IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 21 May 2022, accepted 17 June 2022, date of publication 27 June 2022, date of current version 15 July 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3186305

Tightly Coupled GNSS/INS Integration Spoofing Detection Algorithm Based on Innovation Rate Optimization and Robust Estimation

YE KE[1,2], ZHIWEI LV[1], CHAO ZHANG[1], XU DENG[1], WENLONG ZHOU[1], AND DEBIAO SONG[1]

[1]School of Geospatial Information, PLA Strategic Support Force Information Engineering University, Zhengzhou 450001, China
[2]Unit 31618, People's Liberation Army, Fuzhou 350000, China

Corresponding author: Zhiwei Lv (lvzhiwei@sina.com)

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.

ABSTRACT The spoofing detection algorithm for a global navigation satellite system/inertial navigation system (GNSS/INS) integrated navigation system based on the innovation rate and robust estimation has limitations such as extensive or invalid detection times, high missed detection rates, and false alarm rates. This study addresses these limitations by proposing a tightly coupled GNSS/INS integration spoofing detection algorithm based on innovation rate optimization and robust estimation. The proposed algorithm improved the normalized innovation of a small step or slow-growing ramp, thereby optimizing its innovation rate test statistics. The proposed approach also reduces the spoofing effect on the innovation rate by adaptively adjusting a gain matrix using robust estimation, thus improving the detection ability further. The simulation results show that the detection time of the proposed algorithm is reduced by 51.9% on average when dealing with small step or slow-growing ramp spoofing. Moreover, the missed detection rate decreases by 58% on average, and the false alarm rate remains at approximately zero. The proposed algorithm is suitable for spoofing detection in unmanned aerial vehicle applications of GNSS/INS integrated navigation systems with the advantages of fast detection and good performance.

INDEX TERMS Innovation rate optimization, robust estimation, spoofing detection, tightly coupled GNSS/INS integration.

I. INTRODUCTION

A global navigation satellite system (GNSS) and an inertial navigation system (INS) have complementary error characteristics [1]. A GNSS can provide global all-weather continuous position, velocity, and time services [2]. In contrast, an INS affords advantages such as independence, continuous operation, and short-term anti-spoofing ability. Therefore, a GNSS/INS integrated navigation system manages increased redundancy and reliability. However, due to the low power of the GNSS signal and the open structure, the GNSS service is easily affected by spoofing interference [3]. Spoofing interference implies that a spoofer generates spoofing signals similar to authentic signals (or retransmits authentic signals) to spoof the target receiver, thereby forcing it to generate erroneous and potentially dangerous information [4]. Some typical spoofing cases show that hackers deceive and capture GNSS signals to control sensors such as those in intelligent driving cars [5], yachts, and unmanned aerial vehicles (UAVs) [6]. This affects their trajectory planning schemes [7] and is potentially dangerous. In an integrated GNSS/INS system, the GNSS module locks the spoofing signal and outputs incorrect information. This affects the Kalman filter used to measure the estimated value of the state error in the update phase, outputting incorrect navigation results. Additionally, the estimated value of the incorrect state error is fed back to the INS through information fusion, thereby further affecting the integrated GNSS/INS system [8]. Therefore, real-time and accurate spoofing

The associate editor coordinating the review of this manuscript and approving it for publication was Diego Bellan.

detection is required to ensure the reliability and integrity of the integrated navigation system.

The spoofing detection algorithm of the GNSS/INS integrated navigation system is primarily based on an innovation vector as a test statistic and adopts a binary hypothesis test method. Typical methods include the chi-square test based on innovation or residuals [9], [10], autonomous integrity monitored extrapolation (AIME) [11], extended receiver autonomous integrity monitoring (ERAIM) [12], multiple solution separation (MSS) [13], and innovation rate [14]. The chi-square detection method based on innovation uses Kalman filter innovation as detection statistics, with the advantages of affordability, high efficiency, and computational simplicity. This approach is broadly used as a detection method. These methods can be divided into the ''snapshot method'' and ''sequential method'' [15]. The ''snapshot method'' is a test statistic composed of an innovation vector and its covariance matrix at the current moment, which is suitable for detecting step spoofing. In contrast, the ''sequential method'' implies that all innovation vectors and their covariance matrices from a certain time in the past to the current time constitute the test statistics, which is suitable for detecting ramp spoofing [16]. However, owing to the effect of spoofing, the GNSS input observation introduces errors in the innovation test statistics of the Kalman filter output. This decreases the sensitivity of this method regarding spoofing, resulting in long detection time problems, high false alarm rate, and high missed alarm rate [17]. The challenges of spoofing detection in GNSS/INS integrated navigation systems are related to the small step (or slow growth ramp) spoofing detection delay and closed-loop correction feedback mechanism [18].

Bhatti *et al.*. [14] proposed that the innovation rate should be used to judge whether the GNSS measured value was abnormal. Subsequently, the Kalman filter should be used to estimate the normalized innovation rate in real time. The detection time was 110 s when a single channel was affected by a slow-growing spoofing of 0.1 m/s. However, this method should be combined with AIME. Wang *et al.*. [18] improved the test statistics of the ''snapshot method'' and ''sequential method.'' In particular, the detection time was 28 s for spoofing with a small step of 5 m. Moreover, the detection time was 65 s for spoofing with slow growth of 0.1 m/s. Xu *et al*. [19] proposed the Multipath Estimation Delay Lock Loop (MEDLL) spoofing signal detection method, which successfully detected and identified 2 m/s ramp spoofing. Nevertheless, its ramp slope was 2 m/s, which was challenging to apply to 0.1 m/s slow-growing ramp spoofing. The three methods mentioned above only compared the detection time but did not compare the missed detection and false alarm rates. Thus, explaining the advantages and disadvantages of the detection performance of these algorithms was difficult.

Another method used to reduce the effect of spoofing and improve the reliability of the integrated navigation system is robust estimation. Thus, this approach is used to solve the problem of the closed-loop correction feedback mechanism of integrated navigation. In particular, an improved detection algorithm based on robust estimation and the ''detection window'' was proposed [20]. Its core idea was to select two suitable thresholds to calculate the weight factor, and adaptively adjust the measurement noise covariance matrix to reduce the weight of the spoofing measurement value, adaptively adjusting the gain matrix. When a single channel was subjected to a 0.5 m/s ramp spoofing, the improved algorithm reduced the detection time by 10 s and the missed detection rate by 9% compared with those of the traditional algorithm. In addition, Zhang *et al.*. [8] proposed a robust estimation detection algorithm for the innovation rate, which effectively suppressed the effect of spoofing on the state vectors and improved the data utilization rate and algorithm reliability. Moreover, this algorithm maintained the missed detection and false alarm rates within 4% in a 0.1 m/s slow-growing ramp spoofing in a single channel. However, the detection time of these two algorithms was extensive (or even ineffective) for slow-growing ramp spoofing, especially for spoofing with a slope less than 0.1 m/s. In the recent five years, some scholars studied spoofing detection algorithms such as neural networks [21] and support vector machines [17]. However, the calculation was complex, the compatibility was weak, and cost was high.

To address the above limitations of spoofing detection, this study first analyzes the spoofing model at the level of satellite navigation signals. Subsequently, the spoofing model for a GNSS/INS tightly coupled system measurement level is developed, focusing on analyzing the values added to the measurement pseudorange of the satellite channel and establishing the calculation models of step spoofing and ramp spoofing. Meanwhile, the influence of spoofing on the innovation of the Kalman filter is analyzed. This reduces the spoofing detection performance. The contribution of this study is to overcome the limitations of the traditional spoofing detection algorithm based on innovation rate robust estimation regarding extensive or invalid detection time, high missed detection rate, and high false alarm rate. In particular, a GNSS/INS tightly coupled system spoofing detection algorithm based on innovation rate optimization and robust estimation is proposed. Finally, the effectiveness, rationality, and feasibility of the proposed algorithm are verified by simulations.

II. GNSS SPOOFING MODEL AND INFLUENCE ANALYSIS

A. GNSS SPOOFING MODEL

First, the spoofing model was analyzed at the level of a satellite navigation signal [22] to develop the spoofing simulation environment of the GNSS/INS integrated navigation system and simulate the spoofing model at the GNSS measurement level. The spoofing of the target receiver is shown in Fig. 1.

A raw pseudorange model of the i-th satellite $R^{(i)}$ at time t is expressed as follows:

$$R^{(i)} = c\tau^{(i)} + c((t + \delta t_r) - (t + \delta t^{(i)})). \tag{1}$$

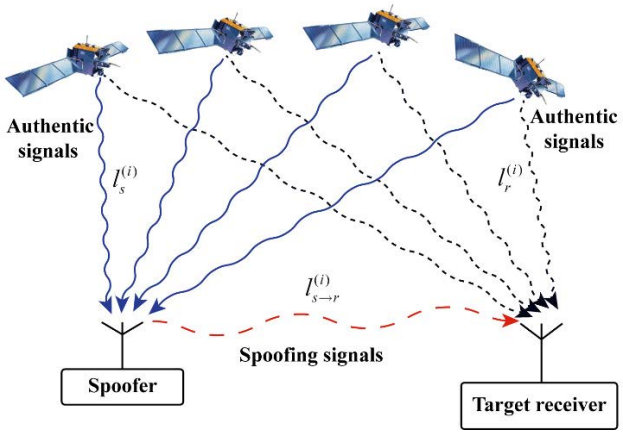

FIGURE 1. Spoofing of the target receiver.

In (1), c, $\tau^{(i)}$, δt_r, and $\delta t^{(i)}$ are the speed of light, signal delay, receiver clock, and satellite clock offsets, respectively.

$$\tau_a^{(i)} = \frac{l_r^{(i)}}{c} + I_a^{(i)} + T_a^{(i)}. \tag{2}$$

In (2), $l_r^{(i)}$, $I_a^{(i)}$, and $T_a^{(i)}$ are the authentic geometric distance, ionospheric, and tropospheric effects, respectively, which constitute the delay $\tau_a^{(i)}$ of the authentic signals.

$$R_a^{(i)} = l_r^{(i)} + c(\delta t_{r,a} - \delta t_a^{(i)} + I_a^{(i)} + T_a^{(i)}) + n_{l,a}^{(i)}. \tag{3}$$

In (3), $\delta t_{r,a}$, $\delta t_a^{(i)}$, and $n_{l,a}^{(i)}$ are the authentic clock, clock offsets, and receiver noise, respectively, which constitute the authentic pseudorange $R_a^{(i)}$.

$$\tau_s^{(i)} = \frac{l_s^{(i)} + l_{s\to r}^{(i)}}{c} + I_s^{(i)} + T_s^{(i)}. \tag{4}$$

In (4), $l_s^{(i)}$ and $l_{s\to r}^{(i)}$ are the geometric range from the spoofer to the satellite and the geometric range from the spoofer to the target receiver, respectively, which constitute the delay $\tau_s^{(i)}$ of spoofing signals. Assuming that external factors and errors for the spoofer and the target receiver are ignored, (4) can be rewritten as follows:

$$\tau_s^{(i)} = \tau_a^{(i)} + \nabla\tau_s^{(i)}, \tag{5}$$

where $\nabla\tau_s^{(i)}$ is the additional signal delay introduced by the spoofer in the target receiver, and the relationship between the spoofing and the authentic pseudoranges is expressed as follows:

$$R_s^{(i)} = R_a^{(i)} + c\nabla\tau_s^{(i)}. \tag{6}$$

Thus, the spoofing model at the measurement level can be obtained, and the authentic and spoofing pseudorange measurements of the i-th channel are $L_a^{(i)}(t)$ and$L_s^{(i)}(t)$, respectively.

$$L_a^{(i)}(t) = c\tau^{(i)} + c((t + \delta t_r) - (t + \delta t^{(i)})). \tag{7}$$

$$L_s^{(i)}(t) = c\tau^{(i)} + c((t + \delta t_r) - (t + \delta t^{(i)})) + s(t). \tag{8}$$

By subtracting the authentic pseudorange from the spoofing pseudorange, the values added to the pseudorange, $s(t)$, after successful spoofing can be obtained as follows:

$$L_s^{(i)}(t) - L_a^{(i)}(t) = \begin{cases} s(t), & t \geq t_{Lock} \\ 0, & t < t_{Lock}, \end{cases} \tag{9}$$

where t_{Lock} is the time when the spoofing signal locks the tracking loop of the target receiver so that $s(t)$ are the values added to the spoofing pseudorange, a is the slope, and $a(t - t_{Lock}) + b$ is the pseudorange deviation between the spoofing and authentic pseudorange. Thus, two methods can be used to develop the spoofing model at the measurement level: 1) $a \neq 0$ and $b = 0$ represent step spoofing; 2) $a = 0$ and $b \neq 0$ represent ramp spoofing.

B. ANALYSIS OF THE SPOOFING INFLUENCE

A tightly integrated navigation system uses the GNSS pseudoranges and pseudorange rates as inputs. In a closed-loop correction, each filter iteration feeds back the estimated position, velocity, and attitude errors to the INS processor to correct the INS solution. The 17-dimensional state vector of the error state extended Kalman filter (EKF) is $\boldsymbol{X}$ expressed as in [23] as follows:

$$\boldsymbol{X} = \left[\delta\boldsymbol{\varphi};\quad \delta\boldsymbol{v};\quad \delta\boldsymbol{r};\quad \boldsymbol{b}_a;\quad \boldsymbol{b}_g;\quad \boldsymbol{b}^{clk};\quad \dot{\boldsymbol{b}}^{clk} \right]^T. \tag{10}$$

In (10), $\delta\boldsymbol{\varphi}$, $\delta\boldsymbol{v}$, and $\delta\boldsymbol{r}$ are the attitude, velocity and position vectors of the INS estimation error, respectively, $\boldsymbol{b}_a$ and $\boldsymbol{b}_g$ are the accelerometer and gyro biases of the inertial sensor, respectively, and $\boldsymbol{b}^{clk}$ and $\dot{\boldsymbol{b}}^{clk}$ are the GNSS clock error and clock drift, respectively. The symbol "$\wedge$" denotes the estimated value, the superscript "$-$" denotes the prior estimate, and the symbol "$+$" denotes the posterior estimate. Let $\boldsymbol{Z}_k$ be the observation vector differing from the GNSS observation value and the INS prediction value, $\boldsymbol{H}_k$ be the observation matrix, $\hat{\boldsymbol{X}}_k^-$ be the prior estimation state vector, $\boldsymbol{P}_k^-$ be the prior estimation state vector covariance matrix, and $\boldsymbol{R}_k$ be the observation noise covariance matrix. Then, the observation $\boldsymbol{Z}_k$, innovation vector $\boldsymbol{r}_k$ and their covariance matrix $\boldsymbol{V}_k$, respectively, can be expressed as in [24]:

$$\boldsymbol{Z}_k = \begin{pmatrix} \boldsymbol{Z}_{\rho,k} \\ \boldsymbol{Z}_{\dot{\rho},k} \end{pmatrix} = \begin{pmatrix} \rho_G^1 - \rho_I^1 \\ \vdots \\ \rho_G^n - \rho_I^n \\ \dot{\rho}_G^1 - \dot{\rho}_I^1 \\ \vdots \\ \dot{\rho}_G^n - \dot{\rho}_I^n \end{pmatrix}. \tag{11}$$

$$\boldsymbol{r}_k = \boldsymbol{Z}_k - \boldsymbol{H}_k\hat{\boldsymbol{X}}_k^-. \tag{12}$$

$$\boldsymbol{V}_k = \boldsymbol{H}_k\boldsymbol{P}_k^-\boldsymbol{H}_k^T + \boldsymbol{R}_k. \tag{13}$$

In (11), ρ_G^i, $\dot{\rho}_G^i$, ρ_I^i, and ρ_I^i are the GNSS pseudorange and pseudorange rate, INS predicted pseudorange, and predicted pseudorange rate, respectively, n represents the number of

visible satellites. The normalized innovation is defined as follows:

$$\omega_i = \frac{r_k^i}{\sqrt{V_k^{ii}}}. \tag{14}$$

In (14), r_k^i is the i-th ($i = 1, \cdots, n$, n is the number of visible satellites) value of the innovation vector at time k, and V_k^{ii} is the variance of r_k^i. Moreover, ω_i represents the i-th innovation value after normalization, which can reflect the i-th GNSS measurement error. The innovation vector reflects the values added to the pseudorange as a result of spoofing, which is called spoofing innovation $\boldsymbol{r}_{k,s}$.

However, because the filter has the effect of spoofing and closed-loop correction in the prediction and update stages, the authentic innovation is not equal to the spoofing innovation. When spoofing is applied at time k, in the state filtering loop, the change of the GNSS observation value $\boldsymbol{Z}_k$ produces spoofing effects, affecting the innovation vector $\boldsymbol{r}_k$ and the state filtering loop at time $k+1$. The analysis and explanation of the spoofing effect are shown in Fig. 2, and the specific derivation is described below.

Assuming that spoofing occurs at time k, the observation is expressed as follows [17]:

$$\boldsymbol{Z}_{k,s} = \boldsymbol{Z}_k + \Delta\boldsymbol{Z}_k. \tag{15}$$

In (15), $\boldsymbol{Z}_{k,s}$, $\boldsymbol{Z}_k$, and $\Delta\boldsymbol{Z}$ are the spoofing observation, the expected observation, and the amplitude of spoofing, respectively. When spoofing occurs, the spoofing innovation $\boldsymbol{r}_{k,s}$ is as follows:

$$\begin{aligned}\boldsymbol{r}_{k,s} &= \boldsymbol{Z}_{k,s} - \boldsymbol{H}_k\hat{\boldsymbol{X}}_k^- \\ &= \boldsymbol{Z}_k + \Delta\boldsymbol{Z}_k - \boldsymbol{H}_k\hat{\boldsymbol{X}}_k^- \\ &= \boldsymbol{r}_k + \Delta\boldsymbol{Z}_k.\end{aligned} \tag{16}$$

According to the Kalman filter theory, the state estimation value is as follows:

$$\begin{aligned}\hat{\boldsymbol{X}}_{k,s}^+ &= \hat{\boldsymbol{X}}_k^- + \boldsymbol{K}_k\boldsymbol{r}_{k,s} \\ &= \hat{\boldsymbol{X}}_k^- + \boldsymbol{K}_k(\boldsymbol{r}_k + \Delta\boldsymbol{Z}_k) \\ &= \hat{\boldsymbol{X}}_k^+ + \boldsymbol{K}_k\Delta\boldsymbol{Z}_k,\end{aligned} \tag{17}$$

where $\hat{\boldsymbol{X}}_k^+$ and $\hat{\boldsymbol{X}}_{k,s}^+$ represent the posterior state estimation at time k and the posterior state estimation with spoofing, respectively. For time update at time $k+1$:

$$\hat{\boldsymbol{X}}_{k+1}^- = \boldsymbol{\Phi}_k\hat{\boldsymbol{X}}_k^+, \tag{18}$$

$$\begin{aligned}\hat{\boldsymbol{X}}_{k+1,s}^- &= \boldsymbol{\Phi}_k\hat{\boldsymbol{X}}_{k,s}^+ \\ &= \boldsymbol{\Phi}_k(\hat{\boldsymbol{X}}_k^+ + \boldsymbol{K}_k\Delta\boldsymbol{Z}_k) \\ &= \hat{\boldsymbol{X}}_{k+1}^- + \boldsymbol{\Phi}_k\boldsymbol{K}_k\Delta\boldsymbol{Z}_k,\end{aligned} \tag{19}$$

$$\boldsymbol{r}_{k+1} = \boldsymbol{Z}_{k+1} - \boldsymbol{H}_{k+1}\hat{\boldsymbol{X}}_{k+1}^-, \tag{20}$$

where $\boldsymbol{\Phi}_k$ and $\boldsymbol{K}_k$ are the transfer matrix and the gain matrix, respectively, the spoofing innovation $\boldsymbol{r}_{k+1,s}$ is derived as follows:

$$\begin{aligned}\boldsymbol{r}_{k+1,s} &= \boldsymbol{Z}_{k+1,s} - \boldsymbol{H}_{k+1}\hat{\boldsymbol{X}}_{k+1,s}^- \\ &= \boldsymbol{Z}_{k+1} + \Delta\boldsymbol{Z}_{k+1} - \boldsymbol{H}_{k+1}\boldsymbol{\Phi}_k\hat{\boldsymbol{X}}_{k,s}^+ \\ &= \boldsymbol{Z}_{k+1} + \Delta\boldsymbol{Z}_{k+1} - \boldsymbol{H}_{k+1}\boldsymbol{\Phi}_k(\hat{\boldsymbol{X}}_k^- + \boldsymbol{K}_k\boldsymbol{r}_{k,s}) \\ &= \boldsymbol{Z}_{k+1} + \Delta\boldsymbol{Z}_{k+1} - \boldsymbol{H}_{k+1}\boldsymbol{\Phi}_k(\hat{\boldsymbol{X}}_k^+ + \boldsymbol{K}_k\Delta\boldsymbol{Z}_k) \\ &= \boldsymbol{r}_{k+1} + \Delta\boldsymbol{Z}_{k+1} - \boldsymbol{H}_{k+1}\boldsymbol{\Phi}_k\boldsymbol{K}_k\Delta\boldsymbol{Z}_k.\end{aligned} \tag{21}$$

which can be expressed as

$$\boldsymbol{r}_{k+1,s} = \boldsymbol{r}_{f(k+1)} - \Delta\boldsymbol{r}_{f(k+1)}, \tag{22}$$

in addition,

$$\begin{aligned}\boldsymbol{r}_{f(k+1)} &= \boldsymbol{r}_{k+1} + \Delta\boldsymbol{Z}_{k+1} \\ \Delta\boldsymbol{r}_{f(k+1)} &= \boldsymbol{H}_{k+1}\boldsymbol{\Phi}_k\boldsymbol{K}_k\Delta\boldsymbol{Z}_k,\end{aligned} \tag{23}$$

where $\boldsymbol{r}_{f(k+1)}$ and $\Delta\boldsymbol{r}_{f(k+1)}$ represent the real value of the innovation when spoofing occurs and the component of the innovation caused by spoofing, respectively. It can be concluded that the increment of innovation decreases $\boldsymbol{H}_{k+1}\boldsymbol{\Phi}_k\boldsymbol{K}_k\Delta\boldsymbol{Z}_k$, which will accumulate over time through the recursive calculation process, resulting in a greater decrease in the increment of innovation, thus reducing the detection performance of spoofing.

III. TIGHTLY COUPLED GNSS/INS INTEGRATION SPOOFING DETECTION ALGORITHM BASED ON INNOVATION RATE AND ROBUST ESTIMATION

A. SPOOFING DETECTION ALGORITHM BASED ON INNOVATION RATE

The innovation rate spoofing detection algorithm is developed to judge whether the GNSS measured value is affected by spoofing by normalizing the change rate of innovation ω_i. Considering the effect of the measurement noise, the Kalman filter is usually used to update the change rate of the normalized innovation ω_i in real time. The detection quantity v_i of the innovation rate was derived in [14].

Assuming that spoofing does not exist, the null hypothesis is $H_0 : v_i \sim N(0, 1)$, and the alternative hypothesis is $H_1 : v_i \sim N(\delta, 1)$, where v_i follows a normal distribution, and δ is a noncentral parameter. According to the integrity requirements of the navigation system [25], if the false alarm probability is set to P_{fa}, the corresponding false alarm probability of the i-th measurement value a_0 is as follows [26]:

$$a_0 = 1 - \sqrt[n]{1 - P_{fa}}. \tag{24}$$

Thus, the detection threshold v_D corresponding to the innovation rate v_i is as follows [16]:

$$v_D = \sqrt{P_{v_i}}Q^{-1}(\frac{a_0}{2}). \tag{25}$$

In (24), Q^{-1} is the inverse of the Gaussian distribution, and P_{v_i} is the variance of the covariance matrix of v_i.

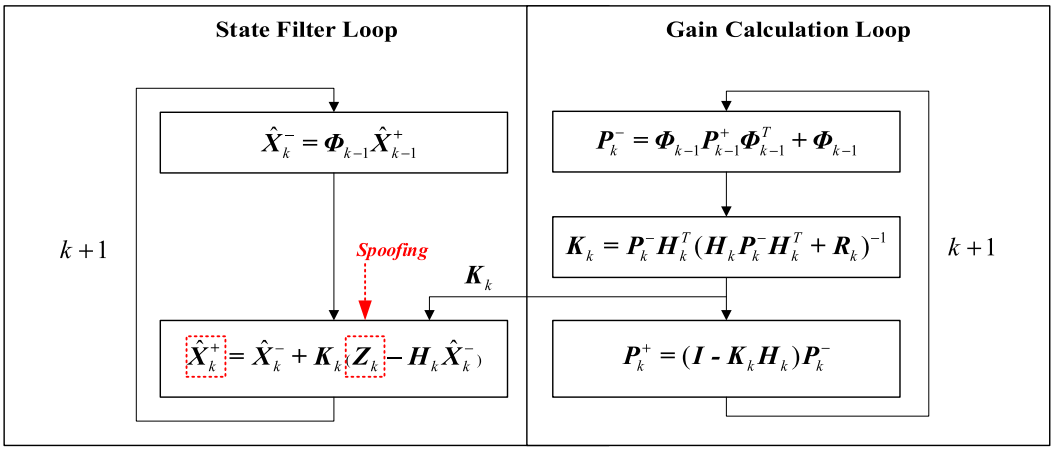

FIGURE 2. Analysis of spoofing influence.

Subsequently, the spoofing detection criteria is

$$\begin{cases} v_i \geq v_D. & \text{With spoofing} \\ v_i < v_D. & \text{Without spoofing.} \end{cases} \tag{26}$$

Because the accumulation of errors will lead to an increase or decrease in innovation, the innovation rate spoofing detection algorithm can determine whether spoofing exists by detecting an increase or decrease in the innovation rate without waiting for the accumulation of errors to a certain extent before being detected. Therefore, the detection time of the innovation rate spoofing detection algorithm is shorter than that of the innovation spoofing detection algorithm. However, the filter for calculating the innovation rate cannot be detected before convergence.

B. SPOOFING DETECTION ALGORITHM BASED ON INNOVATION RATE AND ROBUST ESTIMATION

As discussed in Section II-A, GNSS spoofing affects the performance of the spoofing detection. Based on the innovation rate spoofing detection algorithm, the effect of the spoofing can be well reduced by introducing robust estimation, selecting the IGG-3 equivalent weight function [27], and using the innovation rate v_i to calculate the equivalent weight as follows:

$$w_i = \begin{cases} 1, & |v_i| \leq k_0 \\ \dfrac{k_0}{|v_i|}\left\{\dfrac{k_1 - |v_i|}{k_1 - k_0}\right\}^2, & k_0 < |v_i| \leq k_1 \\ 0, & |v_i| > k_1, \end{cases} \tag{27}$$

where v_i is the innovation rate of the i-th GNSS measurement, and w_i is the corresponding equal weight. In general, $k_1 = v_D$ and $k_0 = 0.5k_1$. When $|v_i| \leq k_0$, it means that there is no spoofing in the i-th measurement, and the weight of the dimensional measurement is equal to 1. When $|v_i| > k$, it means that there is spoofing in the i-th measurement, and the weight of the dimension measurement is equal to zero; therefore, it does not enter the Kalman filter update. When $k_0 < |v_i| \leq k$, it indicates that the i-th measurement may be affected by spoofing, and the weight of the dimension measurement is less than 1. Weight reduction processing is performed to reduce the influence on innovation, thereby improving the spoofing detection performance.

According to the adaptive adjustment of the equivalent weight function, the equivalent weight matrix, $\boldsymbol{W}$, is defined as follows:

$$\boldsymbol{W} = diag(\, w_1 \quad \cdots \quad w_i \quad \cdots \quad w_n \,). \tag{28}$$

Adjusting the gain matrix $\boldsymbol{K}_k$ yields the following [18]:

$$\boldsymbol{K}_R = \boldsymbol{K}_k \cdot \boldsymbol{W}. \tag{29}$$

According to the previous analysis, a $\Delta \boldsymbol{r}_{f(k+1)}$ between the spoofing innovation and the authentic innovation exists, directly causing the innovation to decrease. Therefore, reducing $\Delta \boldsymbol{r}_{f(k+1)}$ is an effective way to improve the ability of spoofing detection. Thus, replacing $\boldsymbol{K}_k$ in (22) by $\boldsymbol{K}_R$, the following equation is obtained:

$$\Delta \boldsymbol{r}_{f(k+1)} = \boldsymbol{H}_{k+1}\boldsymbol{\Phi}_k\boldsymbol{K}_R\Delta\boldsymbol{Z}_k = \boldsymbol{H}_{k+1}\boldsymbol{\Phi}_k(\underbrace{\boldsymbol{K}_k \cdot \boldsymbol{W}}_{\boldsymbol{K}_R})\Delta\boldsymbol{Z}_k. \tag{30}$$

Therefore, when spoofing exists, the element $\Delta \boldsymbol{Z}_i$ in $\Delta \boldsymbol{Z}_k$ increases or decreases, causing the normalized innovation ω_i at time k to increase or decrease, causing the innovation rate $|v_i|$ to increase, while (27) adaptively adjusts the equivalent weight matrix; thus, adjusting the gain matrix to reduce the weight of spoofing, effectively weakening the abnormal effect, and improving the detection ability of the integrated navigation system. However, the algorithm requires extensive time to detect small step and slow-growth spoofing and even fails to detect it.

IV. SPOOFING DETECTION ALGORITHM BASED ON INNOVATION RATE OPTIMIZATION AND ROBUST ESTIMATION

The limitations described above are solved by improving the innovation rate robust estimation spoofing detection algorithm. Thus, a GNSS/INS tightly coupled system spoofing detection algorithm based on innovation rate optimization and robust estimation is proposed. The proposed algorithm improved the normalized innovation of small step or slow-growth spoofing. Thus, it optimized the statistical test amount of the innovation rate, solved the challenge of extensive or even invalid detection time for small step or slow-growth ramp spoofing, and reduced the detection time to improve the detection performance. Next, the improved methods and ideas of the two algorithms will be given.

A. IMPROVED SMALL-STEP SPOOFING DETECTION ALGORITHM

Assuming that small-step spoofing is applied to the pseudorange by adding the value B, the normalized innovation ω_i^{ST} of small-step spoofing is improved when the i-th measurement is performed as follows:

$$\omega_i^{ST} = \frac{B + r_k^i}{\sqrt{V_k^{ii}}} = b + \omega_i. \tag{31}$$

In (31), r_k^i and V_k^{ii} are obtained from (12) and (13), respectively, ω_i is the normalized innovation without spoofing, equivalent to (14), the variable b is equal to the actual small step B divided by the normalized variance $\sqrt{V_k^{ii}}$. The innovation rate v_i^{ST} of the small step is obtained by updating ω_i^{ST} in real time using the Kalman filter.

Defining the state vector as $\boldsymbol{x}$ as follows:

$$\boldsymbol{x} = (\hat{\omega}_i^{ST};\quad v_i^{ST};\quad a_i^{ST};\quad p_i^{ST}). \tag{32}$$

In (32), $\hat{\omega}_i^{ST}$ is the estimated value of ω_i^{ST}, v_i^{ST} is the innovation rate of ω_i^{ST}, a_i^{ST} is the innovation acceleration of ω_i^{ST}, and p_i^{ST} is the constant deviation of ω_i^{ST}.

The system model is defined as in [14] as follows:

$$\begin{bmatrix} \dot{\hat{\omega}}_i^{ST} \\ \dot{v}_i^{ST} \\ \dot{a}_i^{ST} \\ \dot{p}_i^{ST} \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & -\alpha & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} \hat{\omega}_i^{ST} \\ v_i^{ST} \\ a_i^{ST} \\ p_i^{ST} \end{bmatrix} + \begin{bmatrix} 0 \\ \varepsilon \\ 0 \\ 0 \end{bmatrix}. \tag{33}$$

In (33), the improved innovation rate is defined as a time-dependent stochastic process, and α is the correlation coefficient, generally 0.5–0.9, ε is the noise, generally 10^{-7}–10^{-9} [28].

The observation model is defined as follows:

$$\omega_i^{ST} = \begin{bmatrix} 1 & 0 & 0 & -1 \end{bmatrix} \begin{bmatrix} \hat{\omega}_i^{ST} \\ v_i^{ST} \\ a_i^{ST} \\ p_i^{ST} \end{bmatrix} + \upsilon_i^{ST}. \tag{34}$$

In (34), ω_i^{ST} is the measured value input, and υ_i^{ST} is the observed noise. The improved innovation rate test statistic is calculated by using a double-layer Kalman filter. The flow chart of its implementation is shown in Fig. 3. The specific steps and detailed derivation are as follows:

1) SPECIFIC STEPS

Specific steps involve a double-layer Kalman filter: the main navigation Kalman filter was used to calculate the innovation value, and the innovation rate Kalman filter was used to calculate the innovation rate.

1) Calculate the innovation vector. In the main navigation Kalman filter, the innovation vector $\boldsymbol{r}_k$ and the variance V_k^{ii} are calculated from (12) and (13).
2) Calculate the improved normalized innovation. The improved normalized innovation $\boldsymbol{\omega}_i^{ST}$ was computed by substituting $\boldsymbol{r}_k$, V_k^{ii}, and the value of B added to the pseudorange in small steps into (31).
3) Initialize the innovation rate Kalman filter. State variables were initialized, and covariance values, noise matrices, and dynamic matrices were estimated.
4) Calculate the innovation rate. $\boldsymbol{\omega}_i^{ST}$ was fed back to the innovation rate Kalman filter for real-time updating, and the innovation rate $\boldsymbol{v}_i^{ST}$ was obtained.
5) Compare thresholds. $\boldsymbol{v}_i^{ST}$ was compared with the detection threshold v_D.

2) DETAILED DERIVATION

a: TIME UPDATE

Step 1: prior state estimation

$$\hat{\boldsymbol{x}}_k^- = \boldsymbol{\varphi}_{k-1}\hat{\boldsymbol{x}}_{k-1}^+, \tag{35}$$

Step 2: prior covariance estimation

$$\boldsymbol{p}_k^- = \boldsymbol{\varphi}_{k-1}\boldsymbol{p}_{k-1}^+\boldsymbol{\varphi}_{k-1}^T + \boldsymbol{q}_{k-1}, \tag{36}$$

where the symbol "$\wedge$" denotes the estimated value, the superscript "$-$" denotes the prior estimate and the symbol "$+$" denotes the posterior estimate. $\boldsymbol{x}_k^-$, $\boldsymbol{x}_{k-1}^+$, and $\boldsymbol{\varphi}_{k-1}$ represent the prior estimate at time k, the posterior estimate and the state transition matrix at time $k-1$, respectively. $\boldsymbol{p}_k^-$, $\boldsymbol{p}_{k-1}^+$, and $\boldsymbol{q}_{k-1}$ represent the prior error covariance matrix at time k, the posterior error covariance matrix and the system noise covariance matrix at time $k-1$, respectively.

b: MEASUREMENT UPDATES

In the update stage of the traditional Kalman filter, the observation vectors $\boldsymbol{Z}_k$ and $\boldsymbol{H}_k\hat{\boldsymbol{X}}_k^-$ were subtracted to obtain innovation vectors $\boldsymbol{r}_k$. In contrast, in the proposed algorithm, the improved normalized innovation $\boldsymbol{\omega}_i^{ST}$ and $\boldsymbol{H}_k\hat{\boldsymbol{x}}_k^-$ are subtracted to obtain the small-step spoofing innovation vector $\boldsymbol{r}_k^{ST}$ and subsequently updated in real time to obtain $\hat{\boldsymbol{x}}_k^+$.

Step 1: improved spoofing innovation vector

$$\boldsymbol{r}_k^{ST} = \boldsymbol{\omega}_i^{ST} - \boldsymbol{H}_k\hat{\boldsymbol{x}}_k^-, \tag{37}$$

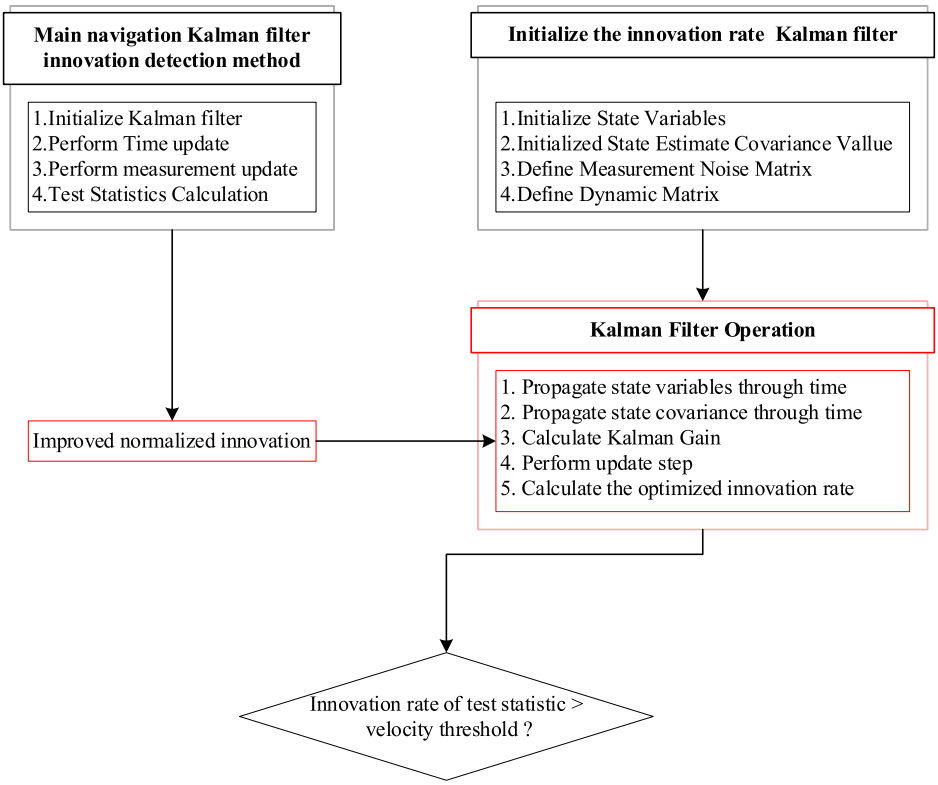

FIGURE 3. Flow chart of improved innovation rate test statistics.

where (37) can be regarded as a variant of (12), $\boldsymbol{\omega}_i^{ST}$ corresponds to the observation value $\boldsymbol{Z}_k$, and $\boldsymbol{\omega}_i^{ST}$ was used as an input for the observation value of the innovation rate.

Step 2: gain matrix

$$\boldsymbol{K}_k = \boldsymbol{p}_k^- \boldsymbol{H}_k^T (\boldsymbol{H}_k \boldsymbol{p}_k^- \boldsymbol{H}_k^T + \boldsymbol{R}_k)^{-1}, \tag{38}$$

Step 3: posteriori state estimation

$$\begin{aligned} \hat{\boldsymbol{x}}_k^+ &= \hat{\boldsymbol{x}}_k^- + \boldsymbol{K}_k \boldsymbol{r}_k^{ST} \\ &= \hat{\boldsymbol{x}}_k^- + \boldsymbol{K}_k (\boldsymbol{\omega}_i^{ST} - \boldsymbol{H}_k \hat{\boldsymbol{x}}_k^-), \end{aligned} \tag{39}$$

Step 4: posteriori covariance estimation

$$\boldsymbol{p}_k^+ = (\boldsymbol{I} - \boldsymbol{K}_k \boldsymbol{H}_k) \boldsymbol{p}_k^-, \tag{40}$$

where $\boldsymbol{H}_k$ and $\boldsymbol{R}_k$ represent the observation matrix and the observation noise covariance matrix. In the measurement update, the improved test statistic, $\boldsymbol{\omega}_i^{ST}$, was inputted into the Kalman filter as the observation value for cyclic updating. Then, the optimized small-step innovation rate $\boldsymbol{v}_i^{ST}$ was calculated through innovation rate output matrices $\boldsymbol{C}$ and $\hat{\boldsymbol{x}}_k^+$ as follows:

$$\boldsymbol{v}_i^{ST} = \boldsymbol{C} \cdot \hat{\boldsymbol{x}}_k^+. \tag{41}$$

In (40), $\boldsymbol{C} = [\,0\ 1\ 0\ 0\,]$.

The criteria for judging whether small-step spoofing was detected are as follows:

$$\begin{cases} v_i^{ST} \geq v_D. & \text{With spoofing} \\ v_i^{ST} < v_D. & \text{Without spoofing.} \end{cases} \tag{42}$$

B. IMPROVED SLOW-GROWING RAMP SPOOFING DETECTION ALGORITHM

Suppose that slow-growing ramp spoofing is applied by adding the value A to the pseudorange, and the change rate a of the normalized innovation amplitude remains unchanged over time, which occurs in the i-th measurement. In this case, the normalized innovation ω_i^{SG} of the improved slow-growing ramp spoofing is as follows:

$$\omega_i^{SG} = \frac{A + r_k^i}{\sqrt{V_k^{ii}}} = \frac{a(t - t_{Lock})}{\sqrt{V_k^{ii}}} + \omega_i = a' + \omega_i. \tag{43}$$

In (43), the variable a' is equal to the actual slow growth $a(t - t_{Lock})$ divided by the normalized variance $\sqrt{V_k^{ii}}$. The innovation rate $\dot{v}_i^{SG}$ of a small step is obtained by updating ω_i^{SG} in real time using the Kalman filter, similar to the small-step spoofing detection algorithm. Thus, this is not described in detail here.

As described above, the improved spoofing algorithm for small step or slow-growth spoofing is shown in Fig. 4, where "#" represents the innovation rate test statistic of the small step ($\dot{v}_i^{ST}$) or slow growth ($\dot{v}_i^{SG}$). The specific steps are as follows:

1) The main navigation Kalman filter for the innovation detection method: perform time and measurement updates to prepare for the next calculation of the normalized innovation.

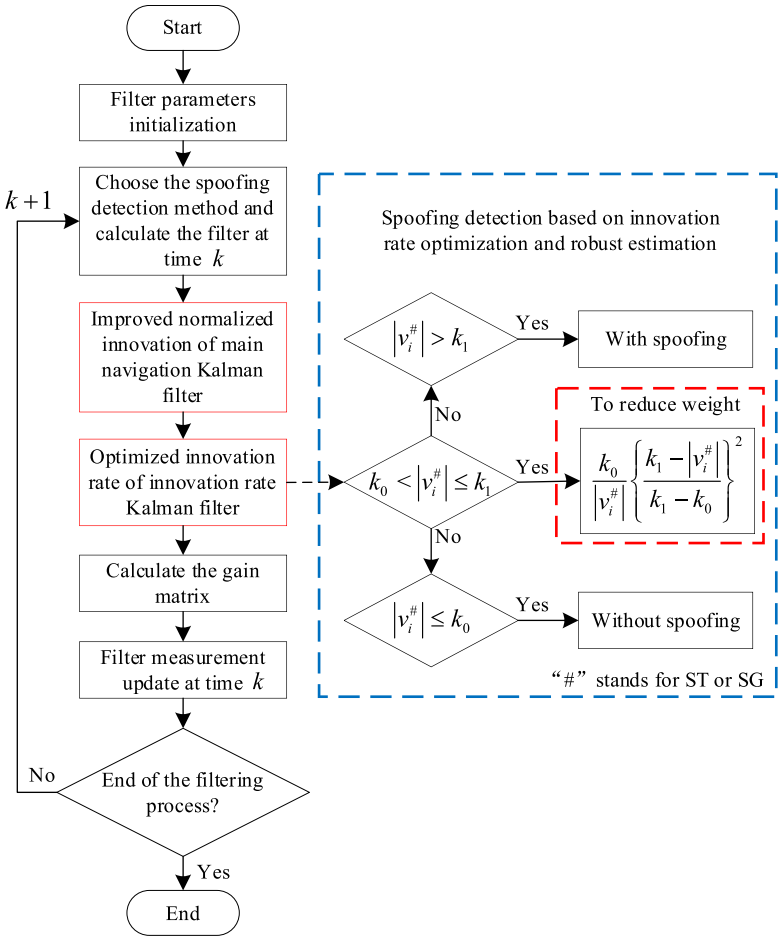

FIGURE 4. Flow chart of the proposed algorithm.

2) Initialize the innovation rate Kalman filter: including state variables, covariance values, measurement noise, and others.
3) Improve normalized innovation: from Section IV-A, using the "improved small-step spoofing detection algorithm," as an example, the improved normalized innovation ω_i^{ST} is calculated from (31) at time k.
4) Optimize the innovation rate: the improved normalized innovation is inputted into the Kalman filter using (37) to obtain a posterior estimated state $\hat{\boldsymbol{x}}_k^+$, and the innovation rate $\boldsymbol{v}_i^{ST}$ is calculated by (41).
5) Robust estimation: the equivalent weight matrix $\boldsymbol{W}$ is calculated from (27).
6) Gain matrix: the gain matrix $\boldsymbol{K}_R$ is calculated from (29) and the measurement is updated.
7) Filter cycle update: the spoofing detection process is completed at time k and step 1) is returned at time $k+1$.

V. RESULTS AND DISCUSSION

Various detection algorithms were implemented to verify the effectiveness of the proposed algorithm. In particular, the innovation rate spoofing (M1), innovation rate robust estimation spoofing (M2), improved small-step spoofing detection algorithm (M3), and improved slow-growth ramp spoofing (M4) detection algorithms were implemented.

Based on simulation experiments with GNSS/INS tightly coupled system spoofing detection, four scenarios were designed. 1) The detection ability of M1 and M2 were compared for the case when three channels were spoofed by step or ramp spoofing with the same value added to the pseudorange. 2) The detection ability of M2 was verified for the case when one channel was spoofed by step or ramp spoofing with a different value added to the pseudorange. 3) The detection abilities of M2 and M3 were compared for the case when one channel was spoofed by a small step. 4) The detection abilities of M2 and M4 were compared for the case when one channel was spoofed by a slow-growth ramp.

A. SIMULATION CONDITIONS

Referring to the simulation software guide [29], the GNSS constellation model was a single constellation, dual-frequency, and circular orbit model. Moreover, the satellites were all distributed on six orbital planes, without GNSS signal occlusion, attenuation, interference, or reflection. In particular, the following simulation conditions were

TABLE 1. Simulation parameters.

Sensors	Parameter	Value
GNSS	Number of visible satellites	8
	Output rate	1 Hz
	Pseudorange noise (1 σ)	2.5 m
IMU	Accelerometer rabdom walk noise	20 mg $/\sqrt{\text{Hz}}$
	Accelerometer biases drift	(30,-45, 26) mg
	Gyro rabdom walk noise	0.002 ° $/\sqrt{\text{h}}$
	Gyro biases drift	(-0.0009, 0.0013,-0.0008) ° / h
	Output rate	100 Hz

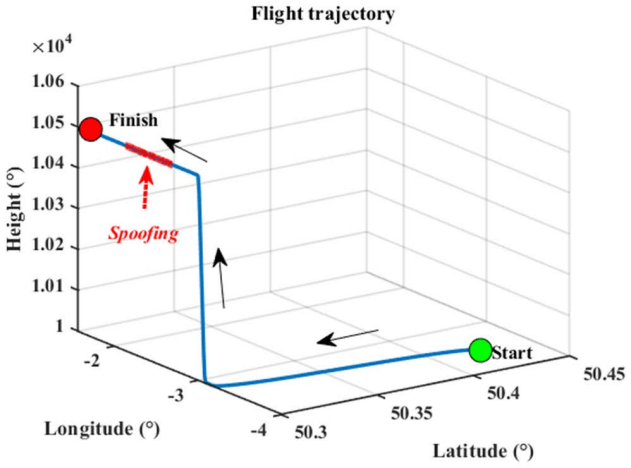

FIGURE 5. Flight trajectory.

TABLE 2. Spoofing scenario 1.

Spoofing type	Pseudorange added value	C	Time
Step	30 m	1, 2, and 3	350–550 s
Ramp	0.3 m/s		

considered: the false alarm rate was $P_{fa} = 4 \times 10^{-6}$ [30], and the thresholds of M1, M2, M3, and M4 were all 0.0029517 m/s. The parameters of the GNSS and IMU modules are listed in Table 1. The airborne motion was simulated in MATLAB, considering a speed of 200 m/s, two 45 turns, and climbs that last 746 s. The flight path is shown in Fig. 5.

B. SIMULATION RESULTS AND ANALYSIS

1) SCENARIO 1

Scenario 1 was set according to Table 2, where "C" stands for channel. Two sets of experiments were set up. The detection capabilities of M1 and M2 were compared when channels 1, 2, and 3 were spoofed by adding the same value to the pseudorange.

The first set of step spoofing simulation results is plotted in Fig. 6. In particular, step spoofing with a pseudorange deviation of 30 m was applied to channels 1, 2, and 3 in 350–550 s. In the legend, "C" and "T" represent channel

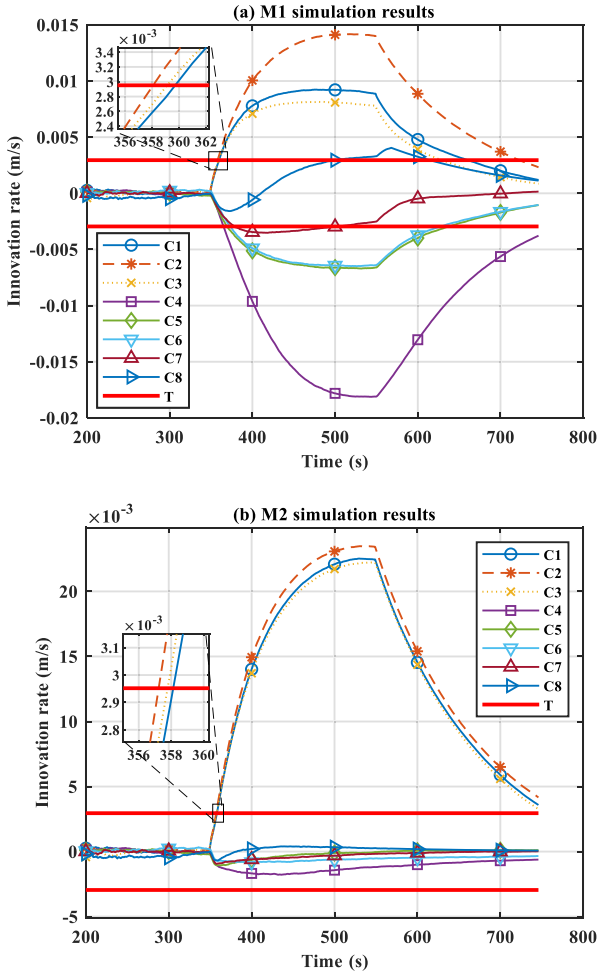

FIGURE 6. Comparison of the simulation results for step spoofing of M1 and M2.

and threshold, that is, "C1," "C2," and "C3" etc. represent channels 1, 2, and 3, etc., respectively, and are not repeated in the following legends. Fig. 6(a) shows the M1 simulation results. Note that the detection times of channels 1, 2, and 3 were 10, 9, and 10 s, respectively. However, spoofing affected the other five channels to varying degrees, resulting in the corresponding innovation rate deviating from the normal value and false alarm. In addition, Fig. 6(b) shows a diagram of the M2 simulation results. Note that the detection times of channels 1, 2, and 3 were 9, 8, and 9 s, respectively, which were 1, 2, and 1 s shorter than that of the corresponding channels in Fig. 6(a). Moreover, the innovation rate of other channels was normal. In addition, as seen in the figure, when step spoofing with a relatively large pseudorange deviation was applied, the detection efficiency of M2 did not improve compared with that of M1. However, M2 can restrain the innovation rate by preventing it from deviating from the normal value, increasing the fault tolerance and robustness of the system.

The second set of ramp spoofing simulation results is shown in Fig. 7. Ramp spoofing with a slope of 0.3 m/s was

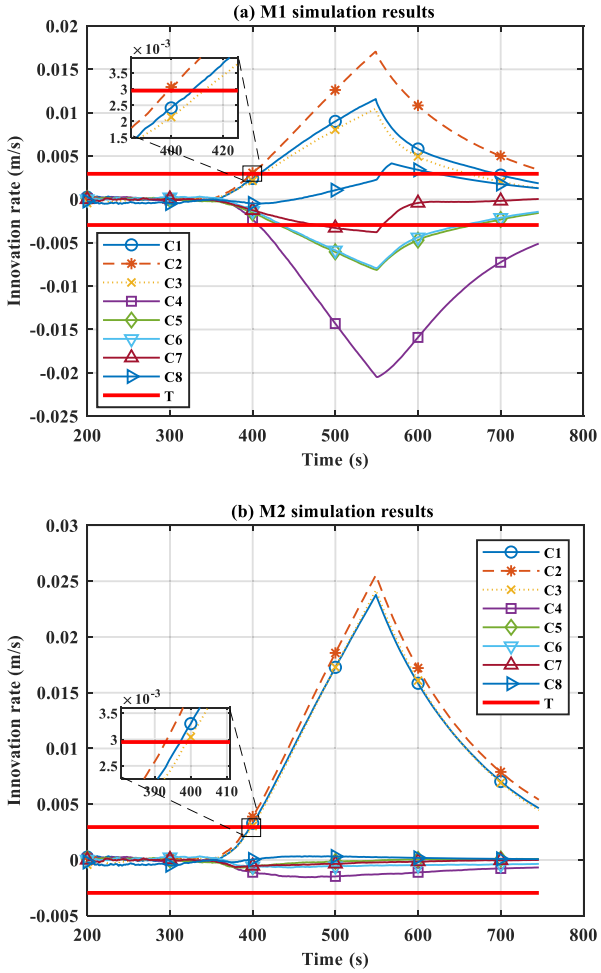

FIGURE 7. Comparison of the simulation results for ramp spoofing of M1 and M2.

TABLE 3. Scenario 1 Monte Carlo simulation results.

Method	Missing detection rate (%)			False alarm rate (%)		
	C1*	C2*	C3*	C4	C5	C6
M1	0	0	0	100	100	100
M2	0	0	0	3	1	1

applied to channels 1, 2, and 3 in 350–550 s. In particular, Fig. 7(a) shows the M1 simulation results. Note that the detection time of channels 1, 2, and 3 were 59, 50, and 64 s, respectively. Moreover, the spoofing affected the other channels to varying degrees, resulting in a false alarm. In addition, Fig. 7(b) depicts the M2 simulation results, showing that the detection times of channels 1, 2, and 3 were 47, 43, and 49 s, respectively, shortened by 12, 7, and 15 s, respectively, as compared with that of the corresponding channels in Fig. 7(a). The innovation rate of the other channels was normal.

Monte Carlo simulation was performed according to Scenario 1 for 100 cycles to illustrate the effect of the M2 robust estimation. The missed detection and false alarm rates of the two algorithms are listed in Table 3.

From the result shown in Figs. 6 and 7 and Table 3, the following conclusions can be drawn: 1) When M2 was

TABLE 4. Spoofing scenario 2.

Spoofing type	Pseudorange added value	C	Time
Step	40, 30, 20,10, and 5 m	3	350-550 s
Ramp	0.4, 0.3, 0.2, 0.1, and 0.05 m/s		

spoofed by the step, the detection time of M2 was reduced by 10%, 22.2%, and 10%, respectively, as compared with that of M1. Moreover, the average time was reduced by 35.5%. Compared with the detection time of M1, that of M2 was reduced by 20.3%, 14%, and 64.2%, respectively. The average time was shortened by 32.8%. Thus, the average detection efficiency of M2 was approximately one-third higher than that of M1. 2) For the missed detection rate, channels 1, 2, and 3 of M1 and M2 were all zero. The false alarm rate of channels 4, 5, and 6 of M1 were 100%, whereas that of channels 4, 5, and 6 of M2 is 3%, 1%, and 1%, respectively, which were reduced by 97%, 99%, and 99%, respectively. The average reduction was 98.3%. Finally, the robust estimation of M2 suppressed the innovation rate of the normal channels from the normal value and reduced the false alarm rate. The detection time was reduced, and the detection performance improved.

2) SCENARIO 2

Scenario 2 was set using the parameters in Table 4. Sun *et al.*. [31] set the scenario of channel 3 by adding different values to the pseudorange for different spoofing types and verified that M2 had limitations on small-step spoofing of 5 m or slow-growth ramp spoofing of 0.05 m/s. The detection time was extensive or even invalid.

The simulation results are shown in Fig. 8. In particular, Fig. 8(a) shows the simulation result of M2 step spoofing. Note that during the time 350–550 s, step spoofing with pseudorange deviations of 40, 30, 20, 10, and 5 m was applied to channel 3, and the detection times were 4, 6, 10, and 25 s, respectively, in which small-step spoofing detection of 5 m is invalid. In addition, Fig. 8(b) depicts the simulation result of M2 ramp spoofing. Ramp spoofing with pseudorange deviations of 0.4, 0.3, 0.2, 0.1, and 0.05 m/s was applied to channel 3; the detection times were 36, 44, 57, 92, and 157 s, respectively. Therefore, this scenario verified that as the pseudorange deviation (applied in small steps in the range 40–5 m) and slope (0.4–0.05 m/s) decreased, the detection time increased (even the detection was ineffective). In particular, the maximum detection time for slow growth ramp spoofing of 0.05 m/s was 157 s and the detection of small-step spoofing of 5 m was invalid.

3) SCENARIO 3

Based on the limitations of M2 in detecting small-step spoofing in Scenario 2, the subsequent small-step spoofing scenario, Scenario 3, was set as in Table 5. In this scenario, the detection capabilities of M2 and M3 were compared.

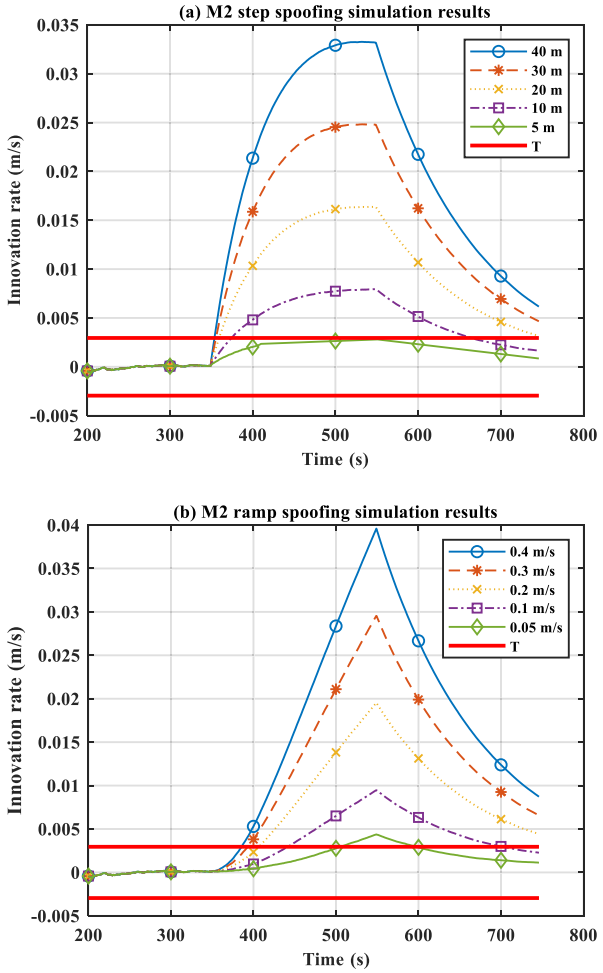

FIGURE 8. Comparison of the simulation results for different pseudorange added values of different spoofing types in M2.

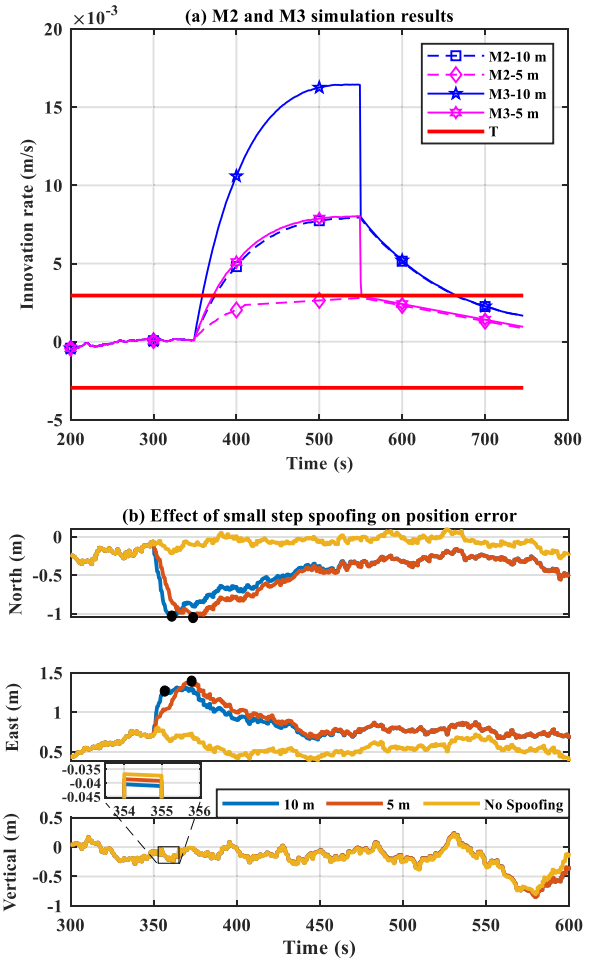

FIGURE 9. Comparison of simulation results for small-step spoofing between M2 and M3.

TABLE 5. Spoofing scenario 3.

Spoofing type	Pseudorange added value	C	Time
Small step	10 and 5 m	3	350–550 s

The simulation results are shown in Fig. 9. Step spoofing with pseudorange deviations of 10 and 5 m was applied to channel 3 for 350–550 s. In particular, Fig. 9(a) shows the simulation results for the small-step spoofing for M2 and M3. Note that, for the pseudorange deviation of 10 m, the detection times of M2 and M3 were 25 and 9 s, respectively. For the 5 m pseudorange deviation, M2 detection was ineffective and the detection time required by M3 was 22 s. Therefore, M3 was more sensitive than M2 in terms of small-step spoofing detection. In addition, Fig. 9(b) shows the effect of small-step spoofing on the position error. When 10 and 5 m spoofing were applied, the maximum errors in the northerly direction are 1.04091 and 1.04169 m, respectively, and those in the easterly direction were 1.30492 and 1.39802 m, respectively. The altitude error only changed slightly, showing that the small-step spoofing was hidden and the error accuracy requirements were satisfied. This is generally difficult to detect, even though it is paramount in high-precision positioning applications, such as missile precision guidance, intelligent driving, and unmanned aerial vehicles.

Furthermore, Monte Carlo simulations were performed for Scenario 3 for 100 cycles to show that M3 was superior to M2. The missed detection and false alarm rates of the two algorithms are listed in Table 6.

The results in Fig. 9 and Table 6 show that: 1) when channel 3 was spoofed by 10 m, the detection time of M3 was shortened by 64% as compared with that of M2. M3 detection was effective, and M2 detection was invalid when small-step spoofing of 5 m was used for interference. 2) The missed detection rate of M3 was 74% lower than that of M2. For the false alarm rate, channels 3, 4, and 5 were approximately zero for M2 and M3. Therefore, M3 was more sensitive to small-step spoofing detection and inherited the robust estimation effect of M2.

4) SCENARIO 4

Based on the limitations of M2 in Scenario 2 to slow-growing ramp spoofing detection, Scenario 4 for slow-growing ramp

TABLE 6. Scenario 3 Monte Carlo simulation results.

Method	Missing detection rate (%)	False alarm rate (%)		
	C3*	C4	C5	C6
M2	74	0	0	1
M3	0	0	0	1

TABLE 7. Spoofing scenario 4.

Spoofing type	Pseudorange added value	C	Time
slow-growing ramp	0.1 and 0.05 m/s	3	350-550 s

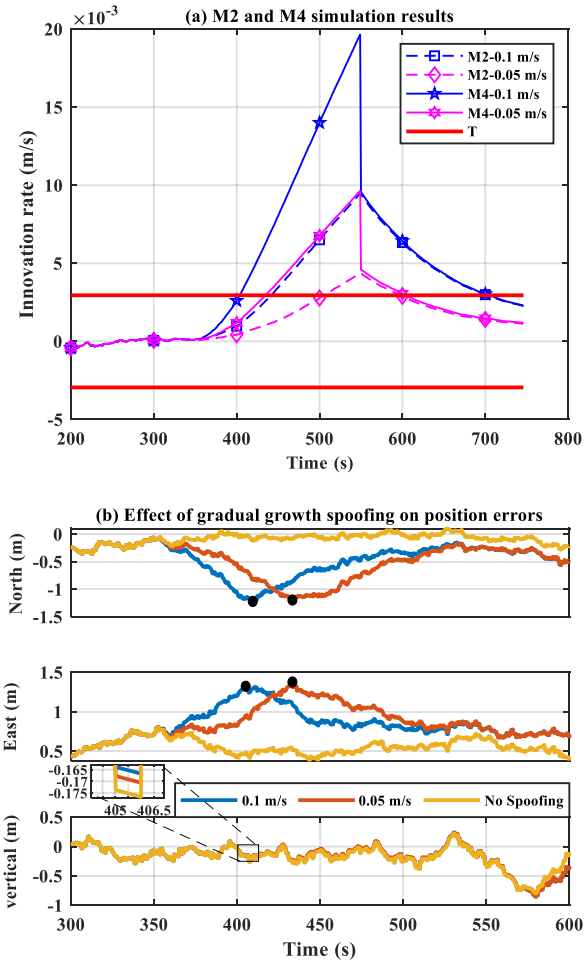

FIGURE 10. Comparison of the simulation results for slow-growth spoofing between M2 and M4.

spoofing was set as in Table 7. The detection capabilities of M2 and M4 were compared.

The simulation results are shown in Fig. 10. In this scenario, ramp spoofing with slopes of 0.1 and 0.05 m/s was applied to channel 3 for 350–550 s. In particular, Fig. 10(a) shows the simulation result of M2 and M4 for slow-growth spoofing. Note that, for the 0.1 m/s ramp, the detection times of M2 and M4 were 92 and 57 s, respectively. Moreover, for 0.05 m/s, the detection times of M2 and M3 were 147 and 86 s, respectively, showing that M3 was more efficient than M2. In addition, Fig. 10(b) shows the effect of the slow-growth spoofing on the position error. When spoofing of 0.1 and 0.05 m/s was applied, the maximum errors in the northerly direction were 1.21345 and 1.17252 m, respectively, and those in the easterly direction were 1.31591 and 1.34444 m, respectively. The height error only changed slightly, showing that the smaller the slope of slow growth, the longer the time to reach the maximum error.

TABLE 8. Scenario 4 Monte Carlo simulation results.

Method	Missing detection rate (%)	False alarm rate (%)		
	C3*	C4	C5	C6
M2	42	0	0	1
M4	0	0	0	1

Monte Carlo simulations were performed for Scenario 4 for 100 cycles to show that M4 was superior to M2. The missed detection and false alarm rates of the two algorithms are listed in Table 8.

The results in Fig. 10 and Table 8 show that: 1) when channel 3 was spoofed by slow growth of 0.1 and 0.05 m/s, the detection time of M4 was reduced by 38% and 41.5%, respectively, as compared with that of M2, with an average reduction of 39.8%. 2) The missed detection rate of M3 was 42% lower than that of M2, and for the false alarm rate, channels 3, 4, and 5 were approximately zero for M2 and M4. Therefore, M4 was more sensitive to slow-growing ramp spoofing detection.

VI. CONCLUSION

A GNSS/INS spoofing detection algorithm based on robust estimation of the innovation rate is effective for large-scale spoofing. However, this algorithm requires substantial time to detect small step and slow-growing ramp spoofing. In this study, a tightly coupled GNSS/INS integration spoofing detection algorithm based on innovation rate optimization and robust estimation was proposed. The proposed algorithm established a two-layer Kalman filter. First, the normalized innovation was improved using an innovation detection method in the main navigation Kalman filter. Subsequently, the improved normalized innovation was inputted into the innovation rate Kalman filter for measurement update, thus optimizing the innovation rate test statistics. Simultaneously, robust estimation was introduced to adaptively adjust the gain matrix, which reduced the effect of spoofing on the innovation rate and further improved the detection and processing ability of small step or slow-growth ramp spoofing. The simulation results showed that the detection time of the proposed algorithm was reduced by 64% and 39.8%, respectively, with an average reduction of 51.9% when detecting step mutation or slow-growth spoofing. Moreover, the missed detection rate decreased by 74% and 42%, respectively, with an average decrease of 58%. The false alarm rate was maintained at approximately zero. Compared with existing algorithms, the proposed algorithm exhibited fast detection and low missed

detection and false alarm rates when detecting small step and slow-growth ramp spoofing. Our algorithm is suitable for the spoofing detection of tightly coupled GNSS/INS integration user high-precision unmanned aerial vehicle applications.

To improve the applicability of the new algorithm, further work could be performed on the following aspects: 1) Investigating the integrity detection level and protection level of navigation systems by changing the false alarm rate to change the detection probability; 2) adding real data to verify the improved algorithm; 3) researching the multi-channel spoofing detection algorithm.

REFERENCES

[1] T.-S. Lou, N.-H. Chen, Z.-W. Chen, and X.-L. Wang, "Robust partially strong tracking extended consider Kalman filtering for INS/GNSS integrated navigation," *IEEE Access*, vol. 7, pp. 151230–151238, 2019, doi: 10.1109/ACCESS.2019.2948229.

[2] S. Bian, B. Ji, and Y. Hu, "Research status and prospect of GNSS anti-spoofing technology," *Scientia Sinica Informationis*, vol. 47, no. 3, pp. 275–287, Mar. 2017, doi: 10.1360/N112016-00073.

[3] R. T. Ioannides, T. Pany, and G. Gibbons, "Known vulnerabilities of global navigation satellite systems, status, and potential mitigation techniques," *Proc. IEEE*, vol. 104, no. 6, pp. 1174–1194, Jun. 2016, doi: 10.1109/JPROC.2016.2535898.

[4] T. E. Humphreys, B. M. Ledvina, M. Psiaki, B. W. O'Hanlon, and P. M. Kintner, "Assessing the spoofing threat: Development of a portable GPS civilian spoofer," in *Proc. 21st Int. Tech. Meeting Satell. Division Inst. Navigat.*, Savannah, GA, USA, 2008, pp. 2314–2325.

[5] L. Zhang, Z. Wang, X. Ding, S. Li, and Z. Wang, "Fault-tolerant control for intelligent electrified vehicles against front wheel steering angle sensor faults during trajectory tracking," *IEEE Access*, vol. 9, pp. 65174–65186, 2021, doi: 10.1109/ACCESS.2021.3075325.

[6] A. J. Kerns, 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, Jul. 2014, doi: 10.1002/rob.21513.

[7] Z. Zhang, L. Zhang, J. Deng, M. Wang, Z. Wang, and D. Cao, "An enabling trajectory planning scheme for lane change collision avoidance on highways," *IEEE Trans. Intell. Vehicles*, early access, Oct. 6, 2021, doi: 10.1109/TIV.2021.3117840.

[8] C. Zhang, Z. W. Lv, L. D. Zhang, and Y. J. Gao, "A spoofing detection algorithm for INS/GNSS integrated navigation system based on innovation rate and robust estimation," (in Chinese), *J. Chin. Inertial Technol.*, vol. 29, no. 3, pp. 328–333, Jun. 2021.

[9] T. S. Abuhashim, M. F. Abdel-Hafez, and M. A. Al-Jarrah, "Building a robust integrity monitoring algorithm for a low cost GPS-aided-INS system," *Int. J. Control, Autom. Syst.*, vol. 8, no. 5, pp. 1108–1122, Oct. 2010, doi: 10.1007/s12555-010-0520-1.

[10] M. Joerger and B. Pervan, "Kalman filter-based integrity monitoring against sensor faults," *J. Guid., Control, Dyn.*, vol. 36, no. 2, pp. 349–361, Mar. 2013, doi: 10.2514/1.59480.

[11] J. Diesel and S. Luu, "GPS/IRS AIME: Calculation of thresholds and protection radius using chi-square methods," in *Proc. 8th Int. Tech. Meeting Satell. Division Inst. Navigat.*, Palm Springs, CA, USA, 1995, pp. 1959–1964.

[12] S. Hewitson and J. Wang, "Extended receiver autonomous integrity monitoring (eRAIM) for GNSS/INS integration," *J. Surveying Eng.*, vol. 136, no. 1, pp. 13–22, 2010, doi: 10.1061/(ASCE)0733-9453(2010)136:1(13).

[13] M. Orejas, Z. Kana, J. Dunik, J. Dvorska, and N. Kundak, "Multiconstellation GNSS/INS to support LPV200 approaches and autolanding," in *Proc. 25th Int. Tech. Meeting Satell. Division Inst. Navigat.*, Nashville, TN, USA, 2012, pp. 790–803.

[14] U. I. Bhatti, W. Y. Ochieng, and S. Feng, "Performance of rate detector algorithms for an integrated GPS/INS system in the presence of slowly growing error," *GPS Solutions*, vol. 16, no. 3, pp. 293–301, 2012, doi: 10.1007/s10291-011-0231-y.

[15] Y. Liu, S. Li, Q. Fu, Z. Liu, and Q. Zhou, "Analysis of Kalman filter innovation-based GNSS spoofing detection method for INS/GNSS integrated navigation system," *IEEE Sensors J.*, vol. 19, no. 13, pp. 5167–5178, Aug. 2019, doi: 10.1109/JSEN.2019.2902178.

[16] U. I. Bhatti, W. Y. Ochieng, and S. Feng, "Integrity of an integrated GPS/INS system in the presence of slowly growing errors. Part I: A critical review," *GPS Solutions*, vol. 11, no. 3, pp. 173–181, 2007, doi: 10.1007/s10291-006-0048-2.

[17] L. Zhong, J. Liu, R. Li, and R. Wang, "Approach for detecting soft faults in GPS/INS integrated navigation based on LS-SVM and AIME," *J. Navigat.*, vol. 70, no. 3, pp. 561–579, May 2017, doi: 10.1017/S037346331600076X.

[18] S. Wang, X. Zhan, and W. Pan, "GNSS/INS tightly coupling system integrity monitoring by robust estimation," *J. Aeronaut., Astronaut. Aviation, A*, vol. 50, pp. 61–80, Mar. 2018, doi: 10.6125/JoAAA.201803_50(1).06.

[19] R. Xu, M. Y. Ding, Q. Meng, and J. Y. Liu, "Spoofing interference identification technique of MEDLL aided GNSS/INS system," (in Chinese), *J. Chin. Inertial Technol.*, vol. 26, no. 2, pp. 223–230, Apr. 2018.

[20] C. Zhang, X. Zhao, C. Pang, Y. Wang, L. Zhang, and B. Feng, "Improved fault detection method based on robust estimation and sliding window test for INS/GNSS integration," *J. Navigat.*, vol. 73, no. 4, pp. 776–796, Feb. 2020, doi: 10.1017/S0373463319000778.

[21] R. Sun, Q. Cheng, G. Wang, and W. Y. Ochieng, "A novel online data-driven algorithm for detecting UAV navigation sensor faults," *Sensors*, vol. 17, no. 10, p. 2243, Oct. 2017, doi: 10.3390/s17102243.

[22] Y. Liu, S. Li, Q. Fu, and Z. Liu, "Impact assessment of GNSS spoofing attacks on INS/GNSS integrated navigation system," *Sensors*, vol. 18, no. 5, p. 1433, May 2018, doi: 10.3390/s18051433.

[23] A. Angrisano, "GNSS/INS integration methods," Ph.D. dissertation, Università degli Studi di Napoli Parthenope, Naples, Italy, vol. 21, 2010.

[24] M. S. Grewal and A. P. Andrews, *Kalman Filtering: Theory and Practice With MATLAB*, 4th ed. Hoboken, NJ, USA: Wiley, 2014.

[25] J. Blanch, T. Walker, P. Enge, Y. Lee, B. Pervan, M. Rippl, A. Spletter, and V. Kropp, "Baseline advanced RAIM user algorithm and possible improvements," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 51, no. 1, pp. 713–732, Jan. 2015, doi: 10.1109/TAES.2014.130739.

[26] R. J. Kelly, "The linear model, RNP, and the near-optimum fault detection and exclusion algorithm," *J. Global Positioning Syst.*, vol. 5, pp. 227–259, Jan. 1998.

[27] Y. Yang, Y. Wen, J. Xiong, and J. Yang, "Robust estimation for a dynamic model of the sea surface," *Surv. Rev.*, vol. 35, no. 271, pp. 2–10, Jan. 1999, doi: 10.1179/sre.1999.35.271.2.

[28] R. Brown and P. Hwang, *Introduction to Random Signals and Applied Kalman Filtering*, vol. 512. New York, NY, USA: Wiley, 1992.

[29] P. D. Groves, "Principles of GNSS, inertial, and multisensor integrated navigation systems," *IEEE Aerosp. Electron. Syst. Mag.*, vol. 30, no. 2, pp. 26–27, Feb. 2015, doi: 10.1109/MAES.2014.14110.

[30] J. Blanch, T. Walker, P. Enge, Y. Lee, B. Pervan, M. Rippl, and A. Spletter, "Advanced RAIM user algorithm description: Integrity support message processing, fault detection, exclusion, and protection level calculation," in *Proc. 25th Int. Tech. Meeting Satell. Division Inst. Navigat.*, Nashville, TN, USA, 2012, pp. 2828–2849.

[31] R. Sun, W. Zhang, J. Zheng, and W. Y. Ochieng, "GNSS/INS integration with integrity monitoring for UAV no-fly zone management," *Remote Sens.*, vol. 12, no. 3, p. 524, Feb. 2020, doi: 10.3390/rs12030524.

YE KE received the B.S. degree in software engineering from East China Jiaotong University, Nanchang, Jiangxi, China, in 2015. He is currently pursuing the M.S. degree with PLA Information Engineering University, Zhengzhou, Henan, China.

He has published several articles on satellite navigation data processing and anti-spoofing techniques. He is currently researching on GNSS/INS integrated navigation anti-spoofing technology.

ZHIWEI LV received the Ph.D. degree in space geodetic survey and navigation from PLA Information Engineering University, Zhengzhou, Henan, China, in 2010.

He is currently a Professor with PLA Information Engineering University. He has published several articles on satellite navigation data processing and space geodetic survey. His current research focuses mainly on satellite navigation data processing, space geodetic survey, and anti-spoofing technology.

CHAO ZHANG received the M.S. degree in software engineering from PLA Information Engineering University, Zhengzhou, Henan, China, in 2021.

He has published several articles on satellite navigation data processing and satellite navigation anti-spoofing technology. His current research focuses mainly on satellite navigation anti-spoofing technology.

XU DENG received the B.S. degree in navigation engineering from PLA Information Engineering University, Zhengzhou, Henan, China, in 2019, where he is currently pursuing the M.S. degree.

His current research mainly focuses on satellite navigation spoofing countermeasures. He has published several articles on satellite navigation data processing and satellite navigation anti-spoofing technology.

WENLONG ZHOU received the B.S. degree in navigation engineering from PLA Information Engineering University, Zhengzhou, Henan, China, in 2020, where he is currently pursuing the M.S. degree.

He has published several articles on satellite navigation data processing and satellite navigation anti-spoof technology. His current research mainly focuses on satellite navigation anti-spoofing countermeasures.

DEBIAO SONG received the B.S. degree in navigation engineering from PLA Information Engineering University, Zhengzhou, Henan, China, in 2020, where he is currently pursuing the M.S. degree.

His current research mainly focuses on the tightly-coupled GNSS/INS, and he is in the stage of verifying the experimental results.