IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Traitement du Signal
Vol. 41, No. 4, August, 2024, pp. 1981-1989
Journal homepage: http://iieta.org/journals/ts

A Repeater Deception Jamming System Based on High Gain Antenna Array Spatial Separation Receiving

Zhichun Dai[1], Ding Pan[1], Peng Wu[2,3,4*], Lanxia Xu[1], Jing Li[1]

[1] Hunan Satellite Navigation Information Technology Company, Changsha 410006, China
[2] Xi'an Key Laboratory of Integrated Transport Big data and Intelligent Control, Xi'an 710064, China
[3] College of Electronic Communication and Electrical Engineering, Changsha University, Changsha 410022, China
[4] Hunan Province Navigation and Attitude Measurement Integrated Application Engineering Technology Research Center, Changsha 410022, China

Corresponding Author Email: wupeng@ccsu.edu.cn

https://doi.org/10.18280/ts.410427

Received: 20 March 2024
Revised: 6 June 2024
Accepted: 28 June 2024
Available online: 31 August 2024

Keywords:
high gain antenna array, satellite navigation, spatial separation, repeater deception jamming, preferred star strategy

ABSTRACT

Aiming at the problems of high cost and high-power consumption of the existing repeater satellite navigation deception jamming system, a repeater deception jamming system based on high gain antenna array spatial separation reception is designed. Through eight sets of high-gain parabolic antennas, the appropriate satellite is selected to obtain a single satellite signal, and then the time delay of each satellite signal is accurately controlled according to the spoofing position point, and the pseudo-range information is changed. Finally, the target receiver is transmitted to the target receiver in a combined way to achieve the purpose of deception. At the same time, in order to ensure the effectiveness of the interference, combined with the satellite space geometry, the optimal satellite strategy algorithm is designed. Field experiments show that the system can successfully deceive typical receivers.

1. INTRODUCTION

The satellite navigation system offers the advantages of wide coverage and high positioning accuracy, and has been extensively utilized in both civilian and military domains [1]. However, owing to the vulnerability of the satellite navigation system, the signal is prone to interference during transmission, especially deception interference, which does not require excessive power and exhibits good concealment, posing a significant threat to the satellite system [2]. GNSS anti-spoofing interference technology is a prominent issue in the field of satellite navigation both domestically and internationally. Nevertheless, unlike suppression interference, anti-spoofing interference methods are generally not universal. The flexible and variable nature of spoofing interference modes determines the diversity of anti-spoofing interference methods. Therefore, it is imperative to focus on the research of spoofing interference methods [3].

According to the method of generating deception signals, deception jamming is divided into two categories: generative deception and forwarding deception [4]. Generative spoofing refers to a spoofing signal that is generated by the spoofing device, consistent with the real GNSS signal format, and then transmitted by the transmitting device [5]. This method requires a comprehensive understanding of the pseudo-code type, encryption method, and navigation message content of satellite navigation signals, making it applicable only to civil navigation signals with an open format [6]. For authorized navigation signals whose message format is not publicly available, only the for-warding deception method can be utilized [7].

Few studies on forwarding navigation spoofing technology are available in foreign literature, while some achievements have been made in domestic research on this topic [8]. Zhang [9] proposed an intelligent forwarding deception jamming technology based on low-orbit satellites. The forwarding station is arranged on low-orbit satellites, which can effectively enhance the range and concealment of deception jamming. Ghanea et al. [10] proposes an algorithm that incorporates core components such as multispectral binary filtering, sub-clustering and single binary filtering, multi-conditional region growing, and post-processing, achieving the extraction of images such as buildings in complex and interfering scenes like urban areas. Shi et al. [11] presented a satellite selection method based on the common GNSS positioning satellite selection method and the satellite's contribution value to the position dilution of precision (PDOP) to select the forwarded satellite. The probability of selecting the optimal result can reach 87.42% and 100%. Zhao et al. [12] proposed a forwarding deception jamming method for the GNSS clock of the target receiver. By adjusting the forwarding delay, the clock of the target receiver is deceived without affecting its position. Schmidt et al. [13] addressed the nature of threat scenarios against common targets, investigated practical impediments to carrying out spoofing attacks, and surveyed the effectiveness of proposed defenses. Zheng et al. [14] proposed a forwarding interference delay algorithm that calculates the delay of different satellite signals according to forwarding coordinate requirements. This algorithm achieves the purpose of adjusting the forwarding coordinate in real-time based on the deception strategy, improving the success rate of interference. Jafarnia-Jahromi et al. [15] proposed the investigation of vulnerability of GPS to a spoofing attack and discussion of different spoofing generation techniques will be. An anti-spoofing techniques and their performance in terms of spoofing detection and spoofing mitigation were provided. And also discussed the limitations of anti-spoofing algorithms. The paper [16] proposed a multichannel position broadcast solution for UAVs, implemented on inexpensive Wi-Fi modules, achieving reliable location updates and demonstrating practical applicability.

This paper introduces a cost-effective forwarding deception jamming system that uses spatial separation reception with a high-gain antenna array. Eight high-gain parabolic antennas track a single satellite for spatial stripping and delayed forwarding to deceive targets. The paper details a method for synchronizing system clocks using a built-in receiving module that utilizes the PPS signal and a 10 MHz clock signal to synchronize the local clock with the actual satellite system. Additionally, to reduce costs associated with high-gain antennas and to enhance the impact on the targeted receiver, an optimal star strategy algorithm based on satellite spatial geometry is developed. The satellite that locates the target receiver is chosen as the forwarding satellite.

2. DESIGN OF REPEATER DECEPTION JAMMING SYSTEM

2.1 Repeater deception signal model

The core problem of repeater deception jamming lies in controlling the delay of the repeater signal, such that the target receiver calculates incorrect coordinates based on the positioning equation, ultimately achieving the objective of deception jamming [17]. The principle of repeater deception jamming is illustrated in Figure 1.

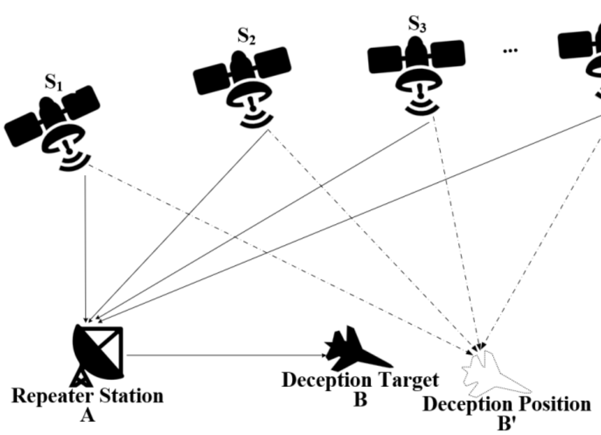


Figure 1. Schematic diagram of repeater deception jamming

The equation for repeater deception jamming is as follows:

$$\begin{cases} \rho_1 = |S_1A| + |\mathrm{AB}| + ct_1 + ct_u \\ \rho_2 = |S_2A| + |\mathrm{AB}| + ct_2 + ct_u \\ \qquad \vdots \\ \rho_i = |S_iA| + |\mathrm{AB}| + ct_i + ct_u \end{cases} \tag{1}$$

where, $\rho_i (i = 1,2,3...)$ represents the pseudo-range calculated based on the forwarded signal, $|S_iA| (i = 1,2,3...)$ represents the actual distance between the participating positioning satellites and the repeater station, $|AB|$ represents the actual distance between the forwarding station and the target receiver, $t_i (i = 1,2,3...)$ represents the artificial delay added to each satellite signal, t_u represents the clock difference between the satellite clock and the target receiver clock.

To mislocate the target receiver to a specific point, the repeater deception jamming equation must be satisfied:

$$\begin{cases} \rho_1 = |S_1B'| + ct_u \\ \rho_2 = |S_2B'| + ct_u \\ \qquad \vdots \\ \rho_i = |S_iB'| + ct_u \end{cases} \tag{2}$$

where, $|S_iB'| (i = 1,2,3...)$ represents the true distance between the satellite and the deception point B', we are:

$$\begin{cases} |S_1B'| = |S_1A| + |AB| + ct_1 \\ |S_2B'| = |S_2A| + |AB| + ct_2 \\ \qquad \vdots \\ |S_iB'| = |S_iA| + |AB| + ct_i \end{cases} \tag{3}$$

Thus, the amount of artificial time delay can be determined as follows:

$$\begin{cases} t_1 = (|S_1B'| - (|S_1A| + |AB|)) / c \\ t_2 = (|S_2B'| - (|S_2A| + |AB|)) / c \\ \qquad \vdots \\ t_i = (|S_iB'| - (|S_iA| + |AB|)) / c \end{cases} \tag{4}$$

2.2 Overall system design

The overall design of the repeater deception jamming system, which is based on high-gain antenna array spatial separation reception, is illustrated in Figure 2. It includes the spatial separation receiving unit, the repeater deception signal generation unit, the deception transmitting unit, and the repeater deception jamming software.

The repeater deception signal generation unit receives the real navigation signals from the sky, completes time synchronization with the sky, and simultaneously obtains the real ephemeris data for the repeater deception jamming software. The repeater deception jamming software controls the spatial separation receiving unit to collect 8-channel satellite navigation signals from different directions in the sky according to the jamming strategy. The repeater deception signal generation unit generates the forwarding deception signals through time-delay calculation and control of the collected and received 8-channel signals. The deception launching unit then wirelessly radiates the forwarding deception signal to construct the forwarding deception test environment.

The overall technical indicators of the system are as follows:

(1) Forwarding frequency: B3;

(2) Maximum number of satellites that can be forwarded simultaneously: ≤ 8;

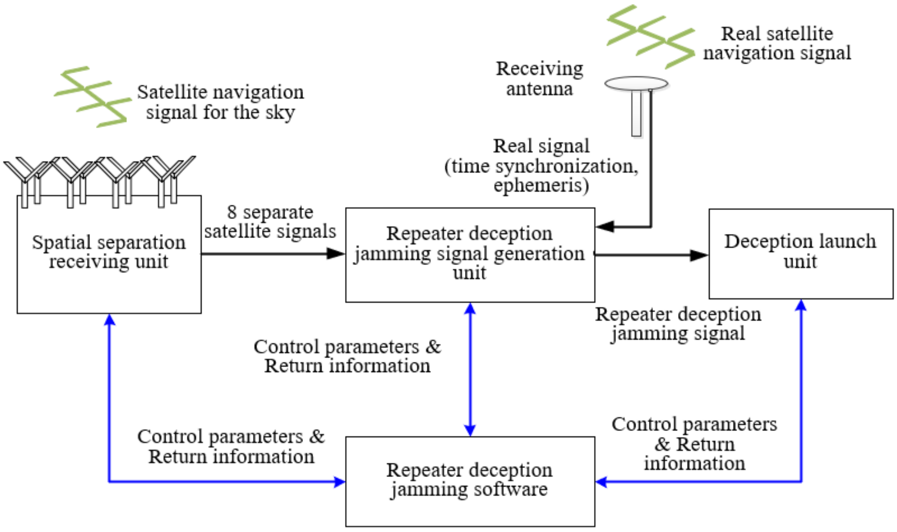
(3) Receiving antenna gain: 20dBi;

(4) Forwarding antenna coverage: azimuth 0°~360°, pitch 30°~90°;

(5) Forwarding spoofing signal delay: < 1ms;

(6) Time delay control accuracy: ≤ 1ns;

(7) Noise coefficient: 2dB.



Satellite navigation signal for the sky
Real satellite navigation signal
Receiving antenna
Real signal (time synchronization, ephemeris)
Spatial separation receiving unit
8 separate satellite signals
Repeater deception jamming signal generation unit
Deception launch unit
Repeater deception jamming signal
Control parameters & Return information
Control parameters & Return information
Control parameters & Return information
Repeater deception jamming software

Figure 2. Structural of the system

2.2.1 Spatial separation receiving unit

The spatial separation receiving unit is primarily utilized for spatial separation and simultaneous reception of multiple real navigation signals. Considering the development difficulty and economy comprehensively, the spatial separation receiving unit employs 8 high-gain parabolic antennas, with the receiving antenna array consisting of a turntable, to achieve directional reception of satellite navigation signals in 8 regions of the sky. The single set of high-gain parabolic antenna and antenna turntable adopts an integrated structural design. The antenna turntable is remotely controlled by the forwarding and deception interference software, with a running speed of over 50°/s and a control accuracy of less than 1°. The installation effect of a single set of high-gain directional antenna with turntable is shown in Figure 3.

2.2.2 Repeater deception signal generation unit

The repeater deception signal generation unit is primarily utilized for time delay and power processing of the signal to achieve flexible and configurable forwarding spoofing signal generation. The repeater deception signal generation unit comprises forwarding interference control software, a down-conversion RF module, a signal processing motherboard, an up-conversion RF module, a crystal module, and a navigation receiving antenna. The block diagram is presented in Figure 4.

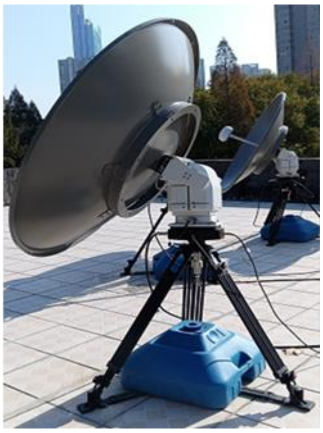
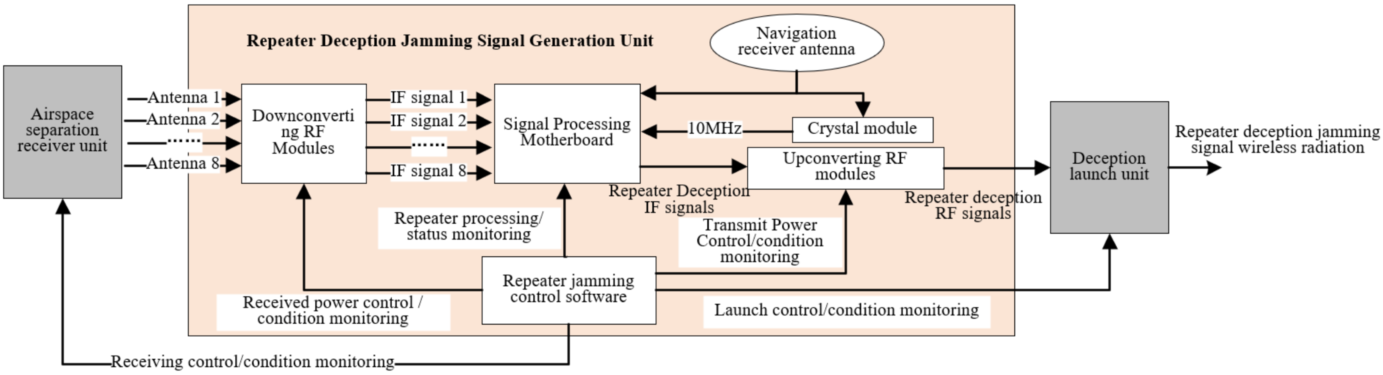


Figure 3. Receiving platform



Repeater Deception Jamming Signal Generation Unit
Navigation receiver antenna
Airspace separation receiver unit
Antenna 1
Antenna 2
......
Antenna 8
Downconverting RF Modules
IF signal 1
IF signal 2
......
IF signal 8
Signal Processing Motherboard
10MHz
Crystal module
Upconverting RF modules
Deception launch unit
Repeater deception jamming signal wireless radiation
Repeater Deception IF signals
Repeater deception RF signals
Repeater processing/ status monitoring
Transmit Power Control/condition monitoring
Repeater jamming control software
Received power control / condition monitoring
Launch control/condition monitoring
Receiving control/condition monitoring

Figure 4. The forwarded spoofing signal generation unit

The signal processing motherboard serves as the core of the forwarding deception signal generation unit. Its hardware primarily consists of an FPGA+GPU circuit, A/D and D/A converters, a navigation receiver module, time-frequency circuits, etc. The main function is to receive the IF signal band-pass sampling, subsequently send it to the FPGA chip for digital filtering and forwarding time-delay control, and then transmit the data processed by the FPGA to the GPU for further processing. The GPU completes various control logic and generates a range of forwarding deception interference styles using algorithms.

2.2.3 Deception launch unit

The deception transmitting unit is primarily utilized for broadcasting and forwarding deception signals. Given that when the system transceiver operates simultaneously, the equipment may experience self-excitation, in order to meet the spatial distance requirements for deception transmitting transceiver isolation, the deception transmitting unit is designed with three types of output modes, namely, RF output, fiber optic transmission, and microwave relay (Figure 5).

(1) Interference analog RF signal output: The forwarding deception signal generation equipment directly outputs the interference analog RF signal. The external transmitter antenna is connected via a long RF cable for transmission, and the transmitter antenna directly transmits the received interference RF signal.

(2) Interference RF signal fiber optic output: The forwarding deception signal generation equipment outputs the interference RF signal as a fiber optic signal. The external transmitting antenna is connected via a long RF cable, and the transmitting antenna converts the received interference RF fiber optic signal into an RF signal for output.

(3) Relay band interference RF wireless output: The forwarding deception signal generation equipment outputs a relay band interference RF signal. The interference transmitting antenna is connected wirelessly, and the interference transmitting antenna down converts the received relay band signal for output.

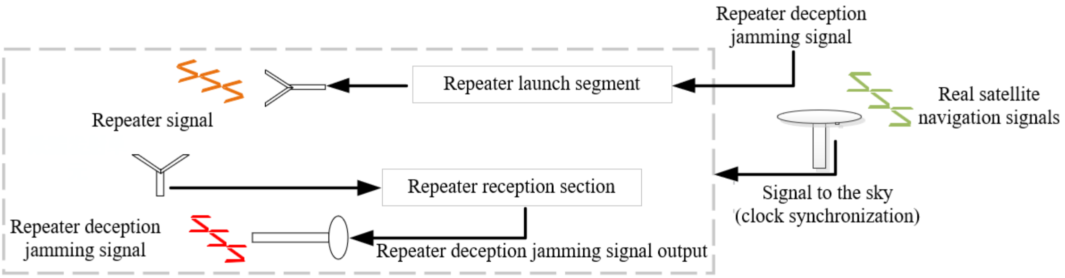


Figure 5. Microwave repeater output

2.2.4 Repeater deception jamming software

The repeater deception jamming software serves as the comprehensive control software of the system. It is responsible for regulating the operation of the equipment, facilitating human-computer interaction, and providing functions such as generating jamming strategies, calculating jamming control parameters, and setting spoofing positions. The forwarding spoofing jamming software operates on the PC terminal.

2.3 Clock synchronization design

To synchronize the system time, the B1/L1 signal receiving module is designed to receive real satellite signals, locate and decode the time, and output the second pulse information in the forward spoofing signal generating unit and spoofing transmitting unit equipment. This synchronized current time is provided to the forwarding deception signal generation unit, and the second pulse is used to discipline the local crystal oscillator, ensuring that the time information of the GNSS forwarding signal generated by this system is consistent with the real satellite signal.

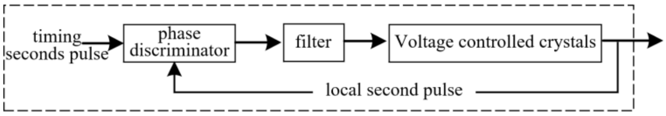


Figure 6. Taming the local crystal phase-locked loop

The structure of the phase-locked loop for disciplining the local crystal oscillator is illustrated in Figure 6. The built-in B1/L1 signal receiving module outputs the timing second pulse signal and compares it with the second pulse output from the local crystal oscillator. It identifies the difference between the frequencies of these two signals and outputs an adjustable DC voltage to control the frequency output of the local crystal oscillator. This ensures that the local clock signal remains synchronized with the real satellite clock signal.

2.4 Repeater deception control algorithm design

The core control algorithms of the forwarding spoofing interference software comprise the optimal star selection policy algorithm and the forwarding delay control algorithm.

2.4.1 Algorithm design for optimal star selection strategy

When implementing forwarding spoofing jamming, the satellite utilized by the target receiver for localization is typically selected as the satellite to be forwarded, in order to ensure the effectiveness of the jamming [11].

This system incorporates the design of an optimal satellite selection strategy algorithm, which is developed in conjunction with the satellite spatial geometry configuration. The process of satellite selection within the optimal satellite selection strategy algorithm is as follows:

S1: Based on the real satellite ephemeris acquired by the receiving antenna, the coordinate system is converted to construct a two-dimensional matrix of all satellites relative to the receiving antenna array:

$$P = \{[\vartheta_1, \varphi_1],[\vartheta_2, \varphi_2],[\vartheta_3, \varphi_3]...[\vartheta_m, \varphi_m]\} \tag{5}$$

where, $[\vartheta_1, \vartheta_2, \vartheta_3 \dots \vartheta_m]$ represents the azimuth of all visible stars in the sky at this time for the receiving antenna array, and the subscript denotes the visible star number; $[\varphi_1, \varphi_2, \varphi_3, \dots \varphi_m]$ represents the pitch angle of all visible stars in the sky at this time for the receiving antenna array, and the subscript denotes the visible star number.

S2: The visible stars in the two-dimensional matrix P are mapped to the respective faceted antenna array according to the azimuthal categorization, based on the spatial range divided by the directional receiving antenna array. This process yields the sub-matrix $P_1, P_2, P_3 ... P_8$, for example:

$$\begin{cases} P_1 = \{[\vartheta_1, \varphi_1]\}, \{[\vartheta_4, \varphi_4]\}, \{[\vartheta_8, \varphi_8]\} \\ P_2 = \{[\vartheta_2, \varphi_2]\}, \{[\vartheta_5, \varphi_5]\}, \{[\vartheta_7, \varphi_7]\} \\ \vdots \\ P_8 = \{[\vartheta_9, \varphi_9]\}, \{[\vartheta_{10}, \varphi_{10}]\}, \{[\vartheta_{13}, \varphi_{13}]\} \end{cases} \tag{6}$$

The data in the above equation are exemplary, with the stars on the P_1 side being #1, #4, #8, and so forth;

S3: After classification, within each sub-matrix $P_1, P_2, P_3, \cdots, P_8$, a one-time localization DOP value set is obtained: $T_1 = \{ [\sigma_1, \sigma_4, \sigma_8 \cdots], [\sigma_2, \sigma_5, \sigma_7 \cdots], [\sigma_3, \sigma_6, \sigma_{11} \cdots], ..., [\sigma_9, \sigma_{10}, \sigma_{13} \cdots]$, where σ represents the DOP value result of each star during one-time localization, with the subscript denoting the satellite number. From each side, the first visible star with the optimal DOP value during one-time localization is filtered out to form the tracking preferred star. These stars are then constructed as the first tracking preferred star set, denoted as D1:

$$D_1 = \begin{cases} \{[\vartheta_1, \varphi_1]\} \\ \{[\vartheta_2, \varphi_2]\} \\ \vdots \\ \{[\vartheta_9, \varphi_9]\} \end{cases} \tag{7}$$

S4: The turntable control parameters of each directional receiving antenna are adjusted according to the azimuth and pitch angles of each visible star in the collection of tracking preferred stars (No. 1, No. 2, ..., and No. 9 visible stars), respectively. This is done to receive the authorized signals in the DOP-valued optimal satellite signal beams from their respective covered spatial ranges for tracking and outputting a total of 8 trans ponding digital IF baseband signal beams.

S5: When the setting cycle T expires, repeat the preceding steps until the end of tracking. Specifically, after the internal timer has elapsed T time, update the ephemeris and obtain the set of DOP values T_2 at the time of secondary localization, as well as the set of preferred stars for secondary tracking D_1. Subsequently, after re-calculating the rotary pointing control of each receiving antenna array, complete the independent beam adjustment for each side until the end of tracking. In other words, the system searches for the star once every T time interval and cycles, where T is related to the directional antenna receiving beamwidth and satellite position.

In satellite navigation systems, the DOP value is an important index for measuring the influence of satellite geometric distribution on positioning accuracy. A smaller DOP indicates a more favorable geometric distribution of satellites for positioning, resulting in higher positioning accuracy. The optimal satellite selection strategy algorithm proposed in this paper comprehensively considers the performance of spoofing equipment and forwarding hardware resources. Based on the satellite selection strategy with the smallest DOP value, 8 satellite signals are selected from all satellite signals in the sub-space domain, realizing the best selection of signals and ensuring the quality of forwarding spoofing.

2.4.2 Repeater delay control algorithm design

After determining the spoofing position point, the forwarding delay for the 8-channel satellite can be calculated using the delay formula, specifically Eq. (4), and each spoofing position point corresponds to a unique set of time delays. Ideally, the forwarding deception jamming system can successfully achieve its deception objective if the satellite signals of different channels are individually controlled by the delays calculated according to the corresponding results [8]. However, an analysis of Eq. (4) reveals that when the distance between the spoofing location point B and the satellite is less than the distance traversed by the forwarding signal, i.e., the direct path between the spoofing point and the satellite is shorter than the path taken by the forwarded signal, certain implications may arise that need to be considered:

$$|S_i B'| < (|S_i A| + |AB|) \tag{8}$$

The calculated forwarding delay amount, denoted as t_i, would result in a negative number, which is not feasible in practical engineering applications.

To correct for negative forwarding delay quantities, the forwarding system employs the method of adding a common delay, denoted as Δt, to each signal forwarded, in order to counteract the effect of the negative delay [18]. The forwarding delay must be satisfied accordingly:

$$t_i + \Delta t \geq 0, i = 1, 2, 3...8 \tag{9}$$

The equation for the forward spoofing interference, corrected for negative delay, is as follows:

$$\rho_i + c\Delta t = |S_i B'| + c\Delta t + ct_u \tag{10}$$

From the above equation, it can be observed that the compensation of time delay t_i does not alter the localization result, but it will cause the target receiver's clock difference to experience a sudden jump. Specifically, the clock difference jumps up by an amount exactly equal to the compensation value of the negative delay, denoted as Δt.

Considering that larger clock jumps are easily detected by the target receiver in forward spoofing interference, the system opts for the minimum compensation delay to minimize the clock jumps when performing negative delay correction. Namely:

$$\Delta t = -\min(t_i) \tag{11}$$

3. FIELD TEST VALIDATION

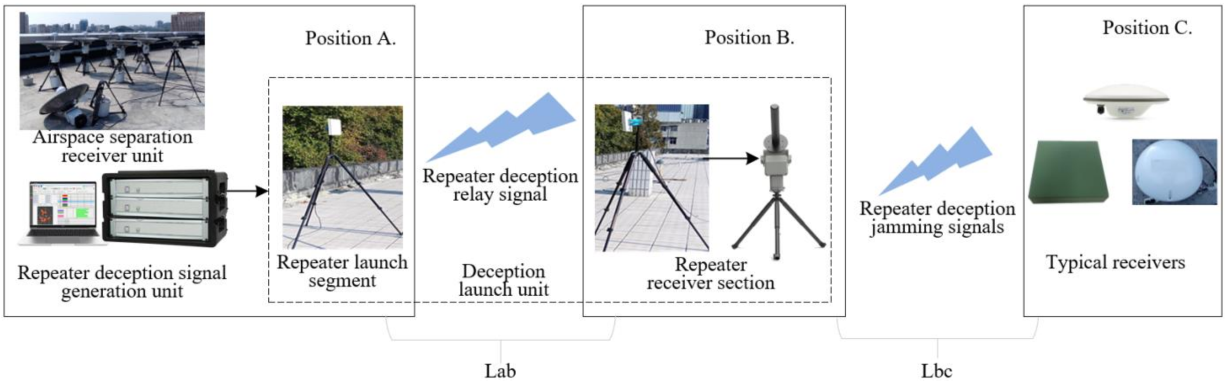
3.1 Testing scenario design

3.1.1 Introduction of test scene

The test was conducted in an open and unobstructed hard field with a favorable electromagnetic environment located in Nantangchong, Baishui Town, Miluo City. For the test, microwave relay was selected to broadcast and forward the deception signal. The deception transmitter unit was divided into two components: relay transmitting and relay receiving.

The relay transmitting component, along with the spatial separation receiving unit and the forwarding deception signal generating unit, were set up at location A, while the relay receiving component was established at location B. The test was executed in the field according to the following diagrams.

The scenario for the field test is illustrated in Figure 7.



Position A.
Airspace separation receiver unit
Repeater deception signal generation unit
Repeater launch segment
Repeater deception relay signal
Deception launch unit
Position B.
Repeater receiver section
Repeater deception jamming signals
Position C.
Typical receivers
Lab
Lbc

Figure 7. Field test

3.1.2 Value analysis

To ensure the credibility of the test results, it is essential to calibrate the spatial insertion loss of the test environment prior to the commencement of the test. This includes the calibration of the relay distance values, denoted as Lab, for both the relay transmitting and receiving parts, as well as the interference distance, denoted as Lbc, between the relay receiving part and the standard receiver under test. Specifically, the value of the interference distance Lbc must satisfy the requirement that the power of the signal sent by the relay deception system reaches the standard receiver under test to achieve deception. Additionally, the value of the interference distance Lab must meet the requirement that the deception unit transmits a specific signal without causing self-excitation of the relay deception interference system [19].

(1) An analysis of the value of the relay distance, denoted as Lab, is conducted.

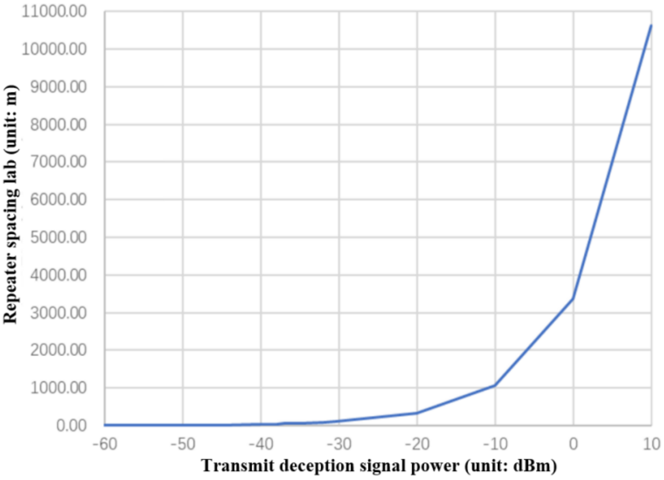


Figure 8. Relay distance Lab and forward spoofing transmit power relationship

The forwarding deception jamming system transmits a deception jamming signal to the spatial separation receiving unit. When the power of this signal is less than -130dBm, which is the power of the real navigation signal, it does not produce self-excitation effects. Generally, as the forward spoofing transmit power increases, the corresponding required relay distance, denoted as Lab, also increases. The relationship between the forward spoofing transmit power and the relay distance Lab is illustrated in Figure 8.

Given the limitations of the test site, the relay distance, denoted as Lab, is set to 100 meters, which corresponds to the maximum spoofed transmit power of -30dBm.

(2) An analysis of the value of the interference distance, denoted as Lbc, is conducted.

In the actual forwarding interference test process, due to the fact that the forwarding spoofing signal lags behind the real satellite signal, the interfered terminal must first be suppressed by high-power interference to lose the lock and enter the recapture phase, before spoofing success becomes possible [20].

From the above, it can be seen that the maximum power of the outfield test spoofing signal transmission is 40dBm, and the power of the real navigation signal when it reaches the receiver is generally -130dBm. For the interference signal with the frequency of 1575.42MHz, the size of the standard receiver under test is about 0.3m*0.3m under pass-through condition, and the minimum interference distance to satisfy the far-field condition is 0.95m, which corresponds to the interference distance The relationship between Lbc and the dry signal ratio of the antenna port face of the receiver terminal under test is shown in Figure 9.

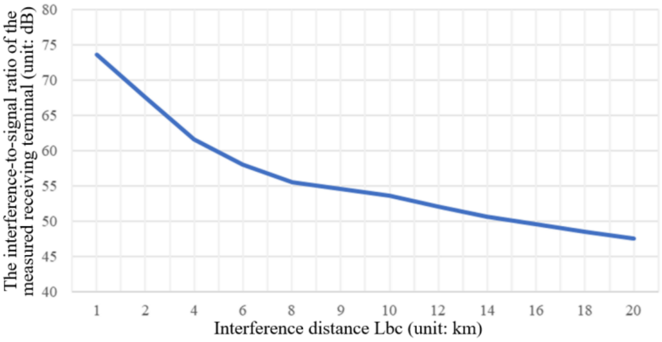


Figure 9. Relationship between interference distance Lbc and dry signal ratio at the receiver terminal

Given that the repeater deception jamming system has an adjustable power attenuation range of 50dB, and considering that the interference distance Lbc is 1km, the maximum interference-to-signal ratio at the receiving terminal port is approximately 76dB. This ratio can meet the effective deception jamming power requirements corresponding to receiving terminals with different technical states (based on the interference-to-signal ratio).

3.2 Test result analysis

3.2.1 Deception effect

When broadcasting and forwarding the spoofing signal, the spoofing signal position is set to be at a fixed point. To avoid any influence from a single navigation receiver model on the test, three typical receivers were selected for the test, namely one ordinary navigation receiver, one four-array receiver, and one six-array receiver.

The Table 1 presents the incomplete statistics of the spoofed cases for both the ordinary receiver and the array receiver in a reliable environment.

3.2.2 System performance

Based on Table 1, it can be observed that the repeater deception jamming system designed in this paper is capable of successfully deceiving the typical receiver. Specifically, under conditions of zero suppression and high-power deception, the deception of the ordinary receiver is successful, while the deception of the four-array receiver and the six-array receiver fails. Under conditions of multiple suppression deception, for the four-array receiver, a combination of 2 to 4 suppressions results in successful deception, while 1 suppression fails to deceive. For the six-array receiver, a combination of 5 to 6 suppressions leads to successful deception, while 1 to 4 suppressions result in failure to deceive.

Table 1. Ordinary receivers and array receivers being spoofed

Test Object	Jamming Implementation Program	Deception Results
General receiver	Amplification of forward spoofing signals using low noise amplifiers	successes
Four-array receiver	Amplification of forward spoofing signals using low noise amplifiers	fail
	First broadcast a suppression signal to suppress the signal to the sky, then broadcast a forwarding spoofing signal	fail
	Broadcast 2 squelch signals to squelch the signal to the sky before broadcasting the forward spoofing signal	successes
	First broadcast 3 suppression signals to suppress the signal to the sky, then broadcast the forwarding spoofing signals	successes
	First broadcast 4 suppression signals to suppress the signal to the sky, then broadcast the forwarding spoofing signals	successes
Six-array receiver	Amplification of forward spoofing signals using low noise amplifiers	fail
	First broadcast a suppression signal to suppress the signal to the sky, then broadcast a forwarding spoofing signal	fail
	First broadcast 2 suppression signals to suppress the signal to the sky, then broadcast the forwarding spoofing signals	fail
	First broadcast 3 suppression signals to suppress the signal to the sky, then broadcast the forwarding spoofing signals	fail
	First broadcast 4 suppression signals to suppress the signal to the sky, then broadcast the forwarding spoofing signals	fail
	First broadcast 5 suppression signals to suppress the signal to the sky, then broadcast the forwarding spoofing signals	successes
	First broadcast 6 suppression signals to suppress the signal to the sky, then broadcast the forwarding spoofing signals	successes

According to the theory of signal propagation in free space, the deception distance is equivalent to signal power attenuation. The distance is substituted by attenuation after accounting for free space loss, and this attenuation is added to the signal link. By combining this with the signal level generated by the repeater deception jamming system, the power of the repeater deception signal at the receiving antenna surface can be calculated. If this power level falls within the power range of the receiving terminal, the deception can be considered successful.

When the deception distance of the system is 1km, the maximum jamming-to-signal ratio at the receiving terminal port is approximately 76dB. This ratio can meet the effective deception jamming power requirements corresponding to receiving terminals with different technical states (based on the jamming-to-signal ratio).

Since the forwarding deception jamming system only forwards signals from 8 satellites, and the Beidou system has 28 visible satellites, the actual forwarded satellites cannot fully cover all these signals, resulting in reduced signal redundancy and potentially affecting positioning accuracy. Additionally, when initiating position deception, the greater the deviation distance, the larger the pseudo-range residual becomes, leading to increased positioning error after the deception is successful. This occurs because, when receiving the signal, a portion of the real signal from the sky participates in the positioning process, causing the receiver to experience a positioning residual. Unfortunately, the real signal from the sky cannot be fully covered or deviated, and achieving high positioning accuracy to meet the target becomes challenging.

Furthermore, the system spoofing process is executed in real-time. When the system initially transmits suppression jamming to suppress the unlocked sky signal and subsequently sends the spoofing signal, the receiver promptly switches to the forwarded signal. However, this process has a prerequisite, namely, that it must occur within a specific range of deviation.

In theory, a higher forwarding and receiving gain results in a better deception effect. Under the current gain conditions, the deception may only be effective against anti-jamming receivers with fewer than six arrays. With more than six array elements, there may be no discernible or no effect at all. As the number of array elements increases, the difficulty of achieving successful deception also increases. If the forwarding and receiving gain can be augmented, this difficulty can be mitigated. However, since the forwarding and receiving gain is currently limited, when the number of array elements reaches a certain threshold, unsuccessful deception becomes a possibility.

4. CONCLUSION

In this paper, a repeater deception jamming system based on high-gain antenna array spatial separation reception is designed and implemented. Firstly, the signal model of repeater deception jamming is established, and the specific calculation method for forwarding delay is analyzed. Subsequently, the overall design scheme of the system is introduced, encompassing detailed discussions on the composition of the spatial separation receiving unit, the forwarding spoofing signal generation unit, the spoofing transmitting unit, and the forwarding spoofing jamming software. The specific design methods for system clock synchronization and the forwarding spoofing control algorithm are also presented. Through the built-in receiving module, the tamed PPS signal and the 10MHz clock signal are provided to achieve synchronization between the local clock and the real satellite system. By employing the deception jamming software, directional selection and controllable delay forwarding of the satellite navigation signal are realized based on the optimal star strategy and the forwarding delay control strategy. Ultimately, a field test is conducted to verify the effectiveness of the designed system. It is noteworthy that, although the proposed forward deception jamming system based on high-gain antenna array spatial separation reception can achieve deception against ordinary receivers, four-array receivers, and six-array receivers, the existing forward reception gain is limited. As such, it may only be effective for receivers with fewer than six arrays, and for receivers with more than six array elements, the effect may not be obvious or may be ineffective. In the future, the forwarding and receiving gain can be increased to reduce the difficulty of achieving successful deception.

ACKNOWLEDGMENT

This paper was supported by the Key Research and Development Projects of the Hunan Provincial Department of Science and Technology (Grant No.: 2022GK2026, 2024JK2062), the Science and Technology Plan Project of the Hunan Provincial Department of Natural Resources (Grant No.: 2023-78, 2022-21), the Aid Program for Science and Technology Innovative Research Teams in Higher Educational Institutions of Hunan Province, the Open Fund of the Xi'an Key Laboratory of Integrated Transport Big Data and Intelligent Control (Chang'an University) (Grant No.: 300102343515),The key program of Hunan Provincial Department of science and technology support (Grant No.: 23A0609).

REFERENCES

[1] Wang, X.Y., Yang, J. J., Huang, M., Wu, J.D., Peng, Z.X. (2023). Research status and prospect of GNSS jamming and spoofing detection. Journal of Signal Processing, 39(12): 2131-2152. https://doi.org/10.16798/j.issn.1003-0530.2023.12.003

[2] Bian, S.F., Hu, Y.F., Chen, C., Li, Z.M., Ji, B. (2017). Research on GNSS repeater spoofing technique for fake Position, fake Time & fake Velocity. In 2017 IEEE International Conference on Advanced Intelligent Mechatronics (AIM), Munich, Germany, pp. 1430-1434. https://doi.org/10.1109/AIM.2017.8014219

[3] Yi, M.J., Li, J.W., Wen, Z.J. (2023). Development status of deception jamming technology to UAV satellite navigation. Shipboard Electronic Countermeasure, 46(6): 44-51. https://doi.org/10.16426/j.cnki.jcdzdk.2023.06.008

[4] Tang, C., Ding, J., Qi, H., Zhang, L. (2024). Smart forwarding deceptive jamming distribution optimal algorithm. IET Radar, Sonar & Navigation, 18(6): 953-964. https://doi.org/10.1049/rsn2.12540

[5] Seo, S.H., Jee, G.I., Lee, B.H. (2021). Spoofing signal generation based on manipulation of code delay and doppler frequency of authentic GPS signal. International Journal of Control, Automation and Systems, 19(2): 1026-1040. https://doi.org/10.1007/s12555-019-0745-6

[6] Gummineni, M., Polipalli, T.R. (2020). Implementation of reconfigurable transceiver using GNU Radio and HackRF One. Wireless Personal Communications, 112(2): 889-905. https://doi.org/10.1007/s11277-020-07080-0

[7] Hu, C.Y., Wang, G.M., Yang, J. (2018). Analysis of positioning error for GPS repeater deception jamming. Aerospace Electronic Warfare, 34(5): 41-45. https://doi.org/10.3969/j.issn.1673-2421.2018.05.009

[8] Kerns, A.J., Shepard, D.P., Bhatti, J.A., Humphreys, T.E. (2014). Unmanned aircraft capture and control via GPS spoofing. Journal of Field Robotics, 31(4): 617-636. https://doi.org/10.1002/rob.21513

[9] Zhang, W.M. (2010). Analysis of multi-beamforming algorithms for GPS adaptive array. Acta Armamentarii, 31(12): 1686-1690.

[10] Ghanea, M., Moallem, P., Momeni, M. (2024). Automatic building extraction in dense urban areas through GeoEye multispectral imagery. International Journal of Remote Sensing, 35(13): 5094-5119. https://doi.org/10.1080/01431161.2014.933278

[11] Shi, P.L., Jin, W.X., Wu, S.X. (2019). Research on satellite selection algorithm of GNSS repeater deception jamming. Transactions of Beijing Institute of Technology, 39(5): 524-531. https://doi.org/10.15918/j.tbit1001-0645.2019.05.015

[12] Zhao, X.X., Chen, X., Guo, X.Q. (2020). A Repeater Spoofing Method for GNSS Clock of Receiver. Telecommunication Engineering, 60(12): 1415-1419. https://doi.org/10.3969/j.issn.1001-893x.2020.12.004

[13] Schmidt, D., Radke, K., Camtepe, S., Foo, E., Ren, M. (2016). A survey and analysis of the GNSS spoofing threat and countermeasures. ACM Computing Surveys (CSUR), 48(4): 64. https://doi.org/10.1145/2897166

[14] Zheng, C., Wang, Q., Jiang, Y., Wang, X.Y. (2022). Time delay control method for GNSS repeater deception jamming. Modern Navigation, 13(2): 79-84. https://doi.org/10.3969/j.issn.1674-7976.2022.02.001

[15] Jafarnia-Jahromi, A., Broumandan, A., Nielsen, J., Lachapelle, G. (2012). GPS vulnerability to spoofing threats and a review of antispoofing techniques. International Journal of Navigation and Observation, 2012(1), 127072. https://doi.org/10.1155/2012/127072

[16] Minucci, F., Vinogradov, E., Pollin, S. (2020). Avoiding collisions at any (low) cost: ADS-B like position broadcast for UAVs. IEEE Access, 8: 121843-121857. https://doi.org/10.1109/ACCESS.2020.3007315

[17] Wang, H., Chang, Q., Xu, Y. (2021). Deception jamming detection based on beam scanning for satellite navigation

systems. IEEE Communications Letters, 25(8): 2703-2707. https://doi.org/10.1109/LCOMM.2021.3083590

[18] Soumekh, M. (2005). SAR-ECCM using phase-perturbed LFM chirp signals and DRFM repeat jammer penalization. In IEEE International Radar Conference, Arlington, VA, USA, pp. 507-512. https://doi.org/10.1109/RADAR.2005.1435879

[19] Wang, Y., Zou, Y., Henrickson, K., Wang, Y., Tang, J., Park, B.J. (2017). Google earth elevation data extraction and accuracy assessment for transportation applications. PloS One, 12(4): e0175756. https://doi.org/10.1371/journal.pone.0175756

[20] Bhatti, J., Humphreys, T.E. (2017). Hostile control of ships via false GPS signals: Demonstration and detection. NAVIGATION: Journal of the Institute of Navigation, 64(1): 51-66. https://doi.org/10.1002/navi.183