DETECTING GNSS SPOOFING ATTACKS USING INS COUPLING

BY

ÇAĞATAY TANIL

Submitted in partial fulfillment of the
requirements for the degree of
Doctor of Philosophy in Mechanical and Aerospace Engineering
in the Graduate College of the
Illinois Institute of Technology

Approved 
Advisor

Chicago, Illinois
December 2016

ACKNOWLEDGMENT

First and foremost, I want to thank to my academic advisor and dissertation committee chair Professor Boris Pervan for his endless support and entrusting me in pursuing this research. His enthusiasm for this research was contagious and motivational for me. I appreciate him for providing me the opportunity to work in this research, perfectly matching my guidance and control experience with navigation. I must also thank my advisor and committee member, Professor Samer Khanafseh, for his technical expertise, endless availability for mentoring me in this research. I would also like to extend my deepest gratitude to the rest of my committee: Professors Kevin Cassel, Geoffrey Williamson, and Seebany Datta-Barua.

I gratefully acknowledge the Federal Aviation Administration (FAA) Ground Based Augmentation Systems (GBAS) working group for funding this research.

I would also like to thank Professor Mathieu Joerger for his precious time and valuable insights into my work, and my fellow colleagues in the Navigation and Guidance Laboratory: Dr. Michael Jamoom, Stefan Stevanovic, Yawei Zhai, Adriano Canolla, Ryan Cassel, and Jaymin Patel who have made my tenure as a PhD candidate as memorable as possible.

I also thank my former supervisors from Roketsan Missiles Industries: Dr. Necip Pehlivantürk, Dr. Sartuk Karasoy, and Bülent Semerci and my former academic advisors from my Master of Science: Professor Emeritus Bülent Platin and Dr. Gökmen Mahmutyazıcıoğlu for their support in my decision to pursue this doctoral degree.

My greatest gratitude goes to my friend, Professor Özgur Keleş for his constant support and encouragement throughout this difficult journey in Chicago. I cannot forget my friend Roohollah Parvizi who went through hard times together,

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABSTRACT

Vulnerability of Global Navigation Satellite Systems (GNSS) users to signal spoofing is a critical threat to positioning integrity, especially in aviation applications, where the consequences are potentially catastrophic. In response, this research describes and evaluates a new approach to directly detect spoofing using integrated Inertial Navigation Systems (INS) and fault detection concepts based on integrity monitoring. The monitors developed here can be implemented into positioning systems using INS/GNSS integration via 1) tightly-coupled, 2) loosely-coupled, and 3) uncoupled schemes. New evaluation methods enable the statistical computation of integrity risk resulting from a worst-case spoofing attack – without needing to simulate an unmanageably large number of individual aircraft approaches. Integrity risk is an absolute measure of safety and a well-established metric in aircraft navigation. A novel closed-form solution to the worst-case time sequence of GNSS signals is derived to maximize the integrity risk for each monitor and used in the covariance analyses. This methodology tests the performance of the monitors against the most sophisticated spoofers, capable of tracking the aircraft position – for example, by means of remote tracking or onboard sensing. Another contribution is a comprehensive closed-loop model that encapsulates the vehicle and compensator (estimator and controller) dynamics. A sensitivity analysis uses this model to quantify the leveraging impact of the vehicle's dynamic responses (e.g., to wind gusts, or to autopilot's acceleration commands) on the monitor's detection capability. The performance of the monitors is evaluated for two safety-critical terminal area navigation applications: 1) autonomous shipboard landing and 2) Boeing 747 (B747) landing assisted with Ground Based Augmentation Systems (GBAS). It is demonstrated that for both systems, the monitors are capable of meeting the most stringent precision approach and landing integrity requirements of the International Civil Aviation Organization (ICAO). The statistical evaluation methods developed here can be used as a baseline

procedure in the Federal Aviation Administration's (FAA) certification of spoof-free navigation systems. The final contribution is an investigation of INS sensor quality on detection performance. This determines the minimum sensor requirements to perform standalone GNSS positioning in general en route applications with guaranteed spoofing detection integrity.

CHAPTER 1

INTRODUCTION

1.1 Spoofing Attacks to GNSS Receivers

The Federal Aviation Administration (FAA) has defined the spoofing attacks as potential integrity threats to aircraft navigation and Air Traffic Control (ATC) tracking systems [2]. Spoofing of Global Navigation Satellite System (GNSS) signals is a process whereby an external agent tries to control the position output of a GNSS receiver by deliberately broadcasting a counterfeit signal. The spoofed signal mimics the original GNSS signal with higher power and thus may go unnoticed by measurement screening techniques used within the target receiver, which ultimately causes the victim to deduce incorrect position estimates. As a result, the trajectory of the victim can be controlled through the fake broadcast signals [17].

1.2 The Need for Spoofing Detection

Spoofing attacks are a serious problem for civil GNSS applications, such as aircraft landing, especially in low visibility, and for existing or near-future unmanned aerial vehicles (UAVs or drones) operated by postal services, police departments and others for surveillance purposes. Also many strategic infrastructures such as offshore oil drilling, surveying, electric power grids or communications networks heavily rely on GNSS for localization, navigation, and time synchronization. Even though military GNSS users are less susceptible to that problem by means of signal encryption, a technique called meaconing could be used as a spoofing-like attack against such users [41]. Meaconing is an attack which involves reception and rebroadcast of original encrypted GNSS signals.

Spoofing attacks are rarely observed but the methods of how to spoof are known and its consequences have been demonstrated to be dangerous. The interest in GNSS spoofing attacks has risen with recent rumors of the capture of a classified Lockheed Martin RQ-170 UAV by an Iranian cyberwarfare unit in 2011. It has been claimed that the UAV was brought down with minimum damage by simultaneous jamming of military signals and spoofing of civilian signals [47]. Since then, no known example of a malicious spoofing attack has yet been confirmed. Some proof-of-concept spoofing tests on standard receivers of a drone [23] and a yacht [5] were successfully conducted, showing that such attacks drag the vehicle off course without being detected.

The passing of the FAA Modernization and Reform Act of 2012 emphasizes that civil aviation use of GNSS is vulnerable to intentional spoofing and the threat of spoofing is likely to increase. Therefore, the FAA is pursuing mitigations to these vulnerabilities by proof-of-concept techniques and recommending manufacturers to consider measures to mitigate and cross-check against independent position sources or employ other detection monitors using GNSS-aided inertial systems [2].

1.3 Critical Aviation Applications Vulnerable to GNSS Spoofing

With its accurate, continuous, and global capabilities, GNSS offers seamless satellite navigation that meets the most stringent requirements for aviation users. Space-based positioning and navigation enables three-dimensional position determination for all phases of flight: departure, en route, approach, and landing.

Improved aircraft approaches to airports, which significantly increase operational accuracy, safety, and cost, are now being implemented even at remote locations where traditional Instrument Landing System (ILS) services are unavailable [36]. Such systems are called Ground Based Augmentation Systems (GBAS), where satellite sig-

nals are augmented with ground signals to assist flight categories (CAT) from CAT I precision approach to CAT III precision landing with guaranteed accuracy (at the meter level) and integrity [44]. A GBAS facility at each equipped airport provides local navigation satellite correction signals, and avionics in each aircraft process and provide guidance and control based on the satellite and GBAS signals. Other aviation applications such as autonomous airborne refueling, autonomous aircraft shipboard landing, formation flight etc., require centimeter-level accuracy. Such high-accuracy applications require relative GNSS positioning where raw GNSS measurements are transmitted between vehicles, and the inter-vehicle position differences are calculated [26, 24].

With the increase in use of GNSS in such mission-critical aviation applications, vulnerability of GNSS users to signal spoofing is a serious threat to positioning integrity 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 ATC system, and the corresponding reduction in reliance on ground-based radar systems by ATC. The spoofing detection methods and analysis introduced in this dissertation focus particularly on aircraft approach and landing using GBAS and relative GNSS positioning operations, since they are the most critical phases of flight. However, the same monitoring concepts can be applied to any other GNSS-based application, including terrestrial or maritime operations.

1.4 Background on Anti–Spoofing Methods

Numerous anti-spoofing techniques have been developed in the last decade and the strengths and vulnerabilities of these existing methods have been discussed in [19, 22, 41]. These include cryptographic authentication techniques employing modified GNSS navigation data [64, 27, 15]; spoofing discrimination using spatial processing by antenna arrays and automatic gain control schemes [1, 29, 35]; GNSS

signal direction of arrival comparison [31], code and phase rate consistency checks [34], high-frequency antenna motion [42], and signal power monitoring techniques [18, 63]. Some of these methods are indeed effective but they have some computational, logistical and physical limitations for aviation applications. For example, the spatial processing techniques increase the hardware complexity as it requires the installation of additional sophisticated antenna-arrays. Most of the powerful cryptographic authentication techniques require some modifications to the existing GNSS infrastructure, therefore they do not seem to be applicable in the short term. The direction of arrival discrimination and signal power monitoring methods require computationally intensive signal processing and are vulnerable to sophisticated spoofers who are capable of directional diversity in transmission and estimating the original signal power. Finally, the downside of using high frequency antenna motion for detection is that it requires the elimination of all the other vibration sources, which is practically impossible in an aircraft.

Augmenting data from auxiliary sensors such as Inertial Measurement Units (IMU), baro-altimeters, and independent radar sensors to discriminate spoofing has also been proposed in [62, 23, 53, 52]. The first thorough description of the performance of IMU-based monitoring against spoofing attacks in terms of integrity risk was introduced in [25]. In this dissertation, IMUs are investigated as a direct means of detecting GNSS spoofing attacks since they are co-located with GNSS receivers to support essentially all aerospace, terrestrial, and maritime navigation applications, and therefore do not require additional cost or modification to existing positioning systems.

1.5 RAIM–Based INS Monitor to Detect GNSS Spoofing Attacks

In this dissertation, we develop and evaluate novel spoofing monitors for GNSS-based navigation systems that are equipped with Inertial Navigation Systems

(INS). INS is a form of dead-reckoning that relies on IMU (accelerometers and gyroscopes) to measure specific force (acceleration) and angular velocity along 3 perpendicular axes [12]. An approximate position can be continuously determined in relation to a known starting position, velocity, and attitude (pitch, roll, yaw) by integrating these measurements over time. However, integration causes errors to grow over time, so in most of the navigation applications, GNSS receiver is coupled with INS for navigating, guiding and controlling vehicles. Depending on the INS quality (e.g., navigation, tactical, industrial, or automative-grade) and its integration scheme with GNSS receivers (e.g., tightly, loosely-coupled, or uncoupled), the vehicle estimator generally prioritizes GNSS solution when satellite signals are available. Upon GNSS signal interruption, INS dead-reckoning solution can be used to continue guidance.

Spoofing signals inject counterfeit pseudoranges into the receiver measurements. These measurements might be deceptive and consequently lead to an unreasonable position solution. Most GNSS receivers perform integrity monitoring when redundant satellites are available, to detect and exclude the inconsistent measurements, which is known as Receiver Autonomous Integrity Monitoring (RAIM) [39]. RAIM monitors the GNSS estimator residuals for fault detection, which is a rudimentary defense against spoofing. It is effective only in unsophisticated spoofing scenarios where only one or two GNSS signals among several authentic signals are spoofed; otherwise, if the majority of the GNSS signals are spoofed, it might reject the authentic measurements to decrease the residual, which is undesirable. In this dissertation, since we assume that all GNSS measurements can simultaneously be spoofed in the worst-case possible, the redundancy required for detection is provided through INS measurements, unlike conventional usage of RAIM where detection is provided through satellite redundancy.

1.6 Integrity Risk for Monitor Performance Evaluation

Table 1.1. Performance Requirements for Landing of Civil Aircraft [37, 51]

Phase of Flight	Alert Limits $(4-5\sigma)$		Integrity Risk
	Vertical	Horizontal	
En route	N/A	3.7 km	1×10^{-7}/h
En route Terminal	N/A	1.85 km	1×10^{-7}/h
Precision Approach CAT I	10 m	40 m	2×10^{-7}/150 s
Precision Landing CAT II-III	5.3 m	17 m	1×10^{-9}/150 s

To statistically evaluate the performance of the INS monitor, we compute the integrity risk, which is a measure of the reliability of the navigation solution [11]. Integrity risk is quantified as the probability that the system provides Hazardously Misleading Information (HMI) [43]. More specifically for the GNSS spoofing detection problem, HMI occurs when the position error exceeds a pre-defined alert limit, but the monitor does not trigger an alert.

The International Civil Aviation Organization (ICAO) identifies the standards for the most common aircraft approach modes, the associated alert limits, and the maximum integrity risk requirements as in Table 1.1. For example, the CAT I precision approach phase of the flight should be performed with integrity assurance such that undetected exceedance of 10 m vertical position error occurs no more frequently than once in 20 million approaches. In the performance evaluation and verification of the INS monitor conducted in this work, this particular set of requirements is used as the standard.

1.7 Dissertation Contributions

There are five main contributions in this dissertation, which are outlined in the following subsections.

1.7.1 Developing INS Monitors for GNSS Spoofers. We develop novel INS monitors for different INS/GNSS integration schemes including tightly-coupled,

loosely-coupled, and uncoupled. Their statistical reliability performances are evaluated and validated for several high-integrity GNSS aviation applications under worst-case spoofing attacks. A novel closed-form solution to the worst-case time sequence of GNSS fault is derived for each monitor and used in the performance analyses. The specific application of interest is aircraft precision approach and landing, but the methods introduced here are also applicable to other GNSS positioning systems that are co-located with inertial sensors.

1.7.2 Leveraging Vehicle Dynamics in Spoofing Detection. We quantify the INS monitor's sensitivity to the spoofer's inability to track high-frequency small disturbances (e.g., wind gusts and aircraft response to autopilot actions) on the actual aircraft trajectory. Spoofing integrity of the monitor is quantified by deriving the statistical dynamic response of an aircraft to a well-established vertical wind gust power spectrum. The main contribution is the development of a rigorous methodology to compute upper bounds on the integrity risk resulting from a worst-case spoofing attack – without needing to simulate individual aircraft approaches with an unmanageably large number of specific gust disturbance profiles (e.g., 10^9 to meet aircraft precision landing integrity requirements). In the gust analysis, a residual-based INS monitor is employed with a general batch estimator. Using the residual-based detector it is possible to analytically determine the worst-case sequence of the spoofed GNSS measurements – that is, the spoofed GNSS signal profile that maximizes integrity risk [20].

1.7.3 Accounting for Spoofers Capable of Tracking Position. The INS monitor is extended to tightly-coupled Kalman filter implementations, which are widely used in relative navigation applications such as aircraft shipboard landing. Its performance is verified against worst-case spoofing attacks, even when the spoofer has the ability to estimate the real-time position of the aircraft. Spoofing detection is accom-

plished by monitoring the Kalman filter innovations in tightly-coupled INS/GNSS mechanizations. Two main contributions here are the derivation of a mathematical framework to quantify the post-monitor spoofing integrity risk and an analytical expression of the worst-case sequence of spoofed GNSS signals, respectively. The simulation results show that GNSS spoofing is easily detected, with high integrity, unless the spoofer's position-tracking devices have unrealistic, near-perfect accuracy and no-delays.

1.7.4 Validating the INS Monitor for GBAS Landing System. Extending the methodology developed for the tightly-coupled INS monitor, we evaluate the performance of the INS monitor in the loosely-coupled integration which is prescribed in GBAS systems. Simulating a worst-case spoofing attack to GBAS-assisted final approaches of a Boeing 747, we show that the loosely-coupled INS monitor efficiently detects spoofing attacks with the integrity assurance satisfying the ICAO requirements. Also, the INS monitor performance in different INS/GNSS integrations is compared by quantifying trade-offs between the loosely and tightly-coupled navigation systems.

1.7.5 Relating Integrity Risk to INS Sensor Requirements. Even though loose and tight integration schemes are widely used for positioning during aircraft approaches and landings, in some en route general aviation (e.g., drones) and maritime (e.g., large ships) applications, standalone GNSS positioning is used for guidance [5]. In such implementations, GNSS spoofing monitoring can be performed by using INS that is uncoupled with GNSS.

The final contribution is the investigation of the impact of INS sensor quality on performance of the uncoupled INS monitor. To do that, we first derive the worst-case spoofing fault for a standalone GNSS receiver. Utilizing this during a terminal en route flight of Boeing 747, we then compute the integrity risk over time when

using the two different quality IMUs: a navigation-grade and a tactical-grade (lower quality), respectively. This sensitivity analysis determines the minimum IMU sensor (used in the uncoupled INS monitor) requirements to perform a standalone GNSS positioning with guaranteed spoofing integrity.

1.8 Dissertation Outline

After this introductory chapter, Chapter 2 constructs the GNSS measurement and INS kinematics models, and explains possible INS/GNSS integration schemes for vehicle guidance. Chapter 3 describes the INS airborne monitors (against GNSS spoofing) which are developed for navigation systems equipped with INS integrated with GNSS receivers in tightly-coupled, loosely-coupled, and uncoupled schemes. Chapter 4 quantifies the monitor's sensitivity to the spoofer's lack of knowledge of small disturbances (e.g., wind gusts) affecting the actual aircraft trajectory. Chapters 5 and 6 evaluate the performance of a more realistic Kalman filter-based monitor implementation for autonomous shipboard landing and GBAS-assisted aircraft approach and landing example applications, which are the major emphasis in this dissertation. An analytical expression of the worst-case fault is derived for the Kalman filter-based monitors. Finally, in Chapter 7, we investigate the impact of INS quality (e.g., tactical grade, navigation grade, etc.) on spoofing detection performance of an uncoupled INS monitor. The monitor performance is demonstrated with a spoofing attack to a standalone GNSS receiver supporting en route guidance. Finally, Chapter 8 provides conclusions and opportunities for future research.

CHAPTER 2

NAVIGATION SENSOR MODELS

This chapter presents the mathematical models of INS and GNSS to facilitate the later derivation of the GNSS/INS integration algorithms. Section 2.1 constructs the measurement models for standalone and differential GNSS implementations in mission-critical applications, which are highly susceptible to spoofing attacks. Within several GNSS constellations, we derive the measurement models for the most widely used civilian Global Positioning System (GPS) with emphasis on material relevant to the dissertation's topics. Section 2.2 describes the INS mechanization including a kinematic model of the user vehicle and an IMU measurement model. Then, the INS/GNSS integration schemes are briefly discussed in Section 2.4

2.1 GNSS Measurement Models

GPS provides two types of instantaneous measurements: the pseudorange code ρ and carrier phase ϕ, which are biased estimates of the range l between user and satellite. The ranging accuracy is limited by error sources including uncertainties in satellite clocks and positions, signal propagation delays in the ionosphere and troposphere, user receiver thermal noise and multipath. Some of the spatially correlated error sources (e.g., the ionosphere and troposphere) can be reduced to negligible levels in Differential GPS (DGPS) by using raw measurements or differential corrections broadcast from a nearby reference receiver, which is discussed in Sections 2.1.2 and 2.1.3. Depending on the GPS application and how these measurements are used, the total GPS positioning accuracy may range from a few centimeters (carrier-phase DGPS) to 10 meters or more (standalone GPS) [32].

The code phase measurement at the user receiver (denoted by the subscript

u) for satellite i is expressed as

$$\rho_u^i = l_u^i + \tau_u - \tau^i + I_u^i + T_u^i + M_{\rho_u}^i + \nu_{\rho_u}^i \tag{2.1}$$

where ρ_u^i is the L1 pseudorange raw measurement, l_u^i is the true range from the user receiver to the satellite, τ_u is the user receiver clock bias in units of length, τ^i is the satellite clock bias, I_u^i is the L1 ionospheric delay error, T_u^i is the tropospheric delay error, $\nu_{\rho_u}^i$ is the user receiver thermal noise, and $M_{\rho_u}^i$ is the code multipath in units of length.

The carrier phase measurement at the user receiver for satellite i is written as

$$\lambda\phi_u^i = l_u^i + \tau_u - \tau^i - I_u^i + T_u^i + \lambda N_u^i + M_{\phi_u}^i + \nu_{\phi_u}^i \tag{2.2}$$

where ϕ_u^i and N_u^i are the L1 carrier phase raw measurement and integer cycle ambiguity in units of cycles, respectively; λ, $\nu_{\phi_u}^i$, and $M_{\phi_u}^i$ are the L1 carrier signal wavelengths and receiver thermal noise, and multipath in units of length, respectively. It is commonly assumed that the receiver thermal noises ν_ρ and ν_ϕ are zero-mean and white random variables whereas the multipath errors M_ρ and M_ϕ are zero-mean colored noise sequences which are usually modeled with a first order Gauss Markov process having a time constant τ_m.

2.1.1 Standalone Systems. The term standalone GPS is used when the user position is estimated without using a reference station. In the absence of the reference station corrections, a user corrects the raw code phase (pseudorange) measurements ρ_u^i for the known errors using information available in navigation data messages broadcast from the satellites. These include estimates of satellite clock bias and ionospheric delay. Also, the tropospheric errors is attenuated by using a tropospheric model [38]. Although further correction can be achieved by smoothing the code using the carrier signal, and using dual frequency (L1-L2) signals [32], for simplicity we consider single frequency (L1) and code phase-only measurement model for the standalone systems.

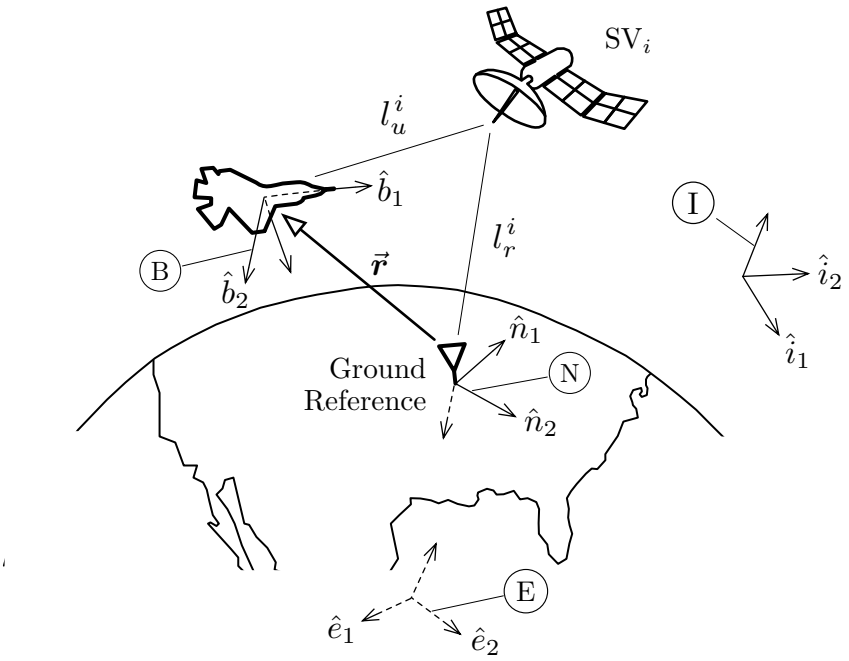

Figure 2.1. Satellite navigation coordinates including inertial frame (I), earth-centered earth-fixed frame (E), ground reference-fixed north-east-down navigation frame (N), and user vehicle-fixed body frame (B).

After correcting the L1 pseudorange for the signal errors using the navigation message, (2.1) is reduced to

$$\rho_{c,u}^i = l_u^i + \tau_u + M_{\rho_u}^i + \nu_{\rho_{c,u}}^i \tag{2.3}$$

where $\rho_{c,u}^i$ is the corrected L1 pseudorange measurement and $\nu_{\rho_{c,u}}^i$ is remaining residual error after the corrections (e.g., $1 \leq \sigma_{\nu_{\rho_{c,u}}} \leq 6$ m) [32].

Let $\boldsymbol{r}_u^{(n)}$ and $\boldsymbol{r}_i^{(n)}$ be the positions of the user receiver and satellite i relative the center of Earth, respectively. The superscripts with parenthesis on the vectors are used to indicate their frame of representation. In this work, it is selected as the navigation frame (N) fixed at a local ground reference (Figure 2.1) to be consistent with the INS mechanization, which is discussed in Section 2.2. Then, the true range l_u^i in (2.3) can be expressed as

$$l_u^i = \|\boldsymbol{r}_i^{(n)} - \boldsymbol{r}_u^{(n)}\|. \tag{2.4}$$

The satellite position $\boldsymbol{r}_i^{(n)}$ can be computed using the orbit ephemeris parameters in the navigation data message. Using the definition in (2.4) and a Taylor series expansion, the nonlinear measurement model in (2.3) can be linearized about a prior (nominal) assumed user state, $\boldsymbol{r}_u^{*(n)}$ and τ_u^* such that $\boldsymbol{l}_u^{*^i} = \|\boldsymbol{r}_i^{(n)} - \boldsymbol{r}_u^{*(n)}\|$; and the standalone measurement equation for k-visible satellites is expressed in vector form [32] as

$$\underbrace{\begin{bmatrix} \rho_{c,u}^1 - l_u^{*^1} - \tau_u^* \\ \vdots \\ \rho_{c,u}^k - l_u^{*^k} - \tau_u^* \end{bmatrix}}_{\boldsymbol{\rho}} = \underbrace{\begin{bmatrix} -\boldsymbol{e}_1^{(n)^T} \\ \vdots \\ -\boldsymbol{e}_k^{(n)^T} \end{bmatrix}}_{\boldsymbol{G}} \delta\boldsymbol{r}_u^{(n)} + \underbrace{\begin{bmatrix} 1 \\ \vdots \\ 1 \end{bmatrix}}_{\mathbf{1}} \delta\tau_u + \underbrace{\begin{bmatrix} M_{\rho_u}^1 \\ \vdots \\ M_{\rho_u}^k \end{bmatrix}}_{\boldsymbol{m}_\rho} + \underbrace{\begin{bmatrix} \nu_{\rho_{c,u}}^1 \\ \vdots \\ \nu_{\rho_{c,u}}^k \end{bmatrix}}_{\boldsymbol{\nu}_\rho} \tag{2.5}$$

where $\boldsymbol{e}_i^{(n)}$ is the line-of-sight unit vector from the prior position of the user $\boldsymbol{r}_u^{*(n)}$ to the known position $\boldsymbol{r}_i^{(n)}$ of the satellite i; $\delta\boldsymbol{r}_u^{(n)}$ and $\delta\tau_u$ are the deviations from the prior position and receiver clock bias of the user, respectively; $\boldsymbol{\nu}_\rho \sim \mathcal{N}(0, \boldsymbol{V}_\rho)$ is the standalone measurement error vector and its diagonal covariance matrix $\boldsymbol{V}_\rho$ is obtained from Table F.2. It should be noted that more accurate values of $l_u^{*^i}$'s $(1 \leq i \leq k)$ are obtained through iterated solutions of (2.5).

2.1.2 Relative Navigation Systems. Relative navigation is a specific DGPS implementation for high-precision critical applications. It can be implemented when a reference station (in the vicinity of the user) broadcasts its raw code ρ_r^i and carrier ϕ_r^i measurements to the user through a data link (Figure 2.2-a). The user incorporates these measurements to mitigate the GPS errors and estimate its position relative to the reference station. The reference station here is not necessarily a fixed station; it can be a moving platform such as the carrier ship for autonomous shipboard landing [26] or an aircraft for autonomous airborne refueling [24].

The following derivation is based on the relative positioning implementation of DGPS using the L1 frequency only. Similar to those in (2.1) and (2.2) for the user

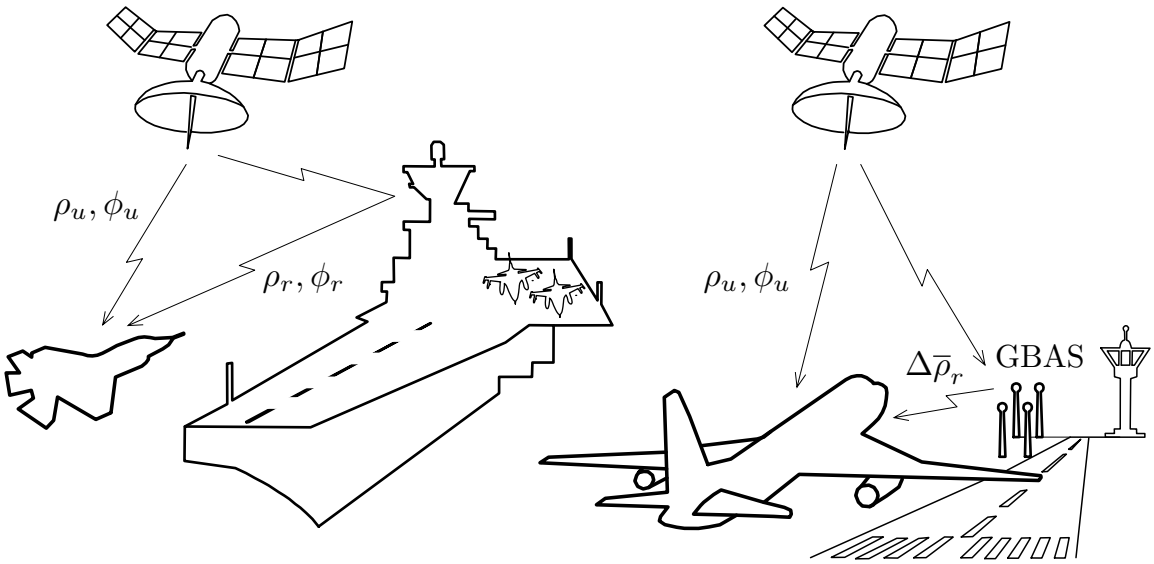

Figure 2.2. Examples of DGPS applications (a) Relative Navigation Systems – Autonomous precision shipboard landing and (b) Ground Based Augmentation Systems (GBAS) – Aircraft approach and landing.

receiver, the raw code and carrier phase measurements at the reference receiver are

$$\rho_r^i = l_r^i + \tau_r - \tau^i + I_r^i + T_r^i + M_{\rho_u}^i + \nu_{\rho_r}^i \tag{2.6}$$

$$\lambda\phi_r^i = l_r^i + \tau_r - \tau^i - I_r^i + T_r^i + \lambda N_r^i + M_{\phi_u}^i + \nu_{\phi_r}^i \tag{2.7}$$

where subscript r refers to the reference receiver.

When the user receives the time tagged reference station measurements, it forms differenced code and carrier phase measurements by subtracting its measurements from the reference measurements. Defining the first difference operation as $\triangle_{ur}^i = \triangle_u^i - \triangle_r^i$, the single difference (SD) code ρ_{ur}^i and carrier measurements ϕ_{ur}^i for the satellite i can be expressed as

$$\rho_{ur}^i = l_{ur}^i + \tau_{ur} + M_{\rho_{ur}}^i + \nu_{\rho_{ur}}^i \tag{2.8}$$

$$\lambda\phi_{ur}^i = l_{ur}^i + \tau_{ur} + \lambda N_{ur}^i + M_{\phi_{ur}}^i + \nu_{\phi_{ur}}^i. \tag{2.9}$$

One can eliminate the receiver clocks bias terms τ_{ur} in (2.8) and (2.9) by taking the difference of the single differences for the satellites i and j, which is referred to as double differencing (DD) (i.e., $\triangle^{ij}_{ur} = \triangle^{i}_{ur} - \triangle^{j}_{ur}$).

Assuming $\|\vec{\boldsymbol{r}}\| \ll l^i_r$ in Figure 2.1, the true range difference l^i_{ur} in (2.9) can be approximated in terms of $\vec{\boldsymbol{r}}$ (the vector from the reference to the user receiver) as $l^i_{ur} = -\boldsymbol{e}^{(n)^T}_i \boldsymbol{r}^{(n)}$. Then, differencing all the measurements from the satellite 1, the linearized DD code ρ^{i1}_{ur} and carrier measurements ϕ^{i1}_{ur} for k visible satellites ($2 \le i \le k$) can be stacked in vector form as

$$\underbrace{\begin{bmatrix} \rho^{21}_{ur} \\ \vdots \\ \rho^{k1}_{ur} \\ \hline \lambda\phi^{21}_{ur} \\ \vdots \\ \lambda\phi^{k1}_{ur} \end{bmatrix}}_{\boldsymbol{z}'_{\rho\phi}} = \underbrace{\begin{bmatrix} -(\boldsymbol{e}^{(n)}_2 - \boldsymbol{e}^{(n)}_1)^T \\ \vdots \\ -(\boldsymbol{e}^{(n)}_k - \boldsymbol{e}^{(n)}_1)^T \\ \hline -(\boldsymbol{e}^{(n)}_2 - \boldsymbol{e}^{(n)}_1)^T \\ \vdots \\ -(\boldsymbol{e}^{(n)}_k - \boldsymbol{e}^{(n)}_1)^T \end{bmatrix}}_{\boldsymbol{G}_{\rho\phi}} \boldsymbol{r}^{(n)} + \underbrace{\begin{bmatrix} 0 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 0 \\ \hline \lambda & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \lambda \end{bmatrix}}_{\boldsymbol{D}} \underbrace{\begin{bmatrix} N^{21}_{ur} \\ \vdots \\ N^{k1}_{ur} \end{bmatrix}}_{\boldsymbol{n}_{\rho\phi}} + \underbrace{\begin{bmatrix} \mathrm{M}^{21}_{\rho_{ur}} \\ \vdots \\ \mathrm{M}^{k1}_{\rho_{ur}} \\ \hline \mathrm{M}^{21}_{\phi_{ur}} \\ \vdots \\ \mathrm{M}^{k1}_{\phi_{ur}} \end{bmatrix}}_{\boldsymbol{m}_{\rho\phi}} + \underbrace{\begin{bmatrix} \nu^{21}_{\rho_{ur}} \\ \vdots \\ \nu^{k1}_{\rho_{ur}} \\ \hline \nu^{21}_{\phi_{ur}} \\ \vdots \\ \nu^{k1}_{\phi_{ur}} \end{bmatrix}}_{\boldsymbol{\nu}_{\rho\phi}} \tag{2.10}$$

where $\boldsymbol{\nu}_{\rho\phi} \sim \mathcal{N}(0, \boldsymbol{V}_{\rho\phi})$ is the DD receiver thermal noise error vector and its covariance matrix $\boldsymbol{V}_{\rho\phi}$ is obtained using the SD standard deviations given in Table F.2; $\boldsymbol{m}_{\rho\phi} \sim \mathcal{N}(0, \boldsymbol{P}_{m_{\rho\phi}})$ is the DD multipath error vector having a covariance matrix of $\boldsymbol{P}_{m_{\rho\phi}}$, and $\boldsymbol{n}_{\rho\phi}$ is the DD integer cycle ambiguity state vector.

For consistency with INS kinematics linearized about a nominal trajectory, which will be explained in Section 2.2, we define $\boldsymbol{r}^{(n)} = \boldsymbol{r}^{*^{(n)}} + \delta\boldsymbol{r}^{(n)}$ where $\boldsymbol{r}^{*^{(n)}}$ is the nominal user position relative to the reference position, and use the perturbation form of (2.10) as

$$\underbrace{\boldsymbol{z}'_{\rho\phi} - \boldsymbol{G}_{\rho\phi}\boldsymbol{r}^{*^{(n)}}}_{\boldsymbol{z}_{\rho\phi}} = \boldsymbol{G}_{\rho\phi}\,\delta\boldsymbol{r}^{(n)} + \boldsymbol{D}\,\boldsymbol{n}_{\rho\phi} + \boldsymbol{m}_{\rho\phi} + \boldsymbol{\nu}_{\rho\phi}. \tag{2.11}$$

2.1.3 Ground Based Augmentation Systems. Ground Based Augmentation

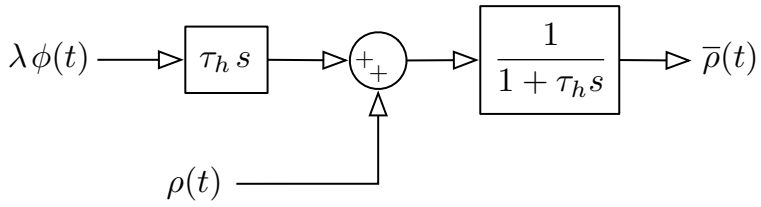

Figure 2.3. Block diagram of the continuous carrier-smoothing system (Hatch filter). The inputs $\rho(t)$ and $\lambda\phi(t)$ are the code and carrier measurements, respectively. The output of the filter $\overline{\rho}(t)$ is the carrier-smoothed code measurement. τ_h is the filter time constant.

Systems (GBAS) are a specific application of code-based DGPS technology which serves as the next generation navigation aid for aircraft precision approach and landing with the objective to replace current Instrument Landing System (ILS).

GBAS is composed of three primary subsystems (Figure 2.2-b): a) satellites, which produce ranging signals; b) ground, which provides a broadcast containing differential corrections; c) airborne Position and Navigation (PAN) equipment, which receives and processes the GBAS signals to compute and output a position solution. The ground and PAN simultaneously run smoothing (Hatch) filters (Figure 2.3) to obtain carrier-smoothed pseudoranges with a filter time constant $\tau_h = 100$ s. The ground broadcasts differential corrections $\Delta\overline{\rho}_r^i$ for the carrier-smoothed code, which are used to correct the airborne carrier-smoothed code $\overline{\rho}_u^i$ [49].

The differentially corrected smoothed code $\overline{\rho}_{c,u}^i = \overline{\rho}_u^i + \Delta\overline{\rho}_r^i$ is expressed as

$$\overline{\rho}_{c,u}^i = l_u^i + \tau_u + \nu_{\overline{\rho}_{c,u}}^i \tag{2.12}$$

and the linearized form of (2.12) for k visible satellites can be stacked to form the GBAS measurement model as

$$\underbrace{\begin{bmatrix} \overline{\rho}_{c,u}^1 - l_u^{*1} - \tau_u^* \\ \vdots \\ \overline{\rho}_{c,u}^k - l_u^{*k} - \tau_u^* \end{bmatrix}}_{\overline{\boldsymbol{\rho}}} = \underbrace{\begin{bmatrix} -\boldsymbol{e}_1^{(n)^T} \\ \vdots \\ -\boldsymbol{e}_n^{(n)^T} \end{bmatrix}}_{\boldsymbol{G}} \delta\boldsymbol{r}_u^{(n)} + \underbrace{\begin{bmatrix} 1 \\ \vdots \\ 1 \end{bmatrix}}_{\mathbf{1}} \delta\tau_u + \underbrace{\begin{bmatrix} \nu_{\overline{\rho}_{c,u}}^1 \\ \vdots \\ \nu_{\overline{\rho}_{c,u}}^k \end{bmatrix}}_{\boldsymbol{\nu}_{\overline{\rho}}} \tag{2.13}$$

where $\boldsymbol{\nu}_{\bar{\rho}} \sim \mathcal{N}(0, \boldsymbol{V}_{\bar{\rho}})$ contains the ground, airborne, and signal-in-space errors and its diagonal covariance matrix $\boldsymbol{V}_{\bar{\rho}}$ is defined as a function of elevation of each satellite in Appendix C. It should be mentioned after the carrier-smoothing and differential corrections, the integer cycle ambiguities drop out and receiver thermal noise and multipath on the code are smoothed and attenuated since the Hatch filter time constant is to be larger than the multipath time constant (i.e. $\tau_h > \tau_m$).

2.2 INS Mechanization

INS is a self-contained dead reckoning navigation system based on integrating acceleration and angular rate measurements from the IMU to provide user position, velocity and attitude information over time. INS mechanization equations represent a kinematic model where the inputs are the IMU measurements (inertial acceleration and angular velocity), and the outputs are the aircraft's position, velocity and attitude in a frame of interest. In this section, we derive the kinematic model and describe how to relate it to the IMU measurement model.

2.2.1 INS Kinematic Model. Before starting linearization of INS kinematics, the main assumptions are:

1. Since the main motivation of this work is detecting GNSS spoofing attacks in aircraft landing approaches, we integrate INS with DGNSS. For consistency and simplicity in the derivation of the mechanization equations, we define the frame of interest (navigation frame) as being fixed at a reference station (e.g., airport-based GBAS station, shipboard platform etc.) having axes in the north, east, and down directions as in Figure 2.1.
2. The position vector $\boldsymbol{r}$ of the aircraft in the mechanization equations is with respect to the position of the reference station.
3. The velocity of the aircraft $\boldsymbol{v}$ is not the inertial velocity but the ground velocity.

4. The 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, the nonlinear kinematic equations of the aircraft [12] can be obtained as

$$\dot{\boldsymbol{x}}_n \triangleq \begin{bmatrix} \dot{\boldsymbol{r}}^{(n)} \\ \dot{\boldsymbol{v}}^{(n)} \\ \dot{\boldsymbol{E}}^{(n)} \end{bmatrix} = \begin{bmatrix} \boldsymbol{v}^{(n)} \\ {}^{N}\boldsymbol{R}^{B}\mathbf{f}^{(b)} - 2\boldsymbol{\omega}_{ie_\times}^{(n)}\boldsymbol{v}^{(n)} + \boldsymbol{g}^{(n)} \\ \boldsymbol{Q}_{BE}^{-1}\big(\boldsymbol{\omega}_{ib}^{(b)} - {}^{B}\boldsymbol{R}^{N}\boldsymbol{\omega}_{ie}^{(n)}\big) \end{bmatrix} \tag{2.14}$$

where the INS state vector $\boldsymbol{x}_n$ is composed of position $\boldsymbol{r}$ relative to reference station, ground velocity $\boldsymbol{v}$, and attitude (Euler angles) $\boldsymbol{E}$. Also, ${}^{N}\boldsymbol{R}^{B}$ is the rotation matrix from body to navigation frame, $\boldsymbol{Q}_{BE}$ is the matrix that transforms Euler angle rates to body rotation rates [12], and $\boldsymbol{\omega}_{ie}$ and $\boldsymbol{\omega}_{ib}$ are the angular velocity vectors of earth and angular velocity of body with respect to I-frame, respectively. $\boldsymbol{\omega}_{ie_\times}$ is the skew symmetric matrix form of $\boldsymbol{\omega}_{ie}$, and $\mathbf{f}$ and $\boldsymbol{g}$ are the specific force and gravitational acceleration acting on the aircraft, respectively. Note that the superscripts with parentheses refer to the frame in which the vector is expressed (see Figure 2.1).

The INS kinematic model is linearized about a nominal constant velocity trajectory assuming small deviations about the nominal trajectory. Expressing all the variables in (2.14) in perturbation form, the position and velocity error equations become [12]

$$\delta\dot{\boldsymbol{r}}^{(n)} = \delta\boldsymbol{v}^{(n)} \tag{2.15}$$

$$\delta\dot{\boldsymbol{v}}^{(n)} = {}^{N}\boldsymbol{R}^{B^*}\mathbf{f}_{\times}^{*(b)}\delta\boldsymbol{E} + {}^{N}\boldsymbol{R}^{B^*}\delta\mathbf{f}^{(b)} - 2\boldsymbol{\omega}_{ie_\times}^{(n)}\delta\boldsymbol{v}^{(n)} \tag{2.16}$$

where $\mathbf{f}_{\times}^{*(b)}$ is the skew symmetric matrix form of specific force acting on aircraft flying along the nominal trajectory, and ${}^{N}\boldsymbol{R}^{B^*}$ is the rotation matrix from the nominal B-frame to N-frame.

Unlike the widely used techniques in [12, 45, 61], we use a different method for the attitude linearization that is more consistent with the velocity and position linearizations and is easier to implement in the dissertation's specific applications of interest. Extracting the last row of (2.14) gives the nonlinear attitude equation as

$$\dot{\boldsymbol{E}}^{(n)} = \boldsymbol{Q}_{BE}^{-1} \underbrace{\left[\boldsymbol{\omega}_{ib}^{(b)} - {}^{B}\boldsymbol{R}^{N}\boldsymbol{\omega}_{ie}^{(n)}\right]}_{\boldsymbol{s}}. \tag{2.17}$$

Knowing that the transformation matrices ${}^{B}\boldsymbol{R}^{N}$ and $\boldsymbol{Q}_{BE}$ in (2.17) are functions of attitude vector $\boldsymbol{E}^{(n)}$ (i.e., Euler angles) and using the definition of $\boldsymbol{s}$ in (2.17), we can expand the deviation in attitude rate $\delta\dot{\boldsymbol{E}}^{(n)}$ using a Taylor Series to linearize the attitude equation as

$$\delta\dot{\boldsymbol{E}}^{(n)} = \boldsymbol{Q}_{BE}^{*-1}\,\delta\boldsymbol{\omega}_{ib}^{(b)} + \underbrace{\begin{bmatrix} \boldsymbol{s}^{*^T} & 0 & 0 \\ 0 & \boldsymbol{s}^{*^T} & 0 \\ 0 & 0 & \boldsymbol{s}^{*^T} \end{bmatrix}}_{\boldsymbol{S}^{*}} \delta\boldsymbol{Q}_{BE}^{-1} + \underbrace{\begin{bmatrix} \boldsymbol{\omega}_{ie}^{(n)^T} & 0 & 0 \\ 0 & \boldsymbol{\omega}_{ie}^{(n)^T} & 0 \\ 0 & 0 & \boldsymbol{\omega}_{ie}^{(n)^T} \end{bmatrix}}_{\boldsymbol{W}_{ie}} \delta{}^{B}\boldsymbol{R}^{N} \tag{2.18}$$

where $\boldsymbol{s}^{*}$ is the nominal value of $\boldsymbol{s}$ and $\delta\boldsymbol{Q}_{BE}^{-1}$ and $\delta{}^{B}\boldsymbol{R}^{N}$ can be written in terms of $\delta\boldsymbol{E}^{(n)}$ as

$$\delta\boldsymbol{Q}_{BE}^{-1} = \left.\frac{\partial\boldsymbol{Q}_{BE}^{-1}}{\partial\boldsymbol{E}^{(n)}}\right|_{*} \delta\boldsymbol{E}^{(n)} \tag{2.19}$$

and

$$\delta{}^{B}\boldsymbol{R}^{N} = \left.\frac{\partial{}^{B}\boldsymbol{R}^{N}}{\partial\boldsymbol{E}^{(n)}}\right|_{*} \delta\boldsymbol{E}^{(n)}, \tag{2.20}$$

respectively. Let us define a matrix $\boldsymbol{K}^{*}$ containing only constant nominal parameters as

$$\boldsymbol{K}^{*} = \boldsymbol{S}^{*} \left.\frac{\partial\boldsymbol{Q}_{BE}^{-1}}{\partial\boldsymbol{E}^{(n)}}\right|_{*} + \boldsymbol{W}_{ie} \left.\frac{\partial{}^{B}\boldsymbol{R}^{N}}{\partial\boldsymbol{E}^{(n)}}\right|_{*} \tag{2.21}$$

where defining the attitude vector (3×1) as $\boldsymbol{E}^{(n)} = [\xi, \theta, \psi]^{T}$ where ξ, θ, and ψ are the roll, pitch, and yaw angles, respectively; the partial derivatives (9×3) can be obtained as

$$\frac{\partial\boldsymbol{Q}_{BE}^{-1}}{\partial\boldsymbol{E}^{(n)}} = \begin{bmatrix} \dfrac{\partial\boldsymbol{Q}_{BE}^{-1}}{\partial\xi} & \dfrac{\partial\boldsymbol{Q}_{BE}^{-1}}{\partial\theta} & \dfrac{\partial\boldsymbol{Q}_{BE}^{-1}}{\partial\psi} \end{bmatrix}^{T} \tag{2.22}$$

and

$$\frac{\partial^B \boldsymbol{R}^N}{\partial \boldsymbol{E}^{(n)}} = \begin{bmatrix} \dfrac{\partial^B \boldsymbol{R}^N}{\partial \xi} & \dfrac{\partial^B \boldsymbol{R}^N}{\partial \theta} & \dfrac{\partial^B \boldsymbol{R}^N}{\partial \psi} \end{bmatrix}^T, \tag{2.23}$$

respectively. Substituting (2.19), (2.20), and (2.21) into (2.18) yields attitude error equation as

$$\delta \dot{\boldsymbol{E}}^{(n)} = \boldsymbol{Q}_{BE}^{*-1}\, \delta \boldsymbol{\omega}_{ib}^{(b)} + \boldsymbol{K}^* \delta \boldsymbol{E}^{(n)}. \tag{2.24}$$

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

$$\begin{bmatrix} \delta \dot{\boldsymbol{r}}^{(n)} \\ \delta \dot{\boldsymbol{v}}^{(n)} \\ \delta \dot{\boldsymbol{E}}^{(n)} \end{bmatrix} = \underbrace{\begin{bmatrix} 0 & 1 & 0 \\ 0 & -2\boldsymbol{\omega}_{ie_\times}^{(n)} & {}^N\boldsymbol{R}^{B^*} \mathbf{f}_\times^{*(b)} \\ 0 & 0 & \boldsymbol{K}^* \end{bmatrix}}_{\boldsymbol{F}_n} \underbrace{\begin{bmatrix} \delta \boldsymbol{r}^{(n)} \\ \delta \boldsymbol{v}^{(n)} \\ \delta \boldsymbol{E}^{(n)} \end{bmatrix}}_{\boldsymbol{x}_n} + \underbrace{\begin{bmatrix} 0 & 0 \\ {}^N\boldsymbol{R}^{B^*} & 0 \\ 0 & \boldsymbol{Q}_{BE}^{*-1} \end{bmatrix}}_{\boldsymbol{G}_u} \underbrace{\begin{bmatrix} \delta \mathbf{f}^{(b)} \\ \delta \boldsymbol{\omega}_{ib}^{(b)} \end{bmatrix}}_{\boldsymbol{u}} \tag{2.25}$$

where $\boldsymbol{x}_n$ is referred to as the INS kinematic state vector, $\boldsymbol{F}_n$ is the plant matrix of the kinematic model, $\boldsymbol{G}_u$ is the input coefficient matrix, and $\boldsymbol{u}$ is the variation of IMU measurements from the nominal values, which are the deviations in specific force and angular velocity of the aircraft. Note that all the superscripts $*$ refer to constant matrices evaluated at nominal values.

2.2.2 IMU Measurement Model. A strapdown IMU typically consists of three gyroscopes and three accelerometers rigidly and orthogonally mounted on a sensor frame installed on a vehicle. They measure the deviations in specific force and angular velocity, and the IMU measurement $\tilde{\boldsymbol{u}}$ is expressed in terms of $\boldsymbol{u}$ in (2.25) as

$$\tilde{\boldsymbol{u}} = \boldsymbol{u} + \boldsymbol{b} + \boldsymbol{\nu}_n \tag{2.26}$$

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

$$\dot{\boldsymbol{b}} = \boldsymbol{F}_b\, \boldsymbol{b} + \boldsymbol{\eta}_b \tag{2.27}$$

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

Using (2.26), we augment the IMU dynamics in (2.27) with the kinematic model in (2.25), which yields

$$\begin{bmatrix} \dot{\boldsymbol{x}}_n \\ \dot{\boldsymbol{b}} \end{bmatrix} = \underbrace{\begin{bmatrix} \boldsymbol{F}_n & -\boldsymbol{G}_u \\ 0 & \boldsymbol{F}_b \end{bmatrix}}_{\boldsymbol{F}} \underbrace{\begin{bmatrix} \boldsymbol{x}_n \\ \boldsymbol{b} \end{bmatrix}}_{\boldsymbol{x}} + \underbrace{\begin{bmatrix} \boldsymbol{G}_u \\ 0 \end{bmatrix}}_{\boldsymbol{G}_{\tilde{u}}} \tilde{\boldsymbol{u}} + \underbrace{\begin{bmatrix} -\boldsymbol{G}_u & 0 \\ 0 & \boldsymbol{I} \end{bmatrix}}_{\boldsymbol{G}_w} \underbrace{\begin{bmatrix} \boldsymbol{\nu}_n \\ \boldsymbol{\eta}_b \end{bmatrix}}_{\boldsymbol{w}}. \tag{2.28}$$

Defining $\overline{\boldsymbol{w}} = \boldsymbol{G}_w \boldsymbol{w}$, the discrete form of the INS model in (2.28) is written as

$$\boldsymbol{x}_k = \boldsymbol{\Phi}\, \boldsymbol{x}_{k-1} + \boldsymbol{\Gamma}\, \tilde{\boldsymbol{u}}_{k-1} + \overline{\boldsymbol{w}}_{k-1} \tag{2.29}$$

where $\boldsymbol{\Phi}$ is the state transition matrix of the process model $\boldsymbol{F}$, $\boldsymbol{\Gamma}$ is the discrete form of $\boldsymbol{G}_{\tilde{u}}$ using a zero-order-hold on the input, $\overline{\boldsymbol{w}}_k \sim \mathcal{N}(0, \overline{\boldsymbol{W}}_k)$ is the augmented process noise, and $\overline{\boldsymbol{W}}_k$ is the covariance matrix of $\overline{\boldsymbol{w}}_k$. The IMU measurement $\tilde{\boldsymbol{u}}_k$ is a deterministic input to the INS model in (2.29), which may be induced by external inputs or disturbances such as autopilot commands and wind gusts.

2.3 IMU Grades

Inertial sensors can be grouped into one of the following four performance categories: 1) Marine/Navigation, 2) Tactical, 3) Industrial, and 4) Consumer/Automative grades [10]. Except for INS systems customized for long-range strategic ballistic missiles, the marine-grade is the best commercially available IMU, typically used on ships, submarines, and some spacecraft, providing an unaided solution that drifts less than 1.8 km per day. Navigation (or aviation) grade has slightly lower accuracy than the marine grade and are typically used on commercial airliners and military aircraft. A navigation grade IMUs are designed to satisfy a maximum position drift of 1.5 km in the first hour of operation [61]. Unlike the marine and navigation-grade IMUs which are suitable for long-range guidance, a tactical-grade IMU can only provide useful inertial navigation for only a few minutes. However, long-term guidance can be achieved by integrating it with GPS. These systems are typically used in guided weapons and unmanned aerial vehicles (UAV).

Table 2.1. The effect of IMU grade in horizontal position drifts over several operation durations [28]

IMU Grade	10 sec	1 min	1 hr
Navigation	12 mm	0.44 m	1.6 km
Tactical	150 mm	5.3 m	19 km
Industrial	1.5 m	53 m	190 km
Automative	60 m	2.2 km	7900 km

The lowest grade of inertial sensors is often referred to as automotive grade, which are not accurate enough even when integrated with other navigation systems such as GPS. Typically these sensors are used as part of an industrial (MEMS) grade sensor, or just as a motion detector such as anti-lock braking systems. The main difference between automotive and industrial grade IMUs is due to the quality of sensor calibration. Smartphone applications use industrial grade sensors. Sometimes, the same industrial grade IMU is sold as automotive grade without calibration. Table 2.1 is an overview of the typical errors in horizontal position for each grade of IMU.

2.4 INS/GNSS Integration Schemes and Related Applications

It is widely known that INS is complementary to GNSS since it is impervious to jamming, spoofing, and blockage of radio signals; therefore, INS systems are crucial to help maintain GPS navigation integrity and continuity. Also, the INS coupling with GPS provides a navigation solution that has the high bandwidth of the inertial sensors, which improves the performance of controller (i.e., autopilot). On the other hand, the position output of GPS when it is available, is stable and reliable whereas INS position outputs drift over time due to the integration of imperfect measurement errors. Nevertheless, the two systems, for example, can be coupled in such a way that INS errors are calibrated by GPS when satellite signals are available. As a result, any subsequent temporary GPS signal outage can be bridged by relatively accurate INS position outputs.

GPS and INS can be coupled using a variety of integration schemes. These range from simple loosely coupled integration to complex ultra-tightly coupled methods in which the INS directly aids the GNSS tracking loops [61]. In this work, we focus on the most widely used implementations in aerospace, terrestrial, and maritime navigation application: 1) tight 2) loose, and 3) uncoupled integrations. The tightly-coupled integration is a well-established method that is suitable for relative navigation systems (e.g., aircraft shipboard landing, autonomous airborne refueling, formation flight etc.) where both raw differential code and carrier measurements are available at the user. These raw DGNSS measurements are directly fed into INS through a Kalman filter. This provides far superior performance to loosely coupled systems but without the excessive cost and complexity of the ultra-tight systems. Unlike the relative navigation systems, for the local area augmentation systems (e.g., GBAS-assisted aircraft landing etc.) where only the DGNSS output position estimates are provided to the user as a navigation solution, the loosely coupled integration is unavoidable. The advantage of the loose integration method is mainly its simplicity in implementation relative to the tightly coupled integration. Although the loose and tight integration strategies are the most commonly used methods, in some maritime and general aviation en route navigation applications (e.g., drones, autonomous cruise boats and large ships etc.), the coarse autopilot is typically driven by GNSS feedback, which is not coupled with INS [5]. Uncoupled integration implies no data feedback from either instrument to the other. The details of these integration schemes are presented when introducing the proposed INS monitors against GNSS deceptions in Chapter 3.

CHAPTER 3

INS AIRBORNE MONITORS AGAINST GNSS SPOOFERS

This chapter introduces novel airborne monitors (detectors) that operate continuously to detect spoofing attacks on GNSS receivers by using INS measurements. The proposed detectors here are simple and efficient and can be directly implemented on top of any type of INS/GNSS integration (e.g., tightly, loosely-coupled, and uncoupled) without requiring any modification to the existing compensator system.

operates continuously

3.1 Kalman Filter Innovations–Based Monitors

In this section, we propose an innovations-based monitor for systems where INS and GNSS are coupled (loosely or tightly) in a Kalman filter to obtain state estimates (position, velocity, and attitude) feeding an autopilot. Spoofing detection is accomplished by monitoring the Kalman filter innovations. First, the tightly and loosely-coupled estimators are briefly explained, which will be needed later for the performance evaluation of the monitor; then, the detector algorithm for them is defined.

3.1.1 Tightly–Coupled INS/GNSS Estimator. Tightly-coupled mechanization of INS/GNSS through a Kalman filter is widely used in relative navigation systems applications [26]. The estimator introduced in this section is an example implementation where both differential code and carrier measurements are available to the user, which is also equipped with inertial sensors (i.e., IMU).

Recalling that the DD GNSS measurement equation and INS model were pre-

viously derived (2.11) and (2.29) as

$$\boldsymbol{z}_{\rho\phi_k} = \boldsymbol{G}_{\rho\phi}\,\delta\boldsymbol{r}_k + \boldsymbol{D}\,\boldsymbol{n}_{\rho\phi_k} + \boldsymbol{m}_{\rho\phi_k} + \boldsymbol{\nu}_{\rho\phi_k} \tag{3.1}$$

and

$$\boldsymbol{x}_k = \boldsymbol{\Phi}\,\boldsymbol{x}_{k-1} + \boldsymbol{\Gamma}\,\tilde{\boldsymbol{u}}_{k-1} + \overline{\boldsymbol{w}}_{k-1}, \tag{3.2}$$

respectively, where $\boldsymbol{x}_k = \left[\delta\boldsymbol{r}_k, \delta\boldsymbol{v}_k, \delta\boldsymbol{E}_k, \boldsymbol{b}_k\right]^T$. It should be mentioned that the multipath $\boldsymbol{m}_{\rho\phi}$ in (3.1) can be modeled as a first order Gauss Markov process and the cycle ambiguity $\boldsymbol{n}_{\rho\phi}$ in (3.1) is constant assuming there are no cycle slips.

Defining a vector $\boldsymbol{x}'_k = \left[\delta\boldsymbol{v}_k, \delta\boldsymbol{E}_k, \boldsymbol{b}_k\right]^T$, the DD GNSS ranging measurements in (3.1) and INS model in (3.2) can be tightly coupled through a unified Kalman filter with the measurement equation

$$\boldsymbol{z}_{\rho\phi_k} = \underbrace{\begin{bmatrix}\boldsymbol{G}_{\rho\phi} & 0 & \boldsymbol{I} & \boldsymbol{D}\end{bmatrix}}_{\boldsymbol{H}_k} \underbrace{\begin{bmatrix}\delta\boldsymbol{r}_k \\ \boldsymbol{x}'_k \\ \boldsymbol{m}_{\rho\phi_k} \\ \boldsymbol{n}_{\rho\phi_k}\end{bmatrix}}_{\mathbf{x}_k} + \boldsymbol{\nu}_{\rho\phi_k} \tag{3.3}$$

where $\boldsymbol{H}_k$ is the observation matrix of the augmented measurement model, and a process model of

$$\begin{bmatrix}\boldsymbol{x}_k \\ \boldsymbol{m}_{\rho\phi_k} \\ \boldsymbol{n}_{\rho\phi_k}\end{bmatrix} = \underbrace{\begin{bmatrix}\boldsymbol{\Phi} & 0 & 0 \\ 0 & \boldsymbol{\Phi}_m & 0 \\ 0 & 0 & \boldsymbol{I}\end{bmatrix}}_{\boldsymbol{\Phi}_\mathrm{x}} \underbrace{\begin{bmatrix}\boldsymbol{x}_{k-1} \\ \boldsymbol{m}_{\rho\phi_{k-1}} \\ \boldsymbol{n}_{\rho\phi_{k-1}}\end{bmatrix}}_{\mathbf{x}_{k-1}} + \underbrace{\begin{bmatrix}\boldsymbol{\Gamma} \\ 0 \\ 0\end{bmatrix}}_{\boldsymbol{\Gamma}_\mathrm{x}} \tilde{\boldsymbol{u}}_{k-1} + \underbrace{\begin{bmatrix}\overline{\boldsymbol{w}}_{k-1} \\ \boldsymbol{\nu}_{m_{k-1}} \\ 0\end{bmatrix}}_{\boldsymbol{w}_{\mathrm{x}_{k-1}}} \tag{3.4}$$

where $\boldsymbol{\Phi}_m$ is a diagonal multipath state transition matrix, the elements of which are $e^{-\Delta t/\tau_m}$ where τ_m and Δt are the multipath time constant and sampling time, respectively, $\boldsymbol{\nu}_m$ is the DD multipath driving noise vector which is white and its covariance matrix $\boldsymbol{V}_m$ can be obtained using the SD standard deviations given in Table F.2. $\boldsymbol{w}_{\mathrm{x}_k} \sim \mathcal{N}(0, \boldsymbol{W}_{\mathrm{x}_k})$ is the augmented process noise having a covariance of $\boldsymbol{W}_{\mathrm{x}_k}$. The Kalman filter state vector $\mathbf{x}_k$ in Equations (3.3) and (3.4) contains the INS states augmented with DD GNSS multipath and cycle ambiguity states.

Given the measurement model in (3.3) and the process model in (3.4), the Kalman filter time update is

$$\overline{\mathbf{x}}_k^{\mathrm{KF}} = \mathbf{\Phi}_{\mathrm{x}}\hat{\mathbf{x}}_{k-1}^{\mathrm{KF}} + \mathbf{\Gamma}_{\mathrm{x}}\tilde{\boldsymbol{u}}_{k-1} \tag{3.5}$$

where $\overline{\mathbf{x}}_k^{\mathrm{KF}}$ and $\hat{\mathbf{x}}_{k-1}^{\mathrm{KF}}$ are the *a priori* estimate of $\mathbf{x}$ at time epoch k and *a posteriori* estimate of $\mathbf{x}$ at $k-1$, respectively. The measurement update at time epoch k gives the a posteriori estimate $\hat{\boldsymbol{x}}_k$ as

$$\hat{\mathbf{x}}_k^{\mathrm{KF}} = \overline{\mathbf{x}}_k^{\mathrm{KF}} + \boldsymbol{L}_k\big(\boldsymbol{z}_{\rho\phi_k} - \boldsymbol{H}_k\overline{\mathbf{x}}_k^{\mathrm{KF}}\big) \tag{3.6}$$

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

$$\boldsymbol{L}_k = \hat{\boldsymbol{P}}_{\mathrm{x}_k}\boldsymbol{H}_k^T\boldsymbol{V}_{\rho\phi_k}^{-1} \tag{3.7}$$

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

$$\hat{\boldsymbol{P}}_{\mathrm{x}_k} = \big(\overline{\boldsymbol{P}}_{\mathrm{x}_k}^{-1} + \boldsymbol{H}_k^T\boldsymbol{V}_{\rho\phi_k}^{-1}\boldsymbol{H}_k\big)^{-1} \tag{3.8}$$

and $\overline{\boldsymbol{P}}_k$ is the pre-measurement state estimate error covariance matrix at time k, computed as

$$\overline{\boldsymbol{P}}_{\mathrm{x}_k} = \mathbf{\Phi}_{\mathrm{x}}\hat{\boldsymbol{P}}_{\mathrm{x}_{k-1}}\mathbf{\Phi}_{\mathrm{x}}^T + \boldsymbol{W}_{\mathrm{x}_{k-1}}. \tag{3.9}$$

The innovation vector $\boldsymbol{\gamma}$ of the Kalman filter at time epoch k is

$$\boldsymbol{\gamma}_k = \boldsymbol{z}_{\rho\phi_k} - \boldsymbol{H}_k\overline{\mathbf{x}}_k^{\mathrm{KF}} \tag{3.10}$$

where $\overline{\mathbf{x}}_k^{\mathrm{KF}}$ is obtained from the time update in (3.5). Using (3.3) and (3.10), the innovation covariance matrix $\boldsymbol{S}_k$ is computed as

$$\boldsymbol{S}_k = \boldsymbol{H}_k\overline{\boldsymbol{P}}_{\mathrm{x}_k}\boldsymbol{H}_k^T + \boldsymbol{V}_{\rho\phi_k} \tag{3.11}$$

3.1.2 Loosely–Coupled INS/GNSS Estimator. In a loosely-coupled architecture, the position solution is first obtained from a least squares estimator using GNSS measurements. This GNSS-only position solution is then directly incorporated into a

Kalman filter to produce the rest of the navigation solution using IMU measurements. This integration scheme is consistent with local area augmentation systems such as GBAS because they output a position solution directly. The estimator introduced in this section is an example for GBAS applications. However, the concepts developed here are applicable to other loosely-coupled applications as well.

3.1.2.1 GBAS–Assisted Weighted Least Squares Estimator. The differentially corrected carrier-smoothed code measurement in (2.13) can be re-expressed for the time epoch k as

$$\overline{\boldsymbol{\rho}}_k = \underbrace{\begin{bmatrix}\boldsymbol{G}_k & \mathbf{1}\end{bmatrix}}_{\boldsymbol{G}_{\overline{\rho}_k}} \begin{bmatrix}\delta\boldsymbol{r}_k \\ \delta\tau_{u_k}\end{bmatrix} + \boldsymbol{\nu}_{\overline{\rho}_k}. \tag{3.12}$$

Utilizing the measurement model in (3.12), the weighted least squares estimate $\delta\hat{\boldsymbol{r}}_k^{\mathrm{LS}}$ of the position is obtained by

$$\delta\hat{\boldsymbol{r}}_k^{\mathrm{LS}} = \boldsymbol{T}_r \boldsymbol{G}_{\overline{\rho}_k}^{+} \overline{\boldsymbol{\rho}}_k \tag{3.13}$$

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

$$\boldsymbol{G}_{\overline{\rho}_k}^{+} = \left(\boldsymbol{G}_{\overline{\rho}_k}^T \boldsymbol{V}_{\overline{\rho}_k}^{-1} \boldsymbol{G}_{\overline{\rho}_k}\right)^{-1} \boldsymbol{G}_{\overline{\rho}_k}^T \boldsymbol{V}_{\overline{\rho}_k}^{-1}. \tag{3.14}$$

Defining $\delta\hat{\boldsymbol{r}}_k^{\mathrm{LS}} = \delta\boldsymbol{r}_k + \delta\tilde{\boldsymbol{r}}_k^{\mathrm{LS}}$ and substituting (3.12) into (3.13), one can obtain the least squares estimation error $\delta\tilde{\boldsymbol{r}}_k^{\mathrm{LS}}$ as

$$\delta\tilde{\boldsymbol{r}}_k^{\mathrm{LS}} = \boldsymbol{T}_r \boldsymbol{G}_{\overline{\rho}_k}^{+} \boldsymbol{\nu}_{\overline{\rho}_k} \tag{3.15}$$

3.1.2.2 Loosely–Coupled Kalman Filter. Recall that the discrete form of the INS process model previously obtained in (2.29), is

$$\boldsymbol{x}_k = \boldsymbol{\Phi}\,\boldsymbol{x}_{k-1} + \boldsymbol{\Gamma}\,\tilde{\boldsymbol{u}}_{k-1} + \overline{\boldsymbol{w}}_{k-1}. \tag{3.16}$$

The GBAS solution $\hat{\boldsymbol{r}}_k^{\mathrm{LS}}$ obtained from the weighted least squares estimator in (3.13), is utilized in a loosely-coupled Kalman filter to calibrate the INS error states. Recalling $\boldsymbol{x}'_k = \left[\delta\boldsymbol{v}_k, \delta\boldsymbol{E}_k, \boldsymbol{b}_k\right]^T$, the measurement model of the Kalman filter in the

loosely-coupled architecture has the typical form

$$\delta\hat{\boldsymbol{r}}_k^{\mathrm{LS}} = \begin{bmatrix} \boldsymbol{I} & 0 \end{bmatrix} \begin{bmatrix} \delta\boldsymbol{r}_k \\ \boldsymbol{x}'_k \end{bmatrix} + \delta\tilde{\boldsymbol{r}}_k^{\mathrm{LS}}. \tag{3.17}$$

The main assumption in a Kalman filter is that the measurements are uncorrelated over time. However, $\delta\hat{\boldsymbol{r}}_k^{\mathrm{LS}}$ in (3.17) is time-correlated because the GBAS measurement noise $\boldsymbol{\nu}_{\bar{\rho}}$ in (3.12) is time-correlated due to the prior Hatch filtering. Assuming that the time constant of the hatch filter τ_h is considerably larger than that of the multipath τ_m, the time correlation of the measurement noise $\boldsymbol{\nu}_{\bar{\rho}}$ can be captured with a first-order Gauss Markov process driven with a white noise $\boldsymbol{\epsilon}_k \sim \mathcal{N}(0, \boldsymbol{E}_k)$ as

$$\underbrace{\begin{bmatrix} \nu^1_{\bar{\rho}_k} \\ \vdots \\ \nu^n_{\bar{\rho}_k} \end{bmatrix}}_{\boldsymbol{\nu}_{\bar{\rho}_k}} = \underbrace{\begin{bmatrix} e^{-\frac{\Delta t}{\tau_h}} & & 0 \\ & \ddots & \\ 0 & & e^{-\frac{\Delta t}{\tau_h}} \end{bmatrix}}_{\boldsymbol{\Phi}_h} \underbrace{\begin{bmatrix} \nu^1_{\bar{\rho}_{k-1}} \\ \vdots \\ \nu^n_{\bar{\rho}_{k-1}} \end{bmatrix}}_{\boldsymbol{\nu}_{\bar{\rho}_{k-1}}} + \underbrace{\begin{bmatrix} \epsilon^1_{k-1} \\ \vdots \\ \epsilon^n_{k-1} \end{bmatrix}}_{\boldsymbol{\epsilon}_{k-1}} \tag{3.18}$$

where Δt is the GNSS receiver sampling time and τ_h is the Hatch filter time constant. The components of $\boldsymbol{\nu}_{\bar{\rho}_{k-1}}$ and $\boldsymbol{\epsilon}_{k-1}$ superscripted from 1 to n are the errors corresponding to the measurements obtained from satellites 1 to n.

The covariance $\boldsymbol{V}_{\bar{\rho}_k}$ of the measurement error vector $\boldsymbol{\nu}_{\bar{\rho}_k}$ in (3.18) is a diagonal matrix obtained from the Hatch filter at steady-state. Incorparating this steady-state value of $\boldsymbol{V}_{\bar{\rho}_k}$ in the process model (3.18), the driving noise covariance matrix $\boldsymbol{E}_k$ is obtained as

$$\boldsymbol{E}_k = (\boldsymbol{I} - \boldsymbol{\Phi}_h^2)\, \boldsymbol{V}_{\bar{\rho}_k}. \tag{3.19}$$

To capture the correlation in the Kalman filter, we first obtain a zero-noise measurement model by substituting (3.15) into (3.17) and augmenting the colored noise $\boldsymbol{\nu}_{\bar{\rho}_k}$ into the state vector as [9]

$$\delta\hat{\boldsymbol{r}}_k^{\mathrm{LS}} = \underbrace{\begin{bmatrix} \boldsymbol{I} & 0 & \boldsymbol{T}_r \boldsymbol{G}_k^{+} \end{bmatrix}}_{\boldsymbol{H}_k} \underbrace{\begin{bmatrix} \delta\boldsymbol{r}_k \\ \boldsymbol{x}'_k \\ \boldsymbol{\nu}_{\bar{\rho}_k} \end{bmatrix}}_{\mathbf{x}_k} \tag{3.20}$$

then, we also augment the Gauss Markov process model for $\boldsymbol{\nu}_{\overline{\rho}}$ in (3.18) with the INS process model in (3.16) as

$$\begin{bmatrix} \boldsymbol{x}_k \\ \boldsymbol{\nu}_{\overline{\rho}_k} \end{bmatrix} = \underbrace{\begin{bmatrix} \boldsymbol{\Phi} & 0 \\ 0 & \boldsymbol{\Phi}_h \end{bmatrix}}_{\boldsymbol{\Phi}_{\mathrm{x}}} \underbrace{\begin{bmatrix} \boldsymbol{x}_{k-1} \\ \boldsymbol{\nu}_{\overline{\rho}_{k-1}} \end{bmatrix}}_{\mathbf{x}_{k-1}} + \underbrace{\begin{bmatrix} \boldsymbol{\Gamma} \\ 0 \end{bmatrix}}_{\boldsymbol{\Gamma}_{\mathrm{x}}} \tilde{\boldsymbol{u}}_{k-1} + \underbrace{\begin{bmatrix} \overline{\boldsymbol{w}}_{k-1} \\ \boldsymbol{\epsilon}_{k-1} \end{bmatrix}}_{\boldsymbol{w}_{\mathrm{x}_k}} \tag{3.21}$$

where $\overline{\boldsymbol{w}}_{\mathrm{x}_k} \sim \mathcal{N}(0, \boldsymbol{W}_{\mathrm{x}})$ is the white process noise of the Kalman filter having a covariance matrix of $\boldsymbol{W}_{\mathrm{x}}$.

Given the augmented process model in (3.21), the Kalman filter time update gives the a priori estimate $\overline{\mathbf{x}}_k^{\mathrm{KF}}$ as

$$\overline{\mathbf{x}}_k^{\mathrm{KF}} = \boldsymbol{\Phi}_{\mathrm{x}} \hat{\mathbf{x}}_{k-1}^{\mathrm{KF}} + \boldsymbol{\Gamma}_{\mathrm{x}} \tilde{\boldsymbol{u}}_{k-1} \tag{3.22}$$

and the measurement update gives the a posteriori estimate $\hat{\mathbf{x}}_k$ as

$$\hat{\mathbf{x}}_k^{\mathrm{KF}} = \overline{\mathbf{x}}_k^{\mathrm{KF}} + \boldsymbol{L}_k \big(\delta \hat{\boldsymbol{r}}_k^{\mathrm{LS}} - \boldsymbol{H}_k \overline{\mathbf{x}}_k^{\mathrm{KF}} \big) \tag{3.23}$$

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

$$\boldsymbol{L}_k = \overline{\boldsymbol{P}}_{\mathrm{x}_k} \boldsymbol{H}_k^T (\boldsymbol{H}_k \overline{\boldsymbol{P}}_{\mathrm{x}_k} \boldsymbol{H}_k^T)^{-1}, \tag{3.24}$$

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

$$\overline{\boldsymbol{P}}_{\mathrm{x}_k} = \boldsymbol{\Phi}_{\mathrm{x}} \hat{\boldsymbol{P}}_{\mathrm{x}_{k-1}} \boldsymbol{\Phi}_{\mathrm{x}}^T + \boldsymbol{W}_{\mathrm{x}_{k-1}}, \tag{3.25}$$

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

$$\hat{\boldsymbol{P}}_{\mathrm{x}_k} = (\boldsymbol{I} - \boldsymbol{L}_k \boldsymbol{H}_k) \overline{\boldsymbol{P}}_{\mathrm{x}_k}. \tag{3.26}$$

It should be reminded that the equations from (3.24) to (3.26) are slightly different from those from (3.7) to (3.9) for the tightly coupled model because the measurement error covariance is assumed zero (i.e., $\boldsymbol{V}_{\delta \hat{\boldsymbol{r}}_k^{\mathrm{LS}}} = 0$) for the loosely-coupled model. The reason is that the post-Hatch filter residual noise is included in the multipath model.

The Kalman filter innovation vector $\boldsymbol{\gamma}_k$ is

$$\boldsymbol{\gamma}_k = \delta \hat{\boldsymbol{r}}_k^{\mathrm{LS}} - \boldsymbol{H}_k \overline{\mathbf{x}}_k^{\mathrm{KF}} \tag{3.27}$$

where $\delta\hat{\boldsymbol{r}}_k^{\mathrm{LS}}$ and $\overline{\mathbf{x}}_k^{\mathrm{KF}}$ are obtained from the weighted least squares estimator in (3.13) and the Kalman filter time update in (3.22), respectively. Using (3.20) and (3.27), the innovation covariance matrix $\boldsymbol{S}_k$ is computed as

$$\boldsymbol{S}_k = \boldsymbol{H}_k \overline{\boldsymbol{P}}_{\mathrm{x}_k} \boldsymbol{H}_k^T \tag{3.28}$$

3.1.3 Innovations–Based INS Monitor. The monitor we describe here has roots in receiver autonomous integrity monitoring (RAIM) techniques, which were originally developed to detect satellite faults by exploiting redundancy in satellite measurements [39]. However, unlike conventional RAIM, the detection concepts used in this work provide the necessary redundancy through INS measurements.

We implement a spoofing monitor (detector) using the Kalman filter innovations. In coupled INS/GNSS integration, the innovation vector $\boldsymbol{\gamma}_k$ defined in (3.10) and (3.27), represents the pure discrepancy between GNSS and INS at time epoch k. Under a smart spoofing attack where the fault is slowly injected through GNSS and contaminates INS state estimation slowly, the current-time innovation will be ineffective for detection; however, the fault should be observable in the innovations if they are accumulated over time. Therefore, we use a cumulative Kalman filter test statistic q at time epoch k which is the sum of squares of the normalized innovation vectors over time:

$$q_k = \sum_{i=1}^{k} \boldsymbol{\gamma}_i^T \boldsymbol{S}_i^{-1} \boldsymbol{\gamma}_i, \tag{3.29}$$

or in vector form as

$$q_k = \begin{bmatrix} \boldsymbol{\gamma}_1^T & \dots & \boldsymbol{\gamma}_k^T \end{bmatrix} \underbrace{\begin{bmatrix} \boldsymbol{S}_1^{-1} & & \\ & \ddots & \\ & & \boldsymbol{S}_k^{-1} \end{bmatrix}}_{\boldsymbol{S}_{1:k}^{-1}} \underbrace{\begin{bmatrix} \boldsymbol{\gamma}_1 \\ \vdots \\ \boldsymbol{\gamma}_k \end{bmatrix}}_{\boldsymbol{\gamma}_{1:k}} \tag{3.30}$$

where $\boldsymbol{S}_{1:k}$ is the block diagonal matrix composed of the innovation covariances $\boldsymbol{S}_i$'s $(0 < i \leq k)$. It should be noted that the innovations are independent [13]:

$\mathbb{E}[\boldsymbol{\gamma}_i \boldsymbol{\gamma}_j^T] = 0$ for $i \neq j$ because the Kalman filters in both the loosely and tightly-coupled integrations are constructed to ensure both the process and measurement noises are white and Gaussian.

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

$$q_k \gtrless T. \tag{3.31}$$

The INS monitor alarms for a fault if $q_k > T$. Let n be the number of measurements for each GNSS measurement update; under fault free conditions, the test statistic q_k is chi-square distributed with nk degrees of freedom for the tightly-coupled implementation and with $3k$ degrees of freedom for the loosely-coupled implementation. Even though n may vary from one time epoch to another due to satellites occasionally rising and setting, for the simplicity in the analysis it is assumed constant. For a given false alarm requirement, the threshold T is determined from the inverse chi-square cumulative distribution function. Under faulted conditions, q_k is non-centrally chi-square distributed with a non-centrality parameter λ_k^2,

$$\lambda_k^2 = \mathbb{E}[\boldsymbol{\gamma}_{1:k}^T]\, \boldsymbol{S}_{1:k}^{-1}\, \mathbb{E}[\boldsymbol{\gamma}_{1:k}] \tag{3.32}$$

which is used to evaluate the probability of missed detection.

3.2 Batch Residual–Based Monitor

In this section, we propose an analogous spoofing monitor that is compatible with systems where INS and GNSS are coupled in a batch estimator rather than a Kalman filter. Spoofing detection is accomplished by monitoring the residual of the batch estimator. Unlike the sequential process in a Kalman filter, a batch estimator processes the entire measurement sequence simultaneously in a least squares estimation algorithm. Its current time epoch estimation accuracy is equivalent to a Kalman filter, however it is computationally expensive and gets slower as the data accumulates. Despite the computational limitations of the batch estimator, in some RAIM

applications [20] it was shown that its detection performance is better than Kalman filter-based monitors since it monitors whole time sequence of the faults.

3.2.1 Tightly–Coupled Batch Estimator. The batch weighted least-squares estimate of a state of interest (e.g., altitude in aircraft approach) is obtained using all available measurements, which is referred to as full-set solution. A general batch realization for linear dynamic systems is described in [20]. This section applies the batch formulation to a tightly-coupled INS/GNSS relative navigation system.

Recalling $\boldsymbol{x}_k^{'} = \left[\delta \boldsymbol{v}_k, \delta \boldsymbol{E}_k, \boldsymbol{b}_k\right]^T$ and defining $\boldsymbol{\nu}_{\rho\phi_k}^{'} = \boldsymbol{m}_{\rho\phi_k} + \boldsymbol{\nu}_{\rho\phi_k}$, the DD GNSS measurement equation in (2.11) and the INS model in (2.29) can be re-expressed as

$$\boldsymbol{z}_{\rho\phi_k} = \underbrace{\begin{bmatrix}\boldsymbol{G}_{\rho\phi_k} & 0\end{bmatrix}}_{\boldsymbol{G}_{\rho\phi_k}^{'}} \underbrace{\begin{bmatrix}\delta \boldsymbol{r}_k \\ \boldsymbol{x}_k'\end{bmatrix}}_{\boldsymbol{x}_k} + \boldsymbol{D}\,\boldsymbol{n}_{\rho\phi} + \boldsymbol{\nu}_{\rho\phi_k}^{'} \tag{3.33}$$

and

$$0 = \boldsymbol{\Phi}\,\boldsymbol{x}_{k-1} - \boldsymbol{I}\,\boldsymbol{x}_k + \boldsymbol{\Gamma}\,\tilde{\boldsymbol{u}}_{k-1} + \overline{\boldsymbol{w}}_{k-1}, \tag{3.34}$$

respectively. So far, we have obtained the measurement and process models in sequential form. The next step is to construct a batch form of the tightly-coupled INS GNSS mechanization by using (3.33) and (3.34). It is first assumed that the INS and cycle ambiguity states have been initialized under fault-free conditions:

$$\underbrace{\begin{bmatrix}\boldsymbol{x}_1^p \\ \boldsymbol{n}_{\rho\phi}^p\end{bmatrix}}_{\boldsymbol{z}_{\rho\phi_0}} = \underbrace{\begin{bmatrix}\boldsymbol{I} \\ 0\end{bmatrix}}_{\boldsymbol{I}_1} \boldsymbol{x}_1 + \underbrace{\begin{bmatrix}0 \\ \boldsymbol{I}\end{bmatrix}}_{\boldsymbol{D}_1} \boldsymbol{n}_{\rho\phi} + \underbrace{\begin{bmatrix}\delta \boldsymbol{x}_1 \\ \delta \boldsymbol{n}_{\rho\phi}\end{bmatrix}}_{\delta \boldsymbol{x}_{1,n_{\rho\phi}}} \tag{3.35}$$

where $\boldsymbol{x}_1^p$ and $\boldsymbol{n}_{\rho\phi}^p$ are the pseudo-measurements (i.e., initial conditions) for $\boldsymbol{x}_1$ and $\boldsymbol{n}_{\rho\phi}$, respectively; $\delta \boldsymbol{x}_1 \sim \mathcal{N}(0, \overline{\boldsymbol{P}}_1)$, $\delta \boldsymbol{n}_{\rho\phi} \sim \mathcal{N}(0, \overline{\boldsymbol{P}}_{n_{\rho\phi}})$, and $\delta \boldsymbol{x}_{1,n_{\rho\phi}} \sim \mathcal{N}(0, \overline{\boldsymbol{P}}_{1,n_{\rho\phi}})$. $\overline{\boldsymbol{P}}_1$ and $\overline{\boldsymbol{P}}_{n_{\rho\phi}}$ are the initial covariance matrices of $\boldsymbol{x}$ and $\boldsymbol{n}_{\rho\phi}$, respectively; and $\overline{\boldsymbol{P}}_{1,n_{\rho\phi}}$ is a diagonal matrix as

$$\overline{\boldsymbol{P}}_{1,n_{\rho\phi}} = \begin{bmatrix}\overline{\boldsymbol{P}}_1 & 0 \\ 0 & \overline{\boldsymbol{P}}_{n_{\rho\phi}}\end{bmatrix}. \tag{3.36}$$

Combining (3.33), (3.34), and (3.35) yields a batch form containing all the time history of process and measurement models with initial conditions as

$$\underbrace{\begin{bmatrix} \boldsymbol{z}_{\rho\phi_0} \\ \boldsymbol{z}_{\rho\phi_1} \\ 0 \\ \boldsymbol{z}_{\rho\phi_2} \\ 0 \\ \vdots \end{bmatrix}}_{\boldsymbol{z}_b} = \underbrace{\left[\begin{array}{cccc|c} \boldsymbol{I}_1 & & & & \boldsymbol{D}_1 \\ \boldsymbol{G}'_{\rho\phi_1} & & & & \boldsymbol{D} \\ \boldsymbol{\Phi} & -\boldsymbol{I} & 0 & & 0 \\ & \boldsymbol{G}'_{\rho\phi_2} & & & \boldsymbol{D} \\ & \boldsymbol{\Phi} & -\boldsymbol{I} & & 0 \\ 0 & & \ddots & & \vdots \end{array}\right]}_{\boldsymbol{H}_b} \underbrace{\begin{bmatrix} \boldsymbol{x}_1 \\ \boldsymbol{x}_2 \\ \boldsymbol{x}_3 \\ \boldsymbol{x}_4 \\ \vdots \\ \hline \boldsymbol{n}_{\rho\phi} \end{bmatrix}}_{\boldsymbol{x}_b} + \underbrace{\begin{bmatrix} \delta\boldsymbol{x}_{1,n_{\rho\phi}} \\ \boldsymbol{\nu}'_{\rho\phi_1} \\ \boldsymbol{\Gamma}\tilde{\boldsymbol{u}}_1 + \overline{\boldsymbol{w}}_1 \\ \boldsymbol{\nu}'_{\rho\phi_2} \\ \boldsymbol{\Gamma}\tilde{\boldsymbol{u}}_2 + \overline{\boldsymbol{w}}_2 \\ \vdots \end{bmatrix}}_{\boldsymbol{\nu}_b} \tag{3.37}$$

where $\boldsymbol{z}_b$ is the batch measurement vector, $\boldsymbol{H}_b$ is the batch observation matrix, $\boldsymbol{x}_b$ is the batch state vector, and $\boldsymbol{\nu}_b$ is the batch measurement noise vector, which has a covariance matrix $\boldsymbol{V}_b$ as

$$\boldsymbol{V}_b = \begin{bmatrix} \overline{\boldsymbol{P}}_{1,n_{\rho\phi}} & & 0 & & \\ & \boldsymbol{V}'_{\rho\phi_1} & & \boldsymbol{V}'_{\rho\phi_{12}} & \cdots \\ & & \overline{\boldsymbol{W}}_1 & & \\ & 0 & & \boldsymbol{V}'_{\rho\phi_2} & \\ & & & & \ddots \end{bmatrix}. \tag{3.38}$$

The first block diagonal term in (3.38) corresponds to the initial state covariance matrix. The diagonal terms $\boldsymbol{V}'_{\rho\phi_i}$ include receiver thermal noise and multipath, while the time correlated effect of multipath is captured in the off-diagonal terms $\boldsymbol{V}'_{\rho\phi_{ij}}$ where multipath is modeled as a first order Gauss Markov process. Recall that the $\tilde{\boldsymbol{u}}_i$ terms in (3.37) are deterministic inputs to the estimator; therefore they do not impact the batch measurement error covariance $\boldsymbol{V}_b$.

Using the batch model in (3.37), the weighted least squares estimate $\hat{\boldsymbol{x}}_b$ and its error covariance $\hat{\boldsymbol{P}}_b$ are computed as

$$\hat{\boldsymbol{x}}_b = \boldsymbol{H}_b^{+}\, \boldsymbol{z}_b \tag{3.39}$$

and

$$\hat{\boldsymbol{P}}_b = \left(\boldsymbol{H}_b^T\, \boldsymbol{V}_b{}^{-1} \boldsymbol{H}_b\right)^{-1}, \tag{3.40}$$

respectively, where $\boldsymbol{H}_b^+$ is the weighted pseudo-inverse matrix of $\boldsymbol{H}_b$

$$\boldsymbol{H}_b^+ = \left(\boldsymbol{H}_b^T \boldsymbol{V}_b^{-1} \boldsymbol{H}_b\right)^{-1} \boldsymbol{H}_b^T \boldsymbol{V}_b^{-1}. \tag{3.41}$$

3.2.2 Residual–Based INS Monitor. In residual-based RAIM, the test statistic is defined as the weighted norm of the residual vector [39]. 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 monitor. The redundancy for detection in the residual-based INS monitor is provided through INS measurements which are the fault-free zero rows of the batch measurement vector $\boldsymbol{z}_b$ in (3.37).

The residual vector $\mathbf{r}$ of the batch estimation in (3.39) is

$$\mathbf{r} = \boldsymbol{z}_b - \boldsymbol{H}_b \hat{\boldsymbol{x}}_b. \tag{3.42}$$

The monitor checks whether the weighted norm of the residual, which we call test statistic q, is larger than a pre-defined threshold T

$$q = \mathbf{r}^T \boldsymbol{V}_b^{-1} \mathbf{r} \gtrless T. \tag{3.43}$$

Let n be the number of GNSS measurements (assumed constant over the batch time interval for simplicity) and m be the number of states at each time epoch. Under fault free conditions, the test statistic q is centrally chi-square distributed with $k(n-m)$ degrees of freedom where k is the number of time epochs. For a given false alarm requirement, the threshold T is determined from the inverse cumulative chi-square distribution. The monitor alarms for a fault if q is larger than T. Under faulted conditions, the test statistic is known to follow a noncentral chi-square distribution with a non-centrality parameter

$$\lambda^2 = \mathbb{E}[\mathbf{r}]^T \boldsymbol{V}_b^{-1} \mathbb{E}[\mathbf{r}] \tag{3.44}$$

3.3 Uncoupled Monitor

In an uncoupled INS/GNSS scheme, GNSS information does not contribute to decreasing the INS error rate. Although the uncoupled integration is not as common as other integration types, some of the general aviation and maritime application use a standalone GNSS uncoupled with INS. The accuracy of the INS solution in standalone mode degrades over time. However depending on its sensor grade (Tables 2.1 and F.1), it can be used as a sanity check for GNSS solution specifically in en route horizontal guidance applications, the accuracy and integrity requirements of which are not as strict as the vertical requirements of landing and approach applications. In this section, we describe a GNSS-only least squares estimator and INS-only dead reckoning estimator, and define a simple spoofing monitor that checks the discrepancy between these two solutions.

3.3.1 GNSS–Only Weighted Least Squares Estimator. The standalone GNSS measurement equation in (2.5) can be re-written as

$$\boldsymbol{\rho}_k = \underbrace{\begin{bmatrix}\boldsymbol{G}_k & \boldsymbol{I}\end{bmatrix}}_{\boldsymbol{H}_k} \begin{bmatrix}\delta\boldsymbol{r}_k \\ \delta\tau_{u_k}\end{bmatrix} + \underbrace{\boldsymbol{m}_{\rho_k} + \boldsymbol{\nu}_{\rho_k}}_{\boldsymbol{\nu}'_{\rho_k}} \tag{3.45}$$

where $\boldsymbol{\nu}'_{\rho_k} \sim \mathcal{N}(0, \boldsymbol{V}'_{\rho_k})$ is the measurement error vector containing both multipath and other residual errors in $\boldsymbol{\rho}_k$. Utilizing the measurement model in (3.45), the weighted least squares estimate of $\delta\boldsymbol{r}_k$ is

$$\delta\hat{\boldsymbol{r}}_k^{\mathrm{LS}} = \boldsymbol{T}_r \boldsymbol{H}_k^{+} \boldsymbol{\rho}_k \tag{3.46}$$

where $\boldsymbol{T}_r$ is the matrix that extracts the position $\delta\boldsymbol{r}_k$ from $[\delta\boldsymbol{r}_k, \delta\tau_{u_k}]^T$, $\boldsymbol{H}_k^{+}$ is the pseudo-inverse matrix

$$\boldsymbol{H}_k^{+} = \hat{\boldsymbol{P}}_{\delta r_k} \boldsymbol{H}_k^T \boldsymbol{V}'^{-1}_{\rho_k} \tag{3.47}$$

and $\hat{\boldsymbol{P}}_k$ is the state estimate error covariance matrix

$$\hat{\boldsymbol{P}}_{\delta r_k} = \left(\boldsymbol{H}_k^T \boldsymbol{V}'^{-1}_{\rho_k} \boldsymbol{H}_k\right)^{-1}. \tag{3.48}$$

3.3.2 INS Propagation. Recalling the INS model defined in (2.29) as

$$\boldsymbol{x}_k = \boldsymbol{\Phi}\, \boldsymbol{x}_{k-1} + \boldsymbol{\Gamma}\, \tilde{\boldsymbol{u}}_{k-1} + \overline{\boldsymbol{w}}_{k-1}, \tag{3.49}$$

the INS-only state estimate $\overline{\boldsymbol{x}}^{\mathrm{INS}}$ and its error covariance matrix $\overline{\boldsymbol{P}}$ can be propagated over time as

$$\overline{\boldsymbol{x}}_k^{\mathrm{INS}} = \boldsymbol{\Phi}\,\overline{\boldsymbol{x}}_{k-1}^{\mathrm{INS}} + \boldsymbol{\Gamma}\,\tilde{\boldsymbol{u}}_{k-1} \tag{3.50}$$

and

$$\overline{\boldsymbol{P}}_{x_k} = \boldsymbol{\Phi}\,\overline{\boldsymbol{P}}_{x_{k-1}}\boldsymbol{\Phi}^T + \overline{\boldsymbol{W}}_{k-1}, \tag{3.51}$$

respectively, where the initial conditions are $\overline{\boldsymbol{x}}_0^{\mathrm{INS}} = \boldsymbol{x}_0$ and $\overline{\boldsymbol{P}}_{x_0} = \boldsymbol{P}_{x_0}$.

3.3.3 Uncoupled INS Monitor. Unlike the coupled integration cases which monitor the cumulative residual (or innovation), the uncoupled monitor can directly check the discrepancy between INS and GNSS solutions. The reason is that the INS in uncoupled integration is not calibrated by GNSS, and is therefore not corrupted over time by faulty GNSS measurements.

The monitor checks whether the test statistic q_k defined as the discrepancy between the estimates of the state of interest (i.e., lateral position) obtained from the GNSS least squares estimation and the INS propagation, is larger than a predefined threshold T as

$$q_k = \left|\boldsymbol{t}_{\varepsilon r}\,\delta\hat{\boldsymbol{r}}_k^{\mathrm{LS}} - \boldsymbol{t}_{\varepsilon x}\,\overline{\boldsymbol{x}}_k^{\mathrm{INS}}\right| \gtrless T \tag{3.52}$$

where $\boldsymbol{t}_{\varepsilon r}$ and $\boldsymbol{t}_{\varepsilon x}$ are the row vectors that extract the lateral position from $\delta\hat{\boldsymbol{r}}_k^{\mathrm{LS}}$ and $\overline{\boldsymbol{x}}_k^{\mathrm{INS}}$, respectively. Under fault free conditions, the test statistic $q_k \sim \mathcal{N}(0, \sigma_{q_k}^2)$ where $\sigma_{q_k}^2$ is the variance of the test statistic

$$\sigma_{q_k}^2 = \boldsymbol{t}_{\varepsilon r}\,\boldsymbol{T}_r\,\hat{\boldsymbol{P}}_{\delta r_k}\,\boldsymbol{T}_r^T\boldsymbol{t}_{\varepsilon r}^T + \boldsymbol{t}_{\varepsilon x}\overline{\boldsymbol{P}}_{x_k}\,\boldsymbol{t}_{\varepsilon x}^T. \tag{3.53}$$

For a given false alarm requirement, the threshold T is determined from the inverse Gaussian distribution. The INS monitor alarms for a fault if $q_k > T$. Under faulted conditions, q_k is normally distributed with a non-zero mean, which is used to evaluate the performance of the monitor by computing the probability of missed detection.

3.4 Monitor Performance Evaluation with Integrity Risk

In this work, integrity risk is used as a metric to quantify the performance of the spoofing monitors. Integrity risk is defined as the probability that the most critical state estimate error exceeds a predefined alert limit without being detected. In presence of a spoofing fault $\boldsymbol{f}$ in the GNSS code and carrier measurements (conditional event H_f), the integrity risk at time epoch k is expressed in terms of the test statistic q_k and the current estimate error of hazardous state ε_k as

$$I_{r_k} = \Pr\left(|\varepsilon_k| > l, q_k < T \mid H_f\right) \Pr\left(H_f\right) \tag{3.54}$$

where $\Pr\left(H_f\right)$ is the probability of fault occurrence, l is the alert limit, and T is a pre-defined threshold for detection which represents those in (3.31), (3.43), and (3.52) for the Kalman filter-based, batch-based, and uncoupled monitors, respectively. An upper bound $\bar{I}_{r_k}$ on the integrity risk I_{r_k} in (3.54) is established by using the worst case fault $\boldsymbol{f}_w$ in computing ε_k and q_k, and conservatively assuming that the probability of the worst case fault occurrence $\Pr\left(H_{f_w}\right)$ is 1:

$$\bar{I}_{r_k} = \Pr\left(|\varepsilon_k| > l, q_k < T \mid H_{f_w}\right) \geq I_{r_k}. \tag{3.55}$$

In the monitor's performance evaluation, ε is selected based on the most stringent requirements defined for a specific application. For example, the error in altitude is the most hazardous in aircraft approach and landing applications (e.g., relative navigation and GBAS) whereas the horizontal position error is more critical in en route navigation in aviation and maritime applications. In the performance analysis, which will be introduced in the following chapters, the estimation error ε_k associated with the hazardous state can be obtained by differencing the state estimate (to be used as a navigation solution) $\hat{\mathbf{x}}$ and the actual state $\mathbf{x}$, and extracting the corresponding row using the row transformation vector $\boldsymbol{t}_\varepsilon$ as

$$\varepsilon_k = \boldsymbol{t}_\varepsilon \left(\hat{\mathbf{x}}_k - \mathbf{x}_k\right) \tag{3.56}$$

where ε_k is normally distributed.

In this chapter, we proposed spoofing monitors for different INS/GNSS integration schemes. In the following chapters, their statistical reliability performance will be evaluated and demonstrated for several example high-integrity GNSS aviation applications under worst-case spoofing attacks.

CHAPTER 4

AIRCRAFT DYNAMICS EFFECTS ON MONITOR PERFORMANCE AGAINST OPEN LOOP SPOOFERS

In this chapter, we show that for an aircraft equipped with an INS, the dynamic response to disturbances (e.g., wind gusts or control actions actuated by autopilot) provides an advantage in detecting spoofing attacks. The reason is that the disturbance response will be instantaneously reflected in INS measurements, but not necessarily in the spoofed GNSS signal. The main contribution is the development of a rigorous methodology to compute upper bounds on the integrity risk resulting from a worst case spoofing attack – without needing to simulate individual aircraft approaches with an unmanageably large number of gust disturbance profiles. We use a B747 (Boeing 747) aircraft model to demonstrate the INS monitor's performance and to investigate disturbance levels (i.e., gust intensity) that are sufficient to meet integrity risk requirements for precision approach and landing.

The methods introduced in this chapter quantify the monitor's sensitivity to the spoofer's lack of knowledge on the aircraft trajectory in an "open-loop" spoofing scenario. The analysis results obtained in this chapter will support further analysis with more sophisticated closed-loop tracking and spoofing scenarios in the following chapters.

4.1 Background and Previous Work

In [25], it was illustrated how a spoofer can inject faults slowly into the GNSS measurements such that they corrupt the tightly coupled solution while going unnoticed by the INS detector. It was also shown that if the spoofer knows the exact trajectory of an aircraft, he or she might eventually cause errors large enough to

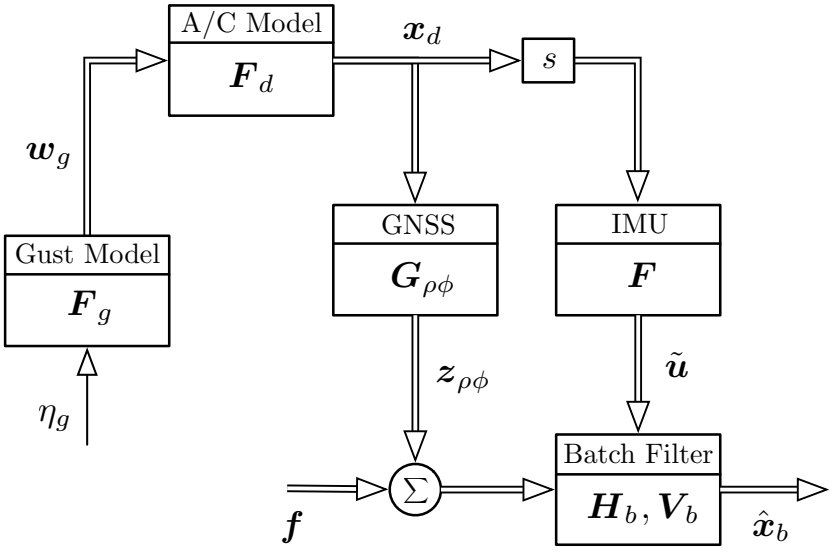

Figure 4.1. Open-loop performance evaluation model capturing the impact of wind gust disturbance on aircraft that uses a tightly-coupled INS/GNSS scheme. The wind gust intensity η_g (white noise) and spoofer's fault vector $\boldsymbol{f}$ are the inputs to the model, which impact the output of the batch estimator, $\hat{\boldsymbol{x}}_b$.

exceed hazard safety limits, again without triggering an alarm from the INS detector. As a case study in [25], in the presence of simple sinusoidal deviations from a nominal straight line final approach trajectory, which are assumed to be unknown to the spoofer, it was concluded that the monitor was effective, for the cases tested at least, in detecting spoofing attacks with quantifiably low integrity risk. However, to make a decisive conclusion, the aircraft trajectory must be tested with generalized disturbance patterns. In reality, these disturbance patterns might be induced by several factors, such as transient characteristic of the altitude-hold autopilot, the aircraft's controller response to the spoofed GNSS signals, or wind gusts. They usually trigger the short-period dynamics of the aircraft and result in a low-magnitude, high-frequency disturbance patterns.

4.2 Overview of Methodology

In this work, we extend the spoofing integrity analysis in [25] by deriving the

statistical dynamic response of an aircraft to a well-established wind gust power spectrum (the Dryden Gust Turbulence model) [16]. This derivation provides a statistical quantification of the trajectory deviations for a stochastic gust environment. Figure 4.1 is an overview of the performance evaluation model that generates open-loop dynamic response of an aircraft due to gust disturbances and feeds it into a relative navigation system using a tightly-coupled INS/GNSS batch estimator. The statistical information on the trajectory deviations obtained from the evaluation model is incorporated to a residual-based detector for performance evaluation. In this way, the impact of the random disturbance on the aircraft nominal trajectory can be directly incorporated into the integrity analysis seamlessly. The performance of the INS monitor is evaluated for an example aircraft landing approach in a nominal stochastic wind gust environment to investigate whether the monitor meets the integrity risk requirement for aircraft precision approach.

4.3 Batch Measurement Model with Fault

For given GNSS fault vectors $\boldsymbol{f}_i$ for $1 \leq i \leq k$, the batch estimator model (3.37) containing DD GNSS measurement and INS models, can be re-written as

$$\boldsymbol{z}_b^s = \boldsymbol{H}_b \boldsymbol{x}_b + \boldsymbol{\nu}_b + \boldsymbol{f}_b \tag{4.1}$$

where $\boldsymbol{x}_b$, $\boldsymbol{H}_b$, and $\boldsymbol{\nu}_b \sim \mathcal{N}(0, \boldsymbol{V}_b)$ are the batch state vector, observation matrix, and measurement noise vector, respectively, $\boldsymbol{z}_b^s = [\boldsymbol{z}_{\rho\phi_0}^s, \boldsymbol{z}_{\rho\phi_1}^s, \boldsymbol{0}, \boldsymbol{z}_{\rho\phi_2}^s, \boldsymbol{0}, \ldots, \boldsymbol{z}_{\rho\phi_k}^s]^T$ is the spoofed batch measurement vector, and $\boldsymbol{f}_b = [\boldsymbol{0}, \boldsymbol{f}_1, \boldsymbol{0}, \boldsymbol{f}_2, \boldsymbol{0}, \ldots, \boldsymbol{f}_k]^T$ is the fault history vector in the batch form. Recall that the zero rows in $\boldsymbol{z}_b^s$ and $\boldsymbol{f}_b$ are the fault-free pseudo-measurements corresponding to the INS kinematics.

4.3.1 Worst–Case Fault for Batch Estimator–Based Monitors. A wide variety of possible spoofing scenarios may exist but it is not necessary to define a threat space because the worst-case sequence of spoofed GNSS measurements can be determined analytically by finding the profile that maximizes the integrity risk [20].

This profile takes into account the impact of spoofed signals on the test statistic and the user position estimate error simultaneously.

The batch state estimate is

$$\hat{\boldsymbol{x}}_b = \boldsymbol{H}_b^+ \, \boldsymbol{z}_b, \tag{4.2}$$

Substituting (4.1) into (4.2), the state estimation error $\tilde{\boldsymbol{x}}_b = \hat{\boldsymbol{x}}_b - \boldsymbol{x}_b$ can be expressed as

$$\tilde{\boldsymbol{x}}_b = \boldsymbol{H}_b^+ \big(\boldsymbol{\nu}_b + \boldsymbol{f}_b\big). \tag{4.3}$$

Since the error in the altitude estimate is the most critical in landing approach, it is convenient to evaluate the performance with respect to vertical direction only. However, the same evaluation procedure can be applied to any other element of $\boldsymbol{x}_b$. Using the row transformation vector $\boldsymbol{t}_\varepsilon$, previously defined in (3.56), the vertical error at time epoch k is extracted from $\tilde{\boldsymbol{x}}_b$ as

$$\varepsilon_k = \boldsymbol{t}_\varepsilon \, \boldsymbol{H}_b^+ \big(\boldsymbol{\nu}_b + \boldsymbol{f}_b\big). \tag{4.4}$$

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 used for fault detection. If a spoofing attack is not detected instantaneously, it may impact INS error state estimates through the tight coupling mechanism, which then impacts subsequent detection capability. Therefore, a smart spoofer may select a fault profile that has smaller faults at the beginning, but increases over time. Qualitatively, the worst case fault profile is one that is injected slowly into the GNSS measurements, thereby corrupting INS calibration without being detected.

A method to obtain the worst case fault profile for least squares RAIM has been derived in [3] and was extended to batch estimation in [20]. The residual of the batch estimation is

$$\mathbf{r} = \boldsymbol{z}_b^s - \boldsymbol{H}_b \, \hat{\boldsymbol{x}}_b. \tag{4.5}$$

Under faulted conditions, substituting (4.2) into (4.5) gives the residual as a function of the fault as

$$\mathbf{r} = \left(\boldsymbol{I} - \boldsymbol{H}_b \boldsymbol{H}_b^{+}\right)\left(\boldsymbol{\nu}_b + \boldsymbol{f}_b\right). \tag{4.6}$$

The test statistic $q_k = \mathbf{r}^T \boldsymbol{V}_b^{-1}\mathbf{r}$ is non-centrally chi-square (χ^2) distributed with $k(n-m)$ degrees of freedom and a non-centrality parameter $\lambda^2 = \mathbb{E}[q_k]$, which using (4.6), (3.40), and (3.41), can be simplified to

$$\lambda^2 = \boldsymbol{f}_b^T \boldsymbol{V}_b^{-1}\left(\boldsymbol{I} - \boldsymbol{H}_b \boldsymbol{H}_b^{+}\right)\boldsymbol{f}_b. \tag{4.7}$$

Integrity risk is a metric to evaluate the performance of the monitor and is defined as the probability that the position error ε_k exceeds an alert limit l without being detected (i.e. $q_k < T$). It is shown in [20] that ε and q are statistically independent. Therefore, the integrity risk I_{r_k} previously defined in (3.55), can be written as a multiplication of two probabilities as

$$I_{r_k} = \Pr\left(|\varepsilon_k| > l\right) \Pr\left(q_k < T\right). \tag{4.8}$$

Using (4.4) and (4.7), the worst case fault vector that maximizes the integrity risk was derived in [20] as

$$\boldsymbol{f}_{w_b} = \alpha \boldsymbol{T}_z^T \left[\boldsymbol{T}_z \left(\boldsymbol{I} - \boldsymbol{H}_b \boldsymbol{H}_b^{+}\right) \boldsymbol{T}_z^T\right]^{-1} \boldsymbol{T}_z \boldsymbol{H}_b^{+^T} \boldsymbol{t}_\varepsilon \tag{4.9}$$

where $\boldsymbol{f}_{w_b} = [\mathbf{0}, \boldsymbol{f}_{w_1}, \mathbf{0}, \boldsymbol{f}_{w_2}, \mathbf{0}, \ldots, \boldsymbol{f}_{w_k}]^T$, $\boldsymbol{T}_z$ is a $kn \times k(n+m)$ sparse matrix of zeroes and ones that extracts the nonzero elements of $\boldsymbol{f}_b$ (or $\boldsymbol{z}_b^s$), and α is a scalar that is determined through iteration to maximize I_r. The fault vector in (4.9) represents the most dangerous fault profile that a spoofer can inject into the GNSS measurements in an open loop tracking and spoofing scenario.

4.3.2 Open–Loop Spoofed Measurements. In Figure 4.2, the blue line represents the deceptive trajectory corresponding to the spoofed GNSS measurements broadcast by the spoofer. The black dotted line is the nominal planned trajectory (for example, the landing approach) and the black curve illustrates the actual flight

path deviating from the nominal trajectory due to wind gusts. For the covariance analysis we perform in this chapter, we assume that the aircraft autopilot does not respond to the spoofed signals, thus the aircraft actual path follows the black curve in the close neighborhood of the nominal trajectory. However, it will be considered in the following chapters.

Including the fault vector $\boldsymbol{f}_k$ as an additional term into (3.33), the spoofed DD GNSS measurement $\boldsymbol{z}^s_{\rho\phi_k}$ at time epoch k can be written as

$$\boldsymbol{z}^s_{\rho\phi_k} = \boldsymbol{G}_{\rho\phi_k}\delta\boldsymbol{r}_k + \boldsymbol{D}\,\boldsymbol{n}_{\rho\phi} + \boldsymbol{\nu}'_{\rho\phi_k} + \boldsymbol{f}_k. \tag{4.10}$$

Knowing the nominal path of the aircraft, a smart spoofer may inject the worst-case fault in (4.9). Therefore, the spoofed measurement $\boldsymbol{z}^s_{\rho\phi_k}$ received by the aircraft at time epoch k can be defined as a function of worst-case fault as

$$\boldsymbol{z}^s_{\rho\phi_k} = \boldsymbol{f}_{w_k} + \boldsymbol{\nu}'_{\rho\phi_k}. \tag{4.11}$$

In the presence of wind gusts − and assuming the spoofer cannot predict the actual trajectory of the aircraft − the actual resultant fault $\boldsymbol{f}$ will be different from the worst-case fault $\boldsymbol{f}_w$. It should be mentioned that $\boldsymbol{G}_{\rho\phi_k}\delta\boldsymbol{r}_k$ term disappears in (4.11) unlike in (4.10), because when computing and generating the worst case fault the spoofer assumes a nominal flight − zero deviation from nominal trajectory $\delta\boldsymbol{r}_k = 0$. Similarly, the spoofer may arbitrarily assume zero cycle ambiguities in computing the spoofed measurements. Substituting (4.11) into the left hand side of (4.10) with $\boldsymbol{n}_{\rho\phi} = 0$ gives the relation between resultant fault $\boldsymbol{f}_k$ and worst-case fault $\boldsymbol{f}_{w_k}$ injected by the spoofer as

$$\boldsymbol{f}_k = \boldsymbol{f}_{w_k} - \boldsymbol{G}_{\rho\phi_k}\delta\boldsymbol{r}_k. \tag{4.12}$$

Recall that $\delta\boldsymbol{r}$ is defined as the deviation in position from the nominal (due to wind gusts) which will be derived and computed using the spectral model in Section 4.4. The worst-case fault vector $\boldsymbol{f}_w$ can be deterministically obtained for a given nominal

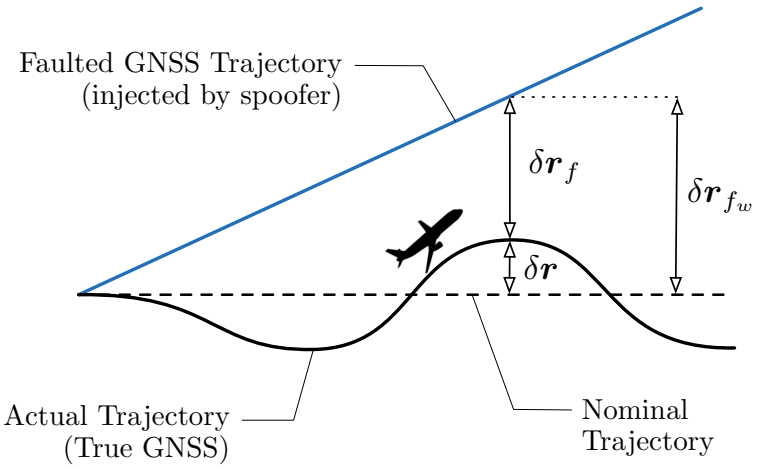

Figure 4.2. Actual and deceptive trajectories in the existence of wind gust and spoofing attack. $\delta \boldsymbol{r}$ is the position deviation from nominal trajectory due to wind gust. $\delta \boldsymbol{r}_{f_w}$ and $\delta \boldsymbol{r}_f$ are the worst case fault and resultant fault in position domain, respectively (i.e., $\boldsymbol{f}_w = \boldsymbol{G}_{\rho\phi}\delta \boldsymbol{r}_{f_w}$ and $\boldsymbol{f} = \boldsymbol{G}_{\rho\phi}\delta \boldsymbol{r}_f$).

trajectory using (4.9). The difference between the worst-case fault that the spoofer intends, and the resultant fault shown in (4.12) will cause a discrepancy that helps the monitor detect the fault, as we will demonstrate in Section 4.6.

4.4 Wind Gust Augmented Aircraft Dynamic Model

The atmosphere is composed of many individual patches of continuous turbulence, each of which may be described by a power spectral density. To model atmospheric turbulence, a random velocity disturbance is generated by filtering white noise, the variance of which is the root-mean-square (rms) gust velocity intensity [16]. Utilizing this stochastic model for longitudinal gust dynamics provides a generalized statistical approach to evaluate the gust impact on aircraft dynamics.

4.4.1 Wind Gust Dynamic Model. Figure 4.3 shows a block diagram for generating the vertical spatial components of gust velocity and the aircraft's response to them. Driving the second-order linear and first-order angular filters G_{w_g} and G_{q_g} with white noise η_g yields linear vertical gust velocity w_g and angular pitch rate q_g which can be used as wind disturbance inputs to an aircraft dynamic model $\boldsymbol{F}_d$.

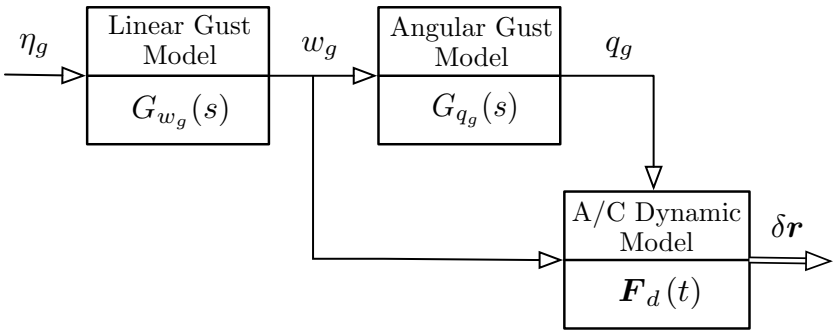

Figure 4.3. Interaction between the Dryden vertical wind gust turbulence model and the linearized aircraft dynamic model. The input η_g is white noise representing the wind gust intensity and the output $\delta \boldsymbol{r}$ is the position deviation due to wind gust disturbance on aircraft.

Among the variety of existing gust filter models, the Dryden and Von Karman models are generally used for continuous gusts in flight dynamics applications [33]. In this work, we chose the Dryden Model to represent longitudinal (vertical) gust dynamics; it is expressed in state-space form as

$$\dot{\boldsymbol{x}}_g = \boldsymbol{F}_g \boldsymbol{x}_g + \boldsymbol{G}_\eta \eta_g \tag{4.13}$$

where $\eta_g \sim \mathcal{N}(0, \sigma_g^2)$, and $\boldsymbol{x}_g = [x_{w_1}, x_{w_2}, x_q]^T$ represents longitudinal gust states where x_{w_1} and x_{w_2} are for linear gust model, and x_q is for angular gust model (details are in Appendix B). Let $\boldsymbol{w}_g$ be the wind gust disturbance to aircraft longitudinal motion containing the perturbations in vertical linear velocity w_g and pitch rate q_g. $\boldsymbol{w}_g = [w_g, q_g]^T$ can be extracted as a function of gust state $\boldsymbol{x}_g$ as

$$\boldsymbol{w}_g = \boldsymbol{C}_g \boldsymbol{x}_g \tag{4.14}$$

where $\boldsymbol{C}_g$ is a constant output coefficient matrix given in Appendix B.

4.4.2 Aircraft Disturbance Response Model. Flight through turbulent air easily excites the short period oscillations for the aircraft. For an airplane in level flight the main source of excitation is the turbulence disturbance [46]. These disturbances are not accounted for by the spoofer, but are sensed by the IMU, which provides the means to detect spoofing attacks. The output of the wind gust model $\boldsymbol{w}_g$ can then

be treated as a disturbance to the open-loop (i.e., $\boldsymbol{\delta}_c = 0$ in (A.15)) vertical aircraft dynamics which can be described as [65]

$$\dot{\boldsymbol{x}}_d = \boldsymbol{F}_d \boldsymbol{x}_d + \boldsymbol{G}_g \boldsymbol{w}_g \tag{4.15}$$

where $\boldsymbol{x}_d = [\delta u, \delta w, \delta q, \delta\theta, \delta h]^T$ including vertical plane velocity components $(\delta u, \delta w)$, and pitch rate δq, pitch angle $\delta\theta$, and altitude δh; $\boldsymbol{G}_g$ is the wind gust disturbance coefficient matrix, the columns of which are the same as the second and third columns of aircraft plant matrix $\boldsymbol{F}_d$, which are defined in detail in Appendix A.

Since the gust noise vector $\boldsymbol{w}_g$ in (4.15) is driven by the gust dynamic model defined in (4.13) and (4.14), the gust-augmented aircraft dynamic model can be written in state-space form as

$$\begin{bmatrix} \dot{\boldsymbol{x}}_d \\ \dot{\boldsymbol{x}}_g \end{bmatrix} = \underbrace{\begin{bmatrix} \boldsymbol{F}_d & \boldsymbol{G}_g \boldsymbol{C}_g \\ \boldsymbol{0} & \boldsymbol{F}_g \end{bmatrix}}_{\boldsymbol{F}_{dg}} \underbrace{\begin{bmatrix} \boldsymbol{x}_d \\ \boldsymbol{x}_g \end{bmatrix}}_{\boldsymbol{x}_{dg}} + \underbrace{\begin{bmatrix} \boldsymbol{0} \\ \boldsymbol{G}_\eta \end{bmatrix}}_{\boldsymbol{G}'_\eta} \eta_g \tag{4.16}$$

where $\boldsymbol{G}'_\eta$ is the noise coefficient matrix of the augmented dynamic model, $\boldsymbol{F}_{dg}$ is the augmented plant matrix, and $\boldsymbol{x}_{dg}$ is the augmented dynamic state vector capturing the additional gust states. The main goal here is to obtain the covariance of position deviation $\delta\boldsymbol{r} = [\delta r_N, \delta r_E, \delta h]^T$ due to wind gust disturbances, which will then be used to compute covariance of the resultant fault in (4.12). It is assumed that there is no deviations on the horizontal (north and east) position components, that is $\delta r_N = \delta r_E = 0$, which conservatively simplifies the analysis. To obtain the vertical position deviation δh, we first compute the covariance of the augmented aircraft states $\boldsymbol{x}_{dg}$ and extract the covariance on δh.

Assuming steady-state wind gust conditions and knowing that the Dryden gust model $\boldsymbol{F}_g$ and aircraft model $\boldsymbol{F}_d$ are stable, we can obtain the steady-state covariance of $\boldsymbol{x}_{dg}$ by numerically solving the Lyapunov equation

$$0 = \boldsymbol{F}_{dg} \boldsymbol{P}^s_{dg} + \boldsymbol{P}^s_{dg} \boldsymbol{F}^T_{dg} + \boldsymbol{G}'_\eta \boldsymbol{G}'^T_\eta \sigma_g^2 \tag{4.17}$$

where $\boldsymbol{P}_{dg}^{s}$ is the steady-state error covariance of $\boldsymbol{x}_{dg}$. The superscript s stands for steady-state value.

The output $\delta\boldsymbol{r}$ of the linearized aircraft model in Figure 4.3, which will feed the GNSS measurement model in the monitor performance evaluation, contains the vertical deviations in aircraft position due to wind gusts. This represents the difference between the actual position and the nominal position that the spoofer assumes.

The discrete form of (4.16) is

$$\boldsymbol{x}_{dg_{k+1}} = \boldsymbol{\Phi}_{dg}\,\boldsymbol{x}_{dg_k} + \boldsymbol{\Gamma}_{\eta}\eta_{g_k} \tag{4.18}$$

where $\boldsymbol{\Phi}_{dg}$ is the state transition matrix of the process model $\boldsymbol{F}_{dg}$ and $\boldsymbol{\Gamma}_{\eta}$ is the discrete form of $\boldsymbol{G}_{\eta}^{'}$. The batch form containing all the time history of the augmented dynamic state $\boldsymbol{x}_{dg}$ in (4.18) can be written as

$$\begin{bmatrix} 0 \\ 0 \\ 0 \\ \vdots \end{bmatrix} = \underbrace{\begin{bmatrix} -\boldsymbol{I} & 0 & 0 & \\ \boldsymbol{\Phi}_{dg} & -\boldsymbol{I} & 0 & \\ 0 & \boldsymbol{\Phi}_{dg} & -\boldsymbol{I} & \\ & & \ddots & \ddots \end{bmatrix}}_{\boldsymbol{H}_{dg_b}} \underbrace{\begin{bmatrix} \boldsymbol{x}_{dg_0} \\ \boldsymbol{x}_{dg_1} \\ \boldsymbol{x}_{dg_2} \\ \vdots \end{bmatrix}}_{\boldsymbol{x}_{dg_b}} + \underbrace{\begin{bmatrix} \delta\boldsymbol{x}_{dg_0} \\ \boldsymbol{\Gamma}_{\eta}\eta_{g_1} \\ \boldsymbol{\Gamma}_{\eta}\eta_{g_2} \\ \vdots \end{bmatrix}}_{\boldsymbol{\nu}_{dg_b}} \tag{4.19}$$

where $\boldsymbol{H}_{dg}$ is the observation matrix of the batch model, $\boldsymbol{x}_{dg_b}$ is the batch state vector, $\delta\boldsymbol{x}_{dg_0} \sim \mathcal{N}(0, \boldsymbol{P}_{dg}^{s})$ is the initial state vector error, and $\boldsymbol{\nu}_{dg_b} \sim \mathcal{N}(0, \boldsymbol{V}_{dg_b})$ is the total batch measurement error vector where

$$\boldsymbol{V}_{dg_b} = \begin{bmatrix} \boxed{\boldsymbol{P}_{dg}^{s}} & & 0 & \\ & \boxed{\boldsymbol{\Gamma}_{\eta}\boldsymbol{\Gamma}_{\eta}^{T}\sigma_g^2} & & \\ & & \boxed{\boldsymbol{\Gamma}_{\eta}\boldsymbol{\Gamma}_{\eta}^{T}\sigma_g^2} & \\ & 0 & & \ddots \end{bmatrix}. \tag{4.20}$$

Using (4.19) and (4.20), batch state estimate error covariance $\boldsymbol{P}_{dg_b}$ is obtained as

$$\boldsymbol{P}_{dg_b} = (\boldsymbol{H}_{dg_b}^{T}\,\boldsymbol{V}_{dg_b}^{-1}\,\boldsymbol{H}_{dg_b})^{-1}. \tag{4.21}$$

In order to obtain the time history of the covariance of position deviation from nominal due to wind gusts, we first define a transformation matrix $\boldsymbol{T}_{r_b}$ that extracts δh rows

from the batch state vector $\boldsymbol{x}_{dg_b}$ and inserts zeros corresponding to the north δr_N and east δr_E position rows in $\delta \boldsymbol{r}_b$ as

$$\delta \boldsymbol{r}_b = \boldsymbol{T}_{r_b} \boldsymbol{x}_{dg_b} \tag{4.22}$$

where $\delta \boldsymbol{r}_b = [0, 0, \delta h_1, 0, 0, \delta h_2, \ldots]^T$ contains the time history of the position deviations; then, using (4.21) and (4.22), its covariance matrix $\boldsymbol{R}_b$ is computed as

$$\boldsymbol{R}_b = \boldsymbol{T}_{r_b} \boldsymbol{P}_{dg_b} \boldsymbol{T}_{r_b}^T \tag{4.23}$$

where $\delta \boldsymbol{r}_b \sim \mathcal{N}(0, \boldsymbol{R}_b)$.

Note that we will utilize the gust and aircraft dynamic models only to evaluate the detection performance of the monitor in the presence of GNSS spoofed signals. In practice, the aircraft dynamic model is not utilized in the actual aircraft's navigation system or the monitor.

4.5 RAIM Formulation for Fault Detection Performance

Recall that using the residual based detector, it is possible to analytically determine the worst-case sequence of spoofed GNSS measurements that maximizes integrity risk. It should be mentioned that the worst-case fault is computed using the nominal trajectory since it is assumed that the spoofer only has knowledge of the nominal trajectory.

Using (4.12), the batch form of the resultant fault vector $\boldsymbol{f}$ can be reformulated in terms of $\delta \boldsymbol{r}$ and worst-case fault $\boldsymbol{f}_w$ as

$$\boldsymbol{f}_b = \underbrace{\begin{bmatrix} 0 \\ \boldsymbol{f}_{w_1} \\ 0 \\ \boldsymbol{f}_{w_2} \\ \vdots \end{bmatrix}}_{\boldsymbol{f}_{w_b}} - \underbrace{\begin{bmatrix} 0 & & & \\ \boldsymbol{G}_{\rho\phi_1} & & 0 & \\ & 0 & & \\ & \boldsymbol{G}_{\rho\phi_2} & & \\ 0 & & \ddots & \end{bmatrix}}_{\boldsymbol{G}_b} \underbrace{\begin{bmatrix} \delta \boldsymbol{r}_1 \\ \delta \boldsymbol{r}_2 \\ \\ \\ \vdots \end{bmatrix}}_{\delta \boldsymbol{r}_b} \tag{4.24}$$

where $\boldsymbol{f}_{w_b}$ is the worst-case fault profile computed using (4.9) and $\delta\boldsymbol{r}_b \sim \mathcal{N}(0, \boldsymbol{R}_b)$ is the time history of position deviations due to wind gust derived in (4.22) with $\boldsymbol{R}_b$ obtained from (4.23).

When quantifying the performance of the monitor, we need to use the resultant fault vector $\boldsymbol{f}_b$ in the residual equation. Therefore, substituting (4.24) into (4.6) results in

$$\mathbf{r} = \big(\boldsymbol{I} - \boldsymbol{H}_b \boldsymbol{H}_b^{+}\big)\big(\boldsymbol{\nu}_b + \boldsymbol{f}_{w_b} - \boldsymbol{G}_b \delta\boldsymbol{r}_b\big) \tag{4.25}$$

The new formulation of the residual in (4.25) captures the wind gust effect in the last term. Therefore, we can quantify the effect of the wind gust on the detection capability of the monitor in terms of integrity risk. Similarly, the state estimate error in (4.4) is modified to

$$\varepsilon_k = \boldsymbol{t}_\varepsilon \boldsymbol{H}_b^{+}\left(\boldsymbol{\nu}_b + \boldsymbol{f}_{w_b} - \boldsymbol{G}_b \delta\boldsymbol{r}_b\right) \tag{4.26}$$

In most RAIM implementations, the test statistics and estimate errors are independent, and therefore the probability on the right hand side of (4.8) is written as a product of the two probabilities. However, due to the influence of wind gusts, which are unknown to the spoofer generating the GNSS measurements, the estimate error ε_k in (4.26) and test statistic q_k obtained from weighted norm of the residual in (4.25) are correlated. Computing the integrity risk with correlated ε and q is difficult because q is χ^2 distributed whereas ε is normally distibuted. Alternatively, it is known (see, for example [40]) that the weighted norm of the residual (test statistic) is equal to the norm of the parity vector. Therefore, we can define an equivalent approach to evaluating the integrity risk by first obtaining a parity vector $\boldsymbol{p}$ using the residual vector of the whitened model. The whitened model can be obtained as

$$\underbrace{\boldsymbol{V}_b^{-1/2}\boldsymbol{z}_b}_{\overline{\boldsymbol{z}}_b} = \underbrace{\boldsymbol{V}_b^{-1/2}\boldsymbol{H}_b}_{\overline{\boldsymbol{H}}_b}\boldsymbol{x}_b + \underbrace{\boldsymbol{V}_b^{-1/2}\boldsymbol{\nu}_b}_{\overline{\boldsymbol{\nu}}_b} + \underbrace{\boldsymbol{V}_b^{-1/2}\boldsymbol{f}_{w_b}}_{\overline{\boldsymbol{f}}_{w_b}} - \underbrace{\boldsymbol{V}_b^{-1/2}\boldsymbol{G}_b}_{\overline{\boldsymbol{G}}_b}\delta\boldsymbol{r}_b \tag{4.27}$$

which results in $\overline{\boldsymbol{\nu}}_b \sim \mathcal{N}\big(\mathbf{0}, \boldsymbol{I}\big)$. Note that the bar notation represents the whitened

model. The residual vector of the whitened system becomes

$$\bar{\mathbf{r}} = \left(\boldsymbol{I} - \overline{\boldsymbol{H}}_b\,\overline{\boldsymbol{S}}_b\right)\left(\overline{\boldsymbol{\nu}}_b + \overline{\boldsymbol{f}}_{w_b} - \overline{\boldsymbol{G}}_b\,\delta\boldsymbol{r}_b\right) \tag{4.28}$$

The parity vector $\boldsymbol{p}$ is defined as

$$\boldsymbol{p} = \boldsymbol{L}\,\bar{\mathbf{r}} \tag{4.29}$$

where $\boldsymbol{L}$ is the unitary left null-space matrix of $\overline{\boldsymbol{H}}_b$ such that $\boldsymbol{L}\overline{\boldsymbol{H}}_b = 0$. It can be obtained using singular value decomposition of $\overline{\boldsymbol{H}}_b$ as

$$\overline{\boldsymbol{H}}_b = [\boldsymbol{U}_1 \;\; \boldsymbol{U}_2] \begin{bmatrix} \boldsymbol{S} \\ 0 \end{bmatrix} \boldsymbol{V}^T \tag{4.30}$$

$$\boldsymbol{L} = \boldsymbol{U}_2^T \tag{4.31}$$

The parity vector $\boldsymbol{p}$ in (4.29) can be expanded as

$$\boldsymbol{p} = \boldsymbol{L}\left(\overline{\boldsymbol{\nu}}_b + \overline{\boldsymbol{f}}_{w_b} - \overline{\boldsymbol{G}}_b\,\delta\boldsymbol{r}_b\right) \tag{4.32}$$

where $\boldsymbol{p}$ is composed of $k(n-m)$ independent Gaussian distributions, and kn and km are the number of measurements and states in the batch, respectively.

By combining the parity vector in (4.32) with the state estimate error in (4.26), we obtain a multi-dimensional Gaussian distribution as

$$[\boldsymbol{p}, \varepsilon_k]^T \sim \mathcal{N}\left(\boldsymbol{\mu}_k, \boldsymbol{\Sigma}_k\right) \tag{4.33}$$

where the mean vector $\boldsymbol{\mu}$ is

$$\boldsymbol{\mu}_k = \begin{bmatrix} \boldsymbol{L} \\ \boldsymbol{t}_\varepsilon \boldsymbol{H}_b^+ \end{bmatrix} \overline{\boldsymbol{f}}_{w_b} \tag{4.34}$$

and the covariance matrix $\boldsymbol{\Sigma}$ is

$$\boldsymbol{\Sigma}_k = \begin{bmatrix} \boldsymbol{I} + \boldsymbol{L}\,\overline{\boldsymbol{G}}_b\,\boldsymbol{R}_b\,\overline{\boldsymbol{G}}_b^T\,\boldsymbol{L}^T & \boldsymbol{H}_b^{+^T}\boldsymbol{t}_\varepsilon^T\,\overline{\boldsymbol{G}}_b\,\boldsymbol{R}_b\,\overline{\boldsymbol{G}}_b^T\,\boldsymbol{L}^T \\ \boldsymbol{L}\,\overline{\boldsymbol{G}}_b\,\boldsymbol{R}_b\,\overline{\boldsymbol{G}}_b^T\,\boldsymbol{t}_\varepsilon\,\boldsymbol{H}_b^+ & \boldsymbol{H}_b^{+^T}\boldsymbol{t}_\varepsilon^T\left(\overline{\boldsymbol{G}}_b\,\boldsymbol{R}_b\,\overline{\boldsymbol{G}}_b^T + \boldsymbol{I}\right)\boldsymbol{t}_\varepsilon\,\boldsymbol{H}_b^+ \end{bmatrix} \tag{4.35}$$

An upper bound on the spoofing integrity risk for a given gust power spectral in (4.36), can be obtained numerically using the multi-dimensional Gaussian distribution derived in (4.33):

$$I_{r_k} < \Pr\left(|\varepsilon_k| > l,\, |\boldsymbol{p}| < \boldsymbol{T}\right) \tag{4.36}$$

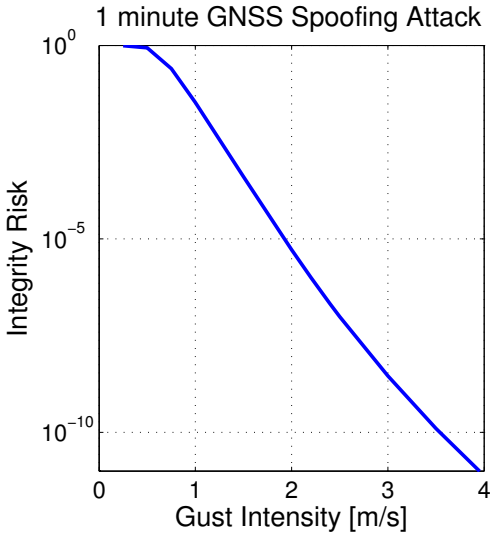

Figure 4.4. The impact of wind gust intensity on integrity risk after 1 minute of level flight of a B747 under a worst-case GNSS spoofing attack.

where $|\boldsymbol{p}|$ is a vector representing element-wise absolute values of $\boldsymbol{p}$, $\boldsymbol{T}$ is a $k(n-m)\times 1$ vector each element of which equals to the square root of the threshold T for the actual detector defined in (3.43), and l is defined as the vertical alert limit. Recall that n and m are the number of measurements and states at each time epoch, respectively.

4.6 Performance Evaluation Results

In this section, a covariance analysis is implemented to quantify the impact of wind gust on the integrity risk during precision landing approach for the worst-case GNSS spoofing attack. However, we assume that the spoofer broadcast has a limited range, and therefore that the spoofing attack is of limited duration. A B747 commercial aircraft model is selected to test the performance of the proposed INS monitor against worst case spoofing attack under various vertical wind gust conditions. The aircraft model parameters are given in Table F.5. The aircraft is assumed to descend in trimmed (level) flight conditions and only the vertical components of the aircraft and gust dynamics are modeled. The nominal flight conditions and corresponding longitudinal aerodynamic coefficients and their derivatives for trimmed

flight conditions are given in Tables F.4 and F.6. The IMU sensor and GNSS receiver specifications can be found in Tables F.1 and F.2, respectively.

The initial covariance $\overline{\boldsymbol{P}}_1$ for the INS states in (3.36) is obtained from a Kalman Filter running during presumed fault free period. At the moment of spoofing, we assume all the GNSS carrier phase cycle ambiguities suffer from cycle slips; therefore we assume no prior knowledge on the cycle ambiguity states, so that $\overline{\boldsymbol{P}}_{n_{\rho\phi}} = \infty$ in (3.36), which is conservative. The reason is that the initial cycle slips increase the uncertainity in the airborne estimator, which allows the spoofer to inject more aggressive faults without being detected.

In Figure 4.4, the results illustrate that the integrity risk diminishes considerably as the wind gust intensity (power spectral density) increases for a worst-case spoofing attack lasting up to 1 minute. The results show that even under light turbulence conditions ($\sigma_g < 2.5$ m/s) [33], integrity risk on the order of 10^{-7} can be achieved. This is a promising result since, although we conservatively select one of the biggest aircraft to lessen the airframe's dynamic sensitivity to wind gusts, the minimum wind gust intensity required for detecting a worst-case spoofing scenario is nevertheless relatively low.

To investigate the impact of spoofing time on integrity risk, we ran simulations with wind gust intensity ranging from 0 to 3 m/s and spoofing attack durations of 30 sec to 3 min. The left plot in Figure 4.5 shows the case with no wind gusts and a worst case spoofing attack. The spoofing integrity risk sharply increases to approximately 1 as time increases from 30 sec to 1 min. We conclude that under no-gust conditions, increasing the spoofing time allows the spoofer to inject faults to the system more slowly, which reduces the monitor's ability to detect spoofing attacks by corrupting the estimation of INS states. On the other hand, with very light wind gust intensities ($\sigma_g < 1$ m/s), it is observed in the right plot of Figure 4.5 that although the spoofer

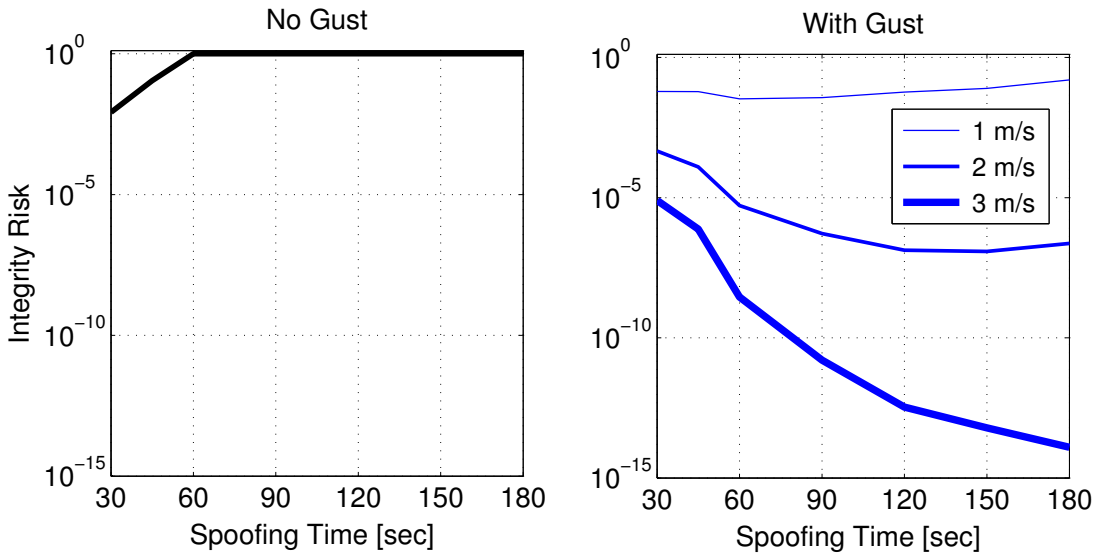

Figure 4.5. The impact of GNSS spoofing attack duration on integrity risk for a B747 landing approach in the no-gust case (left) and several wind gust intensities σ_g ranging from 1 to 3 m/s (right).

Table 4.1. Steady-state Standard Deviations in Vertical Dynamics of a B747 Aircraft Exposed to a 5 m/s Wind Gust Intensity

Standard Deviation	Symbol	Value	Unit
Heading Speed	σ_u	1.42	m/s
Vertical Speed	σ_w	0.24	m/s
Pitch Angle Rate	σ_q	0.13	deg/s
Pitch Angle	σ_θ	0.37	deg

succeeds in deceiving the aircraft's navigation system over time, the integrity risk is still lower than the gust-free case. Furthermore, Figure 4.5 illustrates that with sufficient wind gust intensity ($\sigma_g > 2$ m/s), increasing spoofing time allows for much better detection of GNSS spoofing attacks since the discrepancy between the actual position due to wind gusts and the nominal position assumed by the spoofer grows quickly over time. As a result, the integrity risk decreases over time, unlike gust-free case.

To illustrate that the wind gust intensity values used to generate Figure 4.5 are realistic, we simulate a 3 minute flight of a B747 exposed to a 5 m/s wind gust

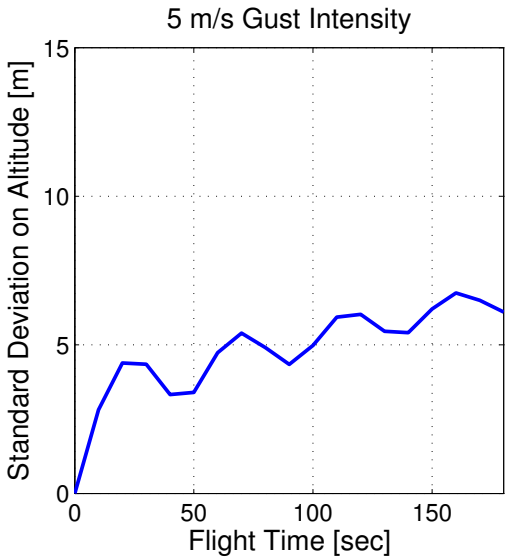

Figure 4.6. The change in altitude standard deviation in the presence of wind gusts having 5 m/s power spectral density for a 3 minute B747 landing approach.

intensity, which is higher than any of the values used in Figure 4.5. The steady-state standard deviations in the vertical dynamics of the aircraft are given in Table 4.1. For example, the steady-state standard deviation in the vertical speed of the aircraft is about 0.24 m/s for the 5 m/s wind gust intensity. Using these steady-state values, the growth in altitude error is shown in Figure 4.6. The standard deviation in vertical position reaches approximately 6 m in 3 min. These values seem realistic given the size of the aircraft and landing approach. Therefore, it can be concluded that, although the wind gust intensities we utilized are not aggressive, the INS monitor is capable of detecting worst-case spoofing attacks.

CHAPTER 5

MONITOR PERFORMANCE AGAINST CLOSED–LOOP TRACKING AND SPOOFING

In this chapter, we evaluate the performance of the Kalman filter innovations-based monitor in a tightly-coupled INS/GNSS mechanization. For performance analysis purposes, we use aircraft shipboard landing as an example application, but the methods introduced here are also applicable to other GNSS relative navigation systems that are tightly-coupled with inertial sensors.

One assumption made in Chapter 4 is that the spoofer does not have real-time knowledge of the actual aircraft position during spoofing attack. In this chapter, we consider spoofers capable of tracking and estimating the real-time position of the target aircraft – for example, by means of remote tracking from the ground. The monitor performance is evaluated against worst-case spoofing attacks by first constructing a mathematical framework to quantify the post-monitor spoofing integrity risk, then deriving an analytical expression of the worst-case sequence of spoofed GNSS signals. We also allow for a maximum level of awareness on the part of the spoofer by introducing a stochastic methodology for the spoofer to account for his/her own tracking sensor errors in his/her worst-case fault derivation. We finally apply these to an example spoofing attack on an aircraft on final approach. The results show that GNSS spoofing is easily detected, with high integrity, unless the spoofer's position-tracking devices have unrealistic, near-perfect accuracy and no-delays.

5.1 Evaluation Model for Spoofing Monitor Performance

In this section, we build a comprehensive performance evaluation model that captures the aircraft controller dynamic response (actuated by either the pilot or

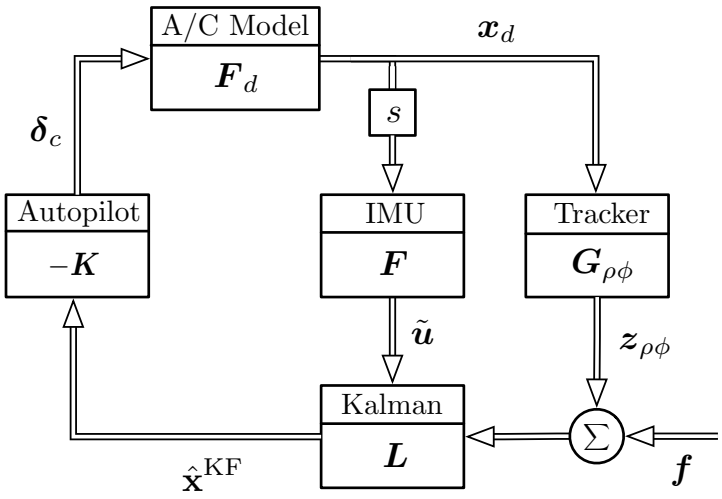

Figure 5.1. INS monitor performance evaluation model capturing the closed-loop relation between the INS estimator (observer) and the altitude hold autopilot (controller) in presence of a GNSS spoofing attack with aircraft position tracking. The spoofer's deliberate fault $\boldsymbol{f}$ is the input of the model, which impacts the output of the Kalman estimator.

autopilot) to a worst-case spoofing attack, augmented with a Kalman filter-based estimator and innovations-based INS detector dynamics. In this model, the spoofed measurements are input to the estimator and detector. The impact of the real-time position tracking and spoofing on the aircraft's compensation system and motion is described in the closed loop block diagram in Fig. 5.1.

5.1.1 Closed Loop Spoofed Measurements. The DD GNSS ranging measurement vector $\boldsymbol{z}_{\rho\phi_k}$ was previously defined in (3.3). Under a spoofing attack, the DD GNSS measurement that the aircraft receives will be the spoofer's broadcast $\boldsymbol{z}^s_{\rho\phi_k}$ which is expressed as

$$\boldsymbol{z}^s_{\rho\phi_k} = \boldsymbol{H}_k \hat{\mathbf{x}}^s_k + \boldsymbol{\nu}_{\rho\phi_k} + \boldsymbol{f}_k \tag{5.1}$$

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

The spoofer's estimate of the aircraft state vector $\hat{\mathbf{x}}^s_k$ can be expressed in terms

of the actual state $\mathbf{x}_k$ as

$$\hat{\mathbf{x}}_k^s = \mathbf{x}_k + \tilde{\mathbf{x}}_k^s \tag{5.2}$$

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

Substituting (5.2) into (5.1), the spoofed measurement becomes

$$\boldsymbol{z}_{\rho\phi_k}^s = \boldsymbol{H}_k \mathbf{x}_k + \boldsymbol{\nu}_{\rho\phi_k} + \underbrace{\boldsymbol{H}_k \tilde{\mathbf{x}}_k^s + \boldsymbol{f}_k}_{\boldsymbol{f}_k^{'}} \tag{5.3}$$

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

It is assumed that the spoofer is capable of measuring the aircraft position using an optical sensor, for example a laser ranging system. The resulting estimation error $\tilde{\mathbf{x}}_k^s$ in (5.3) is modeled as white Gaussian noise, which is a conservative assumption. The reason is that, any filtering or smoothing by the spoofer will cause a phase delay between the aircraft's actual dynamic response to the spoofing attack (actuated by autopilot) and the spoofer's estimate of it. This, in turn, will be reflected as an inconsistency between INS and GNSS measurements and improve the detection capability of the monitor [58].

Under a spoofing attack, the nominal measurement $\boldsymbol{z}_{\rho\phi_k}$ in the estimator's measurement update equation (3.6) is replaced with the spoofed measurement $\boldsymbol{z}_{\rho\phi_k}^s$ in (5.3):

$$\hat{\mathbf{x}}_k^{\mathrm{KF}} = \overline{\mathbf{x}}_k^{\mathrm{KF}} + \boldsymbol{L}_k\big(\boldsymbol{z}_{\rho\phi_k}^s - \boldsymbol{H}_k \overline{\mathbf{x}}_k^{\mathrm{KF}}\big). \tag{5.4}$$

Substituting (5.3) into (5.4) gives

$$\hat{\mathbf{x}}_k^{\mathrm{KF}} = \underbrace{\big(\boldsymbol{I} - \boldsymbol{L}_k \boldsymbol{H}_k\big)}_{\boldsymbol{L}_k^{'}} \overline{\mathbf{x}}_k^{\mathrm{KF}} + \boldsymbol{L}_k \boldsymbol{H}_k \mathbf{x}_k + \boldsymbol{L}_k\big(\boldsymbol{\nu}_{\rho\phi_k} + \boldsymbol{f}_k^{'}\big). \tag{5.5}$$

Substituting the time update equation (3.5) into (5.5), we then have

$$\hat{\mathbf{x}}_k^{\mathrm{KF}} = \boldsymbol{L}_k^{'} \boldsymbol{\Phi}_{\mathrm{x}} \hat{\mathbf{x}}_{k-1}^{\mathrm{KF}} + \boldsymbol{L}_k \boldsymbol{H}_k \mathbf{x}_k + \boldsymbol{L}_k^{'} \boldsymbol{\Gamma}_{\mathrm{x}} \tilde{\boldsymbol{u}}_{k-1} + \boldsymbol{L}_k\big(\boldsymbol{\nu}_{\rho\phi_k} + \boldsymbol{f}_k^{'}\big). \tag{5.6}$$

Let us define the state estimate error as $\tilde{\mathbf{x}}_k^{\mathrm{KF}} = \hat{\mathbf{x}}_k^{\mathrm{KF}} - \mathbf{x}_k$. Subtracting the INS kinematic equation (3.2) from (5.6) gives the state estimate error dynamics as

$$\tilde{\mathbf{x}}_k^{\mathrm{KF}} = \boldsymbol{L}_k^{'}\boldsymbol{\Phi}_{\mathrm{x}}\tilde{\mathbf{x}}_{k-1}^{\mathrm{KF}} - \boldsymbol{L}_k^{'}\overline{\boldsymbol{w}}_{k-1} + \boldsymbol{L}_k\big(\boldsymbol{\nu}_{\rho\phi_k} + \boldsymbol{f}_k^{'}\big). \tag{5.7}$$

Similarly, the innovation vector under a spoofing attack is obtained by replacing the nominal measurement $\boldsymbol{z}_{\rho\phi_k}$ in (3.10) with the spoofed measurement $\boldsymbol{z}_{\rho\phi_k}^{s}$ in (5.3) as

$$\boldsymbol{\gamma}_k = \boldsymbol{z}_{\rho\phi_k}^{s} - \boldsymbol{H}_k\overline{\mathbf{x}}_k^{\mathrm{KF}}. \tag{5.8}$$

Using (3.2) and (3.5), the current innovation vector $\boldsymbol{\gamma}_k$ in (5.8) can be expressed in terms of the previous state estimate error $\tilde{\mathbf{x}}_{k-1}^{\mathrm{KF}}$ as

$$\boldsymbol{\gamma}_k = \boldsymbol{f}_k^{'} + \boldsymbol{\nu}_{\rho\phi_k} - \boldsymbol{H}_k\big(\boldsymbol{\Phi}_{\mathrm{x}}\tilde{\mathbf{x}}_{k-1}^{\mathrm{KF}} - \overline{\boldsymbol{w}}_{k-1}\big). \tag{5.9}$$

Augmenting the INS kinematic model in (3.2) with the state estimate error model in (5.7) and the innovation model in (5.9) results in a performance evaluation model capturing the impact of the error in spoofer's tracking sensors and the fault on the actual state, the state estimate error, and the innovation:

$$\begin{bmatrix} \mathbf{x}_k \\ \tilde{\mathbf{x}}_k^{\mathrm{KF}} \\ \boldsymbol{\gamma}_k \end{bmatrix} = \begin{bmatrix} \boldsymbol{\Phi}_{\mathrm{x}} & 0 & 0 \\ 0 & \boldsymbol{L}_k^{'}\boldsymbol{\Phi}_{\mathrm{x}} & 0 \\ 0 & -\boldsymbol{H}_k\boldsymbol{\Phi}_{\mathrm{x}} & 0 \end{bmatrix} \begin{bmatrix} \mathbf{x}_{k-1} \\ \tilde{\mathbf{x}}_{k-1}^{\mathrm{KF}} \\ \boldsymbol{\gamma}_{k-1} \end{bmatrix} + \begin{bmatrix} \boldsymbol{\Gamma}_{\mathrm{x}} \\ 0 \\ 0 \end{bmatrix} \tilde{\boldsymbol{u}}_{k-1} + \begin{bmatrix} \boldsymbol{I} & 0 \\ -\boldsymbol{L}_k^{'} & \boldsymbol{L}_k \\ \boldsymbol{H}_k & \boldsymbol{I} \end{bmatrix} \begin{bmatrix} \overline{\boldsymbol{w}}_{k-1} \\ \boldsymbol{\nu}_{\rho\phi_k} \end{bmatrix} + \begin{bmatrix} 0 \\ \boldsymbol{L}_k \\ \boldsymbol{I} \end{bmatrix} \boldsymbol{f}_k^{'}. \tag{5.10}$$

5.1.2 Augmented Observer and Controller. To include pilot/autopilot action, whose goal is to follow the prescribed final approach glidepath, we incorporate an altitude autopilot into the aircraft compensator model. Assuming that there is a spoofing attack during the landing approach, this altitude controller will respond to the spoofing attack by inducing control actions; the aircraft's response will be measured by the IMU. To quantify the impact of the motion induced by these control actions on the IMU measurements $\tilde{\boldsymbol{u}}$ in (5.10), we utilize a closed loop compensation model (Fig. 5.1) including an observer feedback based on the output of the Kalman

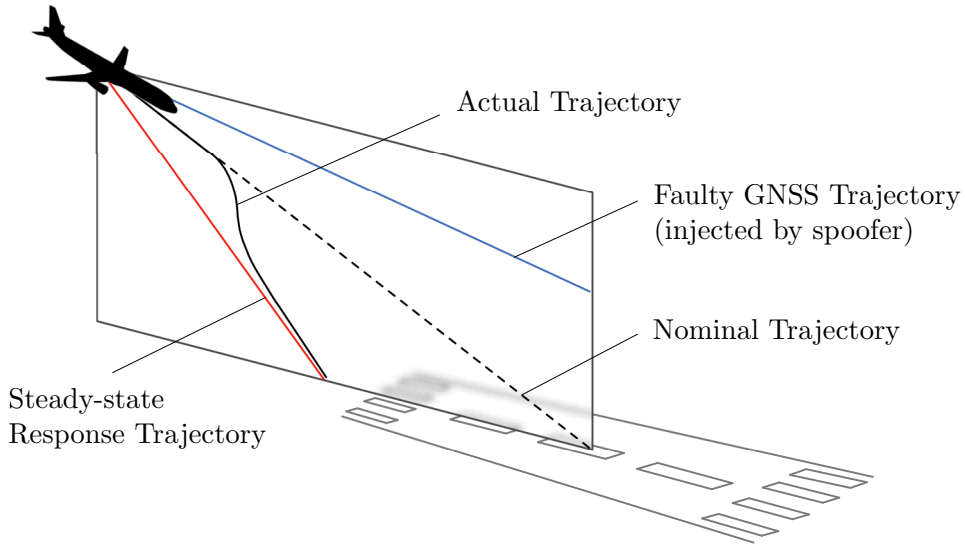

Figure 5.2. Impact of the position fault and the consequent autopilot response to the spoofing attack on the aircraft trajectory. The dotted line is the nominal or planned approach trajectory, the blue line represents the faulty positions injected by the spoofer, the red line is the steady-state trajectory that the aircraft will maneuver toward in response to the spoofed signal, and the black curve is the actual flight path due to autopilots response to the spoofing attack. Note that the blue and red trajectories are symmetric about the nominal approach line.

filter estimator. Due to the presence of the spoofing fault in the estimator's output $\hat{\boldsymbol{x}}$, the altitude-hold autopilot generates a control input $\boldsymbol{\delta}_c$ (elevator and thrust) resulting in a correction maneuver (the black curve in Fig. 5.2).

To capture the aircraft's response in this closed loop system, we use the aircraft dynamic model in (A.15)

$$\dot{\boldsymbol{x}}_d = \boldsymbol{F}_d \boldsymbol{x}_d + \boldsymbol{G}_\delta \boldsymbol{\delta}_c \tag{5.11}$$

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

The discrete form of (5.11) is

$$\boldsymbol{x}_{d_k} = \boldsymbol{\Phi}_d \boldsymbol{x}_{d_{k-1}} + \boldsymbol{\Gamma}_\delta \boldsymbol{\delta}_{c_{k-1}} \tag{5.12}$$

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

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

$$\boldsymbol{\delta}_{c_k} = -\boldsymbol{K}_{\mathrm{x}} \hat{\mathbf{x}}_k^{\mathrm{KF}} - \boldsymbol{K}_q \delta\hat{q}_k \tag{5.13}$$

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

Since the conventional INS state vector $\mathbf{x}_k$ does not contain the pitch rate δq_k, which is required for the controller, the control law in (5.13) is separated into two terms. Remember $\boldsymbol{u}_k = [\ldots, \delta q_k, \ldots]^T$ is the vector containing specific force and angular velocity, therefore the pitch rate estimate $\delta\hat{q}_k$ in (5.13) can be extracted as $\delta\hat{q}_k = \boldsymbol{T}_q \hat{\boldsymbol{u}}_k$. Using (4.15), $\hat{\boldsymbol{u}}_k$ is obtained in terms of the IMU measurement vector $\tilde{\boldsymbol{u}}_k$ as $\hat{\boldsymbol{u}}_k = \tilde{\boldsymbol{u}}_k - \hat{\boldsymbol{b}}_k$. Recall $\mathbf{x}_k = [\ldots, \boldsymbol{b}_k, \ldots]^T$, therefore the bias estimate $\hat{\boldsymbol{b}}_k$ is extracted as $\hat{\boldsymbol{b}}_k = \boldsymbol{T}_b \hat{\mathbf{x}}_k^{\mathrm{KF}}$. Substituting these transformations into (5.13), the control input is re-written as

$$\boldsymbol{\delta}_{c_k} = -\big(\boldsymbol{K}_x - \boldsymbol{K}_q \boldsymbol{T}_q \boldsymbol{T}_b\big)\hat{\mathbf{x}}_k^{\mathrm{KF}} - \boldsymbol{K}_q \boldsymbol{T}_q \tilde{\boldsymbol{u}}_k. \tag{5.14}$$

The main aim of introducing the aircraft dynamic model in (5.11) is to augment the controller and observer through the specific force and angular velocity $\boldsymbol{u}$ measured by the IMU. $\boldsymbol{u}$ can be extracted from the aircraft state derivative $\dot{\boldsymbol{x}}_d$ as $\boldsymbol{u} = \boldsymbol{T}_u \dot{\boldsymbol{x}}_d$ where $\boldsymbol{T}_u$ is a 6×5 matrix that extracts the longitudinal specific forces and angular rates from $\dot{\boldsymbol{x}}_d$ and inserts zeros corresponding to the lateral ones. This can be re-expressed in discrete form by utilizing (5.11) as

$$\boldsymbol{u}_k = \boldsymbol{T}_u\big(\boldsymbol{F}_d \boldsymbol{x}_{d_k} + \boldsymbol{G}_\delta \boldsymbol{\delta}_{c_k}\big) \tag{5.15}$$

Substituting (5.15) with the transformations $\boldsymbol{b}_k = \boldsymbol{T}_b \mathbf{x}_k$ and $\boldsymbol{\nu}_{n_k} = \boldsymbol{T}_\nu \boldsymbol{w}_k$ into

the IMU measurement model (2.26), we obtain the IMU measurement $\tilde{\boldsymbol{u}}_k$ as

$$\tilde{\boldsymbol{u}}_k = \boldsymbol{T}_u\big(\boldsymbol{F}_d\,\boldsymbol{x}_{d_k} + \boldsymbol{G}_\delta\,\boldsymbol{\delta}_{c_k}\big) + \boldsymbol{T}_b\,\mathbf{x}_k + \boldsymbol{T}_\nu\,\boldsymbol{w}_k \tag{5.16}$$

where recall that $\boldsymbol{w}_k \sim \mathcal{N}(0, \boldsymbol{W}_k)$ was previously defined in (2.28).

Using $\hat{\mathbf{x}}_k^{\mathrm{KF}} = \mathbf{x}_k + \tilde{\mathbf{x}}_k^{\mathrm{KF}}$, one can solve for $\tilde{\boldsymbol{u}}_k$ and $\boldsymbol{\delta}_{c_k}$ in (5.14) and (5.16) in terms of the actual navigation state $\mathbf{x}_k$ and its estimate error $\tilde{\mathbf{x}}_k^{\mathrm{KF}}$, the aircraft state $\boldsymbol{x}_{d_k}$, and the INS process noise $\boldsymbol{w}_k$ as

$$\tilde{\boldsymbol{u}}_k = \boldsymbol{U}_{\mathrm{x}}\mathbf{x}_k + \boldsymbol{U}_{\tilde{\mathrm{x}}}\tilde{\mathbf{x}}_k^{\mathrm{KF}} + \boldsymbol{U}_d\,\boldsymbol{x}_{d_k} + \boldsymbol{U}_w\,\boldsymbol{w}_k \tag{5.17}$$

and

$$\boldsymbol{\delta}_k = \boldsymbol{\Delta}_{\mathrm{x}}\mathbf{x}_k + \boldsymbol{\Delta}_{\tilde{\mathrm{x}}}\tilde{\mathbf{x}}_k^{\mathrm{KF}} + \boldsymbol{\Delta}_d\,\boldsymbol{x}_{d_k} + \boldsymbol{\Delta}_w\,\boldsymbol{w}_k, \tag{5.18}$$

respectively, where the coefficient matrices in (5.17) and (5.18) are obtained as functions of the state feedback gain matrices $\boldsymbol{K}_{\mathrm{x}}$ and $\boldsymbol{K}_q$, and aircraft dynamic model parameters $\boldsymbol{F}_d$ and $\boldsymbol{G}_\delta$, which are derived in Appendix E.

5.1.3 Augmented Performance Evaluation Model. Augmenting the aircraft model in (5.12) and the Kalman model in (5.10) with the substitutions in (5.17) and (5.18) yields a closed-loop evaluation model [7] as

$$\begin{bmatrix} \mathbf{x}_k \\ \tilde{\mathbf{x}}_k^{\mathrm{KF}} \\ \boldsymbol{\gamma}_k \\ \boldsymbol{x}_{d_k} \end{bmatrix} = \overbrace{\begin{bmatrix} \boldsymbol{\Phi}_{\mathrm{x}} + \boldsymbol{\Gamma}_{\mathrm{x}}\boldsymbol{U}_{\mathrm{x}} & \boldsymbol{\Gamma}_{\mathrm{x}}\boldsymbol{U}_{\tilde{\mathrm{x}}} & 0 & \boldsymbol{\Gamma}_{\mathrm{x}}\boldsymbol{U}_d \\ 0 & \boldsymbol{L}_k^{'}\boldsymbol{\Phi}_{\mathrm{x}} & 0 & 0 \\ 0 & -\boldsymbol{H}_k\boldsymbol{\Phi}_{\mathrm{x}} & 0 & 0 \\ \boldsymbol{\Gamma}_\delta\boldsymbol{\Delta}_{\mathrm{x}} & \boldsymbol{\Gamma}_\delta\boldsymbol{\Delta}_{\tilde{\mathrm{x}}} & 0 & \boldsymbol{\Phi}_d + \boldsymbol{\Gamma}_\delta\boldsymbol{\Delta}_d \end{bmatrix}}^{\boldsymbol{\Phi}_{y_k}} \overbrace{\begin{bmatrix} \mathbf{x}_{k-1} \\ \tilde{\mathbf{x}}_{k-1}^{\mathrm{KF}} \\ \boldsymbol{\gamma}_{k-1} \\ \boldsymbol{x}_{d_{k-1}} \end{bmatrix}}^{\boldsymbol{y}_{k-1}} + \underbrace{\begin{bmatrix} \boldsymbol{I} & 0 & \boldsymbol{\Gamma}_{\mathrm{x}}\boldsymbol{U}_w \\ -\boldsymbol{L}_k^{'} & \boldsymbol{L}_k & 0 \\ \boldsymbol{H}_k & \boldsymbol{I} & 0 \\ 0 & 0 & \boldsymbol{\Gamma}_\delta\boldsymbol{\Delta}_w \end{bmatrix}}_{\boldsymbol{\Upsilon}_{y_k}} \underbrace{\begin{bmatrix} \overline{\boldsymbol{w}}_{k-1} \\ \boldsymbol{\nu}_{\rho\phi_k} \\ \boldsymbol{w}_{k-1} \end{bmatrix}}_{\boldsymbol{w}_{y_k}} + \underbrace{\begin{bmatrix} 0 \\ \boldsymbol{L}_k \\ \boldsymbol{I} \\ 0 \end{bmatrix}}_{\boldsymbol{\Psi}_{y_k}} \boldsymbol{f}_k^{'} \tag{5.19}$$

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

Using (5.19), the mean $\mathbb{E}[\boldsymbol{y}_k]$ and covariance $\boldsymbol{Y}_k$ of the closed-loop evaluation model state vector $\boldsymbol{y}$ can be propagated as

$$\mathbb{E}[\boldsymbol{y}_k] = \boldsymbol{\Phi}_{y_k} \mathbb{E}[\boldsymbol{y}_{k-1}] + \boldsymbol{\Psi}_{y_k} \boldsymbol{f}'_{w_k} \tag{5.20}$$

and

$$\boldsymbol{Y}_k = \boldsymbol{\Phi}_{y_k} \boldsymbol{Y}_{k-1} \boldsymbol{\Phi}_{y_k}^T + \boldsymbol{\Upsilon}_{y_k} \boldsymbol{W}_{y_k} \boldsymbol{\Upsilon}_{y_k}^T, \tag{5.21}$$

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

5.2 Spoofing Integrity Risk

Recalling (3.56), the vertical position estimate error ε_k is extracted from the state estimate error $\tilde{\mathbf{x}}_k^{\mathrm{KF}}$ as

$$\varepsilon_k = \boldsymbol{t}_\varepsilon \tilde{\mathbf{x}}_k^{\mathrm{KF}}. \tag{5.22}$$

The noncentral chi-square distributed cumulative test statistic q_k and its non-centrality parameter λ_k^2 are previously defined in (3.30) and (3.32), respectively, as

$$q_k = \boldsymbol{\gamma}_{1:k}^T \boldsymbol{S}_{1:k}^{-1} \boldsymbol{\gamma}_{1:k} \tag{5.23}$$

and

$$\lambda_k^2 = \mathbb{E}[\boldsymbol{\gamma}_{1:k}^T] \boldsymbol{S}_{1:k}^{-1} \mathbb{E}[\boldsymbol{\gamma}_{1:k}] \tag{5.24}$$

where $\boldsymbol{\gamma}_{1:k} = [\boldsymbol{\gamma}_1, \ldots, \boldsymbol{\gamma}_k]^T$ is the innovations history vector and $\boldsymbol{S}_{1:k}$ is the block diagonal matrix composed of the innovation covariances $\boldsymbol{S}_i$'s ($0 < i \leq k$) which are extracted from $\boldsymbol{Y}$ in (5.21) as

$$\boldsymbol{S}_i = \boldsymbol{T}_\gamma \boldsymbol{Y}_i \boldsymbol{T}_\gamma^T \tag{5.25}$$

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

Using the evaluation model (5.10), it is proved in Appendix D that $\mathbb{E}[\tilde{\mathbf{x}}_i^{\mathrm{KF}} \boldsymbol{\gamma}_j^T] = 0$ for all $i \geq j$. Therefore, the cumulative test statistic q_k obtained from the current

and past innovations and the altitude error ε_k obtained from the current state estimate error will be statistically independent. As a result, integrity risk I_{r_k} in (3.55) can be written as a product of two probabilities

$$I_{r_k} = \Pr\left(|\varepsilon_k| > l\right) \Pr\left(q_k < T\right) \tag{5.26}$$

5.3 Kalman Filter-based Worst–Case Fault Derivation

Because all GNSS measurements may be impacted by the spoofing attack, it is assumed that all GNSS measurements are faulty during the attack period and that the IMU measurements are the only fault-free sources of redundancy in the monitor. If a spoofing attack is not detected instantaneously, it may impact the INS error state estimates through the tightly coupled mechanism, which can degrade subsequent detection ability. Therefore, a smart spoofer may select a fault profile $\boldsymbol{f}_{1:k} = [\boldsymbol{f}_1, \ldots, \boldsymbol{f}_k]^T$ with smaller faults at the beginning and gradually increasing over time, thereby corrupting INS calibration, leading to a lower probability of detection.

A worst-case fault derivation based on a batch estimator was previously introduced in [20]. Here, we extend the theory to derive the worst-case fault profile that maximizes the Kalman filter estimate error associated with the most hazardous state ε_k while minimizing the cumulative test statistic q_k. To obtain the optimal direction and magnitude of the worst-case fault history vector $\boldsymbol{f}_{1:k}$, we use the evaluation model in (5.19) and conservatively assume that the spoofer has knowledge of the exact error models for the aircraft's INS/GNSS system and his/her own position tracking sensor.

Equations (5.20) and (5.24) indicate that the fault history vector $\boldsymbol{f}_{1:k}$ affects the mean of $\tilde{\mathbf{x}}_k$ and the non-centrality parameter λ_k^2 of the cumulative test statistic q_k. The ratio $\mathbb{E}[\varepsilon_k]^2/\lambda_k^2$ is called the failure mode slope ρ_k^2 [20]. The optimization problem for obtaining the worst-case fault can be formulated as

$$\arg\max_{\boldsymbol{f}_{1:k}} \rho_k^2 \tag{5.27}$$

Recall that ε_k and λ_k^2 are functions of the state estimate error $\tilde{\mathbf{x}}_k$ and the innovation history vector $\boldsymbol{\gamma}_{1:k}$, respectively. Also, $\tilde{\mathbf{x}}_k$ and $\boldsymbol{\gamma}_k$ are both linear functions of $\boldsymbol{f}_{1:k}$. Using (5.20) and (5.19), the means of $\tilde{\mathbf{x}}_k$ and $\boldsymbol{\gamma}_k$ can be extracted as

$$\mathbb{E}[\tilde{\mathbf{x}}_k] = \underbrace{\boldsymbol{L}_k^{'}\boldsymbol{\Phi}_{\mathrm{x}}}_{\boldsymbol{L}_k^{''}}\,\mathbb{E}[\tilde{\mathbf{x}}_{k-1}] + \boldsymbol{L}_k\boldsymbol{f}_k \tag{5.28}$$

and

$$\mathbb{E}[\boldsymbol{\gamma}_k] = -\boldsymbol{H}_k\boldsymbol{\Phi}_{\mathrm{x}}\,\mathbb{E}[\tilde{\mathbf{x}}_{k-1}] + \boldsymbol{f}_k, \tag{5.29}$$

respectively, since $\mathbb{E}[\boldsymbol{f}_k^{'}] = \boldsymbol{f}_k$ with the assumption of $\tilde{\mathbf{x}}^s \sim \mathcal{N}(0, \boldsymbol{P}_{\mathrm{x}}^s)$ – i.e., that the spoofer's tracking error is unbiased, which is conservative.

Given a fault-free initial condition as $\mathbb{E}[\tilde{\mathbf{x}}_0] = \mathbb{E}[\boldsymbol{\gamma}_0] = 0$, the particular solution to the difference equation (5.28) is obtained as a function of $\boldsymbol{f}_{1:k}$ as

$$\mathbb{E}[\tilde{\mathbf{x}}_k] = \underbrace{\begin{bmatrix}\boldsymbol{A}_{1k} & \dots & \boldsymbol{A}_{kk}\end{bmatrix}}_{\boldsymbol{A}_k}\underbrace{\begin{bmatrix}\boldsymbol{f}_1\\ \vdots \\ \boldsymbol{f}_k\end{bmatrix}}_{\boldsymbol{f}_{1:k}} \tag{5.30}$$

where

$$\boldsymbol{A}_{ik} = \begin{cases}\boldsymbol{L}_k^{''}\boldsymbol{L}_{k-1}^{''}\dots\boldsymbol{L}_{1+i}^{''}\boldsymbol{L}_i & \text{if } i < k\\ \boldsymbol{L}_i & \text{if } i = k\end{cases}. \tag{5.31}$$

Substituting (5.30) into (5.29) gives the mean of innovation as a function of $\boldsymbol{f}_{1:k}$ as

$$\mathbb{E}[\boldsymbol{\gamma}_k] = \underbrace{\begin{bmatrix}-\boldsymbol{H}_k\boldsymbol{\Phi}\,\boldsymbol{A}_{k-1} & \boldsymbol{I}\end{bmatrix}}_{\boldsymbol{B}_k}\underbrace{\begin{bmatrix}\boldsymbol{f}_{1:k-1}\\ \boldsymbol{f}_k\end{bmatrix}}_{\boldsymbol{f}_{1:k}}. \tag{5.32}$$

Let $\overline{\boldsymbol{B}}_i = \begin{bmatrix}\boldsymbol{B}_i, \mathbf{0}_{n\times n(k-i)}\end{bmatrix}$ where n is the number of measurements at each time epoch and $0 < i < k$. Then, substituting (5.32) into (5.24) gives the non-centrality parameter of the cumulative test statistic in block matrix form as

$$\lambda_k^2 = \boldsymbol{f}_{1:k}^T\begin{bmatrix}\overline{\boldsymbol{B}}_1^T & \dots & \overline{\boldsymbol{B}}_k^T\end{bmatrix}\underbrace{\begin{bmatrix}\boldsymbol{S}_1^{-1} & & \\ & \ddots & \\ & & \boldsymbol{S}_k^{-1}\end{bmatrix}}_{\boldsymbol{S}_{1:k}^{-1}}\underbrace{\begin{bmatrix}\overline{\boldsymbol{B}}_1\\ \vdots \\ \overline{\boldsymbol{B}}_k\end{bmatrix}}_{\overline{\boldsymbol{B}}_{1:k}}\boldsymbol{f}_{1:k} \tag{5.33}$$

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

Substituting (5.30), (5.33) and (5.22) into (5.27) gives the failure mode slope ρ_k as a function of the fault history vector $\boldsymbol{f}_{1:k}$ as

$$\rho_k^2 = \frac{\boldsymbol{f}_{1:k}^T \boldsymbol{A}_k^T \boldsymbol{t}_\varepsilon^T \boldsymbol{t}_\varepsilon \boldsymbol{A}_k \boldsymbol{f}_{1:k}}{\boldsymbol{f}_{1:k}^T \overline{\boldsymbol{B}}_{1:k}^T \boldsymbol{S}_{1:k}^{-1} \overline{\boldsymbol{B}}_{1:k} \boldsymbol{f}_{1:k}}. \tag{5.34}$$

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

$$\breve{\boldsymbol{f}}_{1:k} = \left(\boldsymbol{S}_{1:k}^{-1/2} \overline{\boldsymbol{B}}_{1:k}\right) \boldsymbol{f}_{1:k}. \tag{5.35}$$

The failure mode slope in (5.34) can be rewritten in terms of $\breve{\boldsymbol{f}}_{1:k}$ as

$$\rho_k^2 = \frac{\breve{\boldsymbol{f}}_{1:k}^T \boldsymbol{\kappa}_k \boldsymbol{\kappa}_k^T \breve{\boldsymbol{f}}_{1:k}}{\breve{\boldsymbol{f}}_{1:k}^T \breve{\boldsymbol{f}}_{1:k}} \tag{5.36}$$

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

$$\boldsymbol{\kappa}_k = \left(\boldsymbol{S}_{1:k}^{-1/2} \overline{\boldsymbol{B}}_{1:k}\right)^{-T} \boldsymbol{A}_k^T \boldsymbol{t}_\varepsilon^T. \tag{5.37}$$

From (5.36), it can be concluded that $\breve{\boldsymbol{f}}_{1:k}$ that maximizes the fault mode slope ρ_k^2 must be in the direction of the vector $\boldsymbol{\kappa}_k$. Let us denote the worst-case fault history vector $\boldsymbol{f}_{w_{1:k}}$ with a magnitude α_w and a direction $\mathbf{f}_{w_{1:k}}$ as

$$\boldsymbol{f}_{w_{1:k}} = \alpha_w \, \mathbf{f}_{w_{1:k}} \tag{5.38}$$

Using (5.35) and (5.37), the worst-case fault direction $\mathbf{f}_{w_{1:k}}$ is obtained as

$$\mathbf{f}_{w_{1:k}} = \overline{\boldsymbol{B}}_{1:k}^{-1} \boldsymbol{S}_{1:k} \overline{\boldsymbol{B}}_{1:k}^{-T} \boldsymbol{A}_k^T \boldsymbol{t}_\varepsilon^T \tag{5.39}$$

So far, we analytically obtained the worst-case fault vector direction $\mathbf{f}_{w_{1:k}}$ in (5.39) from a fully deterministic objective function in (5.27). The worst-case fault magnitude α_w in (5.38) is a scalar that maximizes the integrity risk I_{r_k} in (5.26) along the worst-case fault direction. Unlike the worst-case fault direction optimization, the magnitude optimization has a stochastic objective function I_{r_k} in (5.26), which is influenced by the spoofer's position tracking sensor noise. In Sections 5.1 and 5.2, we explained

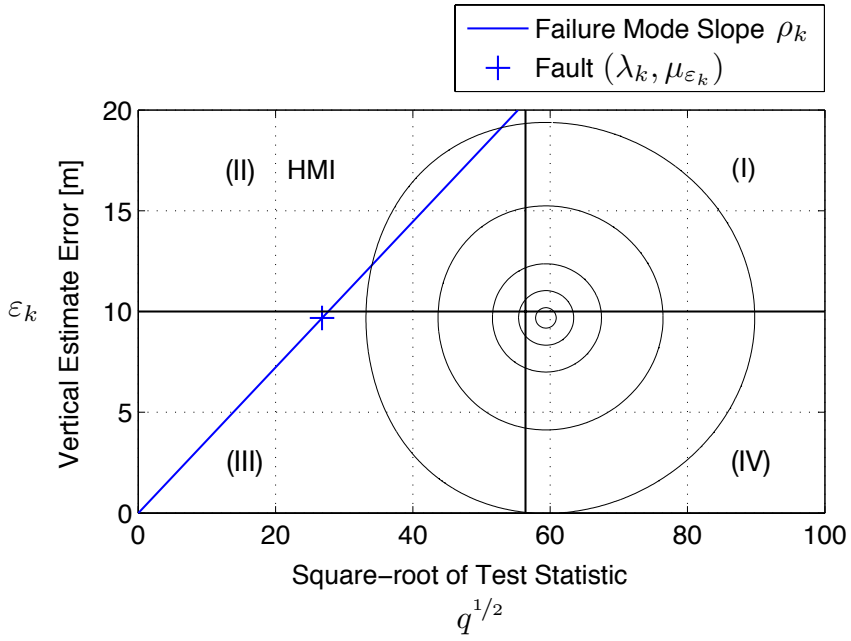

Figure 5.3. The worst-case fault and failure mode slope for a 140 s approach flight of B747 with a GNSS sampling frequency of 2 Hz. The marker (+) on the failure mode slope corresponds to the worst-case fault for this scenario. The black curves are lines of constant joint probability density obtained using (5.26).

how to compute the joint probability $\Pr(|\varepsilon_k| > l, q_k < T)$ for a given vector $\boldsymbol{f}'$, which, as defined in (5.3), assumes a given deterministic spoofer's tracking error $\tilde{\mathbf{x}}^s$. To statistically account for variability in $\tilde{\mathbf{x}}^s$, we express the integrity risk in terms of probability density function $f(\tilde{\mathbf{x}}^s)$ as

$$I_{r_k}(\alpha) = \int_{\tilde{\mathbf{x}}^s} \cdots \int \Pr(|\varepsilon_k| > l, q_k < T; \alpha \mid \tilde{\mathbf{x}}^s)\, f(\tilde{\mathbf{x}}^s)\, \mathrm{d}\tilde{\mathbf{x}}^s \tag{5.40}$$

To compute the integral in (5.40) in the simulation, we generate m samples $\tilde{\mathbf{x}}^s_1, \tilde{\mathbf{x}}^s_2, \ldots, \tilde{\mathbf{x}}^s_m$ from the normally distributed $\tilde{\mathbf{x}}^s \sim \mathcal{N}(0, \boldsymbol{P}^s_{\mathrm{x}})$ and compute the integrity risk for different values of the fault magnitude α

$$I_{r_k}(\alpha) = \frac{1}{m} \sum_{i=1}^{m} \Pr(|\varepsilon_k| > l, q_k < T; \alpha \mid \tilde{\mathbf{x}}^s_i) \tag{5.41}$$

The worst-case value for the fault magnitude α_w is determined through a one dimensional search to maximize $I_{r_k}(\alpha)$ in (5.41). It should be mentioned that even though

a framework for capturing the GNSS measurement fault's effect on the actual aircraft motion (i.e., $\mathbf{x}_k$) in position domain is presented in (5.19), the integrity risk derived in (5.41) is independent from the aircraft motion (i.e., aircraft dynamics). Therefore, the integrity analysis results which are given in the following section apply regardless of the aircraft model. However to illustrate the aircraft's responses to a worst-case spoofing attack, we use an example B747 model since its aerodynamic parameters are publicly available.

5.4 Tightly–Coupled INS Monitor Performance Analysis Results

To test the performance of the INS spoofing monitor, a covariance analysis with a B747 flight on approach is simulated at the standard trimmed flight conditions at 131 knots [14]. The B747 aircraft dynamics are modeled with a generic altitude hold autopilot utilizing the longitudinal stability derivatives in [20] at standard sea-level conditions. The navigation-grade IMU sensor and GNSS receiver specifications are provided in Tables F.1 and F.2, respectively. Since the spoofer is assumed to have a limited range, the spoofing attack will be of limited duration. Therefore, we assume that the state estimator has been running under fault free conditions and has reached steady state before the spoofing attack starts.

To investigate the performance of the INS monitor, we initially assumed a spoofing attack with perfect tracking sensors, capable of tracking the exact aircraft position ($\tilde{\mathbf{x}}_k^s = 0$), and computed the worst-case fault profile for a given spoofing attack period. An example worst-case fault and its failure mode slope for a 140 s B747 approach is illustrated in Fig. 5.3. The square root of the test statistic $q_k^{1/2}$ and vertical position error ε_k are represented on the x-axis and y-axis, respectively. The x-y plane is divided into four quadrants by a vertical alert limit $l = 10$ m and a threshold $T^{1/2} = 56.4$, computed from the inverse cumulative chi-square distribution for a false alarm probability of 10^{-6}. The second quadrant refers to the area of hazardous

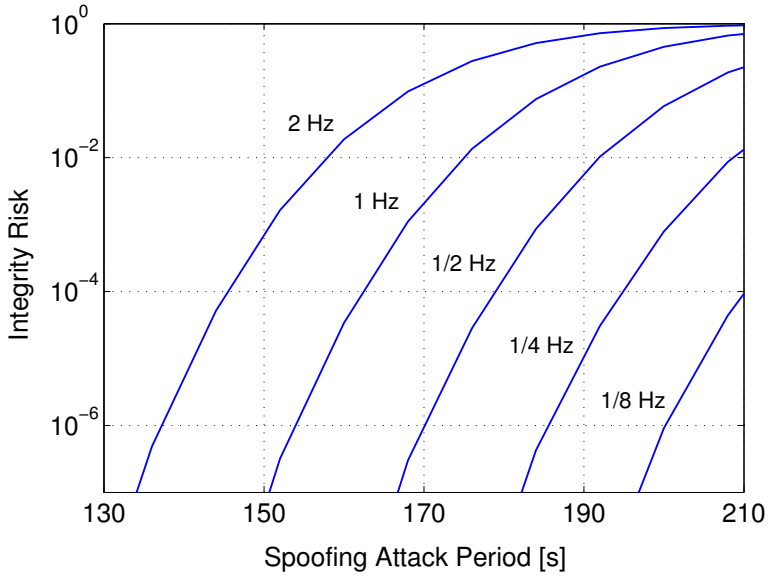

Figure 5.4. The impact of spoofing attack period and GNSS sampling frequency on the integrity risk. The results are obtained for a B747 landing approach in the presence of a worst-case spoofing attack with closed-loop position tracking using a sensor having perfect accuracy and no-delay.

misleading information (HMI), where undetected faults result in unacceptably large estimation errors. The probability of being in the HMI area corresponds to the integrity risk in (5.26). Each point $(\lambda_k, \mu_{\varepsilon_k})$ on or below the failure mode slope line (blue line) on the x-y plane corresponds to a different fault, and for this scenario the worst-case fault $\boldsymbol{f}_{w_{1:k}}$ is obtained at the marker ($\lambda_k = 26.8$ m, $\mu_{\varepsilon_k} = 9.7$ m) located on the worst-case failure mode slope. This worst-case fault results in a distribution represented as the oval shape contours of constant joint probability density (black curves). In this example, the integrity risk for the worst-case fault is computed to be $I_r = 5.9 \times 10^{-6}$.

To quantify the impact of the spoofing attack period on the integrity risk, we obtained the worst-case fault profiles for different attack periods ranging from 130 to 210 s and computed the corresponding integrity risks. As seen in Fig. 5.4, if the spoofer has perfect position tracking sensors, increasing the attack period eventually

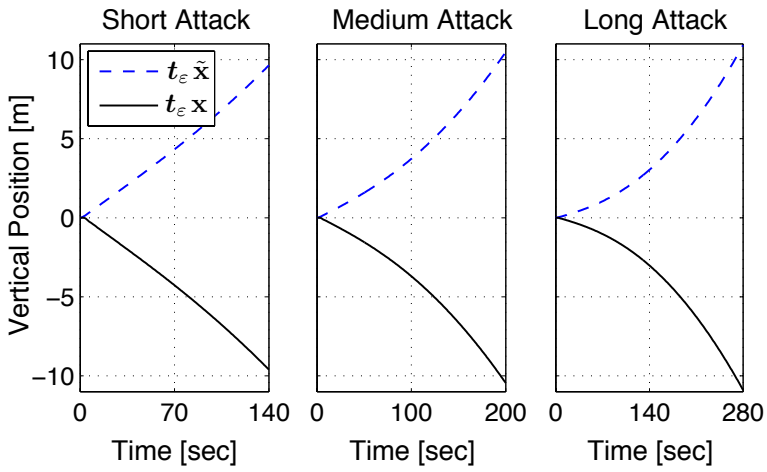

Figure 5.5. The impact of the spoofing attack period on the vertical position components of aircraft true state $\mathbf{x}$ and its estimate error $\tilde{\mathbf{x}}^{\mathrm{KF}}$. In each plot where the worst-case attack periods are ranging from 140 s (left), 200 s (middle), and 280 s (right), the consequent estimate error growth and the aircraft's altitude loss from nominal approach (due to the autopilot response to the injected fault) are plotted. Note that the true state $\mathbf{x}$ and its estimate error $\tilde{\mathbf{x}}^{\mathrm{KF}}$ curves are nearly symmetric due to the autopilot's effort to hold the altitude estimate $\hat{\mathbf{x}}^{\mathrm{KF}}$ at the nominal during approach (i.e., $\hat{\mathbf{x}}^{\mathrm{KF}} = \mathbf{x} + \tilde{\mathbf{x}}^{\mathrm{KF}} = 0$).

causes high integrity risks. The reason is that, increasing the spoofing time allows the spoofer to inject faults to the system in a less aggressive way (see Fig. 5.5), slowly corrupting the estimation of INS states and thereby reducing the monitor's ability to detect the spoofing attack. On the other hand, for limited attack periods, the integrity risk is considerably low. For example, at the GNSS sampling frequency of 2 Hz (Fig. 5.4), the worst-case attacks having a period shorter than 135 s results in integrity risks of less than 10^{-7} even though the spoofer tracks the aircraft position with zero-error. Fig. 5.4 also illustrates that at lower GNSS sampling rates, worst-case spoofing attacks result in lower integrity risks for the same attack periods.

The results so far assume that the spoofer is able to estimate the exact position of the aircraft. In a more realistic scenario, the errors in position tracking must be accounted for. Therefore, we assume that the spoofer's position estimate error is a zero-mean white noise $\tilde{\mathbf{x}}_k^s \sim \mathcal{N}(0, \boldsymbol{P}^s_{\mathrm{x}_k})$ sequence. White noise is typical for laser

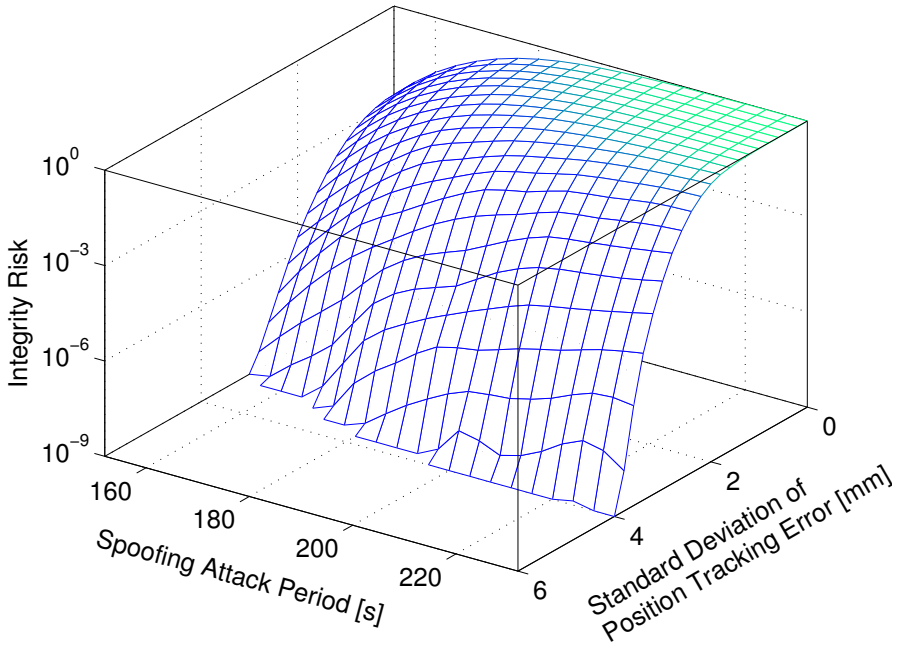

Figure 5.6. The impact of altitude tracking error and attack period on the integrity risk in the presence of worst-case spoofing attacks with a GNSS sampling frequency of 2 Hz.

tracking errors. Utilizing (5.41), we illustrate how the INS monitor leverages the spoofer's altitude tracking errors to detect spoofing attacks. Fig. 5.6 shows that for a position tracking error of more than 4 mm (1-sigma), the integrity risk always remains below 10^{-9}, which is the most stringent safety requirement in aviation applications [37]. Even though 4 mm instantaneous error is very small in the position domain, the monitor integrates these errors over time. The accumulated error has a considerable influence on the detection test statistic, which makes the monitor remarkably sensitive to the spoofing attacks. The results are very promising because such tracking accuracy by the spoofer is unrealistic using any combination of existing high-grade position tracking systems (e.g., laser, radar, vision) [8].

CHAPTER 6

MONITOR PERFORMANCE IN GBAS–ASSISTED AIRCRAFT LANDING APPROACH

In this chapter, we evaluate the performance of the Kalman filter innovations-based monitor in a loosely-coupled INS/GNSS mechanization. Our specific application of interest is aircraft landing approaches assisted by Ground-Based Augmentation Systems (GBAS). In Chapters 4 and 5, we focused on relative navigation applications where both the differential code and carrier measurements are available for use directly in the airborne Kalman filter estimator. On the other hand, in this chapter we assume only the differential carrier-smoothed code measurements are available at the aircraft, which is consistent with both GBAS and SBAS (Space-Based Augmentation Systems) avionics implementations. In this configuration, GBAS position solution is fed into a Kalman filter in a loosely-coupled INS-GNSS integration scheme (Figure 6.1).

In monitor performance evaluation, the Kalman filter-based worst-case fault derivation introduced in Section 5.3 is extended to the loosely-coupled INS-GNSS integration. Utilizing this worst-case fault, we simulate GBAS-assisted landing approaches of a B747 to determine the minimum required accuracy levels of the spoofer's position tracking to produce unacceptably large integrity risk at the aircraft.

6.1 Evaluation Model for Detection Performance

The functional diagram used in the monitor performance evaluation is shown in Figure 6.1. This block diagram captures the closed-loop relation between the Kalman filter (KF), the GBAS airborne smoother (Hatch filter) and weighted least-squares estimator (LSE) in presence of a spoofer capable of tracking the aircraft position and

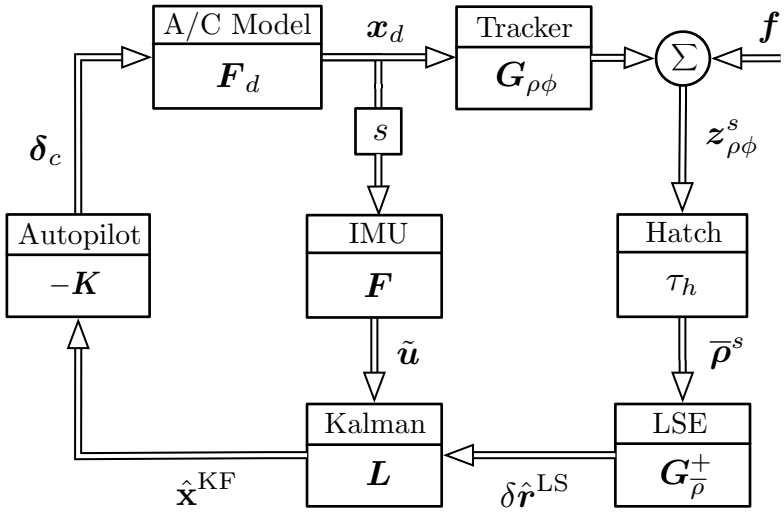

Figure 6.1. The performance evaluation model for the INS spoofing monitor utilizing a loosely-coupled integration of INS and GBAS.

injecting a fault $\boldsymbol{f}$ through GNSS signals $\boldsymbol{\rho}$ and $\boldsymbol{\phi}$.

6.1.1 Spoofed GBAS Position Solution. In a spoofing attack, the spoofer broadcasts raw code and carrier signals, which mimic the actual GNSS signals with an additional fault

$$\begin{bmatrix} \boldsymbol{\rho}^s_k \\ \lambda\boldsymbol{\phi}^s_k \end{bmatrix} = \begin{bmatrix} \boldsymbol{\rho}_k \\ \lambda\boldsymbol{\phi}_k \end{bmatrix} + \begin{bmatrix} \boldsymbol{I} \\ \boldsymbol{I} \end{bmatrix} \underbrace{(\boldsymbol{f}_k + \boldsymbol{G}_k\,\delta\tilde{\boldsymbol{r}}^s_k)}_{\boldsymbol{f}'_k} \tag{6.1}$$

where $\boldsymbol{\rho}^s_k$ and $\boldsymbol{\phi}^s_k$ are the spoofed code and carrier signals, $\boldsymbol{\rho}_k$ and $\boldsymbol{\phi}_k$ are the original code and carrier signals, and $\boldsymbol{f}'_k$ is the resultant fault vector containing the spoofer's position tracking estimation error $\delta\tilde{\boldsymbol{r}}^s_k = \delta\hat{\boldsymbol{r}}^s_k - \delta\boldsymbol{r}_k$ and the computed fault $\boldsymbol{f}_k$. Equation (6.1) assumes that the spoofer preserves the consistency in the code and carrier signals by using the same fault for both the code and carrier signals. Otherwise, the spoofing attack will be detectable by the Code Carrier Divergence (CCD) airborne monitors in [50]. Also, as in Chapter 5, the spoofer's position estimation error $\delta\tilde{\boldsymbol{r}}^s$ in (6.1) is modeled as a white Gaussian noise additive to $\boldsymbol{f}_k$.

It can be shown that the resultant fault $\boldsymbol{f}'_k$ term in (6.1) will not be smoothed

out by the airborne Hatch filter (Fig. 2.3) since it is the same for the spoofed code and carrier signals. Therefore, the spoofed carrier-smoothed code $\overline{\boldsymbol{\rho}}_k^s$ (output of the filter) can be expressed as

$$\overline{\boldsymbol{\rho}}_k^s = \overline{\boldsymbol{\rho}}_k + \boldsymbol{f}_k^{'} \tag{6.2}$$

where $\overline{\boldsymbol{\rho}}_k$ is the original GBAS carrier-smoothed code for the spoof-free case, which was previously defined in (3.12). Substituting (3.12) into (6.2) gives the spoofed carrier-smoothed code measurement

$$\overline{\boldsymbol{\rho}}_k^s = \underbrace{\begin{bmatrix}\boldsymbol{G}_k & \mathbf{1}\end{bmatrix}}_{\boldsymbol{G}_{\overline{\rho}_k}} \begin{bmatrix}\delta \boldsymbol{r}_k \\ \delta \tau_k\end{bmatrix} + \boldsymbol{\epsilon}_k + \boldsymbol{f}_k^{'}. \tag{6.3}$$

Replacing the spoof-free measurement $\overline{\boldsymbol{\rho}}_k$ in (3.12) with the spoofed measurement $\overline{\boldsymbol{\rho}}_k^s$ in (6.3) and re-deriving the equations from (3.13) to (3.20) yield a spoofed GBAS weighted least squares position solution $\delta\hat{\boldsymbol{r}}_k^{\mathrm{LS}}$ in terms of the fault vector $\boldsymbol{f}_k^{'}$ as

$$\delta\hat{\boldsymbol{r}}_k^{\mathrm{LS}} = \boldsymbol{H}_k \mathbf{x}_k + \underbrace{\boldsymbol{T}_r \boldsymbol{G}_{\overline{\rho}_k}^{+} \boldsymbol{f}_k^{'}}_{\boldsymbol{f}_k^{''}} \tag{6.4}$$

which is also the measurement input to the loosely-coupled Kalman filter estimator.

6.1.2 Spoofed Kalman Filter Solution. Substituting (6.4) into (3.23) gives the Kalman filter measurement update as a function of the fault as

$$\hat{\mathbf{x}}_k^{\mathrm{KF}} = \underbrace{\big(\boldsymbol{I} - \boldsymbol{L}_k \boldsymbol{H}_k\big)}_{\boldsymbol{L}_k^{'}} \overline{\mathbf{x}}_k^{\mathrm{KF}} + \boldsymbol{L}_k \boldsymbol{H}_k \mathbf{x}_k + \boldsymbol{L}_k \boldsymbol{f}_k^{''}. \tag{6.5}$$

Also, substituting the Kalman filter time update equation (3.22) into (6.5) yields

$$\hat{\mathbf{x}}_k^{\mathrm{KF}} = \boldsymbol{L}_k^{'} \boldsymbol{\Phi}_{\mathrm{x}} \hat{\mathbf{x}}_{k-1}^{\mathrm{KF}} + \boldsymbol{L}_k \boldsymbol{H}_k \mathbf{x}_k^{\mathrm{KF}} + \boldsymbol{L}_k^{'} \boldsymbol{\Gamma}_{\mathrm{x}} \tilde{\boldsymbol{u}}_{k-1} + \boldsymbol{L}_k \boldsymbol{f}_k^{''}. \tag{6.6}$$

Let us define the state estimate error as $\tilde{\mathbf{x}}_k^{\mathrm{KF}} = \hat{\mathbf{x}}_k^{\mathrm{KF}} - \mathbf{x}_k$. Subtracting the INS process model (3.21) from (6.6) gives the state estimate error dynamics as

$$\tilde{\mathbf{x}}_k^{\mathrm{KF}} = \boldsymbol{L}_k^{'} \boldsymbol{\Phi}_{\mathrm{x}} \tilde{\mathbf{x}}_{k-1}^{\mathrm{KF}} - \boldsymbol{L}_k^{'} \boldsymbol{w}_{\mathrm{x}_{k-1}} + \boldsymbol{L}_k \boldsymbol{f}_k^{''}. \tag{6.7}$$

Similarly, the innovation vector under a spoofing attack is obtained by substituting (6.4) into (3.27) as

$$\boldsymbol{\gamma}_k = \boldsymbol{f}_k^{''} - \boldsymbol{H}_k\big(\boldsymbol{\Phi}_{\mathrm{x}} \tilde{\mathbf{x}}_{k-1} - \boldsymbol{w}_{\mathrm{x}_{k-1}}\big). \tag{6.8}$$

6.1.3 Loosely–Coupled Performance Evaluation Model. Augmenting the state estimate error model in (6.7) with the innovation model in (6.8) results in a performance evaluation model capturing the impact on the state estimate error and the innovation due to the spoofer's deliberate fault and unknown tracking errors (both included in $\boldsymbol{f}_k^{''}$):

$$\begin{bmatrix} \tilde{\mathbf{x}}_k^{\mathrm{KF}} \\ \boldsymbol{\gamma}_k \end{bmatrix} = \underbrace{\begin{bmatrix} \boldsymbol{L}_k^{'}\boldsymbol{\Phi}_{\mathrm{x}} & 0 \\ -\boldsymbol{H}_k\boldsymbol{\Phi}_{\mathrm{x}} & 0 \end{bmatrix}}_{\boldsymbol{\Phi}_{y_k}} \underbrace{\begin{bmatrix} \tilde{\mathbf{x}}_{k-1}^{\mathrm{KF}} \\ \boldsymbol{\gamma}_{k-1} \end{bmatrix}}_{\boldsymbol{y}_{k-1}} + \underbrace{\begin{bmatrix} -\boldsymbol{L}_k^{'} \\ \boldsymbol{H}_k \end{bmatrix}}_{\boldsymbol{\Upsilon}_{y_k}} \boldsymbol{w}_{\mathrm{x}_{k-1}} + \underbrace{\begin{bmatrix} \boldsymbol{L}_k \\ \boldsymbol{I} \end{bmatrix}}_{\boldsymbol{\Psi}_{y_k}} \boldsymbol{f}_k^{''} \tag{6.9}$$

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

6.2 Worst–Case Fault Maximizing Integrity Risk in GBAS

It should be mentioned that the loosely-coupled evaluation model (6.9) is structurally a subset of the the tightly-coupled evaluation model (5.19) derived in Chapter 5. Therefore, the methods for computing the integrity risk and worst-case fault introduced in Sections 5.2 and 5.3, respectively, are also applicable for the loosely-coupled evaluation model in (6.9).

Using (5.38) and (5.39), the worst case fault history vector $\boldsymbol{f}_{w_{1:k}}^{''}$ is written as

$$\boldsymbol{f}_{w_{1:k}}^{''} = \alpha_w \overline{\boldsymbol{B}}_{1:k}^{-1} \boldsymbol{S}_{1:k} \overline{\boldsymbol{B}}_{1:k}^{-T} \boldsymbol{A}_k^T \boldsymbol{t}_\varepsilon^T \tag{6.10}$$

where $\boldsymbol{t}_\varepsilon$ extracts the hazardous state ε (i.e. altitude in the landing approach problem) from the state vector $\mathbf{x}$; and $\boldsymbol{A}_k$ and $\overline{\boldsymbol{B}}_{1:k}$ are the constant matrices defined as functions of the deterministic coefficients $\boldsymbol{H}_i$, $\boldsymbol{\Phi}_{\mathrm{x}}$, $\boldsymbol{L}_i$, and $\boldsymbol{L}_i^{'}$ of the loosely-coupled evaluation model in (6.9) as

$$\begin{aligned} \boldsymbol{A}_k &= \begin{bmatrix} \boldsymbol{A}_{1k} & \dots & \boldsymbol{A}_{kk} \end{bmatrix} \\ \boldsymbol{A}_{ik} &= \begin{cases} \boldsymbol{L}_k^{'}\boldsymbol{\Phi}_{\mathrm{x}}\boldsymbol{L}_{k-1}^{'}\boldsymbol{\Phi}_{\mathrm{x}} \dots \boldsymbol{L}_{1+i}^{'}\boldsymbol{\Phi}_{\mathrm{x}}\boldsymbol{L}_i & \text{if } i < k \\ \boldsymbol{L}_i & \text{if } i = k \end{cases} \end{aligned} \tag{6.11}$$

and

$$\begin{aligned}\overline{\boldsymbol{B}}_{1:k} &= \left[\overline{\boldsymbol{B}}_1^T \ldots \overline{\boldsymbol{B}}_k^T\right]^T \\ \overline{\boldsymbol{B}}_i &= \left[-\boldsymbol{H}_k \boldsymbol{\Phi}_{\mathrm{x}} \boldsymbol{A}_{k-1} \quad \boldsymbol{I}_{n\times n} \quad \boldsymbol{0}_{n\times n(k-i)}\right]\end{aligned} \tag{6.12}$$

where k is the number of GNSS time epochs and n is the number of GBAS measurements feeding the Kalman filter at each time epoch ($n = 3$ in the loosely-coupled integration). Using (5.41), the scalar worst-case fault magnitude α_w in (6.10) is determined through one dimensional search to maximize the integrity risk I_{r_k} as

$$\arg\max_{\alpha} \quad I_{r_k}(\alpha) = \frac{1}{m}\sum_{i=1}^{m} \Pr\left(|\varepsilon_k| > l; \alpha \mid \delta\tilde{\boldsymbol{r}}_i^s\right) \Pr\left(q_k < T; \alpha \mid \delta\tilde{\boldsymbol{r}}_i^s\right) \tag{6.13}$$

where $\delta\tilde{\boldsymbol{r}}_i^s$'s are samples obtained from the normally distributed white error $\delta\tilde{\boldsymbol{r}}^s \sim \mathcal{N}(0, \boldsymbol{P}_{\delta r}^s)$.

6.3 Loosely–Coupled INS Monitor Performance Analysis Results

To test the performance of the loosely-coupled INS monitor, a covariance analysis with a B747 flight on a GBAS-assisted approach is simulated at standard trimmed flight conditions at 131 knots [14]. The navigation-grade IMU sensor specifications and the parameters for the GBAS error model defined in Appendix C are provided in Table F.1 and Table F.3, respectively. We assume that the airborne estimator has been running under fault free conditions and has reached steady state before the spoofing attack starts.

To quantify the impact of the spoofing attack period on the integrity risk, we obtained the worst-case fault profiles for different attack periods ranging from 152 to 232 s and computed the corresponding integrity risks assuming the spoofer has perfect position tracking sensors (i.e., $\delta\tilde{\boldsymbol{r}}_k^s = 0$). As seen in Fig. 6.2, increasing the attack period allows the spoofer to achieve higher integrity risks. On the other hand, even though we conservatively assumed that the spoofer tracks the aircraft position with zero-error, the worst-case spoofing fault for a standard B747 approach of 150 s

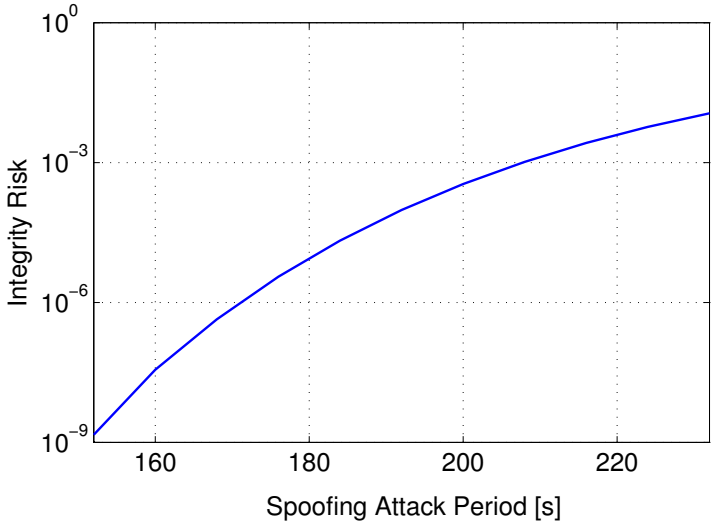

Figure 6.2. The impact of spoofing attack period on the integrity risk. The results are obtained for B747 GBAS-assisted approaches in the presence of worst-case spoofing attacks when the spoofer is capable of tracking the aircraft position with perfect accuracy.

results in an integrity risk of approximately 10^{-9}, which satisfies the most stringent safety requirement in aviation [37].

In a more realistic scenario, we assume that the spoofer's position estimate error is a zero-mean white noise $\delta\tilde{\boldsymbol{r}}_k^s$ sequence. Fig. 6.3 shows that for a position tracking error of more than 7 cm (1-σ), the integrity risk always remains below 10^{-9} for spoofing attacks having a period of up to approximately 230 s. This 230 s attack period is probably high since the standard B747 approach is 150 s and the spoofer will have a limited range. The results are promising because such tracking accuracy is extremely difficult even for the highest technology remote tracking systems. For example, Figure 6.4 illustrates the ranging accuracy of an Sense and Avoid (SAA) radar system [8]. We plot the range accuracy of SAA within 10 km line of sight since it corresponds to a standard B747 approach of 150 s. As seen in the figure, 1-σ range accuracy of the radar (blue line) drops to 170 cm within the approach volume. On the other hand, for the spoofer to achieve an integrity risk of equal or

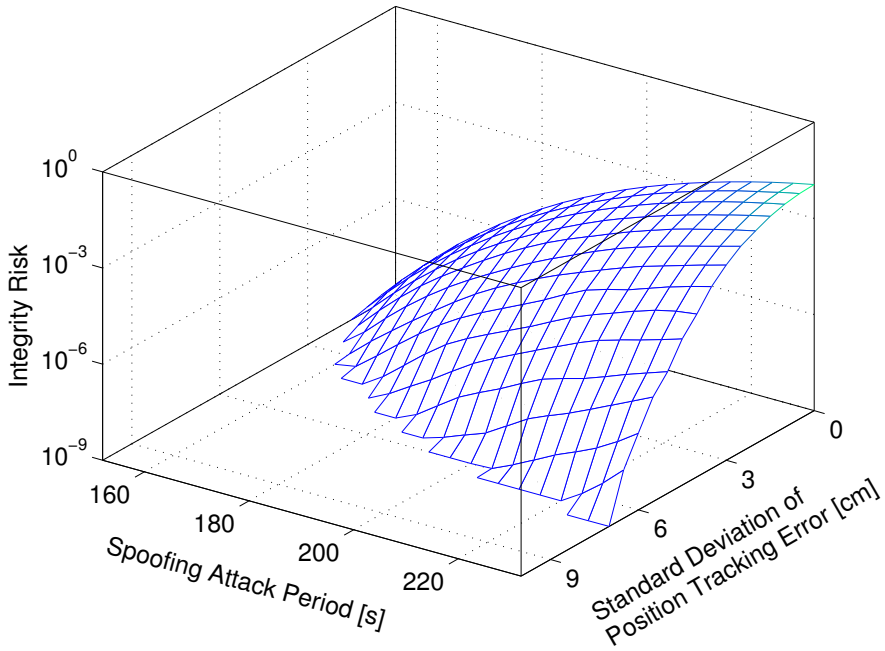

Figure 6.3. The influence of spoofer's tracking errors on detection performance of the monitor using loosely-coupled INS/GNSS integration in terms of the integrity risk.

higher than 10^{-9}, he/she has to maintain a minimum of 7 cm (1-σ) accuracy during whole attack period of 232 s, which is far beyond the capability of existing SAA remote tracking systems. Also, maintaining this high tracking accuracy during whole aircraft approach is unrealistic due to uncertainties in the lever arm from the GNSS antenna location to the spoofer's measurement point on the aircraft.

6.4 Loosely vs. Tightly Coupled INS Monitor Performances

The covariance analysis in this chapter demonstrates the performance of the INS monitor using loosely-coupled systems (i.e., GBAS). The monitor performance for tightly-coupled systems (i.e., shipboard landing and autonomous airborne refueling) was shown in Chapter 5. Fig. 6.5 compares detection capability of the monitor implemented with the loosely and tightly-coupled systems. The left plot shows the integrity risk values as a function of the spoofing attack period in presence of worst-

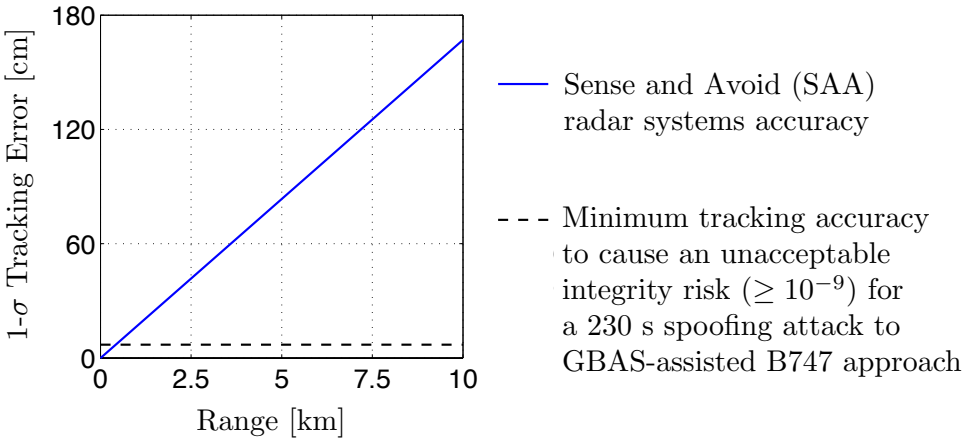

Figure 6.4. Sense and Avoid (SAA) radar system ranging accuracy within a standard B747 landing approach range of 10 km [8].

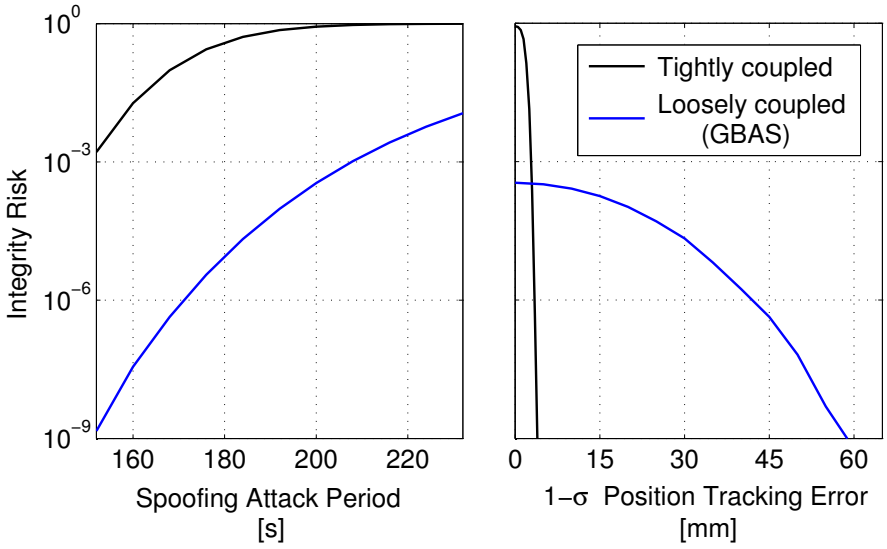

Figure 6.5. Comparison of performance of the INS monitors for the tightly and loosely-coupled systems. The integrity risk are given as a function of spoofing attack period in the presence of worst-case spoofing attacks with perfect tracking (left). The monitor sensitivity to the spoofer's tracking error for an example approach of 200 s is also given in terms of the integrity risk (right). The integrity risk values for the tightly-coupled systems (black curves) are extracted from Figure 5.6.

case spoofing attacks with perfect position tracking. The plot shows that the loosely coupled INS/GNSS integration results in lower integrity risk than the tightly-coupled integration does. The reason is that the tightly-coupled integration scheme gives the spoofer better opportunity to fuse the GNSS spoofing fault into the system (by di-

rectly inputting the spoofed GNSS measurements into the Kalman filter) and thereby corrupt the IMU biases. However, in the more realistic scenario where the spoofer has position tracking errors, the right plot illustrates that the monitor with the tightly-coupled system is more sensitive to the spoofer's tracking errors than that with the loosely-coupled system. For example, for the same spoofing attack period (200 s), the tracking error (1-σ) resulting in a 10^{-9} integrity risk is 4 mm in the tightly-coupled systems, whereas it is 60 mm in the loosely-coupled systems. Regardless, both systems meet 10^{-9} integrity risk requirements for the aviation applications given the realistic tracking accuracy.

CHAPTER 7

UNCOUPLED INS MONITOR PERFORMANCE IN AIRCRAFT EN ROUTE FLIGHT

This chapter evaluates the performance of the uncoupled INS monitor in en route flight applications that use the standalone GNSS for positioning. We investigate whether a free-INS solution can be used as a sanity check to a spoofed GNSS-only least squares position estimate. To do this, we analytically derive and utilize the worst-case spoofing fault for the uncoupled INS/GNSS integration. In the performance analysis, the IMU is assumed to be well-calibrated prior to a spoofing attack. Utilizing different-grade (i.e. navigation and tactical) IMUs, we quantify the maximum allowable time interval between the INS calibration to detect worst-case GNSS spoofing faults with low integrity risk (i.e. $I_{r_k} < 10^{-9}$).

7.1 Uncoupled Monitor Influenced with GNSS Spoofing Fault

In this section, we derive evaluation models capturing the impact of the fault on the GNSS least squares estimator and uncoupled INS detector as shown in Figure 7.1. Using the standalone GNSS measurement model (3.45), the spoofed code measurement $\boldsymbol{\rho}_k^s$ is expressed as

$$\boldsymbol{\rho}_k^s = \underbrace{\begin{bmatrix}\boldsymbol{G}_k & \mathbf{1}\end{bmatrix}}_{\boldsymbol{H}_k} \begin{bmatrix}\delta\boldsymbol{r}_k \\ \delta\tau_{u_k}\end{bmatrix} + \boldsymbol{\nu}'_{\rho_k} + \boldsymbol{f}_k \tag{7.1}$$

where $\boldsymbol{f}_k$ is the fault vector computed by the spoofer. Replacing the spoofed code $\boldsymbol{\rho}_k^s$ in (7.1) with the spoof-free code $\boldsymbol{\rho}_k$ in (3.46) and using the definition of $\delta\tilde{\boldsymbol{r}}_k^{\mathrm{LS}} = \delta\hat{\boldsymbol{r}}_k^{\mathrm{LS}} - \delta\boldsymbol{r}_k$, we obtain the least squares position estimation error as a function of the fault

$$\delta\tilde{\boldsymbol{r}}_k^{\mathrm{LS}} = \boldsymbol{T}_r \boldsymbol{H}_k^{+}\big(\boldsymbol{\nu}'_{\rho_k} + \boldsymbol{f}_k\big). \tag{7.2}$$

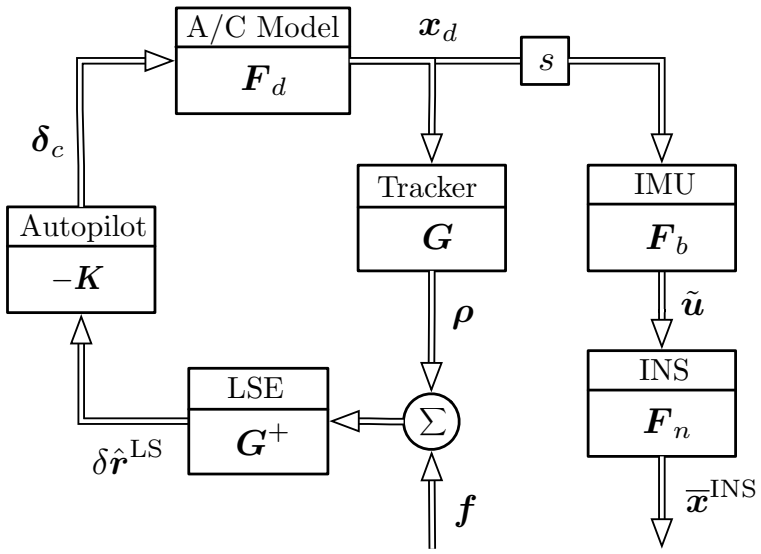

Figure 7.1. Uncoupled INS monitor performance evaluation model capturing the impact of the fault $\boldsymbol{f}$ on the GNSS-only least squares estimation (LSE) and the detection with uncoupled INS.

Similarly, subtracting (3.49) from (3.50) and using the definition of $\tilde{\boldsymbol{x}}_k^{\mathrm{INS}} = \overline{\boldsymbol{x}}_k^{\mathrm{INS}} - \boldsymbol{x}_k$, the state estimate error propagation in INS-only approach is performed as

$$\tilde{\boldsymbol{x}}_k^{\mathrm{INS}} = \boldsymbol{\Phi}\,\tilde{\boldsymbol{x}}_{k-1}^{\mathrm{INS}} - \overline{\boldsymbol{w}}_{k-1}. \tag{7.3}$$

Substituting (7.3) and (7.2) into (3.52), the test statistic is re-expressed as

$$q_k = \boldsymbol{t}_{\varepsilon r}\boldsymbol{T}_r\boldsymbol{H}_k^{+}(\boldsymbol{\nu}'_{\rho_k} + \boldsymbol{f}_k) - \boldsymbol{t}_{\varepsilon x}\big(\boldsymbol{\Phi}\,\tilde{\boldsymbol{x}}_{k-1}^{\mathrm{INS}} - \overline{\boldsymbol{w}}_{k-1}\big). \tag{7.4}$$

7.2 En Route Spoofing Integrity Risk

Recall that the integrity risk is defined in (3.55) as the joint probability $I_{r_k} = \Pr\left(|\varepsilon_k| > l, q_k < T\right)$ where the hazardous state ε in en route applications is typically the horizontal position estimation error, which can be extracted from the GNSS least squares position estimation error $\delta\tilde{\boldsymbol{r}}^{\mathrm{LS}}$ as

$$\varepsilon_k = \boldsymbol{t}_{\varepsilon r}\,\delta\tilde{\boldsymbol{r}}_k^{\mathrm{LS}}. \tag{7.5}$$

Using (7.2), (7.4), and (7.5), it can be shown that the test statistic q_k and hazardous state estimation error ε_k are correlated. To solve the joint probability in (3.55), we

define a vector containing q_k and ε_k and obtain a bi-variate Gaussian distribution as

$$[q_k, \varepsilon_k]^T \sim \mathcal{N}\big(\boldsymbol{\mu}_k, \boldsymbol{\Sigma}_k\big). \tag{7.6}$$

Propagating the equations from (7.2) to (7.5) with $\tilde{\boldsymbol{x}}_0^{\text{INS}} \sim \mathcal{N}(0, \overline{\boldsymbol{P}}_{x_0})$, the mean vector $\boldsymbol{\mu}_k = [\mu_{q_k}, \mu_{\varepsilon_k}]^T$ is obtained as a function of the fault $\boldsymbol{f}_k$

$$\mu_{q_k} = \mu_{\varepsilon_k} = \boldsymbol{t}_{\varepsilon r} \boldsymbol{T}_r \boldsymbol{H}_k^{+} \boldsymbol{f}_k, \tag{7.7}$$

and the covariance matrix $\boldsymbol{\Sigma}_k$ is obtained as

$$\boldsymbol{\Sigma}_k = \begin{bmatrix} \sigma^2_{qq_k} & \sigma^2_{q\varepsilon_k} \\ \sigma^2_{q\varepsilon_k} & \sigma^2_{\varepsilon\varepsilon_k} \end{bmatrix} \tag{7.8}$$

where

$$\sigma^2_{qq_k} = \boldsymbol{t}_{\varepsilon r} \boldsymbol{T}_r \big(\boldsymbol{H}_k^T \boldsymbol{V}'^{-1}_{\rho_k} \boldsymbol{H}_k\big)^{-1} \boldsymbol{T}_r^T \boldsymbol{t}_{\varepsilon r}^T + \boldsymbol{t}_{\varepsilon x} \Big[\boldsymbol{\Phi}^k \overline{\boldsymbol{P}}_{x_0} \boldsymbol{\Phi}^{k^T} + \sum_{i=1}^{k} \boldsymbol{\Phi}^{i-1} \overline{\boldsymbol{W}}_i \boldsymbol{\Phi}^{i-1^T}\Big] \boldsymbol{t}_{\varepsilon x}^T \tag{7.9}$$

$$\sigma^2_{\varepsilon\varepsilon_k} = \sigma^2_{q\varepsilon_k} = \boldsymbol{t}_{\varepsilon r} \boldsymbol{T}_r \big(\boldsymbol{H}_k^T \boldsymbol{V}'^{-1}_{\rho_k} \boldsymbol{H}_k\big)^{-1} \boldsymbol{T}_r^T \boldsymbol{t}_{\varepsilon r}^T. \tag{7.10}$$

The integrity risk in (3.55) can be solved numerically using the bivariate Gaussian distribution derived in (7.6).

7.3 Worst–Case Fault Derivation for Uncoupled Integration

The Kalman filter-based worst case fault derivations for the tightly and loosely-coupled monitors are introduced in Sections 5.3 and 6.2. In this section, we derive the worst-case fault profile for the uncoupled monitor. The worst-case fault maximizes the GNSS-based least squares estimate error associated with the most hazardous state ε_k while minimizing the test statistic q_k and this maximizes the integrity risk. Recall that the ratio $\rho_k = \mu_{\varepsilon_k}/\mu_{q_k}$ is called the failure mode slope, and (7.7) indicates that it is always one for the uncoupled monitor:

$$\rho_k = 1. \tag{7.11}$$

From (7.11), one can conclude that the center of the bi-variate distribution defined in (7.6) will always lie on a failure mode slope line passing from origin with a 45^o

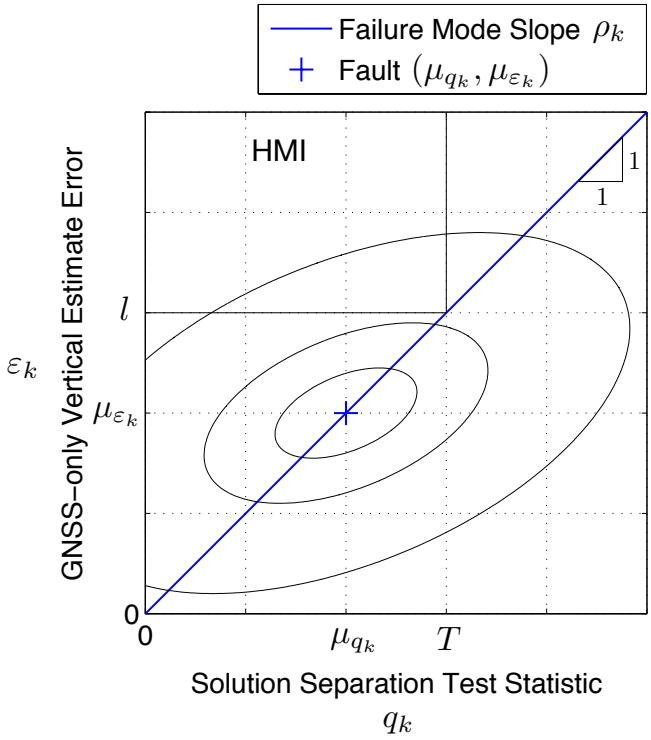

Figure 7.2. An example fault on the solution separation failure mode slope of 1. The marker (+) on the failure mode slope corresponds to the worst-case fault for this scenario. The black curves are the covariance ellipses of the bivariate Gaussian distribution obtained from (7.6).

slope regardless of the fault vector (Fig. 7.2). To obtain the worst-case fault, we first determine the worst-case mean $\boldsymbol{\mu}_k$ of the bi-variate distribution on the failure mode slope, which maximizes the integrity risk I_{r_k} in (3.55) as

$$\arg\max_{\mu_{q_k}} I_{r_k} \tag{7.12}$$

Utilizing Equations (7.6) to (7.10), the unique solution to the worst-case test statistic mean $\mu^*_{q_k}$ is determined through one dimensional search to maximize I_{r_k} in (7.12). Let n be the number of measurements at each time epoch, for a given $\mu^*_{q_k}$, (7.7) yields an $(n-1)$-parameter family of solutions for the worst-case fault vector $\boldsymbol{f}^*_k$, which is used to generate worst-case spoofed GNSS signals broadcast by the spoofer.

In the uncoupled case so far, we assume that the spoofer has perfect knowledge of the aircraft position. Unlike in the tightly and loosely-coupled monitors where the

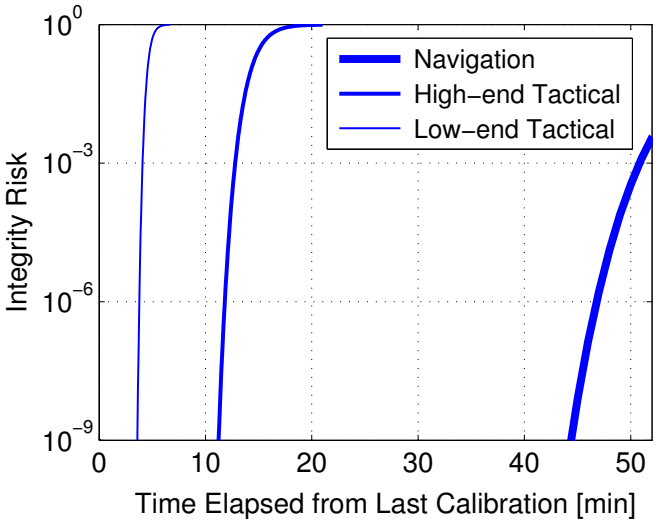

Figure 7.3. The integrity performance of the uncoupled monitor using navigation grade, and high-end and low-end tactical grade IMU sensors.

spoofer's tracking errors accumulate over time, in uncoupled monitor the leveraging effect of this accumulation of tracking error does not exist. The reason is that the monitor in the uncoupled integration (3.52) checks the instantaneous discrepancy between INS and GNSS solutions; and the impact of the tracking errors at that one instant will be small. Therefore, we will only investigate the perfect tracking scenarios.

7.4 Performance Analysis Results

To test the performance of the uncoupled INS monitor, a covariance analysis with a B747 en route flight is simulated by using a standalone GNSS receiver ($\sigma_{\rho_{c,u}} = 3$ m) with free running navigation-grade and tactical-grade IMUs (Table F.1). We assume that the IMU is calibrated until it reaches steady-state before the spoofing attack starts. In the integrity risk computations, we use a horizontal alert limit l of 1.85 km which is a standard requirement for terminal en route in continental operations [37].

As seen in Figure 7.3, if the time elapsed from the last IMU calibration is

sufficiently long, the worst-case spoofing attacks result in high integrity risks, which is expected. On the other hand, with a standalone navigation grade IMU (which is typically used in airliners), the monitor provides a spoofing protection with an integrity risk lower than 10^{-7} (the terminal and en route integrity risk requirement) up to 46 min, which would be an unrealistically long spoofing attack. To also investigate the impact of the IMU quality on the spoofing detection performance of the monitor, we obtain the integrity risk results with high-end and low-end tactical grade IMUs, which are typically used in military aircraft, missiles, and drones. The tactical grade IMUs guarantee the spoofing integrity up to ranging from 4 (low-end) to 12 (high-end) min.

CHAPTER 8

CONCLUSION

GNSS spoofing attacks are an emerging threat; they are not only theoretical but have actually been witnessed in the last decade [60]. The U.S. government had tasked the Department of Transport and Homeland Security in 2014 to develop backup capability in response to these man-made threats to GPS systems. This dissertation has directly addressed the need to detect GNSS spoofing attacks by designing autonomous INS monitors for high safety and precision applications such as manned or unmanned aircraft landings and en route operations. An integrity risk methodology has also been developed to evaluate the monitor's performance under worst-case spoofing attacks. These methods can lead to fully tested and certifiable INS monitors that can be implemented in aviation, and other terrestrial and maritime navigation applications.

8.1 Summary of Accomplishments

The focus of this dissertation has been to investigate inertial sensor fusion and fault monitoring techniques to guarantee spoofing resistance of GNSS-based high-integrity navigation systems. These include aircraft landings to shipboard platforms and airports equipped with GBAS facilities, and terminal en route flights. Areas of contributions are discussed in the following subsections.

8.1.1 Developing INS Monitors. In this dissertation, INS-aided fault detection (monitoring) algorithms against GNSS spoofers were designed, implemented, and validated. The monitors developed here are simple, but efficient and compatible with navigation systems where GNSS receivers and INS sensors are integrated in tightly-

coupled, loosely-coupled, and uncoupled schemes.

8.1.2 Performance Evaluation Methodology. This dissertation developed an integrity risk evaluation methodology to quantify the statistical reliability of the new monitors. The methodology enables quantification of integrity risk without needing to simulate an unmanageably large number of individual flights. A novel closed-form solution to the worst-case time sequence of GNSS fault is derived to maximize the integrity risk for each INS/GNSS integration and it is used in the covariance analyses. This methodology allows of the monitor performance against the most sophisticated spoofers, capable of tracking and estimating the aircraft position – for example, by means of remote tracking or onboard sensing.

8.1.3 Aircraft Dynamics Effect in Detection. Using a batch residual-based monitor, we developed an evaluation model capturing the effect of aircraft dynamics on detection performance. In a realistic flight, an aircraft has transient response to disturbances such as wind gusts or the autopilot's maneuver commands in response to the spoofing faults. These high-frequency responses on the aircraft nominal trajectory are difficult to capture in the spoofer's tracking loop accurately and quickly, and we showed in the analysis is a direct means to detect a spoofing attack. The results illustrated that even under light turbulence conditions (less than 2.5 m/s wind gust intensity) during a B747 approach, integrity risk is on the order of 10^{-7}.

8.1.4 Verifying Monitors in Safety Critical GNSS Applications. GNSS spoofing attacks are a critical threat to high safety GNSS augmentation systems such as relative navigation and GBAS/SBAS. In response, we first designed Kalman filter innovations-based monitors for both tightly-coupled and loosely-coupled INS/GNSS integrations, then validated their performance in two example safety-critical applications: 1) autonomous shipboard landing (relative navigation) and 2) GBAS-assisted B747 landing. We showed that for both systems, the monitors easily detected the

worst-case spoofing attacks with less than 10^{-9} integrity risk, unless the spoofer maintains a position tracking with an accuracy of few millimeters (for shipboard landing) and few centimeters (for GBAS), and no-delays. Such near-perfect accuracies are unrealistic regardless of remote tracking or onboard sensing with the existing technology. We also compared performance and explained the differences therein between the tightly and loosely-coupled systems.

8.1.5 Sensor Requirements in General Enroute GNSS Applications. In some general en route aviation and maritime applications, standalone GNSS positioning is used for guidance. In such applications, INS, in standalone mode, can be used as an external aid against GNSS spoofers. However, in this uncoupled integration scheme, the sensor quality plays a significant role in the detection performance as it drifts over time. In response, this dissertation proposed an uncoupled monitor and quantified its performance with different quality INS sensors ranging from navigation-grade to low tactical-grade IMUs. The results showed that the INS monitor guarantees a spoofing-resistance up to 46 min with navigation-grade IMUs. This sensitivity analysis established a baseline for relating the specific application's integrity requirement to INS sensor requirements.

8.2 Recommended Topics for Future Research

A number of recommendations for future work are given in the following subsections to enhance the INS monitor's performance.

8.2.1 Optimal Detector Design. The proposed detectors in this dissertation are simple, efficient, and can directly be implemented on top of any type of INS/GNSS integrations without requiring any modification to the existing navigation system. However, when building a new integrated navigation system, it is possible to construct the design such that both estimation accuracy and fault detection performance

are maximized. Such flexibility would lead to a computationally more complex but optimal detector. In this dissertation, it was shown that an improved detection performance can be achieved by decreasing the GNSS measurement sampling rate (see Figure 5.4) or varying the INS/GNSS integration scheme. However, for more comprehensive design the optimal detection theory, previously introduced in [21] to minimize integrity risk due to satellite faults, can be considered in optimizing the INS monitors for spoofing faults.

8.2.2 When to Start Monitoring. This dissertation focused on aircraft approach to landing, which is a limited duration of 150 s. Therefore, in the performance analyses in Chapters 4, 5, and 6, it was assumed that the monitoring starts with the landing approach when the spoofing attack simultaneously starts. However, in an en route operation, which allows spoofers (especially onboard spoofers) have a larger time window for spoofing, the detection performance might be influenced adversely if the monitor has been running prior to the spoofing attack (or the spoofing has started prior to the monitor). Therefore, a sensitivity analysis needs to be performed to quantify this effect and to determine the maximum allowable monitoring time window prior to a spoofing attack to guarantee the integrity.

8.2.3 Inertial Sensor Faults. Most commercial drones (e.g., quadrotors) are often equipped with low-cost and lightweight industrial-grade IMUs which together with GNSS receiver, serve an essential role. However, due to their intrinsic components and fabrication process, IMUs are vulnerable to disturbances in the vehicle environment and prone to faults. For example, inertial measurements are susceptible to bias and excessive noise due to temperature variation and vibration [4]. The detection of IMU faults plays a crucial role in safety-critical operations. To enhance the integrity of the INS/GNSS integrated systems, detection of failures in INS and isolation of the faulty

sensor are also needed to be addressed.

8.2.4 INS–Aided RAIM Detection and Exclusion Algorithms. RAIM algorithms have traditionally been designed for the cases when only one satellite failure occurs at a time. However, due to tighter alert limits especially in urban environments, extending the RAIM concept to include multiple failures is currently the main focus. Detection of simultaneous errors is challenging particularly using only satellite redundancy, therefore INS redundancy, as an external aid, can be used to improve the RAIM performance. The detection and evaluation methods presented in this dissertation already cover the worst case of satellite faults (i.e., all satellites are affected). To complete the work, the strategies to exclude the spoofing faults and to continue the operation will need to be addressed.

8.2.5 Hardware Testing. The Illinois Institute of Technology's Navigation Laboratory has ordered a tactical-grade IMU (Sensonor's STIM300) which is to be mounted on a static or dynamic platform (e.g., drone) to test the monitors proposed in this research. The aim of the experiment is to demonstrate that the monitors can be applied real-time and determine whether the nonlinearities in the actual system deteriorate the detection performance. Transmitting live spoofing signals, except with special permission at specified times and locations, is prohibited by Department of Homeland Security. Therefore, instead of actual spoofing and broadcasting, the original GNSS signals sensed by the vehicle's receiver can be manipulated in a worst way by executing a "bug-like" code in the vehicle's flight control computer, which represents a synthetic spoofing. This would enable one to do the hardware test a lot faster and easier.

8.3 Closing

INS monitors are the absolute remedy to achieve GNSS spoofing-resistant

positioning systems, which guarantee the navigation integrity of the most critical aviation applications.

APPENDIX A

AIRCRAFT 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 [65]

$$I_{22}\dot{q} - (I_{33} - I_{11})pr + I_{13}(p^2 - r^2) = M + M_T \tag{A.1}$$

$$m\,(\dot{u} + qw - rv) = -mgsin\theta + X + X_T \tag{A.2}$$

$$m(\dot{w} + pv - qu) = mgcos\theta cos\phi + Z + Z_T \tag{A.3}$$

where u, v, w are the velocity components in body-fixed stability axes in Fig. 2.1, p, q, r are roll, pitch, and yaw rates, α, β, θ 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 (A.1), (A.2) and (A.3) 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 θ 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 [65]

$$\delta F_1^i = m\,\delta\dot{u} \tag{A.4}$$

$$\delta F_3^i = m(\delta\dot{w} - u^*\delta q) \tag{A.5}$$

$$\delta M_2^i = I_{22}\,\delta\dot{q} \tag{A.6}$$

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

simplified as [65]

$$\delta X = m\left(X_u \delta u + X_\alpha \delta\alpha + X_q \delta q + X_{\delta_e}\delta_e\right) \tag{A.7}$$

$$\delta Z = m\left(Z_u \delta u + Z_\alpha \delta\alpha + Z_q \delta q + Z_{\delta_e}\delta_e\right) \tag{A.8}$$

$$\delta M = I_{22}\left(M_u \delta u + M_\alpha \delta\alpha + M_q \delta q + M_{\delta_e}\delta_e\right) \tag{A.9}$$

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

$$\delta\alpha = \frac{\delta w}{u^*} \tag{A.10}$$

Assuming a constant thrust ($\delta X_T = \delta Z_T = \delta M_T = 0$) and equating inertial forces and moment in (A.4) to (A.6) to the external forces and moment in (A.7) to (A.9) respectively, yields

$$\delta\dot{u} = X_u \delta u + \frac{X_\alpha}{u^*}\delta w - gc\theta^*\delta\theta + X_{\delta_e}\delta_e \tag{A.11}$$

$$\delta\dot{w} = Z_u \delta u + \frac{Z_\alpha}{u^*}\delta w + (Z_q + u^*)\delta q - gs\theta^*\delta\theta + Z_{\delta_e}\delta_e \tag{A.12}$$

$$\delta\dot{q} = M_u \delta u + \frac{M_\alpha}{u^*}\delta w + M_q \delta q + M_{\delta_e}\delta_e \tag{A.13}$$

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

$$\delta\dot{h} = s\theta^*\delta u - c\theta^*\delta w + u^*\delta\theta \tag{A.14}$$

This yields a state space representation of EOM describing longitudinal aircraft dynamics including altitude as

$$\begin{bmatrix} \delta\dot{u} \\ \delta\dot{w} \\ \delta\dot{q} \\ \delta\dot{\theta} \\ \delta\dot{h} \end{bmatrix} = \underbrace{\begin{bmatrix} X_u & {}^{X_\alpha}/_{u^*} & 0 & -gc\theta^* & 0 \\ Z_u & {}^{Z_\alpha}/_{u^*} & Z_q + u^* & -gs\theta^* & 0 \\ M_u & {}^{M_\alpha}/_{u^*} & M_q & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ s\theta^* & -c\theta^* & 0 & u^* & 0 \end{bmatrix}}_{\boldsymbol{F}_d} \underbrace{\begin{bmatrix} \delta u \\ \delta w \\ \delta q \\ \delta\theta \\ \delta h \end{bmatrix}}_{\boldsymbol{x}_d} + \underbrace{\begin{bmatrix} X_{\delta_e} & X_{\delta_T} \\ Z_{\delta_e} & Z_{\delta_T} \\ M_{\delta_e} & Z_{\delta_T} \\ 0 & 0 \\ 0 & 0 \end{bmatrix}}_{\boldsymbol{G}_\delta} \underbrace{\begin{bmatrix} \delta_e \\ \delta_T \end{bmatrix}}_{\boldsymbol{\delta}_c} \tag{A.15}$$

where the plant matrix $\boldsymbol{F}_d$ is constant plant matrix that includes terms related to trimmed flight aerodynamic coefficients, mass and inertial properties of the aircraft, $\boldsymbol{x}_d$ is aircraft state vector, $\boldsymbol{G}_\delta$ is input coefficient matrix, and $\boldsymbol{\delta}_c$ is control input including elevator deflection command to control altitude or pitch attitude δ_e and thrust change command δ_T. Note that the model in (A.15) includes both short and long period (phugoid) modes of the aircraft.

APPENDIX B

THE DRYDEN GUST MODEL

This appendix explains the Dryden's continuous power spectral model for vertical wind gusts. It defines vertical translational velocity with a second order transfer function G_{w_g} parameterized by standard deviation on gust intensity σ_g, turbulence length L_w and velocity of the aircraft $\boldsymbol{v}$ as [33]

$$G_{w_g}(s) = \sigma_g \frac{\sqrt{\frac{|\boldsymbol{v}|^3}{\pi {L_w}^3}} + \sqrt{\frac{3|\boldsymbol{v}|}{\pi L_w}} s}{\frac{|\boldsymbol{v}|^2}{L_w^2} + \frac{2|\boldsymbol{v}|}{L_w} s + s^2}. \tag{B.1}$$

It also relates the vertical velocity and pitch rate of the gust with a first order transfer function parameterized by the wingspan of the aircraft b as [33]

$$G_{q_g}(s) = \frac{\frac{s}{|\boldsymbol{v}|}}{1 + \left(\frac{4b}{\pi|\boldsymbol{v}|}\right) s}. \tag{B.2}$$

Using (B.1) and (B.2), the combined third-order gust dynamics can be represented with 3 states in controllable-canonical state-space form as

$$\begin{bmatrix} \dot{x}_{w_1} \\ \dot{x}_{w_2} \\ \dot{x}_q \end{bmatrix} = \underbrace{\begin{bmatrix} 0 & 1 & 0 \\ -\frac{|\boldsymbol{v}|^2}{L_w^2} & -\frac{2|\boldsymbol{v}|}{L_w} & 0 \\ \frac{\pi\sigma_g}{4b}\sqrt{\frac{|\boldsymbol{v}|^3}{\pi L_w^3}} & \frac{\pi\sigma_g}{4b}\sqrt{\frac{3|\boldsymbol{v}|}{\pi L_w}} & -\frac{4b}{\pi|\boldsymbol{v}|} \end{bmatrix}}_{\boldsymbol{F}_g} \underbrace{\begin{bmatrix} x_{w_1} \\ x_{w_2} \\ x_q \end{bmatrix}}_{\boldsymbol{x}_g} + \underbrace{\begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}}_{\boldsymbol{G}_\eta} \eta_g \tag{B.3}$$

where $\eta_g \sim \mathcal{N}(0, \sigma_g^2)$. The first two elements in $\boldsymbol{x}_g$ correspond to vertical gust states, and the last element is related to pitch rate. The disturbances to wind vertical velocity and longitudinal angular velocity can be expressed as an output relation as a function of gust states as

$$\underbrace{\begin{bmatrix} w_g \\ q_g \end{bmatrix}}_{\boldsymbol{w}_g} = \underbrace{\begin{bmatrix} 0 & \frac{\pi\sigma_g}{4b}\sqrt{\frac{|\boldsymbol{v}|^3}{\pi L_w^3}} & \frac{\pi\sigma_g}{4b}\sqrt{\frac{3|\boldsymbol{v}|}{\pi L_w}} \\ 0 & 0 & \frac{1}{|\boldsymbol{v}|} \end{bmatrix}}_{\boldsymbol{C}_g} \boldsymbol{x}_g. \tag{B.4}$$

Driving the linear and angular filters G_{w_g} and G_{q_g} with independent, unit variance white noise η_g yields the linear vertical gust velocity w_g and angular pitch rate q_g, which perturb the aircraft.

APPENDIX C

GBAS ERROR MODELS

In this section, standard error models for GBAS differential processing are given based on Ground Accuracy Designator-C (GAD-C) and Airborne Accuracy Designator-B (AAD-B). The total GBAS measurement error vector $\boldsymbol{\nu}_{\bar{\rho}}$ in (2.13) has a diagonal covariance matrix

$$\boldsymbol{V}_{\bar{\rho}} = \begin{bmatrix} \sigma^2(\theta_1) & & \\ & \ddots & \\ & & \sigma^2(\theta_n) \end{bmatrix} \tag{C.1}$$

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

σ is a function of elevation angle of satellites and composed of airborne σ_a, ground station σ_g, tropospheric σ_t, and ionospheric σ_i standard deviations [49]

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

where σ_a contains airborne receiver noise σ_n and multipath σ_m components [48]

$$\sigma_a = \sqrt{\sigma_n^2 + \sigma_m^2} \tag{C.3}$$

and σ_m is modeled as [49]

$$\sigma_m(\theta) = 0.13 + 0.53\,\mathrm{e}^{-\theta/10^{\circ}}. \tag{C.4}$$

The residual tropospheric error for the airborne equipment σ_t is computed as [49]

$$\sigma_t(\theta) = \sigma_N\, h_0 \frac{10^{-6}}{\sqrt{0.002 + \sin^2\theta}} (1 - \mathrm{e}^{-\Delta h/h_0}) \tag{C.5}$$

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

The ionospheric error model is given as [49]

$$\sigma_i(\theta) = F_p\, \sigma_{\nabla_i} (x_a + 2\,\tau_h\, v_a) \tag{C.6}$$

where $\sigma_{\nabla i}$ is the standard deviation for the nominal ionospheric vertical spatial gradient, x_a is the slant range distance between current aircraft location and the ground station, v_a is the horizontal aircraft velocity, and F_p is the vertical-to-slant obliquity factor defined as [49]

$$F_p = \frac{1}{\sqrt{1 - \left(\frac{R_e \cos\theta}{R_e + h_I}\right)^2}} \tag{C.7}$$

where h_I is the ionospheric shell height.

The total ground station error is composed of the ground reference receiver errors $\sigma_{g,r}$ and the signal-in-space errors $\sigma_{g,s}$ as [30]

$$\sigma_g(\theta) = \sqrt{\frac{\sigma_{g,r}^2}{M} + \sigma_{g,s}^2} \tag{C.8}$$

where M is the number of reference station antennas.

The total ground reference receiver error including noise and multipath is modeled as [30]

$$\sigma_{g,r}(\theta) = \begin{cases} 0.15 + 0.84\,\mathrm{e}^{\theta/15.5^\circ}, & \theta \geq 35^\circ \\ 0.24, & \theta < 35^\circ \end{cases} \tag{C.9}$$

and the ground signal-in-space errors are modeled as [30]

$$\sigma_{g,s}(\theta) = \sqrt{0.04^2 + 0.01^2\, F_p}. \tag{C.10}$$

APPENDIX D

STATISTICAL INDEPENDENCE BETWEEN CURRENT-TIME ESTIMATE ERROR AND INNOVATIONS

As discussed in Section 5.2, the independence between current state estimate error and innovations in the Kalman filter-based estimator allows us to formulate the integrity risk as in (5.26) instead of the more complicated joint probability form in (3.55). In this section, we prove the statistical independence between the current-time state estimate error $\tilde{\mathbf{x}}_k^{\mathrm{KF}}$ and innovation $\boldsymbol{\gamma}_k$.

The current state estimate error $\tilde{\mathbf{x}}_k^{\mathrm{KF}}$ and the innovation vector $\boldsymbol{\gamma}_k$ are extracted from the Kalman filter-based evaluation model in (5.10) as

$$\tilde{\mathbf{x}}_k^{\mathrm{KF}} = \boldsymbol{L}_k^{'}\boldsymbol{\Phi}_{\mathrm{x}}\tilde{\mathbf{x}}_{k-1}^{\mathrm{KF}} - \boldsymbol{L}_k^{'}\overline{\boldsymbol{w}}_{k-1} + \boldsymbol{L}_k\boldsymbol{\nu}_{\rho\phi_k} + \boldsymbol{L}_k\boldsymbol{f}_k^{'} \tag{D.1}$$

$$\boldsymbol{\gamma}_k = -\boldsymbol{H}_k\boldsymbol{\Phi}_{\mathrm{x}}\tilde{\mathbf{x}}_{k-1}^{\mathrm{KF}} + \boldsymbol{H}_k\overline{\boldsymbol{w}}_{k-1} + \boldsymbol{\nu}_{\rho\phi_k} + \boldsymbol{f}_k^{'}. \tag{D.2}$$

Using (D.1) and (D.2), the covariance between $\tilde{\mathbf{x}}_k^{\mathrm{KF}}$ and $\boldsymbol{\gamma}_k$ is obtained as

$$\mathbb{E}[\tilde{\mathbf{x}}_k^{\mathrm{KF}}\boldsymbol{\gamma}_k^T] = -\boldsymbol{L}_k^{'}\big(\boldsymbol{\Phi}_{\mathrm{x}}\hat{\boldsymbol{P}}_{\mathrm{x}_{k-1}}\boldsymbol{\Phi}_{\mathrm{x}}^T + \overline{\boldsymbol{W}}_{k-1}\big)\boldsymbol{H}_k^T + \boldsymbol{L}_k\boldsymbol{V}_{\rho\phi_k}. \tag{D.3}$$

Recalling that $\overline{\boldsymbol{P}}_{\mathrm{x}_k} = \boldsymbol{\Phi}_{\mathrm{x}}\hat{\boldsymbol{P}}_{\mathrm{x}_{k-1}}\boldsymbol{\Phi}_{\mathrm{x}}^T + \overline{\boldsymbol{W}}_{k-1}$ from (3.9) and $\boldsymbol{L}_k^{'} = \boldsymbol{I} - \boldsymbol{L}_k\boldsymbol{H}_k$ from (5.5), and substituting them into (D.3) gives

$$\mathbb{E}[\tilde{\mathbf{x}}_k^{\mathrm{KF}}\boldsymbol{\gamma}_k^T] = \big(\boldsymbol{L}_k\boldsymbol{H}_k - \boldsymbol{I}\big)\overline{\boldsymbol{P}}_{\mathrm{x}_k}\boldsymbol{H}_k^T + \boldsymbol{L}_k\boldsymbol{V}_{\rho\phi_k}. \tag{D.4}$$

Substituting $\boldsymbol{L}_k = \hat{\boldsymbol{P}}_{\mathrm{x}_k}\boldsymbol{H}_k^T\boldsymbol{V}_{\rho\phi_k}^{-1}$ from (3.7) into (D.4) gives

$$\mathbb{E}[\tilde{\mathbf{x}}_k^{\mathrm{KF}}\boldsymbol{\gamma}_k^T] = \big(\hat{\boldsymbol{P}}_{\mathrm{x}_k}\boldsymbol{H}_k^T\boldsymbol{V}_{\rho\phi_k}^{-1}\boldsymbol{H}_k - \boldsymbol{I}\big)\overline{\boldsymbol{P}}_{\mathrm{x}_k}\boldsymbol{H}_k^T + \hat{\boldsymbol{P}}_{\mathrm{x}_k}\boldsymbol{H}_k^T. \tag{D.5}$$

Re-arranging (3.8) gives

$$\boldsymbol{H}_k^T\boldsymbol{V}_{\rho\phi_k}^{-1}\boldsymbol{H}_k = \hat{\boldsymbol{P}}_{\mathrm{x}_k}^{-1} - \overline{\boldsymbol{P}}_{\mathrm{x}_k}^{-1}. \tag{D.6}$$

Substituting (D.6) into (D.5) gives

$$\begin{aligned}\mathbb{E}[\tilde{\mathbf{x}}_k^{\mathrm{KF}}\boldsymbol{\gamma}_k^T] &= \big[\hat{\boldsymbol{P}}_{\mathrm{x}_k}(\hat{\boldsymbol{P}}_{\mathrm{x}_k}^{-1} - \overline{\boldsymbol{P}}_{\mathrm{x}_k}^{-1}) - \boldsymbol{I}\big]\overline{\boldsymbol{P}}_{\mathrm{x}_k}\boldsymbol{H}_k^T + \hat{\boldsymbol{P}}_{\mathrm{x}_k}\boldsymbol{H}_k^T \\ &= -\hat{\boldsymbol{P}}_{\mathrm{x}_k}^{-1}\boldsymbol{H}_k^T + \hat{\boldsymbol{P}}_{\mathrm{x}_k}^{-1}\boldsymbol{H}_k^T = 0.\end{aligned} \tag{D.7}$$

Eq. (D.7) proves that $\tilde{\mathbf{x}}_k^{\mathrm{KF}}$ and $\boldsymbol{\gamma}_k$ are statistically independent.

APPENDIX E

CLOSED-LOOP RELATION BETWEEN THE CONTROL INPUT AND IMU MEASUREMENT

This section provides the coefficients in the control input vector $\boldsymbol{\delta}_k$ and the IMU measurement vector $\tilde{\boldsymbol{u}}_k$ expressions in (5.17) and (5.18), respectively. These two expressions relate $\boldsymbol{\delta}_k$ and $\tilde{\boldsymbol{u}}_k$ in the closed loop evaluation model described in Fig. 5.1. The control input $\boldsymbol{\delta}_k$ is written in terms of the state estimate $\hat{\boldsymbol{x}}$ and the IMU measurement $\tilde{\boldsymbol{u}}_k$ in (5.14) as

$$\boldsymbol{\delta}_{c_k} = -\underbrace{\big(\boldsymbol{K}_x - \boldsymbol{K}_q\boldsymbol{T}_q\boldsymbol{T}_b\big)}_{\boldsymbol{K}'_x}\hat{\boldsymbol{x}}_k - \underbrace{\boldsymbol{K}_q\boldsymbol{T}_q}_{\boldsymbol{K}_{\tilde{u}}}\tilde{\boldsymbol{u}}_k \tag{E.1}$$

and the IMU measurement is written in terms of the true INS state $\boldsymbol{x}$, aircraft dynamic state $\boldsymbol{x}_d$, control input $\boldsymbol{\delta}_{c_k}$, and INS process noise $\boldsymbol{w}_k$ in (5.16) as

$$\tilde{\boldsymbol{u}}_k = \boldsymbol{T}_u\big(\boldsymbol{F}_d\boldsymbol{x}_{d_k} + \boldsymbol{G}_\delta\boldsymbol{\delta}_{c_k}\big) + \boldsymbol{T}_b\boldsymbol{x} + \boldsymbol{T}_\nu\boldsymbol{w}_k. \tag{E.2}$$

Solving the coupled equations (E.1) and (E.2) for $\boldsymbol{\delta}_k$ and $\tilde{\boldsymbol{u}}_k$ yields

$$\begin{aligned}\tilde{\boldsymbol{u}}_k &= \boldsymbol{U}_x\boldsymbol{x}_k + \boldsymbol{U}_{\tilde{x}}\tilde{\boldsymbol{x}}_k + \boldsymbol{U}_d\boldsymbol{x}_{d_k} + \boldsymbol{U}_w\boldsymbol{w}_k\\ \boldsymbol{\delta}_k &= \boldsymbol{\Delta}_x\boldsymbol{x}_k + \boldsymbol{\Delta}_{\tilde{x}}\tilde{\boldsymbol{x}}_k + \boldsymbol{\Delta}_d\boldsymbol{x}_{d_k} + \boldsymbol{\Delta}_w\boldsymbol{w}_k\end{aligned} \tag{E.3}$$

where the coefficients are

$$\begin{aligned}\boldsymbol{U}_x &= \big(\boldsymbol{I} + \boldsymbol{T}_u\boldsymbol{G}_\delta\boldsymbol{K}_{\tilde{u}}\big)^{-1}\big(\boldsymbol{T}_b - \boldsymbol{T}_u\boldsymbol{G}_\delta\boldsymbol{K}'_x\big)\\ \boldsymbol{U}_{\tilde{x}} &= -\big(\boldsymbol{I} + \boldsymbol{T}_u\boldsymbol{G}_\delta\boldsymbol{K}_{\tilde{u}}\big)^{-1}\boldsymbol{T}_u\boldsymbol{G}_\delta\boldsymbol{K}'_x\\ \boldsymbol{U}_d &= \big(\boldsymbol{I} + \boldsymbol{T}_u\boldsymbol{G}_\delta\boldsymbol{K}_{\tilde{u}}\big)^{-1}\boldsymbol{T}_u\boldsymbol{F}_d\\ \boldsymbol{U}_w &= \big(\boldsymbol{I} + \boldsymbol{T}_u\boldsymbol{G}_\delta\boldsymbol{K}_{\tilde{u}}\big)^{-1}\boldsymbol{T}_\nu\end{aligned} \tag{E.4}$$

and

$$\begin{aligned}\boldsymbol{\Delta}_x &= -\big(\boldsymbol{I} + \boldsymbol{K}_{\tilde{u}}\boldsymbol{T}_u\boldsymbol{G}_\delta\big)^{-1}\big(\boldsymbol{K}'_x + \boldsymbol{K}_{\tilde{u}}\boldsymbol{T}_b\big)\\ \boldsymbol{\Delta}_{\tilde{x}} &= -\big(\boldsymbol{I} + \boldsymbol{K}_{\tilde{u}}\boldsymbol{T}_u\boldsymbol{G}_\delta\big)^{-1}\boldsymbol{K}'_x\\ \boldsymbol{\Delta}_d &= -\big(\boldsymbol{I} + \boldsymbol{K}_{\tilde{u}}\boldsymbol{T}_u\boldsymbol{G}_\delta\big)^{-1}\boldsymbol{K}_{\tilde{u}}\boldsymbol{T}_u\boldsymbol{F}_d\\ \boldsymbol{\Delta}_w &= -\big(\boldsymbol{I} + \boldsymbol{K}_{\tilde{u}}\boldsymbol{T}_u\boldsymbol{G}_\delta\big)^{-1}\boldsymbol{K}_{\tilde{u}}\boldsymbol{T}_\nu.\end{aligned} \tag{E.5}$$

APPENDIX F

SIMULATION DATA

This appendix gives the numerical model input parameters utilized in obtaining the simulation results.

Table F.1. Comparison of Different Grade IMU Error Specifications [6]

Parameter	Navigation Grade	Tactical Grade		Unit
		High End	Low End	
Gyro angle random walk	0.001	0.07	0.15	$\text{deg}/\sqrt{\text{h}}$
Gyro bias error	0.01	0.5	10	deg/h
Gyro time constant	3600	3600	3600	s
Accelerometer white noise	$10^{-5}g$	$3 \times 10^{-4}g$	$5 \times 10^{-3}g$	m/s^2
Accelerometer bias error	$10^{-5}g$	$3 \times 10^{-4}g$	$5 \times 10^{-3}g$	m/s^2
Accelerometer bias time constant	3600	3600	3600	s

Table F.2. GNSS Error Specifications [6, 32]

Parameter	Value	Unit
Standalone residual errors and thermal noise	3	m
SD Carrier phase multipath noise	1	cm
SD Code phase multipath noise	30	cm
SD Carrier phase thermal noise	0.2	cm
SD Code phase thermal noise	50	cm
Multipath time constant	100	s

Table F.3. GBAS Error Model Parameters [48]

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

Table F.4. Longitudinal Flight Conditions [14]

Flight Conditions	Value	Unit
Aircraft Speed	131	knots
Flight Path Angle	-5	deg
Air Density	11.85	kg/m^3
Altitude	500	m

Table F.5. B747 Aircraft Properties [14]

Properties	Value	Unit
Mass	$289,550$	kg
Moment of Inertia	44.87×10^6	$kg.m^2$
Wing Span	59.74	m
Wing Chord	8.32	m
Wing Area	510.96	m^2

Table F.6. Aerodynamic Coefficients and their Derivatives [14]

	Drag	Lift	Pitch
Coefficient	0.266	-0.0174	0
AoA Derivative	0.084	4.24	-0.629
Speed Derivative	-0.0064	-0.084	-0.0928
Pitch Rate Derivative	0	-0.0928	-20.5

BIBLIOGRAPHY

[1] D. M. Akos. Who's afraid of the spoofer? GPS/GNSS spoofing detection via automatic gain control (AGC). *NAVIGATION, Journal of The Institute of Navigation*, 59(4):281–290, 2012.

[2] K. Alexander. GNSS intentional interference and spoofing. In *RTCA 2016 Global Aviation Symposium*. Available at `http://www.gps.gov/multimedia/presentations/2016/04/APEC/`.

[3] J. E. Angus. RAIM with multiple faults. *NAVIGATION, Journal of The Institute of Navigation*, 53(4):249–257, 2006.

[4] R. Avram, X. Zhang, and J. Muse. Quadrotor accelerometer and gyroscope sensor fault diagnosis with experimental results. In *Proceedings of the Annual Conference of the Prognostics and Health Management Society*, volume 8, pages 625–623.

[5] J. A. Bhatti. *Sensor Deception Detection and Radio-Frequency Emitter Localization*. PhD thesis, Department of Aerospace Engineering and Engineering Mechanics, The University of Texas at Austin, Austin, TX, 2015.

[6] R. G. Brown and P. Y-C. Hwang. *Introduction to random signals and applied Kalman filtering: with MATLAB exercises and solutions*, volume 1. New York: Wiley, 1997.

[7] A. E. Bryson. *Applied Linear Optimal Control Paperback with CD-ROM: Examples and Algorithms*, volume 1. Cambridge University Press, 2002.

[8] R. H. Chen, A. Gevorkian, A. Fung, W. Chen, and V. Raska. Multi-sensor data integration for autonomous sense and avoid. In *AIAA Infotech at Aerospace Technical Conference*, 2011.

[9] J. L. Crassidis and J. L. Junkins. *Optimal estimation of dynamic systems*. CRC press, 2011.

[10] N. El-Sheimy and X. Niu. The promise of MEMS to the navigation community. *Inside GNSS*, 2(2):46-56, 2007.

[11] P. Enge. Local area augmentation of GPS for the precision approach of aircraft. *Proceedings of the IEEE*, 87(1):111–132, Jan 1999.

[12] J. Farrell. *Aided navigation: GPS with high rate sensors*. McGraw-Hill, Inc., 2008.

[13] A. Gelb. *Applied optimal estimation*. MIT Press, 1974.

[14] R. K. Heffley and W. F. Jewell. Aircraft handling qualities data. *NASA-CR-2144*, 1972.

[15] G. Hein, F. Kneissl, J-A. Avila-Rodriguez, and S. Wallner. Authenticating GNSS proofs against spoofs part 2. *Inside GNSS*, 2(5):58–63, 2007.

[16] F. M. Hoblit. *Gust loads on aircraft: concepts and applications*. AIAA, 1988.

[17] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon, and P. M. Jr. Kintner. Assessing the spoofing threat: Development of a portable GNSS civilian spoofer. In *Proceedings of the 21st International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2008)*, pages 2314–2325, Savannah, GA, Sep 2008.

[18] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle. GPS spoofer countermeasure effectiveness based on signal strength, noise power, and C/N0 measurements. *International Journal of Satellite Communications and Networking*, 30(4):181–191, 2012.

[19] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle. GPS vulnerability to spoofing threats and a review of antispoofing techniques. *International Journal of Navigation and Observation*, 2012, 2012.

[20] M. Joerger and B. Pervan. Kalman filter-based integrity monitoring against sensor faults. *Journal of Guidance, Control, and Dynamics*, 36(2):349–361, Aug 2013.

[21] M. Joerger, S. Stevanovic, S. Langel, and B. Pervan. Integrity risk minimisation in RAIM part 1: Optimal detector design. *Journal of Navigation*, 69(03):449–467, 2016.

[22] A. Jovanovic, C. Botteron, and P. A. Farine. Multi-test detection and protection algorithm against spoofing attacks on GNSS receivers. In *Proceedings of IEEE/ION PLANS 2014*, pages 1258–1271, Monterey, CA, May 2014.

[23] A. J. Kerns, D. P. Shepard, J. A. Bhatti, and T. E. Humphreys. Unmanned aircraft capture and control via gps spoofing. *Journal of Field Robotics*, 31(4):617–636, 2014.

[24] S. Khanafseh and B. Pervan. Autonomous airborne refueling of unmanned air vehicles using the global positioning system. *Journal of Aircraft*, 44(5):1670–1682, Aug 2007.

[25] S. Khanafseh, N. Roshan, S. Langel, F. Chan, M. Joerger, and B. Pervan. GNSS spoofing detection using RAIM with INS coupling. In *Proceedings of IEEE/ION PLANS 2014*, pages 1232–1239, Monterey, CA, Sep 2014.

[26] S. Langel, S. Khanafseh, F-C. Chan, and B. Pervan. Tightly coupled GPS/INS integration for differential carrier phase navigation systems using decentralized estimation. In *Proceedings of IEEE/ION PLANS 2010*, pages 397–409, Indian Wells, CA, May 2010.

[27] M. B. Ledvina, J. W. Bencze, B. Galusha, and I. Miller. An in-line spoofing module for legacy GPS receivers. In *Proceedings of the 2010 International Technical Meeting of The Institute of Navigation*, pages 698–712, San Diego, CA, 2010.

[28] VECTORNAV Embedded Navigation Solutions LLC. Inertial measurement units and inertial navigation, 2016. Available at `http://www.vectornav.com/support/library/imu-and-ins`.

[29] C. E. McDowell. GPS spoofer and repeater mitigation system using digital spatial nulling, Jul 2007. US Patent 7,250,903.

[30] G. A. McGraw, T. Murphy, M. Brenner, S. Pullen, and A. J. Van Dierendonck. Development of the LAAS accuracy models. In *Proceedings of the 13th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GPS 2000)*, pages 1212–1223, Salt Lake City, UT, Sep 2000.

[31] M. Meuer, A. Konovaltsev, M. Cuntz, and C. Hättich. Robust joint multi-antenna spoofing detection and attitude estimation using direction assisted multiple hypotheses RAIM. In *Proceedings of the 25th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2012)*, pages 3007–3016, Nashville, TN, Sep 2012.

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

[33] D. J. Moorhouse and R. J. Woodcock. Background information and user guide for MIL-F-8785C, military specification-flying qualities of piloted airplanes. Technical report, DTIC Document, 1982.

[34] S. Moshavi. Multi-user detection for DS-CDMA communications. *IEEE Communications Magazine*, 34(10):124–136, 1996.

[35] J. Nielsen, A. Broumandan, and G. Lachapelle. Spoofing detection and mitigation with a moving handheld receiver. *GPS World magazine*, 21(9):27–33, 2010.

[36] C. O'Brien. GPS aviation applications, 2006. Available at `http://www.gps.gov/applications/aviation/`.

[37] International Civil Aviation Organization. *International Standards and Recommended Practices, Annex 10*, volume 1: Radio Navigation Aids. New Zealand, 6th edition, 2006.

[38] B. W. Parkinson. *Progress in Astronautics and Aeronautics: Global Positioning System: Theory and Applications*, volume 2. AIAA, 1996.

[39] B. W. Parkinson and P. Axelrad. Autonomous GPS integrity monitoring using the pseudorange residual. *NAVIGATION, Journal of The Institute of Navigation*, 35(2):255–274, 1988.

[40] B. S. Pervan, D. G. Lawrence, and B. W. Parkinson. Autonomous fault detection and removal using GPS carrier phase. *IEEE Transactions on Aerospace and Electronic Systems*, 34(3):897–906, Jul 1998.

[41] M. L. Psiaki and T. E. Humphreys. GNSS spoofing and detection. *Proceedings of the IEEE*, 104(6):1258–1270, June 2016.

[42] M. L. Psiaki, S. P. Powell, and B. W. Ohanlon. GNSS spoofing detection using high-frequency antenna motion and carrier-phase data. In *Proceedings of the 26th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2013)*, pages 2949–2991, Nashville, TN, Sep 2013.

[43] S. Pullen. What are the differences between accuracy, integrity, continuity, and availability, and how are they computed. *Inside GNSS*.

[44] S. Pullen, B. Pervan, P. Enge, and B. Parkinson. A comprehensive integrity verification architecture for on-airport LAAS category iii precision landing. In *Proceedings of the 9th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GPS 1996)*, volume 9, pages 1623–1634, Kansas City, MO, Sep 1996.

[45] R. M. Rogers. *Applied mathematics in integrated navigation systems*, volume 1. AIAA, 2003.

[46] J. W. Rustenburg, D. Skinn, and D. O. Tipps. An evaluation of methods to separate maneuver and gust load factors from measured acceleration time histories. Technical report, DTIC Document, 1999.

[47] P. Faramarzi S. Peterson. Exclusive: Iran hijacked us drone, says iranian engineer, Dec, 2011. Available at `http://www.csmonitor.com/World/Middle-East/2011/1215/Exclusive-Iran-hijacked-US-drone-says-Iranian-engineer-Video`.

[48] RTCA SC-159. *Minimum Aviation System Performance Standards for the Local Area Augmentation System (LAAS)*. RTCA, Incorporated, Dec 2004.

[49] RTCA SC-159. *Minimum Operational Performance Standards for GPS Local Area Augmentation System Airborne Equipment(LAAS)*. Document. RTCA, Incorporated, Dec 2008.

[50] D. V. Simili and B. Pervan. Code-carrier divergence monitoring for the GPS local area augmentation system. In *Proceedings of IEEE/ION PLANS 2006*, pages 483–493, San Diego, CA, Apr 2006.

[51] J. Speidel, M. Tossaint, S. Wallner, J. Á. Ávila-Rodríguez, and G. Hein. Integrity for aviation: Comparing future concepts. *Inside GNSS*, 8(4):54–64.

[52] P. F. Swaszek, R. J. Hartnett, and K. C. Seals. GNSS spoof detection using independent range information. In *Proceedings of the 2016 International Technical Meeting of The Institute of Navigation*, pages 739–747, Monterey, California, Jan 2016.

[53] P. F. Swaszek, K. C. Seals, S. A. Pratz, B. N. Arocho, and R. J. Hartnett. GNSS spoof detection using shipboard IMU measurements. In *Proceedings of the 27th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2014)*, pages 745–758, Tampa, FL, Sep 2015.

[54] C. Tanil, S. Khanafseh, M. Joerger, and B. Pervan. An INS monitor to detect GNSS spoofers capable of tracking vehicle position. *IEEE Transactions on Aerospace and Electronic Systems*, 2016 (in review).

[55] C. Tanil, S. Khanafseh, M. Joerger, and B. Pervan. Kalman filter-based INS monitor to detect GNSS spoofers capable of attacking aircraft position. In *Proceedings of IEEE/ION PLANS 2016*, pages 1027–1034, Savannah, GA, Apr 2016.

[56] C. Tanil, S. Khanafseh, and B. Pervan. Detecting GNSS spoofing attacks using inertial sensing of aircraft disturbance response. *The AIAA Journal of Guidance, Control, and Dynamics*, 2016 (in review).

[57] C. Tanil, S. Khanafseh, and B. Pervan. The impact of wind gust on detectability of GPS spoofing attack using RAIM with INS coupling. In *Proceedings of the ION 2015 Pacific PNT Meeting*, pages 674–686, Honolulu, HI, Apr 2015.

[58] C. Tanil, S. Khanafseh, and B. Pervan. GNSS spoofing attack detection using aircraft autopilot response to deceptive trajectory. In *Proceedings of the 28th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2015)*, pages 3345–3357, Tampa, FL, Sep 2015.

[59] C. Tanil, S. Khanafseh, and B. Pervan. An INS monitor against GNSS spoofing attacks during GBAS and SBAS-assisted aircraft landing approaches. In *Proceedings of the 29th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2016)*, pages 2981–2990, Portland, OR, Sep 2016.

[60] M. Thomas. Global navigation space systems: reliance and vulnerabilities. *The Royal Academy of Engineering. London, UK*, 2011.

[61] D. Titterton and J. L. Weston. *Strapdown Inertial Navigation Technology*, volume 17 of *Electromagnetics and Radar Series*. Institution of Engineering and Technology, 2004.

[62] J. S. Warner and R. G. Johnston. GPS spoofing countermeasures. *Homeland Security Journal*, 25(2):19–27, 2003.

[63] H. Wen, P. Y-R. Huang, J. Dyer, A. Archinal, and J. Fagan. Countermeasures for GPS signal spoofing. In *Proceedings of the 18th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2005)*, pages 1285–1290, Long Beach, CA, Sep 2005.

[64] K. D. Wesson, M. P. Rothlisberger, and T. E. Humphreys. A proposed navigation message authentication implementation for civil GPS anti-spoofing. In *Proceedings of the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2011)*, pages 3129–3140, Portland, OR, Sep 2011.

[65] T. R. Yechout and S. L. Morris. *Introduction to aircraft flight mechanics*. AIAA, 2003.