Overview of spoofing interference detection in satellite navigation

Xuran Gu[a], Ling Xi[*a,b,c]
[a]School of Electronics and Information, Zhengzhou University of Aeronautics, Zhengzhou 450046, Henan, China; [b]Henan Key Laboratory of General Aviation Technology, Zhengzhou 450046, Henan, China; [c]Collaborative Innovation Center of Aeronautics and Astronautics Electronic Information Technology, Zhengzhou 450046, Henan, China

ABSTRACT

With the development of UAV and autonomous driving technology, the accurate acquisition of spatial location information is more and more closely related to people's production and life. However, because the navigation signal is very weak when it reaches the ground, the signal is vulnerable to interference, and human interference has a destructive effect on navigation applications. Human interference to navigation signals can be divided into two categories: suppression interference and deception interference. This paper first briefly introduces the difference between spoofing and squishing jamming and the types of spoofing jamming, and then analyzes spoofing jamming detection technology and its research status from the perspectives of message encryption identity authentication, spatial processing, signal power detection, signal quality detection, Doppler shift consistency, positioning and navigation results and machine learning. The research direction of multi-technology comprehensive detection is prospected.

Keywords: Global navigation satellite system, deceptive interference, deceptive interference detection

1. INTRODUCTION

Global Navigation Satellite System (GNSS) is a system that uses satellites to provide accurate position information for receivers on the ground, at sea or in the air. The current GNSS includes the Global Positioning System (GPS) of the United States, the GLONASS navigation system of Russia, the Galileo navigation system of Europe, and the Beidou navigation satellite system of China.

GNSS is widely used in human military activities, production activities and to provide positioning services for People's Daily life. However, due to the influence of various factors, the landing power of navigation signal is weak, and the signal receiving process is prone to human interference. Jamming to navigation signals is divided into two categories: suppression jamming and deception jamming. Compared with suppression jamming, deception jamming has more subjective purpose and stronger breaking ability. Since Iran successfully captured the US stealth unmanned reconnaissance aircraft RQ-170 in 2011 by using navigation spoofing, there have been many successful cases of actual spoofing. These events have pushed the navigation signal spoofing detection to the research center. In order to obtain reliable navigation and positioning services, people began to study the detection methods of navigation spoofing[1].

2. JAMMING TECHNOLOGY

Human interference of navigation signals mainly falls into two categories: suppression interference and deception interference, as shown in Figure 1. Suppression jamming is a high-power noise signal to suppress the real signal, affecting the receiver so that it cannot detect the real echo signal, so that the receiver loop is out of lock and cannot be located normally. At present, there are relatively mature technologies in the world to detect and suppress the influence of compression interference, such as adaptive space-time filtering and array antenna technology[2]. The principle of spoofing is to forward the real navigation satellite signal or generate a spoofing signal highly similar to the real signal, so that the target receiver can receive the false signal and solve the wrong position or time information. Deception jamming is more intelligent, more purposeful and has a stronger jamming effect than compression jamming, so it is also more threatening.

*21144755@qq.com

International Conference on Optics, Electronics, and Communication Engineering (OECE 2024), edited by Yang Yue, Proc. of SPIE Vol. 13395, 133954Q · © 2024 SPIE · 0277-786X · Published under a Creative Commons Attribution CC-BY 3.0 License · doi: 10.1117/12.3048229

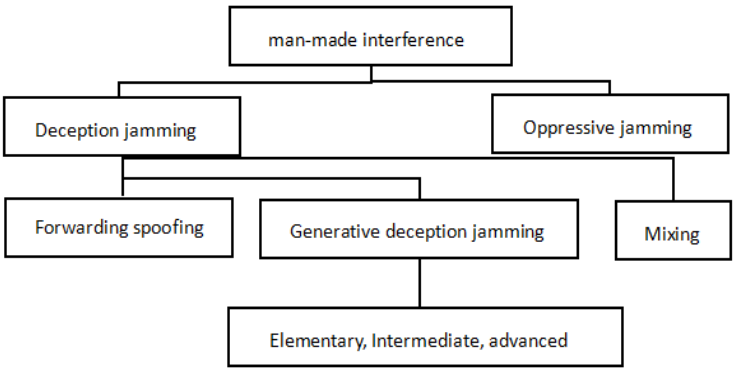

Figure 1. Human disturbance classification.

Spoofing can be divided into generative spoofing and forwarding spoofing according to the different ways of spoofing signal generation. According to the real satellite signal format, the generated spoofing system forges the spoofing signal that is similar to the real signal, and the actively generated position information is compiled into the navigation message and then sent to the target, so that the receiver can receive the wrong position navigation signal. As shown in Figure 2.

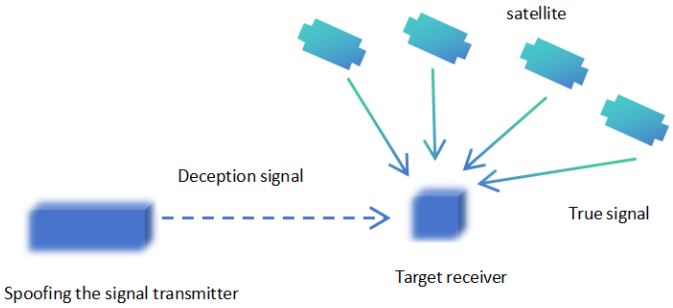

Figure 2. Generative deception jamming model.

2.1 Generative deception jamming

Generative deception jamming includes elementary, intermediate and advanced deception jamming. The primary spoofing jamming uses a strong enough signal power to affect the channel signal quality, resulting in the receiver's capture performance decline or tracking loop lock-out. In the receiver recapture stage, spoofing signals with higher power and better signal quality are captured to achieve the purpose of spoofing. Intermediate spoofing technology not only generates spoofing signals, but also receives real satellite signals and estimates parameters to keep the generated spoofing signals consistent with real signal parameters, the most important of which is to maintain the consistency of code phase and carrier frequency between the two, so as to improve anti-detection performance. The implementation of intermediate deception is more complicated than that of elementary deception, but its concealment is stronger. The current intermediate deception technology mainly relies on the way of transmitting multiple satellite signals from a single antenna, but there is still a big difference between the incoming wave direction of the signal and the real scene. Advanced deception technology uses multi-device simulation to build the distribution scene of real satellites to achieve the purpose of dynamically deceiving target receivers, which is the most expensive, the most complex implementation process, but the most effective deception method at present.

2.2 Forwarding spoofing

Forwarding spoofing is to deceive the target receiver by receiving and forwarding real satellite signals. The spoofing principle is that the spoofing device first receives the real satellite signal, and then transmits it through the transmitting antenna after proper delay and power amplification, so that the target receiver receives the false pseudo distance, and then changes the position calculated by the receiver, as shown in Figure 3. This method is not limited by military code encryption, and can be applied to spoofing military signals with relatively low implementation cost.

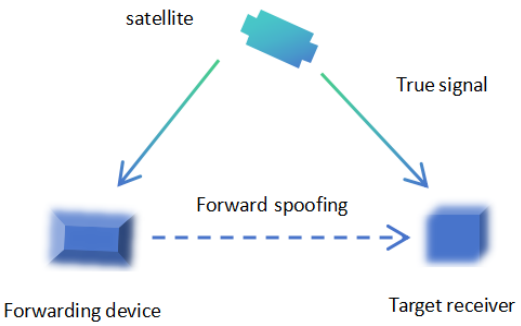

Figure 3. Forwarding spoofing model.

3. RESEARCH ON DECEPTION INTERFERENCE DETECTION

Spoofing interference detection based on message encryption authentication

The technology in the receiver is mainly to complete the identity authentication work, so according to the implementation of the message encryption technology in the receiver, the message encryption technology can be mainly divided into four categories: navigation information authentication (NMA), spread spectrum code authentication (SCA), navigation information encryption (NME), spread spectrum code encryption (SCE).

The NMA is to protect the bit of navigation data and digitally sign the navigation data. The receiver uses the signature for identity authentication. The SCA is to insert an unpredictable chip into an unencrypted open spread spectrum code, and the receiver verifies the validity of the unpredictable chip in the received sequence by encrypting the algorithm. The NME technology first encrypts the navigation data, and then transmits it on the spread spectrum code. SCE encrypts the spread spectrum codes of all satellites before launching them. Compared to the two authentication-based technologies, NME and SCE require a more complex receiver architecture due to the need to manage operations such as keys. Therefore, SCA and NMA are more feasible for detecting spoofing interference[3].

3.2 Spoofing detection based on signal power

In order for the receiver to lock on to the spoofing signal, the power of the signal transmitted by the spoofing device is generally higher than the power of the actual satellite signal. Therefore, the absolute power, carrier-to-noise ratio and power ratio of navigation signals in different bands can be detected to determine whether there is deception. These methods are easy to implement and do not require additional hardware support.

3.2.1 Absolute power detection. Spoofing signals are detected by detecting whether the absolute power received is much greater than the threshold set for the true power of the satellite signal. Because the path loss between the spoofing jammer and the target receiver is difficult to estimate, it is difficult to apply the transmit power required for sufficient signal strength to the target receiver without overdoing the power of the real GPS signal. Therefore, receiving a spoofing signal whose absolute power is much higher than the expected real GPS signal power is a simple and direct way to detect spoofing attacks. However, if only the absolute power of the signal is detected, the alarm leakage rate will be very high, which will affect the detection effect.

3.2.2 Carry/noise ratio. C/N0 ratio is an important parameter to evaluate signal quality. Detection of deception by means of carrier-to-noise ratio is easy to detect and does not require major changes to the receiver. When a high-power spoofing signal attacks a GPS receiver, the C/N0 received by the receiver may suddenly change. Therefore, the receiver can detect the change of carrier-to-noise ratio in real time to find the abnormal change that may be the sign of attack, so as to find whether there is spoofing interference signal. A deception detection algorithm based on carrier-to-noise ratio was proposed in Reference[4]. It is proved that this method can successfully detect high-power dominance deception interference, and the detection probability can reach 95% when the false alarm rate is 0.1%. However, this method is no longer reliable for spoofing interference with power matching. Reference[5] proposed the Automatic Gain Control (AGC), C/N0 and position information of the output of the joint receiver to realize the detection and recognition of weak suppression interference and spoofting interference of satellite navigation. The detection rate of this method can reach 96%. The comparison of signal strength detection methods is shown in Table 1.

Table 1. Comparison of signal strength detection methods.

Detection method	Advantage	Disadvantage
Absolute power	Only a few circuit modifications are required	Not suitable for stepwise pull off spoofing and multipath effect detection
Carrier to noise ratio	No major changes to the receiver	Power matching spoofing is not applicable

3.3 Spoofing interference detection based on spatial processing

Usually the navigation spoofing signal comes from the same spoofing jammer, so all satellite signals are consistent, and the real navigation signal comes from different satellites, from all directions, so it can be determined whether there is spoofing interference by detecting the signal, because the space information is difficult to be imitated, so this method is one of the most effective detection methods.

Huang et al.[6] proposed a two-antenna spoofed interference detection method, which can only be applied to navigation receivers with fixed antennas. In order to solve this problem, Zhang[7] proposed a detection scheme based on rotating double antennas, and the results show that the detection method has relatively excellent performance under the same antenna spacing and short data length.

In Reference[8], Chen et al. proposed a joint pose fixing and deception detection method using three antennas. By using three non-collinear antennas, the signal orientation can be uniquely determined, which greatly reduces the detection blind area and improves the overall detection rate. And no additional equipment such as inertial navigation to provide attitude information, the cost is relatively low.

Reference[9] proposes a spoofing detection and suppression method for satellite navigation based on array antenna. The algorithm can adjust the array parameters adaptively according to the change of external interference environment to achieve the best interference suppression effect. In Reference[10], a deception detection technique based on array antenna satellite and DoA estimation is proposed. Compressed sensing Orthogonal Matching Pursuit (OMP) methods are used to process received signals, which has a relatively good detection effect even with a small number of samples. And it is suitable for the scene with high real-time performance.

Antenna arrays can also be adapted to multipath situations. Reference[11] proposes an anti-spoofing method using antenna array in multi-path environment. This method estimates spoofing channel coefficient by using spatial processing and time-domain processing methods, according to which zero trap can be set to invalidate spoofing signals and multipath signals. Because the method is executed before the descaling, the processing complexity is significantly reduced, and the array calibration is not required, so it has important application prospects.

These methods are all based on array antenna spoofing detection and suppression technology of satellite navigation, they use different means and methods to identify and suppress spoofing interference, improve the accuracy and reliability of navigation. Each method has its unique advantages and application scenarios, and the appropriate method can be selected according to the specific application requirements. The comparison of detection methods based on spatial processing is shown in Table 2.

Table 2. Comparison of detection methods based on spatial processing.

Number of antennas	Advantage	Disadvantage
Double antenna	Wide range of application; more flexible	The antenna needs to be modified
Three-antenna	High detection accuracy; good reliability	Deployment and maintenance are relatively complex; computationally complex
Array antenna	More accurate detection	High cost; calculation load

3.4 Deception detection based on Doppler consistency

The Doppler shift is caused by the interaction between the satellite and the receiver. After the navigation signal passes through the ionosphere, the carrier Doppler shift and the pseudo-code Doppler shift should be consistent, that is, the ratio of the two frequencies should be a constant. However, spoofing signals often cannot keep the consistency of these two

parameters, so spoofing can be detected by detecting the consistency of the two parameters. In Reference[12], two methods, Power Transmission Detection (PTD) and Doppler Offset Detection (DOD), were integrated to improve the detection performance and enhance the robustness of detection.

3.5 Based on signal quality detection technology

Signal Quality Monitoring (SQM) is based on the detection of spoof interference signals interacting with real satellite signals, resulting in tracking phase-dependent peak distortion. SQM generally monitors the possible distortion and anomaly of the signal correlation peak by detecting the asymmetry of the correlation peak or the abnormal sharpness and flatness of the correlation peak. The corresponding detection algorithms are slope (Delta) algorithm and increment (Ratio) algorithm[13]. Wang et al. proposed a spoofing detection method that detects the change of composite SQM index in the code tracking ring[14]. In this method, the composite SQM algorithm can detect spoofing in a shorter time than the Ratio algorithm, which verifies the complementarity of ELP (Early-Late Phase) algorithm and Ratio algorithm. Without increasing the complexity of the algorithm, the algorithm greatly improves the detection performance.

Traditional SQM technology can not solve the problem when dealing with multipath effects, and multipath interference may cause false alarms in the deception detection algorithm based on SQM. Reference[15] proposed a multi-star joint deception detection algorithm based on Slope at Cutoff Score (SCS) of S-curve. The results show that the proposed algorithm not only deals with multi-path effect effectively, but also has better deception detection performance than traditional SQM algorithm, and has strong robustness to multi-path interference.

3.6 Spoofing interference detection based on location navigation results

It is also one of the research directions of spoof-detection to compare the data from GNSS receiver with the data from other high-precision auxiliary equipment. By using high-precision devices that are not affected by electromagnetic, such as the Inertial Navigation System (INS), Chat-level Atomic Clock, and Accelerometer, we compare the measured data with the final calculation results of the receiver to determine whether there is fraud.

3.6.1 Inertial navigation system. INS is a navigation technology based on measuring the acceleration and angular velocity of an object to determine its position, speed and direction. Reference[16] analyzed the consistency relationship of pseudo-range and pseudo-range rate changes under the real signal and the spoofed signal from the inertial information of velocity and position, and constructed a time series model to realize signal discrimination. This method can not only detect single position deception or velocity deception, but also quickly detect induced deception under small positioning deviation, which is convenient for the carrier controller to take timely measures, and make up for the defect that the traditional method of single state assisted detection may have a high probability of missing detection. Moreover, the algorithm is based on the short-time error propagation relationship of INS, and has low requirements on inertial navigation equipment. It has strong application value in the field of navigation such as UAV confrontation.

3.6.2 Chip-scale atomic clock. Chip-Scale Atomic Clock products have the characteristics of small size, high stability, low power consumption, etc. These advantages also make it outstanding in spoofing interference detection. Reference[17] proposes a spoofing detection method for inertial/satellite integrated navigation system based on the assistance of chip-level atomic clock. Spoofing detection is carried out from the time dimension. By analyzing the influence of spoofing interference on receiver time, the spoofing mode of suppression before spoofing interference is analyzed, and the error distribution is predicted based on the clock difference under the real signal and spoofing signal. A cheat-detection model assisted by the atomic clock on chip is constructed. The clock difference prediction accuracy of the atomic clock on chip is more than one order of magnitude higher than the internal clock accuracy of the receiver, and it has good performance.

3.6.3 Accelerometer. Because of its good deviation stability, low cost and no electromagnetic interference, the accelerometer can be used as an auxiliary device in the detection of spoofed interference. Suppose that by comparing the accelerometer output to the estimated acceleration from the GPS output, the accelerometer can be used to detect GPS spoofing signals. By comparing the difference between the output information of accelerometer and that of GPS, Reference[18] can effectively detect the abnormal changes of acceleration parameters caused by deception interference.

Although these auxiliary equipments can play an important role in deception detection, there are many other factors to consider in practical applications. For the inertial navigation system, because it relies on the internal accelerometer and gyroscope to measure the motion state, after a long time of operation, the error may gradually accumulate, resulting in a decline in navigation accuracy. Although the chip atomic clock has the ability of high precision time measurement, its accuracy and stability may be affected by environmental factors such as temperature and electromagnetic interference, and its cost is more expensive. For acceleration, because its working principle involves the measurement of acceleration,

it is necessary to pay attention to avoid collision and falling during use, so as not to cause damage to the equipment or affect the measurement accuracy. At the same time, the accelerometer also needs regular calibration and maintenance to ensure its accuracy and reliability.

3.7 Deception interference detection based on machine learning

In recent years, machine learning has played an increasingly important role in information security, medicine, biology, financial markets, public transportation, manufacturing and many other industries and fields. Machine learning technology provides a powerful tool for deception interference detection, and overcomes the limitations of traditional methods. The detection models based on support vector machine and neural network are introduced below.

In the detection based on support vector machine, Lu et al.[19] proposed a multi-parameter spoofing interference detection algorithm combining cuckoo search algorithm and classification support vector machine. The fusion algorithm has stronger adaptability and robustness, and can maintain stable performance in complex interference environment. Fusion algorithm also has high realizability and scalability, which can be improved and optimized according to specific requirements to adapt to different application scenarios and requirements.

In the detection based on neural network, Reference[20] proposes a detection method based on convolutional neural network algorithm. The experimental results show that this method is effective and has high precision detection ability when the code phase difference between the spoofed signal and the real signal is more than 0.5 chip. Reference[21] proposes a supervised machine learning method based on BP neural network for deception interference detection. According to the result of receiver operation characteristic curve, the classification effect of this method reaches 83%. A Probabilistic Neural Network (PNN) based detection method was proposed in Reference[22]. Compared with some traditional neural networks, the learning process of this method is simpler, the training speed is faster, and it is very suitable for real-time processing. It has certain fault tolerance for noise and outliers of input data, and the number of neurons in each layer is relatively fixed, which makes it easier to implement in hardware.

Although machine learning has great potential in the field of detection, it still faces problems such as data dependency, model complexity and overfitting, interpretability and trustworthiness, real-time and computing resources, adversarial attack and robustness, and algorithm selection and tuning. Therefore, it is necessary to continuously study and improve, and formulate appropriate strategies and methods in combination with specific application scenarios, in order to achieve better results.

4. CURRENT SITUATION AND FUTURE TREND

scientists and researchers are working to improve the level of technology against spoofing interference to ensure the stable operation of critical infrastructure and military systems. Especially in the field of military research, some advanced countries are committed to improving the adaptability and anti-interference of the system to complex electronic battlefield situations.

The future spoofing detection technology will pay more attention to the fusion of multi-source information. By integrating data from satellites, radar, communications and other sensors, the system can more fully understand the current electromagnetic environment and make more accurate judgments. Further deepening the application of machine learning and artificial intelligence in spoofing detection enables the system to identify new spoofing patterns adaptively and improve real-time performance and accuracy. In the face of a globalized electromagnetic environment, international cooperation will be even more important. Only through continued innovation and cooperation will the international community be able to better protect critical infrastructure and military systems from deceptive interference.

5. CONCLUSIONS

In the face of the ever-evolving and complicated spoofing threat of Beidou navigation system, the research of spoofing detection technology is particularly urgent. In this paper, the present situation and development trend of navigation deception interference detection technology are deeply discussed, trying to provide some useful references for the research and practice in this field. At the same time, cross-disciplinary collaboration and experience sharing will also play a key role in dealing with complex deception scenarios.

ACKNOWLEDGEMENTS

This work was supported in part by Post graduate Education Reform and Quality Improvement Project of Henan Province, in part by Henan Key Laboratory of General Aviation Technology, in part by Henan Province Collaborative Innovation Center of Aeronautics and Astronautics Electronic Information Technology, in part by Henan Province Special and Urgent Subject Group of Aeronautical and Astronautical Intelligent Engineering.

REFERENCES

[1] Zhang, L., Zhang, C. and Gao, Y., "Satellite navigation spoofing and detection (I): Typical events and spoofing technology development," Journal of Navigation and Positioning, 9(3), 1-7 (2021).
[2] Zhang, Q., Xu, S., et al., "Research on countermeasures of spoofing jamming for satellite navigation and positioning," Aerospace Electronic Countermeasures, 39(02), 54-60 (2023).
[3] Shen, C. and Guo, C., "Research and evaluation of message encryption technology of satellite navigation signal," Global Positioning System, 43(03), 7-12 (2018).
[4] Deng, X., Lv, Z., et al., "Design of satellite navigation deception detection algorithm based on carrier-to-noise ratio," Journal of Navigation and Positioning, 10(02), 109-118 (2022).
[5] Jin, R., Guo, Y., Yang, H., et al., "GNSS weak interference detection and recognition technology based on navigation receiver," Global Positioning System, 47(06), 91-95 (2022).
[6] Huang, L., Yong, L., et al., "Anti-spooking method of satellite navigation Receiver using dual-antenna carrier phase difference technology," Journal of National University of Defense Technology, 38(4), 103-106 (2016).
[7] Zhang, X., Ding, C. and Chen, S., "Deception interference detection technology based on Double difference carrier phase of rotating double antennas," Navigation Positioning and Timing, 10(2), 32-38 (2023).
[8] Chen, J., Yuan, H., Xu, Y. and Yu, F., "Joint attitude determination and deception detection using three antennas," Journal of Beijing University of Aeronautics and Astronautics, 49(1), 128-137 (2023).
[9] Wang, X., Wu, S., Wang, Y. and Zheng, C., "A spoofing detection and suppression method for satellite navigation based on array antenna," Modern Navigation, 13(3), 163-169 (2022).
[10] Lee, Y. S., Yeom, J. S., Noh, J. H., et al., "A novel GNSS spoofing detection technique with array antenna-based multi-PRN diversity," Journal of Positioning Navigation and Timing, 10(3), 169-177 (2021).
[11] Daneshmand, S., Jafarnia-Jahromi, A., Broumandan, A., et al., "GNSS spoofing mitigation in multipath environments using space-time processing," [2020-04-18].
[12] Zhang, G., Zhang, Y. and Tian, Y., "Research on Beidou deception interference detection Technology based on DOD and PTD," Applied Science and Technology, 46(2), 35-41 (2019).
[13] Zhou, Y., Wang, S., et al., "Overview of GNSS spoofing interference detection," Computer Engineering and Applications, 58(11), 12-22 (2022).
[14] Wang, W. and Gong, J., "GNSS deception interference detection algorithm based on compound SQM variance," Journal of Civil Aviation University of China, 38(04), 7-12(2020).
[15] Zhu, R. and Wang, W., "Multi-star joint induced deception detection algorithm based on SCS," Modern Electronic Technology, 46 (11), 1-8 (2019).
[16] Wu, Z., Wu, W., et al., "Research on stepwise induced deception detection Algorithm based on INS/GNSS tightly coupled combination," Navigation Location and Timing, 6(1), 7-13 (2019).
[17] Liu, Y., Li, S., Fu, Q. and Zhou, Q., "Deception detection method of inertial/Satellite integrated navigation system assisted by atomic clock on chip," Chinese Journal of Inertia Technology, 27(5), 654-660 (2019).
[18] Lee, J. H., Kwon, K. C., et al., "GPS spoofing detection using accelerometers and performance analysis with probability of detection," International Journal of Control Automation and Systems, 13(4), 951-959 (2015).
[19] Lu, D. and Yin, Y., "Multi-parameter GNSS spoofing interference detection based on CS-C-SVM," Journal of Signal Processing, 38(6), 1325-1332 (2019).
[20] Li, J. Z., Zhu, X. W., et al., "Research on multi-peak detection of small delay spoofing signal," IEEE Access, 8, 151777-151787 (2020).
[21] Pan, H. and Cai, C., "Navigation signal deception interference detection based on BP neural network," Modern Electronic Technique, 45(1), 7-10 (2022).
[22] Pang, C., Guo, Z., et al., "Detection method of Beidou relay deception interference signal based on PNN," Chinese Journal of Inertia Technology, 29(4), 554-560 (2021).