sensors

MDPI

Article

Performance Analysis of GNSS/INS Loosely Coupled Integration Systems under Spoofing Attacks

Rui Xu *, Mengyu Ding, Ya Qi, Shuai Yue and Jianye Liu

Navigation Research Center, Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China; mengyuding@nuaa.edu.cn (M.D.); nuaaqiya@nuaa.edu.cn (Y.Q.); yueshuai123@nuaa.edu.cn (S.Y.); ljyac@nuaa.edu.cn (J.L.)

* Correspondence: ruixu@nuaa.edu.cn; Tel.: +86-25-84892304

Received: 13 August 2018; Accepted: 18 November 2018; Published: 23 November 2018

Abstract: The loosely coupled integration of Global Navigation Satellite System (GNSS) and Inertial Navigation System (INS) have been widely used to improve the accuracy, robustness and continuity of navigation services. However, the integration systems possibly affected by spoofing attacks, since integration algorithms without spoofing detection would feed autonomous INSs with incorrect compensations from the spoofed GNSSs. This paper theoretically analyzes and tests the performances of GNSS/INS loosely coupled integration systems with the classical position fusion and position/velocity fusion under typical meaconing (MEAC) and lift-of-aligned (LOA) spoofing attacks. Results show that the compensations of Inertial Measurement Unit (IMU) errors significantly increase under spoofing attacks. The compensations refer to the physical features of IMUs and their unreasonable increments likely result from the spoofing-induced inconsistency of INS and GNSS measurements. Specially, under MEAC attacks, the IMU error compensations in both the position-fusion-based system and position/velocity-fusion-based system increase obviously. Under LOA attacks, the unreasonable compensation increments are found from the position/velocity-fusion-based integration system. Then a detection method based on IMU error compensations is tested and the results show that, for the position/velocity-fusion-based integration system, it can detect both MEAC and LOA attacks with high probability using the IMU error compensations.

Keywords: IMU error compensations; Kalman filter; integration system; GNSS; INS; GNSS spoofing interference

1. Introduction

The vulnerability of Global Satellite Navigation Systems (GNSSs) to various intentional and non-intentional radio frequency interferences is an obstacle of GNSS applications [1,2]. Within them, the spoofing interference is a type of troublesome and malicious interference. Spoofing signals have the same characteristics to the legitimate GNSS signals. Thus, they are able to pass through the correlators of target receivers. Usually stronger than authentic signals, spoofing signals guide the victim receivers to track themselves, and then throw the victims astray [3–5].

Many approaches have been proposed to detect or suppress spoofing attacks. For stand-alone GNSS receivers, multiple antennas are widely used to mitigate the effect of spoofing interference by monitoring the direction of arrival signals [6,7]. For single-antenna GNSS receiver, some signal-processing-based techniques have been implemented as effective ways to find spoofing attacks, including Receive Power Monitoring (RPM) [8], correlation function analysis [9] and Kalman filter-based tracking loop [10].

Besides, INS aided methods have also developed because the inertial navigation system (INS) is autonomous and the integration of GNSS and INS is considered the possibility of countering spoofing attacks. The GNSS/INS integration systems overcome the drawbacks of each

stand-alone system and become popular navigation systems [11–13]. In the integration systems, the defects of INSs, the unknown absolute initial position and the accumulative position errors are compensated by GNSS that provides absolute positioning estimations with stationary noise [11,14,15]. Meanwhile, autonomous INSs independent of surroundings have the capability to improve the robustness of GNSSs [16,17].

Actually, of normal GNSS/INS integration systems, the capability to counter spoofing attacks is limited [18–20], since spoofing effects on GNSS probably pollute the estimations of the integration algorithm, such as the Kalman Filter, and then mis-correct the INS states. Some current researches improve the performance of integration systems under spoofing attacks. Using an INS-aided integrity monitoring algorithm, the tightly GNSS/INS integration systems, which fuse both systems using pseudoranges, effectively mitigate spoofing attacks [21]. INS-estimated positions, as well as the satellite positions and receiver clock errors from the GNSS, are used to generate redundant virtual pseudoranges, considered as spoofing-free reference pseudoranges. When one satellite pseudorange is quite different from its virtual pseudorange, the distribution of pseudorange residuals change and the satellite is likely under spoofing attacks. Besides, as the Kalman Filter innovations in tightly GNSS/INS integration systems show unreasonable fluctuations under spoofing environments, they can be used as an alternative detection method [22–24]. With dual antennas, GNSS is able to measure the vehicle heading. The consistency of attitudes resolved by INS and GNSS is able to detect spoofing attacks, due to the difference from the spoofing heading to the actual heading [25,26].

However, these methods are difficultly realized in low-cost GNSS chips that support neither pseudorange outputs nor dual/multiple antenna inputs. Additionally, for these black-box receivers, there is no access to signal processing-based interference detections. The GNSS/INS loosely coupled integration system, fusing both systems using positions (and velocities in some cases), is easily available and widely employed [20]. Thus, we try to find a method to detect spoofing attacks based on the GNSS/INS loosely coupled integration system without additional hardware, information or special requirements.

Considering different behaviors of spoofing effects and different integration fusions, we analyze the performance of the GNSS/INS loosely coupled integration systems with position and position/velocity fusion under two typical spoofing attacks, Meaconing attacks (MEAC attacks) with constant spoofing-induced relative pseudoranges and Lift-off-aligned attacks (LOA attacks) with gradually increasing relative pseudoranges [27]. In the analysis, we focus on variations of the IMU error compensations estimated by the Kalman filer. The compensations refer to IMU physical characteristics and vary within reasonable ranges. Abnormal increments of compensations are likely to alarm spoofing attacks and deeply discussed in the study. Besides, a spoofing detection algorithm based on the compensations is proposed and tested. MEAC attack could be alarmed by GNSS/INSs with both position and position/velocity fusion within one second and two seconds, respectively. For LOA attack, GNSS/INSs with position/velocity fusion are capable of alarming it instantly, while the system with position fusion fails in perceiving spoofing interference. One obvious merit of the spoofing detection is the easy availability for low-cost GNSS/INSs without extra-hardware or improvement on the receiver structure.

In Section 2, the main features of different types spoofing attacks are introduced, as well as their effects on GNSS position and velocity estimations. In Section 3, the effects of spoofing interferences on GNSS/INS loosely coupled integration system are discussed in detail. The effects of different spoofing interferences are compared by experimental studies and a detection method of spoofing attacks is proposed in Section 4. Finally, the conclusions of this study are given in Section 5.

2. Effects of Spoofing Attacks on GNSS Position and Velocity Estimations

Spoofing attacks can be realized by using special devices, such as a GNSS transmitter, to emit GNSS-like signals. The GNSS-like signals have the same signal structures to the authentic signals, but high signal power and different PRN code delays τ_s. The similar signal structures and high

power cause the spoofing signals passing through the correlators and being tracked by the receiver. The different PRN code delays induce different pseudorange measurements and then the false GNSS position and velocity estimations. The delay τ_s^i of spoofing signal referring to the i-th satellite can be written as:

$$\tau_s^i = \tau_a^i + \Delta\tau^i, \tag{1}$$

where τ_a^i is the delay of the authentic signal from the i-th satellite and $\Delta\tau^i$ is the relative spoofing delay. Correspondingly, the relationship within spoofing, authentic and relative pseudoranges is written as:

$$\boldsymbol{\rho}_s = c\boldsymbol{\tau}_s = \boldsymbol{\rho}_{au} + \Delta\boldsymbol{\rho} = \left[\rho_{au}^i\right]_{N\times 1} + \left[\Delta\rho_s^i\right]_{N\times 1}, \tag{2}$$

where c is the speed of light, $\boldsymbol{\rho}_s$ and $\boldsymbol{\rho}_{au}$ are spoofing and authentic pseudorange vectors, respectively, and N is the number of available satellites. The estimated position $\boldsymbol{P}_{GNSS}$ and receiver clock bias δt_u are

$$\begin{bmatrix} \boldsymbol{P}_{GNSS} \\ \delta t_u \end{bmatrix} = (\boldsymbol{A}^T\boldsymbol{A})^{-1}\boldsymbol{A}^T[\boldsymbol{\rho}_{au} + \Delta\boldsymbol{\rho}] = (\boldsymbol{A}^T\boldsymbol{A})^{-1}\boldsymbol{A}^T\boldsymbol{\rho}_{au} + (\boldsymbol{A}^T\boldsymbol{A})^{-1}\boldsymbol{A}^T\Delta\boldsymbol{\rho} = \begin{bmatrix} \boldsymbol{P}_{au} + \Delta\boldsymbol{p}_s \\ \delta t_{ua} + \Delta\delta t_{us} \end{bmatrix}, \tag{3}$$

where $\boldsymbol{A}$ is the satellite geometry matrix referring to the satellite number and distribution, $\boldsymbol{P}_{au}$ is the authentic position, $\Delta\boldsymbol{p}_s$ is the spoofing induced relative position, δt_{ua} is the authentic receiver clock bias, and $\Delta\delta t_{us}$ is the spoofing induced relative receiver clock bias.

Meanwhile, the simulated motion of the spoofing signals also leads to incorrect interpretation of the Doppler shift ($f_s^i \neq f_d^i$ [Hz]). The false Doppler shifts mis-lead the velocity solution of the victim receiver. The relationship between the Doppler shift and pseudorange rate is expressed as:

$$\dot{\rho}_s^i = \dot{\rho}_{au}^i + \Delta\dot{\rho}_s^i = -\lambda\left(f_d^i + \Delta f_s^i\right) = -\lambda f_s^i, \tag{4}$$

Similarly, the velocity solution can be written as

$$\begin{bmatrix} \boldsymbol{V}_{GNSS} \\ \delta\dot{t}_u \end{bmatrix} = \left(\boldsymbol{A}^T\boldsymbol{A}\right)^{-1}\boldsymbol{A}^T(-\lambda\boldsymbol{f}_s) = -\left(\boldsymbol{A}^T\boldsymbol{A}\right)^{-1}\boldsymbol{A}^T(\lambda\boldsymbol{f}_d) + \left(\boldsymbol{A}^T\boldsymbol{A}\right)^{-1}\boldsymbol{A}^T\Delta\dot{\boldsymbol{\rho}}_s = \begin{bmatrix} \boldsymbol{V}_{au} + \Delta\boldsymbol{v}_s \\ \delta\dot{t}_{ua} + \delta\dot{t}_{us} \end{bmatrix}, \tag{5}$$

where $\boldsymbol{V}_{au}$ is the velocity vector from the authentic signals, $\Delta\boldsymbol{v}_s$ is the spoofing induced relative velocity, $\delta\dot{t}_{ua}$ is the authentic receiver clock error rate, and $\delta\dot{t}_{us}$ is the spoofing induced relative receiver clock drift.

Spoofing attacks can be simply and low-costly realized by a transmitter or a repeater which delay the received GNSS signals and transmit them with high power via a transmitting antenna, as shown in Figure 1. Under the situation, signals collected by the target receiver are transmitted from the spoofer rather than the satellites. Therefore, the pseudoranges measured by the target receiver consist of the ranges from satellites to the spoofer receiving antenna r_{sat-RA}^i, from the spoofer receiving antenna to the spoofer transmitting antenna r_{RA-TA}, and from the spoofer transmitting antenna to the target receiver r_{TA-u}. In addition, the measured pseudoranges include the hardware-time-delay induced range $c\delta\tau_{hard}$ in the spoofer and receiver-clock-bias induced range $c\delta t_{ua}$ in the target receiver.

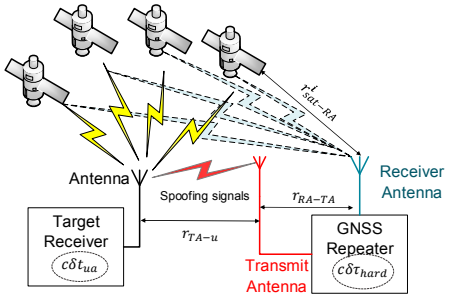

Figure 1. A schema of transmitter-based spoofing attack.

Within these ranges, r^i_{sat-RA} is different in each pseudorange ρ^i_s since its value refers to the different satellite position. The ranges r_{RA-TA}, r_{TA-u}, $c\delta\tau_{hard}$ and $c\delta t_{ua}$ are the same in all pseudoranges. The total pseudorange collected by the target receiver referring to one satellite is written as,

$$\rho^i_s = r^i_{sat-RA} + r_{RA-TA} + r_{TA-u} + c\delta\tau_{hard} + c\delta t_{ua}. \tag{6}$$

From Equations (2) and (6), the relative spoofing pseudorange can be estimated as,

$$\Delta\rho^i = r^i_{sat-RA} - r^i_{au} + r_{RA-TA} + r_{TA-u} + c\delta\tau_{hard}. \tag{7}$$

Equation (7) shows that the spoofing induced position error $\Delta\boldsymbol{p}_s$ depends on the range difference between r^i_{sat-RA} and r^i_{au}. The spoofing induced clock bias error δt_{us} (in the unit of meter) includes r_{RA-TA}, r_{TA-u}, $c\delta\tau_{hard}$ and the common part of $r^i_{sat-RA} - r^i_{au}$. Each them has the same value in all pseudoranges and hence the same behavior to the receiver clock bias. Specially, if $r^i_{sat-RA} = r^i_{au}$ and $r_{TA-u} = 0$, namely the transmitter and the target receiver settled near to each other, it can be obtained that $\Delta\boldsymbol{p}_s = \boldsymbol{0}$.

In Equation (7), the item r_{RA-TA} is constant, equal to the cable length between the spoofer receiving antenna and transmitting antenna. Other items r^i_{sat-RA}, r^i_{au}, r_{TA-u} and $\delta\tau_{hard}$ are time-varying. Thus, the spoofing induced pseudorange rate is written as,

$$\Delta\dot{\rho}^i = \dot{r}^i_{sat-RA} - \dot{r}^i_{au} + \dot{r}_{TA-u} + c\delta\dot{\tau}_{hard}. \tag{8}$$

Similarly, the different part $\dot{r}^i_{sat-RA} - \dot{r}^i_{au}$ in the pseudorange rate leads to velocity variation, which is the spoofing induced velocity. The common parts $\dot{r}_{TA-u}$ and $c\delta\dot{\tau}_{hard}$ affect the receiver clock drift error.

Neither receiver clock bias nor drift is integrated in the GNSS/INS loosely coupled integration system. Their variations under spoofing attacks are simplified in the following analysis. According to Equations (3), (5), (7) and (8), it can be obtained that $\Delta\boldsymbol{p}_s = \Delta\boldsymbol{v}_s t + \Delta\boldsymbol{p}_{s0}$. A common case of $\Delta\boldsymbol{v}_s = \boldsymbol{0}$ and $\Delta\boldsymbol{p}_{s0} \neq \boldsymbol{0}$ would occur under MEAC attack. The item $\Delta\boldsymbol{p}_{s0}$ is the initial position offset, the position difference between the spoofer and the target receiver. The nonzero item $\Delta\boldsymbol{v}_s$ results from the pseudorange rate difference of $\dot{r}^i_{sat-RA}$ and $\dot{r}^i_{au}$ When the spoofer is near to the target receiver and both are relatively static, the item $\Delta\boldsymbol{v}_s$ is close to zero. The value of $\Delta\boldsymbol{p}_s$ steps up to a constant value when spoofing occurs.

Different to the impulsive position error case, the other common case of $\Delta\boldsymbol{v}_s \neq \boldsymbol{0}$ and $\Delta\boldsymbol{p}_{s0} = \boldsymbol{0}$ would occur under Lift-off-aligned attack (LOA attack). In this case, the spoofing signal aligned to the authentic signal at the beginning of the attack, i.e., $\Delta\rho^i = 0$, meanwhile the spoofing induced position deviation $\Delta\boldsymbol{p}_{s0} = \boldsymbol{0}$. Under LOA attack, the spoofing relative delay increases with time. As a result, the spoofing induced relative pseudorange $\Delta\rho^i$ increases with time, i.e., $\Delta\rho^i = \Delta\dot{\rho}^i t$. In this case, pseudorange rate is nonzero and the position estimated from the spoofed receiver are gradually away from the authentic position over time, i.e., $\Delta\boldsymbol{p}_s = \Delta\boldsymbol{v}_s t$. It should be noted that the variation $\Delta\boldsymbol{p}_s = \Delta\boldsymbol{v}_s t$ is also able to realize under MEAC attack. For instance, the spoofer is close to the target receiver and then far away from it. The simple implementation is not exact LOA attack since the spoofing signal with unknown hardware delay is unaligned to the authentic signal.

Generally, the position and velocity measured by GNSS under spoofing attacks can be written as,

$$\begin{gathered} \begin{bmatrix} \boldsymbol{P}_{GNSS} \\ \boldsymbol{V}_{GNSS} \end{bmatrix} = \begin{bmatrix} \boldsymbol{P}_{au} + \Delta\boldsymbol{p}_s \\ \boldsymbol{V}_{au} + \Delta\boldsymbol{v}_s \end{bmatrix}, \\ \Delta\boldsymbol{p}_s = \Delta\boldsymbol{v}_s\boldsymbol{t} + \Delta\boldsymbol{p}_{s0}. \end{gathered} \tag{9}$$

Shortly, under MEAC attack, $\Delta\boldsymbol{v}_s = \boldsymbol{0}$ and $\Delta\boldsymbol{p}_{s0} \neq \boldsymbol{0}$, GNSS-estimated positions step up without significant velocity variations. Under LOA attack, $\Delta\boldsymbol{v}_s \neq \boldsymbol{0}$ and $\Delta\boldsymbol{p}_s = \Delta\boldsymbol{v}_s t$, GNSS-estimated velocities jump up and the estimated positions are gradually away from the actual position.

3. Effects of Spoofing Attacks on the GNSS/INS

The variations of spoofing-induced relative positions and velocities under MEAC and LOA attacks can be described as two typical situations of $\Delta \boldsymbol{p}_s = \Delta \boldsymbol{p}_{s0}$ and $\Delta \boldsymbol{p}_s = \Delta v_s t$, respectively. Their effects on the integration system are investigated after a short introduction to the integration system model under spoofing-free situation.

3.1. The GNSS/INS Loosely Coupled Integration System Model in the Normal Case

GNSS/INS loosely coupled integration systems commonly employ the Kalman Filter to estimate the position and velocity errors, gyroscope bias and first-order Markov process random noise errors, and accelerometer bias error. Then, the state vector $\boldsymbol{X}_k = \begin{bmatrix} \delta \boldsymbol{P}_k & \delta \boldsymbol{V}_k & \boldsymbol{\varepsilon}_{b,k} & \boldsymbol{\varepsilon}_{r,k} & \nabla_k \end{bmatrix}^T$ consists of INS position error $\delta \boldsymbol{P}$, velocity error $\delta \boldsymbol{V}$, gyroscope bias errors $\boldsymbol{\varepsilon}_b$, and first-order Markov process random noise errors of gyroscope $\boldsymbol{\varepsilon}_r$ and accelerometer bias error ∇ [2,6,28]. The process model is commonly as,

$$\boldsymbol{X}_k = \boldsymbol{F}_{k,k-1} \boldsymbol{X}_{k-1} + \boldsymbol{G}_{k-1} \boldsymbol{W}_{k-1}, \tag{10}$$

where $\boldsymbol{F}_{k,k-1}$ is the state transition matrix, $\boldsymbol{G}_k$ is the system noise matrix, and $\boldsymbol{W}_k$ is the process noise, which is assumed as white noise with covariance $\boldsymbol{Q}_k = E\left[\boldsymbol{W}_k \boldsymbol{W}_k^T\right]$.

The acquisition of attitude in GNSS requires multiple antennas, while typical commercial GNSS receivers are equipped with only one receiver antenna and cannot resolve attitudes directly. Therefore, in the GNSS/INS loosely coupled integration systems, GNSS position or GNSS position/velocity are fused with INS. The position and velocity differences between INS and GNSS are considered as measurements. The measurement model is written as:

$$\boldsymbol{Z}_k = \begin{bmatrix} \boldsymbol{Z}_{p,k} \\ \boldsymbol{Z}_{v,k} \end{bmatrix} = \begin{bmatrix} \boldsymbol{P}_{INS,k} - \boldsymbol{P}_{GNSS,k} \\ \boldsymbol{V}_{INS,k} - \boldsymbol{V}_{GNSS,k} \end{bmatrix} = \begin{bmatrix} \delta \boldsymbol{P}_k + \boldsymbol{N}_{g,k} \\ \delta \boldsymbol{V}_k + \boldsymbol{M}_{g,k} \end{bmatrix} = \begin{bmatrix} \boldsymbol{H}_{p,k} \\ \boldsymbol{H}_{v,k} \end{bmatrix} \boldsymbol{X}_k + \begin{bmatrix} \boldsymbol{N}_{g,k} \\ \boldsymbol{M}_{g,k} \end{bmatrix} = \boldsymbol{H}_k \boldsymbol{X}_k + \boldsymbol{V}_k, \tag{11}$$

where $\boldsymbol{N}_g$ and $\boldsymbol{M}_g$ are position error and velocity error of GNSS, respectively. $\boldsymbol{H}_p$, $\boldsymbol{H}_v$ are the measurement matrices. The measurement error $\boldsymbol{V}_k$ is considered as white noise, i.e., $E(\boldsymbol{V}_k) = 0$. Its covariance $\boldsymbol{R}_k$ can be estimated as $\boldsymbol{R_k} = E\left[\boldsymbol{V}_k \boldsymbol{V}_k^T\right]$. Details about the specific parameters of $\boldsymbol{F}, \boldsymbol{G}, \boldsymbol{H}$ can be found in [28]. In Equation (11), the item $\boldsymbol{Z}_k$ represents the position and velocity difference between the GNSS measurements and INS estimation. Under the normal cases, the position and velocity states of GNSS are consistent with that of INS, and hence the position and velocity difference $\boldsymbol{Z}_k$ is small, equal to the sum of GNSS noise and INS errors, i.e., $\boldsymbol{Z}_k = \boldsymbol{V}_k$. If all INS errors are corrected, the item $\boldsymbol{Z}_k$ is GNSS noise. In some loosely coupled integration systems, the velocity difference $\delta \boldsymbol{V}$ is optional. Then, the GNSS/INS integration system becomes integration with position fusion, and the measurement model becomes $\boldsymbol{Z_k} = \boldsymbol{H}_{p,k} \boldsymbol{X}_k + \boldsymbol{N}_{g,k}$.

3.2. Analysis of the Effect of Spoofing Interference on the GNSS/INS

Kalman Filter is most used in the GNSS/INS integration systems. In a standard Kalman Filter, the posteriori state estimate $\hat{\boldsymbol{X}}_k$ is estimated as,

$$\hat{\boldsymbol{X}}_k = \hat{\boldsymbol{X}}_{k,k-1} + \boldsymbol{K}_k \left(\boldsymbol{Z}_k - \boldsymbol{H}_k \hat{\boldsymbol{X}}_{k,k-1} \right), \tag{12.1}$$

$$\hat{\boldsymbol{X}}_{k,k-1} = \boldsymbol{F}_{k,k-1} \hat{\boldsymbol{X}}_{k-1}, \tag{12.2}$$

$$\boldsymbol{K}_k = \boldsymbol{P}_{k,k-1} \boldsymbol{H}_k^T \left(\boldsymbol{H}_k \boldsymbol{P}_{k,k-1} \boldsymbol{H}_k^T + \boldsymbol{R}_k \right)^{-1}, \tag{12.3}$$

where $\hat{\boldsymbol{X}}_{k,k-1}$ is the priori state estimate, $\boldsymbol{K}_k$ is the optimal Kalman gain, $\boldsymbol{P}_{k,k-1} = E\left[\hat{\boldsymbol{X}}_{k,k-1} \hat{\boldsymbol{X}}_{k,k-1}^T\right]$ is the priori error covariance matrix, $\boldsymbol{P}_k = E\left[\hat{\boldsymbol{X}}_k \hat{\boldsymbol{X}}_k^T\right]$ is the posteriori error covariance matrix. The items $\boldsymbol{P}_{k,k-1}$ and $\boldsymbol{P}_k$ are computed as,

$$\boldsymbol{P}_{k,k-1} = \boldsymbol{F}_{k,k-1}\boldsymbol{P}_{k-1}\boldsymbol{F}_{k,k-1}^{T} + \boldsymbol{G}_{k-1}\boldsymbol{Q}_{k}\boldsymbol{G}_{k-1}^{T}, \tag{12.4}$$

$$\boldsymbol{P}_{k} = (\boldsymbol{I} - \boldsymbol{K}_{k}\boldsymbol{H}_{k})\boldsymbol{P}_{k,k-1}, \tag{12.5}$$

The item $\hat{\boldsymbol{X}}_k$ is the optimal estimate of the errors of position, velocity and the IMU errors. It also used to compensate the position, velocity and IMU errors. In the normal case, the item $\hat{\boldsymbol{X}}_k$ is close to zero, meaning that the all errors of INS are compensated. According to the errorless $\hat{\boldsymbol{X}}_k$, the item $\boldsymbol{Z}_k$ equal to the GNSS noise, and $E(\boldsymbol{Z}_k) = 0$. However, when the standard Kalman Filer is in steady state, the matrix $\boldsymbol{P}_{k,k-1}$, $\boldsymbol{P}_k$, and $\boldsymbol{K}_k$ tend to be constant matrices. They slightly vary with the change of measurement noise or process noise. As a result, the Kalman Filter is degraded and equivalent to a constant weighted average method.

Under a spoofing attack, the GNSS position and velocity errors include additional spoofing-induced relative position and relative velocity. The measurement $\boldsymbol{Z}_k$ becomes,

$$\boldsymbol{Z}_{k}^{J} = \begin{bmatrix} \delta\boldsymbol{P}_k + \boldsymbol{N}_{g,k} + \Delta\boldsymbol{p}_{s,k} \\ \delta\boldsymbol{V}_k + \boldsymbol{M}_{g,k} + \Delta\boldsymbol{v}_{s,k} \end{bmatrix} = \boldsymbol{Z}_k + \boldsymbol{J}_k, \tag{13}$$

where the spoofing vector $\boldsymbol{J}_k$ is $\begin{bmatrix} \Delta\boldsymbol{p}_{s,k} & \Delta\boldsymbol{v}_{s,k} \end{bmatrix}^T$. The offsets of position $\Delta\boldsymbol{p}_{s,k}$ and velocity $\Delta\boldsymbol{v}_{s,k}$ generated by spoofing attacks cannot be eliminated by using Equation (11). The spoofed measurements $\boldsymbol{Z}_k^J$ includes the deviation $\boldsymbol{J}_k$. Clearly, spoofing attracts can lead to measurement increase. Besides spoofing attacks, the increase may result from the vehicle motion and IMU error.

Substituting Equation (13) into (12.1), the state compensation $\hat{\boldsymbol{X}}_k^J$ at moment k when spoofing attack appears becomes,

$$\hat{\boldsymbol{X}}_{k}^{J} = \hat{\boldsymbol{X}}_{k,k-1} + \boldsymbol{K}_k\left(\boldsymbol{Z}_{k}^{J} - \boldsymbol{H}_k\hat{\boldsymbol{X}}_{k,k-1}\right) = \hat{\boldsymbol{X}}_k + \boldsymbol{K}_k\boldsymbol{J}_k = \hat{\boldsymbol{X}}_k + \delta\hat{\boldsymbol{X}}_k^J, \tag{14}$$

In Equation (14), the priori state estimate $\hat{\boldsymbol{X}}_{k,k-1}$ is related to the previous state compensation $\hat{\boldsymbol{X}}_{k-1}$, which is independent of the measurement $\boldsymbol{Z}_k^J$ at the $k-1$ moment, and $\hat{\boldsymbol{X}}_k$ is the part of state compensation without spoofing attack effects. Therefore, the spoofing effects on state compensation is $\delta\hat{\boldsymbol{X}}_k^J = \boldsymbol{K}_k\boldsymbol{J}_k$. Since $\boldsymbol{J}_k \neq \boldsymbol{0}$ and $\mathrm{E}\left(\delta\hat{\boldsymbol{X}}_k^J\delta\hat{\boldsymbol{X}}_k^{J,T}\right) > 0$, it can be obtained that $\mathrm{E}\left(\hat{\boldsymbol{X}}_k^J\hat{\boldsymbol{X}}_k^{J,T}\right) > \mathrm{E}\left(\hat{\boldsymbol{X}}_k\hat{\boldsymbol{X}}_k^T\right) = \boldsymbol{P}_k$. The value of $\boldsymbol{P}_k$ in the spoofing environment varies slightly, disagreement with the state error variations. As pointed in Reference [18], it is difficult to detect spoofing attacks using single $\boldsymbol{P}_k$. Meanwhile, the posteriori state estimate $\hat{\boldsymbol{X}}_k$ varies with $\boldsymbol{J}_k$. It means that the spoofing attack causes abnormal corrections on all state compensations, including the navigation compensations ($\delta\boldsymbol{P}$ and $\delta\boldsymbol{V}$) and IMU error compensations ($\boldsymbol{\varepsilon}_b$, $\boldsymbol{\varepsilon}_r$ and ∇). Between the two types of compensation, the navigation information follows the spoofed GNSS [18]; because, without spoofing detection, integration algorithms tend to believe the position and velocity difference between GNSS and INS relating to the carrier motion. Thus, the position and velocity from the integration system are quickly corrected as the similar to the spoofing values.

The IMU errors refer to its inherent physical characteristics, and therefore the compensation of the IMU errors $\boldsymbol{\varepsilon}_b$, $\boldsymbol{\varepsilon}_r$ and ∇ theoretically vary within reasonable ranges. During spoofing, GNSS measured position and velocity are inconsistent with INS estimated ones. The inconsistency leads to abnormal compensation of the IMU errors through the Kalman gain.

Under MEAC attacks $\boldsymbol{J}_k = \left[\Delta\boldsymbol{p}_{s,k}^T, \boldsymbol{0_{3\times 1}}\right]^T$, the item $\delta\hat{\boldsymbol{X}}_k^J$ is $\boldsymbol{K}_{k,p}^{PV}\Delta\boldsymbol{p}_{s,k}$ for the integration system with position/velocity fusion, and $\delta\hat{\boldsymbol{X}}_k^J = \boldsymbol{K}_{k,p}^{P}\Delta\boldsymbol{p}_{s,k}$ for the system with position fusion. The IMU error compensations are the 7–15th elements of $\delta\hat{\boldsymbol{X}}_k^J$ and their values are proportional to $\Delta\boldsymbol{p}_{s,k}$. Both integration systems, with position and position/velocity fusions, are sensitive to the spoofing position deviations under MEAC attacks. Under LOA attack, the spoofing position gradually deviates from the authentic position with small initial position offset $\Delta\boldsymbol{p}_{s,0} \approx \boldsymbol{0}$ ($\boldsymbol{J}_k$=$\begin{bmatrix} \boldsymbol{0_{3\times 1}} & \Delta\boldsymbol{v}_{s,k} \end{bmatrix}^T$). The state

compensation is $\delta\hat{\boldsymbol{X}}_k^J = \boldsymbol{K}_{k,p}^P \mathbf{0} = \mathbf{0}$ in the system with position fusion and the norm $\|\boldsymbol{K}_{k,p}^P \Delta\boldsymbol{p}_{s,k}\| = \mathbf{0}$. In the system with position/velocity fusion, the item $\delta\hat{\boldsymbol{X}}_k^J = \boldsymbol{K}_{k,v}^{PV} \Delta\boldsymbol{v}_{s,k} \neq \mathbf{0}$, is proportional to spoofing velocity deviations $\Delta\boldsymbol{v}_{s,k}$. Therefore, the IMU error compensations in the system with position/velocity fusion have more significant increment at the moment spoofing velocity changes.

Generally, the analysis shows three effects of spoofing attacks on the GNSS/INS loosely coupled integration systems.

(1) Spoofing attack $\boldsymbol{J}_k = \begin{bmatrix} \Delta\boldsymbol{p}_{s,k} & \Delta\boldsymbol{v}_{s,k} \end{bmatrix}^T$ leads to an additional compensation $\delta\hat{\boldsymbol{X}}_k^J = \boldsymbol{K}_k \boldsymbol{J}_k$ in the integration systems. The $\delta\hat{\boldsymbol{X}}_k^J$ modifies the INS estimated position and velocity into spoofed ones.

(2) The $\delta\hat{\boldsymbol{X}}_k^J$ mis-corrects the IMU errors different from its own physical features, which is possibly used to detect spoofing attacks.

(3) The integration systems with position fusion and position/velocity fusion are susceptible to MEAC attacks. To LOA attack, the system with position/velocity fusion is more susceptible.

4. Experimental Results and Discussions

In this section, MEAC attack and LOA attack are implemented. The performances of the Global Positioning System/Inertial Navigation System (GPS/INS) loosely coupled integration systems with position fusion and position/velocity fusion are tested under these two spoofing attacks.

4.1. Experimental

Figure 2 shows the experimental setup of the spoofing interference on the roof of the College of Automation Engineering (CAE) Building 2 in the Nanjing University of Aeronautics and Astronautics (NUAA) campus.

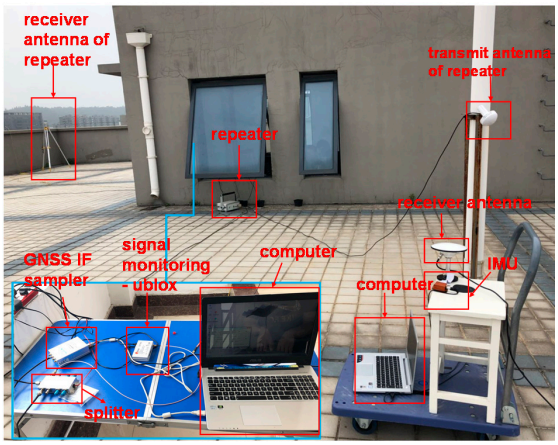

Figure 2. Experimental setup of spoofing attacks on the roof of CEA Building 2.

A GPS repeater is used to generate spoofing signal. Its receiving antenna is about 20 m distance from the target receiver in the case of MEAC attack, and gradually far away from the target receiver in the case of LOA attack. In the test, the spoofing signals cover limited ranges, about 2–5 m. The transmitting antenna should be close to the target receiver to ensure a strong power of spoofing signals. The target receiver is a software-defined GPS receiver with the OLinkStar NS210M IF sampler (OLinkStar Co., Beijing, China) collecting GPS L1 signals. Meanwhile, inertial data are acquired using the low-accurate Xsens MTi-G-710 inertial sensors (Xsens Co., Enschede, The Netherlands), where nominal specifications are shown in Table 1.

Table 1. IMU nominal specifications.

	Gyro	Accelerometer
In-run bias stability	10 deg/h	40 μg
Noise density	0.01 deg/s/Hz$^{1/2}$	80 μg/Hz$^{1/2}$

It should be noted that spoofing attacks in the experiments are not strict MEAC attack or LOA attack, due to the unknown hardware delay of the repeater. The two cases simulate the position and velocity variations of MEAC attack and LOA attack. LOA attack tries to drag the GPS measured position gradually far away from its authentic position. MEAC attack tends to lead a sudden position variation. In MEAC attack case, the distance between antennas of the receiver and repeater is fixed. The collected data length is about 150 s and spoofing attack starts at 83 s. In LOA attack case, the antenna of the repeater is slowly (about 1.2 m/s measured by GPS) away from the receiving antenna of the receiver.

Two common loosely coupled integration systems are tested. One integration system fuses position and velocity information in the Kalman Filter; the other uses position information only. The employed standard Kalman Filter is updated twice per second. The measurement noise covariance matrix is set as $\boldsymbol{R}_k = \mathrm{diag}\left(\begin{bmatrix} 3\,\mathrm{m} & 3\,\mathrm{m} & 6\,\mathrm{m} & 0.2\,\mathrm{m/s} & 0.2\,\mathrm{m/s} & 0.2\,\mathrm{m/s} \end{bmatrix}\right)^2$, based on the accuracy of GPS position errors and velocity errors in ENU coordinate. The process noise, is set as $\boldsymbol{Q}_k = E\left(\begin{bmatrix} \boldsymbol{w}_{wg} & \boldsymbol{w}_{rg} & \boldsymbol{w}_{wa} \end{bmatrix}\begin{bmatrix} \boldsymbol{w}_{wg} & \boldsymbol{w}_{rg} & \boldsymbol{w}_{wa} \end{bmatrix}^T\right)$, where $\boldsymbol{w}_{wg} = \begin{bmatrix} 0.28 & 0.28 & 0.28 \end{bmatrix}$ deg/s, $\boldsymbol{w}_{rg} = \begin{bmatrix} 10 & 10 & 10 \end{bmatrix}$ deg/h, and $\boldsymbol{w}_{wa} = \begin{bmatrix} 98 & 98 & 98 \end{bmatrix}$ μg.

4.2. Navigation Performanceof the GPS/INS under SpoofingAttacks

The average position in East-North-Up coordinate from the GPS receiver under normal situation is considered as the reference value. Figure 3 shows the eastern position errors and eastern velocities from the GPS receiver and the two GPS/INS loosely coupled integration systems.

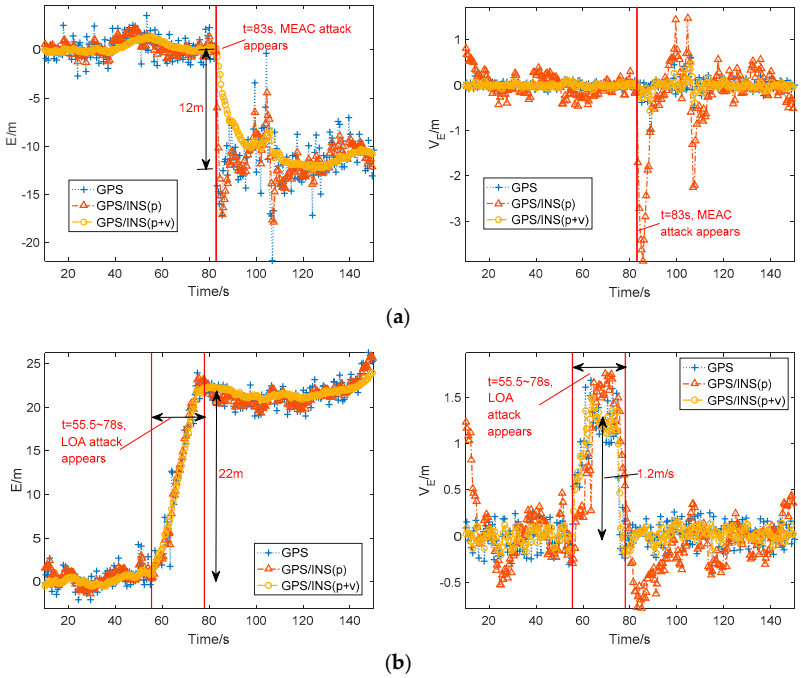

Figure 3. Eastern position error and eastern velocity estimated by Global Positioning System (GPS) and Global Positioning System /Inertial Navigation System (GPS/INS) under Meaconing attacks (MEAC) attack (**a**) and lift-of-aligned (LOA) attack (**b**). MEAC attack begins at 83 s and LOA attack is during 55 s to 78 s.

In Figure 3a, during MEAC attack, the eastern position errors of GPS suddenly jump to −12 m from 0 m and the eastern velocity mainly keeps at zero except a slight increment during 83 s to 90 s. The slight increment on velocity probably results from spoofing attack. The eastern position errors from the two GPS/INS loosely coupled integration systems show the similar performance to that of GPS. Although the velocity fusion smooths the increase of position error, the GPS/INS system has been spoofed under MEAC attack. For the velocity estimation, the integration system with position/velocity fusion performs similar to the GPS receiver, estimated eastern velocity varying slightly and close to zero. However, the integration system with position fusion displays a high sensitivity to MEAC attack, a −3.8 m/s eastern velocity jerk following the occurrence of MEAC attack.

As shown in Figure 3b, under LOA attack, the eastern position errors of GPS deviate gradually from the authentic location during 55.5 s to 78 s, and maintain at about 22 m after 78 s. Like the GPS receiver, the both integration systems are spoofed by LOA attack. Their velocity estimations show the same variation during the spoofing period. A short velocity increase by 0.5–1.8 m/s occurs during the dragging period from 55.5 s to 78 s. Then, the velocity turns back zero after 78 s.

To investigate the overall influence of spoofing attacks on the position and velocity, the norms of position compensation $\|\delta \boldsymbol{p}\|$ and velocity compensation $\|\delta \boldsymbol{v}\|$ are defined as:

$$\begin{aligned} \|\delta \boldsymbol{p}\| &= \sqrt{(\delta p_e)^2 + (\delta p_n)^2 + (\delta p_u)^2} = \sqrt{\sum_{i=1}^{3} \left(\hat{X}_k^J(i)\right)^2}, \\ \|\delta \boldsymbol{v}\| &= \sqrt{(\delta v_e)^2 + (\delta v_n)^2 + (\delta v_u)^2} = \sqrt{\sum_{i=4}^{6} \left(\hat{X}_k^J(i)\right)^2}, \end{aligned} \tag{15}$$

Figure 4 shows the norms of position and velocity compensation under spoofing attacks. Under MEAC attack, the position and velocity compensation norms from the GPS/INS with position fusion increases greatly, while the norms from the GPS/INS with position/velocity fusion change a little. Under LOA attack, both the norms estimated by the GPS/INS with position fusion and position/velocity fusion here have some increments, not as significant as variations under MEAC attack. In addition, the norm increments of position and velocity from the system with position fusion quickly and sharply follow the occurrence of MEAC attack. Under LOA attack, the increment occurs at 64 s, about lagging 9 s to the occurrence of LOA attack. It implies a possible spoofing detection for the integration system with position fusion through using unreasonable increment on norms of position and velocity compensation. The unreasonable norm increment occurs following MEAC attack and a period lagging to LOA attack. It should be pointed out that under LOA attack the position and velocity compensation norms increments is difficult to detect.

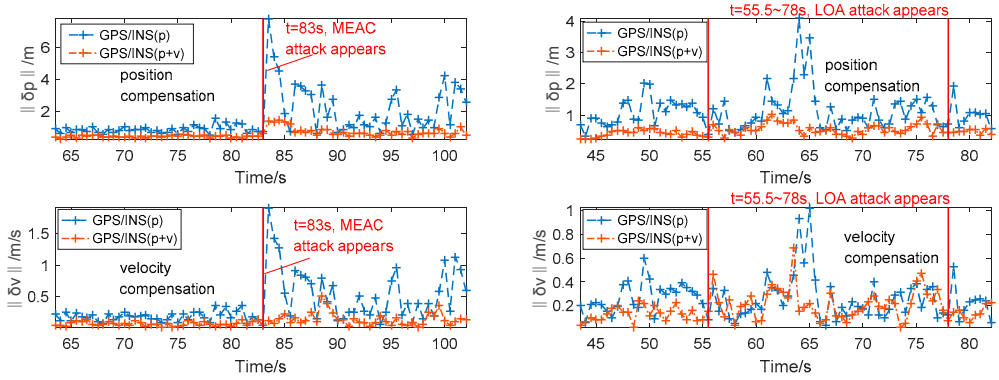

Figure 4. The position and velocity compensation norms estimated by the GPS/INS with position fusion and position/velocity fusion under MEAC attack (**a**) and LOA attack (**b**).

Shortly, the GPS/INS loosely coupled integration systems based on standard Kalman Filter are deceived by both MEAC and LOA attacks.

4.3. The Variations of IMU Error Compensation under MEAC and LOA Attacks

Figure 5 shows the estimated gyroscope bias errors from the GPS/INS with position and position/velocity fusions under MEAC and LOA attacks. Before spoofing, the gyroscope bias errors vary within 0.01 deg/h in Figure 5a and 0.03 deg/h in Figure 5b. Under MEAC attack, the gyroscope bias errors in Z-axis range between −0.07 deg/h and 0.06 deg/h. The two integration systems show the similar performance. The gyroscope bias errors significantly increase during the whole MEAC spoofing. Under LOA attack, the gyroscope bias errors estimated by the position/velocity-fusion-based integration system become large, ranging between −0.08 deg/h and 0.14 deg/h. With the position fusion, the GPS/INS integration system is little disturbed by LOA attack.

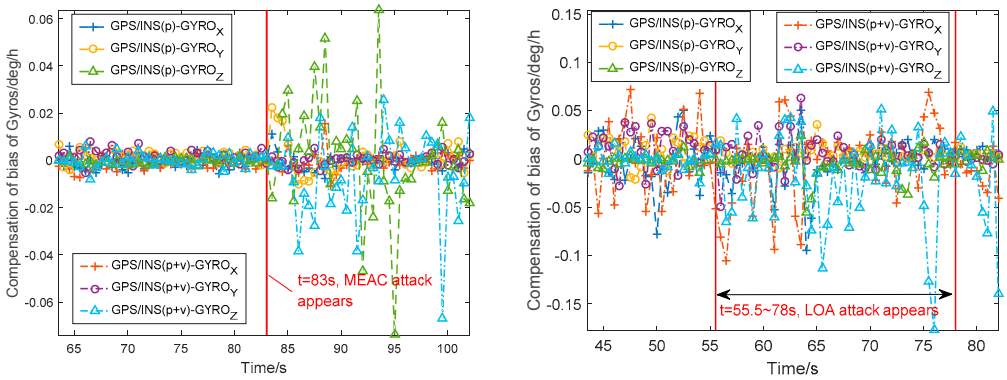

Figure 5. The compensation of gyroscope bias in GPS/INS with position and position/velocity fusions under MEAC attack (**a**) and LOA attack (**b**).

In addition, the effects of spoofing attacks on different axial gyroscopes are different. To investigate the overall influence of the spoofing attack on the IMU, the norms of the XYZ-axis gyroscope bias compensation $\|\varepsilon_b\|$, the gyroscope first-order Markov compensation $\|\varepsilon_r\|$ and the XYZ-axis accelerometers bias compensation $\|\nabla\|$ are defined as,

$$\begin{aligned} \|\varepsilon_b\| &= \sqrt{(\varepsilon_{bx})^2 + \left(\varepsilon_{by}\right)^2 + (\varepsilon_{bz})^2} = \sqrt{\textstyle\sum_{i=7}^{9}\left(\delta\hat{X}_k^J(i)\right)^2}, \\ \|\varepsilon_r\| &= \sqrt{(\varepsilon_{rx})^2 + \left(\varepsilon_{ry}\right)^2 + (\varepsilon_{rz})^2} = \sqrt{\textstyle\sum_{i=10}^{12}\left(\delta\hat{X}_k^J(i)\right)^2}, \\ \|\nabla\| &= \sqrt{(\nabla_x)^2 + \left(\nabla_y\right)^2 + (\nabla_z)^2} = \sqrt{\textstyle\sum_{i=13}^{15}\left(\delta\hat{X}_k^J(i)\right)^2}, \end{aligned} \tag{16}$$

Figure 6 shows the norms of the IMU error compensation under spoofing attacks. Under MEAC attack, as shown in Figure 6a, the norms of the gyroscope bias compensations become much larger than that under spoofing-free period. The norm of the gyroscope bias compensation reaches 0.074 deg/h at 95 s during spoofing period. Under spoofing-free condition, the maximum norm value is 0.007 deg/h at 64.5 s. Similar variations are also found in $\|\varepsilon_r\|$ and $\|\nabla\|$. Although the occurrence of the incorrectness in the GPS/INS loosely coupled integration with position/velocity fusion is 1 s slower than that in the system with position fusion, two systems show the similar sensitivity to MEAC attack. Thus, the norms of the IMU error compensation have the capability to detect MEAC attack.

Under LOA attack, as shown in Figure 6b, the increments of $\|\varepsilon_b\|$, $\|\varepsilon_r\|$ and $\|\nabla\|$ from the integration system with the position fusion become insignificant. Differently, from the system with the position/velocity fusion, the norms also increase during LOA attack. Although the increments are

not as obvious as that under MEAC attack, the maximum value of $\|\varepsilon_b\|$ reaches 0.14 deg/h, 4.6 times larger than the value under spoofing-free periods.

To test the performance of $\|\varepsilon_b\|$, $\|\varepsilon_r\|$ and $\|\nabla\|$ under dynamic situation, the IMU is placed on a turntable to simulate attitude movement, i.e., heading, pitch and roll angle changes simultaneously. The collected inertial data is integrated with the spoofed GPS data to study whether spoofing attacks would have significant impacts on the dynamic IMU error compensation. The results are shown in Figure 7.

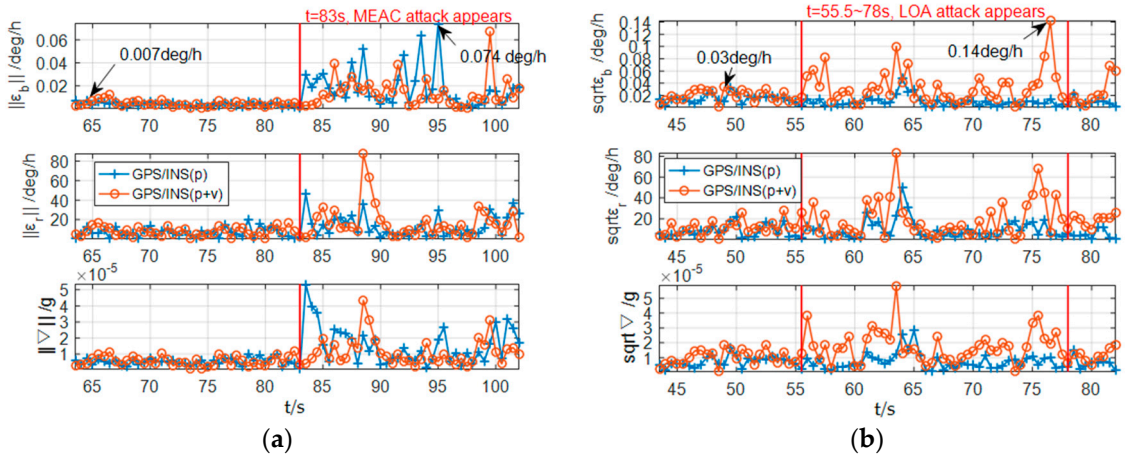

Figure 6. The IMU error compensation norms estimated by GPS/INS with position and position/velocity fusions under MEAC attack (**a**) and LOA attack (**b**).

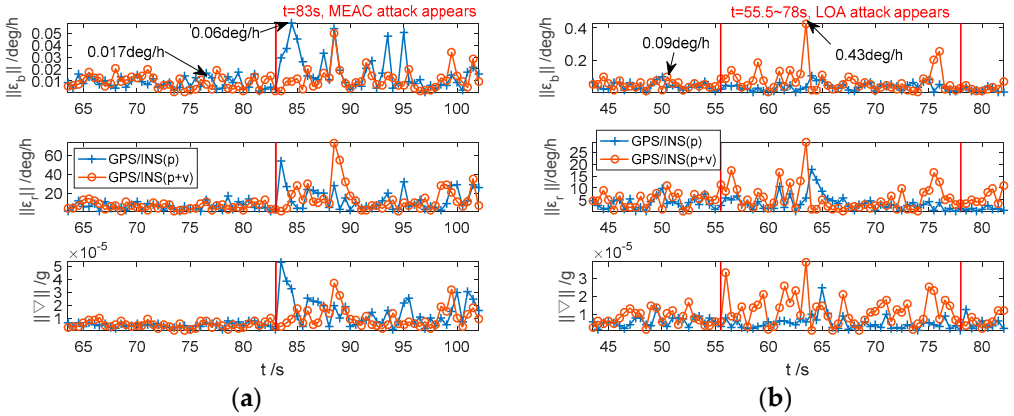

Figure 7. The IMU error compensation norms estimated by the GPS/INS with position and position/velocity fusions under MEAC attack (**a**) and LOA attack (**b**) in the dynamic case.

In Figure 7a, the fluctuations of IMU error compensation norms, under spoofing-free period, are slightly larger than the static IMU. Under MEAC attack, the norms significantly increase regardless of whether the fusion information is position or position/velocity. Similar to the static case, the variation of $\|\varepsilon_b\|$ from the integration system with position fusion is not obvious under LOA attack, as shown in Figure 7b. With the position/velocity fusion, the maximum value of $\|\varepsilon_b\|$ reaches 0.43 deg/h during spoofing period, which is five times of the maximum norm under normal condition. The variations of $\|\varepsilon_r\|$ and $\|\nabla\|$ are similar to $\|\varepsilon_b\|$. It should be noted that the moment with obvious spoofing-induced increments on $\|\varepsilon_b\|$, $\|\varepsilon_r\|$ and $\|\nabla\|$ are later than the moment spoofing appearing. It may be due to the smoothing effects of Kalman Filter on velocity correction.

Shortly, for the loosely coupled integration system with the position/velocity fusion, the IMU error compensations are sensitive to both MEAC and LOA attacks. The compensations increase significantly during spoofing. For the system with position fusion, the IMU error compensation are sensitive to MEAC attacks. Different to the position and velocity compensations which also affected by

the receiver dynamic situation, the IMU error compensations refer to IMU physical features and are possible to detect spoofing attacks in the GPS/INS loosely coupled integration systems.

To test the feasibility of spoofing attack detection based on IMU error compensations, a basic detection is employed. When the instantaneous $\|\varepsilon_b\|$ is larger than its historical statistics, the state of $\|\varepsilon_b\|$ will stay at pre-alarm state (marked as 2 in Figure 8), which means there would be a possibility of spoofing attack. The states of the item $\|\varepsilon_r\|$ and $\|\nabla\|$ are detected using the similar method. Then the alarm of spoofing attack is given through combining detection results of $\|\varepsilon_b\|$, $\|\varepsilon_r\|$ and $\|\nabla\|$. Since both $\|\varepsilon_b\|$ and $\|\varepsilon_r\|$ are the features of gyroscopes and $\|\nabla\|$ is related to accelerometers, the spoofing attack is alarmed when the state of $\|\nabla\|$ is pre-alarm, and any state of $\|\varepsilon_b\|$ or $\|\varepsilon_r\|$ is pre-alarm.

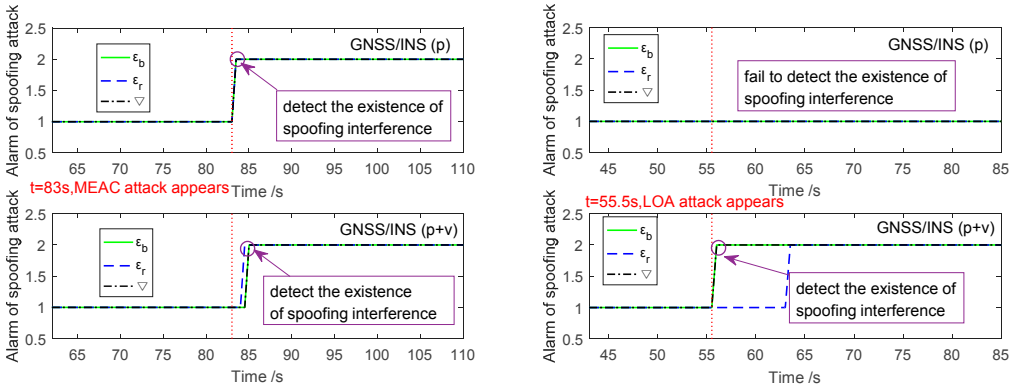

Figure 8. The detection of spoofing attack based on the IMU error compensation norms under MEAC attack (**a**) and LOA attack (**b**).

Figure 8a illustrates the detection results of MEAC attack in GPS/INS with position and position/velocity fusions. Under MEAC attack, $\|\varepsilon_b\|$, $\|\varepsilon_r\|$ and $\|\nabla\|$ of the GNSS/INS with position fusion suddenly rise at 83 s, the moment of MEAC attack beginning. All $\|\varepsilon_b\|$, $\|\varepsilon_r\|$ and $\|\nabla\|$ are into the pre-alarm state and spoofing is detected at 83 s. For the GPS/INS with position/velocity fusion, the visible rise of $\|\varepsilon_b\|$, $\|\varepsilon_r\|$ and $\|\nabla\|$ follows the occurrence of MEAC attack after about two seconds. Each of them alarms the spoofing after a short delay. Therefore, the voted alarm of MEAC attack is about two second later than the moment of spoofing occurrence. By contrast, under LOA attack, as shown in Figure 8b, any item of $\|\varepsilon_b\|$, $\|\varepsilon_r\|$ and $\|\nabla\|$ in system with position fusion fails in alarming spoofing; because, the IMU error compensations increase slightly. Fortunately, these items, especially the $\|\nabla\|$ and $\|\varepsilon_b\|$, of the system with position/velocity fusion, increase dramatically once LOA attack occurs. Although the item $\|\varepsilon_r\|$ switches into pre-alarm state with 8 s delay, the voted spoofing alarm is at 56 s, close to the occurrence moment of LOA attack. In short, INS error compensations, in both integration systems with position and position/velocity fusions, can be used to detect MEAC attack. LOA attack is likely to be detected effectively by using the INS error compensations from the position/velocity fusion-based integration system. Once the spoofing attack being detected, it is suggested to reject GPS information input to Kalman filter, which is shown in Figure 9.

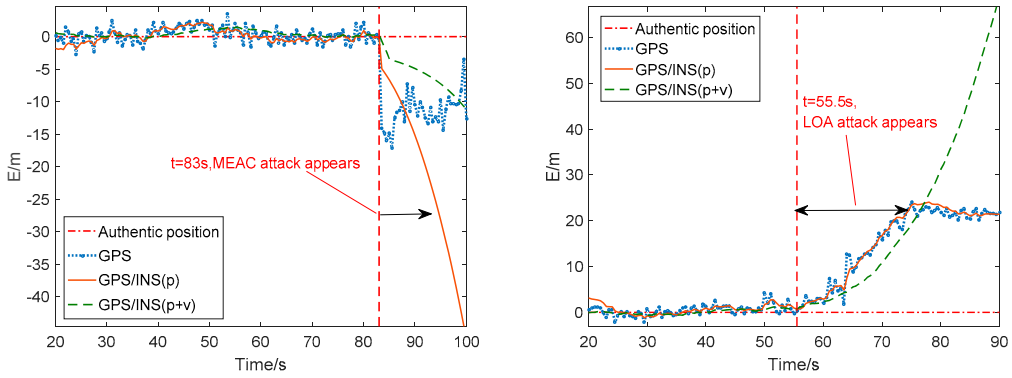

Figure 9. The performance of GPS/INS with position and position/velocity fusions after detection of MEAC attack (**a**) and LOA attack (**b**).

Figure 9 shows the eastern position error estimated by GPS/INS with two types of fusions before and during spoofing attacks. Under MEAC attack, as shown in Figure 9a, both GPS/INS systems with position fusion and position/velocity fusion succeed in detecting the occurrence of MEAC attack with a short delay, about one or two seconds. The integration system degrades into independent INS. The estimated position is no longer deceived by spoofing attacks. It is no doubt that the position error of stand-alone INS increases with time. Therefore, in Figure 9a, the position error of GPS/INS with position fusion increases to 12 m at 88 s. After 5 s since spoofing detection, the position error of the system with position fusion is larger than the spoofing induced position error. With position/velocity fusion, the GPS/INS shows better performances than the one with position fusion. It keeps its position error within 12 m for about 16 s. The improvement is probably due to more accurate error compensation than that estimated by the system with position fusion. Under LOA attack, as shown in Figure 9b, the GPS/INS with position fusion fails in spoofing detection since its $\|\varepsilon_b\|$, $\|\varepsilon_r\|$ and $\|\nabla\|$ increments are too slight to detect spoofing attack. The system with position/velocity fusion still successfully detects the spoofing attack and turns into stand-alone INS at 56 s. The position error under LOA attack quickly increases to 22 m at 76 s. During the 20 s duration, the INS position error keeps less than spoofing induced position error. The slight superiority results from the growth rate of INS position error lower than the spoofing velocity Δv_s. It is a combination result of IMU performance and error compensation, as well as the values of spoofing velocity Δv_s and position deviation Δp_s, which are out of the discussion of the study.

Shortly, IMU error compensation-based spoofing detection is effective. For GPS/INS with position/velocity fusion, it is possible to detect both MEAC attack and LOA attack. Once the integration system turns into the stand-alone INS after spoofing detection, the system is able to isolate spoofing effects. In this case, the accumulative position error is inevitable. High-precise IMUs and advanced IMU error compensation algorithms are helpful in slowing the INS position error growth.

5. Conclusions

In this paper, the performance of the GNSS/INS loosely coupled integration systems with position and position/velocity fusions under MEAC attacks and LOA attacks are analyzed. The GNSS/INS loosely coupled integration systems with either position fusion or position/velocity fusion is easily disturbed by spoofing attacks, similar to GNSS.

However, we can exploit the fact that the position and velocity from GNSS are inconsistent with the physical states measured by the INS. The inconsistency causes abnormal corrections to the IMU error compensations. Specially, the incorrect IMU error compensations from the integration system with the position fusion are significant under MEAC attack, which generates a jump of positioning results. Under LOA attack with slow position variation, as well as MEAC attacks, the compensations from the system with the position/velocity fusion are more sensitive. Thus, it is possible, using IMU

error compensations, which are related to IMU's physical features, to detect spoofing attacks. A simple detection method is implemented and tested. The detection results show that with position/velocity fusion, the GNSS/INS loosely coupled integration system is able to detect both MEAC and LOA spoofing attacks through using the IMU error compensations.

The paper focuses on the possibility of spoofing detection based on IMU error compensation for the loosely coupled integration system. Further studies will interest in the effects of IMUs with different accuracy levels and the spoofing detection and mitigation methods.

Author Contributions: Conceptualization, R.X. and M.D.; Methodology, R.X. and M.D.; Software, M.D.; Validation, M.D., Y.Q. and S.Y.; Formal Analysis, R.X. and M.D.; Investigation, M.D.; Resources, J.L.; Writing-Original Draft Preparation, R.X. and M.D.; Writing-Review and Editing, R.X.; Visualization, M.D.; Supervision, R.X. and J.L.

Funding: This research was funded by the National Natural Science Foundation of China grant number [61603181, 61533008] and Nanjing University of Aeronautics and Astronautics grant number [kfjj20170318].

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

References

1. Sánchez-Naranjo, S.M.; Ferrara, N.G.; Paśnikowski, M.J.; Raasakka, J.; Shytermeja, E.; Ramos-Pollán, R.; Osorio, F.A.O.; Martínez, D.; Lohan, E.-S.; Nurmi, J.; et al. *GNSS Vulnerabilities*; Springer: Berlin, Germany, 2017; pp. 55–77, ISBN 978-3-319-50427-8.
2. Gao, G.X.; Sgammini, M.; Lu, M.; Kubo, N. Protecting GNSS Receivers from Jamming and Interference. *Proc. IEEE* **2016**, *104*, 1327–1338. [CrossRef]
3. 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*, 1–31. [CrossRef]
4. Iran Claims Released Footage Is from Downed U.S. Drone. Available online: http://edition.cnn.com/2013/02/07/world/meast/iran-drone-video (accessed on 7 February 2013).
5. Bhatti, J.; Humphreys, T.E. Hostile Control of Ships via False GPS Signals: Demonstration and Detection. *Navigation* **2017**, *64*, 51–66. [CrossRef]
6. Psiaki, M.L.; O'hanlon, B.W.; Powell, S.P.; Bhatti, J.A.; Wesson, K.D.; Humphreys, T.E. GNSS spoofing detection using two-antenna differential carrier phase. *GPS World* **2014**, *25*, 36–44.
7. Konovaltsev, A.; Cuntz, M.; Haettich, C.; Meurer, M. Autonomous Spoofing Detection and Mitigation in a GNSS Receiver with an Adaptive Antenna Array. In Proceedings of the 26th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2013), Nashville, TN, USA, 16–20 September 2013; pp. 2937–2948.
8. Jafarnia-Jahromi, A.; Broumandan, A.; Nielsen, J.; Lachapelle, G. Pre-Despreading Authenticity Verification for GPS L1 C/A Signals. *Navigation* **2014**, *61*, 1–11. [CrossRef]
9. Manfredini, E.G.; Motella, B.; Dovis, F. Signal quality monitoring for discrimination between spoofing and environmental effects, based on multidimensional ratio metric tests. In Proceedings of the 28th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+ 2015), Tampa, FL, USA, 14–18 September 2015; pp. 3100–3106.
10. Lin, Z.; Chu, H.; Zhang, N. Anti-Spoofing Extended Kalman Filter for Satellite Navigation Receiver. In Proceedings of the Wireless Communications, Networking and Mobile Computing (IEEE), Shanghai, China, 21–25 September 2007; pp. 996–999. [CrossRef]
11. Shaeffer, D.K. MEMS inertial sensors: A tutorial overview. *Commun. Mag. IEEE* **2013**, *51*, 100–109. [CrossRef]
12. Zhang, C.; Li, X.; Gao, S.; Lin, T.; Wang, L. Performance Analysis of Global Navigation Satellite System Signal Acquisition Aided by Different Grade Inertial Navigation System under Highly Dynamic Conditions. *Sensors* **2017**, *17*, 980. [CrossRef] [PubMed]
13. Groves, P.D. *Principles of GNSS Inertial and Multisensor Integrated Navigation Systems*, 2nd ed.; Artech House: Norwood, MA, USA, 2013.
14. Yuan, B.; Liao, D.; Han, S. Error compensation of an optical gyro INS by multi-axis rotation. *Meas. Sci. Technol.* **2012**, *23*, 91–95. [CrossRef]

15. Fang, H.; Feng, Q. Influence of Inertial Sensor Errors on GNSS/INS Integrated Navigation Performance. In Proceedings of the 8th International Conference on Measuring Technology and Mechatronics Automation, Macau, China, 11–12 March 2016; pp. 347–351.
16. Falco, G.; Pini, M.; Marucco, G. Loose and Tight GNSS/INS Integrations: Comparison of Performance Assessed in Real Urban Scenarios. *Sensors* **2017**, *17*, 27. [CrossRef] [PubMed]
17. Yan, K.; Zhang, T.; Niu, X.; Zhang, H.; Zhang, P.; Liu, J. INS-aided tracking with FFT frequency discriminator for weak GPS signal under dynamic environments. *GPS Solutions* **2017**, *21*, 917–926. [CrossRef]
18. Liu, Y.; Li, S.; Fu, Q.; Liu, Z. Impact Assessment of GNSS Spoofing Attacks on INS/GNSS Integrated Navigation System. *Sensors* **2018**, *18*, 1433. [CrossRef] [PubMed]
19. Pozzobon, O.; Sarto, C.; Chiara, A.D. Cooperative DSP-EKF in integrated GNSS-INS for user-based authentication estimation. In Proceedings of the European Navigation Conference (ENC), Helsinki, Finland, 30 May 2016.
20. Broumandan, A.; Lachapelle, G. Spoofing Detection Using GNSS/INS/Odometer Coupling for Vehicular Navigation. *Sensors* **2018**, *18*, 1305. [CrossRef] [PubMed]
21. Khanafseh, S.; Roshan, N.; Langel, S.; Chan, F.C.; Joerger, M.; Pervan, B. GPS spoofing detection using RAIM with INS coupling Position. In Proceedings of the Position, Location and Navigation Symposium—PLANS, Monterey, CA, USA, 5–8 May 2014; pp. 1232–1239.
22. 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, Portland, OR, USA, 12–16 September 2016; pp. 2291–3001.
23. Tanıl, Ç.; Khanafseh, S.; Joerger, M.; Pervan, B. Kalman filter-based INS monitor to detect GNSS spoofers capable of tracking aircraft position. In Proceedings of the Position, Location and Navigation Symposium, Savannah, GA, USA, 11–14 April 2016.
24. Tanıl, Ç.; Khanafseh, S.; Joerger, M.; Pervan, B. An INS Monitor to Detect GNSS Spoofers Capable of Tracking Vehicle Position. *IEEE Trans. Aerosp. Electron. Syst.* **2017**, *54*, 131–143. [CrossRef]
25. Liu, Y.; Fu, Q.; Li, S.; Xiao, X. The Effect of IMU Accuracy on Dual-antenna GNSS Spoofing Detection. In Proceedings of the 2016 International Technical Meeting of The Institute of Navigation, Monterey, CA, USA, 25–28 January 2016; pp. 169–180.
26. Liu, Y.; Li, S.H.; Xiao, X.; Fu, Q.W. INS-Aided GNSS Spoofing Detection Based on Raw Pseudorange and Carrier Phase Measurements. In Proceedings of the Saint Petersburg International Conference on Integrated Navigation Systems, Saint Petersburg, Russia, 25–27 May 2015; pp. 20–27.
27. 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]
28. Qin, Y.; Zhang, H.; Wang, S. *Principles of Kalman Filter and Integrated Navigation*; Northwestern Polytechnical University Press: Xi'an, China, 2015; ISBN 9787561243503.