Spoofing Control Strategy for Precise Position Offset Based on INS/GNSS Tightly Coupled Navigation

SHUHAI LU, YAN GUO, HANG SHANG, KANGHUA TANG, JULIANG CAO, RUIHANG YU, AND SHAOKUN CAI
College of Intelligence Science and Technology, National University of Defence Technology, Changsha 410073, China
Corresponding authors: Yan Guo (guoyan010417@126.com) and Juliang Cao (cjvl@163.com)

This work was supported in part by the National Natural Science Foundation of China under Grant 61973312, and in part by the Junior Faculty Innovation Research Project, College of Intelligence Science and Engineering, National University of Defense Technology, under Grant ZN2019-16.

ABSTRACT To deceive Inertial Navigation System (INS)/Global Navigation Satellite System (GNSS) integrated navigation terminals, the entry point is still to inject GNSS spoofing signals to the target system. However, the spoofing control strategy in integrated navigation mode for particular tasks such as fixed-point capture or directional drive needs further research. Whether applying GNSS spoofing attacks or not, the Kalman filter correction gain matrix element in the tightly coupled navigation system always maintains its stability, which gives us valuable clues to develop an effective spoofing attack. On this basis, this article focuses on the feasibility and operability of spoofing attacks under tightly coupled navigation conditions and innovatively proposes a spoofing control strategy that can achieve accurate position offsets: Specific spoofing signals are implanted to the target tightly coupled navigation terminal at the beginning of the spoofing attack. The amounts of pseudo-range spoofing signals corresponding to different satellites are respectively the projections of the position increments to be deceived on the sight vector of the integrated navigation terminal to each satellite. Simulation experiments and tightly coupled navigation terminal experiments verify the correctness and effectiveness of the spoofing control strategy.

INDEX TERMS INS/GNSS tightly coupled navigation, spoofing control strategy, steady state gain matrix, GNSS spoofing signal, precise position offset.

I. INTRODUCTION
With the progress of science and technology and the rapid development of the economy, GNSS has been widely used in many fields of society [1], [2]. On the military field, with the advantage of durability, maneuverability, and economy, the Unmanned Aerial Vehicle (UAV) systems centered on the INS/GNSS integrated navigation system become an essential part of weapons and equipment in various countries [3]. However, due to the weak power of satellite signals, satellite navigation terminals are incredibly susceptible to interference, which seriously affects the effectiveness of UAV system operations [4]. Many countries treat satellite deceptive interference as an offensive strategy to reduce the effectiveness of the enemy’s modern weapons, including UAV. Using the electronic warfare methods of satellite deceptive interference, the Iranian military capture the top-secret “RQ-170 Sentinel” UAV, “ScanEagle” UAV, and “MQ-9 Reaper” UAV from the Central Intelligence Agency by the year of 2011, 2012 and 2018 [5]–[7].

The Volpe report submitted by the US Department of Transportation in 2001 focused on the analysis of civil satellite deceptive interference, which is worse than other types of intentional communication interference [8], [9]. Regarding the civilian GNSS signals as the breakthrough point, many scholars at home and abroad have carried out related research on GNSS spoofing technology. According to the type of spoofing attack target, the satellite spoofing attacks can be divided into spoofing attacks against pure satellite navigation mode, and spoofing attacks under the combined...
navigation mode with the GNSS navigation system as the auxiliary system terminals (including standard INS/GNSS loosely coupled integration and INS/GNSS tightly coupled integration). In 2003, Professor Warner of the University of California took the lead in completing a deceptive attack experiment against the pure satellite navigation terminal [10]. Professor Warner, using a simple satellite signal jammer (including satellite signal simulator, power amplifier, and signal transmitter) equipped on the truck to disrupt the satellite signal receiver on another target truck, changed the position output of the receiver. In 2011, researchers at Turin Polytechnic University built a simple spoofing test platform called Limpet Spoofer [11]. They confirmed that the use of the satellite spoofing attacks, causing an anomaly of the receiver carrier ring and code loop in the total spoofing process, could pull the target receiver from the tracked real satellite signal to the false satellite signal. Based on this, the Daedeo 305-700 satellite navigation research team further analyzed the effect of anomalous effects caused by false satellite signals [12]. The team found that, when spoofing signals were implanted, not only DLL and PLL tracking loops generate errors, but also pseudo moments could occur linear changes, which in turn led to the wrong navigation results and time offsets. Seong-Hun Seo et al., of Konkuk University in 2015, set up their software-based GNSS signal generator and conducted satellite navigation deceptive attack experiments against UAV [13]. The experimental results showed that despite the specific spoofing protection capabilities of the UAV, the deceptive attack method could accurately cheat the UAV to the target point when the attackers get the grasp of the movement state of the UAV.

In 2008, Professor Todd Humpherys of Texas State University in the United States designed a rough and straightforward civil GPS deception scheme for the INS/GNSS loosely integrated navigation terminal and published several reports to evaluate the threat of GPS deceptive attack [14]. In June 2012, Todd Humpherys successfully changed the flight path of a small UAV based on INS/GPS loosely coupled navigation in a college playground by using GPS civil signal deception equipment which costs less than $1000 [15]. Packing the error information into a seemingly reliable GNSS signal and sending the signal to the target receiver, this experiment made the INS/GPS loosely coupled navigation on the UAV outputs false geographic information and misguides the UAV.

In 2014, researchers at Illinois Institute of Technology in Chicago proposed a UAV deceptive attack method against the INS/GPS loosely coupled navigation UAV [16]. Simulation results showed that if the attacker has an absolute understanding of the UAV track, the process would not be detected by the monitor while generating a significant position error. In 2018, Eric Horton and Prakash Ranganathan of the University of North Dakota (UND) developed a GPS spoofing device and introduced in detail the use of this device to attack Android phones and DJI Matrice 100 quadrotor UAV [17]. This experiment also simply analyzed the offset effect of navigation positioning of Android phones and quadrotor UAV under deceptive interference. In 2019, Yan Guo at the National University of Defense Technology proposed an algorithm of UAV covert deception based on GPS/INS loosely coupled navigation [18]. However, GPS deceivers need to constantly adjust the generated fake GPS signal according to the deviation between the actual state of UAV and the original reference target state.

According to the recent development of the satellite deceptive interference technology, current researches are mainly aimed at the pure satellite navigation terminal. Fewer considerations are given to the integrated navigation mode (such as INS/GNSS, DVL/GNSS, etc.) in which the satellite navigation system is used as an auxiliary system [19]. Furthermore, even though tightly integrated navigation terminals are more widely used in the military and have more complicated structures, we clearly find that the current spoofing control strategies for tightly integrated navigation terminals, have not been studied in depth. Aiming at the task of accurately achieve the position offset of tightly integrated UAV systems in military operations, the third section of this paper combines the simulation experiments to verify the stability of the Kalman filter steady-state gain matrix elements in the tightly integrated navigation system, which lays the theoretical basis for implementing pseudo-range spoofing and achieving accurate position offset in this paper. According to this characteristic of the steady-state gain matrix, the fourth section of this paper focuses on the feasibility and operability of spoofing attacks against tightly coupled navigation and innovatively proposes a spoofing control strategy for a precise position offset against tightly integrated unmanned systems: specific spoofing signals are implanted to the target tightly coupled navigation terminal at the beginning of the spoofing attack. The amount of Pseudo-range spoofing signal corresponding to different satellites are respectively the projections of the position increments to be deceived on the sight vector of the integrated navigation terminal to each satellite. Sections 5 and 6 of this paper verify the correctness and effectiveness of this spoofing control strategy through simulation experiments and tightly integrated navigation terminal experiments. Section 7 gives conclusions.

II. INS/GNSS TIGHTLY COUPLED NAVIGATION ARCHITECTURE

The advantages of INS are good autonomy, high dynamics, and comprehensive output of navigation information, but its errors accumulate over time which causes long-term accuracy decreases. GNSS has the advantages of high precision and no increase in error with time, but the signal is easy to interfere with. Utilizing filtering, the combination of INS/GNSS, recognized as the best-integrated navigation scheme, can improve the overall accuracy and reliability of the system, and have strong complementarity. The first and most successful filter used in the field of integrated navigation is the classical Kalman filter. In this paper, to achieve the task of precise position offset or disperse of the UAV system, we consider the specific analysis of standard
tightly coupled systems that are widely used in the military background.

A. INS/GNSS TIGHTLY COUPLED NAVIGATION STATE MODEL

The definition of the state vector $X$ of the system is combined by the error state vector $X_I$ of INS and the error state vector $X_G$ of GNSS.

The linear Kalman filter takes the navigation parameter error as the state of the filter and uses the estimated error to correct the output of INS. The error state vector of INS is defined as:

$$X_I = [\delta L, \delta \lambda, \delta h, \delta v_N, \delta v_E, \delta v_D, \delta \varphi, \delta \theta, \delta \phi]^T$$  \hspace{1cm} (1)

where $\delta L$, $\delta \lambda$, and $\delta h$ represent the latitude, longitude and height error information of the system; $\delta v_N$, $\delta v_E$, and $\delta v_D$ represent the velocity error information of the system; $\delta \varphi$, $\delta \theta$ and $\delta \phi$ are the roll angle, pitch angle and heading angle error of the system. Note that the subscripts $N$, $E$, $D$ represent the north, east and down components in the navigation frame, respectively.

The expression of INS error state matrix equation is:

$$\dot{X}_I = F_I X_I + G_I W_I$$  \hspace{1cm} (2)

In the formula, $F_I$ is the INS system state matrix, and its parameters can refer to \cite{20}; $G_I$ is the INS system input matrix, whose parameters can refer to \cite{20};

INS system noise is:

$$W_I = \begin{bmatrix} w_{gx} & w_{gy} & w_{gz} & w_{ax} & w_{ay} & w_{az} \end{bmatrix}^T$$  \hspace{1cm} (3)

where $w_{gx}$, $w_{gy}$ and $w_{gz}$ are the noises of the three-axis gyro of the INS, and $w_{ax}$, $w_{ay}$ and $w_{az}$ are the noises of the accelerometers in the front, right and bottom directions respectively.

Compared with the loosely coupled system, the tightly coupled system has not only the error state equation of INS but also the error state equation of GNSS. In error state equation of GNSS, pseudo-range and pseudo-range rate are used as observation information. Generally, two time related errors are selected: clock error $\delta t_u$ and clock frequency error $\delta f_u$, then the error state equation of GNSS can be expressed as:

$$\begin{align*}
    c \delta t_u &= \delta t_{ru} + w_{tu} \\
    c \delta f_u &= \delta f_{ru} + w_{fru}
\end{align*}$$  \hspace{1cm} (4)

where $c$ is the speed of light, $w_{tu}$ and $w_{fru}$ are equivalent GNSS receiver clock error and equivalent GNSS receiver clock drift error. The matrix representation of equation (4) can be defined as:

$$\dot{X}_G = F_G X_G + G_G W_G$$  \hspace{1cm} (5)

where Error state vector of GNSS $X_G = [c \delta t_u, c \delta f_u]^T$, GNSS system state matrix $F_G = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, GNSS system input matrix $G_G = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, GNSS system noise $W_G = \begin{bmatrix} w_{tu} & w_{fru} \end{bmatrix}^T$.

Combining the INS error state equation (2) with GNSS error state equation (5), the state equation of the tightly integrated navigation system can be obtained:

$$\dot{X} = \begin{bmatrix} \dot{X}_I \\ \dot{X}_G \end{bmatrix} = \begin{bmatrix} F_I & 0 \\ 0 & F_G \end{bmatrix} \begin{bmatrix} X_I \\ X_G \end{bmatrix} + \begin{bmatrix} G_I & 0 \\ 0 & G_G \end{bmatrix} \begin{bmatrix} W_I \\ W_G \end{bmatrix}$$  \hspace{1cm} (6)

B. INS/GNSS TIGHTLY COUPLED NAVIGATION MEASUREMENT MODEL

The pseudo-range of the $i$th satellite calculated directly from the inertial navigation is:

$$\rho_{1}^{(i)} = \sqrt{(x_1 - x_i^{(i)})^2 + (y_1 - y_i^{(i)})^2 + (z_1 - z_i^{(i)})^2}$$  \hspace{1cm} (7)

where $(x_i^{(i)}, y_i^{(i)}, z_i^{(i)})$ represents the position of the $i$th satellite in the ECEF coordinate system, and $(x_1, y_1, z_1)$ represents the position of the inertial navigation in the ECEF coordinate system.

The pseudo-range rate of the $i$th satellite calculated directly from the inertial navigation is:

$$\dot{\rho}_i^{(i)} = e_i = \frac{v_e - v_{sat}}{\lambda L_1}$$  \hspace{1cm} (8)

where $\lambda_{L1}$ is the wavelength of L1 carrier, $v_e$ is the velocity vector of the inertial navigation system under the ECEF system, $v_{sat}$ is the velocity vector of the $i$th satellite under the ECEF system, and $e_i$ is the line of sight vector from the inertial navigation system to the $i$th satellite:

$$e_i = \left( e_x^{(i)} e_y^{(i)} e_z^{(i)} \right) = \left( \frac{x - x_i^{(i)}}{r^{(i)}} \frac{y - y_i^{(i)}}{r^{(i)}} \frac{z - z_i^{(i)}}{r^{(i)}} \right)$$  \hspace{1cm} (9)

$r^{(i)}$ is the real distance between the $i$th satellite and the receiver, and $(x, y, z)$ is the real position of the receiver in the ECEF coordinate system.

Pseudo-range observation equation of INS/GNSS tight combination Kalman filter $Z_p$ can be designed as \cite{21}:

$$Z_p = \begin{bmatrix} \rho_{1}^{(1)} - \rho_{G1}^{(1)} \\ \rho_{1}^{(2)} - \rho_{G2}^{(2)} \\ \vdots \\ \rho_{1}^{(r)} - \rho_{Gr}^{(r)} \end{bmatrix} + \begin{bmatrix} e_x^{(1)} e_y^{(1)} e_z^{(1)} \\ e_x^{(2)} e_y^{(2)} e_z^{(2)} \\ \vdots \\ e_x^{(r)} e_y^{(r)} e_z^{(r)} \end{bmatrix} \begin{bmatrix} C_e e_L \\ \delta \lambda \\ \delta h \end{bmatrix}$$  \hspace{1cm} (10)

where

$$H_p = \begin{bmatrix} e_x^{(1)} & e_y^{(1)} & e_z^{(1)} \\ e_x^{(2)} & e_y^{(2)} & e_z^{(2)} \\ \vdots & \vdots & \vdots \\ e_x^{(r)} & e_y^{(r)} & e_z^{(r)} \end{bmatrix}_{r \times 3} C_e.$$
$V_\rho = \begin{bmatrix}
V_\rho^{(1)}_r \\
V_\rho^{(2)}_r \\
\vdots \\
V_\rho^{(r)}_r
\end{bmatrix}_{r \times 1}$
is the pseudo-range error noise of the corresponding satellite.

Pseudo-range rate observation equation of INS/GNSS tight combination Kalman filter $Z_\rho$ can be designed as [21]:

$$Z_\rho = \begin{bmatrix}
\dot{\rho}_G^{(1)} - \dot{\rho}_G^{(2)} \\
\dot{\rho}_G^{(2)} - \dot{\rho}_G^{(3)} \\
\vdots \\
\dot{\rho}_G^{(r)} - \dot{\rho}_G^{(r-1)}
\end{bmatrix} + \begin{bmatrix}
\delta \rho_v^{(1)} \\
\delta \rho_v^{(2)} \\
\vdots \\
\delta \rho_v^{(r)}
\end{bmatrix}_{r \times 3} = C_{eg}^e \begin{bmatrix}
\delta \rho_v \\
\delta \rho_e \\
\delta \rho_D
\end{bmatrix}$$

where

$$H_\dot{\rho} = \begin{bmatrix}
\begin{bmatrix}
\delta \rho_v^{(1)} \\
\delta \rho_v^{(2)} \\
\vdots \\
\delta \rho_v^{(r)}
\end{bmatrix}_{r \times 3} \\
\begin{bmatrix}
\delta \rho_e^{(1)} \\
\delta \rho_e^{(2)} \\
\vdots \\
\delta \rho_e^{(r)}
\end{bmatrix}_{r \times 3} \\
\begin{bmatrix}
\delta \rho_D^{(1)} \\
\delta \rho_D^{(2)} \\
\vdots \\
\delta \rho_D^{(r)}
\end{bmatrix}_{r \times 3}
\end{bmatrix}$$

$C_{eg}^e$ are the transformation matrix from the ECEF coordinate system to the geographical system, and

$$V_\dot{\rho} = \begin{bmatrix}
V_\dot{\rho}^{(1)}_r \\
V_\dot{\rho}^{(2)}_r \\
\vdots \\
V_\dot{\rho}^{(r)}_r
\end{bmatrix}_{r \times 1}$$

are the pseudo-range rate error noise of the corresponding satellite.

The observation equation of INS/GNSS tight combination Kalman filter:

$$Z = \begin{bmatrix}
Z_v \\
Z_\rho
\end{bmatrix} = \begin{bmatrix}
\begin{bmatrix}
\delta \bar{V}_v^{(1)} \\
\delta \bar{V}_v^{(2)} \\
\vdots \\
\delta \bar{V}_v^{(r)}
\end{bmatrix}_{r \times 3} \\
\begin{bmatrix}
\delta \bar{V}_\rho^{(1)} \\
\delta \bar{V}_\rho^{(2)} \\
\vdots \\
\delta \bar{V}_\rho^{(r)}
\end{bmatrix}_{r \times 3}
\end{bmatrix} = \begin{bmatrix}
\bar{V}_v^{(1)} - \bar{V}_v^{(2)} \\
\bar{V}_v^{(2)} - \bar{V}_v^{(3)} \\
\vdots \\
\bar{V}_v^{(r)} - \bar{V}_v^{(r-1)}
\end{bmatrix} + \begin{bmatrix}
\begin{bmatrix}
\delta \rho_v^{(1)} \\
\delta \rho_v^{(2)} \\
\vdots \\
\delta \rho_v^{(r)}
\end{bmatrix}_{r \times 3} \\
\begin{bmatrix}
\delta \rho_e^{(1)} \\
\delta \rho_e^{(2)} \\
\vdots \\
\delta \rho_e^{(r)}
\end{bmatrix}_{r \times 3} \\
\begin{bmatrix}
\delta \rho_D^{(1)} \\
\delta \rho_D^{(2)} \\
\vdots \\
\delta \rho_D^{(r)}
\end{bmatrix}_{r \times 3}
\end{bmatrix}$$

where $\bar{V}_v^{(i)}$ and $\bar{V}_v^{(i)} (i = 1, 2, \ldots, r)$ are the pseudo-range rate and pseudo-range rate obtained from GNSS receiver corresponding to the $i$th satellite.

By substituting pseudo-range observation equation (10) and pseudo-range rate observation equation (11) into equation (12), we can get:

$$Z = \begin{bmatrix}
H_\rho & 0_{r \times 3} & 0_{r \times 1} & 1_{r \times 1} \\
0_{r \times 3} & H_\rho & 0_{r \times 1} & 1_{r \times 1}
\end{bmatrix} X + \begin{bmatrix}
V_\rho \\
V_\dot{\rho}
\end{bmatrix}$$

(13)

III. STEADY-STATE GAIN MATRIX OF COMPACT INTEGRATED NAVIGATION FILTER

From equations (6) and (13), the state-space model of INS/GNSS integrated navigation system can be obtained as follows:

$$\begin{bmatrix}
\dot{X} \\
\dot{V}
\end{bmatrix} = F X + G W_k + V_k$$

$$Z = HX + V_k$$

(14)

Recurrent iteration is the most significant advantage of the discrete Kalman filter. The algorithm does not need to store a large number of measurement data. Therefore, in the actual environment, the separate Kalman filter is used to combine INS and GNSS data.

The integrated navigation model described in equation (14) is discretized to obtain:

$$\begin{bmatrix}
X_k \\
V_k
\end{bmatrix} = \Phi_{k, k-1} X_{k-1} + \Gamma_{k, k-1} W_{k-1}$$

$$Z_k = HX_k + V_k$$

(15)

Among them, $\Phi_{k, k-1}$ is the discrete system state matrix, $\Gamma_{k, k-1}$ is the discrete system input matrix, system noise $V_k$ and observation noise $V_k$ are white noise and uncorrelated, system noise variance is $E [WW^T] = Q$, and observation noise variance is $E [VV^T] = R$.

If the observation value of time $k$ is $Z_k$, the estimation $\hat{X}_k$ of $X_k$ can be solved according to the flow of Figure 1.

![FIGURE 1. Working flow chart of standard Kalman filter(The content of the blue rectangle on the left indicates the state filter loop; The content of the grey rectangle on the right indicates the gain calculation loop).](image-url)
stable state $K_\infty$, and the 200 filtering periods can basically converge stably. Therefore, By adding spoofing signals to $Z_k$, we can directly inject GNSS spoofing attacks into the state filtering loop.

**A. THE SOLUTION OF STEADY-STATE GAIN MATRIX AND THE MEANING OF EACH ELEMENT**

The steady-state gain matrix $K_\infty$ is determined by the system noise variance $Q$ and the observed noise variance $R$, and is calculated and solved according to the steady-state value $P_\infty$ of the state estimation variance matrix. The INS/GNSS tightly integrated navigation uses the discrete Kalman filter. We can explain the steady-state value $P_\infty$ of the variance matrix of the state estimation through the discrete algebraic Riccati equation. Using $P_\infty$ to solve the steady-state gain matrix $K_\infty$, the specific formula can be designed as follows:

$$K_\infty = P_\infty H^T \left( H P_\infty H^T + R \right)^{-1}$$ (16)

According to the proposed deception link $\hat{X}_k = \hat{X}_{k-1} + K_k \left( Z_k - H \hat{X}_{k-1} \right)$ in Figure 1, the spatial correspondence between the state vector $X$ and the observation vector $Z$ can be obtained.

The ground (sky) channel of the inertial navigation system is divergent when there is no external reference information (such as altimeter information) or damping. Due to accuracy limitations, the altitude information and ground speed are not used in the experiment and are not listed in Figure 2 below. To make the expression concise, we choose 4 satellites as an example to illustrate, the spatial correspondence between the state vector $X$ and the observation vector $Z$.

![The spatial correspondence between the state vector X and the observation vector Z.](image)

The pseudo-range and the pseudo-range observations of vector $Z$ could change the element value of state vector $X$ through steady-state gain matrix $K_\infty$.

According to the number of rows and columns of each element in steady-state gain matrix $K_\infty$, we define the meaning of the main elements as follows: $k_{1,i}(i = 1, 2, \ldots, 4)$ is the gain of the estimated latitude error using the pseudo-range observations of $i$th satellites; $k_{2,i}(i = 1, 2, \ldots, 4)$ is the gain of the longitude error estimation value using the pseudo-range observations of $i$th satellites.

**B. SIMULATION EXPERIMENT OF STEADY-STATE GAIN ELEMENTS AFFECTING THE POSITION OUTPUT ESTIMATION OF TIGHTLY INTEGRATED NAVIGATION FILTER**

To explore and verify the law of steady-state gain elements that affect the position output estimation under the condition of whether or not pseudo-range deception is applied, we use the simulation environment to calculate the steady-state gain matrix elements related to the position error estimation respectively for the navigation level tightly coupled navigation system.

Since the order subject to deceptive jamming is the steady-state tightly integrated navigation filter. We conduct two simulation experiments:

1) Experiment 1 obtains the changing trend of the steady-state gain without applying pseudo-range spoofing;
2) Experiment 2 obtains the changing trend of the steady-state gain, which is obtained after the pseudo-range spoofing is imposed on the tightly integrated filter after 300 seconds.

The parameters of INS and GNSS used in the simulation are shown in the table 1.

| TABLE 1. Relevant parameters of IMU and GNSS in the first experiment. |
|-----------------|-----------------|
| **parameter**   | **Value**       |
| Gyro bias       | 0.02° / h       |
| Gyro random walk| 0.001° / √Hz    |
| Accelerometer bias | 5 × 10⁻⁵ g    |
| Accelerometer random walk | 5 × 10⁻⁶ g / √Hz |
| Pseudo-range error | 2.5m        |
| Pseudo-range rate error | 0.1m / s    |
| GNSS receiver clock error | 1m          |
| GNSS receiver clock drift error | 0.1m / s     |

The trend of state gain elements $k_{1,i}(i = 1, 2, \ldots, 4)$ that can cause latitude offset are shown in Figure 3.

The trend of state gain elements $k_{2,i}(i = 1, 2, \ldots, 4)$ that can cause longitude offset are shown in Figure 4.

From Figure 3 and Figure 4, we can find the following three characteristics of steady-state gain elements:

1. All the elements affecting latitude are of the same order of magnitude, and there are no significant elements affecting latitude output;
2. All the elements that also affect longitude are of the same order of magnitude, and there are no major elements that affect longitude output;
3. After receiving pseudo-range deception, all the elements, which affect the latitude or longitude, keep the original steady-state value unchanged after experiencing slight fluctuation.

In Section 3.1 and 3.2, not only are all pseudo-ranges independent of each other verified by theoretical analysis.
and simulation experiments but also it is proved that every element of the steady-state gain matrix keeps its stability no matter whether pseudo-range deception is applied or not. The above conclusions are the theoretical basis for understanding the behavior of the system under spoofing attacks.
for the realization of the spoofing control strategy in the next section.

IV. FEASIBILITY ANALYSIS OF DECEPTIVE JAMMING IN TIGHTLY COUPLED NAVIGATION MODE

To achieve the goal of precise position offset of tightly integrated UAV systems in military operations, this paper needs to ensure the stability and operability of deceptive jamming. The stability of deceptive interference means that the position increment caused by adding the same pseudo-range deception amount at different times remains the same. The operability of deceptive interference implies that the position offset the effect of integrated navigation can be operated by adjusting the amount of pseudo-range deception. Combined with the experimental conclusions of the previous section, this section will verify the operability and stability of deceptive interference to the tightly coupled navigation output at sections 4.1 and 4.2 respectively, so as to verify the feasibility of deceptive interference in the tightly coupled navigation mode and propose the control strategy in section 4.3.

A. OPERATIONAL ANALYSIS OF INFLUENCE DEGREE OF DECEPTIVE INTERFERENCE ON TIGHTLY COUPLED NAVIGATION POSITION OUTPUT

Based on the conclusions drawn in Section 3.2, the following will analyze the maneuverability of the effect of deceptive interference on the estimated output position of the INS/GNSS tightly integrated navigation filter. When accessing the spoofing signal, the pseudo-range and pseudo-range rate output by the GNSS receiver is:

\[
\begin{align*}
\hat{\rho}_G^{(1)} &= \hat{\rho}_G^{(1)} + \delta \rho^{(1)} \\
\hat{\rho}_G^{(2)} &= \hat{\rho}_G^{(2)} + \delta \rho^{(2)} \\
\hat{\rho}_G^{(3)} &= \hat{\rho}_G^{(3)} + \delta \rho^{(3)} \\
\hat{\rho}_G^{(4)} &= \hat{\rho}_G^{(4)} + \delta \rho^{(4)} \\
\hat{\rho}_G^{(1)} &= \hat{\rho}_G^{(1)} + \delta \rho^{(1)} \\
\hat{\rho}_G^{(2)} &= \hat{\rho}_G^{(2)} + \delta \rho^{(2)} \\
\hat{\rho}_G^{(3)} &= \hat{\rho}_G^{(3)} + \delta \rho^{(3)} \\
\hat{\rho}_G^{(4)} &= \hat{\rho}_G^{(4)} + \delta \rho^{(4)}
\end{align*}
\]  

(17)

where \( \hat{\rho}_G^{(i)} \) and \( \hat{\rho}_G^{(i)} \) are the pseudo-range and pseudo-range rate directly obtained by GNSS receiver under deceive interference; \( \hat{\rho}_G^{(i)} \) and \( \hat{\rho}_G^{(i)} \) are the pseudo-range and pseudo-range rate obtained by GNSS receiver under normal conditions, \( \delta \rho^{(i)} \) and \( \delta \rho^{(i)} \) are the imposed pseudo-range and pseudo-range rate offset.

Selecting the navigation parameter error as the state of the filter, we usually use feedback correction to correct the inertial navigation system and then clear the estimated value of the navigation parameter error. Therefore, at time \( k \), the estimated latitude error \( \delta \hat{L}_k \) of the integrated navigation output under deceptive interference is:

\[
\begin{bmatrix}
\hat{\rho}_k^{(1)} - \hat{\rho}_{G_k}^{(1)} \\
\hat{\rho}_k^{(2)} - \hat{\rho}_{G_k}^{(2)} \\
\hat{\rho}_k^{(3)} - \hat{\rho}_{G_k}^{(3)} \\
\hat{\rho}_k^{(4)} - \hat{\rho}_{G_k}^{(4)} \\
\end{bmatrix}
\]

(18)

Among them, \( \hat{\rho}_k^{(i)} \) and \( \hat{\rho}_k^{(i)} \) are the pseudo-range and pseudo-range rate information calculated by the inertial navigation system, respectively. The subscript \( k \) indicates the \( k \)th time.

Substituting equation (17) into equation (18), the estimated latitude error \( \delta \hat{L}_k \) of the tightly integrated navigation output under deceptive interference at time \( k \) can be obtained (19), as shown at the bottom of this page.

\[
\delta \hat{L}_k = \begin{bmatrix} k_{(1,1)} & k_{(1,2)} & \cdots & k_{(1,8)} \end{bmatrix}_{1 \times 8}
\]

(19)
Similarly, the longitude error estimate $\hat{\lambda}_k$ of the tightly combined navigation output under deceptive interference can be obtained:

$$\hat{\lambda}_k = \lambda_k - \Delta \lambda_k$$  \hspace{1cm} (21)

Among them, $\lambda_k$ is the estimated longitude error value of tight combination without deceptive interference, and $\Delta \lambda_k$ is the longitude deviation caused by deceptive interference, and:

$$\Delta \lambda_k = k \delta \rho^1 + k \delta \rho^2 + k \delta \rho^3 + k \delta \rho^4 + \ldots + k \delta \rho^1 + k \delta \rho^2 + k \delta \rho^3 + k \delta \rho^4$$  \hspace{1cm} (22)

Since the inertial navigation system will not be disturbed by satellite spoofing signals, the position offset caused by the deceptive interference, as same as the constant drift of the inertial device, will be accumulated directly to the next moment.

When the latitude error and longitude error estimated by the integrated navigation filter are fed back to the calculation moment, the deceptive interference, as same as the constant drift of the inertial device, will be accumulated directly to the next moment.

The amount of pseudo-range deception for the $i$th satellite in the GNSS receiver at time $k$ is $\delta \rho_k(t)$. At time $k$, the GNSS pseudo-range of the satellite receiver to input the Kalman filter is $\rho^i_G$ and $\delta \rho_k(t)$.

Since INS will not be disturbed by satellite spoofing signals, the position offset caused by the deceptive interference will be accumulated directly to the next moment.

The corrected position result formula (23) (24) at time $k$ can be derived:

$$L_k + \Delta L_k \rightarrow L_{k+1} + \Delta L_k$$  \hspace{1cm} (25)

$$\lambda_k + \Delta \lambda_k \rightarrow \lambda_{k+1} + \Delta \lambda_k$$  \hspace{1cm} (26)

where $L_k$ and $\lambda_k$ enter filter calculation at the next time $k + 1$ as equivalent to the calculation of the correct latitude $L_{k+1}$ and longitude $\lambda_{k+1}$ information of INS; $\Delta L_k$ and $\Delta \lambda_k$ enter the filter calculation at the next time $k + 1$ as a constant deviation.

Taking the $i$th satellite as an example to illustrate the effect of spoofing pseudo-range signals on position offset, equation (20) and equation (22) are simplified as follows:

$$\Delta L_k = k(1, i) \delta \rho_k(t)$$

$$\Delta \lambda_k = k(2, i) \delta \rho_k(t)$$  \hspace{1cm} (27)

The latitude and longitude offset $\Delta L_k$ and $\Delta \lambda_k$ at time $k$ will cause a quantitative deviation to the pseudo-range positioning estimated by the INS at time $k + 1$. The specific definitions are as follows:

$$\rho^i_{k+1}(t) = \rho^i_{k+1}(t) + \Delta \rho^i_k$$  \hspace{1cm} (28)

where $\rho^i_{k+1}(t)$ is the pseudo-range calculated by the INS at the time of $k + 1$ when the signal of the deceptive range is accessed at the last moment; $\rho^i_{k+1}(t)$ is the pseudo-range calculated by the INS at the time of $k + 1$ when there is no spoofing at the last moment, and $\Delta \rho^i_k$ is the pseudo-range deviation calculated by the INS at time $k + 1$ caused by the INS latitude and longitude offset $\Delta L_k$ and $\Delta \lambda_k$; here we will take the proportional relationship between $\Delta \rho^i_k$ and $\delta \rho^i_k$ as

$$\Delta \rho^i_k = \alpha \cdot \delta \rho^i_k$$  \hspace{1cm} (29)

When the spoofing signal is connected, the filter does not output offset information stably in a cycle at a time. From this we can boldly derive the following formula $0 < \Delta \rho^i_k < \delta \rho^i_k, 0 < a < 1$.

Assuming that the tightly coupled navigation is also subject to deceptive interference at time $k + 1$, the pseudo-range deception quantity of the $i$th satellite added into the GNSS receiver is recorded as $\delta \rho^i_{k+1}(t)$. At this time, the GNSS observation is:

$$\tilde{\rho}^i_{Gk+1} = \rho^i_{Gk+1} + \delta \rho^i_{k+1}$$  \hspace{1cm} (30)

For the convenience of the next simplification, we take the ratio of $\delta \rho^i_{k+1}$ to $\delta \rho^i_k$ as $\delta \rho^i_k = n_2 \cdot \delta \rho^i_k$. 

B. STABILITY ANALYSIS AT POSITION OUTPUT OF THE TIGHTLY COUPLED MODE UNDER DECEPTIVE INTERFERENCE

To analyze the stability of the position output of coupled integrated navigation caused by deceptive jamming is to verify that the position output offset of integrated navigation is stable under deceptive jamming. Since each pseudo-range is independent of each other which is proved in section 3 and we do not know the star selection method of the target UAV, it is proper to deceive all the acceptable satellite signals in the same form. For space limitation, we take the $i$th satellite as an example to illustrate the effect of pseudo-range spoofing signals on position offset.
Using feedback correction, the latitude and longitude errors estimated by the filter are:

\[
\delta \hat{L}_{k+1} = k_{i(1)} \left( \left( \rho^{(i)}_{h_{k+1}} \right)^* - \tilde{\rho}^{(i)}_{k_{i(1)}{+1}} \right) \\
= k_{i(1)} \left( \left( \rho^{(i)}_{h_{k+1}} + \Delta \rho^{(i)}_{k} \right) - \left( \rho^{(i)}_{h_{k+1} + \delta \rho^{(i)}_{k_{i(1)}{+1}}} \right) \right) \\
= \delta \hat{L}_{k+1} + k_{i(1)} \Delta \rho^{(i)}_{k} - k_{i(1)} \delta \rho^{(i)}_{k_{i(1)}{+1}} \\
(31)
\]

\[
\delta \hat{\lambda}_{k+1} = k_{i(2)} \left( \left( \rho^{(i)}_{h_{k+1}} \right)^* - \tilde{\rho}^{(i)}_{k_{i(2)}{+1}} \right) \\
= k_{i(2)} \left( \left( \rho^{(i)}_{h_{k+1}} + \Delta \rho^{(i)}_{k} \right) - \left( \rho^{(i)}_{h_{k+1} + \delta \rho^{(i)}_{k_{i(2)}{+1}}} \right) \right) \\
= \delta \hat{\lambda}_{k+1} + k_{i(2)} \Delta \rho^{(i)}_{k} - k_{i(2)} \delta \rho^{(i)}_{k_{i(2)}{+1}} \\
(32)
\]

Among them:

\[
\delta \rho^{(i)}_{k_{i(1)}{+1}} = n_{2} \delta \rho^{(i)}_{k} \\
(33)
\]

Further results of feedback correction can be obtained:

\[
(L_{k+1})^* = L_{k+1} + \Delta L_{k} - \delta \hat{L}_{k+1} \\
= L_{k+1} + \Delta L_{k} - \delta L_{k+1} - \Delta L_{k+1} + k_{i(1)} \Delta \rho^{(i)}_{k} \\
= \left( L_{k+1} - \delta L_{k+1} \right) - \Delta L_{k+1} + \left( 1 - \frac{\Delta \rho^{(i)}_{k}}{\Delta L_{k}} \right) k_{i(1)} \Delta L_{k} \\
(34)
\]

\[
(\lambda_{k+1})^* = \lambda_{k+1} + \Delta \lambda_{k} - \delta \hat{\lambda}_{k+1} \\
= \lambda_{k+1} + \Delta \lambda_{k} - \delta \lambda_{k+1} - \Delta \lambda_{k+1} + k_{i(2)} \Delta \rho^{(i)}_{k} + k_{i(2)} \delta \rho^{(i)}_{k_{i(2)}{+1}} \\
(35)
\]

Substituting equations (27) (29) (33) into equations (34) and (35), we get:

\[
(L_{k+1})^* = L_{k+1} + \left( n_{2} - (1 - \alpha) \right) k_{i(1)} \delta \rho^{(i)}_{k_{i(1)}{+1}} \\
\Delta L_{k_{i(1)}{+1}} \\
(36)
\]

\[
(\lambda_{k+1})^* = \lambda_{k+1} + \left( n_{2} + (1 - \alpha) \right) k_{i(2)} \delta \rho^{(i)}_{k_{i(2)}{+1}} \\
\Delta \lambda_{k_{i(2)}{+1}} \\
(37)
\]

where \((L_{j})^*_{i+1}\) and \((\lambda_{j})^*_{i+1}\) are the position results output after spoofing attack at time \(k + 1\); \(L_{k+1}\) and \(\lambda_{k+1}\) are the latitude and longitude results after correct correction at time \(k + 1\), \(\Delta L_{k \rightarrow k+1}\) and \(\Delta \lambda_{k \rightarrow k+1}\) are the position drift after spoofing attack at time range \(k \rightarrow k + 1\).

Since INS will not be disturbed by satellite spoofing signals, the position offset caused by the deceptive interference will be accumulated directly to the next moment, that is:

\[
L_{k+1} + \Delta L_{k \rightarrow k+1} \rightarrow L_{k_{i(2)}{+2}} + \Delta L_{k \rightarrow k+1} \\
\lambda_{k+1} + \Delta \lambda_{k \rightarrow k+1} \rightarrow \lambda_{k_{i(2)}{+2}} + \Delta \lambda_{k \rightarrow k+1} \\
(38)
\]

where \(L_{k+1}\) and \(\lambda_{k+1}\) enter filter calculation at the next time \(k + 2\) as equivalent to the calculation of the correct latitude \(L_{k_{i(2)}{+2}}\) and longitude \(\lambda_{k_{i(2)}{+2}}\) information of INS. \(\Delta L_{k \rightarrow k+1}\) and \(\Delta \lambda_{k \rightarrow k+1}\) enter the filter calculation at the next time \(k + 2\) as a constant deviation.

It is embodied in the pseudo-range calculated by INS at time \(k + 2\):

\[
(\rho_{h_{k+2}}^{(i)} \right)^* = \rho_{h_{k+2}}^{(i)} + \left( n_{3} + n_{2} (1 - \alpha) + (1 - \alpha) \right) \Delta \rho^{(i)}_{k} \\
\Delta \rho^{(i)}_{k_{i(2)}{+2}} \\
(39)
\]

where \((\rho_{h_{k+2}}^{(i)} \right)^*\) is the pseudo-range calculated by the INS at the time of \(k + 2\) when the signal of the deceptive range is accessed at the last moment; \(\rho^{(i)}_{h_{k+2}}\) is the pseudo-range calculated by the INS at the time of \(k + 1\) when there is no spoofing at the last moment, and \(\Delta \rho^{(i)}_{k} \rightarrow k+1\) is the pseudo-range deviation calculated by the INS at time \(k + 2\) caused by the INS latitude and longitude offset \(\Delta L_{k \rightarrow k+1}\) and \(\Delta \lambda_{k \rightarrow k+1}\).

Supposing that the tightly coupled navigation is also subject to deceptive interference at time \(k + 2\), the pseudo-range deception quantity of the \(i\)th satellite added into the GNSS receiver is recorded as \(\delta \rho^{(i)}_{k_{i(2)}{+2}}\), and the ratio between \(\delta \rho^{(i)}_{k_{i(2)}{+2}}\) and \(\rho^{(i)}_{h_{k+2}}\) is recorded as \(n_{3} \cdot \delta \rho^{(i)}_{k_{i(2)}{+2}}\), then the feedback correction output at time \(k + 2\) can be calculated as follows:

\[
(L_{k+2})^* = L_{k+2} + \left( n_{3} + n_{2} (1 - \alpha) + (1 - \alpha) \right) k_{i(2)} \delta \rho^{(i)}_{k_{i(2)}{+2}} \\
\Delta L_{k_{i(2)}{+2}} \\
(40)
\]

\[
(\lambda_{k+2})^* = \lambda_{k+2} + \left( n_{3} + n_{2} (1 - \alpha) + (1 - \alpha) \right) k_{i(2)} \delta \rho^{(i)}_{k_{i(2)}{+2}} \\
\Delta \lambda_{k_{i(2)}{+2}} \\
(41)
\]

where \(L_{k+2}\) and \(\lambda_{k+2}\) enter filter calculation at the next time \(k + 3\) as equivalent to the calculation of the correct latitude and longitude information of INS. And \(\Delta L_{k \rightarrow k+2}\) and \(\Delta \lambda_{k \rightarrow k+2}\) enter the filter calculation at the next time \(k + 3\) as a constant deviation.

Since INS will not be disturbed by satellite spoofing signals, the position offset caused by the deceptive interference will be accumulated directly to the next moment, that is:

\[
L_{k+2} + \Delta L_{k \rightarrow k+2} \rightarrow L_{k_{i(3)}{+3}} + \Delta L_{k \rightarrow k+2} \\
\lambda_{k+2} + \Delta \lambda_{k \rightarrow k+2} \rightarrow \lambda_{k_{i(3)}{+3}} + \Delta \lambda_{k \rightarrow k+2} \\
(42)
\]

Among them, \(L_{k+2}\) and \(\lambda_{k+2}\) enter filter calculation at the next time \(k + 3\) as equivalent to the calculation of the correct latitude \(L_{k_{i(3)}{+3}}\) and longitude \(\lambda_{k_{i(3)}{+3}}\) information of INS. \(\Delta L_{k \rightarrow k+1}\) and \(\Delta \lambda_{k \rightarrow k+1}\) enter the filter calculation at the next time \(k + 2\) as a constant deviation.

It is embodied in the pseudo-range calculated by INS at time \(k + 3\):

\[
(\rho_{h_{k+3}}^{(i)} \right)^* = \rho_{h_{k+3}}^{(i)} + \left( n_{3} + n_{2} (1 - \alpha) + (1 - \alpha) \right) \Delta \rho^{(i)}_{k} \\
\Delta \rho^{(i)}_{k_{i(3)}{+3}} \\
(43)
\]

where \((\rho_{h_{k+3}}^{(i)} \right)^*\) is the pseudo-range calculated by the INS at the time of \(k + 3\) when the signal of the deceptive range is accessed at the last moment; \(\rho_{h_{k+3}}^{(i)}\) is the pseudo-range calculated by the INS at the time of \(k + 3\) when there is no spoofing.
at the last moment, and \( \Delta \rho_{k+1}^{(i)} \) is the pseudo-range deviation calculated by the INS at time \( k+3 \) caused by the INS latitude and longitude offset \( \Delta L_{k+1} \) and \( \Delta \lambda_{k+1} \).

From time \( k \), the deceptive pseudo-range is applied at each time. The ratio of deception pseudo-range at every time to \( k \) is as follows:

\[
\begin{align*}
\delta \rho_k^{(i)} &= n_1 \delta \rho_k^{(i)} \\
\delta \rho_{k+1}^{(i)} &= n_2 \delta \rho_k^{(i)} \\
\vdots \\
\delta \rho_{k+r}^{(i)} &= n_r \delta \rho_k^{(i)} 
\end{align*}
\]

Among them, \( \delta \rho_{k+t}^{(i)} (t = 1, 2, \ldots, r) \) is the spoofing pseudo-range accessed at time \( k+t-1 \); \( n_r \) is the ratio of the amount of pseudo-range deception at time \( k+t \) to the amount of pseudo-range deception at time \( k \).

According to the law of deducing the formula at each moment above, we can get the position output after feedback correction at \( k+r \) time is obtained:

\[
\begin{align*}
(L_{k+r})^t &= L_{k+r} + \Delta L_{k+r} \\
(\lambda_{k+r})^t &= \lambda_{k+r} + \Delta \lambda_{k+r}
\end{align*}
\]

where \( \Delta L_{k+r} \) and \( \Delta \lambda_{k+r} \) are the latitude and longitude offsets caused by the application of deceptive interference from time \( k \) to time \( k+r \), and the specific expression is as follows:

\[
\begin{align*}
\Delta L_{k+r} &= \sum_{i=1}^{r} n_i (1 - \alpha)^{r-i} \delta \rho_k^{(i)} \\
\Delta \lambda_{k+r} &= \sum_{i=1}^{r} n_i (1 - \alpha)^{r-i} \delta \lambda_k^{(i)} \\
\Delta \rho_{k+r}^{(i)} &= \sum_{i=1}^{r} n_i (1 - \alpha)^{r-i} \delta \rho_k^{(i)}
\end{align*}
\]

That is, the total position offset is a linear combination of the position offsets applied at each past time, and the pseudo-range offset calculated by INS is a linear combination of pseudo-range offsets applied to a GNSS receiver applied at each past time.

It is assumed that the deception pseudo-range generated by the spoofing GNSS signal is the same at each time during the deception attack:

\[
\begin{align*}
\delta \rho_k^{(i)} &= \delta \rho_{k+1}^{(i)} = \cdots = \delta \rho_{k+r}^{(i)} \\
n_1 &= n_2 = \cdots = n_r = 1
\end{align*}
\]

Substituting equations (29) and (41) into equation (40):

\[
\begin{align*}
\Delta L_{k+r} &= k_{(1,0)} \sum_{i=0}^{r} (1 - \alpha)^{r-i} \delta \rho_k^{(i)} \\
\Delta \lambda_{k+r} &= k_{(2,0)} \sum_{i=0}^{r} (1 - \alpha)^{r-i} \delta \lambda_k^{(i)} \\
\Delta \rho_k^{(i)} &= \alpha \sum_{i=0}^{r} (1 - \alpha)^{r-i} \delta \rho_k^{(i)}
\end{align*}
\]

The following will further analyze the convergence of the common coefficient \( \sum_{x=0}^{r} (1 - \alpha)^{r-x} \) in equations (42) (43) and (44):

\[
\lim_{r \to \infty} \sum_{x=0}^{r} (1 - \alpha)^{r-x} = \lim_{r \to \infty} \frac{1 - (1 - \alpha)^{r}}{1 - (1 - \alpha)} = \lim_{r \to \infty} \frac{1 - (1 - \alpha)^{r}}{\alpha} (45)
\]

When spoofing signals are always applied, we further analyze the convergence of \( \Delta L_{k \to \infty} \), \( \Delta \lambda_{k \to \infty} \) and \( \Delta \rho_{k \to \infty}^{(i)} \): Substituting equation (29) (46) into equation (42)(43)(44), we can get:

\[
\Delta L_{k \to \infty} = \frac{\Delta L_k}{\Delta \rho_k^{(i)}} \delta \rho_k^{(i)} \quad (47)
\]

\[
\Delta \lambda_{k \to \infty} = \frac{\Delta \lambda_k}{\Delta \rho_k^{(i)}} \delta \rho_k^{(i)} \quad (48)
\]

\[
\Delta \rho_k^{(i)} \to \infty = \delta \rho_k^{(i)} \quad (49)
\]

According to the relationship between the latitude offset \( \Delta L_k \) and longitude offset \( \Delta \lambda_k \) of the tightly integrated navigation system and the pseudo-range offset \( \delta \rho_k^{(i)} \) from the \( i \)th satellite to the INS, we can infer that the coefficients \( \Delta L_k / \Delta \rho_k^{(i)} \) and \( \Delta \lambda_k / \Delta \rho_k^{(i)} \) in equations (47) and (48) respectively represent the degree of latitude and longitude offset that can be caused by the pseudo-range deviation from the \( i \)th satellite to INS.

From equations (47) to (49), it can be seen that when the spoofing GNSS signal designed and constructed by the attacker always applies a fixed pseudo-range offset signal to the \( i \)th satellite at the beginning of the attack, INS/GNSS coupled integrated navigation filter position estimation will eventually output a stable latitude and longitude offset, where the latitude and longitude offset can cause the pseudo-range offset \( \delta \rho_k^{(i)} \) of the \( i \)th satellite to the INS system.

Due to space limitations in section 4.2, we take the \( i \)th satellite as an example to illustrate that when adding the spoofing pseudo-range signal, the position offset is stable. To achieve the precise position offset of the target tightly coupled UAV, We need to design spoofing pseudo-range signals, which adds pseudo-range spoofing to the pseudo-range between each satellite and the GNSS receiver.

C. DESIGN OF SPOOFING CONTROL STRATEGY CAPABLE OF REALIZING ACCURATE POSITION OFFSET

According to formulas (47)-(49), we can find that after accessing the spoofing GNSS signal, the tightly integrated navigation filter position estimation will eventually show a stable latitude and longitude offset, which will cause
pseudo-range offset the $i$th satellite to the INS system. This pseudo-range offset is the same as the pseudo-range spoofing signal. We can design a spoofing control strategy based on the relationship between this position offset and the pseudo-range spoofing signal to achieve the goal of accurate position offset.

When realizing fixed-point capture and other military missions, the offset distance of the target UAV through the GNSS spoofing attack is generally less than 10km from the north or east, and the GNSS satellite is more than 20,000km from the ground. Combined with Fig. 5 and Fig. 6, we can find that after the GNSS spoofing signal is connected, the line of sight vector from the satellite to the INS system changes little under the influence of positional offset.

We can transform the position offset from the local geographical coordinate system to the ECEF coordinate system, the influence of positional offset.

This spoofing control strategy can carry out precise position offset for UAV that is already hovering or in flight, under the condition of knowing the position of a certain point in the planned path. We already know the exact coordinates of a certain point of UAV and the coordinates of the preset capture position, and we can calculate the position offset $X_{\text{NED}} = (\Delta \lambda, \Delta \phi, 0)$ that the UAV needs to achieve on the local geographic coordinate system.

$C_g^e$ is the transformation matrix from ECEF coordinate system to local geographic system From the conversion relationship $(X_{\text{ECEF}},1x3)^T = C_g^e (X_{\text{NED}},1x3)^T$ between the location offset of the local geographic system and the offset under the ECEF coordinate system, we can get:

$$X_{\text{ECEF}} = \left(C_g^e (X_{\text{NED}})\right)^T = X_{\text{NED}} C_g^e \quad (50)$$

ei is the line of sight vector from the inertial navigation system to the $i$th satellite mentioned in Section 1.1, specific $e_i = \left( e_{ix}^i, e_{iy}^i, e_{iz}^i \right)$, is the unit vector.

According to the angle relationship between two vectors in three-dimensional space, the angle relationship between $X_{\text{ECEF}}$ and $e_i$ can be easily obtained:

$$\cos\left(\langle X_{\text{ECEF}}, e_i \rangle\right) = \frac{X_{\text{ECEF}} \cdot e_i}{|X_{\text{ECEF}}| \cdot |e_i|} \quad (51)$$

The projection $|X_{\text{ECEF}}|$ of the proposed deception $X_{\text{ECEF}}$ on the line of sight vector $e_i$ from the INS to the $i$th satellite can be calculated as:

$$|X_{\text{ECEF}}| = \left| X_{\text{ECEF}} \right| \cos \left( \langle X_{\text{ECEF}}, e_i \rangle \right) = \frac{X_{\text{ECEF}} \cdot e_i}{|X_{\text{ECEF}}| \cdot |e_i|} = X_{\text{ECEF}} \cdot e_i = \left(X_{\text{NED}} C_g^e \right) \cdot \hat{e}_i \quad (52)$$

Because the line of sight vector $\hat{e}_i$ to be shifted to the $i$th satellite is approximately parallel to the line of sight vector $\hat{e}_i$ from the original position to the $i$th satellite, the increment of the pseudo-range of the proposed deception $X_{\text{ECEF}}$ can be equivalent to the projection $|X_{\text{ECEF}}|$ of $X_{\text{ECEF}}$ on the unit line of sight vector $\hat{e}_i$ between the tightly combined system and the $i$th satellite at the moment. If the pseudo-range deception derived from the above strategy is applied to each satellite pseudo-range received by GNSS receiver, the precise offset of longitude and latitude can be completed. We will verify the accuracy of this strategy through the next two sections of simulation test and tightly coupled terminal test.

V. SIMULATION TEST AND ANALYSIS

For the following, we carry out a series of static pseudo-range deception simulation experiments based on the spoofing control strategy designed in Section 4.3. The longitude and latitude used in the simulation experiment are: Changsha north latitude 28.1° east longitude 112.6°. Other simulation
FIGURE 7. The curve of position offset (The red curve shows the offset after receiving the pseudo-range deception signal, and the blue curve shows the offset without receiving the pseudo-range deception signal).

conditions are the same as those in the section 2.3 simulation experiment, see Table 1. The simulation experiment consists of four parts (pseudo-range deception as input and position information as output):

1) Tightly combination simulation positioning experiment 1, with the pseudo-range spoofing signals added at 300s (effect: 4000m north offset and 4000m east offset). We can get the position output of the experiment in Figure 7 (a);

2) Tightly combination simulation positioning experiment 2, with the pseudo-range spoofing signals added at 300s (effect: 2000m north offset and 2000m east offset) and superimposed at 600s (effect: 2000m north offset and 2000m east offset). We can get the position output of the experiment in Figure 7 (b);

3) Tightly combination simulation positioning experiment 3, with the pseudo-range spoofing signals added at 300s (effect: 2000m north offset and 2000m east offset) and superimposed at 350s (effect: 2000m north offset and 2000m east offset). We can get the position output of the experiment in Figure 7 (c);

4) Tightly combination simulation positioning experiment 3, with the pseudo-range spoofing signals added at 300s (effect: 5000m north offset and 5000m east offset) and superimposed at 600s (effect: −1000m north offset and −1000m east offset). We can get the position output of the experiment in Figure 7 (d).

The simulation results are shown in Figure 7. From the overall simulation results, it can be seen that the precise
The position offset of the tightly integrated navigation system can be achieved within 100s after the pseudo-range deception is introduced into the Kalman filter of the compact integrated navigation system, and the accuracy of the east offset is higher than that of the north offset. Combined with Figure 7 (a)(b)(d), we can find that the pseudo-range deception signal designed in Section 3.3 superimposed to the tightly coupled system after the system reaches the set offset position can continue to reach the predetermined offset position. Furthermore, we found that the application of single GNSS spoofing and two GNSS spoofing signals are equivalent in position offset accuracy. This shows that the spoofing control strategy proposed in Section 3.3 can be overlapped in practice, and the position output offset of integrated navigation is stable under deceptive jamming.

Combined with Figure 7 (a)(b)(c), we can find that when the position offset does not reach a stable state, the superposition of pseudo-range deception signal can also achieve the effect that one single pseudo-range deception can achieve. This shows that we can regularly change the deceptive pseudo-range signal through this feature, which can make the UAV trajectory change more slowly, not be detected by the simple GNSS anti-spoofing module, and finally, reach the same deception position.

In order to further analyze the deception effect of the tightly integrated navigation system, this paper defines that the preset position offset \( \mathbf{r}_s \) consists of the preset north offset \( r_{sn} \) and the preset east offset \( r_{se} \), where the subscript \( s \) represents the preset spoofing sign, \( n \) represents the north direction, and \( e \) represents the east direction. The actual location offset \( \mathbf{r}_a \) consists of the actual location offset \( r_{an} \) in the north direction and the actual location offset \( r_{ae} \) in the east direction. For details, \( \mathbf{r}_a = (r_{an}, r_{ae}) \), where the subscript represents the actual offset, \( n \) represents the north direction, and \( e \) represents the east direction.

The calculation formula for defining the position offset effect \( \overline{\theta} \) is as follows:

\[
\overline{\theta} = 1 - \frac{||\mathbf{r}_s - \mathbf{r}_a||}{||\mathbf{r}_s||} = 1 - \frac{\sqrt{(r_{sn} - r_{an})^2 + (r_{se} - r_{ae})^2}}{\sqrt{(r_{sn})^2 + (r_{se})^2}}
\]

The specific analysis and verification of the position offset effect are shown in the table below:

| Preset offset \( r_s \) | Actual offset \( r_a \) | Pull off effect \( \overline{\theta} \) (\%) |
|-------------------------|-------------------------|---------------------------------|
| (20000,20000)           | (19997.19999964)         | 99.97                           |
| (40000,40000)           | (39967.399881)           | 99.94                           |
| (100000,100000)         | (9979.7499952)           | 99.85                           |

It can be seen from the Table 2 that in the simulation experiment, the position offset effect of the deception interference on the estimated offset exceeds 99.85% in the case of north or east direction less than 10km, which can achieve the precise position offset of the tightly integrated navigation system. This can fully verify that the spoofing control strategy designed in Section 4.3 can be used to achieve precise spoofing offset for the INS/GNSS tightly coupled navigation position.

VI. VERIFICATION OF DECEPTION TEST OF INTEGRATED NAVIGATION TERMINAL

In order to fully verify the correctness of the spoofing control strategy proposed in Section 4.3, this paper further conducted tightly integrated navigation terminal experiments.

Firstly, based on the GPS satellite receiver, the satellite signal simulator, the integrated box of power amplifier and the signal transmitter, this paper builds the false satellite signal generator required in Section 4.3, as shown in Figure 8.

![FIGURE 8. Main equipment of fake satellite signal generator, including (a) GPS satellite signal receiver, (b) satellite signal simulator and integrated box of power amplifier, (c) signal transmitter.](image)

By using the spoofing satellite signal generator, the precise position deception offset test is carried out for the tightly integrated navigation terminal (computer and MTI). The specific test plan is: on the university playground, the tightly-coupled terminal follows the path indicated by the red line in Figure 10, during which it receives normal satellite signals. At the spoofing strategy starting point (marked in Figure 10), according to the spoofing strategy derived in Section 4.3, fake satellite signal generator is used to send the pseudo-range spoofing signals to the GPS receiver of MTI to cause a positioning offset of the terminal. The spoofing signals used in the experiment are divided into the following three categories:

Spoofing signal 1: north offset 20m, east offset 20m;
Spoofing signal 2: north offset 40m, east offset 40m;
Spoofing signal 3: north offset 80m, east offset 80m.

Figure 9 shows the spoofing environment of tightly integrated navigation terminal.

Figure 10 and Figure 11 show the test results of the terminal. It can be seen from Figure 10 that when the terminal receives the real satellite signal, the integrated navigation filter outputs the correct positioning result. However, when the fake GPS signal is implanted into the terminal, the positioning...
result of the terminal starts to change and finally reached the preset position offset set by the attacker.

From Figure 11, we can find that when accessing the spoofing signal, the effect of the tightly integrated navigation terminal on the east offset is better than that of the north offset, which is the same as the conclusion of the simulation experiment in Section 5. After the spoofing signal is connected to the terminal, the positioning offset of the tight combination navigation has been achieved. But the error from the predetermined offset distance has fluctuated in the north and east directions. We found that the tightly integrated navigation terminal changed its direction of movement during this period, thereby stimulating some errors. However, if the tight combination terminal keeps its direction of motion unchanged, the error will quickly decay, which will not greatly affect the effect of position shift.

Actually, the reason affecting the accuracy is mainly composed of three parts:

1) The error caused by the fluctuation of the steady-state gain matrix after adding deception, which is very small but difficult to eliminate;

2) The calculation error of the position vector projected on the sight vector, which can be eliminated by fitting or compensation;

3) Experiment site noise and the error caused by the GPS signal generator, which is mainly related to equipment performance.

Through the above experiments, we can surely infer that the spoofing strategy can fulfill the task requirements of the precise offset of the UAV system in tightly integrated navigation.

VII. CONCLUSION AND EXPECTATION

In this paper, a spoofing control strategy for INS/GNSS tightly coupled system has been proposed. The spoofing control strategy neither needs external sensors to understand the flight status of UAV nor need to calculate and adjust the GNSS deception signal at any time. The strategy only needs to know a certain point in the trajectory of UAV(not include the trajectory before stable access to the spoofing signals) to complete the precise position offset of UAV or to know the general direction of UAV travel to complete the directional drive of UAV. To improve the effectiveness of this spoofing control strategy and the improvement of deception interference technology, the following aspects can be promoted in the work:

1) The spoofing control strategy proposed in this paper simplifies the conversion relationship between position offset and pseudo-range offset when calculating the GNSS deception signal. In the next step of work and analysis, the corresponding offset position output error model can be deduced, supplemented and added to the control strategy to compensate the error, and improve the effect of accurate position offset.

2) In this paper, when the spoofing control strategy is applied, the smoothness of the deception trajectory is not
considered according to the different flight speed limits of a specific type of tightly combined UAV. However, according to the additivity of the spoofing control strategy obtained from the simulation experiment, further research can be done in this area. Also the anti-spoofing fault detection scheme is also a very meaningful work in the following research.

3) In this paper, the GNSS spoofing attack is carried out on INS/GNSS tightly coupled Kalman filter, and the position output results of the commonly used Kalman filter in response to access spoofing are derived and analyzed in detail. The simulation and tightly coupled terminal test in this paper show that it is possible to achieve the goal of precise position shift for tightly combined UAV. We can continue to conduct research and comparison on the spoofing control strategies of different combined navigation to achieve better deception control effect, which is worthy of further efforts.

ACKNOWLEDGMENT
The authors acknowledge all the editors and reviewers who give many detailed suggestions which considerably improved the contents.

REFERENCES
[1] A. Bhardwaj, L. Sam, Akanksha, F. J. Martín-Torres, and R. Kumar, “UAVs as remote sensing platform in glaciology: Present applications and future prospects,” Remote Sens. Environ., vol. 175, pp. 196–204, Mar. 2016.
[2] Z. Kaleem and M. H. Rehmani, “Amateur drone monitoring: State-of-the-art architectures, key enabling technologies, and future research directions,” IEEE Wireless Commun., vol. 25, no. 2, pp. 150–159, Apr. 2018, doi: 10.1109/mwc.2018.1700152.
[3] D. He, S. Chan, and M. Guizani, “Communication security of unmanned aerial vehicles,” IEEE Wireless Commun., vol. 24, no. 4, pp. 134–139, Aug. 2017.
[4] M. R. Mosavi, Z. Nasrpooya, and M. Moazedi, “Advanced anti-spoofing methods in tracking loop,” J. Navigat., vol. 69, no. 4, pp. 883–904, 2016.
[5] K. Hartmann and C. Steup, “The vulnerability of UAVs to cyber-attacks—An approach to the risk assessment,” in Proc. 5th Int. Conf. Cyber Con- flict (CyCon), Jun. 2013, pp. 1–23.
[6] 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.
[7] J. Huang, L. L. Presti, B. Motella, and M. Pini, “GNSS spoofing detection: Theoretical analysis and performance of the ratio test metric in open sky,” ICT Express, vol. 2, no. 1, pp. 37–40, Mar. 2016.
[8] G. Gerten, “Protecting the global positioning system,” IEEE Aerosp. Electron. Syst. Mag., vol. 20, no. 11, pp. 3–8, Nov. 2005.
[9] J. V. Carroll, “Vulnerability assessment of the U.S. transportation infrastructure that relies on the global positioning system,” J. Navigat., vol. 56, no. 2, pp. 185–193, May 2003, doi: 10.1109/tvt.2019.2914477.
[10] Y. Guo, M. Wu, K. 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, doi: 10.1109/tvt.2019.2914477.
[11] A. Budiyono, “Principles of GNSS, inertial, and multi-sensor integrated navigation systems,” Ind. Robot, Int. J., vol. 39, no. 3, pp. 191–192, Apr. 2012.
[12] M. Wang, W. Wu, P. Zhou, and X. He, “State transformation extended Kalman filter for GPS/SINS tightly coupled integration,” GPS Solutions, vol. 22, no. 4, Oct. 2018, Art. no. 112, doi: 10.1007/s10291-018-0773-3.

SHUHAI LU received the B.S. degree from the School of Mechatronics and Automation, National University of Defense Technology, China, in 2013. He is currently pursuing the master’s degree with the College of Intelligence Science and Technology, National University of Defense Technology. His current research interests include GPS/INS-integrated navigation system and gravity measurement.

YAN GUO received the B.S. degree in measurement and control technology and instrumentation program and the M.S. degree in control science and engineering from Harbin Engineering University, Harbin, China, in 2013 and 2015, respectively, and the Ph.D. degree in control science and engineering from the National University of Defense Technology, Changsha, China, in 2019. She is currently a Lecturer with the Depart- ment of Automatic Control, National University of Defense Technology. Her research interests include GPS spoofing technology, GPS/INS-integrated navigation systems, and UAV control systems.

HANG SHANG received the B.S. degree from the School of Information Science and Engineering Central South University, China, in 2019. He is currently pursuing the master’s degree with the College of Intelligence Science and Technology, National University of Defense Technology. His current research interests include GPS/INS-integrated navigation system and bionic navigation.
KANGHUA TANG received the Ph.D. degree in control science and engineering from the National University of Defense Technology, Changsha, China, in 2008. He is currently a Associate Researcher with the Department of Automatic Control, National University of Defense Technology. His research interests include GPS spoofing technology and anti-spoofing GPS technology.

JULIANG CAO received the Ph.D. degree in control science and engineering from the National University of Defense Technology, Changsha, China, in 2004. He is currently a Professor with the Department of Automatic Control, National University of Defense Technology. His research interests include inertial navigation technology, gravity measurement, and GPS navigation technology.

RUIHANG YU received the Ph.D. degree in control science and engineering from the National University of Defense Technology, Changsha, China, in 2018. He is currently a Lecturer with the Department of Automatic Control, National University of Defense Technology. His research interests include GPS/INS-integrated navigation systems and gravity measurement.

SHAOKUN CAI received the Ph.D. degree in control science and engineering from the National University of Defense Technology, Changsha, China, in 2014. He is currently an Associate Professor with the Department of Automatic Control, National University of Defense Technology. His research interests include GPS/INS-integrated navigation systems and gravity measurement.