Performance analysis of generated spoofing under integrated navigation conditions

Menghao He¹, Changgeng Li²*, Chao Zhou³ and Chao Ma⁴

¹School of Physics and Electronics, Central South University, Hunan, China
²School of Physics and Electronics, Central South University, Hunan, China
³School of Intelligent Science, National University of Defense Technology, Hunan, China
⁴School of Intelligent Science, National University of Defense Technology, Hunan, China

*Corresponding author e-mail: lcgeng@csu.edu.cn

Abstract. Based on the establishment of the loosely coupled integrated navigation model, this paper realizes generated spoofing by superimposing position increments in the positional state variables of the integrated navigation system. Theoretically deducing the delivery process of the position increment of the spoofing signal in the integrated navigation, thereby analyzing the influence of position increment on global satellite navigation system (GNSS) and GNSS/INS. The generated spoofing is divided into constant slanting and point-by-point slanting. The simulation analyzes the performance of the two spoofing strategies in the presence or absence of spoofing detection and the effect of different values of integrated navigation parameters on spoofing performance. The simulation results show that the point-by-point slanting and the constant value slanting are better in the presence or absence of spoofing detection, respectively. The value of the integrated navigation parameters will affect the spoofing performance.

1. Introduction

With the gradual opening up of low-altitude airspace by national policies, commercial-grade unmanned aerial vehicle (UAV) represented by “DJI” have been widely used in our lives [1]. However, the criminals use the advantages of the strong mobility, fast speed and small size of the UAV are engaged in illegal activities pose a serious threat to the security of the country and the people. Common attacks against non-cooperative UAVs include acoustic interference, navigational spoofing, hacking techniques, laser cannons, and radio control. Their characteristics and effects are different [2]. Navigational spoofing is divided into forwarded spoofing and generated spoofing: the forwarded spoofing uses the navigation spoofing device to forward the received real satellite navigation signal with high quality, increasing the time when the navigation signal reaches the UAV. Thereby changing the pseudorange information in the navigation and positioning equation, and spoofing the navigation system to locate the false position. The generated spoofing use the navigation spoofing device to directly generate spoofing signal and transmit them to the UAV. It ignores the real signal and works under the spoofing signal, thereby solving the wrong position information and achieving the purpose of spoofing [3, 4].
When the UAV has only GNSS, the navigation spoofing device can take over the navigation system of the UAV and achieve arbitrary spoofing. However, most UAVs use the GNSS/INS, including GNSS and inertial navigation system (INS). GNSS/INS overcome the shortcomings of each individual system [5, 6], and improve the positioning accuracy and anti-spoofing of the UAV. At the same time, due to the rapid development of the navigation spoofing technology, the spoofing detection method came into being, and mainly detect the UAV's motion state or navigation signal [7, 8]. Once the spoofing signal is detected, the navigation system will switch to the pure inertial navigation mode causing spoofing failure [9]. The spoofing detection method greatly increase the difficulty of the navigation spoofing. Therefore, how to spoof quickly and concealed the UAV to the fraudulent position becomes an urgent problem to research.

2. Generating spoofing principle

Generated spoofing is based on receiving the real navigation signal at the current moment and measuring the real motion parameters of the UAV and the spoofing requirements. The spoofing signals have the same characteristics to the real signal but has higher power. Then UAV ignores the real signal and works under the spoofing signal, thereby solving the wrong position. This article assumes that the spoofing signal has been generated based on the spoofing requirement and successfully cut into the UAV. The generated spoofing model is shown in Figure 1.

![Figure 1. The generated spoofing model](image)

Take GPS civilian signal as an example [10], the navigation spoofing signal is:

\[ S_c(t) = k A_c D_s(t) C(t+\Delta \tau) \cos(\omega(t+\Delta \tau) + \varphi) \]  

(1)

Where \( k \) is the power amplification factor; \( A_c \) represents the amplitude of \( C/A \) code; \( D_s(t) \) is the ephemeris information of the false satellite signal; \( C(t) \) represents the \( C/A \) code; \( \Delta \tau \) represents the delay of the spoofing signal relative to the real signal; \( \omega \) is the angular frequency of \( L1 \); \( \varphi \) is the initial phase of the \( L1 \) frequency carrier.

3. Loosely coupled integrated navigation model

The GNSS/INS is divided into loose coupling, tight coupling and deep coupling according to the degree of coupling. Since loose coupling is easy to implement in engineering, this paper only discusses the loosely coupled integrated navigation system. In the loosely coupled integrated navigation system, the position and velocity of GNSS and INS are calculated separately, and the difference between the position and speed of GNSS and INS is taken as the measured value. The optimal estimation value of the relevant state variables is obtained by Kalman Filter estimation, and the INS is corrected by the optimal estimation value and the position of the GNSS/INS is output, thereby realizing the data fusion of GNSS and INS [11]. The loosely coupled integrated navigation system model is shown in Figure 2.
Since the height and vertical speed of the UAV are provided by the barometer measurement and will not be deceived, they are not considered in the modeling and analysis. The loosely coupled integrated navigation system selects the error variable of INS as the error state quantity, mainly include position error, speed error, attitude angle error, gyroscope constant deviation, and accelerometer constant deviation.

The error state quantity of the INS is recorded as:

$$X = \begin{bmatrix} \delta L & \delta \lambda & \delta V_x & \delta V_y & \phi_x & \phi_y & \phi_z & e_{bx} & e_{by} & e_{bz} & \nabla_{bx} & \nabla_{by} & \nabla_{bz} \end{bmatrix}$$ \hspace{1cm}(2)$$

Where $\delta L$ and $\delta \lambda$ are the position error vector, $\delta V_x, \delta V_y$ are the velocity error vector, $\phi_x, \phi_y, \phi_z$ are the attitude angle error vector, $e_{bx}, e_{by}, e_{bz}$ are the gyroscope constant zero offset vector, $\nabla_{bx}, \nabla_{by}, \nabla_{bz}$ are the accelerometer constant zero deviation.

The equation of state and the measurement equation of the integrated navigation system can be expressed as:

$$\dot{X}_i = F_{i,i-1}X_{i-1} + G_{i,i-1}W_i$$ \hspace{1cm}(3)$$

$$Z_i = \begin{bmatrix} P_{INS,i} - P_{GNNSS,i} \\ \nu_{INS,i} - V_{GNNSS,i} \end{bmatrix} = H_iX_i + V_i \hspace{1cm}(4)$$

Where $F$ is the state transition matrix, $G$ is the system noise matrix, $W$ is the process noise, $H$ is the measurement matrix, $V$ is white noise.

General process of Kalman Filter Equation:

1. One-step prediction equation of state
   $$\hat{X}_{i,i-1} = F_{i,i-1}\hat{X}_{i-1}$$ \hspace{1cm}(5)$$

2. One-step prediction of mean square error
   $$P_{i,i-1} = F_{i,i-1}P_{i-1}F_{i,i-1}^T + G_{i-1}Q_{i-1}F_{i,i-1}^T$$ \hspace{1cm}(6)$$

3. Filter gain equation
   $$K_i = P_{i,i-1}H_i^T( H_iP_{i,i-1}H_i^T + R_i)^{-1}$$ \hspace{1cm}(7)$$

4. Filter estimation equation (optimal estimate)
   $$\hat{X}_i = \hat{X}_{i,i-1} + K_i(Z_i - H_i\hat{X}_{i,i-1})$$ \hspace{1cm}(8)$$

$Z_i - H_i\hat{X}_{i,i-1}$ can be rewritten as:
\[ Z_i - H_i \hat{X}_{i,i-1} = H_i(\hat{X}_i - \hat{X}_{i,i-1}) + V_i \]  

(9) Filtered mean square error update matrix

\[ P_i = (I - K_i H_i) P_{i,i-1} \]  

(10)

Where \( \hat{X}_{i,i} \) is the filter estimate of the state variable \( X_{i,i} \), \( \hat{X}_{i,i-1} \) is a one-step prediction of the state variable \( X_i \) using the value of \( \hat{X}_{i,i-1} \). \( P_{i,i-1} \) is based on the mean square error matrix \( P_{i,i} \) at the previous moment and the system noise variance \( Q_i \), \( H_i P_{i,i} H_i^T \) and measurement noise covariance \( R_i \) are the mean square error matrix of \( H_i(\hat{X}_i - \hat{X}_{i,i-1}) \) and \( V_i \) in the innovation equation \( \hat{X}_i - \hat{X}_{i,i-1} \), respectively. \( \hat{X}_i - \hat{X}_{i,i-1} \) is called the innovation equation \([12]\) and \( V_i \) is the measurement error.

It can be known from formulas (5) to (10), \( R_i \), \( P_i \), \( Q_i \) affect the size of the filter gain \( K_i \). The larger \( K_i \), the greater the weight of \( \hat{X}_i - \hat{X}_{i,i-1} \) and the smaller the relative weight of the estimate \( \hat{X}_{i,i-1} \), the greater the confidence that the Kalman filter trusts the measured values.

4. Generated spoofing for integrated navigation systems

4.1 Spoofing satellite navigation system

When the UAV uses only the GNSS, once it is deceived, the calculated navigation information includes location increment and speed increment. This article only analyzes the location information, regardless of the speed information. Therefore, under the generated spoofing, false position information can be expressed as:

\[ \begin{bmatrix} P_{i,i}^{\text{GNSS}} \\ V_{i,i}^{\text{GNSS}} \end{bmatrix} = \begin{bmatrix} L_{\text{au}} + \Delta L_i^{\text{GNSS}} \\ \lambda_{\text{au}} + \Delta \lambda_i^{\text{GNSS}} \end{bmatrix} \]  

(11)

Where \( L_{\text{au}}, \lambda_{\text{au}} \) is the real location information, \( \Delta L_i^{\text{GNSS}} \), \( \Delta \lambda_i^{\text{GNSS}} \) is the location increment caused by spoofing.

Once the spoofing signal is cut into the UAV, the navigation spoofing device will take over the navigation system. When the position increment \( \Delta P_i \) is superimposed on the position state variable, the position of the navigation system is pulled off \( \Delta P_i \). When the UAV is only equipped with GNSS, the position increment \( \Delta P_i \) is equal to the position offset \( \Delta P_z \), because there is no other navigation system assistance. It is shown that the navigation system position output can be changed by superimposing the position increment, and the position offset is predictable. By changing \( \Delta L_i^{\text{GNSS}} \) and \( \Delta \lambda_i^{\text{GNSS}} \), the deceiver can pull the UAV to any spoofing position in any direction.

4.2 Spoofing integrated navigation system

The INS is free from spoofing, so the spoofing of the GNSS/INS is essentially deceiving the GNSS. Under the spoofing attack, the GNSS position include additional spoofing-induced the superimposed position increment. Therefore, the volume measurement \( Z_i \) of the GNSS/INS can be expressed as:

\[ \begin{bmatrix} L_{\text{INS}} - L_{\text{GNSS}} \\ \lambda_{\text{INS}} - \lambda_{\text{GNSS}} \end{bmatrix} = \begin{bmatrix} L_{\text{INS}} - (L_{\text{au}} + \Delta L_i^{\text{GNSS}}) \\ \lambda_{\text{INS}} - (\lambda_{\text{au}} + \Delta \lambda_i^{\text{GNSS}}) \end{bmatrix} \]  

(12)

Due to the superposition of the position increment of the GNSS, the INS is corrected incorrectly, and the GNSS/INS outputs the wrong position. The location of the GNSS/INS \( P_{i,i}^{\text{GNSS/INS}} \) is expressed as:
Where $L'_i$ and $\lambda'_i$ are the spurious state of the latitude state and the longitude state variable; $\hat{L}'_i$ and $\hat{\lambda}'_i$ are the optimal estimate of the latitude and the longitude state variable.

Therefore, the position increment caused by spoofing is transmitted during the estimation process, and the erroneous optimal estimate continuously modifies the INS. The wrong optimal estimate is iteratively accumulated, and finally the position offset of the GNSS/INS is obtained. In the GNSS/INS, the position increment $\Delta L_{\text{GNSS}}^p$ and $\Delta \lambda_{\text{GNSS}}^p$ in the spoofing signal and the optimal estimated value $\hat{L}'_i$ and $\hat{\lambda}'_i$ are not equal, which makes it impossible to predict the positional offset and increases the difficulty of spoofing.

5. Spoofing performance analysis

5.1 Spoofing strategy

Under spoofing attacks, position increments are superimposed on the position state variable to achieve spoofing. The position increment in the spoofing signal can be defined as:

$$\begin{align*}
\Delta L_{\text{GNSS}}^p &= L(t) + a \\
\Delta \lambda_{\text{GNSS}}^p &= \lambda(t) + b
\end{align*}$$

(14)

Where $L(t)$ and $\lambda(t)$ is a time-varying function, $a$ and $b$ is a constant. We have designed two different spoofing strategies based on the way they are superimposed:

(1) Constant slanting: When $L(t)$ and $\lambda(t)$ are equal to 0, $P_{\text{GNSS}}^{p}$ is a constant. Taking the UAV's planned trajectory as a reference. Superimposing position increments on the position state variables of the GNSS, so that it is always positioned at the spoofing position. Under spoofing attacks, the GNSS/INS measurement is the difference between the error location of the GNSS and the position of the INS. Obtained the wrong optimal estimate after Kalman filter estimation, which causes the INS to get incorrect corrections. The GNSS/INS is gradually pulled to the false position to achieve constant slanting.

(2) Point-by-point slanting: When $a$ and $b$ are equal to 0, $P_{\text{GNSS}}^{p}$ is a time-varying function. Taking the actual position of the UAV as a reference. Superimposing a relatively small position increment on the position state variable of the GNSS. Adjusting the position increment in the spoofing signal in real time to ensure that the magnitude of each pull is small. The GNSS/INS is slowly pulled to the false position to achieve point-by-point slanting.

5.2 Performance analysis of different spoofing strategies

This paper assumes that the UAV is at rest, analyzes the feasibility and advantages and disadvantages of two spoofing strategies when there is no means of spoofing detection. The method of spoofing detection is to determine the optimal estimate. When the optimal estimated value exceeds the set threshold, the navigation system will switch to the pure inertial navigation mode, and spoofing cannot be achieved. Since the average speed of general commercial UAV can only reach 20m/s, the spoofing threshold is set to 30m.

Scene (1): When there is no spoofing detection means, the spoofing signal is cut in the 1s. The constant slanting is used, that is, the positional increment is superimposed by 2000 meters, so that the GNSS is always positioned at the fraud position. When the point-by-point slanting is used, that is, superimposing a relatively small position increment on the latitude state variable. In the case of no spoofing detection, the constant slanting and the point-by-point slanting diagram are shown in figure 3 and figure 4, respectively.
In figure 3, GNSS is always positioned in the fraud position. The deflection speed is faster within 10s, the maximum position offset reaches 710m at 2s. After 20s, GNSS/INS gradually approaches the fraud position, resulting in a decrease in the measured value and a slower pull speed. Finally, GNSS/INS was deflected to within 100 meters of the spoofing position in 42s. It can be seen from figure 4 that by adjusting the position increment in real time, GNSS/INS gradually approaches the deceiving position with a small positional offset, and finally needs 744s to be slowly pulled to within 100m of the spoofing position.

Comparing the above two figures, both spoofing strategies are feasible, but the constant slanting can pull the GNSS/INS to the spoofing position faster than the point-by-point slanting. It shows that the spoofing performance of the constant slanting is better when there is no spoofing detection.

Scene (2): When there is a spoofing detection method, the spoofing signal is cut in 50s, the static UAV is pulled to the latitude direction by 2000m. In the case of spoofing detection, the constant slanting and the point-by-point slanting diagram are shown in figure 5 and figure 6, respectively.

In Figure 5, the upper graph shows the spoofing distance, and the lower graph shows the optimal estimated value. The GNSS/INS has only a small positional offset before the spoofing signal is cut. After the spoofing signal is cut in the 50s, the position of the superimposed position is too large, and the optimal estimated value reaches 38m, which exceeds the set threshold. The navigation system switches to the pure inertial navigation mode, causing in spoofing failure, the location of GNSS/INS remains unchanged. It can be seen from figure 6, since the real-time adjustment position increment ensures that the position offset is small, the optimal estimator never exceeds the spoofing detection threshold by 30m, and finally the GNSS/INS can be slowly biased to the spoofing position.

Comparing the above two figures. When the constant slanting is used, although the pull speed is fast, it is easy to trigger the spoofing detection threshold, which causes the navigation system to switch to the pure inertial navigation mode, causing in spoofing failure. When the point-by-point slanting is used, although the pull-off speed is slow, the spoofing signal is controllable, and the GNSS/INS can be...
slowly biased to the spoofing position. It shows that when there is a spoofing detection method, the
spoofing performance of the point-by-point slanting is better.

5.3 The effect of navigation parameter on spoofing performance

\( R \) is an important parameter in the filtering process, it represents the accuracy of the GNSS. The
higher the accuracy of the GNSS, the smaller the measurement noise covariance \( R \), the larger the filter
gain \( K_i \), and the greater the weight of the innovation equation \( \hat{X}_i - \hat{X}_{i-1} \), then the more
the Kalman filter trusts the measured value, that is, the more the GNSS/INS trusts the GNSS. The values of
the integrated navigation parameters are shown in Table 1:

| Gyro random offset | Accelerometer bias | Inertial navigation sampling period | Satellite navigation positioning accuracy | Satellite navigation speed measurement accuracy | Satellite navigation sampling period |
|--------------------|-------------------|-----------------------------------|------------------------------------------|-----------------------------------------------|------------------------------------|
| 0.005°/h           | 5*10^-5g          | 10ms                              | 3m/s                                     | 0.01m/s^2                                    | 1s                                 |

The measurement noise covariance is infinitesimal, 0.01R, R, 50R, 100R, infinity, and the spoofing
strategy of constant slanting is applied to the stationary UAV. The simulation results are shown in
Figure 8.

Figure 7. Spoofing performance at different R values

When \( R \) is equal to infinity, the Kalman Filter only trusts the measured value, that is, the
GNSS/INS only trusts the GNSS. At this time, the GNSS/INS is equivalent to only the GNSS., and
only 8.2s can pull the GNSS/INS to the spoofing position within 100m; When 0.01*R and R, it takes
250s and 428s respectively to pull the GNSS/INS to the spoofing position within 100m; When 50*R
and 100*R, it takes 810s or more; When equal to infinity, the Kalman Filter only trusts the predicted
value, that is, the GNSS/INS only trusts the INS. At this time, the GNSS is equivalent to only the INS.
Since the INS is not subject to spoof, it is impossible to pull the GNSS/INS to the spoofing position.
Therefore, under the integrated navigation conditions, the higher the accuracy of the GNSS, the
smaller the measurement noise covariance, and the more the GNSS/INS trusts the GNSS, the faster the
deflection speed.

5.4 Spoofing trajectory control

Once the navigation system is taken over by the navigation spoofing device, the trajectory of the
UAV is precisely controlled by adjusting the position increment in the spoofing signal in real time.
Assuming that the UAV is in a stationary state, generative spoofing is implemented for the GNSS/INS,
and its output trajectory is controlled to be a rectangle. A schematic diagram of the fraudulent
trajectory control is shown in Figure 8:
As shown in Figure 9, under spoofing attacks, the GNSS/INS output trajectory is OABCD, and the O point is the start and end points. During OE spoofing, since the skew is performed only in the latitude direction, the longitude state variable difference between GNSS and INS is zero, and no correction is made in the longitude direction. Therefore, it is only necessary to pull the GNSS from the O point to the A point, so that the GNSS/INS can be pulled from the O point to the E point. During EF spoofing, since the UAV is stationary, the position of the INS is always at point O. There is a difference between the latitude/longitude state variables of GNSS and INS, so it is necessary to simultaneously perform the pull-off in the latitudinal direction and the longitude direction to achieve the GNSS/INS from the E point to the F point. The same is true during FG and GO. Through the simulation of the spoofing trajectory control, the controllability of the generated spoofing is strong, and the spoofing signal can be designed according to the spoofing requirement, thereby realizing precise positional deviation.

6. Conclusion

This paper theoretically derives the transfer process of position increment in integrated navigation. Simulation analysis of the performance of two spoofing strategies and the impact of different values of integrated navigation parameters on spoofing performance. Thereby, it can achieve the purpose of the spoofing trajectory control of GNSS/INS. Obtained the following three conclusions: (1) when there is no spoofing detection, the spoofing performance of the constant slanting is better. Although both spoofing strategies are feasible, the pull-off speed of constant slanting is far more than point-by-point slanting. (2) when there is spoofing detection, the spoofing performance of point-by-point slanting is better. The constant slanting easily triggers the spoofing detection threshold, which causes the spoofing to fail. Although the point-by-point slanting is slow, it can pull the GNSS/INS to the spoofing position and is not found. (3) the higher the accuracy of the GNSS, the more the GNSS/INS trusts the GNSS, resulting in the faster the GNSS/INS is deflected, the better the spoofing performance.

References

[1] Xia Mingyu, Zhao Kai, Ni Wei. Anti-UAV System and Key Technology for Key Point Defense [J]. Command Control & Simulation, 2018, 40(2): 55 － 60. W. Strunk Jr., E.B. White, The Elements of Style, third ed., Macmillan, New York, 1979.
[2] PAN Xinghong, QIN Zhiqiang. A study of anti-UAV-system [J]. scientific Chinese, 2016(5):29.
[3] Schmidt, D.; Radke, K.; Camtepe, S.; Foo, E.; Ren, M. A Survey and Analysis of the GNSS Spoofing Threat and Countermeasures. Acm Comput. Surv. 2016, 48, 1–31.
[4] Bhatti, J.; Humphreys, T.E. Hostile Control of Ships via False GPS Signals: Demonstration and Detection.Navigation 2017, 64, 51 – 66.
[5] Konovaltsev, A.; Cuntz, M.; Haettich, C.; Meurer, M. Autonomous Spoofing Detection and Mitigation in a GNSS Receiver with an Adaptive Antenna Array. In Proceedings of the 26th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2013), Nashville, TN, USA, 16–20 September 2013; pp. 2937–2948.
[6] Shaeffer, D.K. MEMS inertial sensors: A tutorial overview. Commun. Mag. IEEE 2013, 51, 100–109.

[7] Psiaki, M.L.; O’hanlon, B.W.; Powell, S.P.; Bhatti, J.A.; Wesson, K.D.; Humphreys, T.E. GNSS spoofing detection using two-antenna differential carrier phase. GPS World 2014, 25, 36–44.

[8] Dovis, F. GNSS Interference Threats and Countermeasures; Artech House: Norwood, MA, USA, 2015.

[9] Akos D M. “Who's Afraid of the Spoofer? GPS/GNSS Spoofing Detection via Automatic Gain Control (AGC),” Navigation - Journal of The Institute of Navigation, vol. 59, issue 4, pp. 281-290, 2012.

[10] MA Ke, SUN Xun, NIE Yuping. Research on key technologies of GPS generated spoofing [J]. Aerospace Electronic Warfare, 2014, 30(6): 24-26.

[11] Zhou Pengfei. Research on key technologies of GNSS/INS integrated navigation against deceptive interference [D]. National University of Defense Technology, 2015.

[12] Xue Wenting, Zhang Bo, Li Shijian, et al. A New Adaptive Kalman Filter Algorithm for Integrated Navigation [J]. Global Positioning System, 2014, 39(4): 8-11.