GPS Spoofing Detection using RAIM with INS Coupling

Samer Khanafseh, Naeem Roshan, Steven Langel, Fang-Cheng Chan,
Mathieu Joerger, and Boris Pervan
Illinois Institute of Technology
Chicago, IL

***Abstract*— In this work, we develop, implement, and test a monitor to detect GPS spoofing attacks using residual-based Receiver Autonomous Integrity Monitoring (RAIM) with inertial navigation sensors. Signal spoofing is a critical threat to all navigation applications that utilize GNSS, and is especially hazardous in aviation applications. This work develops a new method to directly detect spoofing using a GPS/INS integrated navigation system that incorporates fault detection concepts based on RAIM. The method is also capable of providing an upper bound on the proposed monitor's integrity risk.**

Keywords-component; Spoofing Detection; Integrity Risk; RAIM monitor; Integrated Navigation.

I. INTRODUCTION

A spoofing attack happens when a counterfeit signal is intentionally broadcast to a target user, resulting in incorrect position estimates. The spoofed signal mimics the original GPS signal with higher power and thus may go unnoticed by measurement screening techniques used within the receiver. As a result, the trajectory of the target user can be controlled through the fake broadcast measurements [1]. Numerous anti-spoofing techniques have been developed, including employing modified GPS navigation data [2], using antenna arrays and automatic gain control schemes [3], high-frequency antenna motion [4], or signal power analysis techniques. Intuitive approaches to monitor for spoofing attacks using redundant sensors have also been proposed, however a thorough description of their implementation and performance in terms of probability of false alarm, probability of missed detection and integrity risk has never been provided.

The detector proposed in this work monitors discrepancies between GPS spoofed measurements and INS measurements. Without inertial bias calibration, the monitor's ability to detect spoofing will deteriorate quickly due to INS error drift. For this monitor, the INS unit is assumed to be pre-calibrated under fault free conditions prior to a spoofing attack. This assumption is reasonable, for example, for aviation applications with a ground-based spoofer. It is assumed that the aircraft is being initialized on the ground prior to take off. Any spoofing attack near the airport may be easily detected by the ground station's static antennas. Furthermore, the aircraft may be out of reach of the spoofer at high altitude due to the spoofer's limited power.

One method to detect GPS spoofing attacks is to compare a free inertial solution to the GPS-derived position solution. In the free-inertial approach, the previously calibrated INS unit runs without further calibration during the spoofing attack. However, without continuous calibration of the inertial sensor biases, position estimate errors, and their covariance, will grow without bound (Figure 1).

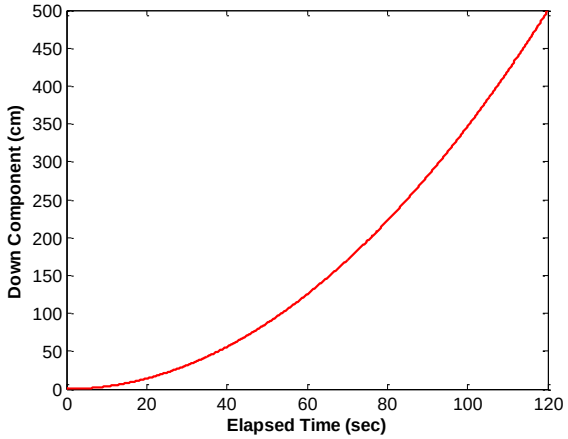

Fig. 1. Free inertial coasting error for down component of relative position vector.

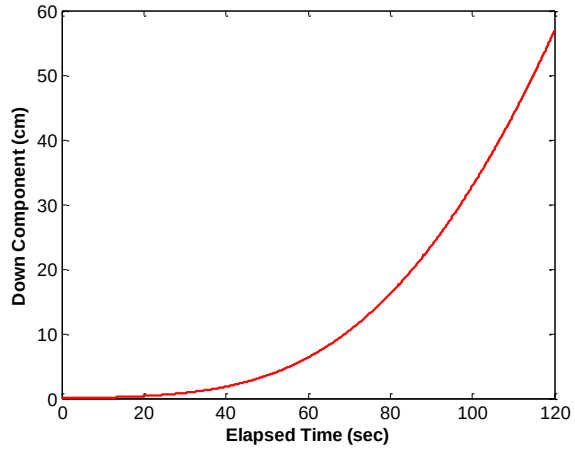

Fig. 2. Tightly coupled coasting error for down component of relative position vector.

The authors gratefully acknowledge the FAA for supporting this research.

Therefore, if a monitor is based on simply comparing the GPS position solution to the free-INS position solution, even using the highest quality inertial sensors, spoofing attacks can quickly cause large GPS position errors without being detected by the monitor. For the tightly coupled implementation, continuous calibration of INS errors increases monitor sensitivity to position-domain discrepancies caused by the spoofing attack (Figure 2). This feature can be exploited together with a time history of residuals to design an efficient detection algorithm for GPS spoofing.

RAIM detection concepts are used in this work where the redundancy is provided through INS measurements, unlike conventional usage of RAIM where detection is provided through satellite redundancy. To enhance detection capability, a time history of GPS measurements is used to estimate the position vector as well as compute measurement residuals in a batch weighted least squares estimator. Integrity risk for this batch estimator and RAIM monitor depends on the time-sequence of spoofed GPS signals. A wide variety of possible spoofing scenarios may exist, but when using residual-based RAIM, it is not necessary to define a threat space because the worst-case spoofing attack can be determined by finding the profile that maximizes integrity risk [5]. This profile takes into account the impact of spoofed signals on the test statistic and the user position estimate simultaneously.

Next, we provide a brief description of the INS mechanization equations and the tightly coupled GPS/INS system used in the rest of this work. We then introduce residual RAIM techniques and a summary of the worst case fault vector derived in [5] and which will be utilized in the computation of integrity risk. Finally, using different flight path scenarios and INS specifications, we conduct covariance analysis simulations to quantify the performance of the monitor in terms of integrity risk.

II. TIGHTLY COUPLED GPS/INS SYSTEM

GPS 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 GPS tracking loops [6]. This work uses tightly coupled integration to limit INS error drifts, which makes it easier to detect erroneous GPS position estimates. The tightly coupled approach combines GPS and INS states into one centralized Kalman filter [7].

A. INS Mechanization Equations

The derivation of the INS mechanization equations can be found in many textbooks devoted to the fundamental theory of inertial navigation, such as [6], [7] and [8]. Inertial measurement units (IMUs) use accelerometers and gyroscopes to determine a user's position and orientation in space. The equations of motion for these devices are derived from physics, and are stated below :

$$\begin{bmatrix} {}^{E}\dot{\mathbf{V}}^{U} \\ \dot{\mathbf{E}} \end{bmatrix} = \begin{bmatrix} -\left(2\ {}^{I}\boldsymbol{\omega}^{E} + {}^{E}\boldsymbol{\omega}^{U}\right)\times & \mathbf{0} \\ -\mathbf{F}_{Eu}\ {}^{B}\mathbf{R}^{U}\mathbf{F}_{V2T} & \mathbf{0} \end{bmatrix} \begin{bmatrix} {}^{E}\mathbf{V}^{U} \\ \mathbf{E} \end{bmatrix} + \begin{bmatrix} {}^{U}\mathbf{R}^{B}\boldsymbol{f} + \mathbf{g} \\ \mathbf{F}_{Eu}\left({}^{I}\boldsymbol{\omega}^{B} - {}^{B}\mathbf{R}^{U}\ {}^{I}\boldsymbol{\omega}^{E}\right) \end{bmatrix} \quad (1)$$

where $\mathbf{c}\times$ is the skew semmteric matrix representation of an arbitrary vector $\mathbf{c}$, ${}^{E}\mathbf{V}^{U}$ is the ground velocity of the user, $\mathbf{E}$ is the attitude vector of the user (roll, pitch, and yaw), ${}^{I}\boldsymbol{\omega}^{E}$ is the rotation rate of the earth, ${}^{E}\boldsymbol{\omega}^{U}$ is the rotation rate of the user navigation frame relative to earth, ${}^{B}\mathbf{R}^{U}$ is the transformation matrix from the user navigation frame to body frame, $\boldsymbol{f}$ is the specific force measured by the accelerometers, $\mathbf{g}$ is the gravity vector, ${}^{I}\boldsymbol{\omega}^{B}$ is the inertial angular velocity of the user measured by the gyroscopes, $\mathbf{F}_{Eu}$ is the transformation matrix which translates the instantaneous body-to-navigation rotation rate into Euler angle rotation rate [7], and $\mathbf{F}_{V2T}$ is the matrix which translates the user velocity into the navigation frame rotation rate [6].

The fundamental states in equation (1) are velocity and attitude. In addition to these fundamental INS states, one must also include states which model the variation in the gravity vector from vertical as well as inertial sensor bias errors. Adding these states to the dynamic model given in (1) results in [6,9]:

$$\begin{bmatrix} {}^{E}\dot{\mathbf{V}}^{U} \\ \dot{\mathbf{E}} \\ \dot{\mathbf{b}}_{g} \\ \dot{\mathbf{b}}_{a} \\ \dot{\mathbf{g}}_{gm} \end{bmatrix} = \mathbf{F}_{I}' \begin{bmatrix} {}^{E}\mathbf{V}^{U} \\ \mathbf{E} \\ \mathbf{b}_{g} \\ \mathbf{b}_{a} \\ \mathbf{g}_{gm} \end{bmatrix} + \begin{bmatrix} {}^{U}\mathbf{R}^{B}\boldsymbol{f} + \mathbf{g} \\ \mathbf{F}_{Eu}\left({}^{I}\boldsymbol{\omega}^{B} - {}^{B}\mathbf{R}^{U}\ {}^{I}\boldsymbol{\omega}^{E}\right) \\ \mathbf{0} \\ \mathbf{0} \\ \mathbf{0} \end{bmatrix} \quad (2)$$

where the dynamic matrix $\mathbf{F}_{I}'$ is defined as [9]:

$$\mathbf{F}_{I}' = \begin{bmatrix} -\left(2\ {}^{I}\boldsymbol{\omega}^{E} + {}^{E}\boldsymbol{\omega}^{U}\right)\times & \mathbf{0} & \mathbf{0} & -{}^{U}\mathbf{R}^{B} & \mathbf{F}_{gm2V} \\ -\mathbf{F}_{Eu}\ {}^{B}\mathbf{R}^{U}\mathbf{F}_{V2T} & \mathbf{0} & -\boldsymbol{F}_{Eu} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \boldsymbol{I}\left(\frac{-1}{\tau_{g}}\right) & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \boldsymbol{I}\left(\frac{-1}{\tau_{a}}\right) & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \boldsymbol{I}\left(\frac{-1}{\tau_{gm}}\right) \end{bmatrix}$$

The states $\mathbf{b}_{g}$ and $\mathbf{b}_{a}$ model the gyroscope and accelerometer random bias and are described by first order Gauss Markov processes with time constants τ_{g} and τ_{a}, respectively. In addition, the gravity vector will change in magnitude and direction due to the inhomogeneous mass distribution of the earth. These effects are captured in the state $\mathbf{g}_{gm}$, also modeled as first order Gauss Markov with a time constant τ_{gm}.

Notice that equation (2) is a continuous time non-linear dynamic model for an inertial navigation system. For simulation purposes, it is customary to simulate such a system by using a linearized Kalman filter. This involves linearizing equation (2) about some nominal trajectory using either a Taylor series expansion or a perturbation method. The details of this linearization process will not be carried out in detail here, but can be found in [9, 6, 7]. Using a linearized Kalman filter recasts the state estimation problem in terms of estimating deviations of the actual state from a nominal trajectory. For example, instead of estimating the user's ground velocity,

${}^{E}\mathbf{V}^{U}$, one would be estimating the deviation $\delta^{E}\mathbf{V}^{U}$ of the user's velocity from the reference value. Hence, the linearized INS equations become:

$$\begin{bmatrix} \delta^{E}\dot{\mathbf{V}}^{U} \\ \delta\dot{\mathbf{E}} \\ \delta\dot{\mathbf{b}}_{g} \\ \delta\dot{\mathbf{b}}_{a} \\ \delta\dot{\mathbf{g}}_{gm} \end{bmatrix} = \mathbf{F}_{I} \begin{bmatrix} \delta^{E}\mathbf{V}^{U} \\ \delta\mathbf{E} \\ \delta\mathbf{b}_{g} \\ \delta\mathbf{b}_{a} \\ \delta\mathbf{g}_{gm} \end{bmatrix} + \mathbf{W}_{I} \tag{3}$$

where the linearized dynamic matrix $\mathbf{F}_I$ is defined as:

$$\mathbf{F}_{I} = \begin{bmatrix} \mathbf{0} & \left({}^{U}\mathbf{R}^{B}\boldsymbol{f}\right)\times & \mathbf{0} & -{}^{U}\mathbf{R}^{B} & \mathbf{F}_{gm2V} \\ \mathbf{F}_{V2T} & {}^{I}\boldsymbol{\omega}^{U}\times & {}^{U}\mathbf{R}^{B} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \boldsymbol{I}\left(\frac{-1}{\tau_{g}}\right) & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \boldsymbol{I}\left(\frac{-1}{\tau_{a}}\right) & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \boldsymbol{I}\left(\frac{-1}{\tau_{gm}}\right) \end{bmatrix}$$

The process noise term, $\mathbf{W}_I$, is inserted here to factor in random disturbances such as random sensor noise in the accelerometer and gyroscopes. This term can be written as [9]

$$\mathbf{W}_{I} = \begin{bmatrix} -{}^{U}\mathbf{R}^{B}\boldsymbol{v}_{a} \\ {}^{U}\mathbf{R}^{B}\boldsymbol{v}_{g} \\ \boldsymbol{\eta}_{g} \\ \boldsymbol{\eta}_{a} \\ \boldsymbol{\eta}_{gm} \end{bmatrix} \tag{4}$$

where $\boldsymbol{v}_a$ is the random sensor noise in the accelerometer, $\boldsymbol{v}_g$ is the random sensor noise in the gyroscope, and $\boldsymbol{\eta}_g$, $\boldsymbol{\eta}_a$, and $\boldsymbol{\eta}_{gm}$ are the driving white noise processes for the Gauss-Markov models.

B. Tightly Coupled GPS/INS

In this work, we assume that external aiding measurements from the GPS include double difference L1 carrier phase measurements ($\nabla\Delta\phi$) and double difference pseudorange measurements ($\nabla\Delta\rho$). Code measurements are used to reduce the time to estimate the ambiguities and the double difference carrier phase measurements are used to gain the maximum possible accuracy for velocity estimates, which impacts the quality of the INS calibration.

The double difference code and carrier phase measurements are formed by first differencing measurements between the user and reference station. This process eliminates the satellite clock and ephemeris errors. Then, these subsequent measurements are differenced again relative to a master satellite, eliminating the receiver clock bias. Hence, we obtain the following measurement models:

$$z_{\rho} = \nabla\Delta\rho^{ij} = -(\hat{\mathbf{e}}^{i} - \hat{\mathbf{e}}^{j})^{T}\Delta\mathbf{x} + \nabla\Delta m_{\rho}^{ij} + \delta T^{ij} + \delta I^{ij} + v_{\nabla\Delta\rho}^{ij} \tag{5}$$

$$z_{\phi} = \nabla\Delta\phi^{ij} = -(\hat{\mathbf{e}}^{i} - \hat{\mathbf{e}}^{j})^{T}\Delta\mathbf{x} + \lambda\nabla\Delta N^{ij} + \nabla\Delta m_{\phi}^{ij} + \delta T^{ij} - \delta I^{ij} + v_{\nabla\Delta\phi}^{ij} \tag{6}$$

where $\nabla\Delta N^{ij}$ is the double difference L1 cycle ambiguity, $\nabla\Delta m_{\rho}^{ij}$ and $\nabla\Delta m_{\phi}^{ij}$ are the double difference code and carrier phase multipath errors for satellite *i* and *j*, δT^{ij} is the residual tropospheric error, δI^{ij} is the residual ionospheric error and $v_{\nabla\Delta\rho}^{ij}$ and $v_{\nabla\Delta\phi}^{ij}$ are the double difference code and carrier phase measurement noise, respectively.

In this algorithm, multipath states are modeled as 1st order Gauss-Markov processes. In order to model the spatial decorrelation errors for the troposphere and ionosphere, the LAAS accuracy models from [10] are employed. The resulting GPS state vector for relative positioning is described by:

$$\mathbf{X}_{G} = \begin{bmatrix} \Delta\mathbf{x} \\ \nabla\Delta\mathbf{N} \\ \mathbf{a} \end{bmatrix} \tag{7}$$

where **a** is a vector that includes atmospheric and multipath error states. In what follows, the vector **a** will be dropped from the state vector $\mathbf{X}_G$. However, its impact will be properly accounted for when we introduce the batch implementation.

In order to tie the GPS and INS dynamic models together, a relationship between the position state estimated with GPS in (7) and the velocity state estimated with the INS in (3) must be derived. This type of integration was first implemented in [9] for a stationary reference station.

Let $\Delta\mathbf{x}_N$ be the position of the user relative to the reference station expressed in the reference station local level frame, N.

$$\Delta\mathbf{x}_{N} = \mathbf{x}_{r_N} - \mathbf{x}_{u_N} \tag{8}$$

where $\mathbf{x}_{r_N}$ is the absolute position of the reference station, and $\mathbf{x}_{u_N}$ is the absolute position of the user expressed in the *N* frame. Differentiating both sides of (8) in the *N* frame results in:

$$\frac{{}^{N}d\Delta\mathbf{x}_{N}}{dt} = \frac{{}^{N}d\mathbf{x}_{r_N}}{dt} - \frac{{}^{N}d\mathbf{x}_{u_N}}{dt} = -\frac{{}^{N}d\mathbf{x}_{u_N}}{dt} \tag{9}$$

where the term $\frac{{}^{N}d\mathbf{x}_{u_N}}{dt} = 0$ because the reference station is stationary. Before (9) can be used in the dynamic model, it must be put in a differential form using the same process as in deriving (3). It is also worth mentioning that since we are using a linearized Kalman filter, the GPS states must also be written in terms of deviations from the nominal trajectory. However, since the GPS dynamic model is already linear, the structure of the state transition matrix remains unchanged. The resulting link between GPS and INS states can be written as:

$$\delta\Delta\dot{\mathbf{x}}_{N} = -{}^{N}\mathbf{R}^{U}\delta\,{}^{E}\mathbf{V}^{U} \tag{10}$$

Combining the GPS dynamic model with the INS model in (3-5), the appropriate dynamic model for the GPS/INS states is given by:

$$\begin{bmatrix} \delta^E\dot{\mathbf{V}}^U \\ \delta\dot{\mathbf{E}} \\ \delta\dot{\mathbf{b}}_g \\ \delta\dot{\mathbf{b}}_a \\ \delta\dot{\mathbf{g}}_{gm} \\ \delta\Delta\dot{\mathbf{x}}_N \\ \delta\nabla\Delta\dot{\mathbf{N}} \end{bmatrix} = \begin{bmatrix} \mathbf{0} & -({}^U\mathbf{R}^B\boldsymbol{f})\times & \mathbf{0} & -{}^U\mathbf{R}^B & \mathbf{F}_{gm2V} & \mathbf{F}_{X2V} & \mathbf{0} \\ \mathbf{F}_{V2T} & {}^I\boldsymbol{\omega}^U\times & {}^U\mathbf{R}^B & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \boldsymbol{I}\left(\frac{-1}{\tau_g}\right) & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \boldsymbol{I}\left(\frac{-1}{\tau_a}\right) & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \boldsymbol{I}\left(\frac{-1}{\tau_{gm}}\right) & \mathbf{0} & \mathbf{0} \\ -{}^N\mathbf{R}^U & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \end{bmatrix} \begin{bmatrix} \delta^E\mathbf{V}^U \\ \delta\mathbf{E} \\ \delta\mathbf{b}_g \\ \delta\mathbf{b}_a \\ \delta\mathbf{g}_{gm} \\ \delta\Delta\mathbf{x}_N \\ \delta\nabla\Delta\mathbf{N} \end{bmatrix} + \begin{bmatrix} -{}^U\mathbf{R}^B\boldsymbol{v}_a \\ {}^U\mathbf{R}^B\boldsymbol{v}_g \\ \boldsymbol{\eta}_g \\ \boldsymbol{\eta}_a \\ \boldsymbol{\eta}_{gm} \\ \mathbf{0} \\ \mathbf{0} \end{bmatrix} \tag{11}$$

Equation (11) can be written in block matrix notation as

$$\begin{bmatrix} \delta\nabla\Delta\dot{\mathbf{N}} \\ \dot{\boldsymbol{\xi}}_I \\ \delta\Delta\dot{\mathbf{x}}_N \end{bmatrix} = \begin{bmatrix} \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{F}_I & \mathbf{F}_{I2G} \\ \mathbf{0} & \mathbf{F}_{G2I} & \mathbf{0} \end{bmatrix} \begin{bmatrix} \delta\nabla\Delta\mathbf{N} \\ \boldsymbol{\xi}_I \\ \delta\Delta\mathbf{x}_N \end{bmatrix} + \begin{bmatrix} \mathbf{0} \\ \mathbf{W}_I \\ \mathbf{0} \end{bmatrix} \tag{12}$$

where $\boldsymbol{\xi}_I$ and $\mathbf{W}_I$ are the INS state and process noise vectors as defined by (3) and (11), respectively, and the definitions of $\mathbf{F}_I$, $\mathbf{F}_{I2G}$ and $\mathbf{F}_{G2I}$ is determined by comparing (12) to (11). To summarize, (12) provides an equation for the linearized dynamic model of the GPS/INS integrated architecture where all GPS and INS states have been put in one state vector which can be estimated using a linearized Kalman filter. Since the only external measurements are the GPS measurements, the measurement model is:

$$\begin{bmatrix} \mathbf{z}_{\rho 1} \\ \mathbf{z}_{\phi 1} \end{bmatrix} = \begin{bmatrix} \mathbf{0} & \mathbf{0} & \mathbf{H}_G \\ \lambda\mathbf{I} & \mathbf{0} & \mathbf{H}_G \end{bmatrix} \begin{bmatrix} \delta\nabla\Delta\mathbf{N} \\ \boldsymbol{\xi}_I \\ \delta\Delta\mathbf{x}_N \end{bmatrix} + \begin{bmatrix} \boldsymbol{\nu}_{\rho 1} \\ \boldsymbol{\nu}_{\phi 1} \end{bmatrix} \tag{13}$$

where $\mathbf{H}_G$ is the GPS observation matrix given in equation (5).

By integrating INS with GPS as shown in (12) and (13), INS error drift remains bounded. This allows INS to be used as a consistency check against GPS spoofing faults. This check is accomplished by computing the magnitude of the residual vector and comparing that to a predefined threshold, which is determined using RAIM techniques.

III. RAIM FOR DETECTING SPOOFING FAULTS

RAIM was originally developed to detect satellite faults [11-13] 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 residual based RAIM 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.

In this work, since all GPS measurements may be impacted by the spoofing attack, it is assumed that all GPS 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 GPS measurements, thereby corrupting INS calibration without being detected.

Integrity risk is defined as the probability that the position error exceeds an acceptable limit (referred to as an *alert limit* ℓ) without being detected (the test statistic q is less than the threshold T), i.e.,

$$I_r = P\{|\varepsilon| > \ell, |q| < T|H_s\}P\{H_s\} \tag{14}$$

where ε is the position error, ℓ is the alert limit and H_s is the hypothesis of a spoofing attack. In this work, we conservatively assume that the prior probability of a spoofing attack is 1.

Finding the worst case fault profile for least squares RAIM has been derived in [14] and was extended to batch estimation in [5]. A brief description of this approach is discussed below, and more details concerning the derivation can be found in [5].

The measurement model in a batch formulation can be represented as

$$\mathbf{z} = \mathbf{H}\mathbf{x} + \mathbf{v} + \mathbf{f} \tag{15}$$

where $\mathbf{z}$ is the measurement vector, $\mathbf{x}$ is the state vector, $\mathbf{v}$ is the measurement noise vector, and $\mathbf{f}$ is the fault vector. The measurement noise vector is assumed to follow a zero mean Gaussian distribution with covariance matrix $\mathbf{V}$. Equation (15) is then partitioned based on faulty measurements $\mathbf{z}_A$ and fault-free measurements $\mathbf{z}_B$. For example, in the case of a spoofing attack, $\mathbf{z}_A$ is the GPS measurements and $\mathbf{z}_B$ corresponds to INS measurements. More details concerning the batch implementation of tightly coupled GPS/INS will be provided in the next section.

$$\begin{bmatrix} \mathbf{z}_\mathbf{A} \\ \mathbf{z}_\mathbf{B} \end{bmatrix} = \begin{bmatrix} \mathbf{H}_\mathbf{A} \\ \mathbf{H}_\mathbf{B} \end{bmatrix} \mathbf{x} + \begin{bmatrix} \mathbf{v}_\mathbf{A} \\ \mathbf{v}_\mathbf{B} \end{bmatrix} + \begin{bmatrix} \mathbf{f}_\mathbf{A} \\ \mathbf{0} \end{bmatrix} \tag{16}$$

Based on (16), the state estimate error ($\boldsymbol{\varepsilon} = \hat{\mathbf{x}} - \mathbf{x}$) and its corresponding covariance matrix $\mathbf{P}$ can be computed as,

$$\boldsymbol{\varepsilon} = (\mathbf{H}^\mathbf{T}\mathbf{V}^{-\mathbf{1}}\mathbf{H})^{-\mathbf{1}}\mathbf{H}^\mathbf{T}\mathbf{V}^{-\mathbf{1}}(\mathbf{v} + \mathbf{f}) = \mathbf{S}(\mathbf{v} + \mathbf{f}) \tag{17}$$

$$\mathbf{P} = (\mathbf{H}^\mathbf{T}\mathbf{V}^{-\mathbf{1}}\mathbf{H})^{-\mathbf{1}} \tag{18}$$

It is customary to be interested in one element of the state vector, for example, the vertical component of the relative position vector. The error associated with the state of interest is related to $\boldsymbol{\varepsilon}$ as:

$$\varepsilon = \mathbf{s}^T(\mathbf{v} + \mathbf{f}) \tag{19}$$

where $\mathbf{s}^T$ is a single row of the matrix $\mathbf{S}$ corresponding to the state of interest.

The residual vector $\mathbf{r}$ is defined as

$$\mathbf{r} = (\mathbf{I} - \mathbf{H}\mathbf{S})\mathbf{z} = (\mathbf{I} - \mathbf{H}\mathbf{S})(\mathbf{v} + \mathbf{f}) \tag{20}$$

with a weighted norm defined by

$$q = \mathbf{r}^\mathbf{T}\mathbf{V}^{-\mathbf{1}}\mathbf{r} \tag{21}$$

Let n be the number of measurements, and m be the number of states. Under fault free conditions, the test statistic q is centrally chi square distributed with (n – m) degrees of

freedom. For a given false alarm requirement, the threshold is determined from the inverse cumulative chi square distribution.

Under faulted conditions, q is non-centrally chi square distributed with $(n - m)$ degrees of freedom and a non-centrality parameter λ^2 (22) and (23) [5].

$$q \sim \chi^2(n-m, \lambda^2) \tag{22}$$

$$\lambda^2 = \mathbf{f}^{\mathbf{T}}\mathbf{V}^{-\mathbf{1}}(\mathbf{I} - \mathbf{HS})\mathbf{f} \tag{23}$$

It has been shown in [15] that ε and q are statistically independent. Therefore, (14) can be written as:

$$I_r = P\{|\varepsilon| < \ell | H_s\} P\{q < T | H_s\} \tag{24}$$

The fault vector that maximizes the integrity risk in (24) was derived in [5] and is given by

$$\bar{\mathbf{f}} = \alpha \mathbf{A}\mathbf{M}_A\mathbf{M}_A^T\mathbf{M}_X^T \tag{25}$$

where $\mathbf{A}$ is defined from the relation $\mathbf{f} = \mathbf{A}\mathbf{f}_A$, and

$$\mathbf{M}_X = \mathbf{s}^T\mathbf{A} \tag{26}$$

$$\mathbf{M}_A = (\mathbf{A}^T\mathbf{V}^{-1}(\mathbf{I} - \mathbf{HS})\mathbf{A})^{-1/2} \tag{27}$$

and α is a scalar that is determined through iteration to maximize I_r.

The fault vector in (25) represents the most dangerous fault profile that a spoofer can inject into the GPS measurements and represents the most dangerous threat for aviation users.

In order to use this result, the tightly coupled GPS/INS algorithms developed earlier needs to be converted to a batch formulation. To illustrate the conversion, consider the Kalman filter measurement and time updates with three GPS measurements:

$$\begin{bmatrix} \mathbf{z}_{\rho 1} \\ \mathbf{z}_{\phi 1} \\ \mathbf{0} \\ \mathbf{0} \\ \mathbf{z}_{\rho 2} \\ \mathbf{z}_{\phi 2} \\ \mathbf{0} \\ \mathbf{0} \\ \mathbf{z}_{\rho 3} \\ \mathbf{z}_{\phi 3} \end{bmatrix} = \begin{bmatrix} \mathbf{0} & \mathbf{0} & \mathbf{H}_{G1} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \lambda\mathbf{I} & \mathbf{0} & \mathbf{H}_{G1} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{\Phi}_{I,2} & \mathbf{\Phi}_{I2G,2} & -\mathbf{I} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{\Phi}_{G2I,2} & \mathbf{\Phi}_{G,2} & \mathbf{0} & -\mathbf{I} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{H}_{G2} & \mathbf{0} & \mathbf{0} \\ \lambda\mathbf{I} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{H}_{G2} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{\Phi}_{I,3} & \mathbf{\Phi}_{I2G,3} & -\mathbf{I} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{\Phi}_{G2I,3} & \mathbf{\Phi}_{G,3} & \mathbf{0} & -\mathbf{I} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \boldsymbol{H}_{G3} \\ \lambda\mathbf{I} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{H}_{G3} \end{bmatrix} \begin{bmatrix} \nabla\Delta\mathbf{N} \\ \boldsymbol{\xi}_{I1} \\ \delta\Delta\mathbf{x}_1 \\ \boldsymbol{\xi}_{I2} \\ \delta\Delta\mathbf{x}_2 \\ \boldsymbol{\xi}_{I3} \\ \delta\Delta\mathbf{x}_3 \end{bmatrix} + \begin{bmatrix} \boldsymbol{v}_{\rho 1} \\ \boldsymbol{v}_{\phi 1} \\ \mathbf{W}_{I2} \\ \mathbf{0} \\ \boldsymbol{v}_{\rho 2} \\ \boldsymbol{v}_{\phi 2} \\ \mathbf{W}_{I3} \\ \mathbf{0} \\ \boldsymbol{v}_{\rho 3} \\ \boldsymbol{v}_{\phi 3} \end{bmatrix} + \begin{bmatrix} \mathbf{f}_{\rho 1} \\ \mathbf{f}_{\phi 1} \\ 0 \\ 0 \\ \mathbf{f}_{\rho 2} \\ \mathbf{f}_{\phi 2} \\ 0 \\ 0 \\ \mathbf{f}_{\rho 3} \\ \mathbf{f}_{\phi 3} \end{bmatrix} \tag{28}$$

where $\mathbf{\Phi}$ is the discrete form of the dynamic matrix $\mathbf{F}$ in (12). Multipath and residual atmospheric errors are absorbed in the noise terms $\boldsymbol{v}_\rho$ and $\boldsymbol{v}_\phi$. Therefore, $\boldsymbol{v}_\rho$ and $\boldsymbol{v}_\phi$ are colored and the correlation is accounted for in the measurement noise covariance matrix. Notice that we conservatively assume that the spoofer is also capable of injecting different faults to the code and carrier measurements.

The model in (28) has weak observability. An initial estimate of the state vector can be obtained from a Kalman filter running during the presumed fault free period. At the first epoch after the fault free period, we assume the GPS spoofing attack begins. Prior knowledge from the Kalman filter is incorporated in the batch using pseudo measurements as shown in (29).

$$\begin{bmatrix} \nabla\Delta\mathbf{N}_i \\ \boldsymbol{\xi}_{Ii} \\ \delta\Delta\mathbf{x}_i \\ \mathbf{z}_{\rho 1} \\ \mathbf{z}_{\phi 1} \\ \mathbf{0} \\ \mathbf{0} \\ \mathbf{z}_{\rho 2} \\ \mathbf{z}_{\phi 2} \\ \mathbf{0} \\ \mathbf{0} \\ \mathbf{z}_{\rho 3} \\ \mathbf{z}_{\phi 3} \end{bmatrix} = \begin{bmatrix} \mathbf{I} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{I} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{I} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{H}_{G1} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \lambda\mathbf{I} & \mathbf{0} & \mathbf{H}_{G1} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{\Phi}_{I,2} & \mathbf{\Phi}_{I2G,2} & -\mathbf{I} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{\Phi}_{G2I,2} & \mathbf{\Phi}_{G,2} & \mathbf{0} & -\mathbf{I} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{H}_{G2} & \mathbf{0} & \mathbf{0} \\ \lambda\mathbf{I} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{H}_{G2} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{\Phi}_{I,3} & \mathbf{\Phi}_{I2G,3} & -\mathbf{I} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{\Phi}_{G2I,3} & \mathbf{\Phi}_{G,3} & \mathbf{0} & -\mathbf{I} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \boldsymbol{H}_{G3} \\ \lambda\mathbf{I} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{H}_{G3} \end{bmatrix} \begin{bmatrix} \nabla\Delta\mathbf{N} \\ \boldsymbol{\xi}_{I1} \\ \delta\Delta\mathbf{x}_1 \\ \boldsymbol{\xi}_{I2} \\ \delta\Delta\mathbf{x}_2 \\ \boldsymbol{\xi}_{I3} \\ \delta\Delta\mathbf{x}_3 \end{bmatrix} + \begin{bmatrix} \boldsymbol{\varepsilon}_{Ni} \\ \boldsymbol{\varepsilon}_{\xi i} \\ \boldsymbol{\varepsilon}_{xi} \\ \boldsymbol{v}_{\rho 1} \\ \boldsymbol{v}_{\phi 1} \\ \mathbf{W}_{I2} \\ \mathbf{0} \\ \boldsymbol{v}_{\rho 2} \\ \boldsymbol{v}_{\phi 2} \\ \mathbf{W}_{I3} \\ \mathbf{0} \\ \boldsymbol{v}_{\rho 3} \\ \boldsymbol{v}_{\phi 3} \end{bmatrix} + \begin{bmatrix} \mathbf{0} \\ \mathbf{0} \\ \mathbf{0} \\ \mathbf{f}_{\rho 1} \\ \mathbf{f}_{\phi 1} \\ 0 \\ 0 \\ \mathbf{f}_{\rho 2} \\ \mathbf{f}_{\phi 2} \\ 0 \\ 0 \\ \mathbf{f}_{\rho 3} \\ \mathbf{f}_{\phi 3} \end{bmatrix} \tag{29}$$

Equation (29) can now be put in the form of (16), which enables computation of the worst case fault vector in (25). The performance of the RAIM detector is quantified in terms of integrity risk and will be shown in the next section.

IV. Simultions and Results

In this section we show the results using the residual RAIM INS monitor for an aircraft en route or in the precision landing phase of flight. Due to the limited range of the spoofer, we assume that the spoofing attack is of short duration. Furthermore, for computational purposes, we limit the spoofing attack window to 8 minutes. In future work, we will derive a worst case fault vector for a Kalman filter implementation, which may relax the computational burden of the batch filter and allow for larger time windows. The 8 minute window is based on an aircraft that enters the service volume at 20nmi and at a speed of 150 knots (77 m/s). In this analysis, we assume that the aircraft is running a Kalman filter for at least 10 seconds prior to starting the monitor.

TABLE I. INS Error Parameters

Sensor Parameter	INS Quality	
	High	***Low***
Gyro bias	0.01 °/hr	10 °/hr
Gyro white noise	3×10^{-5} °/sec/$\sqrt{Hz}$	0.001 °/sec/$\sqrt{Hz}$
Accelerometer bias	10 μg	1 mg
Accelerometer white noise	10 μg/$\sqrt{Hz}$	50 μg/$\sqrt{Hz}$

For GPS measurements, we assume that the standard deviation of the carrier phase and code measurement noise is 1cm and 1m, respectively, with multipath time constants of 100 sec. For the INS, we consider two different grades: low-grade (e.g. automotive) and high-grade (e.g. navigation grade). INS error specifications are summarized in Table I [16]. The time constants τ_g, τ_a and τ_{gm} are assumed to be 3600 sec.

An arbitrarily chosen 6 satellite GPS geometry is used to compute the worst case fault vector for different spoofing attack periods. For computational purposes, the batch uses GPS measurements every 10 seconds with an INS update rate of 20Hz. A new fault profile is computed at each GPS measurement update. Figure 3 shows the impact of the fault profile on the position of the aircraft for a period of 60 sec. Figure 4 shows the weighted norm of the residual and the threshold at different times throughout the approach. The threshold is based on an example false alarm requirement of 10^{-6}. Recall that the threshold is directly related to the degrees of freedom of the batch estimator, which is related to the number of measurements and size of the state vector. Figure 4 shows that the threshold (in black) increases with time due to an increase in the degrees of freedom ($n - m = 18 + 10 \times$ number of GPS epochs). The weighted norm of the deterministic residual $(\mathbf{I} - \mathbf{HS})\mathbf{f}$ from (20), which we refer to as the residual for compactness, is computed and shown in red and blue. At the beginning, the residual is larger than the threshold, which illustrates that the monitor may detect a spoofing attack if the aircraft was vulnerable to the attack for only 30 seconds. However, if the aircraft is susceptible to the attack for longer periods, a smart spoofer that is generating a fault profile as in (25) is able to cause the residual to tremendously decrease while inducing larger errors in the position estimate (as shown in Figure 3) due to corrupting the INS calibration. This effect is even worse for low-grade INS. Table II shows the integrity risk for an alert limit of 10 meters versus the spoofing period during the approach. The table shows that if a smart spoofer subjects the user to its attack for about 5 minutes, 99.9% of the time it will be capable of producing errors larger than 10 m without being detected even for high grade inertial.

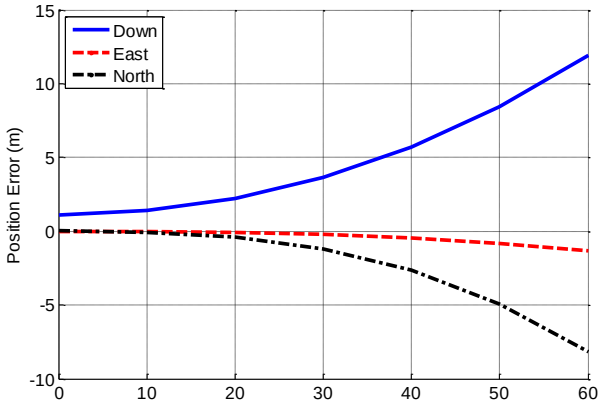

Fig. 3. Impact of the spoofing fault on the position estimate.

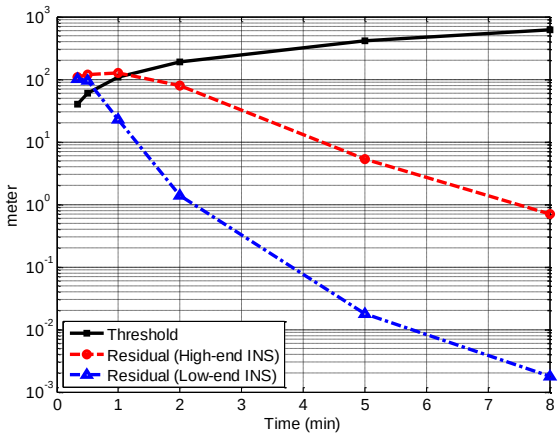

Fig. 4. Threshold and residuals of RAIM monitor for different spoofing periods for two different INS units.

TABLE II. RESIDUAL AND INTEGRITY RISK FOR DIFFERENT SPOOFING PERIODS FOR TWO DIFFERENT INS UNITS

Attack Period	Thresh. (m)	High End INS		Low End INS	
		Residual (m)	*Integrity Risk*	*Residual (m)*	*Integrity Risk*
20 sec	41	106	4.8×10^{-12}	103	2.4×10^{-10}
30 sec	60	119	1.8×10^{-9}	94	5.1×10^{-5}
1 min	108	126	5.4×10^{-5}	23	0.993
2 min	191	79	0.538	1.4	0.999
5 min	416	5	0.999	0.018	0.999
8 min	627	0.7	0.999	0.0018	0.999

Although the results in Table II may seem uninspiring, they illustrate that if the spoofer knows the exact trajectory of the user or aircraft, he may eventually cause errors that exceed the alert limits without triggering the RAIM detector. In reality, however, although the aircraft may intend to fly on a straight line trajectory, its actual path will deviate from the straight line due to wind gusts and environmental and physical disturbances. This extra motion is unknown to the spoofer who is computing the worst case fault profile based on the assumed straight line trajectory. However, the INS senses the actual motion of the aircraft and it is this discrepancy between what the INS measures due to the actual dynamic motion of the user and what the spoofer assumes that may provide detection capability to the developed INS RAIM monitor (Figure 5). In order to quantify the impact of such motion, sinusoidal based trajectories are initially simulated as the actual flight path. In the future, more elaborate aircraft dynamic models or power spectral density information will be incorporated.

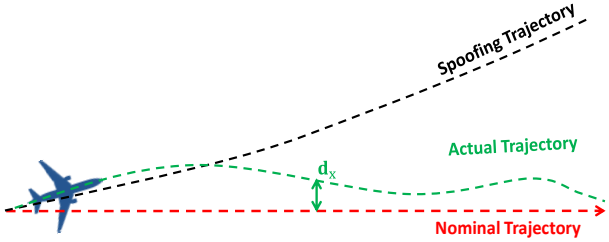

Fig. 5. Example of a nominal, actual and spoofed trajectory

The sinusoidal motion is restricted to the east direction, as an example, but several frequencies and amplitudes are considered. Figure 6 shows trajectories for two different frequencies and Figure 7 shows the specific force in the east direction for the same trajectories. This specific force is then used in the dynamic matrix $\mathbf{\Phi}$. The fault vector that is used in computing the integrity risk should account for the difference between the trajectory due to the fault profile injected by the spoofer and the actual path of the aircraft. The resultant fault vector $\bar{\mathbf{f}}_t$, may be computed as

$$\bar{\mathbf{f}}_t = \bar{\mathbf{f}} - \mathbf{G}\mathbf{d}_\mathbf{x} \tag{30}$$

where $\mathbf{G}$ is a projection matrix that converts the deviation history from the linear trajectory $\mathbf{d}_\mathbf{x}$ to the measurement domain, and $\bar{\mathbf{f}}$ is the worst case fault profile generated by the spoofer from (25).

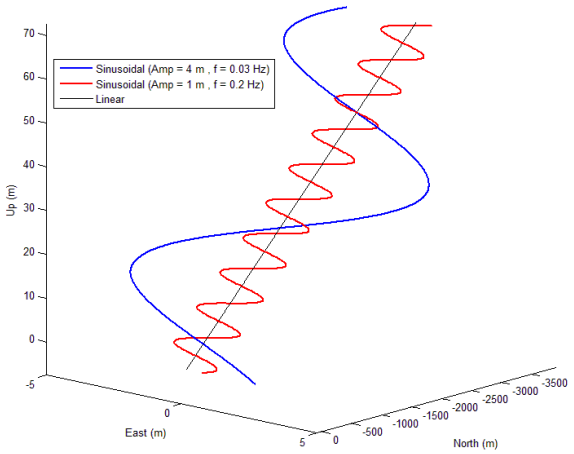

Fig. 6. Simulated linear and sinusoidal trajectories in East-North-Up coordinate frame.

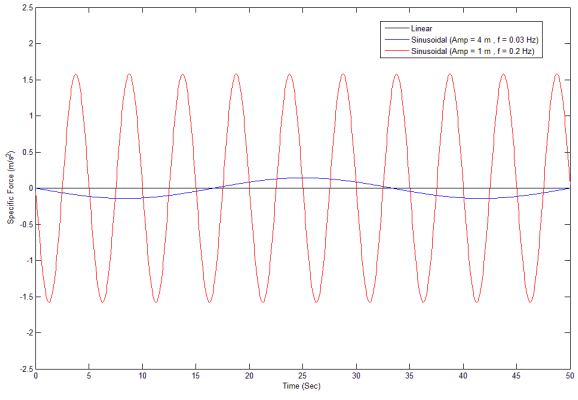

Fig. 7. East specific force of the simulated trajectories in Figure 6.

When running the previous simulations with the sinusoidal trajectories and their associated fault vectors from (30) for different amplitudes larger than 25 cm and frequencies higher than 0.03 Hz, the resultant integrity risk of the INS RAIM monitor is consistently zero for spoofing attacks lasting up to 8 minutes. This implies that it is extremely unlikely that the monitor will not detect a spoofing attack which causes the vertical position error to exceed 10 m. This result applies to both high and low grade INS units specified in Table I. This result also applies to slowly varying sinusoidal trajectories. Using the same 8 minute window and a frequency of 1mHz (equivalent to approximately 17 min period) and a 4 m amplitude the integrity risk was zero. When the amplitude is lowered to 1 cm at 0.03Hz, the computed integrity risk was 2×10^{-3}. However, this case is well below the nominal nonlinear motion of the aircraft.

V. Conclusions

In this work, an INS batch RAIM monitor was developed to detect GPS spoofing attacks. This monitor allows evaluating the integrity risk of the position solution and probability of missed detection, which is critical for aviation applications. A worst case spoofing attack profile that maximized the integrity risk of the monitor was used to quantify its performance. It was shown that if the spoofer has absolute knowledge of the trajectory of the user, it will be able to go undetected by the monitor while inducing large position errors. However, due to the lack of knowledge of the actual trajectory, it was shown that the integrity risk was negligibly small; meaning that the monitor can detect any spoofing attack.

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.

References

[1] 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," *Proceedings of the 21st International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2008)*, Savannah, GA, September 2008, pp. 2314-2325.

[2] Wesson, K. D., Rothlisberger, M. P., Humphreys, T. E., "A Proposed Navigation Message Authentication Implementation for Civil GPS Anti-Spoofing," *Proceedings of the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2011)*, Portland, OR, September 2011, pp. 3129-3140.

[3] Akos, Dennis M., "Who's 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.

[4] 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.

[5] 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, September 2012.

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

[7] Jekeli, C., *Inertial Navigation Systems with Geodetic Applications*, Berlin, New York: Walter de Gruyter 2001.

[8] Farrell, J. A., *Aided Navigation: GPS With High Rate Sensors*, New York: The McGraw-Hill Company 2008.

[9] Chan, F. C., "A State Dynamics Method for Integrated GPS/INS Navigation and Its Application To Aircraft Precision Approach," *PhD Dissertation, Illinois Institute of Technology*, Chicago, IL, May, 2008.

[10] McGraw, G. A., Murphy, T., Brenner, M., Pullen, S. and Van Dierendonck, A. J., "Development of the LAAS Accuracy Models," *Proceedings of the Institute of Navigation's ION GPS-2000*, Salt Lake City, UT, September 19-22, 2000.

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

[12] Brown, R. Grover, "A Baseline GPS RAIM Scheme and a Note on the Equivalence of Three RAIM Methods", *NAVIGATION*, Vol. 39, No. 3, Fall 1992, pp. 301-316.

[13] Sturza, M, "Navigation System Integrity Monitoring Using Redundant Measurements," *NAVIGATION: Journal of the Institute of Navigation*, Washington, DC, Vol. 35 No. 4, 1988, pp. 69-87.

[14] Angus, J. E., "RAIM with Multiple Faults", *NAVIGATION*, Vol. 53, No. 4, Winter 2006-2007, pp. 249-257.

[15] Joerger, M., and B. Pervan. "Kalman Filter-Based Integrity Monitoring Against Sensor Faults." accepted for publication in *AIAA Journal of Guidance, Control and Dynamics*.

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