A Slowly Varying Spoofing Algorithm Avoiding Tightly-Coupled GNSS/IMU With Multiple Anti-Spoofing Techniques

Yangjun Gao and Guangyun Li

***Abstract*—Vehicle and airborne navigation users are facing more and more complex signal interference and even spoofing. If vehicles and aircraft do not strengthen their anti-spoofing ability, their navigation performance is bound to be adversely affected. global navigation satellite system (GNSS) spoofing technology has gradually become a preferred interference method for spoofer because of its high concealment and great harm. For spoofer, user terminal increasingly adopts GNSS with inertial measurement unit (IMU): tightly-coupled GNSS/IMU, on this basis, user also configures a variety of anti-spoofing techniques to effectively deal with spoofing. Even if spoofer slowly changes user's positioning, if spoofing strategy is unreasonable, it will lead to the violation of parameter rationality of coupled filter output parameters and spoofing observation, which greatly increases the difficulty of spoofing. In view of the above problems, from the perspective of spoofer, in order to effectively counter the non cooperative target of assembling tightly-coupled GNSS/IMU by using GNSS spoofing, this paper establishes GNSS spoofing mathematical model, and proposes a slowly varying spoofing algorithm to avoid tightly-coupled GNSS/IMU with multiple anti-spoofing techniques based on the analysis of the influence mechanism of spoofing on the positioning of tightly-coupled GNSS/IMU, the algorithm proposes a measurement deviation determination method to avoid a variety of anti-spoofing techniques, which can gradually pull the positioning results of coupled system, and successfully avoid anti-spoofing techniques detection of least squares residual receiver autonomous integrity monitoring (RAIM) and parameter rationality check. The experimental results show that the algorithm can gradually change positioning of tightly-coupled GNSS/IMU within 30 s, and the north, east and down displacements basically achieve the spoofing effect, the errors with the expected offset are −0.5 m, 1.9 m and 12.7 m respectively. At the same time, the detection of the above anti-spoofing techniques is avoided. The mean value of test statistics for tightly-coupled system is reduced by 75.4% and does not exceed the alarm threshold, so as to achieve the purpose of spoofing, the effectiveness and high concealment of the spoofing algorithm are proved.**

Manuscript received 22 December 2021; revised 9 April 2022; accepted 9 May 2022. Date of publication 11 May 2022; date of current version 15 August 2022. This work was supported in part by the State Key Laboratory of Geo-Information Engineering, under Grant SKLGIE2020-Z-2-1 and in part by the National Natural Science Foundation of China under Grant 42174036. The review of this article was coordinated by Prof. Yi Qian. *(Corresponding author: Guangyun Li.)*

Yangjun Gao is with the PLA Strategic Support Force Information Engineering University, Henan 450001, China, and also with the State Key Laboratory of Geo-Information Engineering, Xi'an 710054, China (e-mail: 951242669@qq.com).

Guangyun Li is with the State Key Laboratory of Geo-Information Engineering, Xi'an 710054, China (e-mail: guangyun_li_chxy@163.com).

Digital Object Identifier 10.1109/TVT.2022.3174406

***Index Terms*—Anti-spoofing techniques, least squares residual RAIM, rationality check, slowly varying spoofing, tightly-coupled GNSS/IMU.**

I. Introduction

With the construction and vigorous development of global navigation satellite system (GNSS), satellite navigation and positioning technology has been widely used in many fields of civil and military. Due to the inherent vulnerability of satellite navigation signals, vehicle and aircraft users are facing more and more complex signal interference and even spoofing. If the anti-spoofing ability of vehicles and aircraft is not strengthened, their navigation performance is bound to be adversely affected [1]. Among them, GNSS spoofing technology has gradually become a popular interference technology for spoofer because of its high concealment and great harm [2]–[4]. In 2012, Todd E. Humphreys team used low-cost GPS spoofer to lower the unmanned helicopter that should have maintained a fixed altitude [5].

It should be noted that spoofing technology can be used for positive purposes, such as using spoofing to control and even counter non cooperative unmanned aerial vehicles, protecting the location information of sensitive areas, etc. In fact, anti UAV using spoofing technology is an effective soft killing means [6], [7]. On the other hand, users increasingly adopt the tightly-coupled GNSS/IMU to deal with spoofing. On the basis of sensor combination, users configure anti-spoofing algorithm, for example, receiver autonomous integrity monitoring (RAIM) and parameter rationality inspection of integrated navigation filtering results [8], the above means greatly increase the difficulty for spoofer to realize spoofing. In order to effectively counter the unknown object equipped with integrated navigation system by using spoofing technology, it is very necessary to research new spoofing algorithms.

Considering the navigation strategy of coupled targets, GNSS spoofing can gradually increase the cumulative error of integrated navigation device, and even affect the SLAM (Simultaneous Localization and Mapping) function of some unmanned platforms [9]. When the difference between position velocity and time (PVT) and real PVT is large, the user can detect spoofing by comparing with measurement results of other sensors. Therefore, it is necessary to gradually pull the PVT results to make the variation within the allowable range of sensor error [10]. For example, intermediate

spoofing can make the loop gradually controlled by spoofing signal without inter-rupting the tracking state of receiver [11], [12].

II. Related Work

The research on spoofing coupled system is summarized as follows. Experiments by Zhen han *et al.* show that forwarding spoofing can effectively affect tightly-coupled solution results, and Chi-Square verification method can effectively identify step-type spoofing and slope-type spoofing, among them, residual Chi-Square verification method has more obvious identification effect on spoofing [13]. For tightly-coupled GPS/INS system, Samer Khanafseh *et al.* proposed a GPS/INS spoofing detection method based on residual RAIM, which can evaluate the integrity risk of the position solution and probability of missed detection. If spoofer is difficult to grasp real trajectory of the target, the experimental results show that integrity risk is negligible [10]. However, if spoofer fully grasps real trajectory of target, spoofer can order target to produce large position error without being detected by this method. Actually, normalized innovation squared (NIS) detection of navigation system is also a direct, effective and feasible spoofing detection method, which has been mature and applied to navigation system of unmanned platform [14]. Shuhai Lu *et al.* show that the Kalman filter correction gain matrix element in tightly-coupled navigation system always maintains its stability whether there is GNSS spoofing or not. Based on this characteristic, a spoofing control strategy that can realize accurate position offset is proposed: firstly, the specific spoofing signal is taken over the target tightly-coupled navigation terminal, pseudorange spoofing signals corresponding to different satellites are respectively the projection of the position increment to be spoofed on the line of sight vector of different satellites. Simulation experiments verify the correctness and effectiveness of the spoofing control strategy [15]. In addition, the data fusion algorithm based on factor graph optimization can effectively reduce the linearization error to achieve higher positioning accuracy of coupled GNSS/IMU system [16]. Wen *et al.* analyzed the accuracy of the fusion algorithm based on EKF and factor graph optimization, the latter showed better positioning performance [17].

To sum up, the difficulty of the current spoofing coupled system is that even if the spoofer gradually changes the position of coupled system, spoofer should pay close attention to whether the spoofing process leads to abnormal changes in other filter estimators of coupled system; In addition, although tightly-coupled system itself has good anti-spoofing ability, if coupled system is additionally equipped with other anti-spoofing techniques, spoofer needs to consider how to introduce appropriate amount of spoofing in order to make spoofing process as imperceptible as possible.

The research work of this paper is briefly summarized as follows: when spoofing signal completely cuts into and takes over the GNSS module of coupled system, based on the analysis of influence mechanism of spoofing on positioning of tightly-coupled GNSS/IMU, a slowly varying spoofing algorithm avoiding tightly-coupled GNSS/IMU with multiple anti-spoofing techniques is proposed, and a measurement deviation determination method avoiding multiple anti-spoofing techniques is proposed, it can gradually pull the positioning results of coupled system, and successfully avoid the detection of anti-spoofing techniques of least squares residual RAIM and parameter rationality check, so as to achieve the purpose of spoofing. Finally, experiments verify the effectiveness and concealment of the algorithm.

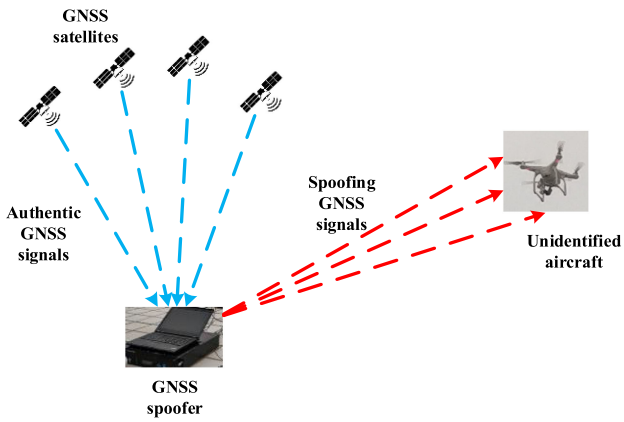

Fig. 1. Schematic diagram of GNSS spoofing scenario.

III. Influence Mechanism of Spoofing on Tightly-Coupled GNSS/IMU

A. Mathematical Model of GNSS Spoofing

GNSS spoofing can be divided into generating spoofing and forwarding spoofing according to the generation mode of spoofing signal. Generative spoofing can independently generate spoofing signal with the same structure as authentic GNSS signal. Forwarding spoofing refers to transmitting the received authentic GNSS signal with a certain delay after power adjustment. GNSS spoofing scenario is shown in Fig. 1. Fig. 1 shows that GNSS spoofer is used to spoof the unidentified aircraft. GNSS spoofer first receives authentic GNSS signal from the sky, and spoofer generates spoofing signals after signal analysis, or directly forwards authentic signals to broadcast spoofing signals to unidentified aircraft, so as to achieve the purpose of controlling unidentified aircraft.

Firstly, GNSS spoofing signal is broadcast to tightly-coupled GNSS/IMU, and the process that spoofing signal takes over target to output wrong positioning result of spoofing signal is the signal spoofing stage. The complex signal model at this stage can be expressed as [18]:

$$r(nT_s) = \sum_{h=J^a} \sqrt{P_h^a} D_h^a(nT_s - \tau_h^a) c_h^a(nT_s - \tau_h^a) e^{j\varphi_h^a + j2\pi f_h^a nT_s} + \sum_{m=J^s} \sqrt{P_m^s} D_m^s(nT_s - \tau_m^s) c_m^s(nT_s - \tau_m^s) e^{j\varphi_m^s + j2\pi f_m^s nT_s} + \eta(nT_s) \quad (1)$$

TABLE I
DEFINITION OF PARAMETERS

Paramater	Definition
h	received authentic satellite signal
m	received spoofing satellite signal
J^a	sets of authentic signals
J^s	sets of spoofing signals
a	received authentic satellite signal
s	received spoofing satellite signal
T_s	sampling interval
P	received signal power
c	PRN code sequence
D	navigation message
φ	carrier phase of received signal
f	carrier Doppler frequency of received signal
τ	code phase of received signal
$\eta(nT_s)$	additive white Gaussian noise

Where, subscripts h and m respectively represent the received authentic satellite signal and spoofing signal, J^a and J^s are the sets of authentic and spoofing signals respectively, and superscript a and s respectively represent the received authentic satellite signal and spoofing signal. T_s is the sampling interval, P is the received signal power, c is the pseudo-random noise (PRN) code sequence, D is the navigation message, φ, f, τ respectively represent the carrier phase, carrier Doppler frequency and code phase of received signal, and $\eta(nT_s)$ is the additive white Gaussian noise with zero mean and σ_n^2 variance. To improve readability, the definition of parameters defined in Eq (1) are listed in Table I.

When spoofing signal takes over target GNSS loop, the process of controlling and guiding target to move according to spoofing trajectory is the trajectory spoofing stage. At this stage, GNSS positioning results can be changed by reasonably modifying satellite position and pseudorange observation. Assuming that the deviation of space rectangular coordinate $\boldsymbol{x}_i = [\,x_i,\, y_i,\, z_i\,]^{\mathrm{T}}$ of the ith satellite is $\Delta\mathbf{x}_i = [\,\Delta x_i,\, \Delta y_i,\, \Delta z_i\,]^{\mathrm{T}}$, and there is a deviation $\Delta\rho_i$ for the pseudorange ρ_i of the corresponding satellite, the observation equation of target receiver corresponding to the ith satellite is:

$$\bar{R}_i + \delta t_u + \Delta\delta t_u = \rho_i + \Delta\rho_i \tag{2}$$

Where, δt_u represents receiver clock offset (equivalent in m), and $\Delta\delta t_u$ represents the deviation of receiver clock offset caused by modifying pseudorange (equivalent in m). $\bar{R}_i$ is expressed as:

$$\begin{aligned}\bar{R}_i^2 = {} & [x_i + \Delta x_i - (x_u + \Delta x_u)]^2 \\ & + [y_i + \Delta y_i - (y_u + \Delta y_u)]^2 \\ & + [z_i + \Delta z_i - (z_u + \Delta z_u)]^2\end{aligned} \tag{3}$$

$\Delta x_u = [\,\Delta x_u,\, \Delta y_u,\, \Delta z_u\,]^{\mathrm{T}}$ represents the deviation of receiver space rectangular coordinates caused by modifying pseudorange and satellite position. The above observation equation is expanded by first-order Taylor in satellite space rectangular coordinate $\boldsymbol{x}_i = [\,x_i,\, y_i,\, z_i\,]^{\mathrm{T}}$, receiver space rectangular coordinate $\boldsymbol{x}_u = [\,x_u,\, y_u,\, z_u\,]^{\mathrm{T}}$ and receiver clock offset δt_u. if N satellites are used for pseudorange positioning, it can be obtained:

$$\boldsymbol{G}\delta \approx \Delta\rho + \Delta\boldsymbol{s} \tag{4}$$

Where, $\boldsymbol{G}$ represents the Jacobian matrix, which is only related to the geometric position of each satellite relative to the user, δ represents the deviation of receiver spatial rectangular coordinate and receiver clock offset caused by modifying pseudorange and satellite position, and $\Delta\rho + \Delta\boldsymbol{s}$ represents pseudorange and satellite position deviation vector of N satellites. According to the pseudorange positioning principle, (4) can be solved as:

$$\boldsymbol{\delta} \approx (\boldsymbol{G}^{\mathrm{T}}\boldsymbol{G})^{-1}\boldsymbol{G}^{\mathrm{T}}(\Delta\boldsymbol{s} + \Delta\rho) \tag{5}$$

According to (5), positioning and timing deviation caused by satellite space rectangular coordinate deviation can be calculated.

B. Tightly-Coupled GNSS/IMU System Model

Tightly-coupled GNSS/IMU uses IMU navigation parameter error, GNSS receiver clock offset and clock drift as the estimated parameters of the state equation. The IMU obtains position and velocity through inertial navigation solution, and then uses the output ephemeris of GNSS receiver to calculate the corresponding pseudorange and pseudorange rate. The difference between pseudorange and pseudorange rate predicted by IMU and the output pseudorange and pseudorange rate of GNSS receiver is taken as the measurement of Kalman filter of tightly-coupled GNSS/IMU. The estimated state error of IMU and GNSS is obtained through Kalman filter and fed back to IMU and GNSS for correction, the corrected IMU navigation parameter is the output of tightly-coupled GNSS/IMU system.

The tightly-coupled structure block diagram is shown in Fig. 2 [19].

Select IMU navigation parameter error and GNSS receiver clock offset and clock drift as the state of the filter, and the error state vector is:

$$\begin{aligned}\boldsymbol{X} = \big[& \delta\phi \quad \delta\theta \quad \delta\varphi \quad \delta v_x \quad \delta v_y \quad \delta v_z \quad \delta x \quad \delta y \quad \delta z \\ & b_{ax} \quad b_{ay} \quad b_{az} \quad b_{gx} \quad b_{gy} \quad b_{gz} \quad \delta t_u \quad \delta f_u \big]^{\mathrm{T}}\end{aligned} \tag{6}$$

Where, $\delta\phi, \delta\theta, \delta\varphi$ represent attitude angle error, $\delta v_x, \delta v_y, \delta v_z$ represent velocity error in Earth-centered, Earth-fixed (ECEF) coordinate system, δx, δy, δh respectively represent position

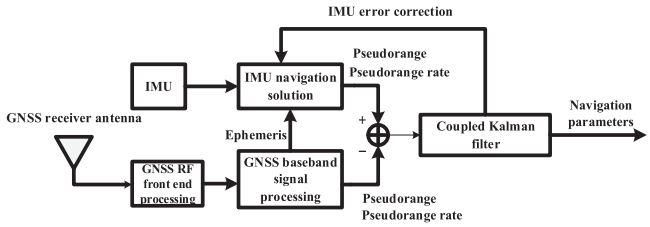

Fig. 2. Structure block diagram of tightly-coupled GNSS/IMU system.

error in ECEF coordinate system, b_{ax}, b_{ay}, b_{az} represent acceleration biases, b_{gx}, b_{gy}, b_{gz} represent gyro biases, δt_u represents receiver clock offset, δf_u represents receiver clock drift.

The system model of tightly-coupled GNSS/IMU is as follows:

The state transition matrix $\mathbf{\Phi}$ is expressed as:

$$\mathbf{\Phi} \approx \begin{bmatrix} \boldsymbol{I}_3 - \boldsymbol{\Omega}_{ie}^e \tau_s & 0_3 & 0_3 & 0_3 & \hat{\boldsymbol{C}}_b^e \tau_s & 0_1 & 0_1 \\ \boldsymbol{F}_{21}^e \tau_s & \boldsymbol{I}_3 - 2\boldsymbol{\Omega}_{ie}^e \tau_s & \boldsymbol{F}_{23}^e \tau_s & \boldsymbol{C}_b^e \tau_s & 0_3 & 0_1 & 0_1 \\ 0_3 & \boldsymbol{I}_3 \tau_s & \boldsymbol{I}_3 & 0_3 & 0_3 & 0_1 & 0_1 \\ 0_3 & 0_3 & 0_3 & \boldsymbol{I}_3 & 0_3 & 0_1 & 0_1 \\ 0_3 & 0_3 & 0_3 & 0_3 & \boldsymbol{I}_3 & 0_1 & 0_1 \\ 0_1 & 0_1 & 0_1 & 0_1 & 0_1 & 1 & \tau_s \\ 0_1 & 0_1 & 0_1 & 0_1 & 0_1 & 0_1 & 1 \end{bmatrix} \tag{7}$$

Where, $\boldsymbol{F}_{21}^e = [-(\hat{\boldsymbol{C}}_b^e \hat{\boldsymbol{f}}_{ib}^b)\Lambda]$, $\boldsymbol{F}_{23}^e = -\frac{2\hat{\boldsymbol{\gamma}}_{ib}^e}{r_{eS}^e(\hat{L}_b)} \frac{\hat{r}_{eb}^{e\,\mathrm{T}}}{|\hat{r}_{eb}^e|}$.

In the above equations, $\mathbf{\Omega}_{ie}^e$ represents the antisymmetric matrix of the earth's rotational angular velocity vector, τ_s represents the state transfer time interval, $\boldsymbol{C}_b^e$ represents the directional cosine matrix from the body to ECEF coordinate, $\hat{\boldsymbol{C}}_b^e$ represents the estimated directional cosine matrix from the body to ECEF coordinate, $\hat{\boldsymbol{f}}_{ib}^b$ represents the estimated specific force measurement, r_{eS}^e represents the radius of the earth's center, $\boldsymbol{I}_3$ represents the third-order unit matrix, and $\hat{\boldsymbol{\gamma}}_{ib}^e$ represents the gravitational acceleration at the estimated position $\hat{r}_{ib}^e$, Λ represents the corresponding antisymmetric matrix, $\hat{r}_{eb}^e$ represents the projection of the estimated position relative to ECEF coordinate and on ECEF coordinate, and $\hat{L}_b$ represents the estimated latitude. To improve readability, the definition of parameters defined in Eq (7) are listed in Table II.

The system noise covariance matrix can be approximately expressed as:

$$\boldsymbol{Q} \approx \begin{bmatrix} \boldsymbol{S}_{rg}\boldsymbol{I}_3 & 0_3 & 0_3 & 0_3 & 0_3 & 0_1 & 0_1 \\ 0_3 & \boldsymbol{S}_{ra}\boldsymbol{I}_3 & 0_3 & 0_3 & 0_3 & 0_1 & 0_1 \\ 0_3 & 0_3 & 0_3 & 0_3 & 0_3 & 0_1 & 0_1 \\ 0_3 & 0_3 & 0_3 & \boldsymbol{S}_{bad}\boldsymbol{I}_3 & 0_3 & 0_1 & 0_1 \\ 0_3 & 0_3 & 0_3 & 0_3 & \boldsymbol{S}_{bgd}\boldsymbol{I}_3 & 0_1 & 0_1 \\ 0_1 & 0_1 & 0_1 & 0_1 & 0_1 & S_{c\phi}^a & 0_1 \\ 0_1 & 0_1 & 0_1 & 0_1 & 0_1 & 0_1 & S_{cf}^a \end{bmatrix} \tau_s \tag{8}$$

In the above equation, $\boldsymbol{S}_{rg}$, $\boldsymbol{S}_{ra}$, $\boldsymbol{S}_{bad}$ and $\boldsymbol{S}_{bgd}$ respectively represent the power spectral density (PSD) of gyro random noise, the PSD of accelerometer random noise, the PSD of accelerometer biases change and the PSD of gyro biases change. It is assumed that all gyroscopes and accelerometers have the same noise characteristics. $S_{c\phi}^a$ represents the PSD of phase drift of receiver clock, and S_{cf}^a represents the PSD of frequency drift of receiver clock.

TABLE II
DEFINITION OF PARAMETERS

Paramater	Definition
$\boldsymbol{\Omega}_{ie}^e$	antisymmetric matrix of the earth's rotational angular velocity vector
τ_s	state transfer time interval
$\boldsymbol{C}_b^e$	directional cosine matrix from the body to ECEF coordinate
$\hat{\boldsymbol{C}}_b^e$	estimated directional cosine matrix from the body to ECEF coordinate
$\hat{\boldsymbol{f}}_{ib}^b$	estimated specific force measurement
r_{eS}^e	radius of the earth's center
$\boldsymbol{I}_3$	third-order unit matrix
$\hat{\boldsymbol{\gamma}}_{ib}^e$	gravitational acceleration at the estimated position
$\hat{r}_{ib}^e$	estimated position
Λ	corresponding antisymmetric matrix
$\hat{r}_{eb}^e$	projection of the estimated position relative to ECEF coordinate and on ECEF coordinate
$\hat{L}_b$	estimated latitude

TABLE III
PARAMETERS CONSUMER-GRADE IMU

Paramater	Value	Unit
IMU accelerometer biases	[9000;-13000;8000]	μg
IMU accelerometer noise root PSD	1000	$\mu g / \sqrt{\mathrm{Hz}}$
IMU gyro biases	[-180;260;-160]	$^\circ / \mathrm{h}$
IMU gyro noise root PSD	1	$^\circ / \sqrt{\mathrm{h}}$

The propagation of state estimation over time is expressed as:

$$\hat{\boldsymbol{X}}_{i|i-1} = \mathbf{\Phi}_{i,i-1} \hat{\boldsymbol{X}}_{i-1} \tag{9}$$

Where, $\hat{\boldsymbol{X}}_{i|i-1}$ represents the error estimation of IMU navigation parameters predicted at time i, and $\hat{\boldsymbol{X}}_i$ represents the error estimation of IMU navigation parameters at time i; $\mathbf{\Phi}_{i,i-1}$ represents the system state transition matrix from time $i-1$ to time i.

The propagation model of error covariance matrix of state estimation is:

$$\boldsymbol{P}_{i|i-1} \approx \mathbf{\Phi}_{i,i-1} \left(\boldsymbol{P}_{i-1} + \frac{1}{2}\boldsymbol{Q}'_{i-1} \right) \mathbf{\Phi}_{i,i-1}^{\mathrm{T}} + \frac{1}{2}\boldsymbol{Q}'_{i-1} \tag{10}$$

$\boldsymbol{P}_{i|i-1}$ represents the prediction error covariance matrix at time i; $\boldsymbol{P}_{i-1}$ represents estimation error covariance matrix at time $i-1$; $\boldsymbol{Q}_{i-1}$ represents the system noise covariance matrix at time $i-1$.

The measurement model of tightly-coupled GNSS/IMU is as follows:

The pseudorange $\hat{\rho}_{a,C}^{j-}$ predicted by IMU is expressed as:

$$\begin{aligned}\hat{\rho}_{a,C}^{j-} &= \sqrt{\left[\boldsymbol{C}_e^I(\tilde{t}_{st,a}^j)\hat{r}_{ej}^e(\tilde{t}_{st,a}^j) - \hat{r}_{ea}^{e-}\right]^{\mathrm{T}}\left[\boldsymbol{C}_e^I(\tilde{t}_{st,a}^j)\hat{r}_{ej}^e(\tilde{t}_{st,a}^j) - \hat{r}_{ea}^{e-}\right]} \\ &\quad + c\cdot\delta t_u \end{aligned} \tag{11}$$

In the above equation, $\hat{\rho}_{a,C}^{j-}$ represents the predicted corrected pseudorange measurement from transmitting antenna j to receiver antenna a, $\tilde{t}_{st,a}^j$ represents the measured signal transmission time, I in $\boldsymbol{C}_e^I$ represents the Earth centered inertial frame (ECI) coordinate synchronized with ECEF coordinate at the arrival time of satellite signal, and $\boldsymbol{C}_e^I$ represents the directional cosine matrix from ECEF coordinate to ECI coordinate caused by the earth's rotation within the propagation time of satellite signal. $\hat{r}_{ej}^e$ represents the estimated satellite position and $\hat{r}_{ea}^{e-}$ represents the estimated receiver position.

The pseudorange rate $\hat{\dot{\rho}}_{a,C}^{j-}$ predicted by IMU is expressed as:

$$\begin{aligned}\hat{\dot{\rho}}_{a,C}^{j-} &= \hat{u}_{as,j}^{e-\mathrm{T}}\Big[\boldsymbol{C}_e^I(\tilde{t}_{st,a}^j)(\hat{v}_{ej}^e(\tilde{t}_{st,a}^j) + \boldsymbol{\Omega}_{ie}^e\hat{r}_{ej}^e(\tilde{t}_{st,a}^j)) \\ &\quad -(\hat{v}_{ea}^{e-} + \boldsymbol{\Omega}_{ie}^e\hat{r}_{ea}^{e-})\Big] + c\cdot\delta f_u + \delta n \end{aligned} \tag{12}$$

In the above equation, $\hat{\dot{\rho}}_{a,C}^{j-}$ represents the predicted corrected pseudorange rate measurement from transmitting antenna j to receiver antenna a, $\hat{v}_{ej}^e$ represents the estimated satellite motion speed, $\hat{v}_{ea}^{e-}$ represents the estimated receiver motion speed, and $\hat{u}_{as,j}^{e-\mathrm{T}}$ represents the directional cosine between the estimated satellite position and receiver position.δn represents the observation noise and hardware noise considering the realistic effects.

The measurement matrix $\boldsymbol{H}$ is:

$$\boldsymbol{H} \approx \begin{bmatrix} 0_{1\times3} & 0_{1\times3} & u_{a1}^{\mathrm{T}} & 0_{1\times3} & 0_{1\times3} & 1 & 0 \\ 0_{1\times3} & 0_{1\times3} & u_{a2}^{\mathrm{T}} & 0_{1\times3} & 0_{1\times3} & 1 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0_{1\times3} & 0_{1\times3} & u_{am}^{\mathrm{T}} & 0_{1\times3} & 0_{1\times3} & 1 & 0 \\ 0_{1\times3} & u_{a1}^{\mathrm{T}} & 0_{1\times3} & 0_{1\times3} & 0_{1\times3} & 0 & 1 \\ 0_{1\times3} & u_{a2}^{\mathrm{T}} & 0_{1\times3} & 0_{1\times3} & 0_{1\times3} & 0 & 1 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0_{1\times3} & u_{am}^{\mathrm{T}} & 0_{1\times3} & 0_{1\times3} & 0_{1\times3} & 0 & 1 \end{bmatrix} \tag{13}$$

Where $u_{a1},\ldots,u_{am}$ represents the directional cosine between satellite position and receiver position.

The measurement noise covariance matrix $\boldsymbol{R}$ is expressed as:

$$\boldsymbol{R} = \begin{bmatrix} \sigma_\rho^2 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ 0 & \sigma_\rho^2 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \sigma_\rho^2 & 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & \sigma_r^2 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 0 & \sigma_r^2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & \sigma_r^2 \end{bmatrix} \tag{14}$$

In the above equation, it is assumed that all pseudorange measurements and pseudorange rate measurements are independent and the variance of the same measurement type is equal. σ_ρ^2 represents the measurement noise variance of pseudorange and σ_r^2 represents the measurement noise variance of pseudorange rate.

The Kalman gain matrix is expressed as:

$$\boldsymbol{K}_i = \boldsymbol{P}_{i|i-1}\boldsymbol{H}_i^{\mathrm{T}}(\boldsymbol{H}_i\boldsymbol{P}_{i|i-1}\boldsymbol{H}_i^{\mathrm{T}} + \boldsymbol{R}_i)^{-1} \tag{15}$$

In the above equation, $\boldsymbol{K}_i$ represents the Kalman gain matrix at time i.

GNSS outputs the measurements of pseudorange and pseudorange rate. The predicted values of pseudorange and pseudorange rate can be obtained according to the corrected inertial navigation parameters, estimated receiver clock offset and clock drift, and navigation messages including satellite position and velocity. The difference between the pseudorange and pseudorange rate output by GNSS and the calculated predicted values of pseudorange and pseudorange rate at the same time constitutes the measurement innovation vector, that is:

$$\begin{aligned}&\delta\boldsymbol{z}_i = \begin{bmatrix}\delta\boldsymbol{z}_{\rho,i}\\ \delta\boldsymbol{z}_{r,i}\end{bmatrix} \\ &\begin{cases}\delta\boldsymbol{z}_{\rho,i} = \left(\tilde{\rho}_{a,C}^1 - \hat{\rho}_{a,C}^{1-}, \tilde{\rho}_{a,C}^2 - \hat{\rho}_{a,C}^{2-}, \cdots\ \tilde{\rho}_{a,C}^m - \hat{\rho}_{a,C}^{m-}\right)_i \\ \delta\boldsymbol{z}_{r,i} = \left(\tilde{\dot{\rho}}_{a,C}^1 - \hat{\dot{\rho}}_{a,C}^{1-}, \tilde{\dot{\rho}}_{a,C}^2 - \hat{\dot{\rho}}_{a,C}^{2-}, \cdots\ \tilde{\dot{\rho}}_{a,C}^m - \hat{\dot{\rho}}_{a,C}^{m-}\right)_i\end{cases}\end{aligned} \tag{16}$$

In the above equation, $\tilde{\rho}_{a,C}^1,\ldots,\tilde{\rho}_{a,C}^m$ represents m pseudorange measurement values at time i, $\hat{\rho}_{a,C}^{1-},\ldots,\hat{\rho}_{a,C}^{m-}$ represents m pseudorange prediction values at time i, $\tilde{\dot{\rho}}_{a,C}^1,\ldots,\tilde{\dot{\rho}}_{a,C}^m$ represents m pseudorange rate measurement values at time i, and $\hat{\dot{\rho}}_{a,C}^{1-},\ldots,\hat{\dot{\rho}}_{a,C}^m$ represents m pseudorange rate prediction values at time i. $\delta\boldsymbol{z}_{\rho,i}$ and $\delta\boldsymbol{z}_{r,i}$ represent pseudorange measurement innovation vector and pseudorange rate measurement innovation vector respectively.

Update the state variable with the observation vector as:

$$\hat{\boldsymbol{X}}_i = \hat{\boldsymbol{X}}_{i|i-1} + \boldsymbol{K}_i\delta\boldsymbol{z}_i \tag{17}$$

Corresponding error covariance matrix update:

$$\boldsymbol{P}_i = (\boldsymbol{I} - \boldsymbol{K}_i\boldsymbol{H}_i)\boldsymbol{P}_{i|i-1} \tag{18}$$

Finally, closed-loop correction is carried out to correct the position, velocity and attitude of IMU.

C. Influence of Spoofing on Tightly-Coupled GNSS/IMU

When tightly-coupled GNSS/IMU system is spoofed, firstly, GNSS spoofing signal changes the pseudorange and pseudorange rate of GNSS output, and then affects the measured value of Kalman filter input of tightly-coupled system. Finally, Kalman filter affects the estimated value of state parameters.

Suppose GNSS/IMU is in normal working state before time i, and GNSS/IMU is spoofed by GNSS spoofing at time i, then measurement innovation vector of the system at time i is $\delta \boldsymbol{z}_i + \Delta \boldsymbol{z}_i$, and $\Delta \boldsymbol{z}_i$ represents the deviation of measurement innovation vector introduced by GNSS spoofing. $\delta \boldsymbol{z}_i + \Delta \boldsymbol{z}_i$ is expressed as (19) shown at the bottom of this page.

In (19), $\Delta\tilde{\rho}^1_{a,C}, \ldots, \Delta\tilde{\rho}^m_{a,C}$ represents the deviation of m pseudorange measurements at time i, and $\Delta\tilde{\dot{\rho}}^1_{a,C}, \ldots, \Delta\tilde{\dot{\rho}}^m_{a,C}$ represents the deviation of m pseudorange rate measurements at time i. $\Delta \boldsymbol{z}_{\rho,i}$ and $\Delta \boldsymbol{z}_{r,i}$ represent the deviation of pseudorange measurement innovation vector and pseudorange rate measurement innovation vector respectively.

In the process of GNSS spoofing, $\boldsymbol{P}_i$, $\boldsymbol{Q}_i$, $\boldsymbol{R}_i$ and gain matrix $\boldsymbol{K}_i$ of Kalman filter can be approximately unchanged, and GNSS/IMU error estimation under GNSS spoofing can be obtained as follows [20]:

$$\hat{\boldsymbol{X}}_i = \boldsymbol{\Phi}_{i,i-1}\hat{\boldsymbol{X}}_{i-1} + \boldsymbol{K}_i\left(\delta \boldsymbol{z}_i + \Delta \boldsymbol{z}_i\right) \tag{20}$$

Since GNSS/IMU output results are IMU navigation parameters corrected by error estimation, error estimation deviation is system deviation of GNSS/IMU. Therefore, system deviation expression of GNSS/IMU is [20]:

$$\boldsymbol{\Delta}\hat{\boldsymbol{X}}_i = \hat{\boldsymbol{X}}_i^{'} - \hat{\boldsymbol{X}}_i = \begin{cases} \boldsymbol{K}_1\Delta \boldsymbol{z}_1 \\ (\boldsymbol{I} - \boldsymbol{K}_i\boldsymbol{H}_i)\boldsymbol{\Phi}_{i,i-1} \\ \quad \boldsymbol{\Delta}\hat{\boldsymbol{X}}_{i-1} + \boldsymbol{K}_i\Delta \boldsymbol{z}_i \end{cases} \quad , i = 2, 3, \ldots \tag{21}$$

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

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

A. Avoiding Spoofing Detection of Least Squares Residual RAIM

The tightly-coupled GNSS/IMU can effectively detect faults and even spoofing through RAIM algorithm [10]. The basic principle of RAIM algorithm is mostly based on checking the consistency between measured values of various satellites. The purpose of RAIM is to judge whether a group of measured data contains wrong measured values and which measured values are wrong [21].

The least squares residual RAIM algorithm uses all GNSS pseudorange measurements to calculate the least squares estimation $\hat{\boldsymbol{x}}_i$ of the n-dimensional state vector, where $\hat{\boldsymbol{x}}_i$ is the four-dimensional state vector, including GNSS user positioning results and receiver clock offset, namely:

$$\delta\hat{\boldsymbol{x}}_i = \left(\boldsymbol{H}_i^{\mathrm{T}}\boldsymbol{H}_i\right)^{-1}\boldsymbol{H}_i^{\mathrm{T}}\delta \boldsymbol{z}_i^{-} \tag{22}$$

Where, $\delta \boldsymbol{z}_i^{-}$ represents the m-dimensional measurement innovation vector, $\delta\hat{\boldsymbol{x}}_i$ is the state innovation vector, $\boldsymbol{H}_i$ is measurement matrix, and i represents the epoch. Calculate the measurement residual $\delta \boldsymbol{z}_i^{+}$ according to the following equations:

$$\delta \boldsymbol{z}_i^{+} = \delta \boldsymbol{z}_i^{-} - \boldsymbol{H}_i\delta\hat{\boldsymbol{x}}_i \tag{23}$$

Construct the normalized test statistic $u_{\delta z}$ for χ^2-test:

$$u_{\delta z} = \left(\delta \boldsymbol{z}_i^{+}\right)^{\mathrm{T}}\left(\boldsymbol{C}_{\delta z,i}^{+}\right)^{-1}\delta \boldsymbol{z}_i^{+} \tag{24}$$

Where, $\boldsymbol{C}_{\delta z,i}^{+}$ represents measurement residual covariance matrix, the diagonal element of $\boldsymbol{C}_{\delta z,i}^{+}$ is the estimated variance of each pseudorange error and each pseudorange rate error, and $\boldsymbol{C}_{\delta z,i}^{+}$ is:

$$\boldsymbol{C}_{\delta z,i}^{+} = \begin{bmatrix} \sigma_\rho^2 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ 0 & \sigma_\rho^2 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \sigma_\rho^2 & 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & \sigma_r^2 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 0 & \sigma_r^2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & \sigma_r^2 \end{bmatrix} \tag{25}$$

In the above equation, assuming that all pseudorange and pseudorange rate measurements are independent. $u_{\delta z}^2$ has the χ^2 distribution of $2(m-n)$ degrees of freedom.

Next, from the perspective of spoofer, spoofing algorithm to avoid least squares residual RAIM is proposed. The value range of pseudorange deviation and pseudorange rate deviation of tightly-coupled GNSS/IMU introduced by GNSS spoofing under the threshold constraint of least squares residual RAIM algorithm is derived below.

If the absolute value of $u_{\delta z}$ exceeds threshold T_u, the navigation system sends an alarm and considers that the measurement is abnormal. That is, the alarm judgment criteria are:

$$\begin{cases} |u_{\delta z}| > T_u, Alarm \\ |u_{\delta z}| \leq T_u, Not\ Alarm \end{cases} \tag{26}$$

Where, T_u is the RAIM threshold, which can be determined according to the χ^2 distribution.

In order to make spoofing have good concealment, it should meet $|u_{\delta z}| \leq T_u$. next, calculate value range of single epoch measurement deviation according to the $|u_{\delta z}|$ threshold. To meet $|u_{\delta z}| \leq T_u$. The single epoch is analyzed below. Since $\boldsymbol{C}_{\delta z,i}^{+}$ is

$$\begin{cases} \delta \boldsymbol{z}_{\rho,i} + \Delta \boldsymbol{z}_{\rho,i} = \left(\tilde{\rho}^1_{a,C} + \Delta\tilde{\rho}^1_{a,C} - \hat{\rho}^{1-}_{a,C}, \tilde{\rho}^2_{a,C} + \Delta\tilde{\rho}^2_{a,C} - \hat{\rho}^{2-}_{a,C}, \cdots\ \tilde{\rho}^m_{a,C} + \Delta\tilde{\rho}^m_{a,C} - \hat{\rho}^{m-}_{a,C}\right)_i \\ \delta \boldsymbol{z}_{r,i} + \Delta \boldsymbol{z}_{r,i} = \left(\tilde{\dot{\rho}}^1_{a,C} + \Delta\tilde{\dot{\rho}}^1_{a,C} - \hat{\dot{\rho}}^{1-}_{a,C}, \tilde{\dot{\rho}}^2_{a,C} + \Delta\tilde{\dot{\rho}}^2_{a,C} - \hat{\dot{\rho}}^{2}_{a,C}, \cdots\ \tilde{\dot{\rho}}^m_{a,C} + \Delta\tilde{\dot{\rho}}^m_{a,C} - \hat{\dot{\rho}}^{m}_{a,C}\right)_i \end{cases} \tag{19}$$

diagonal matrix, $|u_{\delta z}| \leq T_u$ can be converted into:

$$\begin{cases} \left|\left(\delta \boldsymbol{z}_i^- - \boldsymbol{H}_i \delta \hat{\boldsymbol{x}}_i\right)^{\mathrm{T}} \cdot \left(\delta \boldsymbol{z}_i^- - \boldsymbol{H}_i \delta \hat{\boldsymbol{x}}_i\right)\right| \\ \quad \leq T_u \cdot \sigma_\rho^2, i = 1, \ldots, m \\ \left|\left(\delta \boldsymbol{z}_i^- - \boldsymbol{H}_i \delta \hat{\boldsymbol{x}}_i\right)^{\mathrm{T}} \cdot \left(\delta \boldsymbol{z}_i^- - \boldsymbol{H}_i \delta \hat{\boldsymbol{x}}_i\right)\right| \\ \quad \leq T_u \cdot \sigma_r^2, i = m+1, \ldots, 2m \end{cases} \tag{27}$$

The above equation can be equivalent to:

$$\begin{cases} \left|\left(\delta \boldsymbol{z}_i^- - \boldsymbol{H}_i \delta \hat{\boldsymbol{x}}_i\right)\right| \leq \sigma_\rho \cdot \sqrt{T_u}, i = 1, \ldots, m \\ \left|\left(\delta \boldsymbol{z}_i^- - \boldsymbol{H}_i \delta \hat{\boldsymbol{x}}_i\right)\right| \leq \sigma_r \cdot \sqrt{T_u}, i = m+1, \ldots, 2m \end{cases} \tag{28}$$

In order to further solve (28), let $\delta z_{i,j}^-$ represents the j-th component of $\delta \boldsymbol{z}_i^-$, analyze the component $\delta z_{i,j}^-$ in measurement innovation vector $\delta \boldsymbol{z}_i^-$, and convert (28) into:

$$\begin{cases} \left|\left(\delta z_{i,j}^- - \boldsymbol{H}_{i,j} \delta \hat{\boldsymbol{x}}_i\right)\right| \leq \sigma_\rho \sqrt{\frac{T_u}{m}}, i = 1, \ldots, m, j = 1, \ldots, m \\ \left|\left(\delta z_{i,j}^- - \boldsymbol{H}_{i,j} \delta \hat{\boldsymbol{x}}_i\right)\right| \leq \sigma_r \sqrt{\frac{T_u}{m}}, i = m \\ \quad +1, \ldots, 2m, j = 1, \ldots, m \end{cases} \tag{29}$$

In fact, (29) is a sufficient and unnecessary condition of (28). If (29) is satisfied, equation (28) must be satisfied.

From the above equation, $\delta z_{i,j}^-$ shall meet the following value range:

$$\begin{cases} \boldsymbol{H}_{i,j} \hat{\boldsymbol{x}}_i^+ - \boldsymbol{H}_{i,j} \hat{\boldsymbol{x}}_i^- - \sigma_\rho \\ \cdot \sqrt{\frac{T_u}{m}} \leq \delta z_{i,j}^- \leq \boldsymbol{H}_{i,j} \hat{\boldsymbol{x}}_i^+ - \boldsymbol{H}_{i,j} \hat{\boldsymbol{x}}_i^- + \sigma_\rho \\ \cdot \sqrt{\frac{T_u}{m}}, i = 1, \ldots, m, j = 1, \ldots, m \\ \boldsymbol{H}_{i,j} \hat{\boldsymbol{x}}_i^+ - \boldsymbol{H}_{i,j} \hat{\boldsymbol{x}}_i^- - \sigma_\rho \\ \cdot \sqrt{\frac{T_u}{m}} \leq \delta z_{i,j}^- \leq \boldsymbol{H}_{i,j} \hat{\boldsymbol{x}}_i^+ - \boldsymbol{H}_{i,j} \hat{\boldsymbol{x}}_i^- + \sigma_r \\ \cdot \sqrt{\frac{T_u}{m}}, i = m+1, \ldots, 2m, j = 1, \ldots, m \end{cases} \tag{30}$$

From the above equation, pseudorange measurement $\tilde{\rho}_{a,C}^j$ and pseudorange rate measurement $\tilde{\dot{\rho}}_{a,C}^j$ from transmitting antenna j to receiver antenna a shall meet the following range:

$$\begin{cases} \hat{\rho}_{a,C}^{j-} + \boldsymbol{H}_{i,j} \hat{\boldsymbol{x}}_i^+ - \boldsymbol{H}_{i,j} \hat{\boldsymbol{x}}_i^- - \sigma_\rho \\ \cdot \sqrt{\frac{T_u}{m}} \leq \tilde{\rho}_{a,C}^j \leq \hat{\rho}_{a,C}^{j-} + \boldsymbol{H}_{i,j} \hat{\boldsymbol{x}}_i^+ - \boldsymbol{H}_{i,j} \hat{\boldsymbol{x}}_i^- + \sigma_\rho \\ \cdot \sqrt{\frac{T_u}{m}}, i = 1, \ldots, m, j = 1, \ldots, m \\ \hat{\dot{\rho}}_{a,C}^j + \boldsymbol{H}_{i,j} \hat{\boldsymbol{x}}_i^+ - \boldsymbol{H}_{i,j} \hat{\boldsymbol{x}}_i^- - \sigma_r \\ \cdot \sqrt{\frac{T_u}{m}} \leq \tilde{\dot{\rho}}_{a,C}^j \leq \hat{\dot{\rho}}_{a,C}^j + \boldsymbol{H}_{i,j} \hat{\boldsymbol{x}}_i^+ - \boldsymbol{H}_{i,j} \hat{\boldsymbol{x}}_i^- + \sigma_r \\ \cdot \sqrt{\frac{T_u}{m}}, i = m+1, \ldots, 2m, j = 1, \ldots, m \end{cases} \tag{31}$$

The above equation shows that when spoofing on tightly-coupled GNSS/IMU, in order to avoid spoofing detection of the least squares residual RAIM algorithm, spoofing pseudorange measurement $\tilde{\rho}_{a,C}^j$ and pseudorange rate measurement $\tilde{\dot{\rho}}_{a,C}^j$ cannot change arbitrarily and needs to meet the range of (31).

B. Avoiding Parameter Rationality Check

Tightly-coupled GNSS/IMU can detect faults and even spoofing through parameter rationality check. Parameter rationality check includes sensor output, navigation parameters and Kalman filter estimation [8]. Check the sensor output to respond to simple spoofing; Checking navigation parameters provides an additional protection. Checking Kalman filter estimation can check slowly faults and even spoofing.

Next, spoofing algorithm to avoid parameter rationality check is proposed from the perspective of spoofer. Firstly, the influence of gain matrix $\boldsymbol{K}_i$ in Kalman filtering process on GNSS spoofing is analyzed. $\boldsymbol{K}_\infty$ represents the stable state of $\boldsymbol{K}_i$ and $\boldsymbol{K}_\infty$ is $17 \times 2m$ matrix. According to (21), the relationship between system deviation of GNSS/IMU and measured deviation can be expressed in the following matrix form:

$$\begin{bmatrix} \Delta\delta\phi \\ \Delta\delta\theta \\ \Delta\delta\varphi \\ \Delta\delta v_x \\ \Delta\delta v_y \\ \Delta\delta v_z \\ \Delta\delta x \\ \Delta\delta y \\ \Delta\delta z \\ \Delta b_{ax} \\ \Delta b_{ay} \\ \Delta b_{az} \\ \Delta b_{gx} \\ \Delta b_{gy} \\ \Delta b_{gz} \\ \Delta\delta t_u \\ \Delta\delta f_u \end{bmatrix} = \begin{bmatrix} \boldsymbol{K}_\infty(1,1) & \cdots & \boldsymbol{K}_\infty(1,m) & \boldsymbol{K}_\infty(1,m+1) & \cdots & \boldsymbol{K}_\infty(1,2m) \\ \boldsymbol{K}_\infty(2,1) & \cdots & \boldsymbol{K}_\infty(2,m) & \boldsymbol{K}_\infty(2,m+1) & \cdots & \boldsymbol{K}_\infty(2,2m) \\ \boldsymbol{K}_\infty(3,1) & \cdots & \boldsymbol{K}_\infty(3,m) & \boldsymbol{K}_\infty(3,m+1) & \cdots & \boldsymbol{K}_\infty(3,2m) \\ \boldsymbol{K}_\infty(4,1) & \cdots & \boldsymbol{K}_\infty(4,m) & \boldsymbol{K}_\infty(4,m+1) & \cdots & \boldsymbol{K}_\infty(4,2m) \\ \boldsymbol{K}_\infty(5,1) & \cdots & \boldsymbol{K}_\infty(5,m) & \boldsymbol{K}_\infty(5,m+1) & \cdots & \boldsymbol{K}_\infty(5,2m) \\ \boldsymbol{K}_\infty(6,1) & \cdots & \boldsymbol{K}_\infty(6,m) & \boldsymbol{K}_\infty(6,m+1) & \cdots & \boldsymbol{K}_\infty(6,2m) \\ \boldsymbol{K}_\infty(7,1) & \cdots & \boldsymbol{K}_\infty(7,m) & \boldsymbol{K}_\infty(7,m+1) & \cdots & \boldsymbol{K}_\infty(7,2m) \\ \boldsymbol{K}_\infty(8,1) & \cdots & \boldsymbol{K}_\infty(8,m) & \boldsymbol{K}_\infty(8,m+1) & \cdots & \boldsymbol{K}_\infty(8,2m) \\ \boldsymbol{K}_\infty(9,1) & \cdots & \boldsymbol{K}_\infty(9,m) & \boldsymbol{K}_\infty(9,m+1) & \cdots & \boldsymbol{K}_\infty(9,2m) \\ \boldsymbol{K}_\infty(10,1) & \cdots & \boldsymbol{K}_\infty(10,m) & \boldsymbol{K}_\infty(10,m+1) & \cdots & \boldsymbol{K}_\infty(10,2m) \\ \boldsymbol{K}_\infty(11,1) & \cdots & \boldsymbol{K}_\infty(11,m) & \boldsymbol{K}_\infty(11,m+1) & \cdots & \boldsymbol{K}_\infty(11,2m) \\ \boldsymbol{K}_\infty(12,1) & \cdots & \boldsymbol{K}_\infty(12,m) & \boldsymbol{K}_\infty(12,m+1) & \cdots & \boldsymbol{K}_\infty(12,2m) \\ \boldsymbol{K}_\infty(13,1) & \cdots & \boldsymbol{K}_\infty(13,m) & \boldsymbol{K}_\infty(13,m+1) & \cdots & \boldsymbol{K}_\infty(13,2m) \\ \boldsymbol{K}_\infty(14,1) & \cdots & \boldsymbol{K}_\infty(14,m) & \boldsymbol{K}_\infty(14,m+1) & \cdots & \boldsymbol{K}_\infty(14,2m) \\ \boldsymbol{K}_\infty(15,1) & \cdots & \boldsymbol{K}_\infty(15,m) & \boldsymbol{K}_\infty(15,m+1) & \cdots & \boldsymbol{K}_\infty(15,2m) \\ \boldsymbol{K}_\infty(16,1) & \cdots & \boldsymbol{K}_\infty(16,m) & \boldsymbol{K}_\infty(16,m+1) & \cdots & \boldsymbol{K}_\infty(16,2m) \\ \boldsymbol{K}_\infty(17,1) & \cdots & \boldsymbol{K}_\infty(17,m) & \boldsymbol{K}_\infty(17,m+1) & \cdots & \boldsymbol{K}_\infty(17,2m) \end{bmatrix} \times \begin{bmatrix} \Delta\tilde{\rho}_{a,C}^1 \\ \vdots \\ \Delta\tilde{\rho}_{a,C}^m \\ \Delta\tilde{\dot{\rho}}_{a,C}^1 \\ \vdots \\ \Delta\tilde{\dot{\rho}}_{a,C}^m \end{bmatrix} \tag{32}$$

For spoofer, in order to ensure that 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 GNSS/IMU system introduced to target equal to the expected position deviation values $\Delta\delta x_{Ex}$, $\Delta\delta y_{Ex}$ and $\Delta\delta z_{Ex}$ as much as possible; At the same time, single epoch velocity deviation $\Delta\delta v_x$, $\Delta\delta v_y$ and $\Delta\delta v_z$ of GNSS/IMU system introduced into target are loosely constrained, and the absolute value of velocity deviation meets absolute value of position deviation less than or equal to; Meanwhile, the receiver clock offset δt_u and receiver clock drift δf_u shall not exceed the corresponding reference crystal oscillator indexes $T_{\delta t_u}$ and $T_{\delta f_u}$. In fact, if GNSS spoofing has too much impact on the attitude estimation of target, the expected purpose of spoofing may not be achieved. The reasons are: on the one hand, target (such as UAV) is more sensitive to attitude change relative to position and velocity change, and spoofing detection means of target is easier to detect the abnormality of attitude estimation; On the other hand, if GNSS spoofing causes the attitude change to exceed the physical threshold of target, it is easy to cause motion failure of target [22] and cannot be induced to expected position by spoofer. Therefore, GNSS spoofing should keep single epoch attitude angle deviation values $\Delta\delta\phi$, $\Delta\delta\theta$ and $\Delta\delta\varphi$ of GNSS/IMU system introduced into target as normal as possible. To sum up, the equation can be expressed as:

$$\begin{cases} \Delta\delta x \approx \Delta\delta x_{Ex} \\ \Delta\delta y \approx \Delta\delta y_{Ex} \\ \Delta\delta z \approx \Delta\delta z_{Ex} \\ \Delta\delta t_u \leq T_{\delta t_u} \\ \Delta\delta f_u \leq T_{\delta f_u} \end{cases} \tag{33}$$

If biases estimated by tightly-coupled GNSS/IMU Kalman filter exceeds the 5 times the nominal value, it is considered that the sensor may be faulty [23]. Here, when GNSS spoofing is implemented, the bias caused by spoofing shall not exceed 5 times the nominal biases. That is, equation (32) shall meet the constraints:

$$\begin{cases} \Delta b_{ax} \leq T_{5\sigma_1} \\ \Delta b_{ay} \leq T_{5\sigma_2} \\ \Delta b_{az} \leq T_{5\sigma_3} \\ \Delta b_{gx} \leq T_{5\sigma_4} \\ \Delta b_{gy} \leq T_{5\sigma_5} \\ \Delta b_{gz} \leq T_{5\sigma_6} \end{cases} \tag{34}$$

Where, $T_{5\sigma_i}, i = 1, 2, \ldots, 6$ represents 5 times nominal biases of b_{ax}, b_{ay}, b_{az}, b_{gx}, b_{gy}, respectively.

According to (32), spoofer calculates measurement deviation required for spoofing according to system deviation of GNSS/IMU required for single epoch and estimated gain matrix $\boldsymbol{K}_i$. The position constraint in (33) is taken as the objective function of the product of gain matrix $\boldsymbol{K}_i$ and measured value deviation, the clock offset and clock drift constraint in (33) and (34) are taken as constraints to solve the optimal measured value deviation.

In combination with Section III.A and this section, spoofing quantity is solved by the method in Section III.B to avoid parameter rationality check. At this time, tightly-coupled GNSS/IMU system uses least squares residual RAIM algorithm for spoofing detection. In this case, it is necessary to reconsider spoofing quantity $\Delta \boldsymbol{z}_i$ to avoid RAIM detection. Based on this, $\delta z_{k,j}^{-}$ needs to satisfy (31), so (31) is also used as the constraint condition in Section III.B to resolve $\Delta \boldsymbol{z}_i$ that is not detected by RAIM. In conclusion, the flow of the proposed slowly varying spoofing algorithm avoiding tightly-coupled GNSS/IMU with multiple anti-spoofing techniques is shown in Fig. 3.

According to Fig. 3, after spoofing signal completely takes over GNSS tracking loop, first determine spoofing position, analyze anti-spoofing techniques such as least squares residual RAIM and parameter rationality check, and use the slowly varying spoofing algorithm to determine the pseudorange and pseudorange rate introduced by spoofing, so as to offset the positioning of tightly-coupled system. If coupled system has not been offset to spoofing position, continue to execute the algorithm flow, cycle this process until coupled system is offset to spoofing position, and the spoofing is completed.

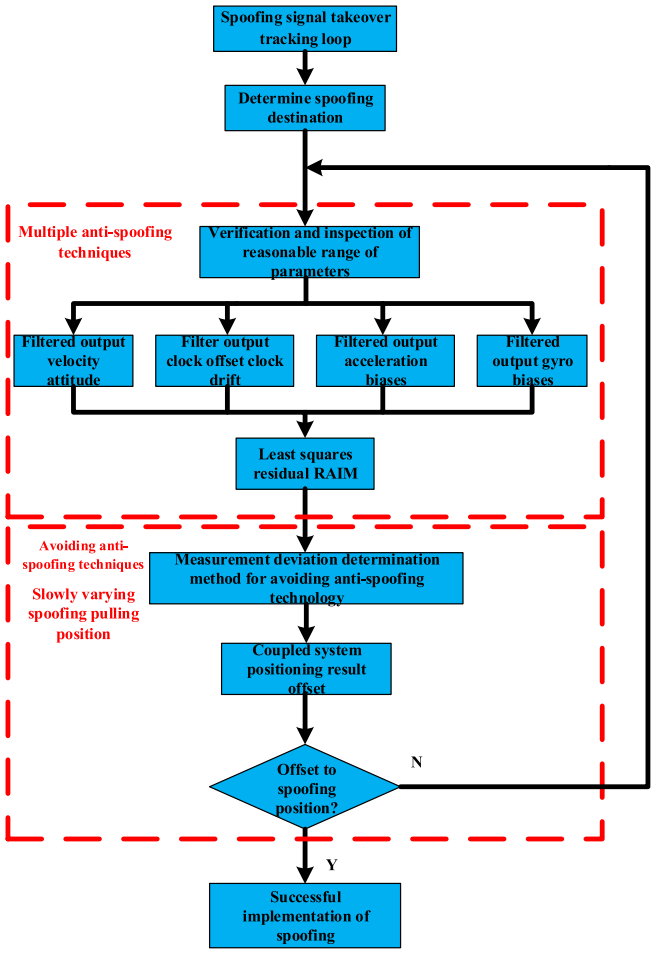

Fig. 3. Flow chart of spoofing tightly-coupled GNSS/IMU algorithm.

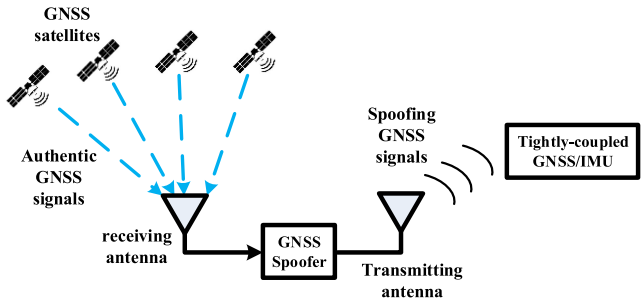

Fig. 4. Schematic diagram of simulation experiment scenario.

V. Experimental Analysis

In the experimental scenario, the real state of tightly-coupled GNSS/IMU equipment always remains stationary at point O. Tightly-coupled GNSS/IMU has the above anti-spoofing techniques: least squares residual RAIM and parameter rationality check, once spoofer violates the relevant threshold of anti-spoofing techniques, tightly-coupled GNSS/IMU system will alarm and spoofing fails. The schematic diagram of simulation experiment scenario is shown in Fig. 4.

According to Fig. 4, the experimental steps and process can be described as: GNSS spoofer is used to spoof tightly-coupled GNSS/IMU. GNSS spoofer first receives authentic GNSS signal from the sky, and spoofer generates spoofing signals after signal analysis, or directly forwards authentic signals to broadcast spoofing signals to tightly-coupled GNSS/IMU, after a period of time, we observe the experimental results, analyze the experimental data and draw conclusions,so as to achieve the purpose of spoofing.

The IMU in tightly-coupled system is consumer-grade IMU, and the device parameters are shown in Table III.

In the experiment, parameter settings of tightly-coupled GNSS/IMU Kalman filter are shown in Table IV:

TABLE IV
PARAMETER SETTING OF KALMAN FILTER FOR TIGHTLY-COUPLED SYSTEM

Paramater	Value	Unit
Accelerometer bias random walk PSD	10^{-5}	m^2/s^5
Gyro bias random walk PSD	4×10^{-11}	rad^2/s^3
Pseudorange measurement noise SD	2.5	m
Pseudorange rate measurement noise SD	0.1	m/s
Receiver clock frequency-drift PSD	1	m^2/s^3
Receiver clock phase-drift PSD	1	m^2/s

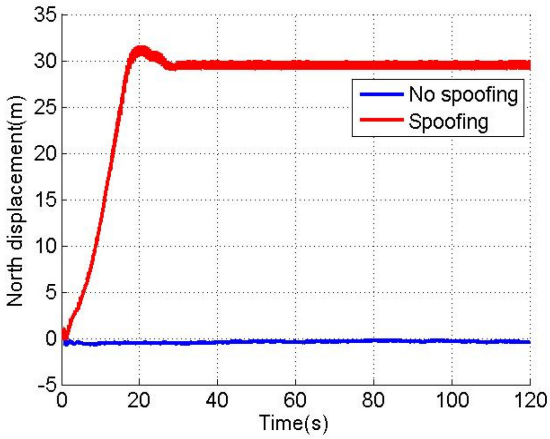

Fig. 5. North displacement without/with spoofing .

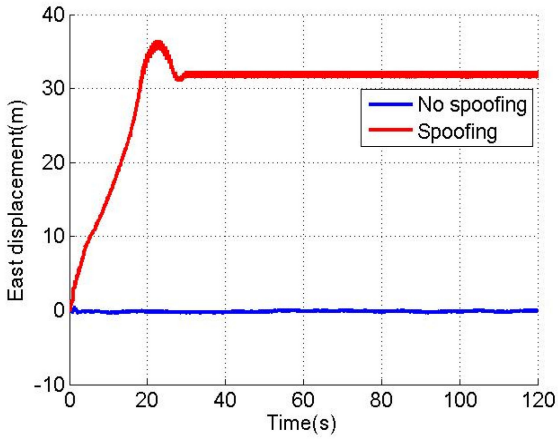

Fig. 6. East displacement without/with spoofing.

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

Figs. 5–7 shows the north, east and down position offsets of tightly-coupled GNSS/IMU system without spoofing and with spoofing respectively. The blue line indicates no spoofing, and the red line indicates spoofing. In the experiment of spoofing tightly-coupled GNSS/IMU system (red line), it is shown that

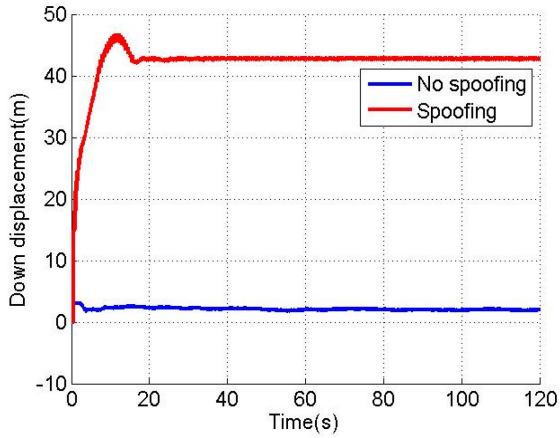

Fig. 7. Down displacement without/with spoofing.

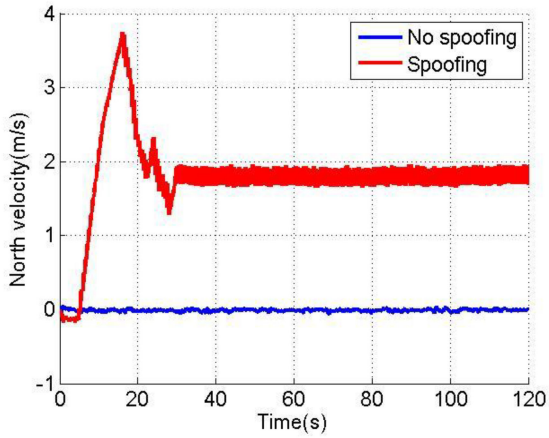

Fig. 8. North velocity without/with spoofing.

spoofer realizes position spoofing (compared with the result without spoofing, which is also the reason for comparison with no spoofing) and avoids the detection of anti-spoofing techniques. Experiments show the spoofing results when anti-spoofing techniques are used for detection.

As shown in Figs. 5–7, when tightly-coupled system is spoofed by slowly varying spoofing, north displacement is gradually offset by 29.5 m, east displacement is gradually offset by 31.9 m and down displacement is gradually offset by 42.7 m in the period of 0–30 s; In the period of 30–120 s, north displacement is stable around 29.5 m, east displacement is stable around 31.9 m, and down displacement is stable around 42.7 m. In terms of spoofing effect, north displacement completely achieves spoofing effect, east displacement basically achieves spoofing effect, and errors with ex-pected offset are -0.5 m and 1.9 m, respectively; Down displacement also basically achieves spoofing effect, but the effect is slightly worse than that in north and east directions, and the error with the expected offset is 12.7 m.

Figs. 8–10 shows north, east and down velocitys of tightly-coupled GNSS/IMU system without spoofing and with spoofing respectively. The blue line indicates no spoofing, and the red line indicates spoofing.

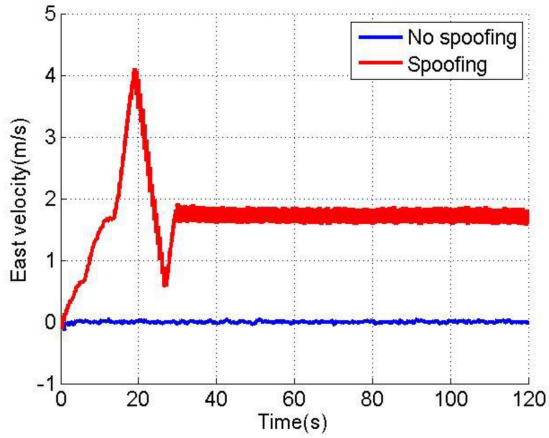

Fig. 9. East velocity without/with spoofing.

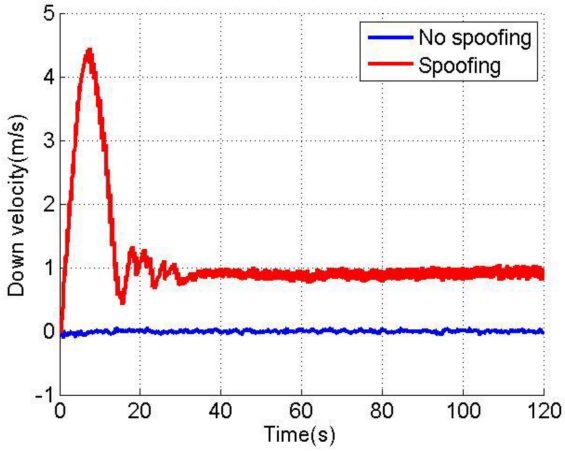

Fig. 10. Down velocity without/with spoofing.

As shown in Figs. 8–10, when tightly-coupled system is spoofed by slowly varying spoofing, north velocity gradually shifts to 1.8m/s, east velocity gradually shifts to 1.7m/s and down velocity gradually shifts to 0.9 m/s in the period of 0–30 s; In the period of 30–120 s, north velocity is stable around 1.8 m/s, east velocity is stable around 1.7 m/s, and down velocity is stable around 0.9 m/s. To sum up, the velocity change of tightly-coupled conforms to parameter rationality check, and is also close to the velicity change without spoofing.

Figs. 11–13 shows the changes of roll angle, pitch angle and yaw angle of tightly-coupled GNSS/IMU system without spoofing and with spoofing respectively. The blue line indicates no spoofing, and the red line indicates spoofing.

As shown in Figs. 11–13, when tightly-coupled system is spoofed by slowly vary-ing spoofing, although roll angle fluctuates slightly compared with the case without spoofing, it can always remain greater than $-0.6°$ and less than $4.8°$; Although pitch angle fluctuates slightly, it can always remain greater than $-3°$ and less than $0.8°$; Although yaw angle fluctuates slightly, it can always remain greater than $-1.3°$ and less than $3.7°$. To sum up, the change of tightly-coupled attitude angle is also close to the change of attitude angle without spoofing.

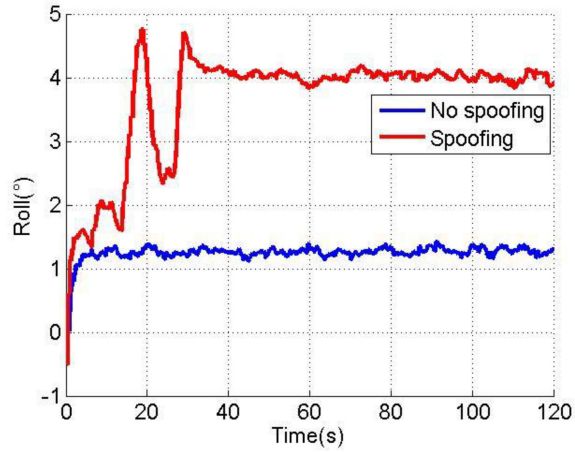

Fig. 11. Roll angle without/with spoofing.

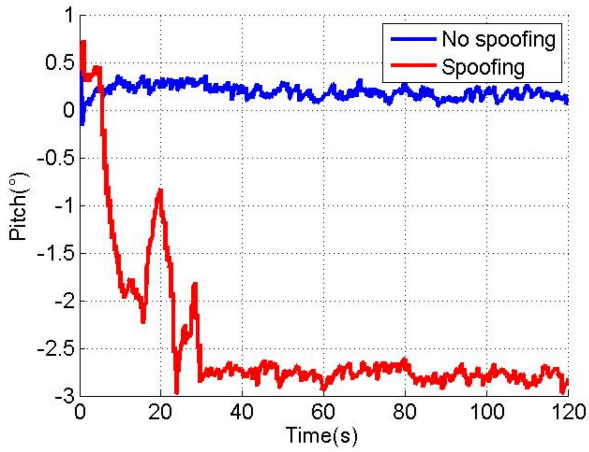

Fig. 12. Pitch angle without/with spoofing.

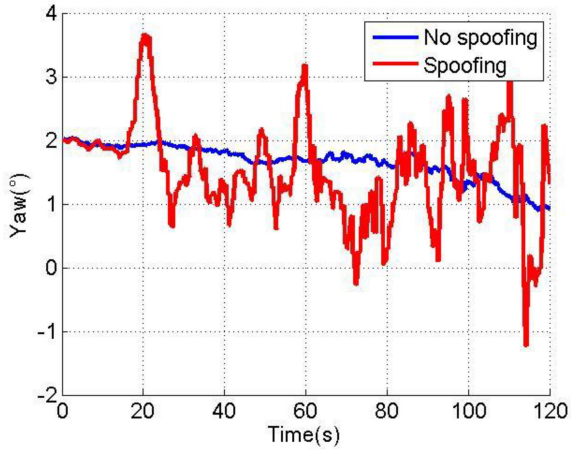

Fig. 13. Yaw angle without/with spoofing.

Fig. 14 shows the change of test statistic of tightly-coupled GNSS/IMU system without spoofing and with spoofing, where the threshold is set to 30. The blue line indicates no spoofing, the red line indicates spoofing, and the green line indicates alarm threshold line.

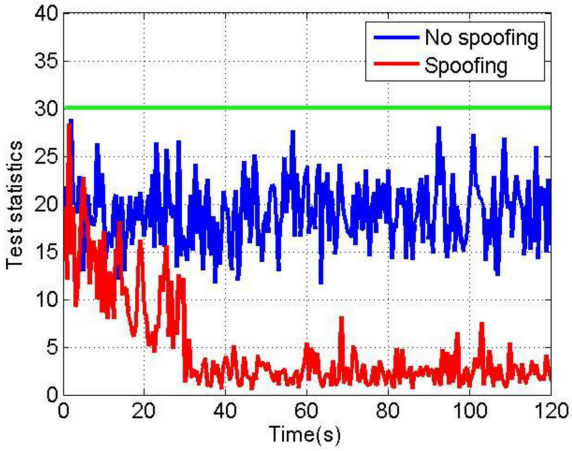

Fig. 14. Test statistics without/with spoofing.

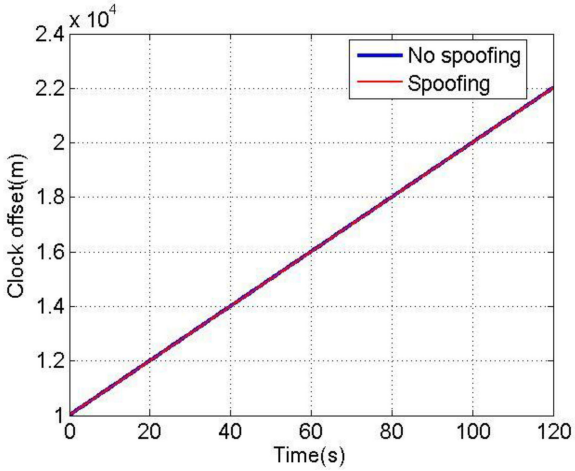

Fig. 15. Clock offset without/with spoofing.

As shown in Fig. 14, when tightly-coupled system is spoofed by slowly varying spoofing, compared with the case without spoofing, the tightly-coupled test statistic $u_{\delta z}$ does not exceed the alarm threshold, The average value of test statistic $u_{\delta z}$ is reduced by 75.4%. To sum up, when tightly-coupled system is spoofed by slowly varying spoofing, its test statistics $u_{\delta z}$ will not alarm.

Figs. 15 and 16 shows the changes of clock offset estimation and clock drift estimation of tightly-coupled GNSS/IMU without spoofing and with spoofing respectively. The blue line indicates no spoofing, and the red line indicates spoofing.

As shown in Figs. 15 and 16, when tightly-coupled system is spoofed by slowly vary-ing spoofing, the estimated of tightly-coupled clock offset is close to the same com-pared with the case without spoofing; Although the estimated of clock drift fluctuates slightly, it can always remain greater than 99.7 m/s and less than 100.2 m/s. To sum up, the changes of tightly-coupled clock offset estimation and clock drift esti-mation are also close to those without spoofing.

Figs. 17 and 18 shows the changes of accelerometer biases estimation and gyro biases estimation of tightly-coupled GNSS/IMU system without spoofing. The red line, green line and blue line respectively represent the X, Y and Z axis directions along body coordinate.

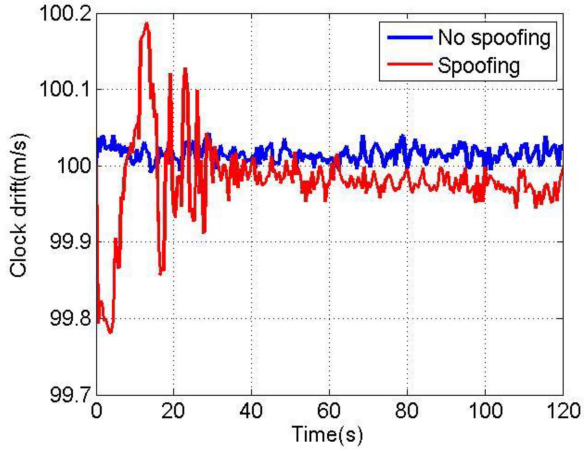

Fig. 16. Clock drift without/with spoofing.

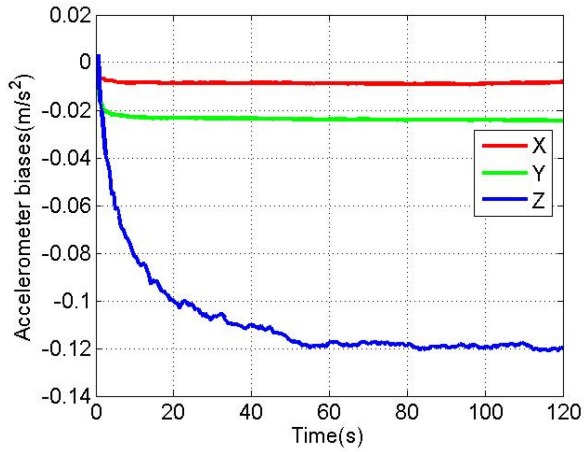

Fig. 17. Accelerometer biases without spoofing.

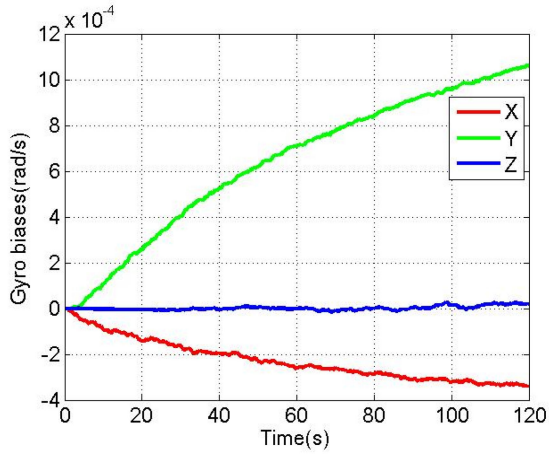

Fig. 18. Gyro biases without spoofing.

Figs. 19 and 20 shows the changes of accelerometer biases estimation and gyro biases estimation of tightly-coupled GNSS/IMU system with spoofing. The red line, green line and

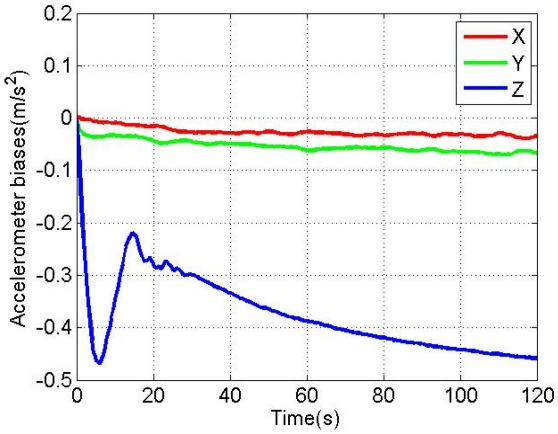

Fig. 19. Accelerometer biases with spoofing.

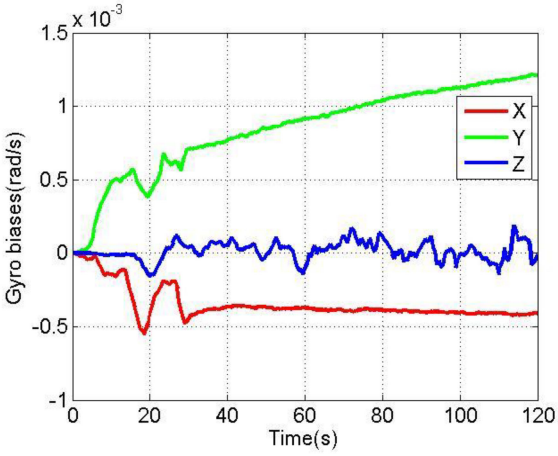

Fig. 20. Gyro biases with spoofing.

blue line respectively represent the X, Y and Z axis directions along body coordinate.

As shown in Figs. 17 and 20, when tightly-coupled system is spoofed by slowly varying spoofing, compared with the case without spoofing, although the estimated of acceleration biases fluctuates slightly in the X direction, it can always remain greater than $-3.9 \times 10^{-2}\ \mathrm{m/s^2}$ and less than $2.9 \times 10^{-3}\ \mathrm{m/s^2}$, although there is a small fluctuation in the Y direction, it can always remain greater than $-7 \times 10^{-2}\ \mathrm{m/s^2}$ and less than 0, although there is a small fluctuation in the Z direction, it can always remain greater than $-4.7 \times 10^{-1}\ \mathrm{m/s^2}$ and less than 0; Although the estimated of gyro biases fluctuates slightly in the X direction, it can always remain greater than $-5.5 \times 10^{-4}\mathrm{rad/s}$ and less than 0, although there is a small fluctuation in the Y direction, it can always remain greater than 0 and less than $1.2 \times 10^{-3}\mathrm{rad/s}$, although there is a small fluctuation in the Z direction, it can always remain greater than $-1.5 \times 10^{-4}\mathrm{rad/s}$ and less than $1.9 \times 10^{-4}\mathrm{rad/s}$. To sum up, the variation of biases estimation of accelerometer and gyro is also close to variation without spoofing.

Based on the above experimental analysis, in terms of spoofing effect, north displacement completely achieves spoofing effect, east displacement basically achieves spoofing effect, and errors with expected offset are -0.5 m and 1.9 m, respectively; Down displacement also basically achieves spoofing effect, but the effect is slightly worse than that in north and east directions, and error with the expected offset is 12.7 m. When slowly varying spoofing is applied to tightly-coupled system, the changes of velocity, attitude angle, clock offset, clock drift, accelerometer bias estimation and gyro bias estimation of tightly-coupled system comply with parameter rationality check, and are also close to the change when there is no spoofing. At the same time, the test statistics will not alarm, and the average value will be reduced by 75.4%.

VI. Conclusion and Future Work

In order to effectively counter the non cooperative target of assembling tightly-coupled GNSS/IMU system by using GNSS spoofing technology, this paper establishes GNSS spoofing mathematical model, and proposes a slowly varying spoofing algorithm to avoid tightly-coupled GNSS/IMU with multiple anti-spoofing techniques based on the analysis of the influence mechanism of spoofing on the positioning of tightly-coupled GNSS/IMU, the algorithm proposes a measurement deviation determination method to avoid a variety of anti-spoofing techniques, which can gradually pull the positioning results of coupled system, and successfully avoid anti-spoofing techniques detection of least squares residual RAIM and parameter rationality check. The experimental results show that the algorithm can gradually change positioning of tightly-coupled GNSS/IMU within 30 s, and the north, east and down displacements basically achieve the spoofing effect, the errors with the expected offset are -0.5 m, 1.9 m and 12.7 m respectively. At the same time, the detection of the above anti-spoofing techniques is avoided. The mean value of test statistics for tightly-coupled system is reduced by 75.4% and does not exceed the alarm threshold, so as to achieve the purpose of spoofing, the effectiveness and high concealment of the spoofing algorithm are proved. The research results provide an effective solution for non cooperative targets equipped with tightly-coupled GNSS/IMU system to implement GNSS spoofing. On the other hand, it also provides reference for tightly-coupled GNSS/IMU system to detect and suppress GNSS spoofing.

In the future work, first, we will try to propose spoofing algorithm for coupled GNSS/IMU system with more complex anti-spoofing techniques, and carry out a large number of practical experiments. Second, we will try to propose spoofing algorithm for simultaneous interpreting of different sensors in integrated navigation system to enhance the flexibility of spoofing.

References

[1] M. Zhou *et al.*, "Induced spoofing detection of global navigation satellite system," *J. Nat. Univ. Defense Technol.,* vol. 41, no. 4, pp. 129–135, Aug. 2019.

[2] X. R. Zhang *et al.*, "Influence of spoofing interference on GNSS vector tracking loops," *J. Tsinghua Univ.*, vol. 62, no. 1, pp. 163–171, 2022, doi: 10.16511/j.cnki.qhdxxb.2021.21.023.

[3] M. Zhou, H. Li, and M. Q. Lu, "Calculation of the lower limit of the spoofing-signal ratio for a GNSS receiver-spoofer," *EURASIP J. Wireless Commun. Netw.,* vol. 1, Feb. 2018, Art. no. 44.

[4] T. E. Humphreys *et al.*, "Assessing the spoofing threat: Development of a portable GPS civilian spoofer," in *Proc. 21st Int. Tech. Meeting Satell. Division Inst. Navigation*, 2008, pp. 1169–1180.
[5] D. P. Shepard *et al.*, "Evaluation of smart grid and civilian UAV vulnerability to GPS spoofing attacks," in *Proc. 25th Int. Tech. Meeting Satell. Division Inst. Navigation*, 2012, pp. 2743–2757.
[6] Y. Guo, M. P. Wu, K. H. Tang, J. Tie, and X. Li, "Covert spoofing algorithm of UAV based on GPS/INS integrated navigation," *IEEE Trans. Veh. Technol.*, vol. 68, no. 7, pp. 6557–6564, Jul. 2019.
[7] K.-W. Huang and H.-M. Wang, "Combating the control signal spoofing attack in UAV systems," *IEEE Trans. Veh. Technol.,* vol. 67, no. 8, pp. 7769–7773, Aug. 2018.
[8] P. D. Groves, *Principles of GNSS, Inertial, and Multisensor Integrated Navigation Systems*, 2nd ed. Norwood, MA, USA: Artech House, 2013.
[9] W. Wang *et al.*, "Research on countering unmanned ground system and analysis and review of key technology," *Acta Aeronautica et Astronautica Sinica*, vol. 43, no. 3, pp. 1–27, Jan. 2021.
[10] S. Khanafseh, N. Roshan, S. Langel, F. C. Chan, M. Joerger, and B. Pervan, "GPS spoofing detection using RAIM with INS coupling," in *Proc. IEEE/ION Position, Location Navigation Symp.*, 2014, pp. 1232–1239.
[11] C. X. Peng, H. Li, and M. Q. Lu, "Research on the responses of GNSS tracking loop to intermediate spoofing," in *Proc. 32nd Int. Tech. Meeting Satell. Division Inst. Navigation*, 2019, pp. 943–952.
[12] Y. Gao *et al.*, "Intermediate spoofing strategies and countermeasures," *Tsinghua Sci. Technol.,* vol. 18, no. 06, pp. 599–605, Dec. 2013.
[13] Z. Han, Y. Z. Wang, and D. Ding, "Simulation analysis of GPS spoofing and its recognition based on tightly coupled integrated navigation," *Electron. Opt. Control*, vol. 25, no. 2, pp. 42–47, Feb. 2018.
[14] D. P. Shepard, J. A. Bhatti, and T. E. Humphreys, "Unmanned aircraft capture and control via GPS spoofing," *J. Field Robot.,* vol. 31, no. 4, pp. 617–636, 2014.
[15] S. Lu *et al.*, "Spoofing control strategy for precise position offset based on INS/GNSS tightly coupled navigation," *IEEE Access*, vol. 8, pp. 103585–103600, 2020.
[16] S. Zhao, Y. M. Chen, and J. A Farrell, "High-precision vehicle navigation in urban environments using an MEM's IMU and single-frequency GPS receiver," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 10, pp. 2854–2867, Oct. 2016.
[17] W. S. Wen, Y. C. Kan, and L. T. Hsu, "Performance comparison of GNSS/INS integrations based on EKF and factor graph optimization," in *Proc. 32nd Int. Tech. Meeting Satell. Division Inst. Navigation*, 2019, pp. 3019–3032.
[18] Y. J. Gao, "Research on key technology of satellite navigation spoofing interference," M.S. thesis, PLA Strategic Support Force Information Engineering Univ. for the Degree of Master of Engineering, Zhengzhou, China, 2020.
[19] X. L. Wang, *SINS/GPS Integrated Navigation Technology*. Beijing, China: Beihang Univ. Press, 2015.
[20] Y. J. Gao, Z. W. Lv, and L. D. Zhang, "Two-step trajectory spoofing algorithm for loosely coupled GNSS/IMU and NIS sequence detection," *IEEE Access*, vol. 7, pp. 96359–96371, 2019.
[21] G. Xie, *Principles of GPS and Receiver Design*. Beijing, China: Publishing House of Electronics Industry, 2009.
[22] Y. Guo, "Research on covert spoofing algorithm of UAV based on INS/GNSS integrated navigation," Ph. D. dissertation, National Univ. of Defense Technol., Changsha, China, 2019.
[23] Y. Liu *et al.*, "Impact assessment of GNSS spoofing attacks on INS/GNSS integrated navigation system," *Sensors,* vol. 18, no. 5, May 2018, Art. no. 1433.

Yangjun Gao was born in 1995. He received the B.S. and M.S. degrees in 2017 and 2020 from PLA Strategic Support Force Information Engineering University, Zhengzhou, China, where he is currently working toward the Ph.D.degree with the College of Geospatial Information. His research interests include GNSS applications.

Guangyun Li was born in 1965. He received the M.S. degee from the PLA Institute of Surveying and Mapping, Zhengzhou, China, in 1987. He is currently a Professor of the College of Geospatial Information, PLA Strategic Support Force Information Engineering University, Zhengzhou, China. He is responsible for teaching and researching in navigation and location services and applications.