innovation vectors

from time epoch 1 to  $k$ , the test statistic can be written in terms of 2-norm of  $\bar{\gamma}_{1|k}$

$$q_k = \|\bar{\gamma}_{1|k}\|_2 \quad (55)$$

where  $\bar{\gamma}_{1|k}$  is a Gaussian and identically distributed in  $n \times k$  space.  $n$  is the number of measurements at each time epoch.

Substituting (55) into (6), the detection test can be re-expressed as

$$\|\bar{\gamma}_{1|k}\|_2 < T^2 \quad (56)$$

The detection test condition in (56) represents a hypersphere which is conservatively over-bounded by a hyperbox as

$$|\bar{\gamma}_{1|k}| < T \quad (57)$$

Since  $\bar{\gamma}_{1|k}$  is equally distributed in all dimensions, each element of  $\bar{\gamma}_{1|k}$  should be less than threshold  $T$ .

Vertical estimate error  $\varepsilon$  is extracted from the state estimate error  $\tilde{\mathbf{x}}^N$  as

$$\varepsilon_k = \mathbf{T}_v \tilde{\mathbf{x}}_k^N \quad (58)$$

where  $\mathbf{T}_v$  extracts the row in  $\tilde{\mathbf{x}}^N$  corresponding to altitude.

To compute the integrity risk, we combine the cumulative innovation vector and the current altitude estimate error and obtain a multi-dimensional Gaussian distribution as

$$[\bar{\gamma}_{1|k-1} \mid \bar{\gamma}_k \mid \varepsilon_k]^T \sim \mathcal{N}(\boldsymbol{\mu}_k, \boldsymbol{\Sigma}_k) \quad (59)$$

Using the transformation matrices  $\mathbf{T}_\gamma$ ,  $\mathbf{T}_{\tilde{\mathbf{x}}}$ , and  $\mathbf{T}_v$ , the mean  $\boldsymbol{\mu}_k$  can be expressed in terms of  $\boldsymbol{\mu}_{y_k}$  in (50) as

$$\boldsymbol{\mu}_k = \begin{bmatrix} \mathbf{S}_1^{-1/2} \mathbf{T}_\gamma \boldsymbol{\mu}_{y_1} \\ \vdots \\ \mathbf{S}_{k-1}^{-1/2} \mathbf{T}_\gamma \boldsymbol{\mu}_{y_{k-1}} \\ \hline \mathbf{S}_k^{-1/2} \mathbf{T}_\gamma \boldsymbol{\mu}_{y_k} \\ \hline \mathbf{T}_v \mathbf{T}_{\tilde{\mathbf{x}}} \boldsymbol{\mu}_{y_k} \end{bmatrix} \quad (60)$$

and the covariance  $\boldsymbol{\Sigma}_k$  is obtained in terms of  $\mathbf{Y}_k$  in (51) as

$$\boldsymbol{\Sigma}_k = \begin{bmatrix} \mathbf{I} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{I} & \mathbf{S}_k^{-1/2} \mathbf{T}_\gamma \mathbf{Y}_k \mathbf{T}_{\tilde{\mathbf{x}}}^T \mathbf{T}_v^T \\ \mathbf{0} & \mathbf{T}_v \mathbf{T}_{\tilde{\mathbf{x}}} \mathbf{Y}_k \mathbf{T}_\gamma^T \mathbf{S}_k^{-1/2 T} & \mathbf{T}_v \mathbf{T}_{\tilde{\mathbf{x}}} \mathbf{Y}_k \mathbf{T}_{\tilde{\mathbf{x}}}^T \mathbf{T}_v^T \end{bmatrix} \quad (61)$$

The correlated terms in the covariance matrix in (61) are due to the dependency between  $\gamma_k$  and  $\tilde{\mathbf{x}}_k$ . There are zero blocks in (61) since the innovations are uncorrelated:  $\mathbb{E}\{\bar{\gamma}_i \bar{\gamma}_j^T\} = 0$  for  $i \neq j$  [15], therefore the current state estimate error is also uncorrelated with the previous innovations  $\mathbb{E}\{\bar{\gamma}_i \varepsilon_j^T\} = 0$  for  $i \neq j$ . The integrity risk at time epoch  $k$  for a given spoofing hypothesis  $H_s$  in (62), can be solved numerically using the multi-dimensional Gaussian distribution defined by (59) - (61).

$$I_{rk} = P\{|\varepsilon_k| > l, |\bar{\gamma}_{1|k}| < T \mid H_s\} \quad (62)$$

where  $l$  is the vertical alert limit, and  $T$  is the same threshold for the actual detector defined in (14).

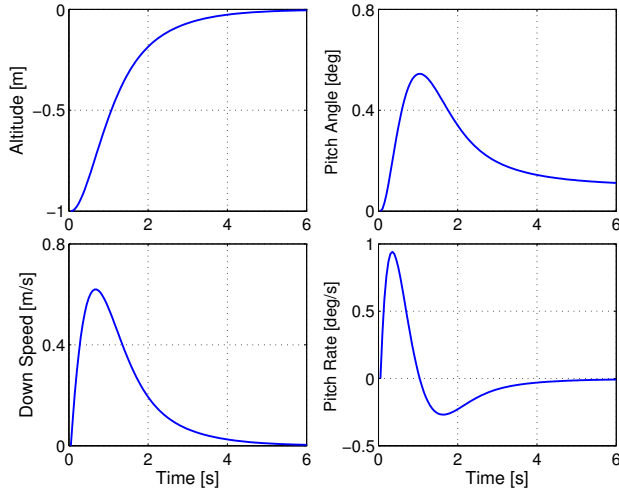


Fig. 3. The closed loop responses of the generic altitude-hold autopilot for B747 to a  $-1$  m initial perturbation on altitude.

#### IV. SIMULATION RESULTS

To quantify the impact of autopilot response on the integrity risk, we simulated several scenarios for B747 landing approach under a worst case spoofing attack. Due to limited range of the spoofer, we assumed that the spoofing attack does not exceed 150 seconds, which is the standard approach time for B747. Using (16), the worst case fault is computed based on the assumptions that the spoofer has the exact knowledge of the nominal approach trajectory, INS model, and IMU errors of the aircraft. To test the performance of the RAIM Monitor with this worst case fault, B747 aircraft is modeled with a generic altitude hold autopilot for the nominal flight conditions given in Table II, III, and IV in Appendix E.

The gain matrix for the altitude hold autopilot is obtained using the dynamic stability guidelines in MIL-F-8785C standards in [13]. Using this gain matrix, the aircraft's response to an example initial disturbance on the altitude is given in Fig. 3. As seen from the figure, the autopilot time constant is approximately 5 s., which is typical for large, heavy, low-to-medium maneuverability airplanes such as B747 [9]. To decrease the computational burden in the simulations, we assumed that the time interval for GNSS updates equals to the autopilot time constant (i.e. 0.2 Hz) since the autopilot does not practically respond to GNSS inputs at higher rates.

In this analysis, we assume that the INS states has been initialized by a Kalman Filter for few GPS epochs under fault-free nominal flight prior to the GNSS spoofing attack. The INS and GNSS error models used in the simulation can be found in Table IV in Appendix E.

The spoofer computes a worst case fault profile over time such that it minimizes the probability of detection and maximizes the probability of error exceeding an alert limit of 10 m. Fig. 4 illustrates the vertical state estimate error and actual vertical position deviation from the nominal altitude resulting from two different worst case spoofing attack periods

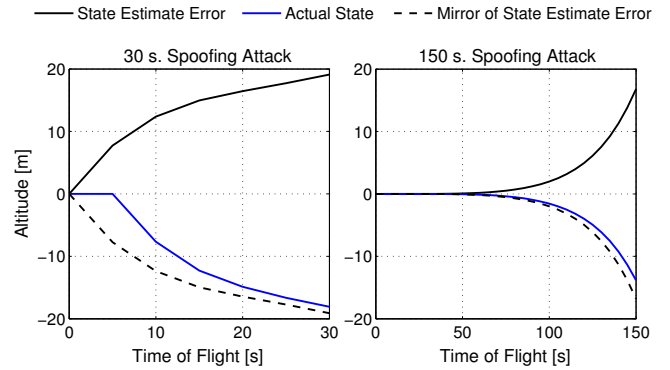


Fig. 4. The altitude estimate error and resulting altitude deviations from nominal in the existence of 2 different worst case spoofing attack periods: 30 s and 150 s. Blue curve represents the aircraft vertical position, black curve is the estimate error in the vertical position, and black dotted curve is the mirror image of the black curve with respect to nominal.

of 30 s and 150 s, respectively. In both scenarios, the spoofer results in a growth in the state estimate error (black curve), which triggers the altitude hold autopilot and causes aircraft to deviate from the nominal altitude (blue curve). Due to the deceptive position estimates, autopilot steers the aircraft to downward such that its response trajectory follows the mirror of the state estimate error curve (black dotted curve). The reason is that the autopilot generates commands such that the state estimate  $\hat{x}$  be zero, which is equivalent to  $x = -\hat{x}$ . In Fig. 4, it can also be observed that the state estimate error growth in the 150 s attack scenario is slower than that in the 30 s attack scenario. The reason is that the spoofer has more time to inject the fault that results in the same amount of hazardous information.

The impact of the maneuvers commanded by the autopilot on the spoofing monitor performance is given in terms of integrity risk in Fig. 5. We performed simulations for two different scenarios: when the autopilot is on and off. When the autopilot is off, aircraft follows its nominal trajectory without any maneuver, which results in high integrity risk of approximately 1 for most of the attack periods. The reason is that the nominal trajectory that the spoofer assumes exactly matches the actual trajectory of the aircraft since aircraft does not steer. On the other hand, the integrity risk when the autopilot is on, is significantly lower than the autopilot off case since the aircraft autopilot induces transient maneuvers as a response to the spoofing attack. For instance, a worst case spoofing attack during a 150 s standard approach, results in an integrity risk of  $3 \times 10^{-16}$  satisfying the integrity risk requirement (i.e.  $10^{-9}$ ) whereas it is almost 1 if there is no autopilot response. This is a promising result since, although we conservatively select one of the biggest aircraft which has the least maneuverability, the autopilot's response to the deceptive GNSS signal is adequate to tremendously improve the detection capability of the aircraft against worst case spoofing attacks.

As seen in Fig. 4, short attack periods cause large initial maneuver due to a large hazardous input ( $\tilde{x}$ ) injected by the

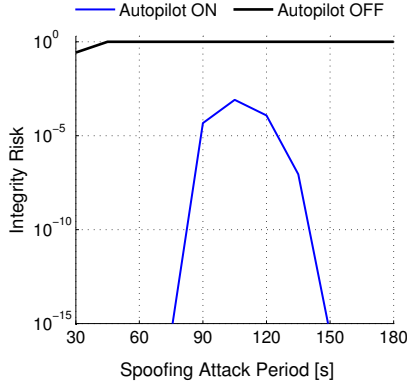


Fig. 5. The impact of the autopilot response on the integrity risk in the existence of the worst case spoofing attack with a GNSS frequency of 0.2 Hz for different spoofing attack periods. The black and blue curves represent the worst case spoofing attack when the autopilot is off and on, respectively.

spoofers at the beginning whereas long attack periods lead to a large final maneuver due to a slow but exponentially increasing hazardous input to the aircraft's autopilot. The accelerations induced by both of these maneuvers improve the detection since they are sensed by the IMU but not reflected in the spoofed GNSS measurements. The trade-off between having initial and final maneuvers results in obtaining a bell-shaped integrity risk curve as seen in Fig. 5, where both the short and long attack periods have low integrity risk. Within intermediate attack periods, there is a critical attack period of 105 s, where the integrity risk is the maximum ( $8 \times 10^{-4}$ ). However, this maximum value of the integrity risk with the autopilot is still much less than that when there is no autopilot response.

## V. CONCLUSION

In this work, we investigate the leveraging effect of the autopilot reaction to a faulted GNSS signal in the performance of the proposed RAIM-like spoofing monitor. We developed a generalized statistical approach to quantify the integrity risk of the monitor by deriving a closed-loop performance evaluation model, where the GNSS fault is fed into the autopilot through a tightly-coupled INS-GNSS Kalman filter. Utilizing a worst case fault profile computed based on the nominal approach trajectory and aircraft error models, we performed a covariance analysis to quantify the detector performance in terms of integrity risk. The results show that, for INS-RAIM-equipped aircrafts, the aircraft autopilot response to faulted GNSS signals provides a direct means for detection of the spoofing attack even in the existence of the worst-case spoofing scenarios.

## ACKNOWLEDGMENT

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

## Appendix A COORDINATE FRAMES

This appendix illustrates the coordinate frames which are used in derivation of aircraft dynamics, INS mechanization and GNSS measurement model.

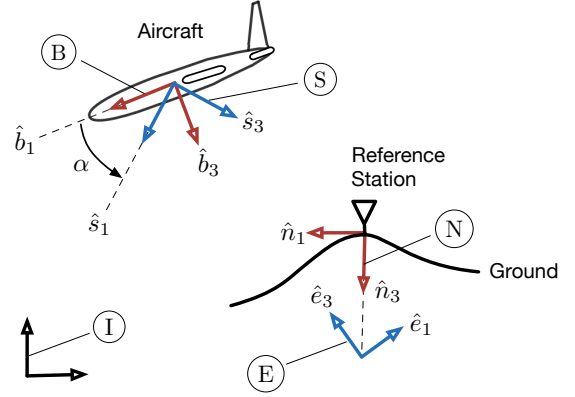


Fig. 6. Coordinate Frames

I, E, N, B, and S are inertial, earth-centered earth-fixed, navigation, aircraft body and stability frames, respectively. We assume navigation frame is fixed at a static ground reference frame which is denoted with  $r$  in Fig. 6.

## Appendix B AIRCRAFT FLIGHT DYNAMIC MODEL

This appendix is for the derivation of linearized vertical aircraft dynamics. Nonlinear aircraft longitudinal equations of motion in the form of coupled state equations are given as [9]

$$I_{22}\dot{q} - (I_{33} - I_{11})pr + I_{13}(p^2 - r^2) = M + M_T \quad (63)$$

$$m(\dot{u} + qw - rv) = -mg\sin\theta + X + X_T \quad (64)$$

$$m(\dot{w} + pv - qu) = mg\cos\theta\cos\phi + Z + Z_T \quad (65)$$

where  $u$ ,  $v$ ,  $w$  are the velocity components in body-fixed stability axes in Fig. 6,  $p$ ,  $q$ ,  $r$  are roll, pitch, and yaw rates,  $\alpha$ ,  $\beta$ ,  $\theta$  are angle of attack, side slip angle and flight path angle,  $m$  is the aircraft mass;  $I_{11}$ ,  $I_{22}$ ,  $I_{33}$  are mass moment of inertias represented in body frame;  $X_T$ ,  $Z_T$ ,  $M_T$  are forces and moment due to thrust;  $X$ ,  $Z$ ,  $M$  are aerodynamic forces and moments including drag, lift, pitch moment. The three longitudinal EOMs in (63), (64) and (65) consist of the  $x$ -force,  $z$ -force, and  $y$ -moment equations.

As we assume a perturbation from longitudinal trim flight, the nonlinear equations of motions (EOM) can be linearized by recasting each variable in terms of perturbed variables and corresponding nominal values, which are the trimmed flight conditions ( $p^* = q^* = r^* = 0$ ). Variables with the superscript  $*$  correspond to the equilibrium (trim) state. Note that only the axial velocity  $u$  and pitch angle  $\theta$  have non-zero equilibrium values. The trim values of all lateral/directional variables are zero ( $v = \phi = \beta = 0$ ) because the initial trim condition corresponds to longitudinal equilibrium; the

equilibrium value of  $w$  is zero because we use stability axes. These simplifications produce a perturbed inertial forces and moment as [9]

$$\delta F_1^i = m \delta \dot{u} \quad (66)$$

$$\delta F_3^i = m(\delta \dot{w} - u^* \delta q) \quad (67)$$

$$\delta M_2^i = I_{22} \delta \dot{q} \quad (68)$$

Neglecting the effect of change in angle of attack on aerodynamic forces and moment ( $M_{\dot{\alpha}}, Z_{\dot{\alpha}} \ll 1$ ), aerodynamic force and moment equations in variational form can be simplified as [9]

$$\delta X = m(X_u \delta u + X_\alpha \delta \alpha + X_q \delta q + X_{\delta_e} \delta_e) \quad (69)$$

$$\delta Z = m(Z_u \delta u + Z_\alpha \delta \alpha + Z_q \delta q + Z_{\delta_e} \delta_e) \quad (70)$$

$$\delta M = I_{22}(M_u \delta u + M_\alpha \delta \alpha + M_q \delta q + M_{\delta_e} \delta_e) \quad (71)$$

where the symbols X, Z, and M with subscripts indicate aerodynamic stability derivatives representing the linear or angular acceleration per motion or control variable (speed, angle of attack, pitch rate, and control deflection). Under small variations in angle of attack around zero, angle of attack can be expressed in terms of vertical body speed and total speed of the aircraft as

$$\delta \alpha = \frac{\delta w}{u^*} \quad (72)$$

Assuming a constant thrust ( $\delta X_T = \delta Z_T = \delta M_T = 0$ ) and equating inertial forces and moment in (66) to (68) to the external forces and moment in (69) to (71) respectively, yields

$$\delta \dot{u} = X_u \delta u + \frac{X_\alpha}{u^*} \delta w - g c \theta^* \delta \theta + X_{\delta_e} \delta_e \quad (73)$$

$$\delta \dot{w} = Z_u \delta u + \frac{Z_\alpha}{u^*} \delta w + (Z_q + u^*) \delta q - g s \theta^* \delta \theta + Z_{\delta_e} \delta_e \quad (74)$$

$$\delta \dot{q} = M_u \delta u + \frac{M_\alpha}{u^*} \delta w + M_q \delta q + M_{\delta_e} \delta_e \quad (75)$$

Since the autopilot controls altitude, it should be expressed in terms of other longitudinal states as

$$\delta \dot{h} = s \theta^* \delta u - c \theta^* \delta w + u^* \delta \theta \quad (76)$$

This yields a state space representation of EOM describing

longitudinal aircraft dynamics including altitude as

$$\begin{aligned} \begin{bmatrix} \delta \dot{u} \\ \delta \dot{w} \\ \delta \dot{q} \\ \delta \dot{\theta} \\ \delta \dot{h} \end{bmatrix} &= \overbrace{\begin{bmatrix} X_u & \frac{X_\alpha}{u^*} & 0 & -g c \theta^* & 0 \\ Z_u & \frac{Z_\alpha}{u^*} & Z_q + u^* & -g s \theta^* & 0 \\ M_u & \frac{M_\alpha}{u^*} & M_q & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ s \theta^* & -c \theta^* & 0 & u^* & 0 \end{bmatrix}}^{\mathbf{F}_d} \underbrace{\begin{bmatrix} \delta u \\ \delta w \\ \delta q \\ \delta \theta \\ \delta h \end{bmatrix}}_{\mathbf{x}_d} \\ &+ \underbrace{\begin{bmatrix} X_{\delta_e} & X_{\delta_T} \\ Z_{\delta_e} & Z_{\delta_T} \\ M_{\delta_e} & M_{\delta_T} \\ 0 & 0 \\ 0 & 0 \end{bmatrix}}_{\mathbf{G}_\delta} \underbrace{\begin{bmatrix} \delta_e \\ \delta_T \end{bmatrix}}_{\delta_c} \end{aligned} \quad (77)$$

where the plant matrix  $\mathbf{F}_d$  is constant plant matrix that includes terms related to trimmed flight aerodynamic coefficients, mass and inertial properties of the aircraft,  $\mathbf{x}_d$  is aircraft state vector,  $\mathbf{G}_\delta$  is input coefficient matrix, and  $\delta_c$  is control input including elevator deflection command to control altitude or pitch attitude  $\delta_e$  and thrust change command  $\delta_T$ . Note that the model in (77) includes both short and long period (phugoid) modes of the aircraft.

## Appendix C INS ERROR KINEMATICS MODEL

This appendix includes the derivations for the INS mechanization equations. Before starting linearization, the significant assumptions are listed as

- 1) Navigation frame  $N$  is fixed at the ground reference station  $r$  (Fig. 6).
- 2) Position  $\mathbf{r}$  and attitude  $\mathbf{E}$  of the aircraft in mechanization equations are with respect to position of the reference station.
- 3) Velocity of the aircraft  $\mathbf{v}$  is not the inertial velocity but the ground velocity.
- 4) Since we assume a level flight, all of the nominal values of variations are assumed to be constant in linearization.
- 5) Gravity vector error variations are not modeled in the velocity error equation since their contribution over the duration of an aircraft approach is negligibly small.

Using the assumptions above, nonlinear kinematic equations of the aircraft [10] can be obtained as

$$\dot{\mathbf{x}}_n \triangleq \begin{bmatrix} \dot{\mathbf{r}}^{(n)} \\ \dot{\mathbf{v}}^{(n)} \\ \dot{\mathbf{E}}^{(n)} \end{bmatrix} = \begin{bmatrix} \mathbf{v}^{(n)} \\ {}^N \mathbf{R}^B \mathbf{f}^{(b)} - 2\tilde{\boldsymbol{\omega}}_{ie}^{(n)} \mathbf{v}^{(n)} + \mathbf{g}^{(n)} \\ \mathbf{Q}_{BE}^{-1} \{ \boldsymbol{\omega}_{ib}^{(b)} - {}^N \mathbf{R}^E \boldsymbol{\omega}_{ie}^{(e)} \} \end{bmatrix} \quad (78)$$

where the INS state vector  $\mathbf{x}_n$  is defined in  $N$ -frame and composed of position relative to reference station  $\mathbf{r}^{(n)}$ , ground

velocity  $\mathbf{r}^{(n)}$ , and attitude (Euler angles)  $\mathbf{E}^{(n)}$ . Also,  ${}^N\mathbf{R}^B$  and  ${}^N\mathbf{R}^E$  are rotation matrices from body and earth to navigation frame respectively;  $\mathbf{Q}_{BE}$  is the matrix that transforms Euler angle rates to body rotation rates, and  $\tilde{\boldsymbol{\omega}}_{ie}$  and  $\tilde{\boldsymbol{\omega}}_{ib}$  are the skew symmetric matrices of angular velocity vectors of earth and body with respect to  $I$ -frame. Also,  $\mathbf{f}_b$  is the specific force acting on aircraft. Note that the superscripts with parentheses refer to the frame in which the vector is expressed.

Expressing all the variables in (78) in perturbation form in [10], position and velocity error equations come out as

$$\delta \dot{\mathbf{r}}^{(n)} = \delta \mathbf{v}^{(n)} \quad (79)$$

$$\delta \dot{\mathbf{v}}^{(n)} = \left[ {}^N\mathbf{R}^{B*} \tilde{\mathbf{f}}^{(b)*} \right] \delta \mathbf{E} + \left[ {}^N\mathbf{R}^{B*} \right] \delta \mathbf{f}^{(b)} + \left[ -2 \tilde{\boldsymbol{\omega}}_{ie}^{(n)} \right] \delta \mathbf{v}^{(n)} \quad (80)$$

where  $\tilde{\mathbf{f}}^{(b)*}$  is the skew symmetric matrix of specific force acting on aircraft flying over nominal trajectory, and  ${}^N\mathbf{R}^{B*}$  is rotation matrix for the nominal  $B$ -frame to  $N$ -frame. Variation on gravity vector is not modeled in the velocity error equation since its contribution over the duration of an aircraft approach is negligibly small.

Using the summation rule for angular velocities, we can write attitude rate  $\dot{\mathbf{E}}^{(n)}$  as a function of body angular rate  $\boldsymbol{\omega}_{ib}^{(b)}$  and Earth's constant rotation rate  $\boldsymbol{\omega}_{ie}^{(e)}$  relative to inertial frame as

$$\dot{\mathbf{E}}^{(n)} = \mathbf{Q}_{BE}^{-1} \underbrace{\left[ \boldsymbol{\omega}_{ib}^{(b)} - {}^B\mathbf{R}^N \boldsymbol{\omega}_{ie}^{(n)} \right]}_{\mathbf{s}} \quad (81)$$

Using the definition of  $\mathbf{s}$  in (81), we can apply Taylor Series Expansion to linearize the attitude equation as

$$\delta \dot{\mathbf{E}}^{(n)} = \mathbf{Q}_{BE}^{*-1} \delta \boldsymbol{\omega}_{ib}^{(b)} + \underbrace{\begin{bmatrix} \mathbf{s}^{*T} & 0 & 0 \\ 0 & \mathbf{s}^{*T} & 0 \\ 0 & 0 & \mathbf{s}^{*T} \end{bmatrix}}_{\mathbf{S}^*} \delta \mathbf{Q}_{BE}^{-1} + \underbrace{\begin{bmatrix} \boldsymbol{\omega}_{ie}^{(n)T} & 0 & 0 \\ 0 & \boldsymbol{\omega}_{ie}^{(n)T} & 0 \\ 0 & 0 & \boldsymbol{\omega}_{ie}^{(n)T} \end{bmatrix}}_{\mathbf{W}_{ie}} \delta {}^B\mathbf{R}^N \quad (82)$$

where  $\delta \mathbf{Q}_{BE}^{-1}$  and  $\delta {}^B\mathbf{R}^N$  can be written in terms of  $\delta \mathbf{E}^{(n)}$  as

$$\delta \mathbf{Q}_{BE}^{-1} = \left. \frac{\partial \mathbf{Q}_{BE}^{-1}}{\partial \mathbf{E}^{(n)}} \right|_* \delta \mathbf{E}^{(n)} \quad (83)$$

$$\delta {}^B\mathbf{R}^N = \left. \frac{\partial {}^B\mathbf{R}^N}{\partial \mathbf{E}^{(n)}} \right|_* \delta \mathbf{E}^{(n)} \quad (84)$$

Let us define a matrix called  $\mathbf{K}^*$  containing only constant nominal parameters as

$$\mathbf{K}^* = \mathbf{S}^* \left. \frac{\partial \mathbf{Q}_{BE}^{-1}}{\partial \mathbf{E}^{(n)}} \right|_* + \mathbf{W}_{ie} \left. \frac{\partial {}^B\mathbf{R}^N}{\partial \mathbf{E}^{(n)}} \right|_* \quad (85)$$

and substituting Equations (83) to (85) into (82) yields attitude error equation as

$$\delta \dot{\mathbf{E}}^{(n)} = \mathbf{Q}_{BE}^{*-1} \delta \boldsymbol{\omega}_{ib}^{(b)} + \mathbf{K}^* \delta \mathbf{E}^{(n)} \quad (86)$$

The overall linearized INS kinematic model can be expressed in vector form as

$$\begin{bmatrix} \delta \dot{\mathbf{r}}^{(n)} \\ \delta \dot{\mathbf{v}}^{(n)} \\ \delta \dot{\mathbf{E}}^{(n)} \end{bmatrix} = \underbrace{\begin{bmatrix} 0 & 1 & 0 \\ 0 & -2 \tilde{\boldsymbol{\omega}}_{ie}^{(n)} & {}^N\mathbf{R}^{B*} \tilde{\mathbf{f}}^{(b)*} \\ 0 & 0 & \mathbf{K}^* \end{bmatrix}}_{\mathbf{F}_n} \underbrace{\begin{bmatrix} \delta \mathbf{r}^{(n)} \\ \delta \mathbf{v}^{(n)} \\ \delta \mathbf{E}^{(n)} \end{bmatrix}}_{\mathbf{x}_n} + \underbrace{\begin{bmatrix} 0 & 0 \\ {}^N\mathbf{R}^{B*} & 0 \\ 0 & \mathbf{Q}_{BE}^{*-1} \end{bmatrix}}_{\mathbf{G}_u} \underbrace{\begin{bmatrix} \delta \mathbf{f}^{(b)} \\ \delta \boldsymbol{\omega}_{ib}^{(b)} \end{bmatrix}}_{\mathbf{u}} \quad (87)$$

where  $\delta \mathbf{x}_n$  is referred to as the INS state vector,  $\mathbf{F}_n$  is plant matrix of the kinematic model,  $\mathbf{G}_u$  is input coefficient matrix, and  $\delta \mathbf{u}$  is the variation on IMU measurements, which are the specific force and angular velocity of the aircraft. Note that all the superscripts \* refers to constant nominal values.

## Appendix D GNSS MEASUREMENT MODEL

This appendix gives a linearized measurement model for DD carrier and code GNSS [11] in the form of

$$\underbrace{\begin{bmatrix} \phi \\ \rho \end{bmatrix}}_{\mathbf{z}} = \underbrace{\begin{bmatrix} \mathbf{G}' \\ \mathbf{G}' \end{bmatrix}}_{\mathbf{G}^*} \delta \mathbf{r}^{(e)} + \underbrace{\begin{bmatrix} \lambda \mathbf{I} \\ 0 \end{bmatrix}}_{\mathbf{D}} \mathbf{N} + \underbrace{\begin{bmatrix} \boldsymbol{\nu}_\phi \\ \boldsymbol{\nu}_\rho \end{bmatrix}}_{\boldsymbol{\nu}_{\rho\phi}} \quad (88)$$

where  $\lambda$  is L1 carrier frequency,  $\mathbf{N}$  is cycle ambiguity states,  $\mathbf{r}^{(e)}$  is position from reference station expressed in  $E$ -frame.  $\phi$  and  $\rho$  are carrier and code measurements after correcting for the nominal term  $\mathbf{G}^* \delta \mathbf{r}^*$ .  $\mathbf{G}'$  is observation matrix including line-of-sight vectors from reference station to  $n$ -satellites as

$$\mathbf{G}' = \begin{bmatrix} -(e_2^T - e_1^T) \\ \vdots \\ -(e_n^T - e_1^T) \end{bmatrix} \quad (89)$$

where  $e_i$  represents the unit line-of-sight vector of the  $i^{th}$  satellite in  $E$ -frame. The DD carrier and code phase measurement errors  $\boldsymbol{\nu}_\phi$  and  $\boldsymbol{\nu}_\rho$ , are assumed to be zero-mean Gaussian distribution with a covariance which can be expressed in terms of single difference (SD) code and carrier measurement standard deviations  $\sigma_\phi$  and  $\sigma_\rho$  as

$$\begin{aligned} \boldsymbol{\nu}_\phi &\sim \mathcal{N}(0, \boldsymbol{\Lambda} \boldsymbol{\Lambda}^T \sigma_\phi^2) \\ \boldsymbol{\nu}_\rho &\sim \mathcal{N}(0, \boldsymbol{\Lambda} \boldsymbol{\Lambda}^T \sigma_\rho^2) \end{aligned} \quad (90)$$

where  $\boldsymbol{\Lambda}$  is the transformation matrix that transforms SD measurement noise vector to DD noise vector. Note that DD

method allows eliminating ephemeris, satellite and receiver clock errors for improving the accuracy in descending phase of the flight.

## Appendix E SIMULATION DATA

TABLE I  
INS-GNSS ERROR PARAMETERS [12]

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

TABLE II  
B747 AIRCRAFT PHYSICAL PROPERTIES [13]

Properties	Symbol	Value	Unit
Mass	<i>m</i>	289,550	<i>kg</i>
Moment of Inertia	$I_{yy}$	$44.87 \times 10^6$	$kg.m^2$

## References

- [1] Joerger, M., F.-C. Chan, S. Langel, and B. Pervan. RAIM Detector and Estimator Design to Minimize the Integrity Risk. Proceedings of the 25th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2012). Nashville, TN. (2012).
- [2] 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.
- [3] Tanil, C., Khanafseh, S., Pervan, B., Impact of Wind Gusts on Detectability of GNSS Spoofing Attacks Using RAIM with INS Coupling, Institute of Navigation (ION), Pacific PNT Conference, Honolulu, HI, April 2015.
- [4] Khanafseh, S., Roshan, N., Langel, S., Chan, F., Joerger, M., Pervan, B. GNSS Spoofing Detection Using RAIM with INS Coupling, Position, Location and Navigation Symposium - PLANS 2014, 2014 IEEE/ION
- [5] 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 GNSS Civilian Spoofer," Proceedings of the 21st International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2008), Savannah, GA, September 2008, pp. 2314-2325.
- [6] 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.
- [7] Akos, Dennis M., "Whos Afraid of the Spoofer? GNSS/GNSS Spoofing Detection via Automatic Gain Control (AGC)", NAVIGATION, Journal of The Institute of Navigation, Vol. 59, No. 4, Winter 2012, pp. 281-290.
- [8] Mark L. Psiaki, Steven P. Powell, and Brady W. O'Hanlon, 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

TABLE III  
B747 LONGITUDINAL STABILITY DERIVATIVES AT ITS MACH 0.198 APPROACH AT STANDARD SEA-LEVEL CONDITIONS [13]

Parameter	Unit	Value
$X_u$		-0.021 $1/s$
$X_{\alpha}$		2.343 $m/s^2$
$X_{\delta_e}$		0.959 $m/s^2$
$X_{\delta_T}$		0.3 <i>g</i> $m/s^2$
$Z_u$		-0.202 $1/s$
$Z_{\alpha}$		-9.831 $m/s^2$
$Z_q$		-6.22 $m/s$
$Z_{\delta_e}$		-6.42 $m/s^2$
$Z_{\delta_T}$		0 $m/s^2$
$M_u$		0.00012 $1/m.s$
$M_q$		-0.357 $1/s$
$M_{\alpha}$		-0.4140 $1/s^2$
$M_{\delta_e}$		-0.034 $1/s^2$
$M_{\delta_T}$		0 $1/s^2$

TABLE IV  
B747 APPROACH TRIMMED FLIGHT CONDITIONS [13]

Flight Conditions	Symbol	Value	Unit
Speed	<i>u</i>	63	<i>m/s</i>
Angle of Attack	$\alpha$	8	<i>deg</i>
Flight Path Angle	$\gamma$	-3	<i>deg</i>
Pitch Angle	$\theta$	5	<i>deg</i>
Altitude	<i>h</i>	Sea Level	<i>m</i>

- [9] Morris, S., L., Bossert, D., E., Hallgren, W., F., Introduction to Aircraft Flight Mechanics, AIAA Education Series. ISBN-13: 978-1624102547
- [10] Farrell, J. (2008). Aided navigation: GNSS with high rate sensors. McGraw-Hill, Inc.
- [11] Misra, P., Enge, P. (2006). Global Positioning System: Signals, Measurements and Performance Second Edition. Lincoln, MA: Ganga-Jamuna Press.
- [12] Brown, R. G., P. Y. C Hwang, Introduction to Random Signals and Applied Kalman Filtering. 3rd Ed. New York: John Wiley Sons, 1997.
- [13] Heffley, R. K., Jewell, W. F. (1972). Aircraft Handling Qualities Data.
- [14] Bryson, A., Ho, Y., Applied Optimal Control: Optimization, Estimation, and Control, Hemisphere, 1975
- [15] Gelb, A., Applied Optimal Estimation. MIT Press, 1974.