Journal of Multidisciplinary Engineering Science and Technology (JMEST)
ISSN: 2458-9403
Vol. 12 Issue 5, May - 2025

Identification Method of Deception Interference Signals Based on Synchronous Variation of CNR among Navigation Satellite Signal

Min Liu,

School of Electrical and Electronic Engineering, Tiedao University Shijiazhaung 050043, Hebei, China

Email: liumin_stdu@163.com

Ronghua Hao

School of Electrical and Electronic Engineering, Tiedao University Shijiazhaung 050043, Hebei, China

Email:haorh_stdu@163.com

***Abstract*— In response to the susceptibility of the BD (BeiDou) navigation system to deception interference, the traditional single satellite CNR (Carrier to Noise Ratio) anomaly detection method is prone to false alarms caused by environmental factors and data jumps, and the direct direction finding of deception interference signals is affected by low SNR(Signal-to-Noise Ratio), which leads to the low accuracy in direction detection. In the paper, it investigates the key technologies for monitoring, evaluating and identification deception interference in BD navigation system.**

A deception interference signals detection method based on synchronous changes in CNR was proposed through using the K-Means clustering algorithm. A deception CNR change domain was defined, which can avoid false alarms caused by external factors and fully utilize the observation information of high elevation visible stars during the current observation period.An under channel direction detection method based on antenna grouping rotation was adopted to select different antenna elements in different time intervals in the receiving channel and restore the complete covariance matrix. Nine spatial spectrum estimation directions can be achieved through three receiving channels.

Through observing the visible SNR of each satellite during the normal receiving time period of B1I frequency point, a certain value slightly higher than the SNR of each satellite is determined as the detection threshold, it can be s found that the accuracy distribution of direction finding evaluation after despreading the deceptive interference signal is between 96.67% and 98%, which is significantly higher than the accuracy of direction finding before despreading, it can meets the general requirements for direction finding evaluation of deceptive interference signals.

Keywords—Navigation Signal; Interference Identification; Synchronous Variation ; CNR; Evaluation ;Method

I. INTRODUCTION

The Global Navigation Satellite System (GNSS) has been widely used in modern life, such as agriculture, forestry, transportation systems, power systems, financial systems, civil aviation systems, or defense systems, it has demonstrated its important value through providing all-weather and high-precision position velocity and time (PVT) information services for various users worldwide. With the increasing application of global satellite navigation systems, spatiotemporal information security has become an important factor that directly affects national security and people's livelihood. Spatiotemporal information security is facing huge challenges, which requires sufficient and comprehensive detection and early warning technologies for potential threats to spatiotemporal information security. According to this demand, it is of great research significance to timely detect various interferences against BeiDou Navigation Satellite System (BDS) and take corresponding measures for protection.

Due to the distance of navigation satellites is too far, usually 20000 to 30000 kilometers away from ground, the signal strength received on the ground is extremely weak. As the weak navigation signal, which is even buried under noise, the BD navigation signal is highly susceptible to interference, which can bring a serious threat to the integrity and availability of the BD satellite navigation system's service performance. Due to the fact that natural interference can be overcome by changing the environment in which the receiver is located, the real serious threat to receiver performance is human interference. This type of interference is malicious interference generated by the attacker against the receiver, which can bring the greatest influence on GNSS receiver performance [1-3].

In fact, with the increasing of satellite navigation guidance weapons, there have been numerous cases of interference against them, mainly including suppression interference and deception interference. Suppressive interference uses interference sources to generate high-power signals that completely mask the real navigation signal, which makes it impossible for the receiver to receiver the real navigation signal

normally [4-7]; Deceptive interference is a method of inducing the receiver to lock in false navigation signals, which are very similar in signal format to real navigation signals, but with slightly higher power. It can control the receiver's positioning results through false navigation signals, thus affects the receiver's service performance [8]. Although suppression interference is simple to implement, it is easily detected by anti-radiation equipment and can be eliminated. Deceptive interference, although is relatively complex to implement, but it has great harm.

II. Material and Methods

A. Signal layer deception interference detection method

The signal layer detection method of deception interference refers to the detection and recognition of deception interference signals from the perspectives of signal spatial domain, correlation domain, measurement domain, etc. The signal layer deception interference detection and recognition methods mainly include: detection of the number of correlated peaks in the capture/recapture stage, detection of the quality of correlated peaks, detection of signal power rationality, Doppler frequency shift consistency detection, signal arrival angle detection, etc.

- Detection of peak count during capture/recapture phase

In the receiver capture stage and the lock out recapture stage, if the received signal contains both real navigation signals and deception interference signals, when the receiver captures a satellite signal during the capture stage, that is, after a correlation peak exceeding the capture threshold appears, it continues to search within a certain range before and after the satellite signal. If the second correlation peak exceeding the capture threshold can be found, it is determined that the satellite signal may have deception interference signals [8-11].

- Testing of related peak quality

The receiver adopts a Delay Locked Loop (DLL) to track the received signal pseudocode, which means that the local pseudocode generator of the receiver generates three different phase local pseudocodes, lead code , real-time code , and lag code. If the loop can achieve stable tracking, the correlation value corresponding to the instant code should reach its maximum [12]. When the phase difference between the deception signal and the real signal is too small, the correlation peak of the deception signal overlaps with the correlation peak of the real signal. Therefore, the deception interference signal can be detected by comparing the output values of the leading, real-time, and lagging correlators [13-15].

- Detection of signal power rationality

Due to the distance between navigation satellites and the ground, the received signal is relatively weak. However, compared to the real signal, the power of deceptive interference signals is generally higher than real signal. Therefore, when the receiver receives a higher power of deceptive interference, the received signal power will be increased. Through comparing the received signal power with the preset detection threshold, the detection of deceptive interference will be achieved.

- Detection of Doppler frequency shift consistency

In fact, the relative motion between navigation satellites and receivers results in a certain Doppler frequency shift in the signal received by the receiver. The change in Doppler frequency shift can be estimated based on the receiver's altitude and velocity. The Doppler consistency detection statistic of real navigation signals is generally small. When there is a certain frequency offset in the deceptive interference signal or the RF device of the forwarding device [24], the detection statistic is generally large. Therefore, it is possible to detect deceptive interference signals based on the historical data of Doppler frequency shift.

- Detection of signal arrival angle

There are mainly two types of signal arrival angle detection. One is to use the correlation based direction finding method to actually measure the incoming direction of each satellite signal, and determine whether it is a deceptive interference signal based on the rationality of the incoming direction. Another method does not require determining the direction of each satellite signal, but it can use the spatial distribution characteristics of the array to detect the spatial correlation of each satellite signal. If there are multiple satellites with high spatial correlation, it is judged as a deceptive interference signal. If the spatial correlation is relatively scattered, it is considered as a true navigation satellite signal.

B. The proposed CNR detection method

The CNR, as one of the output statistics of the BD receiver, it is an important means of signal quality evaluation. Using the CNR as an observation to detect deceptive interference has two advantages: firstly, the CNR can be directly obtained from the output results of the receiver, which is conducive to users monitoring and statistics; Secondly, there is no need to add additional hardware equipment, which make it easy to implement.

- Method for estimating CNR

For the BD system, the CNR is basically estimated by the correlation values of the same direction and orthogonal branches after despreading the input signal. There are three common estimation methods: 1)

Moment method ; 2) Sum of variance method [16,17]; 3) Power ratio method [18,19].

(1) Moment method

This type of method calculates the second-order and fourth-order moments output by the real-time correlator, then it estimates the SNR using equation (1), and then calculates the SNR using equation (2) based on the relationship between the SNR

(SNR) value and the CNR:

$$SNR = \frac{\sqrt{2M_2^2 - M_4}}{M_2 - \sqrt{2M_2^2 - M_4}} \quad (1)$$

$$C/N_0 = SNR \times B_n \quad (2)$$

In the formula, M_2 and M_4 respectively represent the second-order and fourth-order moment estimates for the output of the correlator, and their expressions are as below:

$$M_2 = \frac{1}{N}\sum_{i=1}^{N}\left(I_i^2 + Q_i^2\right) \quad (3)$$

$$M_4 = \frac{1}{N}\sum_{i=1}^{N}\left(I_i^2 + Q_i^2\right)^2 \quad (4)$$

If the number of samples N is represented in the equation, then the CNR can be obtained from equation (5):

$$C/N_0 = 10\log_{10}(SNR) - 10\log_{10}(T_{coh}) \quad (5)$$

In the formula, T_{coh} represents the coherent integration time.

(2) Sum of variance method

For the output values of the I and Q branches in coherent integration time, the k is a time series. Assuming Z_k represents a sample amplitude sequence, it can be expressed as(6):

$$Z_k = I_k^2 + Q_k^2 \quad (6)$$

Assuming the output time interval of the CNR is KT_{coh} and K is a positive integer, then the amplitude sequence of each interval can calculate a mean $\overline{Z}$ and variance σ_Z^2, which can be expressed as follows(7) (8):

$$\overline{Z} = \frac{1}{K}\sum_{k=1}^{K} Z_k \quad (7)$$

$$\sigma_Z^2 = \frac{1}{K-1}\sum_{k=1}^{K}\left(Z_k - \overline{Z}\right)^2 \quad (8)$$

The average carrier power $\overline{P_C}$ can be calculated from the above two equations as follows (9):

$$\overline{P_C} = \left(\frac{NA}{2}\right)^2 = \sqrt{\overline{Z}^2 - \sigma_Z^2} \quad (9)$$

In the formula, N represents the number of samples and A represents the amplitude of the signal output by the RF front-end. The noise variance of in-phase and orthogonal branches is:

$$\sigma_\eta^2 = \frac{1}{2}\left(\overline{Z} - \sqrt{\overline{Z}^2 - \sigma_Z^2}\right) \quad (10)$$

The formula for calculating the CNR can be obtained through combining the above two equations:

$$C/N_0 = 10\log_{10}\left(\frac{(NA/2)^2}{2T_{coh}\sigma_\eta^2}\right) \quad (11)$$

(3) Power ratio method

This type of method estimates the SNR first, and then obtains the estimated value of the CNR from equation (2). Assuming the bandwidth of broadband power at the moment is $1/T_{coh}$, the bandwidth of narrowband power is $1/(MT_{coh})$, and M is the number of samples, the calculation formula for broadband and narrowband power is:

$$W_k = \sum_{i=1}^{M}\left(I_i^2 + Q_i^2\right) \quad (12)$$

$$N_k = \left(\sum_{i=1}^{M} I_i\right)^2 + \left(\sum_{i=1}^{M} Q_i\right)^2 \quad (13)$$

It should be noted that samples should be selected within the same navigation message bit dimension. Due to the navigation message code rate being 50Hz, if the relevant integration time is $1ms$, the maximum value is 20. The power ratio at the moment k is R_k .

$$R_k = \frac{N_k}{W_k} \quad (14)$$

In order to estimate the CNR, it is defined μ_R as the $h = K/M$ average of the power ratios and K is the number of samples in the calculation interval of the CNR. The expression of μ_R is:

$$\mu_R = \frac{1}{h}\sum_{k=1}^{h} R_k \quad (15)$$

The formula for calculating the CNR can be obtained as follows:

$$C/N_0 = 10\log_{10}\left(\frac{\mu_R - 1}{T_{coh}\left(M - \mu_R\right)}\right) \quad (16)$$

- Single satellite CNR jump detection method

In general deception and interference scenarios, in order to achieve better deception effects, the attacking party will make the power of the deception signal higher than the true signal power, which will

correspondingly cause a jump in the CNR output by the receiver. Based on this change, detection of deception interference can be achieved.In the experiment, PRN 6 and PRN 13 satellites are collected for 2 minutes each before and after applying deceptive interference at the BD B1I frequency point. The changes in CNR before and after applying deceptive interference are shown in Fig1. Similarly, data was collected for PRN13 and PRN16 satellites at the BD B3I frequency point under the same conditions. The changes in the CNR before and after applying deceptive interference are shown in Fig.2.

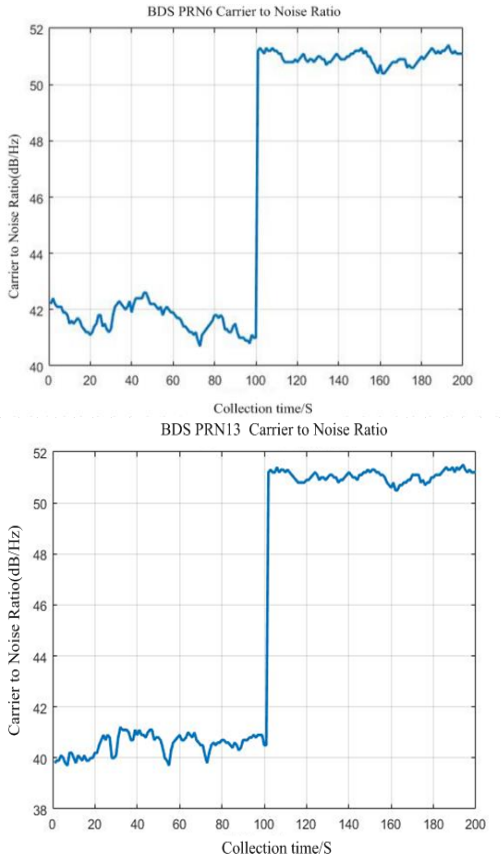
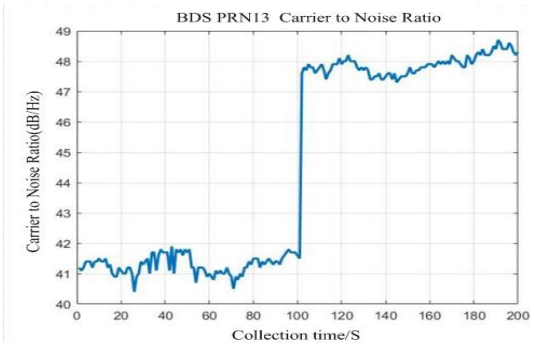


Fig. 1. *Changes in the SNR between satellite 6 and*

satellite 13 in the presence of deceptive interference



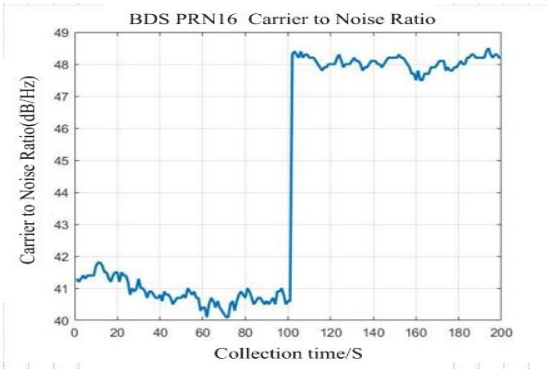


Fig. 2. *Changes in the Noise Ratio between Satellite 13*

and Satellite 16 in the Presence of Deceptive Interference

After the application of deceptive interference, the CNR of satellite signals received at frequencies B1I and B3I undergoes jumps compared to normal conditions. Although detecting the jump in CNR of a single satellite can also achieve the detection of deceptive interference signals, detecting only the abnormal CNR of a single satellite is susceptible to the impact of environmental changes and data jumps. When the receiver is in a complex environment, it cannot be determined whether the jump in CNR is caused by multipath or occlusion, or by deceptive interference, resulting in false alarms [20-22]. In order to avoid false alarms caused by data jumps caused by external factors and fully utilize the observation information of high elevation visible stars during the current observation period, in the paper, it proposes a deceptive interference detection method based on synchronous changes in CNR.

C. Multi satellite CNR detection method proposed

- K-Means clustering algorithm

K-means clustering algorithm is a classic distance based algorithm that uses distance as the evaluation criterion. The smaller the distance between two objects, the higher the similarity between them will be. Objects that are close in distance form a cluster.

The algorithm uses a given data sample X , $X=\{x_1,x_2,...,x_n\}$, which contains objects, each of which includes attributes of m dimensions. Firstly, initialize k cluster center $\{c_1,c_2,...,c_n\}$ $(1\le k\le n)$, and then calculate the Euclidean distance from each object to each cluster center :

In the formula, X_i represents the i th sample, C_j represents the j th cluster center, and t represents the order of attributes.

$$\mathrm{dis}(X_i, C_j) = \sqrt{\sum_{t=1}^{m} (X_{it} - C_{jt})} \quad (17)$$

Calculate the distance can be obtained through equation (17), then compare them with each other, and assign the samples to k clusters according to the nearest principle $\{S_1, S_2, ..., S_k\}$.

The formula for calculating cluster centers is shown in Equation (18):

$$C_t = \frac{(\sum_{X_i \in S_i} X_i)}{|S_l|} \quad (18)$$

The algorithm process can be summarized as follows:

(1) Point selection: Randomly select k samples from the sample data as initial center points;

(2) Classification: Classify clusters based on the calculated Euclidean distance from each sample to each cluster center;

(3) Iteration: Recalculate the cluster center point and repeat the previous steps until the center point converges.

- Deception interference detection method based on synchronous changes in CNR

Due to the fact that navigation satellites are located at an altitude of tens of thousands of kilometers from the ground, the CNR received under normal circumstances will not undergo significant changes for real navigation signals . In general deceptive interference environments, different deceptive interference signals are emitted by the same antenna, so after being attacked by deceptive interference, the CNR of different visible stars at the same frequency point will have the same trend of change. In test experiments, actual tests are conducted on the B1I and B3I frequency points of BD system. The CNR of visible stars at various high elevation angles has undergone significant changes before and after applying deceptive interference to the normal satellite reception through the receiver.

The CNR of visible stars before and after deception at B1I frequency point is shown in Fig.3 and 4, and the distribution of visible stars in the sky is shown in Fig.3.

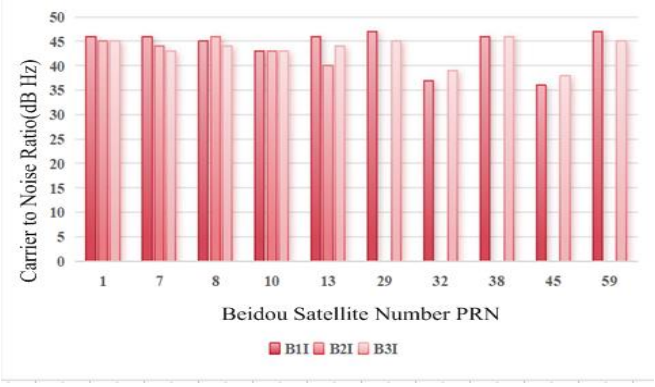


Fig. 3. *Diagram of normal satellite borne noise ratio without deception interference*

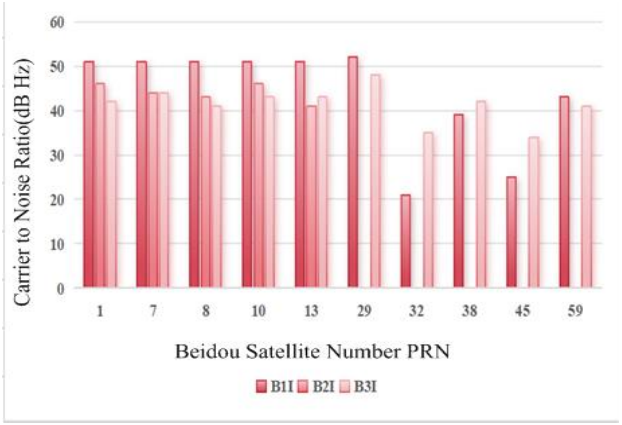
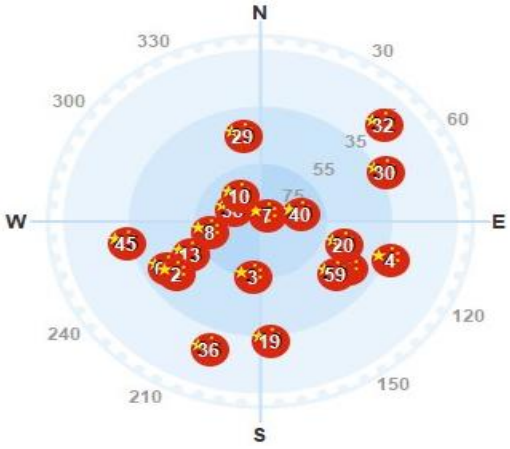
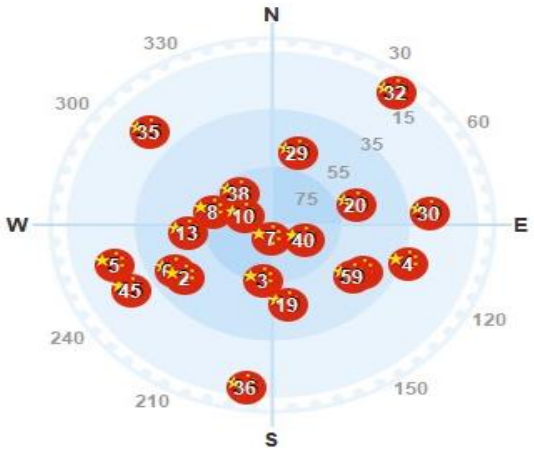


Fig. 4. *Diagram of the SNR of the receiving satellite when applying B1I frequency point deception interference*



（a）Normal distribution map of visible stars in the sky without deception



（b）Distribution map of visible stars in the sky when deceiving

Fig. 5. *B1I frequency point distribution map of visible stars in the sky*

The CNR of visible stars before and after deception at B3I frequency are shown in Fig.5 and Fig.6, and the distribution of visible stars in the sky is shown in Fig.7.and Fig.8

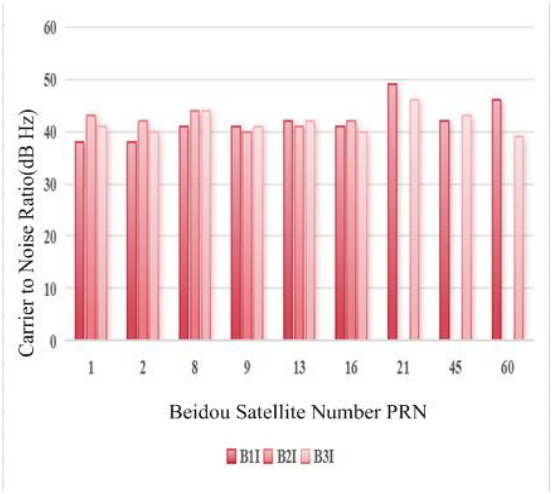


Fig. 6. *shows the normal SNR when there is no deception interference*

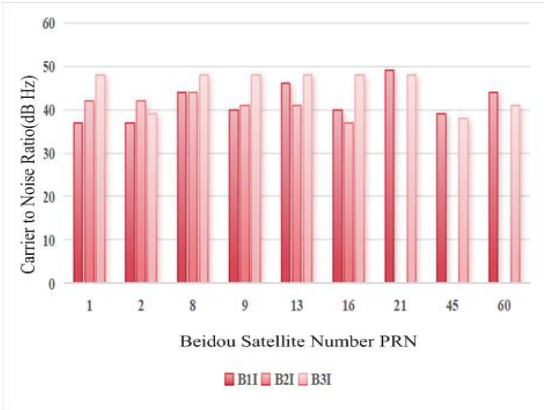
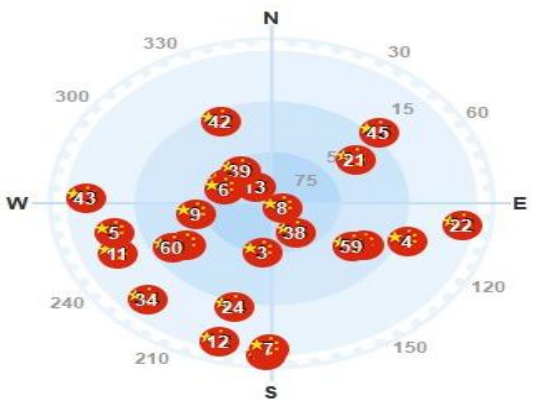
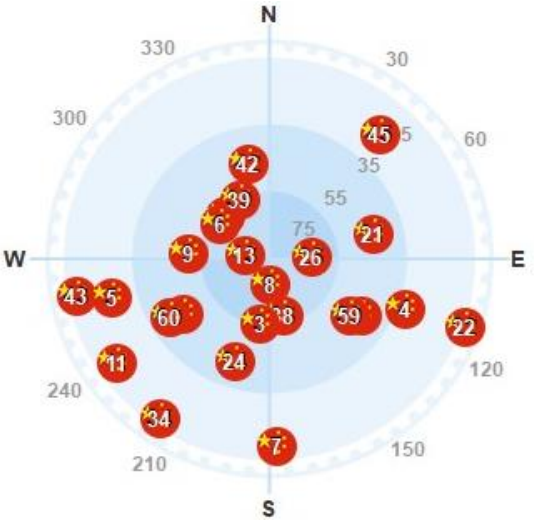


Fig. 7. *shows the SNR of the receiving satellite when B3I frequency point deception interference is applied*



（a）Normal distribution map of visible stars in the sky without deception



（b）Distribution map of visible stars in the sky when deceiving

Fig. 8. *Distribution of visible stars in the sky at B3I frequency point*

Observing the SNR of each visible satellite before and after the application of deception interference, it can be seen that the SNR of each visible satellite at the current observation frequency point changes significantly before and after the application of deception interference. The SNR of satellites 1, 7, 8, 10, 13, and 29 at B1I frequency point shows the same trend, while the SNR of satellites 1, 8, 9, 13, 16, and 21 at B3I frequency point shows the same trend, which indicates a significant increase compared to normal conditions, and the final SNR is basically the same. That is to say, regardless of the CNR of visible stars at the current observation frequency under normal circumstances, the CNR of high elevation visible stars will change to a basically identical determined range after applying deceptive interference emitted by the same antenna.

Based on this rule, in the paper, it proposes a deception interference detection method, which extracts the CNR of each visible star at the current observation frequency point in the received signal as the detection quantity. If the CNR of more than three visible stars at the current observation frequency point changes significantly and exceeds the preset detection threshold before and after applying deception interference, the K-Means clustering algorithm is adopted to analyze the CNR before and after applying deception. The method flowchart is shown in Fig.9.

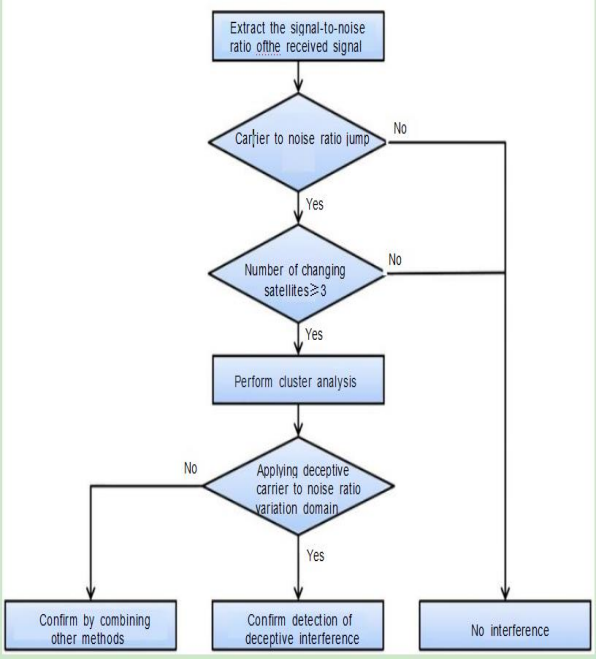


Fig. 9. *Flow Chart of Detection Method*

The cluster centers of the CNR of the i-th observation satellite before and after applying deception interference can be expressed as:

$$C_{REAL,i} = \frac{(\sum_{C_i \in S_{REAL,i}} C_i)}{|S_l|} \quad (19)$$

$$C_{SPOOFING,i} = \frac{(\sum_{C_i \in S_{SPOOFING,i}} C_i)}{|S_l|} \quad (20)$$

Among them, represents the length of the observation data interval, and then calculates the Euclidean distance from each object to the center of each cluster, compares them with each other, and allocates samples to different clusters according to the nearest principle. For the k high elevation visible stars selected at the current observation frequency, their cluster centers are basically the same after applying deceptive interference, namely:

$$C_{SPOOFING,1} \approx C_{SPOOFING,2} \approx \cdots \approx C_{SPOOFING,k} = C_{SPOOFING} \quad (21)$$

When the distance between the CNRs of these visible stars that exceed the detection threshold is less than a certain value (because the CNR of the satellite is basically a stable value in a short period of time, there may be fluctuations of 1-2 dB· Hz, so this certain value can be set to 1 dB· Hz), that is

$$\mathrm{dis}(C_i, C_{SPOOFING,i}) = \sqrt{\sum_{t=1}^{l} (C_{it} - C_{SPOOFING,it})} \le 1 \quad (22)$$

At this point, it can be considered that the CNR similarity of these satellites is high and they have all entered a cluster. This type of cluster is defined as the domain of deceptive CNR variation, and it can be determined that these signals are deceptive interference signals emitted by the same antenna. This enables the detection of high-power dominant deceptive interference signals emitted by the same interfering antenna.

- Deceptive interference direction finding method based on despreading

If the MUSIC algorithm is directly used for direction detection of deceptive interference signals, assuming that the power of the deceptive interference signal is -150dBW and the directions are 20° and 60°, the MUSIC direction finding results are shown in Fig.10.

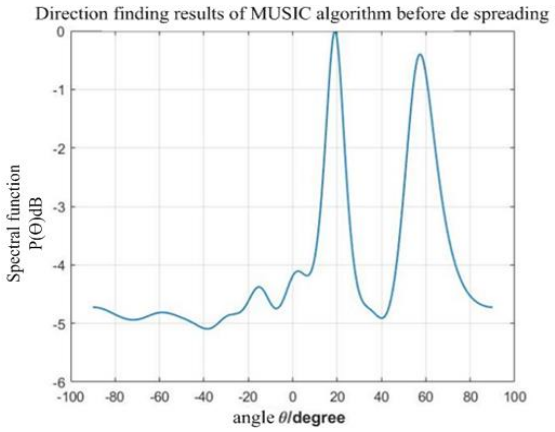


Fig. 10. *Deception interference direct direction finding result diagram*

It can be seen that using the MUSIC algorithm for direct direction finding of deceptive interference signals before despreading results in low resolution and accuracy in direction finding. This requires the BD receiver to detect the deceptive interference signals through detection methods and treat them as an "alternative" real navigation satellite signal for despreading operation, in order to improve its direction finding resolution and accuracy. The directional vector of the BD receiver array antenna can be expressed as:

$$a(\theta_i) = \left[1, e^{-j\omega_i}, \ldots, e^{-j(P-1)\omega_i}\right]^T \quad (23)$$

Among them

$$\omega_i = \frac{2\pi \sin\theta_i d}{\lambda} \quad (24)$$

In the formula, θ_i represents the direction of arrival, λ represents the wavelength of the received signal, and d represents the spacing between antenna

elements. Assuming the total number of signals received by the receiver is M, the signal received by the p-th antenna element is:

$$x_p(t)=\sum_{i=1}^{M}a_p(\theta_i)s_i(t)+n_p(t) \quad (25)$$

In the formula, $s_i(t)$ represents the received signal and $a_p(\theta_i)$ represents the directional vector of the signal i to be tested. The received signal is represented as:

$$h_p(\tau)=\sum_{i=1,i\neq j}^{M}a_p(\theta_i)q_i(t)+a_p(\theta_j)y_j(t)+n_p(t) \quad (26)$$

In the formula, j represents the jth correlated channel of the receiver, $q_i(t)$ represents the correlation result between the locally generated pseudocode in the jth correlated channel and the satellite signal with a non local channel number, and $y_j(t)$ represents the correlation result between the locally generated pseudocode in the jth correlated channel and the jth satellite signal.

In the pseudocode correlation stage, the correlation result $q_i(t)$ between the locally generated pseudocode in a channel and the satellite signal with a non channel number is much smaller than its correlation result $y_j(t)$ with the satellite signal with the channel number $y_j(t)$. Therefore $q_i(t)$ $y_j(t)$, equation (4.61) can be simplified as follows:

$$h_p^j(\tau)=a_p(\theta_j)y_j(t)+n_p(t) \quad (27)$$

Combine the data from the jth channel of P antenna elements into a data vector:

$$H^j(\tau)=\left[h_1^j(\tau),...,h_P^j(\tau)\right]^H \quad (28)$$

The covariance matrix after correlation is:

$$R_{hh}^j=E\left[H^j(t)H^j(t)^H\right]=AR_{yy}A^H+\sigma_N^2I \quad (29)$$

$$R_{yy}=E\left[y_j(t)y_j(t)^H\right] \quad (30)$$

The covariance matrix of the complex envelope of the signal R_{yy}, I is the P dimensional identity matrix, and the noise power σ_N^2. After arranging the feature vectors of feature decomposition in descending order of eigenvalues, the (31) can be obtained.

$$R=U_s\sum_s U_s^H+U_n\sum_n U_n^H$$
$$=\sum_{m=1}^{K}\lambda_m e_m e_m^H+\sum_{m=K+1}^{M}\lambda_m e_m e_m^H \quad (31)$$

At this point, the spatial spectrum can be constructed from equation (31) for peak search, achieving estimation of the signal direction.

Assuming that the power of the deceptive interference signal is -150dBW and the directions are 20° and 60°, respectively, after despreading the deceptive interference signal, the despreading gain $G=46.12dB$ obtained through despreading is analyzed by equation (4) At this time, the direction finding result of the deceptive interference signal is shown in Fig.11.

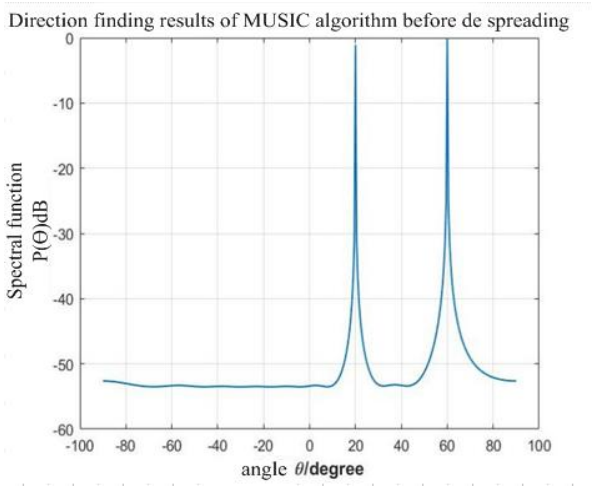


Fig. 11. *Deception interference direction finding result diagram after despreading*

By comparing Fig.10 and 11, it can be seen that the direction finding resolution of deceptive interference signals significantly increases after despreading. By treating deceptive interference signals as an alternative real navigation signal and performing normal spreading operations on them, the obtained amplification benefits can be fully utilized to improve direction finding resolution and accurately evaluate the direction of deceptive interference signals.

III. EXPERIMENTAL VERIFICATION OF DECEPTIVE INTERFERENCE DETECTION AND DIRECTION FINDING EVALUATION

In the previous sections, the multi correlation peak detection method and the CNR synchronous change detection method were used to detect the deceptive interference received by the BD system in the capture and tracking stages of the BD receiver. Then, in response to the low signal strength of deceptive interference signals threatening the BD system, which are close to real navigation signals, and the characteristics of multiple signals on the same frequency, a spatial spectrum estimation direction finding method based on despreading was adopted to improve the accuracy of evaluating deceptive interference signals by obtaining despreading gains. By designing a BD deceptive interference detection and direction finding receiver scheme, the detection

and direction finding evaluation of deceptive interference signals in the BD system are achieved, and experimental testing is conducted in an outdoor environment.

A. Deceptive interference detection and direction finding receiver scheme

For deceptive interference signals, whether they are generative or forwarding deceptive interference signals, they can be regarded as an "alternative" real navigation signal. They can be captured and tracked normally like general real navigation signals, and the direction of deceptive interference signals can be evaluated after obtaining the spreading gain.

Based on the deception interference detection and direction finding methods introduced in the previous two chapters, this section designs a receiver scheme to achieve detection and direction finding evaluation of deception interference signals in the BD system.

Firstly, the signal received by the antenna array is passed through a low noise amplifier and a band-pass filter, and then down converted into a base-band signal that is easy for the receiver to process. At this time, the received signal may contain deceptive interference signals. In the capture phase, the multi correlation peak detection method is used to detect the channels of each numbered satellite separately. When two correlation peaks are detected, a standby tracking channel is activated, and the receiver is changed from one tracking channel to two tracking channels for this numbered satellite. The signals corresponding to the detected two correlation peaks are tracked separately. In the tracking phase, the detection of deceptive interference signal channels is achieved through the CNR synchronous change detection method. At this time, the two tracking channels correspond to the real navigation signal and the deceptive interference signal, respectively. The deceptive interference signal channel obtains a 46.12dB despreading gain after despreading. At this time, the MUSIC method is used to detect and evaluate the direction of deceptive interference signals.

B. Experimental Environment Construction

In order to verify the effectiveness of the design scheme in this article, experimental environments were set up outside Guangzhou and Shijiazhuang for experimental verification. The experimental locations and environments are shown in Fig.12 and Fig.13, respectively.

Fig. 12. *Field experiment location*

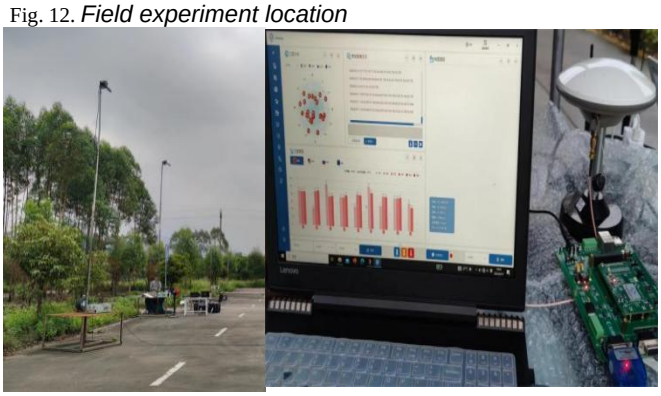


Fig. 13. *Outdoor experimental environment*

Choose an unobstructed open area for the outdoor location to ensure the stability of the received signal and sufficient number of visible satellites during the observation period. The equipment used to build the experimental environment is as follows:

1) Five NGS4000 multifunctional interference sources for satellite navigation;

2) One multi-functional portable interference source NGS4010 for satellite navigation;

3) Six right-handed polarized transmission antennas;

4) Six omnidirectional antennas used to deceive interference sources for satellite reception;

5) Seven mobile power supplies;

The deception interference source equipment used in the experiment is shown in Fig.13.

Distribute 6 deceptive interference sources around the experimental site, with each deceptive interference source equipped with a right-handed polarized transmitting antenna and an omnidirectional antenna for satellite reception.

Firstly, the external omnidirectional antenna of the deceptive interference source is connected to the sky for normal satellite reception. After waiting for the deceptive interference source to successfully update the internal stored ephemeris information, one can choose whether to use the built-in ephemeris to transmit generative deceptive interference or use the external omnidirectional antenna to transmit forward deceptive interference after real-time satellite reception.

The experimental steps are as follows:

1) Deceptive interference source equipment powering on;

2) Calibrate the transmission loss from antenna transmission power to receiving antenna interface power;

3) Select one of the six deception interference source devices and use the built-in ephemeris to transmit a generative deception interference signal for the B1I frequency point. Adjust the output power of the deception interference source so that the power of the deception interference signal to the receiver antenna interface is -120dBm~-110dBm, and record the actual azimuth angle of the deception interference source transmission antenna relative to the receiver antenna at this time;

4) Record the detection results of the receiver's multi correlation peak detection method and the CNR synchronous change detection method at this time;

5) Select one of the six deceptive interference source devices and use an external antenna to transmit a forwarding deceptive interference signal targeting the B3I frequency point in real-time after receiving the satellite. Adjust the output power of the deceptive interference source so that the power of the deceptive interference signal to the receiver antenna interface is -120dBm~-110dBm, and record the actual azimuth angle of the deceptive interference source transmission antenna relative to the receiver antenna at this time;

6) Record the detection results of the receiver's multi correlation peak detection method and the CNR synchronous change detection method at this time;

7) If deceptive interference signals are detected in steps 4 and 6, perform direction finding on the deceptive interference signals and record the direction finding results.

8) Compare the direction finding results with the actual azimuth angle and record the direction finding error for this time.

Results

The actual data results of the CNR of visible stars 1, 3, 8, 10, and 13 at the B1I frequency point of the BD system before and after the application of deception interference are shown in Fig.14.

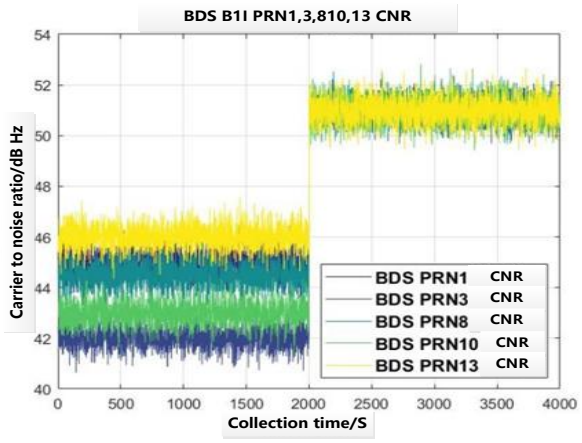


Fig. 14. *Schematic diagram of satellite carrier to noise ratio changes at frequency points PRN1, 3, 8, 10, and 13 of BD B1I*

By observation, the approximate CNR of the 5 visible stars selected for B1I frequency point before and after deception is shown in Table.1.

Tab.1 B1I frequency points PRN1, 3, 8, 10, and 13 show the approximate CNR of visible stars

B1I frequency point satellite PRN	Normal circumstances, the SNR/dB·Hz	Apply deceptive SNR/dB·Hz
1	45	51
3	42	51
8	44	51
10	43	51
13	46	51

Through analyzing the data results, it can be seen that under normal circumstances, the CNR of visible star signals with different numbers is basically stable around a certain value, but there are also differences due to the different elevation angles of visible stars. However, after applying deceptive interference, the CNR of high elevation visible stars is enhanced to a certain extent, and the CNR ultimately overlaps within the same numerical range. That is, when applying deceptive CNR variation range, it can be determined that the receiver has been subjected to deceptive interference at this time.

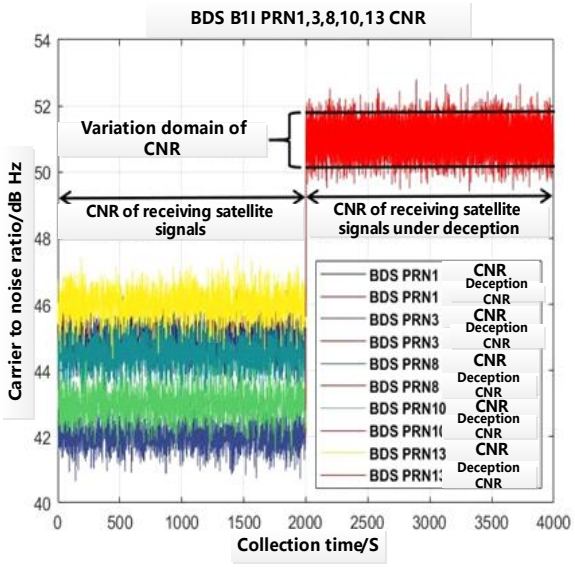


Fig. 15. *Schematic diagram of deception carrier to noise ratio variation domain applied to B1I frequency point*

Similarly, for the B3I frequency point, the actual data results of the CNR of satellites 1, 8, 13, 16, and 21 are shown in Fig.15.

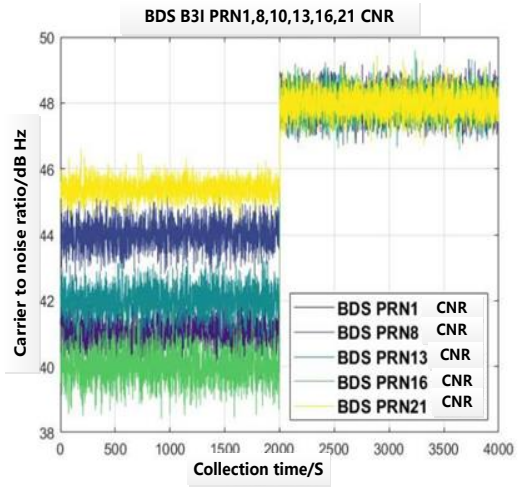


Fig. 16. *Schematic diagram of changes in carrier to noise ratio of BD B3I frequency points PRN1,8,13,16,21 satellites*

The approximate CNRs of the 5 visible stars selected for B3I frequency point before and after deception are shown in Table.2.

Tab.2 shows the approximate CNR of visible stars at B3I frequency points PRN1, 8, 13, 16, and 21

B1I frequency point satellite PRN	Normal circumstances, the SNR/dB·Hz	Apply deceptive SNR/dB·Hz
1	41	48
8	44	48
13	42	48
16	40	48
21	45	48

The schematic diagram of the variation domain of the applied deception CNR at B3I frequency point is shown in Fig.17.

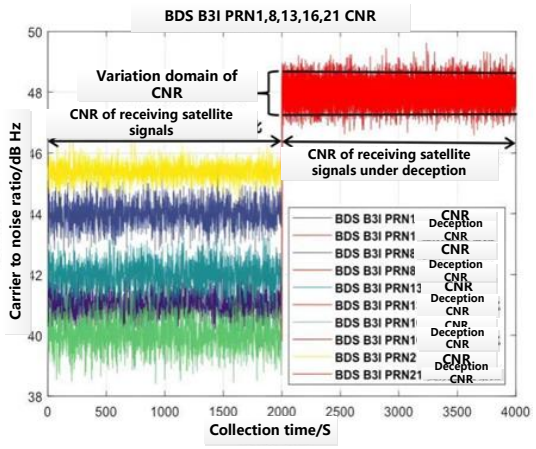


Fig. 17. *Schematic diagram of the variation domain of deception CNR applied at B3I frequency point*

The results of the B3I frequency point are similar to those of the B1I frequency point, and after applying deception, the CNR of visible stars at all high elevations overlap within the same numerical range.

Using the CNR of satellite signals as an observation, K-means algorithm is used for clustering analysis. Firstly, the CNR of each satellite under normal receiving conditions is treated as a cluster without deceptive interference. Then, after applying deceptive interference, the distance to the center of the deceptive CNR change domain is set to 1dBHz. After clustering analysis, if the CNR of these high elevation visible stars that exceed the detection threshold during the observation time fall within the deceptive CNR change domain, they are divided into another cluster, namely the deceptive interference change domain, to achieve detection of deceptive interference.

C. Discussion

Cluster detection was performed on the actual collected data of B1I frequency point and B3I frequency point before and after applying deception interference for 1 minute each in the actual experimental environment. The schematic diagrams of the results are shown in Fig18 and Fig19, respectively:

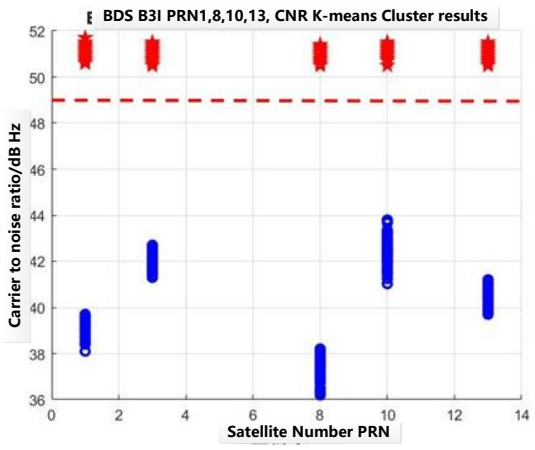


Fig. 18. *Schematic diagram of B1I frequency clustering detection results*

Through observing the visible SNR of each satellite during the normal receiving time period of B1I frequency point, a certain value slightly higher than the SNR of each satellite is determined as the detection threshold, as shown in the red dashed line in Fig18. During the current observation time period, the detection threshold is set to 49dBHz, and the SNR exceeding this threshold are clustered and analyzed to form a deception cluster. From the figure, it can be seen that after using K-Means clustering, the original data is divided into two clusters, namely the blue no deception interference and the red deception cluster. It can be seen that the variation domain of the deception SNR applied to B1I frequency point at this time is 511dBHz, and the first cluster is selected. The CNR of the five high elevation visible stars, 3, 8, 10, and 13, after being deceived, all fall within the variation range of the deceived CNR, indicating the detection of deceptive interference.

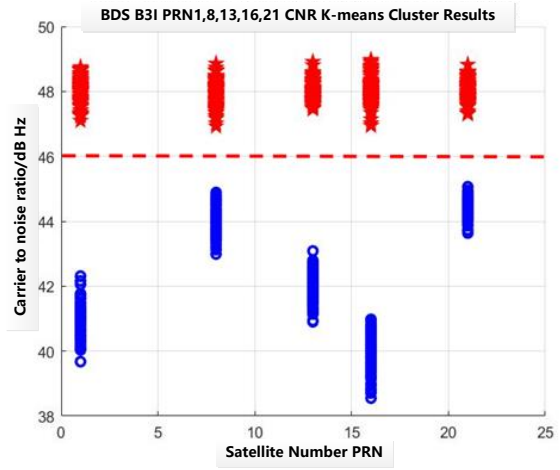


Fig. 19. *Schematic diagram of B3I frequency clustering detection results*

Similarly, by observing the CNR of each visible star during the normal receiving time period of B3I frequency point, 46dBHz was determined as the detection threshold. As shown by the red dashed line in Fig.18, it can be seen that the variation domain of the CNR under deception at B3I frequency point is 481dBHz. The CNR of the first, eighth, thirteenth, sixteenth, and twenty-first high elevation visible stars under deception fall within this variation domain, which indicates the detection of deception interference.

Firstly, it makes the receiver receive real navigation signals in the sky normally. Observe the status and CNR of each satellite received through the receiver software interface. Under normal circumstances, the CNR of each satellite signal received varies according to the elevation angle of the receiving satellite, as shown in Fig20.

Fig. 20. *Under normal circumstances, receive the SNR of each satellite*

At this time, it was observed that at least 6 visible stars at the B1I frequency point had their CNRs falling within the range of the applied deceptive CNR. An alarm was triggered to detect deceptive interference signals.

According to experimental steps, the deception interference source is connected to an omnidirectional antenna for real-time satellite reception, and a forwarding deception interference signal is transmitted for the B3I frequency point. The multi-correlation peak detection results of the receiver displayed by the serial port debugging assistant At this time, the receiver alarm detects the deception interference signal, and the receiver software interface displays the CNR of each satellite received BD B3I frequency point,

It can be seen that at this time, at least 6 stars under the B3I frequency point have a CNR that is within the range of applied deceptive CNR, indicates the detection of deceptive interference. At this time, an alarm is issued to detect deceptive interference signals. Record the actual azimuth angle of the deception interference source transmitting antenna relative to the receiver antenna at this time. The azimuth angle of the deception interference signal measured by the receiver is shown as in Fig.21.

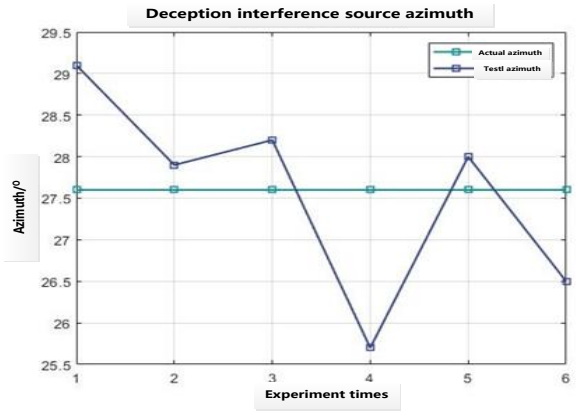


Fig. 21. *Deception of interference source azimuth angle*

It can be seen that in the 6 experiments, the receiver's direction finding evaluation error for deceptive interference sources is all less than, 3° which meets the general direction finding accuracy requirements, and it can achieve direction finding evaluation for deceptive interference signals. From Fig.22, it can be seen that the accuracy distribution of direction finding evaluation after despreading the deceptive interference signal is between 96.67% and 98%, which is significantly higher than the accuracy of direction finding before despreading, it can meets the general requirements for direction finding evaluation of deceptive interference signals.

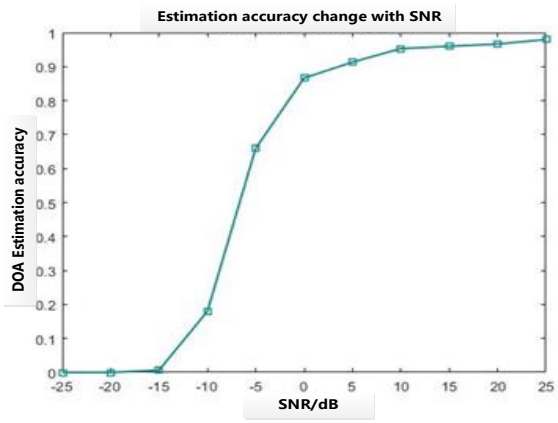


Fig. 22. *Accuracy Curve of Deceptive Interference Direction Finding Evaluation*

3. CONCLUSION

For the common deceptive interference signals in the BD satellite navigation system, it detects deceptive interference signals from the receiver capture stage and the tracking stage, respectively. This article uses the K-Means clustering algorithm to propose a deceptive interference detection method based on synchronous changes in CNR. By utilizing the CNR observation information of all high elevation visible stars during the current observation period, a deceptive CNR variation domain is defined. When the CNR of multiple high elevation visible stars enters this variation domain, it can be determined that the receiver is affected by deceptive interference at this time.

Due to the fact that deceptive interference signals can be regarded as an "alternative" real navigation signal, and the signal strength is similar to the real navigation signal, the accuracy and precision of direct direction finding evaluation are very poor. It first analyzes the despreading gain of the BD receiver, and then selects the MUSIC method as the direction finding method based on the performance comparison of CBF method, Capon method, MUSIC method, and ESPRIT method. A deceptive interference direction finding method based on despreading is used for direction finding evaluation. Simulation results show that this method can significantly improve the resolution and accuracy of direction finding evaluation for deceptive interference. Finally, in practical applications, in order to save system costs and volume, a switch matrix structure is used to select different antenna elements in different time intervals in the receiving channel and restore the complete covariance matrix. Nine elements of spatial spectrum estimation direction finding are achieved through three receiving channels.

A deceptive interference detection and direction finding receiver scheme for the BD system was designed. After receiving and capturing the received signal uniformly, one tracking channel of the original receiver was transformed into two tracking channels based on the detected multiple correlation peaks. The signals corresponding to the two correlation peaks were tracked separately. In the tracking stage, the detection method of synchronous changes in CNR was used to determine the true navigation signal channel and the deceptive interference signal channel. After code stripping, decoding, and spreading in the receiver, detection and direction finding evaluation of deceptive interference signals in the BD system are achieved, and experimental tests are conducted in the field. The evaluation accuracy of deceptive interference signals is less than, and the accuracy of direction finding evaluation after despreading is distributed between 96.67% and 98%, which has good detection and direction finding evaluation effects.

LIST OF ABBREVIATIONS

BD =BeiDou

SNR= Signal to Noise Ratio

CNR= CNR

PVT=Position Velocity and Time

GNSS=Global Navigation Satellite System

BDS=BeiDou Navigation Satellite System

DLL=Delay Locked Loop

IV. REFERENCES

[1] Deng Xu Research on GNSS Deceptive Interference Detection Method Based on CNR Zhengzhou: Strategic Support Force Information Engineering University, 2023

[2] Wang Xuxu Research on Detection and Suppression Methods of Beidou Deception Interference Hangzhou: Hangzhou University of Electronic Science and Technology, 2021.

[3] Hoey D, Benshoof P. Civil GPS systems and potential vulnerabilities[. Proceedings of the 18th International Technical Meeting of the Satellite

Division of the Institute of Navigation, 2005: 1291-1295.

[4] Liu Ruihua, Wang Jing Assessment of the Impact of Interference on the Reception Performance of Beidou Signals ,Journal of Civil Aviation University of China, 2019, 37 (03): 1-4, 16

[5] Zhang Yao Research on Beidou forwarding deception interference detection technology Harbin: Harbin Engineering University, 2019

[6] Wang Wei, Zhao Yanlei Overview of Satellite Navigation Terminal Adversarial Technology Digital Technology and Applications, 2020, 38 (11): 37-40

[7] Hu Yuan Research on GPS Interference in Navigation Warfare Space Electronics Technology, 2009 (04): 48-52.

[8] Wang Xuan, Tang Bin, Zheng Chong, et al. Overview of Satellite Navigation Receiver Deception and Anti Deception Technologies, Proceedings of the 12th China Satellite Navigation Annual Conference Beijing: Academic Exchange Center of China Satellite Navigation System Management Office, 2021

[9] O'Hanlon B.W., Psiaki M.L., Bhatti, J.A., et al. Real-time GPS spoofing detection via correlation of encrypted signals(Article). Navigation, Journal of the Institute of Navigation, 2013, 60(4): 267-278.

[10] Zhang Lundong, Zhang Chao, Gao Yangjun Satellite Navigation Deception and Detection (Part 1): Typical Events and Development of Deception Technologies, Journal of Navigation and Positioning, 2021, 9 (03): 1-7.

[11] Zhou Yan, Wang Shanliang, Yang Wei, etc Overview of GNSS Deceptive Interference Detection , Computer Engineering and Applications, 2022, 58 (11): 12-22.

[12] Zou Yunfei, Yang Junping, Wang Haochen, etc GNSS Comprehensive Monitoring, Direction Finding, Analysis and Evaluation Technology for Complex Electromagnetic Environment Navigation positioning and timing, 2021, 8 (05): 88-95.

[13] Zhang Xin Research on Key Technologies for Simulation and Detection of Satellite Navigation Deception Interference Signals Changsha: University of Defense Science and Technology, 2017.

[14] Fan Guangwei, Wei Baoguo, Deng Zhixin Research on Beidou deception interference detection technology based on cyclic correlation capture Satellite Navigation Positioning and Beidou System Application 2014- Strengthening Beidou Industry's Innovative Location Services China Satellite Navigation and Positioning Association, 2014.

[15] Zhang Yao Research on Beidou forwarding deception interference detection technology Harbin: Harbin Engineering University, 2019

[16] Li Juanli, Liang Liming, Zhang Hua A GPS signal forwarding deception interference detection technology Modern Navigation, 2017, 253-256

[17]]WANG F, LI H, LU M Q. GNSS spoofing detection and mitigation based on maximum likelihood estimation. Sensors, 2017, 17(7): 1532.

[18] PHELTS R E. Multi-correlator techniques for robust mitigation of threats to GPS signal quality. Stanford: Stanford University, 2001.

[19] PINI M, FANTINO M, CAVALERI A, et al. Signal quality monitoring applied to spoofing detection. Proc.of the Institute if Navigation GNSS Meeting, 2001.

[20] Dehghanian V, Nilsen J, Lachapelle G. GNSS Spoofing Detection based on Receiver C/N0 Estimates. Proceedings of the 25th International Technical Meeting of the Satellite Division of the Institute of Navigation(ION GNSS 2012), Nashville, TN: The Institute of Navigation, 2012:2878-2884.

[21] WEN Heng-qing, HUANG P Y I, DYER J. Countermeasures for GPS Signal Spoofing. Proceedings of the 18th International Technical Meeting of the Satellite Division of the Institute of Navigation(ION GNSS 2005), Nashville, TN: The Institute of Navigation, 2005.

[22] Jafarnia-jahromi A, Broumandan A, Nilsen J, et al. GPS Spoofer Countermeasure effectiveness based on signal strength, noise power, and C/N0 measurements. International Journal of Satellite Communications and Networks, 2012, 30(4): 181-191.