A Composite Detection Method for Direct GPS Deception Attack

Kunjun Hu and Yuanfeng Huang
School of Electronic and Information Engineering, Wuhan Institute of Technology, Wuhan 430200, China

*Corresponding author

Abstract: On account of the GPS initial technology limitations, it is vulnerable to interference, deception and other security attacks; GPS is widely used. If it is attacked, it will bring very serious consequences. Due to the problem of cost, civil GPS seldom considers how to defend against security attack. Therefore, it is necessary to study a fast and efficient GPS deception signal detection method to resist the attack. By improving the existing detection methods of GPS deception signal, a composite detection method of GPS deception signal is proposed. Based on DOA detection, the detection of signal propagation time difference is added, and the existence of GPS deception signal is judged synthetically according to whether the signal angle of arrival and the signal propagation time difference exceed the threshold value of real signal. The improved method improves the detection efficiency by reducing the calculation times of the signal angle of arrival. By reducing the number of detection signals to improve the detection accuracy of signal propagation time difference when there are more detection signals and less deception signals, thus ensuring the accuracy of composite detection. And subsequent simulation experiments successfully detected direct GPS deception signals, which verified the feasibility of this method for rapid detection of direct deception signals.

Keywords: Global positioning system (GPS); security attacks; location deception; deception signal detection.

1. Introduction

GPS is a global positioning system composed of 24 satellites, which can realize navigation and positioning functions at any point on the earth and at any time[1]. GPS is vulnerable to security attacks such as jamming and deception because of the limitations of its initial technology. In order to reduce the manufacturing cost, the existing civil GPS seldom considers how to defend against attacks. GPS is widely used, once it is attacked, the loss is hard to estimate.

The security problem of GPS has aroused widespread interest in academia. The common methods of GPS deception signal detection, including signal power attenuation detection, DOA (Direction Of Arrival) detection and the application fields of these detection methods, have been introduced in reference [2], but they have not been realized in detail. In reference [3], the space-time zero-adjustment technique is introduced to counteract GPS deception signals. Although it can counteract deception signals with high signal-to-noise ratio, it cannot counteract deception signals with low signal-to-noise ratio effectively. In reference [4], the signal attenuation method is used to detect GPS deception signals, but this method is susceptible to noise interference. In reference [5], the GPS deception signal is detected by satellite signal correlation, and the detection result is clear but the realization is complicated. In reference [6], the detection of propagation time difference and its application are introduced. The calculation efficiency is high, but the detection accuracy is low. The
The application of DOA technology in detecting GPS deception signals is introduced in reference [7]. The method has high detection accuracy, can determine the number of deception signals, and avoids the influence of noise and signal power, but the calculation is complicated and difficult to realize. In this paper, by improving single DOA detection, a composite detection method is proposed: some signals are detected by DOA, and the remaining signals are detected by propagation time difference. The existence of GPS deception signal is judged synthetically according to whether the signal angle of arrival and the signal propagation time difference exceed the threshold value of real signal. On the premise of ensuring accuracy, the composite detection method takes less time and has higher detection efficiency than the single DOA detection method. Compared with the detection of signal propagation time difference, the detection accuracy is higher when the number of detection signals is larger and the number of deception signals is smaller.

2. Principle of DOA and Signal Propagation Time Difference Detection

The composite detection method is based on DOA detection and the propagation time difference detection is added. The principle of the two signal detection methods is introduced briefly.

2.1. DOA Principle

DOA means direction of arrival estimation of signals, and its common methods include: AOA (Angle Of Arrival), TOA (Time Of Arrival), FDOA (Frequency Difference Of Arrival), and so on [8]. The basic model is shown in Figure 1: In a three-dimensional spatial coordinate system, point A is the coordinate origin, and N array antennas with a spacing of \(x_d\) are arranged on the x-axis. Assume that the signal source located at B\((x, y, z)\) emits a signal incident on A in a direction of incidence of \((\varphi, \theta)\). The angle of arrival \(\theta\) represents the angle between the positioning signal and the projection of point A on the \(xoy\) plane, the azimuth angle \(\varphi\) represents the angle between the projection of the angle of arrival \(\theta\) on the \(xoy\) plane and the \(x\)-axis, and the zenith angle \(\alpha\) represents the remainder of the angle of arrival \(\theta\).

Assuming that the direction of the signal is constant and that the noise is white noise unrelated to the signal during signal reception, after receiving \(N\) signals, a MUSIC algorithm is adopt to construct that signal correlation matrix \(R\), and according to the orthogonality of signal subspace and noise subspace, \(R\) is decomposed into eigenvalues, \(N\) different eigenvalues and eigenvectors are obtained, then the signal matrix \(G\) is composed of eigenvectors corresponding to the first \(D\) larger eigenvalues equal to the number of signals obtained. The azimuth angle \(\varphi\) is calculated according to the formula:

\[
P_{MUSIC}(\theta) = \left(\| E^H_n a(\theta) \| \right)^{-1} = \left(\| G^H_n a(\theta) \| \right)^{-1}, \quad a(\theta) = [1, e^{-j\varphi}, e^{-j2\varphi}, \ldots, e^{-j(N-1)\varphi}],
\]

In which \(a(\theta)\) is the direction matrix of the signal matrix \(G\) and \(e^{-j(N-1)\varphi}\) is the phase difference generated when the same signal is received by different array antennas, and the signal arrival angle \(\theta\) is calculated according to the geometric relationship between \(\varphi\) and \(\theta\)[9].

![Figure 1. Schematic diagram of DOA model.](image)

2.2. Principle of Signal Propagation Time Difference

As shown in Figure 2, that basic principle of the signal propagation time difference is as follow: point \(A\) is a GPS satellite, point \(B\) is a requesting end, point \(C\) is an authenticate end, and the distance...
between BC is l (known). Assuming that both points B and C are positioned by GPS, according to GPS positioning formula: 
\[ \rho_i = c \cdot t = [(x_i - x)^2 + (y_i - y)^2 + (z_i - z)^2]^\frac{1}{2} + c \cdot \tau_i, \ i = \{1,2,3,4\} \]
where \( \rho_i \) is pseudo-range, \( c \) is speed of light, \( t \) is signal propagation time, \((x_i, y_i, z_i)\) is satellite position coordinate, \((x, y, z)\) is target position coordinate, \( \tau_i \) is time deviation between satellite clock and target point; 
\[ t = \rho_i c^{-1} = c^{-1} \left\{ [(x_i - x)^2 + (y_i - y)^2 + (z_i - z)^2]^\frac{1}{2} + c \cdot \tau_i \right\}, \ i = \{1,2,3,4\} \]
according to the satellite coordinates received by the B point antenna array and the position coordinates of the C point, the difference value \( \Delta t \) between the signal propagation time of AB and the signal propagation time of AC is obtained after calculation[10].

Figure 2. Schematic diagram for principle of signal propagation time difference.

3. Improved GPS Deception Signal Detection Method

Single DOA has high detection accuracy and can determine the number of deceptive signals, but the calculation is complicated and the detection efficiency is low. The detection efficiency of DOA can be improved by reducing the number of detection signals, but the number of deception signals cannot be determined because of missing deception signals, which reduces the detection accuracy. The calculation of propagation time difference detection is simple, and the detection efficiency is high, but the number of deceptive signals cannot be detected. What is more, because the time difference of signal propagation is obtained by weighted average of satellite positioning coordinates and positioning formulas, and the deception signal occupies a relatively low proportion in the detection signal when the number of detection signals is large and the number of deception signals is small, the influence is small and the accuracy is low. In order to improve the efficiency of DOA detection and ensure its accuracy, a composite detection method is proposed. Based on the DOA detection of some signals, the propagation time difference of the remaining signals is detected, and the existence of GPS deception signal is judged comprehensively according to whether the angle of arrival and the propagation time difference of the signals exceed the threshold value of the real signals. After the two methods are combined, the efficiency of composite detection is improved by reducing the calculation times of signal angle of arrival. Moreover, due to the addition of signal transmission time difference detection, the deception signal which may be stored in the remain signal is not omitted. At the same time, because the number of detection signals is reduced, the accuracy of signal propagation time difference detection is improved when the detection signals are more and the deception signals are less, which ensuring the accuracy of complex detection. In the case of no need to give the number of detection deception signals, the composite detection method can quickly detect the existence of GPS deception signals, with good feasibility and practicability.

3.1. Steps of Composite Detection Method

After receiving \( m \) \( (m \geq 8) \) satellite signals, the array antenna randomly selects 4 signals to calculate the angle of arrival \( \theta \), and the propagation time difference \( \Delta t \) is calculated by residual signal; the existence of GPS deception signal is judged by the values of the angle of arrival and the propagation time difference. The threshold range of the real signal angle of arrival is \( \theta \in (5^\circ, 90^\circ) \)[11], and the propagation time difference between two points at a distance of 30m is less than 0.1ms[12]. Thus, the
deception signal angle of arrival $\theta e(0^\circ,5^\circ)$, and the propagation time difference is greater than 0.1\textit{ms}.

The existence of deception signal can be determined when the detection result satisfies the signal angle of arrival $\theta e(0^\circ,5^\circ)$ or the propagation time difference is greater than 0.1\textit{ms}.

3.1.1. Calculate the signal arrival angle
(1) $m(m\geq4)$ satellite signals were received by $n(n\geq10)$ array antennas in the form of $x = As + n$ three-dimensional space signals; Let the angle between the signal of a satellite and the $x, y$ axes be $\Phi_1, \Phi_2$ when it reaches the target point, and construct three signal sub matrices:

$$X = AS + n_1, Y = A\Phi_1 S + n_2, Z = A\Phi_2 S + n_3;$$

Where $X = [x_1(t), x_2(t), \cdots, x_n(t)]^T$, and $Y, Z$ are similar, are matrices of order $1*n$;

(2) Let $R_{XX} = E(XX^H) = AR_S A^H + \sigma^2 I$, $\sigma^2 I$ be noise matrices, $R_{XY} \sim R_{ZZ}$ can be obtained in the same way, and let $C_{XX} = R_{XX} - \sigma^2 I = AR_S A^H$, $C_{XY} \sim C_{ZZ}$, $R_{XX} \sim R_{ZZ}$ and $C_{XX} \sim C_{ZZ}$ can be obtained in the same way that they are all matrices of order $1*n$;

(3) The matrix $C = [C_{xx} \ C_{xy} \ C_{xz}]$ of order $2*3n$ is composed by $C_{xx} \sim C_{zz}$, and its subspace $U_S = [U_1 \ U_2 \ U_3]$ is obtained by eigenvalue decomposition of the matrix $C$, in which $U_2 = U_1, U_3 = U_1, U_2$, and $\Phi_1, \Phi_2$ can be obtained;

(4) Let the angle of arrival be $\theta$ and the azimuth angle be $\phi$. From the mathematical relation, we can know that the angle of arrival $\theta$ and the azimuth angle $\phi$ can be obtained by the simultaneous solution of $\cos \Phi_1 = \cos \theta \ast \cos \phi, \cos \Phi_2 = \cos \theta \ast \sin \phi$.

3.1.2. Calculate the signal propagation time difference
(1) Locating the target point, receiving $m(m\geq4)$ sets of satellite spatial position coordinate signals by the array antenna, and forming $m$ sets of signals into an $m*3$ order multi-satellite position matrix; (2) A specific location coordinate $(x_0, y_0, z_0)$ is received after the authentication point is located $l$ meters away;

(3) According to GPS basic positioning formula:

$$\rho_i = [(x_1 - x)^2 + (y_1 - y)^2 + (z_1 - z)^2]^{\frac{1}{2}} + c\tau_i, i = \{1,2,3,4\}$$

By introducing the multi-satellite position matrix into the formula above, and then combining the equations, a nonlinear equation group $F(X)$ with $m$ equations can be obtained.

$$F(X) = e^{-1} \left[ [(x_1 - x)^2 + (y_1 - y)^2 + (z_1 - z)^2]^{\frac{1}{2}} + c(\tau_1 + \Delta t) \right] ;$$

$$[(x_m - x)^2 + (y_m - y)^2 + (z_m - z)^2]^{\frac{1}{2}} + c(\tau_m + \Delta t)].$$

(4) Let $F(X) = 0$, $\dot{F}(X) = 0$, and calculate by Newton iteration method, in which the number of iterations is $3m$, so the output of calculation result is $X_1 = [x \ y \ z \ \tau_1]$, and the position coordinate of the target point $(x, y, z$ and the time deviation $\tau_i$ between the satellite clock and the target point can be obtained;

(5) The target point position coordinate $(x, y, z)$ and the authentication point position coordinate $(x_0, y_0, z_0)$ are brought into the equation

$$\tilde{e}_s = \sum_{i=1}^{n} \rho_i cn^{-1} = \sum_{i=1}^{n} cn^{-1} \left( [(x_1 - x)^2 + (y_1 - y)^2 + (z_1 - z)^2]^{\frac{1}{2}} + c\tau_1 \right), s = 1,2,$$

Respectively, and the result $\tilde{e}_1, \tilde{e}_2$ can be obtained. If the propagation time difference between the two points is $\Delta \tau_1$, then $\Delta \tau_1 = \tilde{e}_1 - \tilde{e}_2$.

3.2. Efficiency Analysis of Composite Detection
Assuming that the number of signals received by $n(n\geq10)$ array antennas is $m(m\geq4)$, DOA detection requires $[6n(n+1)]$ additions and $[6n(n+1)]$ multiplications for calculating the angle of arrival $\theta$ of a
satellite signal, and $6n$ multiplications for calculating the intermediate matrix $R_{XX} \sim R_{ZZ}$; $6n$ subtraction operations are required to compute that intermediate matrix $C_{XX} \sim C_{ZZ}$; $6n^2$ multiplication and $6n^2$ additions are required to calculate that angle of arrival $\theta$ by the numerical matrix $C$. And it requires $12m$ addition operations and $m$ multiplication operations to calculate the propagation time difference of $m$ ($m \geq 4$) satellite signals by Newton iteration method and arithmetic mean value when the number of iterations is $3m$.

4 times of angle of arrival calculation and $(m-4)$ times of propagation time difference calculation are needed for $m(m \geq 8)$ satellite signals to pass the composite detection, and a total of $[24n(n+1)+12(m-4)]$ addition operations and $[24n(n+1)+m(m-4)]$ multiplication operations are needed. $[6mn (n+1)]$ addition and subtraction operations and $[6mn (n+1)]$ multiplication operations are requiring for a single DOA detection.

Let the time of one addition be $a$ $s$, the time of one multiplication be $b$ $s$, the time of single DOA detecting $m$ satellite signals be $t_3= [6mn(n+1)(a+b)]$ $s$ and the time of composite detecting $m$ satellite signals be $t_4= [24an(n+1)+12a(m-4)+24bn(n+1)+bm(m-4)]$ $s$, then the calculated time difference between the two methods is $\Delta t_2= [6a(m-4)(n-1)+b(m-4)(6n^2+6n+m)]$ $s$, and $\Delta t_2>0$ in the case of the number of signals $m \geq 8$ and the number of antenna arrays $n \geq 10$, as well as $a>0, b>0$; Therefore, compared with the single DOA detection method, the composite detection method takes less time and has higher efficiency.

3.3. Result Judgment
After the composite detection, it is judged whether there is deception signal or not according to the difference of signal angle of arrival and propagation time. The possible results are as follows:
1) If the result of DOA detection accords with the threshold range of deception signal, the existence of deception signal can be determined regardless of the propagation time difference;
2) The result of DOA detection accords with the threshold range of the real signal, the difference of propagation time accords with the threshold range of the deception signal, and the existence of the deception signal can be determined;
3) If the results of DOA detection and propagation time difference both accord to the threshold range of the real signal, it can be determined that there is no deception signal.

4. Realization of GPS Direct Deception Signal Composite Detection

4.1. Simulation Detection
The GPS deception signal composite detection method is simulated under the condition of constructing deception signal transmitter and successfully direct locating deception. The steps are as follows:
1) Locate the authentication point 30 $m$ away to obtain the location coordinates;
2) Turn on the deception signal transmitting source and transmit the deception signals, wherein the signal sampling frequency is 10MHz, the antenna array is a uniform linear array, and the array spacing is half of the wavelength of the GPS (C/A) signal; The number of GPS signals received by the target antenna array is shown in Figure 3.

![Figure 3. Schematic diagram of satellite signals received by array antenna.](image)
(3) The received signals are subjected to composite detection, 4 received signals are randomly selected for DOA detection, and the remaining signals are subjected to signal propagation time difference detection, as shown in Figure 4: the horizontal axis is the zenith angle $\alpha$ (the residual angle of the angle of arrival $\theta$), and the vertical axis is the azimuth angle $\phi$. The zenith angle and arrival angle of the 4 signals detected by DOA are between $30^\circ$-$70^\circ$ and $20^\circ$-$60^\circ$, respectively, and the propagation time difference of the remaining signals is $0.643ms$. The zenith angle of the 4 signals detected by DOA is between $80^\circ$-$90^\circ$, the angle of arrival is between $0^\circ$-$5^\circ$, and the propagation time difference of the remaining signals is $0.042ms$. In the 4 signals detected by DOA in the right figure, the zenith angle of 2 signals is between $30^\circ$-$50^\circ$, the angle of arrival is between $40^\circ$-$60^\circ$, and the zenith angle of another 2 signals is between $80^\circ$-$90^\circ$, the angle of arrival is between $0^\circ$-$5^\circ$, and the propagation time difference of the remaining signals is $0.246ms$. Repeated experiments were carried out to eliminate accidental errors, and the time of 20 successful experiments was $0.81s$.

(4) The received signal is detected by single DOA, as shown in Figure 5: the horizontal axis is zenith angle $\alpha$ (residual angle of arrival angle $\theta$), the vertical axis is azimuth angle $\phi$, and as shown, the zenith angle of most signals is between $30^\circ$-$70^\circ$ the angle of arrival is between $20^\circ$-$60^\circ$, the zenith angle of about 4 signals is between $80^\circ$-$90^\circ$, and the angle of arrival is between $0^\circ$-$5^\circ$. Repeated experiments were carried out to eliminate accidental errors, and the time of 20 successful experiments was $0.88s$.

(5) Set up the deception signal source to transmit different number of deception signals, and carry out single propagation time difference detection and composite detection on all received signals respectively. When the DOA detection in the composite detection is all real signals, the comparison results of the single propagation time difference detection are shown in Table 1: When the number of deceptive signals is 1, the detection result of single propagation time difference is $0.083ms$, and the propagation time difference of residual signals is $0.114ms$ under the composite detection. When the number of deceptive signals is 2, the detection result of single propagation time difference is $0.148ms$, and the propagation time difference of residual signals is $0.295ms$ under composite detection. When the number of deceptive signals is 3, the detection result of single propagation time difference is $0.233ms$, and the propagation time difference of residual signals is $0.475ms$ under composite detection. When the number of deceptive signals is 4, the detection result of single propagation time difference is
0.331 ms, and the propagation time difference of residual signals is 0.643 ms under the composite detection.

Table 1. Comparison of single propagation time difference detection and composite propagation time difference detection for different deceptive signal numbers

| Number of deceptive signals | 1       | 2       | 3       | 4       |
|-----------------------------|---------|---------|---------|---------|
| Single propagation time difference detection results/s | 8.323e-5 | 1.485e-4 | 2.332e-4 | 3.315e-4 |
| Propagation time difference detection results under composite detection/s | 1.142e-4 | 2.955e-4 | 4.758e-4 | 6.432e-4 |

4.2. Result Analysis

The composite detection results are shown in Figure 4: In the detection of DOA in the left figure, the value of the signal angle of arrival accords with the threshold range of the normal signal, and the propagation time difference also accords with the threshold range of the deceptive signal, which indicates that there is a deceptive signal in the remaining signal; In the detection of DOA in the middle figure, the value of the signal angle of arrival accords with the threshold range of the deceptive signal, and the difference of the propagation time also accords with the threshold range of the normal signal, which indicates that the deceptive signal exists in the signal detected by the DOA; In the DOA detection in the right figure, the values of the angle of arrival and the propagation time difference of the signal are all accord with the threshold range of the deception signal, which indicates that the deceptive signal exists in both the signal detected by the DOA and the remaining signal, and the deceptive signal can be detected by the above three results. In the case of repeated tests to eliminate accidental errors, the average calculation time of the composite detection method is 0.040 s/time.

Single DOA detection results are shown in Figure 5: Among the 16 signals detected, 12 signals' angle of arrival values conform to the threshold range of normal signals, 4 signals' angle of arrival values conform to the threshold range of deceptive signals, which indicates that deception signal exists and the number is 4. Under the condition of eliminating accidental errors by repeated tests, the average calculation time of single DOA detection is 0.043 s/time.

When different numbers of deceptive signals are transmitted, the detection results of the propagation time difference of the remaining signals under the single propagation time difference detection and the composite detection are as shown in Table 1. When the number of deception signals is not less than 2, the detection results of the composite detection and the single propagation time difference are both in accordance with the deceptive signal threshold range and the deception signal can be detected. When the number of deceptive signals is less than 2, the detection result of single propagation time difference is in accordance with the threshold range of normal signal, and the deceptive signal cannot be detected; when the composite detection is performed, the value of the angle of arrival conforms to the threshold range of the normal signal, but the detection result of the propagation time difference of the remaining signal after the number of the detection signals is reduced conforms to the threshold range of the deceptive signal, and the deceptive signal can still be detected.

According to the experimental results, GPS deceptive signals can be detected by both composite detection and single DOA detection, and the number of deceptive signals can be determined by single DOA detection. When the number of deceptive signals is less than 2, the deceptive signal cannot be detected by single propagation time difference detection, but can still be detected by composite detection, with higher accuracy. Compared with single DOA detection, the computational efficiency of composite detection is improved by about 8%. It can be seen that the composite detection can quickly detect the existence of deceptive signals while ensuring the accuracy, and has a higher feasibility when the number of deceptive signals is not required to be detected.

5. Conclusion

In this paper, a direct GPS positioning deception composite detection method is proposed. On the
basis of DOA detection, the detection of signal propagation time difference is added, and the existence of deceptive signal is judged by the numerical value of signal angle of arrival and signal propagation time difference. Composite detection not only ensures the accuracy but also improves the detection efficiency of a single DOA, and also improves the accuracy of signal propagation time difference detection when the number of detection signals is large and the number of deception signals is small. The simulation results show that the GPS deceptive signal can be detected in the case of successful direct positioning deception, and the feasibility of this method is verified. When the number of deception signals is not required to be detected, the composite detection can quickly detect deceptive signals, which lay a foundation for the subsequent counterattack of GPS positioning deception and improve the security of GPS.

References
[1] Elliott D. Kaplan. Principle and Application of GPS [M]. 2007.
[2] Lv Dengkui, Zhang Yingjie. A space-time frequency domain based on the GPS anti-jamming technology [J]. Electronic design engineering, 2019, 27(1):94-98.
[3] LV D K, ZHANG Y J. A space-time frequency domain based on the GPS anti-jamming technology [J]. Electronic design engineering, 2019, 27(1):94-98.
[4] Li M, Kou Y, Yong X, et al. Design and Field Test of a GPS Spoofer for UAV Trajectory Manipulation[C]// Proceedings of the 9th China Satellite Navigation Annual Conference--S03 Satellite Navigation Signals and Anti-jamming Techniques. 2018.
[5] Li Yabin, Guo Chengjun, Tian Zhong. Research on GPS anti-deception based on zero adjustment technology [J]. Electronics Optics & Control, 2017(01):41-44+99.
[6] LI Y B, GUO C J,TIAN Z. Research on GPS anti-deception based on zero adjustment technology [J]. Electronics Optics & Control, 2017(01):41-44+99.
[7] Song Huiliang. Anti-jamming technology of GPS satellite positioning [J]. Telecom World, 2018, No.335(4):249-250
[8] SONG H L. Anti-jamming technology of GPS satellite positioning [J]. Telecom World, 2018, No.335(4):249-250
[9] Based on the improved study on the method of spread spectrum technology of GPS anti-interference [D]. Xidian University, 2018
[10] Based on the improved study on the method of spread spectrum technology of GPS anti-interference [D]. Xidian University, 2018
[11] Milaat F A, Hang L. Decentralized Detection of GPS Deception in Vehicular Ad Hoc Networks [J]. IEEE Communications Letters, 2018, PP(99):1-1. [8] hafiee E, Mosavi M R, Moazedi M. Detection of Deception Attack using Machine Learning based on Multi-Layer Neural Network in Single-Frequency GPS Receivers[J]. Journal of Navigation, 2017, 71(1):1-20.
[12] Kai J, Schäfer M, Moser D, et al. Crowd-GPS-Sec: Leveraging Crowd Sourcing to Detect and Localize GPS Deception Attacks[C]// 2018:1018-1031.
[13] Chang H K, Sun Y K, Chan G P. Adaptive complex-EKF-based DOA estimation for GPS deception detection[J]. Iet Signal Processing, 2018, 12(2):174-181.
[14] Shi Wensen, Zhu Hai, Cai Peng. GPS deception signal identification based on received signal DOA estimation [J]. Ship Science and Technology, 2013, 35(4):111-116.
[15] SHI W S, ZHU H, CAI P, GPS deception signal identification based on received signal DOA estimation [J]. Ship Science and Technology, 2013, 35(4):111-116.
[16] Dai Weihao, Xu Rui, Liu Jiany, et al. The GNSS and forwarded to cheat system based on software simulation [J]. Navigation and control, 2017, 16 (5).
[17] DAI WH, XU R, LIU J Y, et al. The GNSS and forwarded to cheat system based on software simulation [J]. Navigation and control, 2017, 16 (5).
[18] Chen Liang, Meixia Miao, Jianfeng Ma,Hongyan Yan, Qun Zhang, Xinghua Li, Teng Li."Chapter 10 Detection of GPS Spoofing Attack on Unmanned Aerial Vehicle System", Springer Science and Business Media LLC, 2019