sensors

MDPI

Article

Impact Assessment of GNSS Spoofing Attacks on INS/GNSS Integrated Navigation System

Yang Liu *, Sihai Li, Qiangwen Fu and Zhenbo Liu

School of Automation, Northwestern Polytechnical University, Xi'an 710072, China; lisihai@nwpu.edu.cn (S.L.); fuqiangwen@nwpu.edu.cn (Q.F.); zhnbliu@gmail.com (Z.L.)

* Correspondence: liuyang@mail.nwpu.edu.cn; Tel.: +86-29-8843-1369

Received: 29 March 2018; Accepted: 1 May 2018; Published: 4 May 2018

Abstract: In the face of emerging Global Navigation Satellite System (GNSS) spoofing attacks, there is a need to give a comprehensive analysis on how the inertial navigation system (INS)/GNSS integrated navigation system responds to different kinds of spoofing attacks. A better understanding of the integrated navigation system's behavior with spoofed GNSS measurements gives us valuable clues to develop effective spoofing defenses. This paper focuses on an impact assessment of GNSS spoofing attacks on the integrated navigation system Kalman filter's error covariance, innovation sequence and inertial sensor bias estimation. A simple and straightforward measurement-level trajectory spoofing simulation framework is presented, serving as the basis for an impact assessment of both unsynchronized and synchronized spoofing attacks. Recommendations are given for spoofing detection and mitigation based on our findings in the impact assessment process.

Keywords: GNSS spoofing; impact assessment; integrated navigation system

1. Introduction

Global Navigation Satellite System (GNSS) spoofing is a technique to trick the victim receiver into generating an erroneous position fix and/or clock offset, by deliberately broadcasting legitimate-appearing false satellite signals [1,2]. Civil GNSS service is vulnerable to spoofing due to the open structure and low power of GNSS satellite signals [1]. GNSS spoofing is difficult to detect and may result in more serious situations than jamming, since the user may not be aware of it [3].

GNSS spoofing is not a new topic. When Global Positioning System (GPS) was first declared full operational in 1995, researchers from MITRE examined GPS spoofing and its countermeasures [4]. The Volpe report, released by US Department of Transportation clearly pointed out the potential for spoofing attacks [1]. However, the GNSS community gave little attention to this threat, until a portable GPS spoofer was successfully developed and demonstrated [5]. Several proof-of-concept spoofing tests have been carried out against unmanned aerial vehicles [6,7], super yachts [8], cars and smartphones [6,9]. Besides these filed demonstrations, the Iran-US RQ-170 incident and the recently reported GPS problem in central Moscow [10] and the Black Sea [11], have further intensified the interest in this area. With open source GPS signal simulators available online and the fast developing software-defined radio technology, GNSS spoofing has become "*not only feasible but also affordable*" [12].

In response to the emerging GNSS spoofing threats, many contributions have been made, which can be divided into spoofing implementation, assessment, detection and mitigation. (1) *Spoofing implementation* focuses on the mechanisms of spoofing attacks, serving as the basis for impact analysis and validation of anti-spoofing methods. Several research groups have implemented the so-called receiver-spoofer as defined in [5], while the others rely on simulators/repeaters for spoofing simulation. (2) *Spoofing impact assessment* evaluates the spoofing effects on GNSS receivers and systems that depend on, or relate to, GNSS. (3) Research on *spoofing detection and mitigation*, which take up the majority of the

GNSS community's efforts has resulted in the development of methods to revel, classify and eliminate spoofing threats. These methods can be classified into signal-processing based, encryption-based, drift-monitoring-based, signal geometry-based and multipronged spoofing defense strategies, as summarized in [2]. Detailed reviews of spoofing detection and mitigation methods can also be found in [13–16].

Among the existing spoofing defenses, inertial measurement unit (IMU) or inertial navigation system (INS) aided methods have been developed. With specific force and angular rate being the only required measurements for dead-reckoning, INS is self-contained and thus, invulnerable to radio frequency interference, like jamming and spoofing. The widely used INS/GNSS integrated navigation system inherits this nature to some extent. Attitude solutions of INS have been used to detect GNSS spoofing with a dual antenna configuration [17]. INS/GNSS Kalman filter innovations have been investigated to detect spoofing attacks [18–21]. The popularity of IMU/INS makes these methods very promising as many vehicle systems (land/sea/air/space) rely on them to serve a broad variety of applications.

The 2001 Volpe report raised the issue that "little publicly available information or test results exist concerning the response of commercial receivers to spoofing" [1]. This belongs to the impact assessment and has been answered by many contributions over the last decade. The US Department of Homeland Security hosted the 2017 GPS Equipment Testing for Critical Infrastructure, which provided manufacturers of commercial GPS receivers with a valuable testing opportunity against live-sky spoofing. Although the GNSS community has begun to carry out a standard and unified process to thoroughly assess the spoofing impacts on GNSS receivers, unfortunately, there is still a lack of comprehensive spoofing impact assessment on the widely used INS/GNSS integrated navigation system. When INS is integrated with GNSS, it can be affected by spoofing attacks due to cascade effects of the integration mechanism. To address the impact assessment problem for INS/GNSS systems under spoofing attacks, we focus on the response of the integrated navigation system's Kalman filter to spoofed GNSS measurements, including its error covariance, innovation sequence and inertial sensor bias estimation. Understanding the behavior of INS/GNSS systems in the face of GNSS spoofing is crucial to hardening the integrated system against spoofing threats. In order to avoid the complexity and high cost of setting up live-sky GNSS spoofing tests (which must be authorized) for INS/GNSS systems, we propose a simple and straightforward high fidelity simulation framework. Based on the clues found in the impact assessment process, recommendations are given for potential spoofing detection and mitigation methods. In this paper, we make three main contributions:

- Based on the authentic and spoofed signal model, a comparison between unsynchronized and synchronized GNSS spoofing attacks is given. A framework for a measurement-level trajectory spoofing simulation is proposed, which simplifies the process of impact assessment for integrated navigation systems.
- We systematically analyze the impact of spoofing on the integrated navigation filter's error covariance, innovation and inertial sensor bias estimation, revealing how the conventionally used Kalman filer responds to spoofing attacks.
- According to the impact assessment, we make recommendations for the cautious use of (1) error covariance for integrity monitoring, and (2) calibrated inertial sensors for pure INS solutions. Spoofing detection methods based on innovations and inertial sensor bias monitoring are suggested.

The remainder of this paper is organized as follows. Section 2 briefly introduces the INS/GNSS model used in this paper; Section 3 introduces basic GNSS spoofing attack modes and presents two methods for measurement-level spoofing simulation; Section 4 focuses on the impact assessment analysis and our recommendations for spoofing detection and mitigation; Section 5 verifies our findings through simulations, and the conclusions are given in Section 6.

2. INS/GNSS Integrated Navigation Model

In this paper, for simplicity, the loosely coupled INS/GNSS integrated navigation system is considered. As we focused on the Kalman filter's error covariance matrix, innovation and inertial sensor bias estimation, the analytical derivation and analysis in the following sections are also applicable to the tightly coupled system. The underlying INS/GNSS integrated system is a nonlinear time-varying system, so the extended Kalman filter was used for the integration. The error state, instead of the total state, of the navigation system was chosen as the state vector, which is defined as [22]

$$\boldsymbol{x}(t) = \begin{bmatrix} \boldsymbol{\phi}^T & (\delta \boldsymbol{v}^n)^T & (\delta \boldsymbol{p})^T & (\boldsymbol{\varepsilon}^b)^T & (\nabla^b)^T \end{bmatrix}^T, \tag{1}$$

where $\boldsymbol{\phi} = [\phi_E, \phi_N, \phi_U]^T$ is the misalignment angle vector; $\delta \boldsymbol{v}^n = [\delta v_E^n, \delta v_N^n, \delta v_U^n]^T$ is the velocity error vector; $\delta \boldsymbol{p} = [\delta L, \delta \lambda, \delta H]^T$ is the position error vector, consisting of latitude, longitude and height components; and $\boldsymbol{\varepsilon}^b = [\varepsilon_R^b, \varepsilon_F^b, \varepsilon_U^b]^T$ and $\nabla^b = [\nabla_R^b, \nabla_F^b, \nabla_U^b]^T$ represent the gyro and accelerometer bias vectors, respectively. Note that the subscripts E, N, U represent the east, north and up components in the navigation frame, respectively. The subscripts, R, F, U represent the right, forward and up components in the body frame, respectively.

After the linearization, the system dynamic model and measurement model can be written as [22]

$$\begin{cases} \dot{\boldsymbol{x}}(t) = \boldsymbol{F}(t)\boldsymbol{x}(t) + \boldsymbol{w}(t) \\ \boldsymbol{z}(t) = \widetilde{\boldsymbol{p}}_{\mathrm{INS}} - \widetilde{\boldsymbol{p}}_{\mathrm{GNSS}} = \boldsymbol{H}(t)\boldsymbol{x}(t) + \boldsymbol{v}(t) \end{cases}, \tag{2}$$

where $\boldsymbol{F}(t)$ is the system matrix; $\boldsymbol{w}(t)$ is the process noise vector; $\boldsymbol{z}(t)$ represents the difference between the position solution of INS $\widetilde{\boldsymbol{p}}_{\mathrm{INS}}$ and GNSS $\widetilde{\boldsymbol{p}}_{\mathrm{GNSS}}$; $\boldsymbol{H}(t)$ is the measurement matrix; and $\boldsymbol{v}(t)$ represents the noise of GNSS solutions. The system matrix, $\boldsymbol{F}(t)$, takes the form [23]

$$\boldsymbol{F}(t) = \begin{bmatrix} \boldsymbol{F}_{11} & \boldsymbol{F}_{12} & \boldsymbol{F}_{13} & -\boldsymbol{C}_b^n & \boldsymbol{0}_3 \\ \boldsymbol{F}_{21} & \boldsymbol{F}_{22} & \boldsymbol{F}_{23} & \boldsymbol{0}_3 & \boldsymbol{C}_b^n \\ \boldsymbol{0}_3 & \boldsymbol{F}_{32} & \boldsymbol{F}_{33} & \boldsymbol{0}_3 & \boldsymbol{0}_3 \\ \boldsymbol{0}_3 & \boldsymbol{0}_3 & \boldsymbol{0}_3 & \boldsymbol{0}_3 & \boldsymbol{0}_3 \\ \boldsymbol{0}_3 & \boldsymbol{0}_3 & \boldsymbol{0}_3 & \boldsymbol{0}_3 & \boldsymbol{0}_3 \end{bmatrix}, \tag{3}$$

where $\boldsymbol{F}_{ij}$ is a 3-by-3 matrix; $\boldsymbol{C}_b^n$ is a 3-by-3 body frame to navigation frame rotation matrix; and $\boldsymbol{0}_3$ is a 3-by-3 zero matrix. The details of $\boldsymbol{F}_{ij}$ are given in Appendix A [23]. The measurement matrix is a constant matrix and is defined as $\boldsymbol{H}(t) = \begin{bmatrix} \boldsymbol{0}_3 & \boldsymbol{0}_3 & \boldsymbol{I}_3 & \boldsymbol{0}_3 & \boldsymbol{0}_3 \end{bmatrix}$, in which $\boldsymbol{I}_3$ is a 3-by-3 identity matrix.

3. GNSS Spoofing Attacks and Measurement-Level Simulation

3.1. GNSS Spoofing Attacks

A brief illustration of a GNSS spoofing attack is given in Figure 1.

Assuming that the spoofing attack starts at t_{Init}, the received GNSS signal, $y(t)$, at the receiver can be expressed as [2],

$$y(t) = y_a(t) + y_s(t) + n(t), \qquad t \geq t_{\mathrm{Init}}, \tag{4}$$

where $y_a(t)$ and $y_s(t)$ are authentic and spoofed signals, respectively. $n(t)$ is the receiver noise. Taking GPS L1 coarse/acquisition code spoofing as an example, the received authentic signal $y_a(t)$ is given by

$$y_a(t) = \sum_i^{N_a} \sqrt{2P_a^{(i)}} D_a^{(i)}\left(t - \tau_a^{(i)}\right) C_a^{(i)}\left(t - \tau_a^{(i)}\right) \sin\left(2\pi\left(f_{1,a}^{(i)} + f_{d,a}^{(i)}\right)t + \theta_{1,a}^{(i)}\right). \tag{5}$$

The received spoofed signal $y_s(t)$ has a similar form:

$$y_s(t) = \sum_{i}^{N_s} \sqrt{2P_s^{(i)}} D_s^{(i)}\left(t - \tau_s^{(i)}\right) C_s^{(i)}\left(t - \tau_s^{(i)}\right) \sin\left(2\pi\left(f_{1,s}^{(i)} + f_{d,s}^{(i)}\right)t + \theta_{1,s}^{(i)}\right), \quad (6)$$

where the superscript (i) represents the ith satellite, the subscripts a and s represent the authentic and spoofed signals, respectively. N is the number of visible satellites; P is the signal power; D is the navigation data bit stream; C is the pseudo random noise (PRN) code sequence; τ is the signal propagation delay; f_1 is the GPS L1 signal frequency; f_d is the Doppler shift; and θ_1 is the received initial carrier phase.

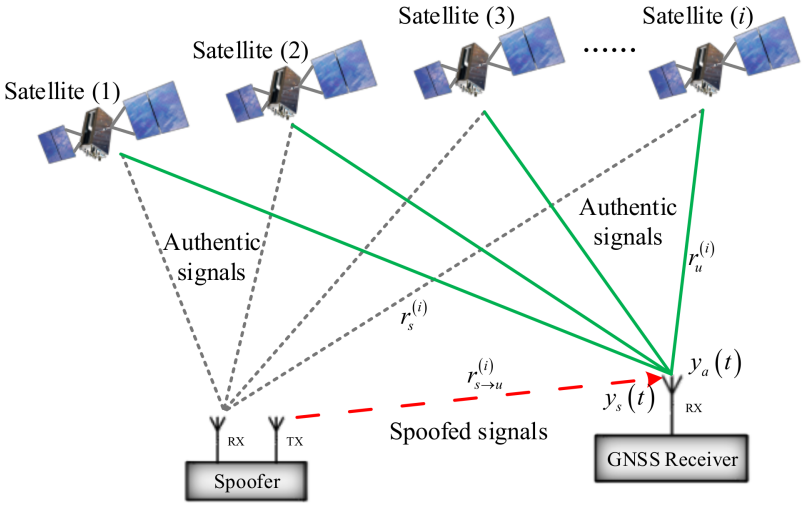

Figure 1. Global Navigation Satellite System (GNSS) spoofing attack illustration.

There are several essential features of GNSS spoofing attacks [2,24]. The spoofing signals must have exactly the same PRN code sequence and signal frequency to those of the authentic signals. The number of spoofed satellites is generally equal to the number of authentic signals; if not, the introduction of inconsistency may trigger the receiver autonomous integrity monitoring algorithm. The structure of the navigation data bit stream should be the same as that of the authentic stream, but the content may be manipulated to introduce the intended deception. The received initial carrier phase is generally unknown and it is practically impossible for the spoofer to align with the authentic, unless a very precise (cm-level) relative position between the spoofer and the target receiver is known. The Doppler shift of the spoofed signal is not necessarily the same as the authentic signal; however, it must be consistent with the spoofer's own code phase variation.

GNSS spoofing attacks can be divided into unsynchronized and synchronized spoofing, based on whether the spoofed signals are time synchronized (code-phase aligned) with the authentic ones [16]. This classification highlights the error characteristics of spoofing attacks on raw GNSS measurements, which has an analogy to the step and ramp faults in integrity analysis. If the spoofer cannot know the target receiver's position accurately (meter-level to maximum of a half code chip) [16], only unsynchronized spoofing attacks can be carried out. For synchronized spoofing attacks, the spoofer accurately knows the target receiver's real-time position, which makes it possible for the spoofed signals' delay and the Doppler shift to be consistent with the authentic signal at the target receiver end [25]. A comparison between these two spoofing attack modes is given in Appendix B. Understanding the characteristics of different spoofing attacks is essential to achieve high fidelity spoofing simulation for impact assessment and defense verification.

3.2. Measurement-Level Spoofing Attack Simulation

To analyze the signal-level response of the GNSS receivers to spoofing attacks, a sophisticated signal-level spoofing simulator is necessary. However, for an impact assessment on INS/GNSS integrated navigation systems focusing on the Kalman filter performance with spoofed GNSS measurements, a measurement-level simulator is sufficient. The measurement-level simulation of spoofing attacks has the advantage of easy and rapid implementation, avoiding the complexity and high cost of setting up live-sky GNSS spoofing tests which must be authorized. The measurement-level simulator generates raw GNSS observations based on given a constellation, error model and predefined trajectory profile (each epoch with a seven-dimensional noise free PVT solution). Using the synchronized spoofing attack as an example, we show how the pseudorange measurements of the target receiver are affected, which also shows how the spoofer or spoofing simulator construct pseudorange measurements for a synchronized spoofing attack. While for unsynchronized spoofing, the spoofing simulator can generate arbitrary measurements without considering the relationship with the authentic signals.

A raw pseudorange measurement for the ith satellite $\rho^{(i)}$ at time t is modeled as

$$\rho^{(i)} = c\tau^{(i)} + c\Big((t + \delta t_u) - \Big(t + \delta t^{(i)}\Big)\Big), \tag{7}$$

where $\tau^{(i)}$ is the signal transmission delay; c is the speed of light; and δt_u and $\delta t^{(i)}$ are the receiver and satellite clock offset, respectively. For authentic signals, the signal delay, $\tau_a^{(i)}$, consists of the delay caused by the geometric range, $r_u^{(i)}$, the ionospheric effect, $I_a^{(i)}$, and the tropospheric, effect $T_a^{(i)}$, that is,

$$\tau_a^{(i)} = \frac{r_u^{(i)}}{c} + I_a^{(i)} + T_a^{(i)}. \tag{8}$$

Considering the receiver noise, $n_{\rho,a}^{(i)}$, the authentic pseudorange is obtained with

$$\rho_a^{(i)} = r_u^{(i)} + c\Big(\delta t_{u,a} - \delta t_a{}^{(i)}\Big) + cI_a^{(i)} + cT_a^{(i)} + n_{\rho,a}^{(i)}. \tag{9}$$

For spoofed signals, the signal delay, $\tau_s^{(i)}$, is

$$\tau_s^{(i)} = \frac{r_s^{(i)} + r_{s\to u}}{c} + I_s^{(i)} + T_s^{(i)} + \nabla\tau_{proc}^{(i)} + \nabla\tau_{ctrl}^{(i)}, \tag{10}$$

where $r_s^{(i)}$ is the geometric range from the spoofer to the satellite, and $r_{s\to u}$ is the geometric range from the spoofer to the target receiver (common for all satellites). $\nabla\tau_{proc}^{(i)}$ and $\nabla\tau_{ctrl}^{(i)}$ are the signal processing delay and controlled signal delay, respectively. Assuming a common atmospheric effect for the spoofer and target receiver, Equation (10) can be written as

$$\begin{aligned}\tau_s^{(i)} &= \frac{r_u^{(i)} + \left(r_s^{(i)} + r_{s\to u} - r_u^{(i)}\right)}{c} + I_a^{(i)} + T_a^{(i)} + \nabla\tau_{proc}^{(i)} + \nabla\tau_{ctrl}^{(i)} \\ &= \underbrace{\frac{r_u^{(i)}}{c} + I_a^{(i)} + T_a^{(i)}}_{\tau_a^{(i)}} + \underbrace{\frac{\left(r_s^{(i)} + r_{s\to u} - r_u^{(i)}\right)}{c} + \nabla\tau_{proc}^{(i)} + \nabla\tau_{ctrl}^{(i)}}_{\nabla\tau_s^{(i)}},\end{aligned} \tag{11}$$

where $\nabla\tau_s^{(i)}$ is the additional signal delay introduced by the spoofer at the target receiver end. For a receiver/spoofer with the ability to predict the navigation bits, $\delta t_{adv\_ctrl}^{(i)}$ is introduced to represent the advanced prediction time by the spoofer to compensate for additional signal delays. Then, we get

$$\begin{aligned}\rho_s^{(i)} &= c\left(\tau_a^{(i)} + \nabla\tau_s^{(i)}\right) + c\left((t+\delta t_{u,a}) - \left(t + \delta t_{adv\_ctrl}^{(i)} + \delta t_a^{(i)}\right)\right) \\ &= c\tau_a^{(i)} + c\left(\delta t_{u,a} - \delta t_a{}^{(i)}\right) + c\nabla\tau_s^{(i)} - c\delta t_{adv\_ctrl}^{(i)} \\ &= \rho_a^{(i)} + c\nabla\tau_s^{(i)} - c\delta t_{adv\_ctrl}^{(i)}\end{aligned} . \tag{12}$$

Assuming that $\nabla\tau_{proc}^{(i)}$ is the same for all satellites, the superscript of $\nabla\tau_{proc}^{(i)}$ will thus be omitted thereafter. In $\nabla\tau_s^{(i)}$, both the transmission delay, $r_{s\to u}/c$, and the signal processing time, $\nabla\tau_{proc}$, will be estimated as the clock offset. Finally, we obtain

$$\rho_s^{(i)} = \rho_a^{(i)} + \underbrace{c\nabla\tau_{proc} + r_{s\to u}}_{c\delta t'_{u,s}} + \underbrace{r_s^{(i)} - r_u^{(i)} + c\nabla\tau_{ctrl}^{(i)} - c\delta t_{adv\_ctrl}^{(i)}}_{c\tau_s'^{(i)}}, \tag{13}$$

where $\delta t'_{u,s}$ and $\tau_s'^{(i)}$ are the additional clock offset and signal delay introduced by the spoofing attacks. While $\nabla\tau_{proc}$ can be calibrated by the spoofer [26], $r_{s\to u}$, $r_s^{(i)}$ and $r_u^{(i)}$ should be calculated in real-time with the knowledge of the spoofer's and target receiver's locations. The spoofer adjusts $\nabla\tau_{ctrl}^{(i)}$ and $\delta t_{adv\_ctrl}^{(i)}$ to control the pseudorange measurements of the target receiver. The composite terms, $\delta t'_{u,s}$ and $\tau_s'^{(i)}$, are used to control the time and position solution of the target receiver, respectively.

For measurement-level spoofing simulation, we define the authentic and spoofed trajectory profiles as $\boldsymbol{tr}_a(t)$ and $\boldsymbol{tr}_s(t)$, respectively. The two trajectories satisfy

$$\boldsymbol{tr}_s(t) - \boldsymbol{tr}_a(t) = \begin{cases} \boldsymbol{s}(t), & t \geq t_{\text{Init}} \\ \boldsymbol{0}, & t < t_{\text{Init}} \end{cases}, \tag{14}$$

where $\boldsymbol{s}(t)$ is the desired spoofing profile which can be further defined as $\boldsymbol{s}(t) = \boldsymbol{\alpha}(t) + \boldsymbol{b}$. The term $\boldsymbol{\alpha}(t)$ can be any time-related function and $\boldsymbol{b}$ is a constant vector. With $\boldsymbol{\alpha}(t_{\text{Init}}) = \boldsymbol{0}$ and $\boldsymbol{b} = \boldsymbol{0}$, synchronized spoofing attacks can be simulated. As a good start, $\boldsymbol{\alpha}(t)$ can be a simple ramp function similar to integrity analysis in the GNSS community. For unsynchronized spoofing, the term $\boldsymbol{b}$ is used to represent the jumps introduced to the authentic GNSS solutions. There are two ways to achieve the measurement level spoofing attack simulation:

- When $\boldsymbol{s}(t)$ is determined, the components $\delta t'_{u,s}$ and $\tau_s'^{(i)}$ in Equation (13) can be calculated accordingly. They are added to the authentic measurements generated based on $\boldsymbol{tr}_a(t)$ to construct the spoofed measurements. In this way, the critical parameters of the spoofer can also be simulated.
- If we only focus on the INS/GNSS integrated navigation system, a simpler method can be used without direct calculation of $\delta t'_{u,s}$ and $\tau_s'^{(i)}$. This is done by directly feeding $\boldsymbol{tr}_a(t)$ and $\boldsymbol{tr}_s(t)$ to the GNSS measurement-level simulator as two independent trajectories. A switch from $\boldsymbol{tr}_a(t)$ to $\boldsymbol{tr}_s(t)$ during the simulation can easily introduce the spoofed measurements to the integrated navigation system.

4. Impact Assessment and Recommendations

4.1. Error Covariance

The diagonal elements of the Kalman filter error covariance matrix, $\boldsymbol{P}_k$, represent the error variance of each state estimation when the filter is properly modeled. They are often used to evaluate the

performance of the integrated navigation system. In face of GNSS spoofing attacks, there is a necessity to analyze its impacts on the Kalman filter $\boldsymbol{P}_k$ calculation.

A standard Kalman filter implementation is given in Figure 2 with spoofing attacks introduced. GNSS spoofing attacks are injected directly into the state filtering loop by adding a spoofing profile to z_k. For a typical spoofing attack, a positioning error of several tens of meters to several kilometers is sufficient to cause serious problem for safety critical applications. It should be noted that, in order to analyze the effects solely caused by the spoofing attacks, the system dynamic/measurement model (including the associated model parameters such as the process noise covariance matrix, $\boldsymbol{Q}_k$ and the measurement noise covariance matrix, $\boldsymbol{R}_k$) and the filter initialization process, are assumed to be exactly the same under spoofed and authentic conditions in the impact assessment analysis. This ensures that all the other factors that may influence the Kalman filter's performance are excluded.

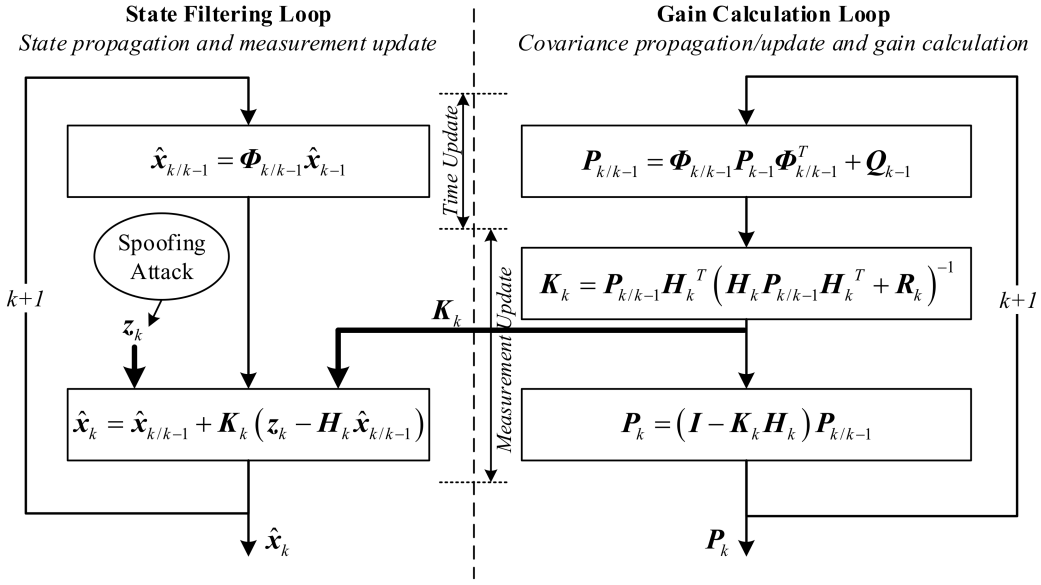

Figure 2. Standard Kalman filter implementation with spoofing attacks introduced.

As shown in Figure 2, the only link between the state filtering loop (left) and the gain calculation loop (right) is the Kalman filter gain matrix, $\boldsymbol{K}_k$. Intuitively, this is a one-way connection which means that the left loop is affected by the right but not vice versa. For linearized Kalman filter implementation, in which the system equation is linearized along the predefined reference trajectory, the gain calculation loop (which can be done off-line) is completely independent to the state filtering loop. For the more commonly used extended Kalman filter, there is a minor difference between the open-loop feedforward and closed-loop feedback mechanisms. If the feedforward integration is used, in which only the outputs of the integrated navigation system are corrected, the pure INS-based reference trajectory remains unaffected, and thus, the state filtering loop is also completely independent of the gain calculation loop. However, for the feedback integration, the error states estimated by the Kalman filter are used to correct the velocity, position, attitude, and inertial sensor measurements of the inertial navigation system, which means that the reference trajectory is corrected and updated periodically, and thus, the state filtering loop will affect the gain calculation loop through the calculation of $\boldsymbol{\Phi}_{k/k-1}$. However, the changes in position induced by typical spoofing attacks do not significantly influence the $\boldsymbol{\Phi}_{k/k-1}$ calculation. A simple and intuitional numerical demonstration is given in Appendix C, in which an assumption of a 5 km position error is introduced to each of the three dimensions. The maximum relative change of each element of $\boldsymbol{\Phi}_{k/k-1}$ is less than 2.5%. This is because a position change of several kilometers is only a small perturbation compared to the earth radius for the $\boldsymbol{\Phi}_{k/k-1}$ calculation, as

shown in Appendix A. Generally speaking, the gain calculation loop is weakly correlated with the state filtering loop.

As explained above, the spoofing profile introduced to the state filtering loop will have little impact on the $\boldsymbol{\Phi}_{k/k-1}$ calculation, so $\boldsymbol{P}_k$ will basically remain unchanged under the assumption that the other terms ($\boldsymbol{Q}_k$, $\boldsymbol{R}_k$, $\boldsymbol{H}_k$) and the filter initialization are exactly the same under spoofed and authentic conditions. This can be verified from the simulations in Section 5. In other words, $\boldsymbol{P}_k$ can no longer reflect the filter's performance under spoofing attacks. The basic premise of using $\boldsymbol{P}_k$ for performance evaluation is proper modeling of both system dynamics and observations. Under spoofing attacks, the measurement model is considered to be incorrect, because the spoofing profile is not modeled and the constant $\boldsymbol{R}_k$ cannot reflect the error of the spoofed GNSS measurements. The measurement model used under authentic conditions is no longer valid when the spoofing attacks are introduced. This is the main reason why $\boldsymbol{P}_k$ is unreliable and cannot reflect the filter's performance under spoofing attacks. Therefore, $\boldsymbol{P}_k$ should be used cautiously to evaluate the navigation performance, taking spoofing attacks into account.

In civil aviation, the commonly used integrity monitoring algorithms, Honeywell Inertial GPS Hybrid (HIGH) and Autonomous Integrity Monitored Extrapolation (AIME), calculate the horizontal protection level based on $\boldsymbol{P}_k$ [27]. Under GNSS spoofing attacks, if the spoofed signals are not detected and removed in time, the horizontal protection level derived from $\boldsymbol{P}_k$ is unreliable, which may cause potential integrity risk. Here, we recommend that the integrity algorithm designers reconsider and evaluate the integrity monitoring methods that rely on or relate to $\boldsymbol{P}_k$, with spoofing attacks taken into consideration.

4.2. Kalman Filter Innovation

The Kalman filter innovations are often used to construct the fault detection statistics for INS/GNSS integrated navigation systems. It is necessary to analyze the effects of spoofing attacks on the Kalman filter innovations to gain a better understanding about spoofing detection methods that are based on them. The discrete system dynamics and measurement model can be written as [22].

$$\boldsymbol{x}_k = \boldsymbol{\Phi}_{k/k-1}\boldsymbol{x}_{k-1} + \boldsymbol{W}_{k-1}, \tag{15}$$

$$\boldsymbol{z}_k = \boldsymbol{H}_k\boldsymbol{x}_k + \boldsymbol{V}_k. \tag{16}$$

The Kalman filter time and measurement update process are implemented in accordance with Figure 2. The Kalman filter innovation, $\boldsymbol{v}_k$, is defined as [28]

$$\boldsymbol{v}_k = \boldsymbol{z}_k - \boldsymbol{H}_k\hat{\boldsymbol{x}}_{k/k-1}. \tag{17}$$

Under normal conditions, when the filter approaches a steady state, the innovation has zero expectation and known covariance [28], that is

$$E(\boldsymbol{v}_k) = \boldsymbol{0}, \tag{18}$$

$$\boldsymbol{P}_{v_k} = \boldsymbol{H}_k\boldsymbol{P}_{k/k-1}\boldsymbol{H}_k^T + \boldsymbol{R}_k. \tag{19}$$

The test statistic of a Chi-squared test for fault detection in the INS/GNSS integrated navigation system at epoch k has the simplest form as [22]

$$\beta_k = \boldsymbol{v}_k^T\boldsymbol{P}_{v_k}^{-1}\boldsymbol{v}_k. \tag{20}$$

If there is no failure, the test statistic obeys a central Chi-squared distribution with m degrees, where m is the dimension of the measurement vector. The detection threshold is determined given a constant false alarm rate based on the Chi-squared distribution. The Kalman filter innovations can be

used to construct a variety of test statistics, and Equation (20) gives the simplest and most commonly used one. The mean of the innovations can be tested and the innovations within a time window can be accumulated or averaged to build different forms of Chi-squared tests [19,23,29].

GNSS spoofing detection is a complex fault detection problem, in which the spoofing attacks can be modeled as drifts or abrupt changes in the sensor measurements. Change in the expectation of the innovation sequence under a drift fault has been investigated in the pressure sensor drift detection problem of a nuclear power plant [30]. Here, we generally follow the derivation given in [30] but extend the fault profile from a simple ramp manner with a fixed rate to a general spoofing attack vector to clearly show the statistical property of the innovation sequence under spoofing attacks. Assume that the spoofing vector, $\boldsymbol{S}_n$ (n = 0, 1, 2, 3 . . .), is introduced from t_{Init}. For simplicity, we use the new subscript, n, to represent the time epoch in a spoofing attack. Now the measurement model becomes

$$\boldsymbol{z}_{n,s} = \boldsymbol{H}_n\boldsymbol{x}_n + \boldsymbol{V}_n + \boldsymbol{S}_n. \tag{21}$$

The Kalman filter innovation under spoofing attacks turns to

$$\begin{aligned} \boldsymbol{v}_{n,s} &= \boldsymbol{z}_{n,s} - \boldsymbol{H}_n\hat{\boldsymbol{x}}_{n/n-1} \\ &= \boldsymbol{H}_n\boldsymbol{x}_n + \boldsymbol{V}_n + \boldsymbol{S}_n - \boldsymbol{H}_n\hat{\boldsymbol{x}}_{n/n-1} \\ &= \boldsymbol{H}_n(\boldsymbol{x}_n - \hat{\boldsymbol{x}}_{n/n-1}) + \boldsymbol{V}_n + \boldsymbol{S}_n \end{aligned}. \tag{22}$$

Define the one-step prediction error at time n as

$$\breve{\boldsymbol{x}}_n = \boldsymbol{x}_n - \hat{\boldsymbol{x}}_{n/n-1}. \tag{23}$$

Then, the expectation of the innovation under spoofing attacks is

$$E(\boldsymbol{v}_{n,s}) = \boldsymbol{H}_n E\left(\breve{\boldsymbol{x}}_n\right) + \boldsymbol{S}_n. \tag{24}$$

The measurement update equation can be rewritten as

$$\hat{\boldsymbol{x}}_n = \hat{\boldsymbol{x}}_{n/n-1} + \boldsymbol{K}_n\boldsymbol{H}_n(\boldsymbol{x}_n - \hat{\boldsymbol{x}}_{n/n-1}) + \boldsymbol{K}_n(\boldsymbol{V}_n + \boldsymbol{S}_n). \tag{25}$$

Multiply both sides of Equation (25) by the state transition matrix $\boldsymbol{\Phi}_{n+1/n}$ to get

$$\hat{\boldsymbol{x}}_{n+1/n} = \boldsymbol{\Phi}_{n+1/n}(\boldsymbol{I} - \boldsymbol{K}_n\boldsymbol{H}_n)\hat{\boldsymbol{x}}_{n/n-1} + \boldsymbol{\Phi}_{n+1/n}\boldsymbol{K}_n\boldsymbol{H}_n\boldsymbol{x}_n + \boldsymbol{\Phi}_{n+1/n}\boldsymbol{K}_n(\boldsymbol{V}_n + \boldsymbol{S}_n). \tag{26}$$

Define

$$\boldsymbol{\Psi}_n = \boldsymbol{\Phi}_{n+1/n}(\boldsymbol{I} - \boldsymbol{K}_n\boldsymbol{H}_n). \tag{27}$$

Then,

$$\hat{\boldsymbol{x}}_{n+1/n} = \boldsymbol{\Psi}_n\hat{\boldsymbol{x}}_{n/n-1} + \boldsymbol{\Phi}_{n+1/n}\boldsymbol{K}_n\boldsymbol{H}_n\boldsymbol{x}_n + \boldsymbol{\Phi}_{n+1/n}\boldsymbol{K}_n(\boldsymbol{V}_n + \boldsymbol{S}_n). \tag{28}$$

Based on the system dynamic model,

$$\boldsymbol{x}_{n+1} = \boldsymbol{\Phi}_{n+1/n}\boldsymbol{x}_n + \boldsymbol{W}_n. \tag{29}$$

We obtain the one-step prediction error at time n + 1 by subtracting Equation (28) from (29):

$$\breve{\boldsymbol{x}}_{n+1} = \boldsymbol{\Psi}_n\breve{\boldsymbol{x}}_n - \boldsymbol{\Phi}_{n+1/n}\boldsymbol{K}_n(\boldsymbol{V}_n + \boldsymbol{S}_n) + \boldsymbol{W}_n. \tag{30}$$

Then, the expectation of $\breve{\boldsymbol{x}}_{n+1}$ is

$$E\left(\breve{\boldsymbol{x}}_{n+1}\right) = \boldsymbol{\Psi}_n E\left(\breve{\boldsymbol{x}}_n\right) - \boldsymbol{\Phi}_{n+1/n}\boldsymbol{K}_n\boldsymbol{S}_n. \tag{31}$$

Given a fault free initial condition, $E\left(\breve{\boldsymbol{x}}_0\right) = 0$, the expectation of $\breve{\boldsymbol{x}}_n$ can be obtained from

$$E\left(\breve{\boldsymbol{x}}_n\right) = -\sum_{i=0}^{n-1} \boldsymbol{\Lambda}_{n-1,i} \boldsymbol{\Phi}_{i+1/i} \boldsymbol{K}_i \boldsymbol{S}_i, \tag{32}$$

where

$$\boldsymbol{\Lambda}_{n,i} = \begin{cases} \prod_{j=0}^{n-1-i} \boldsymbol{\Psi}_{n-j}, & n > i \\ \boldsymbol{I}, & n = i \end{cases}. \tag{33}$$

Finally, we obtain the analytical expectation of the Kalman filter innovation under spoofing attacks:

$$E(\boldsymbol{v}_{n,s}) = \boldsymbol{S}_n - \boldsymbol{H}_n \sum_{i=0}^{n-1} \boldsymbol{\Lambda}_{n-1,i} \boldsymbol{\Phi}_{i+1/i} \boldsymbol{K}_i \boldsymbol{S}_i. \tag{34}$$

From Equation (34), it is obvious that the spoofing profile at the current epoch has a direct effect on the expectation of the current innovation, while the spoofing profile history has indirect, but accumulated, impacts. If the spoofing profile of each epoch is known, Equation (34) can be solved recursively. As the expectation of the innovation changes under spoofing attacks, carrying out a statistical test directly on the mean of the innovation is a simple and straightforward spoofing detection method. For the error covariance of the innovation, if the spoofing vector does not include additional measurement noise, the error covariance will remain the same as that defined in Equation (19), that is

$$\boldsymbol{P}_{v_{n,s}} = \boldsymbol{H}_n \boldsymbol{P}_{n/n-1} \boldsymbol{H}_n^T + \boldsymbol{R}_n. \tag{35}$$

Meanwhile, the test statistic in Equation (20) does not obey a central Chi-squared distribution anymore, but changes to a non-central Chi-squared distribution with the non-centrality parameter calculated with [19,21]

$$q_n = E(\boldsymbol{v}_{n,s})^T \boldsymbol{P}_{v_{n,s}}^{-1} E(\boldsymbol{v}_{n,s}). \tag{36}$$

The change in the statistical property of the innovations under spoofing attacks leads to a series of innovation-based spoofing detection methods. Furthermore, Tanil [19,21] established a novel, worst-case spoofing profile aimed at maximizing the position error without being detected, based on a similar expression of Equation (34) with slightly different derivations. The worst-case spoofing profile was used instead of the typical ramp and step fault profile that is commonly seen in the GNSS community to evaluate the spoofing detection performance. A linearized Kalman filter implementation was used in [19,21], in which a predefined and known nominal trajectory greatly simplified the spoofing detection and evaluation problem. However, the application of the linearized Kalman filter for INS/GNSS integration is limited to very certain type of applications, like the precision approach, orbiting satellites or interplanetary travel. For the more commonly used extended Kalman filter integration without a predefined reference trajectory, with linearization carried out along the real-time estimation, the spoofing profile is tightly coupled with the Kalman filter real-time estimation, so the worst-case spoofing profile derivation is not applicable. For the general INS/GNSS integration navigation system, typical ramp and step fault profiles (corresponding to synchronized and unsynchronized spoofing attacks) are used in this paper for the simulation analysis. The existence and derivation of a more advanced or, so-called, worst-case spoofing profile that maximizes the integrity risk still needs further effort. The analytical expression derived here could serve as a basis for further investigations.

4.3. Inertial Sensor Bias Estimation

In addition to introducing errors in the position and velocity solutions, the spoofing attacks also affect the estimation of inertial sensor biases. Following the derivation in Section 4.2, as we

have already obtained the expectation of the one-step prediction error, $\breve{\boldsymbol{x}}_n$, and the expectation of the innovation, $\boldsymbol{v}_{n,s}$, we can further obtain the expectation of the inertial sensor bias estimation error under spoofing attacks using the following derivation.

First, define the state estimation error at time n as

$$\widetilde{\boldsymbol{x}}_n = \boldsymbol{x}_n - \hat{\boldsymbol{x}}_n. \tag{37}$$

The relationship of the state estimation error, $\widetilde{\boldsymbol{x}}_n$, and the one-step prediction error, $\breve{\boldsymbol{x}}_n$, can be obtained by combining Equation (37) and Equation (23). Then, we get

$$\widetilde{\boldsymbol{x}}_n = \breve{\boldsymbol{x}}_n - (\hat{\boldsymbol{x}}_n - \hat{\boldsymbol{x}}_{n/n-1}). \tag{38}$$

The state estimation is given by

$$\hat{\boldsymbol{x}}_n = \hat{\boldsymbol{x}}_{n/n-1} + \boldsymbol{K}_n(\boldsymbol{z}_{n,s} - \boldsymbol{H}_n\hat{\boldsymbol{x}}_{n/n-1}) = \hat{\boldsymbol{x}}_{n/n-1} + \boldsymbol{K}_n\boldsymbol{v}_{n,s}. \tag{39}$$

Substituting Equation (39) into Equation (38), we get

$$\widetilde{\boldsymbol{x}}_n = \breve{\boldsymbol{x}}_n - \boldsymbol{K}_n\boldsymbol{v}_{n,s}. \tag{40}$$

As the expectations of $\breve{\boldsymbol{x}}_n$ and $\boldsymbol{v}_{n,s}$ have already been given in Equations (32) and (34), respectively, the expectation of the state estimation error can be obtained with

$$\begin{aligned} E(\widetilde{\boldsymbol{x}}_n) &= E\left(\breve{\boldsymbol{x}}_n\right) - \boldsymbol{K}_n E(\boldsymbol{v}_{n,s}) \\ &= (\boldsymbol{K}_n\boldsymbol{H}_n - \boldsymbol{I}) \sum_{i=0}^{n-1} \boldsymbol{\Lambda}_{n-1,i}\boldsymbol{\Phi}_{i+1/i}\boldsymbol{K}_i\boldsymbol{S}_i - \boldsymbol{K}_n\boldsymbol{S}_n \end{aligned}, \tag{41}$$

where the term, $\boldsymbol{\Lambda}_{n,i}$, has been defined in Equation (33). Recall that the definition of the state vector is $\boldsymbol{x}(t) = \begin{bmatrix} \boldsymbol{\phi}^T & (\delta\boldsymbol{v}^n)^T & (\delta\boldsymbol{v})^T & (\boldsymbol{\varepsilon}^b)^T & (\nabla^b)^T \end{bmatrix}^T$; the last six elements of $E(\widetilde{\boldsymbol{x}}_n)$ give the expectation of the error of inertial sensor bias estimation. As with the explanation given under Equation (34), the inertial sensor bias estimation is affected by the spoofing profile in an accumulated way. If the spoofing profile of each epoch is exactly known, Equation (41) can be solved. However, as we pointed out at the end of Section 4.2, when the extended Kalman filter is used, the spoofing vector will be tightly coupled with the real-time state estimation, which makes it difficult to build a quantitative relationship between a given spoofing profile and its impacts on the inertial sensor bias estimation without a full simulation analysis. We use a simple analytical demonstration below to give a qualitative analysis here. A simulation is given in Section 5 for more intuitional and quantitative demonstration.

As a common way to demonstrate and analyze the error propagation, we consider a simple static situation of the north channel for qualitative analysis of spoofing impacts on the inertial sensor bias estimation. The north position, north velocity and east misalignment angle error equation can be simplified with Equations (42)–(44), respectively [31].

$$\delta\dot{r}_N = \delta v_N, \tag{42}$$

$$\delta\dot{v}_N = g\phi_E + \nabla_N, \tag{43}$$

$$\dot{\phi}_E = -\delta v_N/R + \varepsilon_E, \tag{44}$$

where δr_N, δv_N and ϕ_E are the north position error, north velocity error and east misalignment angle, respectively. ∇_N and ε_E represent the north accelerometer bias and the east gyro bias, respectively. g and R represent the gravity and the earth radius, respectively. Assuming that the spoofer introduces a north position or velocity error, as shown in Equation (43), both the east misalignment angle and north accelerometer bias will be affected. Furthermore, when the east misalignment angle is influenced, the

east gyro bias is affected through Equation (44). Generally speaking, a spoofing attack on the north will introduce estimation errors on the north accelerometer bias, east gyro bias, and east misalignment angle. Note that the above analysis only serves as a simple demonstration. The impacts will be much more complicated due to cross coupling of different errors in dynamic situations.

As the gyro and accelerometer bias estimations are affected by the spoofing attacks, spoofing attacks may be detected by monitoring the bias estimation of the inertial sensors from the Kalman filter. This can be done by directly setting upper and lower bounds on the estimated biases. Based on the authors' experience, the threshold should be set at least three to five times larger than a nominal value provided by the manufacturer. This method is generally conservative, and the user should take the risk that the inertial sensors suffer from performance degradation for other reasons rather than spoofing attacks.

After successful detection of the spoofing attacks, the integrated navigation filter should discard the GNSS solutions if spoofed signals are not removed in time. The navigation filter will output a pure INS solution instead. Conventionally, the estimated inertial sensor biases are used to compensate the raw gyro and accelerometer measurements in the pure INS solution when GNSS measurements are not available for jamming or blockage. In the spoofing scenario, however, the estimated inertial sensor biases are no longer reliable and should not be used. Meanwhile, the spoofing attacks can also affect the misalignment angle estimation, as illustrated above, which also leads to large, pure INS errors. To mitigate the spoofing impacts, the backtracking mechanism, which records the raw IMU measurements in a time window and starts the pure INS solution from a backward time, is recommended after successful spoofing detection. This mechanism has been applied to the initial alignment [32] and can be transferred to spoofing mitigation with minor modifications.

5. Simulation Analysis

To verify our analyses, we carried out a series of simulations based on the proposed measurement-level trajectory spoofing simulator presented in Section 3.2. We directly fed the spoofing and authentic trajectories to the GNSS measurement-level simulator and switched from authentic to spoofing trajectories during the simulation to introduce the designed spoofing attacks. A GNSS positioning engine was implemented separately into the simulation, with spoofed pseudoranges as inputs and position solutions as outputs for the loosely coupled integration. A flight trajectory lasting 1100 s near Xi'an, China was simulated as the authentic trajectory. The simulated position profiles are given in Figure 3. The parameters of the Kalman filter used in the simulation are listed in Appendix D.

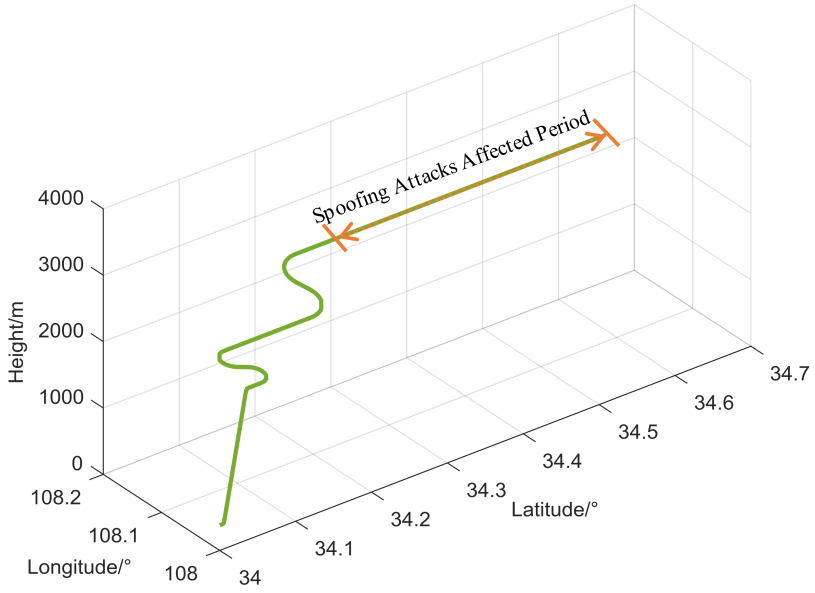

Figure 3. Simulated flight trajectory.

We introduced the spoofing attacks (in the longitude channel in all cases) in the straight-and-level flight period, starting at 800 s; the total period of spoofing was 300 s. For the GNSS simulation, we used the baseline 24-slot GPS constellation at an epoch of 00:00:00 on 1 July 1993 [33], which is also recommended in the RTCA/DO-229 MOPS for INS/GPS system evaluation. The aviation-grade INS and single-frequency GPS receiver were adopted in the simulation with the specifications listed in Table 1. All the following simulations were carried out under the same dynamic scenario as described above.

Table 1. Inertial measurement unit (IMU) and GPS specifications [23].

Sensor	Parameter	Value	Unit
IMU	Gyro bias	0.01	$^\circ$/h
	Gyro random walk	0.005	$^\circ/\sqrt{\text{h}}$
	Accelerometer bias	100	μg
	Accelerometer random walk	20	$\mu\text{g}/\sqrt{\text{Hz}}$
GPS	Residual satellite clock and ephemeris errors	0.5	m
	Residual ionosphere error (single-frequency)	4.0	m
	Residual troposphere error	0.2	m
	Tracking noise	0.67	m
	Short-range multipath error	0.94	m

Note: all the specifications are root mean square (RMS) values.

Figure 4 gives the comparison between the covariance matrix-indicated position errors and true position errors in the longitude channel for both authentic and spoofed scenarios. No matter whether the spoofer introduced a small ramp spoofing profile (0.3 m/s, leads to 90 m longitude error) or a fairly larger one (12.4 m/s, leads to about 2 nautical miles longitude error), the error covariance matrix ($\boldsymbol{P}_k$)-indicated error bounds remained the same as the authentic signal, while the actual position errors obviously grew out of the error bounds.

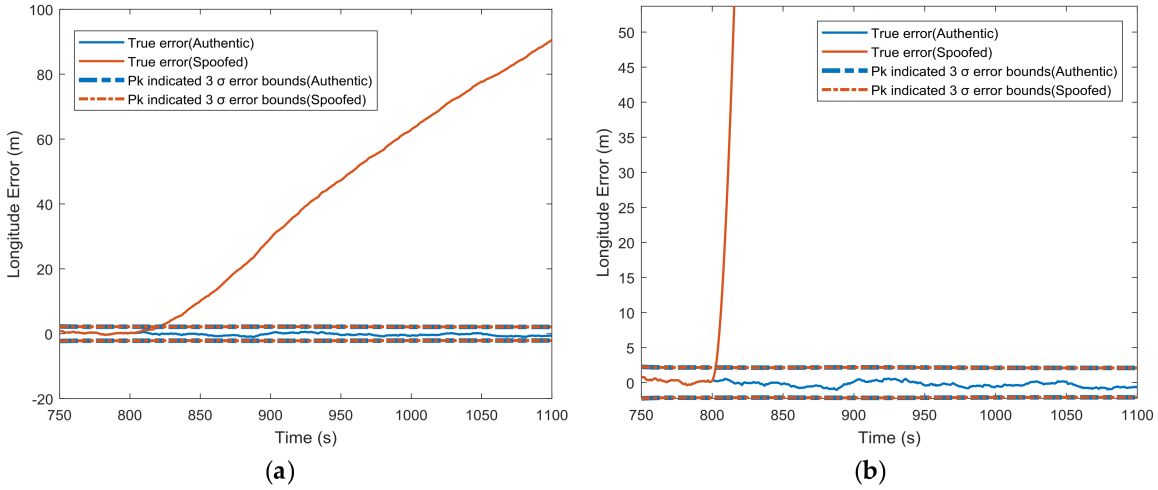

Figure 4. Error covariance matrix ($\boldsymbol{P}_k$)-indicated and true position errors under normal conditions and (**a**) 0.3 m/s synchronized spoofing attack; (**b**) 12.4 m/s synchronized spoofing attack.

We further compared each diagonal element of $\boldsymbol{P}_k$ under spoofed and authentic conditions for all of the estimated states in the scenario shown in Figure 4b at t = 1100 s, when about 2 nautical miles longitude error had been introduced. The absolute change in the square root of each diagonal element of $\boldsymbol{P}_k$ was defined as

$$\Delta sqrtPk = \left| \sqrt{P_{k,s(i,i)}} - \sqrt{P_{k,a(i,i)}} \right|, \tag{45}$$

where the subscripts, s and a, represent the spoofed and authentic conditions, respectively. i = 1, 2, 3, . . . , 15 represents the index of the diagonal element of $\boldsymbol{P}_k$. The relative change was defined as

$$\delta sqrtPk = \frac{\Delta sqrtPk}{\sqrt{P_{k,a(i,i)}}}. \tag{46}$$

Both the absolute change and relative change are given in Table 2, which clearly shows that the changes in $\boldsymbol{P}_k$-indicated state estimation errors were nearly negligible. This verifies that spoofing attacks injected into the state filtering loop have little impact on Kalman filter error covariance calculation. Using $\boldsymbol{P}_k$ to evaluate the integrated navigation system's performance and for integrity monitoring is unreliable under spoofing attacks.

Table 2. The absolute and relative change of the square root of each diagonal element of $\boldsymbol{P}_k$.

State	Absolute (Relative)	State	Absolute (Relative)	State	Absolute (Relative)
ϕ	3.43×10^{-6}° (0.20%)	ϕ_N	4.40×10^{-6}° (0.26%)	ϕ_U	1.06×10^{-5}° (0.19%)
δv_E^n	1.52×10^{-6} m/s (0.01%)	δv_N^n	1.96×10^{-5} m/s (0.14%)	δv_U^n	8.63×10^{-7} m/s (0.02%)
δL	3.69×10^{-4} m (0.05%)	$\delta\lambda$	1.02×10^{-5} m (0.002%)	δH	2.87×10^{-5} m (0.004%)
ε_R^b	1.59×10^{-5} °/h (0.11%)	ε_F^b	2.52×10^{-5} °/h (0.18%)	ε_U^b	7.72×10^{-6} °/h (0.03%)
∇_R^b	6.33×10^{-2} µg (0.29%)	∇_F^b	7.17×10^{-2} µg (0.35%)	∇_U^b	1.14×10^{-3} µg (0.07%)

Note: absolute and relative represent the absolute change, $\Delta sqrtPk$, as defined in Equation (45), and relative change,$\delta sqrtPk$, as defined in Equation (46), respectively.

Figure 5a shows the three dimensional innovations under a 0.5 m/s spoofing attack. The abnormal innovations were found only in the longitude channel, because the spoofing attacks introduce only longitudinal errors. Separately, tests on the mean of each component of the innovation vector have the potential to detect and distinguish which component is affected. In Figure 5b, the longitude channel innovations are given for different spoofing profiles, which shows that it may be easier to detect spoofing attacks with larger fault ramps. Also, there is only a limited spoofing detection window [34], as the Kalman filter dynamically tunes itself to track the spoofing profiles, and the means of innovations will approach to zero again in a new steady state. In addition to testing the means of innovations, the other innovation-based tests, like the snapshot Chi-squared test [22,23] or averaged/summed innovation test [19,23,29], can also be used.

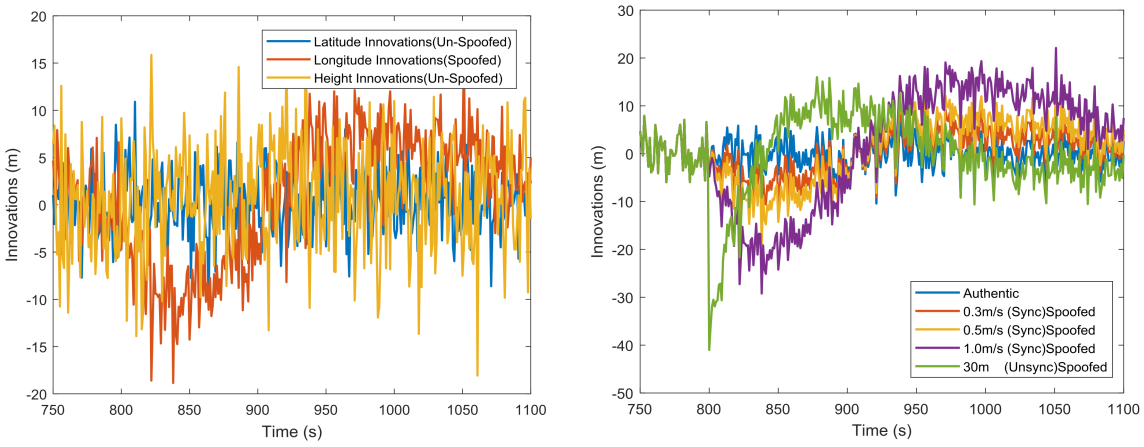

Figure 5. (**a**) Three dimensional Kalman filter innovations; (**b**) longitude channel Kalman filter innovations. (Sync) is short for synchronized and (Unsycn) is short for unsynchronized.

The impacts of spoofing attacks on the inertial sensor bias and misalignment angle estimation are illustrated in Figure 6a. Taking the gyro bias estimation as an example, the Kalman filter gives an estimation of the *y*-axis gyro bias of over 0.3 °/h under a 1 m/s synchronized spoofing attack, far beyond the 0.01 °/h specification. This gives an obvious sign that abnormal GPS measurements exist. Assuming that the spoofing attack is detected at 825 s, and the GPS measurements in the integrated system are directly disconnected, the horizontal error of pure INS grows quickly to about 150 m, as shown in Figure 6b. When the backtracking mechanism given in [32] (with 50 s backtracking) was used, the unaffected inertial sensor bias and misalignment angle estimation contributed to a better pure INS solution performance with position errors about 90 m. This shows the potential benefits of the backtracking mechanism for spoofing mitigation.

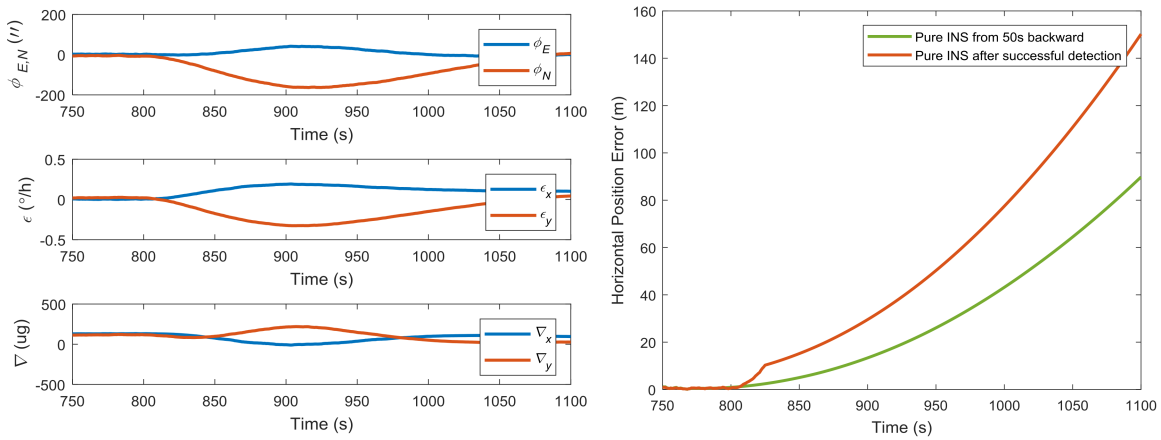

Figure 6. (**a**) Inertial sensor bias estimation and misalignment angle under a 1 m/s synchronized spoofing attack; (**b**) horizontal position accuracy comparison between two pure INS modes.

6. Conclusions and Future Works

Understanding the behavior of INS/GNSS integrated navigation systems under spoofing attacks is crucial to allow the development of effective spoofing detection and mitigation methods. In this paper, we analyzed the spoofing impacts with a focus on the Kalman filter of the integrated navigation system. Through theoretical analysis and simulations, we came to the conclusion that (1) Kalman filter state error covariance is not affected by spoofing attacks and thus, should be reconsidered for performance evaluation and integrity monitoring; (2) the statistical properties of innovations have changed, which leads to several potential statistical tests for spoofing detection; (3) the estimated inertial sensor biases are no longer reliable under spoofing attacks, which makes bias estimation range check and the backtracking mechanism promising for spoofing detection and mitigation.

What we touched on in this paper is only the tip of the iceberg; this paper opens many research opportunities for the integrated navigation community, taking spoofing attacks into consideration. Simulations in this paper give an intuitional view of the possibility of innovation-based and inertial sensor bias monitoring methods for spoofing detection. Detailed investigations of the recommended spoofing defenses with a comparison and maybe a combination of these defenses deserve further efforts.

Author Contributions: Conceptualization, Y.L.; Methodology, Y.L. and S.L.; Software, Y.L. and Q.F.; Validation, Y.L., Z.L.; Formal Analysis, Y.L. and S.L.; Investigation, Y.L.; Resources, Q.F. and Z.L.; Writing-Original Draft Preparation, Y.L.; Writing-Review & Editing, Y.L., S.L., Q.F. and Z.L.; Visualization, Y.L.; Supervision, S.L.

Acknowledgments: We would like to express our great appreciation to the anonymous reviewers for their careful reading of our manuscript and their insightful comments and suggestions.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A

The details of each component of the system matrix, $\boldsymbol{F}(t)$ can be written as

$$\boldsymbol{F}_{11} = (-(\boldsymbol{\omega}_{ie}^{n} + \boldsymbol{\omega}_{en}^{n})\times), \tag{A1}$$

$$\boldsymbol{F}_{12} == \begin{bmatrix} 0 & -1/R_{Mh} & 0 \\ 1/R_{Nh} & 0 & 0 \\ \tan L/R_{Nh} & 0 & 0 \end{bmatrix}, \tag{A2}$$

$$\boldsymbol{F}_{13} = \begin{bmatrix} 0 & 0 & v_N^n/R_{Mh}^2 \\ -\omega_{ie}\sin L & 0 & -v_E^n/R_{Nh}^2 \\ \omega_{ie}\cos L + v_E^n \sec^2 L/R_{Nh} & 0 & -v_E^n \tan L/R_{Nh}^2 \end{bmatrix}, \tag{A3}$$

$$\boldsymbol{F}_{21} = \left(\left(\boldsymbol{C}_b^n \boldsymbol{f}^b\right)\times\right), \tag{A4}$$

$$\boldsymbol{F}_{22} = (\boldsymbol{v}^n\times)\boldsymbol{F}_{12} - ((2\boldsymbol{\omega}_{ie}^{n} + \boldsymbol{\omega}_{en}^{n})\times), \tag{A5}$$

$$\boldsymbol{F}_{23} = (\boldsymbol{v}^n\times)\begin{bmatrix} 0 & 0 & v_N^n/R_{Mh}^2 \\ -2\omega_{ie}\sin L & 0 & -v_E^n/R_{Nh}^2 \\ 2\omega_{ie}\cos L + v_E^n \sec^2 L/R_{Nh} & 0 & -v_E^n \tan L/R_{Nh}^2 \end{bmatrix}, \tag{A6}$$

$$\boldsymbol{F}_{32} = \begin{bmatrix} 0 & 1/R_{Mh} & 0 \\ \sec L/R_{Nh} & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \tag{A7}$$

$$\boldsymbol{F}_{33} = \begin{bmatrix} 0 & 0 & -v_N^n/R_{Mh}^2 \\ v_E^n \sec L \tan L/R_{Nh} & 0 & -v_E^n \sec L/R_{Nh}^2 \\ 0 & 0 & 0 \end{bmatrix}, \tag{A8}$$

where

$(*)\times$ denotes the skew-symmetric matrix of the corresponding vector.

R_{Mh} and R_{Nh} are the meridian and transverse radii of the curvature plus the height.

$\boldsymbol{v}^n = \begin{bmatrix} v_E^n \\ v_N^n \\ v_U^n \end{bmatrix}$ is the navigation frame velocity vector, consisting of east, north, and up components.

L represents the latitude.

$\boldsymbol{C}_b^n$ is the 3-by-3 body frame to navigation frame rotation matrix, defined as

$$C_b^n = \begin{bmatrix} \cos\gamma\cos\psi + \sin\gamma\sin\psi\sin\theta & \sin\psi\cos\theta & \sin\gamma\cos\psi - \cos\gamma\sin\psi\sin\theta \\ -\cos\gamma\sin\psi + \sin\gamma\cos\psi\sin\theta & \cos\psi\cos\theta & -\sin\gamma\sin\psi - \cos\gamma\cos\psi\sin\ \theta \\ -\sin\gamma\cos\theta & \sin\theta & \cos\gamma\cos\theta \end{bmatrix}, \tag{A9}$$

where θ, γ, ψ represent the pitch, roll and yaw angle, respectively.

$\boldsymbol{f}^b = \begin{bmatrix} f_R^b \\ f_F^b \\ f_U^b \end{bmatrix}$ is the body frame specific force vector, consisting of right, forward and up components.

ω_{ie} is the constant earth rotation rate (=7.292115 $\times$ 10^{-5} rad/s).

$\boldsymbol{\omega}_{ie}^{n}$ is the earth rotation vector resolved into the local navigation frame, defined as

$$\boldsymbol{\omega}_{ie}^{n} = \begin{bmatrix} 0 \\ \omega_{ie}\cos L \\ \omega_{ie}\sin L \end{bmatrix}. \tag{A10}$$

$\boldsymbol{\omega}_{en}^{n}$ is the rotation vector of the navigation frame with respect to the earth-fixed-earth-centered frame represented in the local navigation frame, defined as

$$\boldsymbol{\omega}_{en}^{n} = \begin{bmatrix} -v_N^n / R_{Mh} \\ v_E^n / R_{Nh} \\ v_E^n \tan L / R_{Nh} \end{bmatrix}. \tag{A11}$$

Appendix B

Table A1. A comparison between unsynchronized and synchronized spoofing attacks.

	Parameters	Unsynchronized Spoofing	Synchronized Spoofing
Signal	Signal power	$P_s > P_a$	$P_s << P_a \rightarrow P_s > P_a$
	Signal delay	Arbitrarily determined for simulator attacks; generally, $\tau_s > \tau_a$ for meaconing attacks	$\tau_s \approx \tau_a$ in the transition process, then determined arbitrarily by the spoofer
	Doppler	Consistent with the spoofer's code phase variations	$f_{d,s} \approx f_{d,a}$ in the transition process, then varies consistently with the code phase
	Visible satellites	Generally, N_s equals N_a	
	Data sequence	Same structure as D_a the content can be changed	Same as D_a in the transition process, then the content can be changed
	Code sequence	Strictly the same as the authentic signals	
	Carrier frequency	Strictly the same as the authentic signals	
Measurement	Pseudorange	Arbitrarily determined	Matched with ρ_a in the transition process, then determined by the spoofer
	Carrier phase	Consistent with code phase, hard to align with the authentic signals	
PVT	Position	Arbitrarily determined	Matched with the authentic condition in the transition process, then determined arbitrarily by the spoofer
	Velocity	Consistent with position	
	Time	Arbitrarily determined for simulator attacks; generally earlier than true time for meaconing attacks	
Implementation	Platform	Repeater Simulator	Advanced repeater Receiver/spoofer
	Requirements	Jam-and-spoof	Know the real-time position of the target receiver

Appendix C

To give a simple and intuitional demonstration of the effect of introduced position error on the system state transition matrix $\boldsymbol{\Phi}$ calculation, we take a snapshot of the simulation scenario presented in Section 5. Under the authentic condition, at t = 1100 s, the snapshot system state is given as

- Position: $L = 34.6887^\circ$, $\lambda = 108.1915^\circ$, $H = 2282.8941$ m
- Velocity: $v_E^n = -0.0058$ m/s, $v_N^n = 149.9911$ m/s, $v_U^n = 0.0081$ m/s
- Attitude: $\theta = -0.0018^\circ$, $\gamma = 0.0017^\circ$, $\psi = 359.9941^\circ$
- Specific force: $f_R^b = -0.0128$ m/s^2, $f_F^b = -0.0016$ m/s^2, $f_U^b = 9.7900$ m/s^2
- Meridian radius of curvature plus height: R_{Mh} = 6,358,383 m
- Transverse radius of curvature plus height: R_{Nh} = 6,387,345 m

Assuming that 5 km position errors (denoted by δL, $\delta\lambda$ and δH) are directly added to the reference trajectory for all the three dimensions, elements of the state transition matrix, $\boldsymbol{\Phi}_{i,j}$ (element in the ith

row and *j*th column), are calculated before and after the introduction of position errors. Let $\boldsymbol{\Phi}_{i,j(a)}$ and $\boldsymbol{\Phi}_{i,j(s)}$ represent the element under authentic and spoofed conditions, respectively. The elements of $\delta\boldsymbol{\Phi}$, representing the relative change of $\boldsymbol{\Phi}$, are defined and calculated as

$$\delta\boldsymbol{\Phi}_{i,j} = \left| \frac{\boldsymbol{\Phi}_{i,j(s)} - \boldsymbol{\Phi}_{i,j(a)}}{\boldsymbol{\Phi}_{i,j(a)}} \right|, \tag{A12}$$

where $\delta\boldsymbol{\Phi}_{i,j}$ is the element in the *i*th row and *j*th column of $\delta\boldsymbol{\Phi}$. The first order solution, $\boldsymbol{I} + \boldsymbol{F}(t)T_s$, is used to compute the transition matrix, where $\boldsymbol{F}(t)$ is the system matrix, as defined in Equation (3) and Appendix A, and T_s is the propagation interval which equals 0.01 s in this demonstration. Here, take the calculation of $\boldsymbol{\Phi}_{8,4}$ as an example (corresponding to the term of $\sec L/R_{Nh}$ in Equation (A7)). The relative change of $\boldsymbol{\Phi}_{8,4}$ is calculated as

$$\delta\boldsymbol{\Phi}_{8,4} = \left| \frac{\boldsymbol{\Phi}_{8,4(s)} - \boldsymbol{\Phi}_{8,4(a)}}{\boldsymbol{\Phi}_{8,4(a)}} \right| = \left| \frac{(0 + \sec(L + \delta L)/(R_{Nh} + \delta H) \cdot T_s) - (0 + \sec L/R_{Nh} \cdot T_s)}{0 + \sec L/R_{Nh} \cdot T_s} \right|. \tag{A13}$$

Replacing all the terms with the known numerical values, we get

$$\delta\boldsymbol{\Phi}_{8,4} = \left| \frac{(0+\sec(0.6054+5000/6378137)/(6387345+5000)\cdot 0.01) - (0+\sec(0.6054)/6387345\cdot 0.01)}{0+\sec(0.6054)/6387345\cdot 0.01} \right| \approx 0.02\%, \tag{A14}$$

which shows that a very small amount of change has been introduced. All the elements of $\delta\boldsymbol{\Phi}$ are calculated in the same way. Finally, we get the relative change of $\boldsymbol{\Phi}$ in percentage form as

$$\delta\boldsymbol{\Phi}_{i=1:8,j=1:15} = \begin{bmatrix} – & 0.01 & 0.05 & – & 0.08 & – & – & – & 0.16 & – & 0.09 & 0.57 & – & – & – \\ 0.11 & – & 0.08 & 0.08 & – & – & 0.11 & – & 0.15 & 0.09 & – & 0.14 & – & – & – \\ 0.05 & 0.08 & – & 0.09 & – & – & 0.05 & – & 0.01 & 0.57 & 0.14 & – & – & – & – \\ – & – & 0.03 & – & 0.11 & 0.05 & 0.05 & – & 0.01 & – & – & – & – & 0.09 & 0.57 \\ – & – & 0.01 & 0.01 & – & 0.08 & 0.05 & – & 2.19^{**} & – & – & – & 0.09 & – & 0.14 \\ 0.03 & 0.01 & – & 0.05 & 0.08 & – & 0.12 & – & 0.16 & – & – & – & 0.57 & 0.14 & – \\ – & – & – & – & 0.08 & – & – & – & 0.16 & – & – & – & – & – & – \\ – & – & – & 0.02^{*} & – & – & 0.15 & – & 0.10 & – & – & – & – & – & – \end{bmatrix} \%. \tag{A15}$$

Note that only part of $\delta\boldsymbol{\Phi}$ is given; all the omitted elements and the elements denoted by "–" are not influenced by introduced position errors (elements with relative change $<1 \times 10^{-9}$ are also denoted by "–") .The superscripts, * and **, are used to indicate $\delta\boldsymbol{\Phi}_{8,4}$ for demonstration in Equation (A14) and $\delta\boldsymbol{\Phi}_{5,9}$ for the maximum relative change, respectively.

Appendix D

The parameters of the Kalman filter used in the simulation are listed here for reference:

$$\boldsymbol{P}_o = \mathrm{diag}([20'';20'';180'';\ 0.1\ \mathrm{m/s};\ 0.1\ \mathrm{m/s};\ 0.1\ \mathrm{m/s};\ 3.7\ \mathrm{m};\ 3.7\ \mathrm{m};6\mathrm{m};0.01^{\circ}/\mathrm{h};0.01^{\circ}/\mathrm{h};0.01^{\circ}/\mathrm{h};100\ \mu\mathrm{g};100\ \mu\mathrm{g};100\ \mu\mathrm{g}] \times 3)^2,$$

$$\boldsymbol{Q}_k = \mathrm{diag}\Big(\Big[0.005^{\circ}/\sqrt{\mathrm{h}};0.005^{\circ}/\sqrt{\mathrm{h}};0.005^{\circ}/\sqrt{\mathrm{h}};20\ \mu\mathrm{g}/\sqrt{\mathrm{Hz}};20\ \mu\mathrm{g}/\sqrt{\mathrm{Hz}};20\ \mu\mathrm{g}/\sqrt{\mathrm{Hz}};1\ \mathrm{m}/\sqrt{\mathrm{h}};1\ \mathrm{m}/\sqrt{\mathrm{h}};1\mathrm{m}/\sqrt{\mathrm{h}};\mathrm{zeros}(6,1)\Big]\Big)^2 \times Ts,$$

$$\boldsymbol{R}_k = \mathrm{diag}([3.7\mathrm{m};3.7\mathrm{m};6\mathrm{m}])^2,$$

$$\boldsymbol{x}_0 = \mathrm{zeros}(15,1).$$

Note that *Ts* = 0.01 s is the propagation interval in the simulation. The parameters are set according to IMU and GPS specifications, as listed in Table 1. The units given above are just for easy interpretation. They should be changed to SI in practical implementations.

References

1. John, A. Volpe National Transportation Systems Center. In *Vulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System*; John A. Volpe National Transportation Systems Center: Cambridge, MA, USA, 2001.
2. Psiaki, M.L.; Humphreys, T.E. GNSS Spoofing and Detection. *Proc. IEEE* **2016**, *104*, 1258–1270. [CrossRef]
3. Warner, J.S.; Johnston, R.G. GPS Spoofing Countermeasures. *J. Secur. Adm.* **2003**, *25*, 19–27.
4. Key, E.L. *Techniques to Counter GPS Spoofing*; The MITRE Corporation: Bedford, MA, USA, 1995.
5. Humphreys, T.E.; Ledvina, B.M.; Psiaki, M.L.; O'Hanlon, B.W.; Kintner, P.M., Jr. Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer. In Proceedings of the 21st ION GNSS International Technical Meeting of the Satellite Division (ION GNSS 2008), Savannah, GA, USA, 16–19 September 2008; pp. 2314–2325.
6. Huang, L.; Yang, Q. GPS Spoofing: Low-Cost GPS Simulator. Presented at DEF CON 23, Las Vegas, NV, USA, August 2015. Available online: https://www.researchgate.net/publication/286330869_Low-cost_GPS_simulator_-_GPS_spoofing_by_SDR (accessed on 4 May 2018).
7. Kerns, A.J.; Shepard, D.P.; Bhatti, J.A.; Humphreys, T.E. Unmanned Aircraft Capture and Control via GPS Spoofing. *J. Field Robot.* **2014**, *31*, 617–636. [CrossRef]
8. Bhatti, J.; Humphreys, T.E. Hostile Control of Ships via False GPS Signals: Demonstration and Detection. *Navig. J. Inst. Navig.* **2017**, *64*, 51–66. [CrossRef]
9. Wang, K.; Chen, S.; Pan, A. *Time and Position Spoofing with Open Source Projects*; Black Hat Europe: Amsterdam, The Netherlands, 2015; Available online: https://www.blackhat.com/docs/eu-15/materials/eu-15-Kang-Is-Your-Timespace-Safe-Time-And-Position-Spoofing-Opensourcely-wp.pdf (accessed on 16 April 2018).
10. Rothrock, K. The Kremlin Eats GPS for Breakfast: Why Geolocation in Central Moscow Has Become a Real Headache. Available online: https://themoscowtimes.com/articles/the-kremlin-eats-gps-for-breakfast-55823 (accessed on 20 March 2018).
11. Goward, D. Mass GPS Spoofing Attack in Black Sea? Available online: http://maritime-executive.com/editorials/mass-gps-spoofing-attack-in-black-sea (accessed on 20 March 2018).
12. Borio, D.; Gioia, C. A Sum-of-Squares Approach to GNSS Spoofing Detection. *IEEE Trans. Aerosp. Electron. Syst.* **2016**, *52*, 1756–1768. [CrossRef]
13. Günther, C. A Survey of Spoofing and Counter-Measures. *Navig. J. Inst. Navig.* **2014**, *61*, 159–177. [CrossRef]
14. Jafarnia-Jahromi, A.; Broumandan, A.; Nielsen, J.; Lachapelle, G. GPS Vulnerability to Spoofing Threats and a Review of Antispoofing Techniques. *Int. J. Navig. Obs.* **2012**, *2012*. [CrossRef]
15. Schmidt, D.; Radke, K.; Camtepe, S.; Foo, E.; Ren, M. A Survey and Analysis of the GNSS Spoofing Threat and Countermeasures. *ACM Comput. Surv.* **2016**, *48*. [CrossRef]
16. Dovis, F. *GNSS Interference Threats and Countermeasures*; Artech House: Norwood, MA, USA, 2015.
17. Liu, Y.; Li, S.; Xiao, X.; Fu, Q. INS-Aided GNSS Spoofing Detection Based on Two Antenna Raw Measurements. *Gyrosc. Navig.* **2016**, *7*, 178–188. [CrossRef]
18. Manickam, S.; O'Keefe, K. Using Tactical and MEMS Grade INS to Protect Against GNSS Spoofing in Automotive Applications. In Proceedings of the 29th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+ 2016), Portland, OR, USA, 12–16 September 2016; pp. 2291–3001.
19. Tanil, C.; Khanafseh, S.; Joerger, M.; Pervan, B. Kalman Filter-based INS Monitor to Detect GNSS Spoofers Capable of Tracking Aircraft Position. In Proceedings of the IEEE/ION PLANS 2016, Savannah, GA, USA, 11–14 April 2016; pp. 1027–1034.
20. Liu, Y.; Fu, Q.; Liu, Z.; Li, S. GNSS Spoofing Detection Ability of a Loosely Coupled INS/GNSS Integrated Navigation System for Two Integrity Monitoring Methods. In Proceedings of the 2017 International Technical Meeting of the Institute of Navigation, Monterey, CA, USA, 30 January–2 February 2017; pp. 912–921.
21. Tanil, C.; Khanafseh, S.; Joerger, M.; Pervan, B. An INS Monitor to Detect GNSS Spoofers Capable of Tracking Vehicle Position. *IEEE Trans. Aerosp. Electron. Syst.* **2018**, *54*, 131–143. [CrossRef]
22. Qin, Y.; Zhang, H.; Wang, S. *Principles of Kalman Filter and Integrated Navigation*; Northwestern Polytechnical University Press: Xi'an, China, 2015.
23. Groves, P.D. *Principles of GNSS, Inertial, and Multisensor Integrated Navigation Systems*, 2nd ed.; Artech House: Norwood, MA, USA, 2013.

24. Ioannides, R.T.; Pany, T.; Gibbons, G. Known Vulnerabilities of Global Navigation Satellite Systems, Status, and Potential Mitigation Techniques. *Proc. IEEE* **2016**, *104*, 1174–1194. [CrossRef]
25. Humphreys, T.E. Interference. In *Springer Handbook of Global Navigation Satellite Systems*; Teunissen, P.J.G., Montenbruck, O., Eds.; Springer International Publishing AG: Cham, Switzerland, 2017; pp. 469–503.
26. Humphreys, T.E.; Bhatti, J.A.; Shepard, D.P.; Wesson, K.D. *A Testbed for Developing and Evaluating GNSS Signal Authentication Techniques*; International Symposium on Certification of GNSS Systems & Services (CERGAL): Dresden, Germany, 2014; Available online: https://radionavlab.ae.utexas.edu/images/stories/files/papers/tb.pdf (accessed on 16 April 2018).
27. Lee, Y.C.; O'Laughlin, D.G. Performance Analysis of a Tightly Coupled GPS/Inertial System for Two Integrity Monitoring Methods. *Navig. J. Inst. Navig.* **2000**, *47*, 175–189. [CrossRef]
28. Grewal, M.S.; Andrews, A.P. *Kalman Filtering: Theory and Practice with MATLAB*, 4th ed.; John Wiley & Sons, Inc.: Hoboken, NJ, USA, 2015.
29. Zhong, L.; Liu, J.; Li, R.; Wang, R. Approach for Detecting Soft Faults in GPS/INS Integrated Navigation based on LS-SVM and AIME. *J. Navig.* **2017**, *70*, 561–579. [CrossRef]
30. Cho, S. A Study for Detection of Drift in Sensor Measurements. Ph.D. Thesis, The University of Western Ontario, London, ON, Canada, 2012.
31. Gao, Z. *Inertial Navigation System Technology*; Tsinghua University Press: Beijing, China, 2012.
32. Li, W.; Wu, W.; Wang, J.; Lu, L. A Fast SINS Initial Alignment Scheme for Underwater Vehicle Applications. *J. Navig.* **2013**, *66*, 181–198. [CrossRef]
33. U.S. Department of Defense. *Global Positioning System Standard Positioning Service Performance Standard*, 4th ed.; U.S. Department of Defense: Arlington, VA, USA, 2008.
34. Lo, S.; Chen, Y.H.; Reid, T.; Perkins, A.; Walter, T.; Enge, P. The Benefit of Low Cost Accelerometers for GNSS Anti-Spoofing. In Proceedings of the ION 2017 Pacific PNT Meeting, Honolulu, HI, USA, 1–4 May 2017; pp. 775–796.