Acta Geodaetica et Geophysica
https://doi.org/10.1007/s40328-024-00453-y

ORIGINAL STUDY

A forwarding spoofing detection algorithm for Beidou navigation satellite system vulnerability

Jiangtao Xu[1] · Yajuan Guo[1] · Daohua Zhu[1] · Yunxiao Sun[1] · Wei Huang[1] · Xindong Zhao[1]

Received: 8 December 2023 / Accepted: 25 August 2024

Abstract
With the Beidou navigation system's fast expansion in China, it is popular in military and civilian aspects. However, since the satellite orbit operates at an extremely high position and there is energy loss during the propagation process, the receiver only picks up a very faint signal, which makes the Beidou receiver very vulnerable to interference. The interference of the receiver is divided into natural interference and human interference, of which the human interference is particularly serious. Deception is commonly used in human interference. The deception interference detection technology in Beidou navigation system is studied in this research. Firstly, the signal in the signal capture stage is detected by multi-peak detection algorithm to determine the signal type. If it cannot be determined, the signal is detected by the half-peak full-width algorithm, so as to determine the signal type. In the stage of signal tracking, the Doppler shift of the spoofing signal is applied to determine whether the signal is spoofed or not. When the spoofing signal forwarding delay is set to 0.5 and 1 chip respectively, the full width of half peak is 8.56 and 11.35 after fitting the main peak. If the half-peak full width exceeds the normal navigation signal, it indicates spoofing interference. The constructed model can effectively track downspoofing signals and improve the Beidou navigation system's detection performance.

Keywords Beidou navigation System · Multi-peak detection algorithm · Deception interference · Half-peak full width algorithm · Doppler shift

1 Introduction

With the development of economy, the country invests more economy into the research of science and technology, and the global satellite navigation system has irreplaceable strategic significance both economically and militarily (Bai et al. Jan. 2019). Many political and military powers are making great efforts to develop and improve their satellite navigation systems. In recent years, China's self-developed BeiDou Navigation Satellite

✉ Jiangtao Xu
xujiangtaojiangsu@163.com

[1] Electric Power Research Institute of State Grid Jiangsu Electric Power Co., Ltd, Nanjing 211106, China

System (BDS) has been applied to military and civilian fields. However, Beidou navigation user's receivers are very susceptible to interference (Kang et al. 2021). The satellite orbits at an extremely high position. Therefore, it is extremely vulnerable to interference, of which human interference is the greatest threat to the signal. Aiming at the problem that the signals of the Beidou system are easily interfered by human beings in the process of transmitting information, this study proposes an algorithm to detect whether the signals are interfered by deception. In this method, the characteristics of the transformational deception signal are analyzed. The half-maximum Full width (FWHM) algorithm is applied to determine whether the signal is disturbed. As stated by the Doppler frequency change characteristics of the spoofing signal, whether the signal is interfered by spoofing in the signal acquisition stage is determined. Compared to other existing methods, the method used in this study combines a multi-peak detection algorithm with a FWHM detection algorithm, and then analyzes the number tracking phase by means of Doppler offset and Doppler rate of change consistency detection algorithms.This research is divided into four parts. The first part is a brief introduction of other scholar's research topics on signal deception interference detection. The second part is a review of the main methods used in this study. The third part is to use the method to study the model results and analyze the results. The fourth part is the summary of all the above studies and the prospect of future studies.

1.1 Related work

Global satellite navigation system is popular, but the user receiver is susceptible to spoofing interference. Shi et al. (2019) found that phase modulation technology has excellent performance in generating interference signals in electronic countermeasures. Through the analysis of scattered wave interference and phase modulation, the research team came up with a radar jamming technique. By fusing periodic binary phase values into radar signals, the frequency characteristics of radar signals could be changed. The signal was then re-transmitted to the target, producing a pseudo-target image. This method could effectively realize deception jamming and blocking jamming (Shi et al. 2019). Aiming at the problem that radar signals are very susceptible to interference, H. Yu et al. established a signal model of two-dimensional vector sensor and spoofting interference by studying the difference between target scattering and interference generation mechanism. The model proposed a detection algorithm based on the Neyman Pearson criterion. This model could solve the interference problem in radar signal effectively. The proposed method had good performance for radar recognition of interference signals (Yu et al. 2019). Wang et al. (2019) proposed an anti-jamming front end. Firstly, an RF module was designed, and then an interference recognition model based on linear constraint minimum variance was constructed. The model could recognize the interference signal effectively by the spatial domain of the signal. This model had relatively good recognition performance for interference signals and had certain anti-interference ability (Wang et al. 2019). Guo et al. (2019) conducted research on the recognition of spoofs in radar systems, and found that errors in traditional methods would lead to low accuracy of radar systems for spoofs and target recognition. Therefore, the research team constructed a new method to identify the interference signal based on the characteristics of bistatic radar. The proposed method had a high recognition accuracy and could effectively identify interference signals (Guo et al. 2019).

Jiang et al. (2021) found that the traditional peak-seeking algorithm was not ideal when detecting the reflection spectrum of multi-peak fiber Bragg grating. To solve this problem, an improved method was proposed. In this method, the multi-peak optical fiber Bragg grating reflected spectral signals were processed by a five-point sliding filter. The suggested technique might dynamically find various sensor system reflection spectra, and showed relatively good stability (Jiang et al. 2021). L. Pei et al. proposed an improved model to process toll data of expressways by analyzing traffic time data in a large number of expressways. The research team first analyzed the toll data of the highway, and proposed a data cleaning method to analyze the original data. Aiming at the shortcomings of the original model, an improved model was proposed. This method could accurately and efficiently detect abnormal conditions in expressway toll data (Pei et al. 2021). G. Yang et al. believed that peak detection played a very important role in the processing of spectral signals. However, there were always noise and baseline signals in the measured spectrum, and these interference signals would produce false peaks. Therefore, the study team suggested a continuous wavelet transform and image segmentation based spectral peak detection technique, which was able to successfully remove the influence of noise and baseline from the data. The proposed method could identify and process noise signals in the spectrum, and Spectral peak's individual properties might be brought into sharper focus (Yang et al. 2020). O. Eriksson et al. proposed a new data processing method, which could detect weak signals and local signals in the peak distribution through peak detection. The peak detection method could better detect the real substance composition, which made recognition far more precise and time-saving (Eriksson et al. 2019). He et al. (2019) believed that due to the high degree of similarity between the genuine signal and the navigation data in GNSS, spoofing signals were readily identifiable. To solve this problem, the research team proposed a new two-antenna deception detection technology, which estimated the real signal consistency by analyzing the carrier phase and navigation information. This method had good detection ability for the signals in GNSS and could well identify the spoofing signals (He et al. 2019).

To sum up, many scholars have done research in the field of signal deception interference detection, which have achieved remarkable results. However, most methods are difficult to accurately identify and track signals in complex environments, and the recognition accuracy rate cannot meet the requirements well. Therefore, an algorithm is proposed to detect whether the signal is subject to spoofing interference. In this method, signal's highest point of correlation is detected by the characteristic analysis of the transformational deception signal, the multi-peak detection method and the half-peak full width algorithm, so as to determine whether the signal is interfered.

2 Research on forwarding spoofing detection algorithm of Beidou System

With the wide application of BDS in various fields, the problem that its signal is susceptible to interference is becoming more serious. In this study, the characteristics of Beidou signal and the principle of deceptive interference are analyzed, and through the analysis results, the capture stage and tracking stage of the signal are modeled to identify the interference signal or the navigation signal.

3 Research on Beidou signal characteristics and deceptive interference

The signal launched by Beidou satellite can be divided into three levels from the structure, which are carrier, ranging code and data code. The range code of Beidou signal refers to one of satellite-transmitted navigation signals in the BDS (Zhang et al. 2019). Its role is to spread spectrum processing of navigation signals, so that it occupies a wider bandwidth, so that the receiver can more easily distinguish and receive the signal. Meanwhile, the range code can also be used to calculate the spread out from the satellite to the receiver, so as to achieve high-precision positioning. Data code refers to the code that carries navigation data in the signal sent by the satellite in the BDS. Its function is to transmit the navigation data to the receiving end in the form of binary coding, so as to achieve accurate positioning and navigation functions. The signals of the BDS are modulated using BPSK, as shown by Eq. (1).

$$S_{BPSK}(t) = AC(t)D(t)\sin(2\pi ft + \varphi) \tag{1}$$

In Eq. (1), C represents the ranging code; f represents the signal carrier frequency; A represents the signal's amplitude; φ represents the initial phase of the carrier; D is data code. In the structure of the Beidou signal, the transmitting end of the satellite signal first adds the data code and the ranging code, and this step is to complete the modulation of the ranging code through the data code. Then the combination code of data code and range code is combined, and the carrier is modulated by BPSK. Finally, a carrier center frequency version of the range code signal is sent via satellite. The carrier is used in Beidou satellite navigation because the frequency of the ranging code is a low-frequency electromagnetic wave segment, which is very vulnerable to electromagnetic interference. The frequency of the carrier signal is different from that of the ranging code, which belongs to the ultra-high frequency electromagnetic wave segment. The frequency wave propagates through the form of direct wave. Propagation in the form of direct wave can have good penetration performance to the ionosphere and buildings, thus reducing the interference of noise. The navigation signal receiver can also accurately locate the target through the carrier phase (Lin and Zhang 2019).

The Beidou signal is generally divided into B1I and B2I, and the ranging code of these two signals is a pseudo-random code. The range code is generated by the two 11-level linear shift registers inside each satellite to generate two different sequences, and then by the gold code generated by the two linear sequences to shorten 1 code slice.The two shift registers share the same starting code phase, and both C_{B1I} code and C_{B2I} code have relatively good autocorrelation and cross-correlation characteristics, as shown in Eq. (2).

$$\begin{cases} R(\tau) = \dfrac{1}{L_P} \displaystyle\sum_{i=1}^{L_P} [a(i)a(i-\tau)] \\ R(\tau) = \dfrac{1}{L_P} \displaystyle\sum_{i=1}^{L_P} [a(i)b(i-\tau)] \end{cases} \tag{2}$$

In Eq. (2), $a(i)$ represents the i code slice of C_{B1I} code; $b(i)$ represents the i slice of C_{B2I} code; τ denotesthe number of code elements representing the equivalent delay time between two sequences; L_p is the code element number of a cycle (Nicolae et al. 2019). It can be calculated from Eq. (2) that the autocorrelation value of the satellite reaches the maximum value at 1, and the correlation value at other times is almost 0. The peak value of cross-correlation between two different satellites is also almost 0, so the Beidou signal can be tracked by the good characteristics of the ranging code.

A data code is a binary code that contains a navigation message. Satellite navigation messages contain a set of satellite-movement data parameters, including orbit parameters, ionospheric delay parameters, signal transmitting time and so on. When the receiver receives the navigation signal, as a result of the satellite's relative velocity to Earth,, the signal will appear Doppler effect when propagating, resulting in a certain. This error is the Doppler shift generated by the Doppler effect, and its calculation equation is shown in Eq. (3).

$$f_r = f_c(1 - \frac{av_r}{c}) \tag{3}$$

In Eq. (3), v_r represents the vector of the relative speed between the satellite and the signal receiver; f_c represents the carrier frequency of the received signal; c represents the speed of light. Since the satellite's velocity dominates the Doppler shift while the receiver is immobile, its calculation equation is shown in Eq. (4).

$$f_d = \frac{f_r v_d}{c} \tag{4}$$

In Eq. (4), when the receiver is stationary, f_r denotes the transmission frequency of the signal; v_d denotes projection of satellite speed along receiver-satellite transmission axis (Alejandro et al. 2020). From this, satellite and signal receiver's greatest velocity on the projection, as shown in Eq. (5).

$$v_{dm} = \frac{v_s r_e}{r_s} \tag{5}$$

In Eq. (5), r_e denotes the radius of the earth; v_s is the speed of motion of the satellite; r_s is the size of the orbit radius. It can be calculated that when the receiver is at rest, the maximum Doppler shift due to the satellite motion is 4.83 kHz. The signal of Beidou satellite is defective, which leads to its vulnerability. Beidou signals are public except for military codes.The orbit of the Beidou satellite is particularly high because of the loss of energy during transmission. The signal is sent to Earth with very little power and can be easily interfered with.There are two main types of interference to satellite navigation system, The structure of forwarding spoofing is shown in Fig. 1.

In Fig. 1, the forwarding spoofing device is composed of a receiver, a delay device, a power amplifier and a transmitting antenna. The interference source device first captures the signal emitted by the satellite through the receiving antenna, and then according to the needs of the deception, the captured signal is delayed by the delay operator, and then a power amplifier boosts a signal's volume. The reason for this operation is that the signal after delay processing will be attenuated, so the signal is amplified to better allow the target receiver to capture the signal. Finally, through the transmitting antenna, the signal is sent to the intended recipient. Figure 2 illustrates the forwarding spoofing concept.

Figure 2 shows the principle of forwarded spoofing, A denotes the location of the intended recipient; A_1 indicates thelocation of the receiver after being spoofed. When the target receiver is not spoofed, set the coordinate of point A as $(x_A, y_A, z_A)$and measure the distance of the four satellites, as shown in Eq. (6).

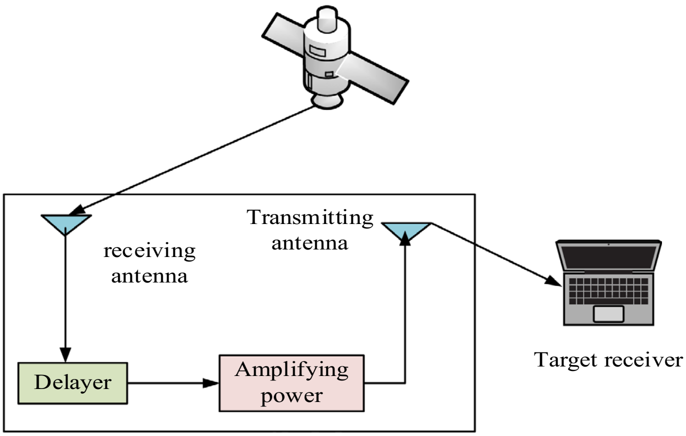

Fig. 1 Forward forward cheat interference structure

$$\rho_i = \|S_i - A\| + ct_u \tag{6}$$

In Eq. (6), ρ_i represents the pseudo-distance value from each satellite to the signal target receiver; A coordinates of the target receiver; S_i is the coordinate of the target receiver; c denotes the speed of light. By simplifying the equation, the positioning equation of point A is shown in Eq. (7).

$$\rho_i = \sqrt{(x_i - x_A)^2 + (y_i - y_A)^2 + (z_i - z_A)^2} + ct_u \tag{7}$$

In Eq. (7), x_i, y_i, z_i denotes the coordinates of the i satellite; t_u represents receiver clock difference. When the signal target receiver is subject to forwarded spoofing interference, the signal received by the receiver is not the direct signal sent by the satellite, but the spoofing signal forwarded by the interference source. The target receiver positioning expression is shown in Eq. (8).

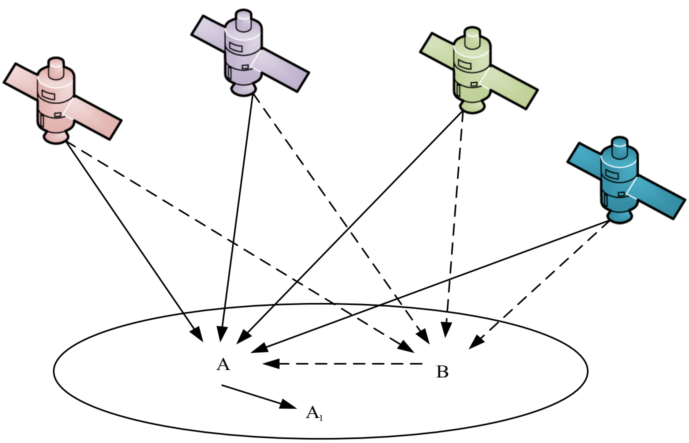

Fig. 2 The Principle of Forward Deception Jamming

$$\begin{cases} \rho_i = \sqrt{(x_i - x_A)^2 + (y_i - y_A)^2 + (z_i - z_A)^2} + ct_x \\ t_x = t_u - t_1 - t_2 - t_3 \end{cases} \quad (8)$$

In Eq. (8), t_1 represents the delay between the receiving antenna and the transmitting antenna of the interference source;t_2 represents the path delay from the transmitting antenna to the receiver; t_3 indicates artificial delay (Kou and Feng 2022). Based on the study of the signal structure, vulnerability and the principle of forwarding spoofing, the overall scheme of this study is proposed, as shown in Fig. 3.

In Fig. 3, the captured signal is detected whether the signal is deceived by the half-peak full-width algorithm, and whether the signal is deceived by the monitoring of the Doppler shift change of the deceptive signal. The half peak full width algorithm is a common method used to determine the width of signal peaks. The FWHM algorithm is easy to understand and implement, and can be applied to various types of signals, including but not limited to spectrum, waveform, sound, etc. Therefore, it has a wide range of applications in different fields. The FWHM algorithm is relatively robust to noise and changes in data, and can to some extent handle interference in the data. In many cases, full width at half maximum is a good measure of signal characteristics and can provide reliable estimates of signal width.

4 Research on Beidou signal deception interference detection algorithm

Multimodal detection algorithms are often used in forwarding spoofing. However, in the case of hour delay, it can not show good recognition performance and has certain limitations. Therefore, the detection delay of FWHM algorithm is proposed. The FWHM algorithm detects the deception signal by detecting the geometry of the correlation peak and the half-height width of the correlation peak. Generally, the width of the correlation function is 2 slices, and its equation is shown in Eq. (9).

$$R(\tau) = \begin{cases} \tau + 1 , -1 \le \tau \le 0 \\ -\tau + 1,\ 0 \le \tau \le 1 \\ 0 \text{ , others} \end{cases} \quad (9)$$

In Eq. (9), τ is the number of code elements equivalent to the delay time between two sequences. When the phase of the pseudo-code is completely coincident, the correlation

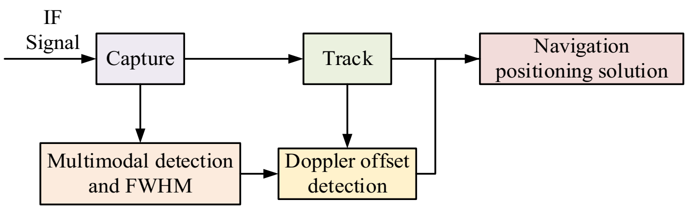

Fig. 3 Overall interference detection plan

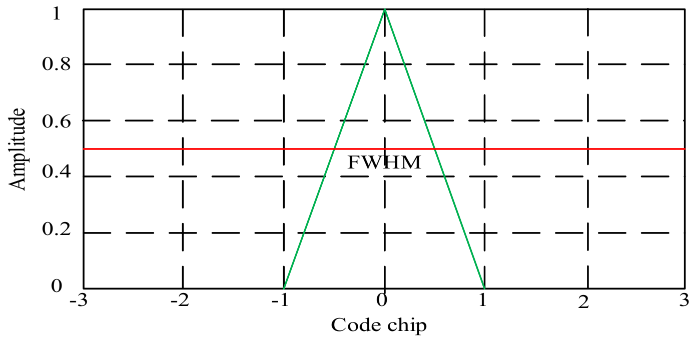

Fig. 4 FWHM Sketch Map

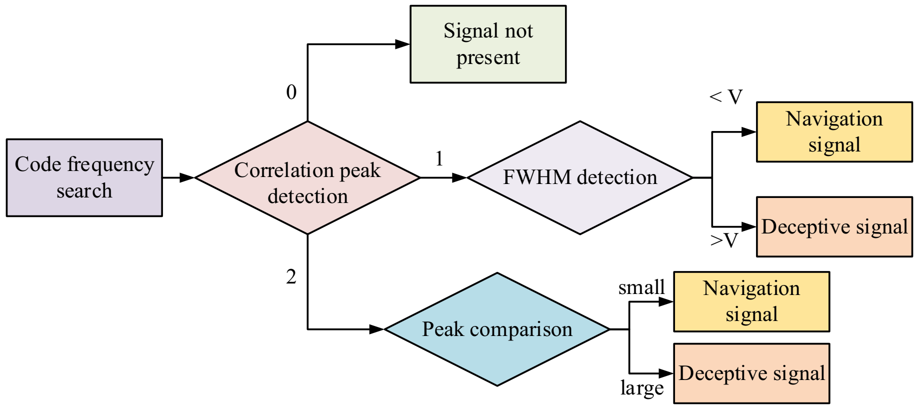

Fig. 5 Capture phase interference detection process

peak can reach the maximum value. When one chip width is offset, the correlation peak is the minimum value. As long as the correlation peak in the frequency domain is the width of two chips, then the half-height width of the correlation peak is the width of one chip. Therefore, the correlation peak's half-height breadth is constant when there is no deception signal.

The schematic diagram of FWHM is shown in Fig. 4. Based on the schematic diagram of FMHM, the detection threshold can be obtained by using the similar triangle principle as shown in Eq. (10).

$$V_w = 2(V_m - V_t)/V_m + \varepsilon \tag{10}$$

In Eq. (10),V_w represents the threshold value of detection; V_m represents the maximum number of relevant results; V_t represents half of the relevant peak value; ε represents the penalty factor (Liu et al. 2021). The signal is a forgery if the half-height of the recorded correlation peak is larger than the detection threshold. The flow of interference detection in receiver signal acquisition stage is shown in Fig. 5.

In Fig. 5, code frequency search is performed on the received signal first. If the detection result is 0, it means that there is no correlation peak, that is, no signal. If the detection result is greater than 1, it indicates that the receiver is subject to spoofing interference. The peak value of the signal is compared, if it exceeds the power detection threshold, the signal is a deception signal, otherwise it is a navigation signal. If the detection result is 1, FWHM detection is performed on the signal. A comparison is made between the signal and the detection threshold. A signal is considered deceptive if its strength exceeds the detection threshold; otherwise, it is a navigation signal.

In the capture stage, the signal may be missed or false capture, so in the tracking phase, detecting spoofing interference is crucial. After the completion of signal capture, the signal is tracked; Accurate satellite signal carrier frequency and coding phase can be obtained through signal tracking. The signal tracking of the receiver mainly includes two parts, one is the tracking of the code ring, and the other is the tracking of the carrier ring. Code ring tracking accomplishes pseudo-code stripping by continually tuning the local pseudo-code to match the pseudo-code of the incoming signal. The tracking of the carrier ring is similar to that of the code ring, and carrier stripping is realized by adjusting the local carrier ring to be consistent with the carrier ring in the received signal to complete the signal tracking (Wang et al. 2020; Zhang et al. 2022). There is a Doppler effect in the signal transmission because the satellite and the receiver are moving at different speeds. Equation (11) is the receiver's actual signal frequency.

$$f_r = f_{carr} + f_d^i \tag{11}$$

In Eq. (11), f_r represents the carrier frequency received by the receiver; f_{carr} denotes the frequency of the standard carrier from which the Beidou satellite is launched; f_d^i represents the Doppler shift due to relative motion. The Doppler shift is shown in Eq. (12).

$$f_d^i = (V^o - V^i) \cdot I_o^i / \lambda \tag{12}$$

In Eq. (12), λ represents the wavelength of the carrier; V^o represents the speed of motion of the receiver; I_o^i represents the direction cosine of the target receiver to the satellite. V^i indicates the motion speed of the Beidou satellite. The signal receiver's carrier frequency for the incoming satellite signal will change when forwarding spoofed interference is carried out. The signal received by the target receiver changes as shown in Eq. (13).

$$\begin{cases} f_{rs} = f_{carr} + f_d^s + f_d^{os} \\ f_d^s = (V^s - V^i) \cdot I_s^i / \lambda \\ f_d^{os} = (V^o - V^s) \cdot I_o^s / \lambda \end{cases} \tag{13}$$

In Eq. (13), V_s represents the motion speed of the interference source; I_o^s denotes the direction cosine of the forward interference source to the target receiver; I_s^i denotes the direction cosine of the forwarded interference source to the satellite (Zhao et al. May 2021). The received signal change rate is shown in Eq. (14).

$$\Delta f_d = f_d^s + f_d^{os} - f_d^i \tag{14}$$

In Eq. (14), f_d^{os} represents the Doppler frequency shift of the target receiver relative to the spoofing interference source; f_d^s represents the Doppler shift of the spoofing source relative to the satellite motion. Since the received signal of the forwarded spoofing is from the same interference source, the frequency of the signal will show a high degree of similarity. It is necessary to detect the Doppler frequency change of the received signal to identify spoofing interference. The specific process is shown in Fig. 6.

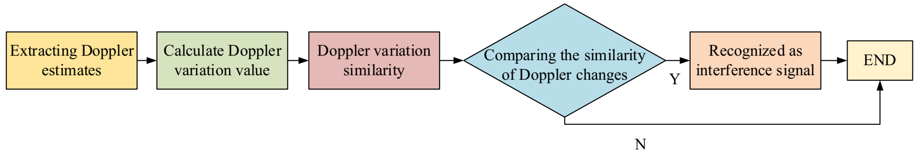

Fig. 6 Doppler rate of change consistency detection

In Fig. 6, initialization of the tracking loop requires all parameters to be specified on the target receiver; Then the carrier is extracted. After the extraction is complete, the Doppler estimates are sampled. The Doppler change value is calculated based on the Doppler sampling data. Then the correlation value is calculated by the Doppler change value to detect the similarity of the Doppler change. Finally, the calculated Doppler correlation values are compared with the set detection thresholds. If it is less than the threshold, it means that it is interfered by deception (Li 2022; Du et al. 2022). The process of BDS forwarding deception jamming is shown in Fig. 7.

In Fig. 7, the received signal is first captured and processed. The detection of the signal power is applied to identify the kind of signal when the number is larger than 1. The FWHM detection method is applied to identify the kind of signal present when the number of correlation peaks is equal to 1. If the half-height of the signal is wider than the detection threshold, it is a deceptive signal. In the event that it is lower than the detection threshold, the signal will be sent into the tracking stage in order to undergo detection.

When the real navigation signal is received by the target receiver, the similarity of Doppler frequency variation between different satellite signals recorded by carrier ring tracking is low. However, since the spoofing signals come from the same interference source, the Doppler frequency variation rules between the signals will have a high similarity. Spoofing interference can be effectively detected by monitoring the consistency of Doppler frequency variation between received satellite signals. The design of Doppler change rate consistency detection scheme is as follows: Firstly, the Doppler sampling frequency and

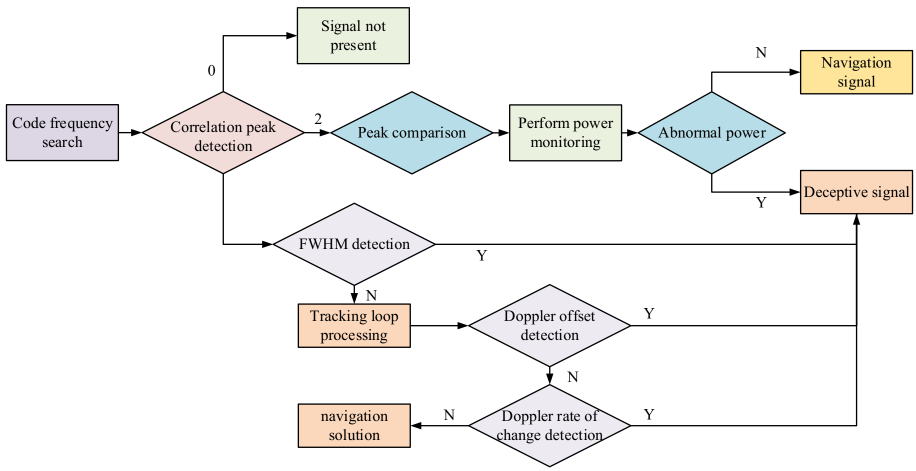

Fig. 7 General process of deception interference detection

sampling time of the receiver tracking loop are set, and then the estimated value extracted from the carrier loop of the receiver tracking loop is sampled according to the parameters. Mark the sampling result as $S_i(k)$; i represents different channels; k represents the sample value at a certain time. Then, based on the Doppler sampling data $\Delta S_i(k) = S_i(k) - S_i(0)$ within each tracking loop.The correlation value is calculated for the Doppler change value of any two tracking loops, and finally the correlation value is compared with the set detection threshold. If it is greater than the detection threshold, no spoofing interference occurs. If it is less than the detection threshold, it indicates a spoofing attack,and the spoofing signals are those of the i and j tracking loops.

5 Performance analysis of BDS forwarding spoofing detection algorithm

In the first section of this chapter, the performance of the Beidou signal acquisition stage is analyzed, and the recognition accuracy of the model is tested by setting different forwarding delay chips for the hourly delay deception signal. In the second section, the identification performance of the Beidou signal tracking stage is tested. To evaluate the detection capabilities of the algorithm, the static experiment and the dynamic experiment that make up the Doppler offset detection experiment are separated into two distinct categories.

5.1 Performance analysis of Beidou system acquisition phase detection algorithm

Since the strength of each satellite signal is almost identical, the following signal characteristics have been determined: The navigation signal load to noise ratio is 45 dB·Hz; The center frequency is 4.1 MHz; The sampling frequency is 20 MHz; The coherence integration time is 1 ms; The interference detection experiment is set under different circumstances. The experimental parameter settings are shown in Table 1. Among them, ISR is Interference to Signal Ratio.

This experiment focuses on the detection of hourly delay deception. The hourly delay spoofing signal usually refers to the interference signal that has been delayed, together with the spoofing signal, and the real signal in two chips. In the BDS signal, the signal is set to be interfered, and the spoofing signal is added to the signal, and the spoofing signal forwarding delay is 2 chips.

In Fig. 8, due to the small forwarding delay, the correlation peaks of the spoofing signal and the navigation signal are too close to distinguish well. Therefore, the correlation peak of the one-dimensional test diagram of the code phase is amplified, and

Table 1 Experimental parameter settings

Signal type	ISR/dB	Number of chips	Number of related peaks	FWHM
Forward deception jamming signal	0	0.5	1	8.56
	0	1	1	11.35
	0	1.5	1	13.56
	0	2	2	7.15
Normal navigation signal	/	1	1	7.32

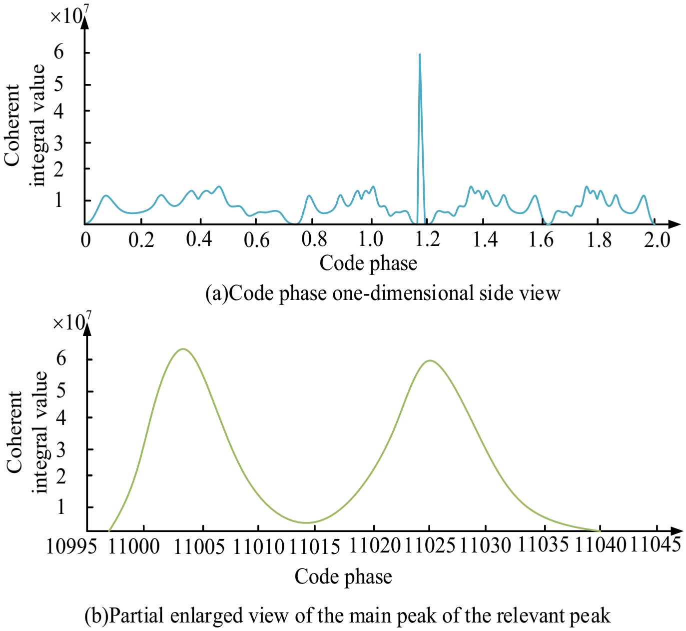

Fig. 8 Signal capture detection results

the correlation peak amplification diagram shown in Fig. 8b is obtained. Among them, although the two correlation peaks of deception signal and navigation signal are very close, they do not coincide together. The existence of two correlated peaks can be detected, indicating that the signal is a spoofing interference signal. When the spoofing signal forwarding delay is 2 chips, the jamming signal can be accurately identified, which shows that the algorithm has good performance. The spoofing signal forwarding delay is set to 1 chip, and the result is shown in Fig. 9.

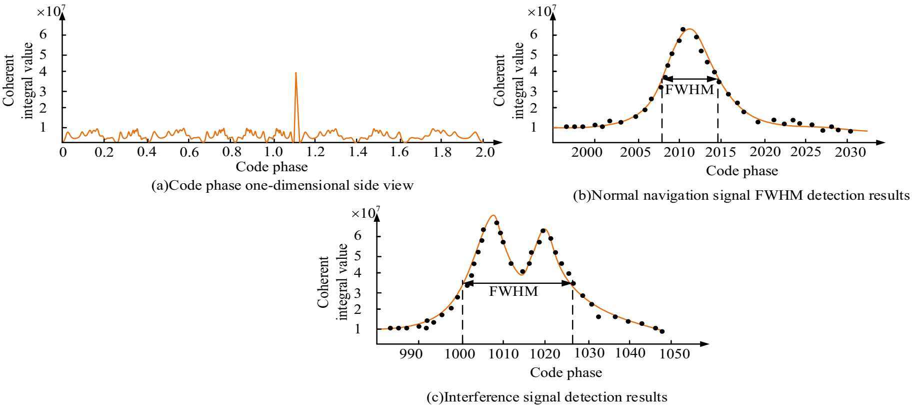

Fig. 9 Satellite 2 interference signal detection result diagram

Figure 9 represents a one-dimensional view of multi-modal detection results, Fig. 9b represents the FWHM detection results of normal navigation signals, and Fig. 9c represents the FWHM detection results of captured Beidou signals. With a 1 chip spoofing signal forwarding delay, the correlation peaks of interference signal and navigation signal coincide. The signal is detected by multi-peak detection algorithm, and a correlation peak exceeding the threshold is detected. The FWHM algorithm is used to fit the correlation peaks, and the FWHM value is 11.35. Comparing the FWHM value with the normal navigation signal, it is found that the FWHM value is larger than the normal navigation signal, and the signal is judged to be spoofed. When the delay in sending the deception signal is short, the multi-modal detection algorithm cannot detect the interference signal, and the FWHM algorithm can detect the interference signal, and the effectiveness of the FWHM detection algorithm is better. Set the spoofing signal forwarding delay to 0.5 chip, and the result is shown in Fig. 10.

Figure 10represents a one-dimensional view of multi-modal detection results, Fig. 10b represents the FWHM detection results of normal navigation signals, and Fig. 10c represents the FWHM detection results of captured Beidou signals. When using a spoofing signal with a forwarding delay of 0.5 bits, the correlation peaks of interference signal and navigation signal coincide. The interference can not be determined by the multi-peak recognition algorithm, and then the signal is detected by the FWHM algorithm. After fitting the main peak, the FWHM value is 8.56, which exceeds the FWHM value of normal navigation signal. When the delay in transmitting the spoofing signal is 0.5 bits, the proposed algorithm can still recognize spoofing interference signals. Monte Carlo method is applied to analyze the recognition probability of deception jamming algorithm in the acquisition stage under different chip conditions, as shown in Fig. 11.

In Fig. 11, the detection effectiveness of the detection algorithm becomes better with the increase of the spoofing number slice. When the transmission delay is 1 chip, the signal detection probability of four different satellites reaches 75%. When the spoofing signal forwarding delay exceeds 2 chips, the detection probability reaches 100%. The detection performance of deception interference signals with large delay is very good. For small delay spoofing signals, when the forwarding delay reaches 1 chip, the

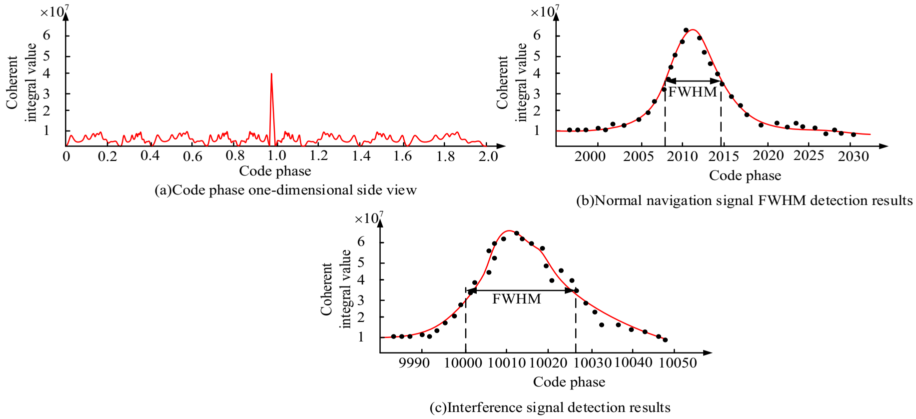

Fig. 10 Satellite 3 interference signal detection result diagram

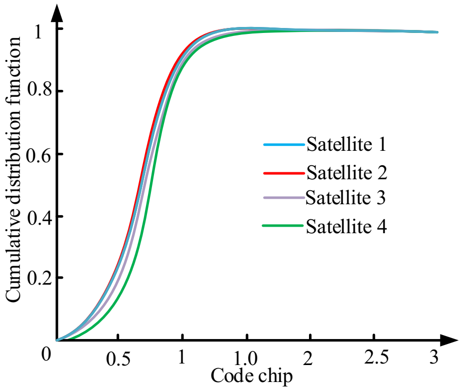

Fig. 11 The Relationship between deception signal number delay and detection probability

detection performance is better. The speed of detection is also one of the performance of the judgment recognition algorithm.

Figure 12a represents the relationship between the time used by the algorithm to detect signals and the detection accuracy rate; Fig. 12b represents the relationship between the time used by the algorithm to detect signals and the number of forwarding delay chips. The algorithm's detection accuracy improves steadily with more time spent on detection. The more the number of forwarding delay chips, the less time it takes. As the number of chips increases, the signal can be detected by multi-modal detection. If the number of chips is small, the multi-peak detection method can not detect the spoofing interference signal, and more detection steps are needed to detect the signal, so the detection time is increased.

5.2 Performance analysis of BDS tracking phase detection algorithm

The Doppler offset detection experiment is divided into static experiment and dynamic experiment. The data parameters of the navigation signal are set in this experiment. The data sampling frequency is set to 20 MHz; The center frequency is set to 4.1 MHz, and

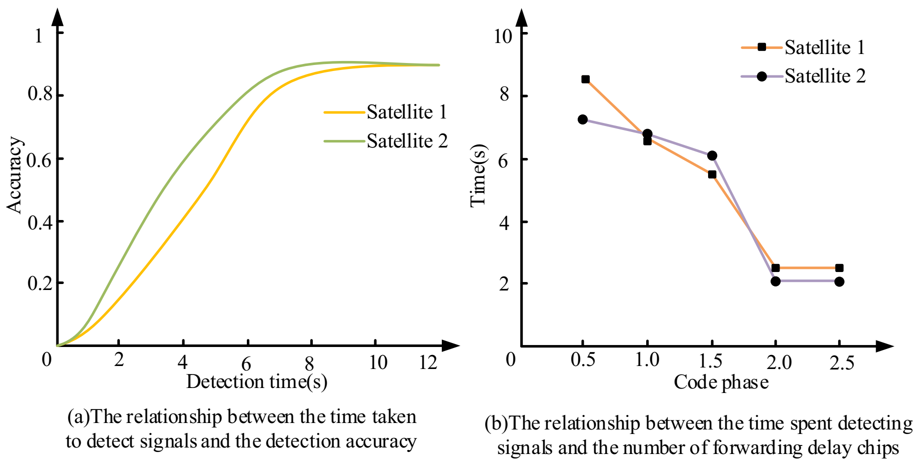

Fig. 12 Efficiency chart of detection algorithm

the data length is set to 3000 ms. The detection results of spoofing interference of the receiver at rest are shown in Fig. 13.

Figure 13 and Fig. 13b represent the Doppler shift and Doppler shift variance of satellite 1 before and after receiving forwarded spoofing at 2 s, respectively. Figure 13c, d respectively show the Doppler shift and Doppler shift variance of satellite 2 without forwarded spoofing interference. Satellite 1 receives the forwarding deception interference at 2 s. Through the carrier information extracted from the carrier ring, it is found that the Doppler frequency changed greatly. By monitoring the Doppler movement variance, it is found that there is an obvious peak change at 2 s, indicating that satellite 1 is spoofed. The Doppler shift and Doppler shift variance of satellite 2 fluctuate normally within a certain range, so the satellite is not spoofed. The detection results of spoofing interference of the moving receiver are shown in Fig. 14.

Figure 14 and Fig. 14b respectively show the Doppler shift and Doppler shift variance of satellite 3 before and after receiving forwarded spoofing interference. Figure 14c, d respectively show the Doppler shift and Doppler shift variance of satellite 4 before and after receiving forwarded spoofing interference. For about 25 min, both satellites were tricked by relays. The Doppler shift of satellite 3 obviously changes after spoofing interference, and the Doppler shift variance of satellite 3 has a peak value of about 600 at 2 s. After spoofing, the Doppler shift of satellite 4 does not change significantly, but its Doppler shift variance also has an obvious peak. As long as the Doppler shift changes under the influence of the spoofing signal, the Doppler offset detection algorithm can detect the signal and identify whether the signal is interfered.

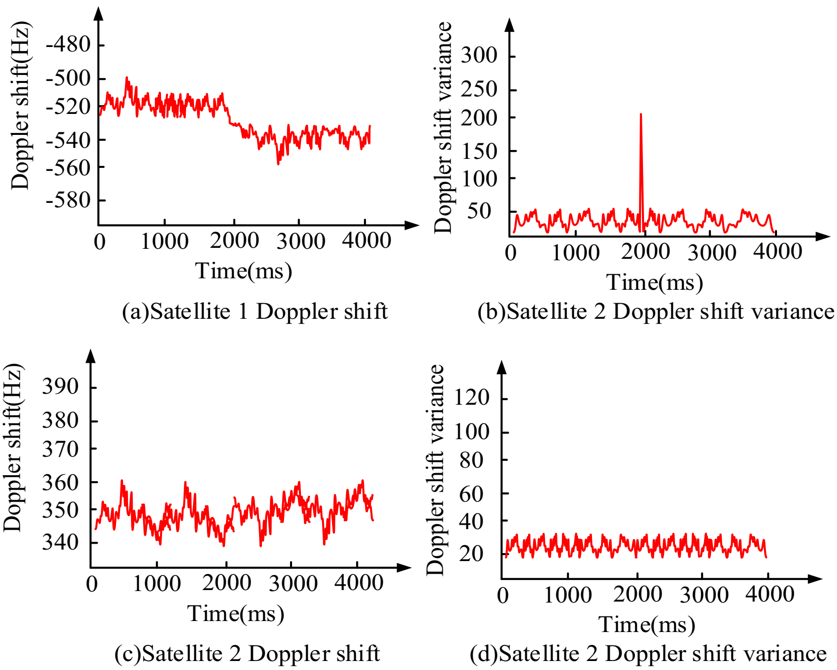

Fig. 13 Static receiver deception interference detection results

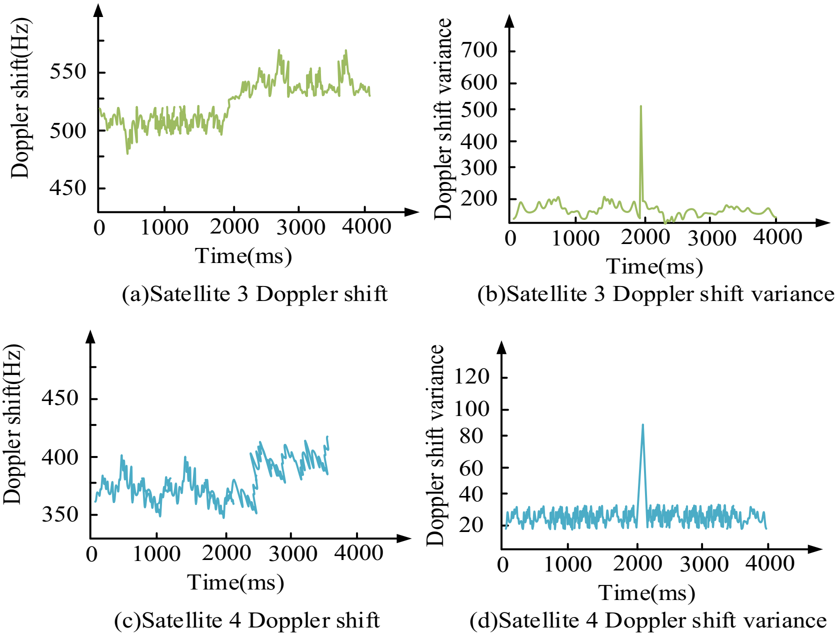

Fig. 14 Motion receiver deception interference detection results

6 Conclusion

The BDS is widely used in military and civilian applications. Aiming at the spoofing satellites of the BDS, this study proposes a method to detect spoofing through the change of the delay and Doppler shift of spoofing signals. When the lag in sending the spoofing signal is set to 0.5 and 1 chip respectively, the multi-peak detection algorithm can not recognize the interference signal. After fitting the main peak with FWHM algorithm, the half-peak full width is 8.56 and 11.35, which exceeds the half-peak full width of normal navigation signal. If the spoofing signal's forwarding latency is 2 chips, the interference signal can be accurately identified by multi-peak detection algorithm. When the transmission delay is 1 chip, the signal detection probability of four different satellites reaches 75%. When the spoofing signal forwarding delay exceeds 2 chips, the detection probability reaches 100%. There are still shortcomings in this study, which is conducted in a laboratory environment. Due to the control of forwarding delay and power, the signal mode of deception signal in this study is the same as that of navigation signal. FWHM detection may identify navigation signals as spoofing signals, so the subsequent research needs to further optimize the detection algorithm.

Funding Science and technology project of SGCC (Grant No. J2022069).

References

Bai X, Zhao Y, Ma J, Guo R, Zhang H (2019) Grain size characterization by laser-based ultrasonics based on the centroid frequency shift method. Mater Charact 155(8):808–812. https://doi.org/10.1016/j.matchar.2019.109800

Du Z, Yu L, Zhang J, Cai M, Jiang T (2022) Speed interference suppression for PD radar based on adaptive dictionary. Appl Comput Electromagn Soc J 37(3):354–362. https://doi.org/10.13052/2022.ACES.J.370313

Eriksson O, Rezeli M, Hefner M, Marko-Varga G, Horvatovich P (2019) Clusterwise peak detection and filtering based on spatial distribution to efficiently mine mass spectrometry imaging data. Anal Chem 91(18):11888–11896. https://doi.org/10.1021/acs.analchem.9b02637

Garzón A, Rodriguez W, Cristancho F, Tao M (2020) AhKin: A modular and efficient code for the Doppler shift attenuation method. Comput Phys Commun 246:106854. https://doi.org/10.1016/j.cpc.2019.07.017

Guo Y, Liao G, Li J, Kang H (2019) An improved range deception jamming recognition method for bistatic MIMO radar. Digital Sign Proc 95:102578. https://doi.org/10.1016/j.dsp.2019.102578

Hengli Y, Zhang J, Zhang L, Li S (2019) Polarimetric multiple-radar architectures with distributed antennas for discriminating between radar targets and deception jamming. Digital Signal Proc 90:46–53. https://doi.org/10.1016/j.dsp.2019.03.012

He L, Li H, Mingquan L (2019) Dual-antenna GNSS spoofing detection method based on Doppler frequency difference of arrival. GPS Solut. https://doi.org/10.1007/s10291-019-0868-5

Jiang H, Zhang X, Li D, Zhao Y, Zhang Z (2021) Multi-peak detection algorithm based on wavelength feature recognition in FBG sensor networks. Opt Eng 60(10):154–164. https://doi.org/10.1117/1.OE.60.10.106104

Kang B, Li X, Fan Y, Zhang J, Liang D, Gao Y (2021) Wideband microwave Doppler frequency shift measurement based on acousto-optic frequency shift and DP-QPSK receiver. Measurement 178(8):1093–1102. https://doi.org/10.1016/j.measurement.2021.109388

Kou S, Feng X (2022) Angle-micro-Doppler frequency image of underwater target multi-highlight combining with sparse reconstruction. Appl Acoust 188:108563. https://doi.org/10.1016/j.apacoust.2021.108563

Lin X, Zhang B (2019) Normal doppler frequency shift in negative refractive-index systems. Laser Photonics Rev 13(12):105–114. https://doi.org/10.1002/lpor.201900081

Liu L, Han Y, Zheng X, Qiu Y (2021) Observation of the extreme Doppler shift of acoustic rotating waves in the time domain. J Appl Phys 130(23):2349–2356

Li S, Guo J (2022) An angle error extraction algorithm based on JADE for three-channel radar seeker system with the existence of deception jamming. Digital Sign Proc 131:103754. https://doi.org/10.1016/j.dsp.2022.103754

Nicolae I, Miu D, Viespe C (2019) Sub-limit detection in SAW sensors by FFT spectral analysis of frequency time instability. Sensor Rev 39(2):246–251. https://doi.org/10.1108/SR-02-2018-0048

Pei L, Sun Z, Han Y, Li W, Zhao H (2021) Highway event detection algorithm based on improved fast peak clustering. Math Probl Eng 202(8):7312–7325. https://doi.org/10.1155/2021/7318216

Shi Q, Huang J, Xie T, Wang C, Yuan N (2019) An active jamming method against isar based on periodic binary phase modulation. IEEE Sens J 19(18):7950–7960. https://doi.org/10.1109/JSEN.2019.2905557

Wang F, Liu H, Zhang C (2019) Anti-jamming front-end design of satellite navigation receiver. Appl Comput Electrom 34(11):1739–1749

Wang J, Wang C, Han Z, Wang Y, Huang X (2020) Submarine karst morphology detection method based on multi-frequency ultrasound. Measurement 155:107532. https://doi.org/10.1016/j.measurement.2020.107532

Yang G, Dai J, Liu X, Chen M, Wu X (2020) Spectral feature extraction based on continuous wavelet transform and image segmentation for peak detection. Anal Methods 12(2):169–178. https://doi.org/10.1039/C9AY02052G

Zhang P, Wang J, Ren P, Yang S, Song H (2020) Improved ASM-TER training sequence detection and fine doppler frequency estimation methods from a satellite. J Sens 2020:1–11. https://doi.org/10.1155/2020/3625184

Zhang H, Liu W, Zhang Q, Xie J (2022) Joint resource optimization for a distributed MIMO radar when tracking multiple targets in the presence of deception jamming. Signal Proc 200:108641. https://doi.org/10.1016/j.sigpro.2022.108641

Zhao Z, Qian Z, Yong Y (2021) Frequency shift prediction of a shear mode multi-layered FBAR sensor in viscous media using transfer matrix method. Appl Math Modell 99(6):555–565. https://doi.org/10.1016/j.apm.2021.07.009