Article

A Slowly Varying Spoofing Algorithm on Loosely Coupled GNSS/IMU Avoiding Multiple Anti-Spoofing Techniques

Yangjun Gao 1,2 and Guangyun Li 1,*

1 College of Geospatial Information, PLA Strategic Support Force Information Engineering University, Zhengzhou 450001, China; yangjun_gao@163.com
2 State Key Laboratory of Geo-Information Engineering, Xi’an 710054, China
* Correspondence: guangyun_li_chxy@163.com

Abstract: When satellite navigation terminal sensors encounter malicious signal spoofing or interference, if attention is not paid to improving their anti-spoofing ability, the performance of the sensors will be seriously affected. The global navigation satellite system (GNSS) spoofing has gradually become a research hotspot of the jammer because of its great harm and high concealment. In the face of more and more sensors coupling GNSS and inertial measurement unit (IMU) to varying degrees and configuring a variety of anti-spoofing techniques to effectively detect spoofing, even if the spoofer intends to gradually pull the positioning results, if the spoofing strategy is unreasonable, the parameters of the coupled filter output and spoofing observation measurement will lose their rationality, which will lead to the spoofing being detected. To solve the above problems, in order to effectively counter the non-cooperative target sensors of assembling loosely coupled GNSS/IMU using GNSS spoofing, based on the analysis of the influence mechanism of spoofing on the positioning of loosely coupled GNSS/IMU, a slowly varying spoofing algorithm to avoid loosely coupled GNSS/IMU with multiple anti-spoofing techniques is proposed in this paper, and a measurement deviation determination method to avoid multiple anti-spoofing techniques is proposed, which can gradually pull the positioning results of the coupled system and successfully avoid the detection of anti-spoofing techniques of innovation sequence monitoring and a rationality check on parameters. Simulation experimental results show that the proposed algorithm gradually changes the positioning of loosely coupled GNSS/IMU, the north and east displacements achieve the purpose of spoofing, and error with expected offset is $-0.2$ m and $2.3$ m, respectively. Down displacement also basically achieves the purpose of spoofing, and error with the expected offset is $13.2$ m. At the same time, the spoofer avoids the detection of multiple anti-spoofing techniques, does not trigger the system alarm, and realizes the purpose of spoofing; thus, the effectiveness and high concealment of the spoofing algorithm are verified.

Keywords: slowly varying spoofing; loosely coupled GNSS/IMU; anti-spoofing techniques; innovation sequence monitoring; rationality check

1. Introduction

The global navigation satellite system (GNSS) spoofing technology has gradually become the focus of interference technology research because of its great threat and high concealment [1,2]. Spirent can manufacture a simple spoofing source by configuring the corresponding power amplifier and transmitting antenna on its product, GSS8000 [3]. In 2002, Jon S. Warner et al. used a simple GPS signal simulator to spoof a GPS receiver of a freight truck, demonstrating that the civil GPS receiver is vulnerable to a simple spoofing attack [4]. In 2012, Todd E. Humphrey’s team used a low-cost GPS spoofer to continuously lower the unmanned helicopter that should have maintained a fixed altitude [5]. In addition, GNSS spoofing can seriously affect GNSS timing information [6–8].
At present, there are many spoofing detection methods based on the single GNSS module [9,10], but any method is difficult when dealing with all spoofing methods [11]. In GNSS and the inertial measurement unit (IMU) system, IMU constantly uses measurement information of GNSS to correct its own error. Slow spoofing can also spoof the GNSS/IMU system, for example, traction spoofing can take over the loop without destroying the tracking loop [12]. When the difference between the position velocity and time (PVT) and real PVT is large, the user can detect spoofing by comparing with the measurement results of other sensors. Therefore, it is necessary to gradually pull PVT results to make the variation within the allowable range of the sensor error [13].

The research on the spoofing coupled system is summarized as follows. Mi Shi’s theoretical derivation and simulation show the influence of GNSS spoofing on the positioning results of loose coupling, but the mathematical model is not consistent with the actual situation that the target will adjust the trajectory after being affected by spoofing [14]. Yang Liu et al. studied the influence of GNSS spoofing on the Kalman filter error covariance matrix, innovation sequence and inertial sensor deviation estimation of a loosely coupled GNSS/INS system; their simulation showed that the Kalman filtering error covariance is not affected by spoofing, and innovation sequence and estimated inertial sensor deviation change [15]. Rui Xu et al. analyzed the performance of the position fusion and position/velocity fusion loosely coupled GNSS/IMU system under forwarding spoofing and traction spoofing. Under forwarding spoofing, the error compensation of the position fusion loosely coupled system for IMU is very significant, resulting in a jump in the positioning results. Under intermediate spoofing, the compensation increment of the loosely coupled system based on position/velocity fusion is more sensitive [16]. The navigation system adopts normalized innovation squared (NIS) detection; it is a direct, effective and feasible spoofing detection method, which is mature and has been applied to the navigation system of unmanned aerial vehicles (UAVs) and other targets [17]. Gao Yangjun et al. analyzed the influence of spoofing on the positioning of loosely coupled GNSS/IMU. Aiming at the problem that the equation is easy to be ill conditioned when the measurement deviation is introduced, a Kalman gain matrix local regularization method is proposed to accurately calculate the measurement deviation; in order to avoid the NIS detection alarm of the target navigation system, the range of measurement deviation is calculated, so that the spoofing process has strong concealment; then a two-step trajectory guidance algorithm is proposed so that the target can be quickly induced to the spoofing trajectory [18]. The above comprehensive literature review shows the representative research work on spoofing loosely coupled GNSS/IMU systems. After the summary, the difficulties of the current spoofing on a coupled system are described.

The background and motivation of this research work can be described as follows: using GNSS spoofing technology to control or even counter moving objects, such as unidentified aircraft, such as UAV, that may pose threats is a very effective means. However, as more and more navigation systems of unmanned aircraft are equipped with coupled GNSS/IMU systems, which can effectively detect spoofing, it is more and more difficult for the spoofer to achieve effective spoofing. For the spoofer, the specific difficulties of spoofing are as follows: to sum up, the difficulty of spoofing the coupled system is that even if the spoofer intends to slowly change the positioning of the coupled system, they should pay close attention to whether other state parameters of the coupled system change abnormally in the process of spoofing; in addition, although the loosely coupled system itself has good anti-spoofing ability, if the coupled system is additionally equipped with other anti-spoofing techniques, the spoofer needs to consider how to introduce an appropriate amount of spoofing observation, so that the spoofing process will not raise the alarm of the coupled system.

Based on the above research background, the research motivation of this paper is to propose a spoofing algorithm that can slowly pull the positioning results of a loosely coupled GNSS/IMU system and avoid a variety of anti-spoofing techniques so as to
realize successful spoofing on a loosely coupled GNSS/IMU system and further realize the effective control of the unidentified aircraft that poses threats.

The research work of this paper is briefly summarized as follows. In Section 1, the background, current situation and significance of the research are introduced. In Section 2, the influence mechanism of spoofing on loosely coupled GNSS/IMU is analyzed, including the loosely coupled GNSS/IMU system model and influence of spoofing on loosely coupled GNSS/IMU. In Section 3, a slowly varying spoofing algorithm to avoid multiple anti-spoofing techniques is proposed, after the spoofing signal completely takes over the GNSS module of the coupled system, based on the analysis of the influence mechanism of spoofing on the positioning of loosely coupled GNSS/IMU, a slowly varying spoofing algorithm avoiding loosely coupled GNSS/IMU with multiple anti-spoofing techniques, a measurement deviation determination method is proposed to avoid a variety of anti-spoofing techniques, which can gradually pull the positioning results of the loosely coupled system, and successfully avoid the anti-spoofing techniques’ detection of innovation sequence monitoring and parameter rationality check so as to achieve the purpose of spoofing. In Section 4, experiments verify the effectiveness and concealment of the algorithm. In Section 5, we give a summary and outlook on the work of the paper.

2. Influence Mechanism of Spoofing on Loosely Coupled GNSS/IMU

2.1. Loosely Coupled GNSS/IMU System Model

Loosely coupled GNSS/IMU takes the error equation of GNSS and IMU as the system state equation, takes the difference of navigation information output by GNSS and IMU as the measurement, establishes the measurement equation, uses the optimal filter to fuse the two data and give the optimal estimation results, and finally feeds back to IMU for correction to realize high-precision navigation [19].

The measurement information used by loosely coupled GNSS/IMU is position difference and velocity difference, that is, the difference between position and velocity obtained by GNSS and position and velocity calculated by IMU is used as the input of the Kalman filter, and the output is closed-loop correction. The estimation result of the Kalman filter is used to correct the IMU measurement [19]. The block diagram of the loosely coupled structure is shown in Figure 1.

![Figure 1. Structure block diagram of loosely coupled GNSS/IMU system.](image)

Selecting the 15-dimensional IMU navigation parameter error as the state of the filter, closed-loop correction is carried out to correct the position, velocity and altitude of IMU.

2.2. Influence of Spoofing on Loosely Coupled GNSS/IMU

From the analysis of the composition mechanism of loosely coupled GNSS/IMU, when loosely coupled GNSS/IMU is spoofed by GNSS, firstly, the GNSS spoofing signal affects the positioning results of the GNSS output, and then affects the measured value of the Kalman filtering process of a loosely coupled system. Finally, the Kalman filter affects the error estimation of state parameters [18].
Suppose GNSS/IMU is in a normal working state before time \( i \), and GNSS/IMU is spoofed by GNSS spoofing at time \( i \), and then the measurement innovation vector of the system at time \( i \) is \( \delta \mathbf{z}_i + \Delta \mathbf{z}_i \), and \( \Delta \mathbf{z}_i \) represents the deviation of the measurement innovation vector introduced by GNSS spoofing. \( \delta \mathbf{z}_i \) is expressed as

\[
\delta \mathbf{z}_i + \Delta \mathbf{z}_i = \left[ \delta \mathbf{z}_{i,j} + \Delta \mathbf{z}_{i,j} \right] = \left[ \delta \mathbf{e}_i \mathbf{GNSS} - \delta \mathbf{e}_i \mathbf{IMU} + \Delta \mathbf{e}_i \mathbf{GNSS} \right]
\]

(1)

In the above formula, \( \Delta \mathbf{e}_i \mathbf{GNSS} \) represents the position deviation at time \( i \), and \( \Delta \mathbf{e}_i \mathbf{GNSS} \) represents the velocity deviation at time \( i \). \( \Delta \mathbf{z}_{r,j} \) and \( \Delta \mathbf{z}_{v,j} \) represent the deviation of the position innovation vector and velocity innovation vector, respectively.

In the process of GNSS spoofing, \( P_i, Q_i, R_i \) and gain matrix \( K_i \) of Kalman filter can be approximately unchanged, and the GNSS/IMU error estimation under GNSS spoofing can be obtained as follows:

\[
\hat{X}_i = \Phi_{i,j-1} \hat{X}_{i-1} + K_i \left( \delta \mathbf{z}_i + \Delta \mathbf{z}_i \right) \]

(2)

Since the GNSS/IMU output results are IMU navigation parameters corrected by error estimation, error estimation deviation is the system deviation of GNSS/IMU. Therefore, the system deviation expression of GNSS/IMU is

\[
\Delta \hat{X}_i = \hat{X}_i - \mathbf{X}_i = \left\{ \begin{array}{l}
K_i \Delta \mathbf{z}_i \\
(I - K_i \mathbf{H}) \Phi_{i,j-1} \Delta \hat{X}_{i-1} + K_i \Delta \mathbf{z}_i 
\end{array} \right., \quad i = 2, 3, \ldots 
\]

(3)

In the above formula, when \( i \geq 2 \), \( \Delta \hat{X}_i \) represents the cumulative value of the GNSS/IMU system deviation.

3. Slowly Varying Spoofing Algorithm to Avoid Multiple Anti-Spoofing Techniques

3.1. Avoiding Innovation Sequence Monitoring

In the Kalman filtering process of the loosely coupled GNSS/IMU system, innovation sequence monitoring can be used to detect small anomalies in a certain period of time [19]. For the GNSS spoofing method of slowly pulling the positioning of the loosely coupled system, it is difficult for single epoch innovation detection to detect the gradually accumulated measurement error introduced by spoofing, and innovation sequence monitoring is an effective spoofing detection method to test the small and slowly accumulated deviation between the measurement and state estimation through the recent \( n \) normalized innovation vectors. Normalized innovation is defined as

\[
y_{ij} = \frac{Z_{ij} - H_{ij} \hat{X}_{i/j-1}}{\sqrt{S_{i,j,j}}} 
\]

(4)

where \( Z_{ij} \) is the \( j \)-th component of measurement vector \( Z_i \) at time \( i \), \( H_{ij} \) is the \( j \)-th line component of measurement matrix at time \( i \), \( \hat{X}_{i/j-1} \) is the predicted value of \( \mathbf{X}_i \) calculated by \( \hat{X}_{i-1} \), \( Z_{ij} - H_{ij} \hat{X}_{i/j-1} \) is a measurement innovation vector of \( Z_{ij} \), \( S_{i,j,j} \) represents the \( (j,j) \)-th value of the innovation covariance \( S_i \), and \( S_i \) is the sum of measurement noise covariance and error covariance of state estimation converted to measurement space, that is

\[
S_i = H P_{i/j-1}^T H^T + R 
\]

(5)

where \( R \) is the measurement noise variance matrix.
The test statistic $u_{ij}$ is composed of the latest $n$ measurements to detect the smaller and slowly accumulated deviation between the measurement and state estimation:

$$u_{ij} = \frac{1}{n} \sum_{i=k+1-n}^{k} y_{ij}$$

(6)

where $n$ is the independent samples of zero mean unit variance Gaussian distribution, and the standard deviation of its mean is $1/\sqrt{n}$. If the absolute value of $u_{ij}$ exceeds the threshold $\frac{T_u}{\sqrt{n}}$, the navigation system sends an alarm and considers that the measured value is abnormal. That is, the alarm judgment criteria are

$$\left\{ \begin{array}{ll}
|u_{ij}| > \frac{T_u}{\sqrt{n}}, & \text{Alarm} \\
|u_{ij}| \leq \frac{T_u}{\sqrt{n}}, & \text{Not Alarm}
\end{array} \right.$$

(7)

where $T_u$ is the innovation threshold, which can be determined according to Gaussian distribution.

In order to make spoofing have good concealment, it should meet $|u_{ij}| \leq \frac{T_u}{\sqrt{n}}$. Next, calculate the value range of single epoch measurement deviation according to the threshold of $|u_{ij}|$. To satisfy $|u_{ij}| \leq \frac{T_u}{\sqrt{n}}$, convert the problem to $|y_{ij}| \leq \frac{T_u}{\sqrt{n}}$ for each epoch. In fact, satisfying $|y_{ij}| \leq \frac{T_u}{\sqrt{n}}$ is a sufficient and unnecessary condition to satisfy $|u_{ij}| \leq \frac{T_u}{\sqrt{n}}$. Therefore, if the single epoch satisfies $|y_{ij}| \leq \frac{T_u}{\sqrt{n}}$, it must satisfy $|u_{ij}| \leq \frac{T_u}{\sqrt{n}}$.

The single epoch is analyzed below. Solve $|y_{ij}| \leq \frac{T_u}{\sqrt{n}}$ to obtain

$$\left\{ \begin{array}{ll}
H_{ij} \hat{X}_{i/i-1} - T_u \sqrt{\frac{S_{i|i-1}}{n} + \hat{\sigma}^2_{eb,j}} \leq \hat{\theta}^e_{eaG,j} \leq \left( H_{ij} \hat{X}_{i/i-1} + T_u \sqrt{\frac{S_{i|i-1}}{n} + \hat{\sigma}^2_{eb,j}} \right) \\
H_{ij} \hat{X}_{i/i-1} - T_u \sqrt{\frac{S_{i|i-1}}{n} + \hat{\sigma}^2_{eb,j}} \leq \hat{\theta}^e_{eaG,j} \leq \left( H_{ij} \hat{X}_{i/i-1} + T_u \sqrt{\frac{S_{i|i-1}}{n} + \hat{\sigma}^2_{eb,j}} \right)
\end{array} \right.$$

(8)

The above formula shows that when spoofing loosely coupled GNSS/IMU, in order to avoid innovation sequence monitoring, the output position $\hat{X}_{eaG,i}$ and velocity $\hat{v}^e_{eaG,i}$ of GNSS spoofing signal cannot change arbitrarily, and the value range of Formula (8) needs to be met.

3.2. Avoiding Parameter Rationality Check

Loosely coupled GNSS/IMU can detect faults and even spoofing through the parameter rationality check. The parameter rationality check includes the sensor output, navigation parameters and Kalman filter estimation [19]. Check the output of the sensors to respond to simple spoofing. Checking the navigation parameters provides additional protection. Checking the Kalman filter estimation can check slow faults and even spoofing.

Next, the spoofing algorithm to avoid the parameter rationality check is proposed from the perspective of the spoofer. Firstly, the influence of gain matrix $K_e$ in the Kalman filtering process on GNSS spoofing is analyzed. $K_{\infty}$ represents the stable state of $K_e$, and $K_{\infty}$ is the $15 \times 6$ matrix. According to Formula (3), the relationship between the system deviation of GNSS/IMU and measured deviation can be expressed in the following matrix form:
where in, $\Delta X$, $\Delta Y$ and $\Delta Z$ represent position measurement deviation under the ECEF coordinate system, and $\Delta V_x$, $\Delta V_y$ and $\Delta V_Z$ represent the velocity measurement deviation under ECEF coordinate system.

For the spoofer, in order to ensure that the spoofing deviation can achieve the purpose of spoofing, GNSS spoofing shall make single epoch position deviation $\Delta \delta x$, $\Delta \delta y$ and $\Delta \delta z$ of the GNSS/IMU system introduced to target the desired position deviation $\Delta \delta x_{Ex}$, $\Delta \delta y_{Ex}$ and $\Delta \delta z_{Ex}$ as far as possible; at the same time, the constraint condition of single epoch velocity deviation $\Delta \delta v_x$, $\Delta \delta v_y$ and $\Delta \delta v_z$ of the GNSS/IMU system introduced into the target is the absolute value of the velocity deviation which meets the absolute value of the position deviation to which it is less than or equal. In fact, if GNSS spoofing has too much impact on the altitude estimation of the target, the expected purpose of spoofing may not be achieved. The reasons are that, on the one hand, the target (such as UAV) is more sensitive to altitude change relative to the position and velocity change, and the spoofing detection means of the target is easier to detect the abnormality of altitude estimation; on the other hand, if GNSS spoofing causes the altitude change to exceed the physical threshold of the target, it is easy to cause motion failure of the target [20] and it cannot be induced to the expected position by the spoofer. Therefore, GNSS spoofing should keep single epoch altitude angle deviation values $\Delta \delta \phi$, $\Delta \delta \theta$ and $\Delta \delta \phi$ of GNSS/IMU system introduced into target as normal as possible. To sum up, the formula can be expressed as

$$
\begin{align*}
\Delta \delta x & \approx \Delta \delta x_{Ex} \\
\Delta \delta y & \approx \Delta \delta y_{Ex} \\
\Delta \delta z & \approx \Delta \delta z_{Ex}
\end{align*}
$$

If biases estimated by the loosely coupled GNSS/IMU Kalman filter exceeds five times the nominal value, it is considered that the sensor may be faulty [15]. Here, when
GNSS spoofing is implemented, the bias caused by spoofing shall not exceed five times the nominal biases. That is, (9) shall meet the following constraints:

$$
\begin{align*}
\Delta \varepsilon_{lx} &\leq T_{5r1} \\
\Delta \varepsilon_{ly} &\leq T_{5r2} \\
\Delta \varepsilon_{lz} &\leq T_{5r3} \\
\Delta g_{lx} &\leq T_{5r4} \\
\Delta g_{ly} &\leq T_{5r5} \\
\Delta g_{lz} &\leq T_{5r6}
\end{align*}
$$

(11)

where $T_{5r1}$, $i = 1, 2, \cdots, 6$ represents five times the nominal biases of $b_{ax}$, $b_{ay}$, $b_{az}$, $b_{gx}$, and $b_{gy}$, $b_{gz}$ respectively.

According to (9), the spoofer calculates the measurement deviation required for spoofing according to the system deviation of the GNSS/IMU required for a single epoch and estimated gain matrix $K_i$. The position constraint in (10) is taken as the objective function of the product of gain matrix $K_i$ and measured value deviation; (11) is taken as the constraints to solve the optimal measured value deviation.

In combination with Section 3.1 and this section, the spoofing quantity is solved by the method in Section 3.2 to avoid the parameter rationality check. At this time, the loosely coupled GNSS/IMU system uses an innovation sequence monitoring algorithm for spoofing detection. In this case, it is necessary to reconsider spoofing quantity $\hat{\Delta z}_j^\prime$ to avoid innovation sequence monitoring. Based on this, $\hat{\delta z}_k^\prime$ needs to satisfy (8), so (8) is also used as the constraint condition in Section 3.2 to resolve $\Delta z_j$ that is not detected by the innovation sequence monitoring. In conclusion, the flow of the proposed slowly varying spoofing algorithm avoiding loosely coupled GNSS/IMU with multiple anti-spoofing techniques is shown in Figure 2.

According to Figure 2, the proposed algorithm can be described in detail as follows: after the spoofing signal completely takes over the GNSS tracking loop, the spoofer first determines the target location of spoofing. After comprehensively considering the parameter rationality check and innovation sequence monitoring of the loosely coupled system, the reasonable spoofing offset of each epoch is calculated to avoid the detection of the above anti-spoofing techniques and ensure that the positioning result of the loosely coupled GNSS/IMU is slowly changed. If the coupled system has not been spoofed to the target location after one spoofing, the spoofing algorithm will continue to be executed. Finally, it is spoofed to the target position so as to gradually achieve the purpose of spoofing.
Figure 2. Flow chart of spoofing loosely coupled GNSS/IMU algorithm.

4. Simulation Analysis

Based on the MATLAB simulation software provided by [19], we modified and upgraded the software to realize the experimental work of this paper. The experimental environment can well show the spoofing effect of spoofing signal on loosely coupled...
GNSS/IMU. In the experimental environment, the spoofing signal is fully controllable to the spoofer.

In the simulation experimental scenario, the real state of loosely coupled GNSS/IMU equipment always remains stationary at point O. The IMU in the loosely coupled system is tactical-grade IMU, and the device parameters are shown in Table 1.

Table 1. Parameters of tactical-grade IMU.

| Parameter                  | Value               | Unit  |
|----------------------------|---------------------|-------|
| IMU accelerometer biases   | [900; −1300; 800]   | µg    |
| IMU accelerometer noise root PSD | 100              | µg/√HZ|
| IMU gyro biases            | [−9; −13; −8]       | ◦/h   |
| IMU gyro noise root PSD    | 0.01                | ◦/√h  |

In the experiment, the parameter settings of the loosely coupled GNSS/IMU Kalman filter are shown in Table 2:

Table 2. Parameters setting of Kalman filter for loosely coupled system.

| Parameter                   | Value          | Unit     |
|-----------------------------|----------------|----------|
| Accelerometer bias random walk PSD | $10^{-7}$     | m²/s²    |
| Gyro bias random walk PSD    | $2 \times 10^{-12}$ | rad²/s³ |
| Position measurement noise SD | 2.5           | m        |
| Velocity measurement noise SD | 0.1           | m/s      |

At the initial time, the output positioning result of the loosely coupled system is the O point, and at this time, the loosely coupled system is taken over by the GNSS spoofing signal. The purpose of the GNSS spoofer is to offset the positioning result of the loosely coupled GNSS/IMU system to point S, which deviates from point O by 30 m to the north, 30 m to the east and 30 m down.

Figures 3–5 show the north, east and down position offsets of the loosely coupled GNSS/IMU system without spoofing and with spoofing, respectively. The blue line indicates no spoofing, and the red line indicates spoofing.

Figure 3. North displacement without/with spoofing.
As shown in Figures 3–5, when the loosely coupled system is spoofed by slowly varying spoofing, the north displacement gradually shifts by 29.8 m in the period of 0–66 s, and stabilizes around 29.8 m in the period of 66–120 s; in the 0–15 s period, eastward displacement gradually shifts by 32.3 m, and in the 15–120 s period, the eastward displacement is stable around 32.3 m; in the period of 0–66 s, down displacement gradually deviates by 43.2 m; and in the period of 66–120 s, down displacement is stable around 43.2 m. In terms of the spoofing effect, the north displacement basically achieves a spoofing effect, and the error between the north displacement and expected offset is −0.2 m; the east displacement basically achieves a spoofing effect, and the error between the east displacement and expected displacement is 2.3 m; the down ground displacement also basically achieves a spoofing effect, but the effect is slightly worse than that in the north and east directions, and the error with the expected offset is 13.2 m.
Figures 6–8 show the north, east and down velocities of the loosely coupled GNSS/IMU system without spoofing and with spoofing, respectively. The blue line indicates no spoofing, and the red line indicates spoofing.

Figure 6. North velocity without/with spoofing.

Figure 7. East velocity without/with spoofing.
As shown in Figures 6–8, when the loosely coupled system is spoofed by slowly varying spoofing, although there is a small fluctuation in the north velocity compared with the case without spoofing, it can always remain greater than \(-0.02\) m/s and less than \(1.94\) m/s; although the east velocity fluctuates slightly, it can always remain greater than \(-0.43\) m/s and less than \(1.3\) m/s; although the down velocity fluctuates slightly, it can always remain greater than \(-0.98\) m/s and less than \(0.24\) m/s. To sum up, the velocity change of the loosely coupled system conforms to the parameter rationality check, and is also close to the velocity change without spoofing.

Figures 9–11 show the changes of the roll angle, pitch angle and yaw angle of the loosely coupled GNSS/IMU system without spoofing and with spoofing, respectively. The blue line indicates no spoofing, and the red line indicates spoofing.
Figure 10. Pitch angle without/with spoofing.

Figure 11. Yaw angle without/with spoofing.

As shown in Figures 9–11, when the loosely coupled system is spoofed by slowly varying spoofing, although the roll angle fluctuates slightly compared with the case without spoofing, it can always remain greater than $-0.21^\circ$ and less than $1.88^\circ$; although the pitch angle fluctuates slightly, it can always remain greater than $-2.07^\circ$ and less than $0.25^\circ$; although the yaw angle fluctuates slightly, it can always remain greater than $-11.21^\circ$ and less than $1.01^\circ$. To sum up, the change of the loosely coupled altitude angle is also close to the change of the altitude angle without spoofing.

Figures 12 and 13 show the changes of each test statistic $\sqrt{\sum_{i,j} (\hat{x}_{ij})^2}$ of the loosely coupled GNSS/IMU system without spoofing and with spoofing, respectively. Here, the threshold $T_u$ is set to 50. $P_x$, $P_y$, $P_z$, $V_x$, $V_y$ and $V_z$ respectively represent the test statistics of the position in the X direction, Y direction and Z direction; the test statistics of the velocity in the X direction, Y direction and Z direction in the ECEF coordinate system; and the red line represents the alarm threshold line.
The test statistics in Figures 12 and 13 are analyzed, and the results are shown in Table 3.

As shown in Figures 12 and 13, when loosely coupled GNSS/IMU is spoofed by slowly varying spoofing, although the test statistics of the loosely coupled system increase compared with the case without spoofing, they do not exceed the alarm threshold. To sum up, when the loosely coupled system is spoofed by slowly spoofing, its test statistics will not raise an alarm.

Figures 14 and 15 show the changes of the clock offset estimation and clock drift estimation of loosely coupled GNSS/IMU without spoofing and with spoofing, respectively. The blue line indicates no spoofing, and the red line indicates spoofing.
Table 3. Analysis of test statistics of loosely coupled without/with spoofing.

| Test Statistics | Without/With Spoofing | Average | Maximum |
|-----------------|----------------------|---------|---------|
| Px              | Without              | 0.29    | 0.85    |
|                 | With                 | 6.23    | 11.27   |
| Py              | Without              | 0.22    | 0.63    |
|                 | With                 | 2.18    | 7.05    |
| Pz              | Without              | 0.37    | 0.99    |
|                 | With                 | 27.12   | 37.39   |
| Vx              | Without              | 0.20    | 0.68    |
|                 | With                 | 3.86    | 13.08   |
| Vy              | Without              | 0.18    | 0.80    |
|                 | With                 | 2.44    | 10.21   |
| Vz              | Without              | 0.23    | 2.20    |
|                 | With                 | 3.60    | 6.32    |

Figure 14. Clock offset without/with spoofing.

Figure 15. Clock drift without/with spoofing.
As shown in Figures 14 and 15, when the loosely coupled system is spoofed by slowly varying spoofing, the estimated loosely coupled clock offset is close to the same, compared with the case without spoofing; although the estimated clock drift fluctuates slightly, it can always remain greater than 99.7 m/s and less than 100.1 m/s. To sum up, the changes of the loosely coupled clock offset estimation and clock drift estimation are also close to those without spoofing.

Figures 16 and 17 show the changes of the accelerometer biases estimation and gyro biases estimation of the loosely coupled GNSS/IMU system without spoofing. The red line, green line and blue line respectively represent the X, Y and Z axis directions along the body coordinate.

Figure 16. Accelerometer biases without spoofing.

Figure 17. Gyro biases without spoofing.

Figures 18 and 19 show the changes of the accelerometer biases estimation and gyro biases estimation of the loosely coupled GNSS/IMU system with spoofing. The red line,
green line and blue line respectively represent the X, Y and Z axis directions along the body coordinate.

Figure 18. Accelerometer biases with spoofing.

Figure 19. Gyro biases with spoofing.

As shown in Figures 16–19, when the loosely coupled system is spoofed by slowly varying spoofing, compared with the case without spoofing, although the estimated acceleration biases fluctuate slightly in the X direction, it can always remain greater than $-1.2 \times 10^{-3}$ m/s$^2$ and less than $5.8 \times 10^{-3}$ m/s$^2$; although there is a small fluctuation in the Y direction, it can always remain greater than $-1.1 \times 10^{-3}$ m/s$^2$ and less than $7.9 \times 10^{-3}$ m/s$^2$; and although there is a small fluctuation in the Z direction, it can always remain greater than $-1.0 \times 10^{-3}$ m/s$^2$ and less than $4.8 \times 10^{-2}$ m/s$^2$. Although the estimated gyro biases fluctuate slightly in the X direction, it can always remain greater than $-2.6 \times 10^{-4}$ rad/s and less than $6.1 \times 10^{-5}$ rad/s; although there is a small fluctuation in the Y direction, it can always remain greater than $-2.9 \times 10^{-4}$ rad/s and less than
1.5 \times 10^{-4} \text{ rad/s}; and although there is a small fluctuation in the Z direction, it can always remain greater than 0 and less than 2.1 \times 10^{-5} \text{ rad/s}. To sum up, the variation of the biases estimation of the accelerometer and gyro is also close to the variation without spoofing.

Based on the above experimental analysis, in terms of the spoofing effect, the north displacement completely achieves the spoofing effect, and errors with the expected offset are $-0.2 \text{ m}$; the east displacement basically achieves the spoofing effect, and the error with expected offset is $2.3 \text{ m}$; the down displacement also basically achieves the spoofing effect, but the effect is slightly worse than that in the north and east directions, and error with the expected offset is $13.2 \text{ m}$. When slowly varying spoofing is applied to a loosely coupled system, the velocity change of the loosely coupled system is close to the velocity change of that without spoofing, and the change of the altitude angle is also close to the change of the altitude angle without spoofing. At the same time, its test statistics will not raise an alarm, and the changes of the accelerometer bias estimation and gyro bias estimation of a tightly coupled system are also close to the change without spoofing.

5. Conclusions and Future Work

In order to effectively counter the non-cooperative target of an assembly integrated navigation system by using spoofing technology, a new spoofing algorithm needs to be proposed. In order to effectively counter the non-cooperative target of assembling a loosely coupled GNSS/IMU by using GNSS spoofing, based on the analysis of the influence mechanism of spoofing on the positioning of loosely coupled GNSS/IMU, a slowly varying spoofing algorithm to avoid loosely coupled GNSS/IMU with multiple anti-spoofing techniques is proposed, and a measurement deviation determination method to avoid multiple anti-spoofing techniques is proposed, which can gradually pull the positioning results of coupled system and successfully avoid anti-spoofing techniques’ detection of innovation sequence monitoring and a parameter rationality check. The experimental results show that the proposed algorithm gradually changes the positioning of the loosely coupled GNSS/IMU; the north and east displacements achieve the purpose of spoofing; and the errors with the expected offset are $-0.2 \text{ m}$ and $2.3 \text{ m}$, respectively. The down displacement also basically achieves the purpose of spoofing, and the error with the expected offset is $13.2 \text{ m}$. At the same time, it avoids the detection of multiple anti-spoofing techniques, does not trigger the system alarm, and realizes the purpose of spoofing, thus the effectiveness and high concealment of the spoofing algorithm are verified. The research results provide an effective solution for the target equipped with a loosely coupled GNSS/IMU system to implement GNSS spoofing. On the other hand, it also provides reference for a loosely coupled GNSS/IMU system to detect and suppress GNSS spoofing.

The research work of this paper, which needs to be improved in the follow-up research, may be that the spoofing in the experiment is positioning spoofing, and the set spoofing destination is not very complex. Future research work will focus on, first, how to spoof the more complex coupled system of GNSS and IMU, and second, how to spoof more complex anti-spoofing techniques to deal with the threat of unknown moving objects.

**Author Contributions:** Methodology, Y.G.; writing—original draft preparation, Y.G.; writing—review and editing, Y.G. and G.L. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research was funded by State Key Laboratory of Geo-Information Engineering, grant number SKLGIE2020-Z-2-1.

**Institutional Review Board Statement:** Not applicable.

**Informed Consent Statement:** Not applicable.

**Data Availability Statement:** The data used in this research are not publicly available.

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

1. Humphreys, T.E.; Ledvina, B.M.; Psiaki, M.L.; O’Hanlon, B.W.; Kintner, P.M. Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofor. In Proceedings of the 21st International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS 2008), Savannah Convention Center Savannah, Savannah, GA, USA, 16–19 September 2008; pp. 1169–1180.

2. Liu, Y.; Li, S.; Fu, Q.; Liu, Z.; Zhou, Q. Analysis of Kalman Filter Innovation Based GNSS Spoofing Detection Method for INS/GNSS Integrated Navigation System. IEEE Sens. J. 2019, 19, 5167–5178. [CrossRef]

3. Scott, L. Anti-Spoofing and Authenticated Signal Architectures for Civil Navigation Systems. In Proceedings of the 16th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GPS/GNSS 2003), Portland, OR, USA, 9–12 September 2003; pp. 1543–1552.

4. Warner, J.S.; Johnston, R.G. A Simple Demonstration that the Global Positioning System (GPS) is Vulnerable to Spoofing. J. Secur. Adm. 2002, 25, 19–27.

5. Shepard, D.P.; Bhatti, J.A.; Humphreys, T.E.; Fansler, A.A. Evaluation of Smart Grid and Civilian UAV Vulnerability to GPS Spoofing Attacks. In Proceedings of the 25th International Technical Meeting of Satellite Division of the Institute of Navigation, Nashville, TN, USA, 17–21 September 2012; pp. 2743–2757.

6. Lu, Q.; Feng, X.Z.; Zhou, C. A Detection and Weakening Method for GNSS Time-Synchronization Attacks. IEEE Sens. J. 2021, 21, 19069–19077. [CrossRef]

7. Erick, S.; Junhwan, L.; Nikolaos, G.; Akopian, D. Rejection of Smooth GPS Time Synchronization Attacks via Sparse Techniques. IEEE Sens. J. 2021, 21, 776–789.

8. Borio, D.; Gioia, C. Interference mitigation: Impact on GNSS timing. GPS Solut. 2021, 20, 37. [CrossRef]

9. Hu, Y.; Biaı, S.; Li, B.; Zhou, L. A novel array-based spoofing and jamming suppression method for GNSS receiver. IEEE Sens. J. 2018, 18, 2952–2958. [CrossRef]

10. Li, J.; Zhu, X.; Ouyang, M.; Li, W.; Chen, Z.; Fu, Q. GNSS Spoofing Jamming Detection Based on Generative Adversarial Network. IEEE Sens. J. 2021, 21, 10. [CrossRef]

11. Psiaki, M.L.; Humphreys, T.E. GNSS Spoofing and Detection. Proc. IEEE 2016, 104, 1258–1270. [CrossRef]

12. Gao, Y.; Lv, Z.; Zhang, L. Asynchronous Lift-Off Spoofing on Satellite Navigation Receivers in the Signal Tracking Stage. IEEE Sens. J. 2020, 20, 8604–8613. [CrossRef]

13. Khanafseh, S.; Roshan, N.; Langel, S.; Chan, F.C.; Pervan, B. GPS spoofing detection using RAIM with INS coupling. In Proceedings of the IEEE/ION Position, Location and Navigation Symposium-planes, Monterey, CA, USA, 5–8 May 2014.

14. Shi, M.; Mu, J.Y.; Chen, S.X. Bias Analysis of GPS/INS Integrated Navigation Under GPS Deception. Electron. Opt. Control 2016, 23, 16–20.

15. 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]

16. Xu, R.; Ding, M.; Qi, Y.; Yue, S.; Liu, J. Performance Analysis of GNSS/INS Loosely Coupled Integration Systems under Spoofing Attacks. Sensors 2018, 18, 4108. [CrossRef] [PubMed]

17. 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]

18. Gao, Y.; Lv, Z.; Zhang, L. Two-step Trajectory Spoofing Algorithm for Loosely Coupled GNSS/IMU and NIS Sequence Detection. IEEE Access 2019, 7, 96359–96371. [CrossRef]

19. Groves, P.D. Principles of GNSS, Inertial, and Multisensor Integrated Navigation Systems, 2nd ed.; Artech House: Norwood, MA, USA, 2013.

20. Guo, Y. Research on Covert Spoofing Algorithm of UAV Based on INS/GNSS Integrated Navigation. Ph.D. Thesis, National University of Defense Technology, Changsha, China, 2019.