Article

Two Regional Deployment Algorithms of Distributed GNSS Forwarding Spoofer for Multiple Receiver Sensors

Yangjun Gao $^{1,2}$ and Guangyun Li $^{1,*}$

$^1$ College of Geospatial Information, PLA Strategic Support Force Information Engineering University, Zhengzhou 450001, China
$^2$ State Key Laboratory of Geo-Information Engineering, Xi’an 710054, China
* Correspondence: guangyun_li_chxy@163.com

Abstract: Global navigation satellite system (GNSS) spoofing technology is an effective way to protect sensitive facilities and control foreign objects. To realize effective distributed GNSS forwarding spoofing for multiple receiver sensors in the area, the following research work is carried out: first, the GNSS forwarding spoofing model is established, including a forwarding spoofing mathematical model and an asynchronous traction spoofing method; second, the function scope of forwarding spoofing is fully evaluated; third, two forwarding spoofing area deployment algorithms for multi-spoofing multi-target (MSMT) are proposed—the multi-target same-point spoofing algorithm (MSPSA) is suitable for the same-point spoofing of multiple receiver sensors, and the multi-target different-point spoofing algorithm (MDPSA) is suitable for the different-point spoofing of multiple receiver sensors; and four, the experimental tests of MSPSA and MDPSA for MSMT were carried out. The experimental results show that MSPSA and MDPSA can respectively give the most appropriate deployment scheme of spoofing according to the various needs of the spoofer. For example, the number of spoofing devices is 1, the total distance between each spoofer and each receiver is 40,345.1 m, and the critical spoofing rate (CSR) and spoofing success rate (SSR) are both 100%. The performance of the spoofing deployment scheme can meet the needs of the spoofer.

Keywords: multiple receiver sensors; forwarding spoofing; distributed spoofing; regional deployment; GNSS

1. Introduction

At present, the major global navigation satellite systems (GNSS) are in the stage of rapid development and stable operation. Thanks to the steadily improved service performance of GNSS, the vast number of GNSS users can easily obtain high-precision, all-weather, and continuous stable positioning, navigation, and timing (PNT) services. On the other hand, a GNSS navigation signal, as a radio signal from a long-distance navigation satellite, has certain vulnerabilities, such as low signal power and partial signal structure disclosure. Based on this, a jammer can carry out complex and changeable signal interference and even spoofing to GNSS users [1] to achieve the tactical and even strategic intent of driving away unknown aircraft and protecting sensitive parts [2,3]. For the jammer, the harmfulness and concealment of GNSS spoofing are far better than other forms of interference [4,5], so GNSS spoofing has gradually become a navigation-jamming technology favored by jammers [6]. Many spoofing methods have emerged and can affect various navigation terminals [2,4]. For different spoofed navigation terminals and purposes of spoofing, the forwarding spoofing adds a specific delay to each GNSS signal and reasonably deploys the distributed spoofing devices to achieve the purpose of spoofing to the maximum extent. Forwarding spoofing can be used to spoof the military code receiver sensor. This advantage is difficult to achieve by generating spoofing, so its application prospect is broad.
The delay control of a retransmitted signal is one of the key technologies of forwarding spoofing. Huisuo Zhang et al. implemented the algorithm of simultaneous spoofing of position and velocity by applying different propagation delays and Doppler control quantities on each satellite to slowly pull the GNSS positioning results [7]. Shangyue Wang et al. adopted an iterative algorithm and introduced an offset rate parameter to add delay to the GNSS signal to realize the forwarding spoofing scheme of point-by-point deviation of a user’s track. A simulation shows that the user does not have location jump when being cheated, and the spoofing effect is obvious [8]. In addition, Jiaqi Zhang et al. proposed an intelligent forwarding spoofing scheme based on the low Earth orbit (LEO) satellite platform, improving the signal spatial separation algorithm, which was more suitable for the fast-moving LEO satellite platform [9]. The main contribution of the above research is that the position and velocity spoofing of the victim receiver can be realized through a flexible time-delay-control algorithm.

On the other hand, it is difficult to accurately control the carrier Doppler and code phase of the retransmitted signal for forwarding spoofing, so it is necessary to control the transmission power of the retransmitted signal to achieve effective spoofing. Through simulation analysis, Yanbin Liu et al. found that when the forwarding gain does not exceed 30 dB and the forwarding space delay exceeds 1 chip, there is almost no correlation interference between the retransmitted signal and the direct signal; when the retransmitted signal and the direct signal coexist, the retransmitted signal only needs to have 7~10 dB power gain to have a high acquisition probability [10]. Pengliang Shi et al. pointed out that when the retransmitted signal is 30 dB higher than the direct signal, the carrier tracking loop will lose lock, and the receiver will track the spoofing signal with a large probability after recapture [11]. Although the above research results are only for the case of spoofing a single victim receiver, the main contribution is, first, as the theoretical basis for the spoofing multiple receivers below, and, second, it is also the theoretical basis for the following analysis of the scope of forwarding spoofing.

The research results of distributed deployment of forwarding spoofing are summarized as follows. The angle of arrival detection algorithm is one of the effective spoofing detection methods to deal with spoofing signals broadcast from a single spoofing device [12]—for example, the antenna-array carrier phase double-difference detection method [13], inertial navigation-assisted three-element antenna-array detection method [14], and Doppler-based spoofing source-direction-finding method [15]. Jingshu Yang et al. used multiple directional antennas and delay controllers to control the delay of different satellite signals to achieve position spoofing of the target receiver, established a four-station forwarding spoofing model, and gave the mapping relationship between the real position and the spoofing position [16]. Tippenhauer et al. pointed out that it is applicable to the forwarding spoofing of military code signals, and a spoofer is limited to fewer specific spatial positions [17]. Ting He proposed to lay spoofing devices according to the regular hexagonal network type. For the target receiver with the robust adaptive clock difference jump detection function, the optimal value of the coverage radius of a single spoofing device is determined to be 10 km, and the optimal value of the distance between adjacent spoofing devices is determined to be 17 km [18]. Song Zhang et al. established the mathematical model of multi-objective planning and array optimization of the minimum and maximum evaluation function, and solved the model by the multiplier penalty function method. Under the condition of long-term operation of the system, based on the method of nonlinear programming, the motion model of the air platform was established, and the solution steps of the quadratic programming quadratic constraint motion model were given [19]. The main contribution of the above research results is to preliminarily explore the theoretical possibility of multiple spoofers to spoof together. However, first of all, there is a lack of specific analysis of the scope of forwarding spoofing; second, it fails to provide a reasonable deployment plan according to the specific location of victim receivers; and finally, no reasonable deployment scheme was designed according to the different spoofing requirements of the spoofer.
What is more, for multi-target navigation terminals that form a group with each other, such as unmanned aerial vehicles (UAVs), each UAV can resist spoofing by detecting the relative position. At present, the spoofer still lacks a timely and effective regional deployment algorithm to achieve collective spoofing. At the same time, the excellent regional deployment algorithm of distributed GNSS spoofer can provide a technical route for building a perfect GNSS spoofing defense zone. At this time, the spoofer does not excessively cling to the spoofing effect of a certain target but takes the overall spoofing success rate of multiple targets in the spoofing defense zone as an evaluation index. Therefore, it is extremely urgent to propose a regional deployment algorithm of distributed GNSS forwarding spoofing for multiple targets.

The structure and contents of this paper are as follows. The introduction summarizes the research background and current situation of distributed GNSS forwarding spoofing. In Section 1, the GNSS forwarding spoofing model is established, including the GNSS asynchronous traction spoofing method and the forwarding spoofing mathematical model. In Section 2, the scope of the forwarding spoofing is analyzed and evaluated. In Section 3, the forwarding spoofing region deployment algorithm for multi-spoofer multi-target (MSMT) is proposed. In Section 4, different MSMT spoofing scenarios are analyzed, and the performance of the proposed algorithm is verified and evaluated. Section 4 gives a comprehensive summary and a prospect of this paper.

2. GNSS Forwarding Spoofing Model
2.1. Mathematical Model of Forwarding Spoofing

The purpose of the forwarding spoofer is to spoof the positioning result of a victim receiver whose real physical location is \( P_{r1} \) to the point \( P_{f1} \). From the spoofer’s point of view, the forwarding spoofer first receives authentic signals from the sky, and the corresponding satellite positions are expressed as \( S_1, S_2, \ldots, S_n \). Then, according to the purpose of spoofing, the spoofer adds the corresponding time delay to each channel of authentic signals, and finally broadcasts through the omnidirectional antenna. As shown in Figure 1, here we aim at a more advanced forwarding spoofer; that is, the forwarding spoofer can separate different signals and add different time delays to spoof the receiver at point \( P_{f1} \) to point \( P_{r1} \).

![Figure 1. Mathematical model of forwarding spoofing.](image-url)
On the one hand, the retransmitted signal does not change the navigation message. After demodulating the navigation message, the victim receiver will obtain the real satellite position information. The real positions of the \( n \) satellites used by the receiver for a positioning solution are respectively expressed as \( S_1, S_2, \cdots, \) and \( S_n \). On the other hand, for the signals of these \( n \) satellites, the propagation time from satellite to spoofer and the processing delay are expressed as \( t_1, t_2, \cdots, \) and \( t_n \), and the forwarding spoofer also performs corresponding delay processing, as shown in Figure 1. Therefore, the following expression is satisfied for a spoofing signal:

\[
A : \begin{cases}
\rho_1' = c \cdot t_1 + |P_T - P_{r1}| \\
\rho_2' = c \cdot t_2 + |P_T - P_{r1}| \\
\vdots \\
\rho_n' = c \cdot t_n + |P_T - P_{r1}|
\end{cases}
\]

where \( \rho_1', \rho_2', \cdots, \) and \( \rho_n' \) represent the pseudorange measurements when the victim receiver receives spoofing signal for positioning, and \( c \) represents the speed of light. Meanwhile, when a victim receiver receives a spoofing signal for positioning, it satisfies the following equation:

\[
V : \begin{cases}
|S_1 - P_{f1}| = \rho_1' - c \cdot \delta t_k \\
|S_2 - P_{f1}| = \rho_2' - c \cdot \delta t_k \\
\vdots \\
|S_n - P_{f1}| = \rho_n' - c \cdot \delta t_k
\end{cases}
\]

where \( \delta t_k \) represents the receiver clock offset calculated by the victim receiver. Different from generative spoofing, since the delay added by the spoofer to each channel of signals is positive, the corresponding propagation times \( t_1, t_2, \cdots, \) and \( t_n \) need to meet the following restrictions:

\[
A : \begin{cases}
c \cdot t_1 > |S_1 - P_T| \\
c \cdot t_2 > |S_2 - P_T| \\
\vdots \\
c \cdot t_n > |S_n - P_T|
\end{cases}
\]

It should be pointed out that for the multi-channel retransmitted signal broadcast by single omnidirectional antenna, if a spoofer keeps the above spoofing purpose unchanged, that is, the positioning result of victim receiver with the real physical position of \( P_{r1} \) is spoofed to point \( P_{f1} \), the spoofing signal can still spoof another victim receiver with the real physical position of \( P_{r2} \), as shown in Figure 1. For the receiver at point \( P_{r2} \), if a spoofing signal has a sufficient power advantage, the tracking loop can still be directly destroyed to control the positioning of the receiver. At this time, the spoofing signal satisfies the following equation:

\[
A : \begin{cases}
\rho_1' = c \cdot t_1 + |P_T - P_{r2}| \\
\rho_2' = c \cdot t_2 + |P_T - P_{r2}| \\
\vdots \\
\rho_n' = c \cdot t_n + |P_T - P_{r2}|
\end{cases}
\]
Similarly, the propagation times \( t_1, t_2, \ldots, \) and \( t_n \) at this time still need to satisfy the restriction condition of Equation (3). Meanwhile, when a victim receiver at \( P_2 \) receives a spoofing signal for positioning, the following equation is satisfied:

\[
V : \begin{cases} 
S_1 - P_{f1} = p_1' - (c \cdot \delta t_k + |P_T - P_{f2}| - |P_T - P_{f1}|) \\
S_2 - P_{f1} = p_2' - (c \cdot \delta t_k + |P_T - P_{f2}| - |P_T - P_{f1}|) \\
\vdots \\
S_n - P_{f1} = p_n' - (c \cdot \delta t_k + |P_T - P_{f2}| - |P_T - P_{f1}|)
\end{cases}
\]

(5)

For the above equation, we need to explain that, according to the principle of single-point pseudorange positioning, the calculated receiver clock offset is the common deviation part \([20]\) in the range observation of each satellite. Therefore, compared with the case of Equation (2), the increased common part \(|P_T - P_{f2}| - |P_T - P_{f1}|\) of each pseudorange observation will be absorbed by receiver clock offset at this time, and the victim receiver will still be located at point \( P_{f1} \), as shown in Figure 1. According to the above inference, it can be explained that if a spoofer wants to cheat the multiple targets constituting the group, on the one hand, different single targets will be spoofed to different positions and, at the same time, the relative positions between the single targets in the group will remain unchanged; then the spoofer cannot achieve this goal through a single forwarding spoofer. Therefore, it is necessary to consider deploying multiple spoofer in a distributed manner to jointly achieve the spoofing purpose.

### 2.2. GNSS Asynchronous Traction Spoofing Method

On the basis of Section 2.1, the process of invading the loop and controlling the loop after a retransmitted signal reaches the antenna of a victim receiver will be discussed below.

For asynchronous traction spoofing in forwarding spoofing, although the forwarding signal usually lags behind the authentic signal by a certain time delay, if the time delay is not too large, the correlation peaks formed by the forwarding signal and authentic signal at the tracking loop may overlap. In this case, the spoofing signal intrudes into the loop at a power higher than the authentic signal, and then, in the process of spoofing signal gradually moving the correlation peak, the loop can naturally lock to the higher power spoofing signal correlation peak through the power advantage.

When a GNSS retransmitted signal intrudes into the loop that remains locked to authentic satellite signal, taking the \( P \) branch of a loop as an example, its coherent integral output is expressed as \([21]\):

\[
P(n) = \sqrt{D(n)} R(\tau_p) \sin(f_{\text{rep}}^a T_{\text{coh}}) \cos(\phi_{\text{rep}}) + \sqrt{D(n)} R(\tau_p) \sin(f_{\text{rep}}^s T_{\text{coh}}) \cos(\phi_{\text{rep}}) \\
Q_p(n) = \sqrt{D(n)} R(\tau_p) \sin(f_{\text{rep}}^a T_{\text{coh}}) \sin(\phi_{\text{rep}}) + \sqrt{D(n)} R(\tau_p) \sin(f_{\text{rep}}^s T_{\text{coh}}) \sin(\phi_{\text{rep}}) \\
P(n) = \sqrt{P(n)} + Q_p(n)
\]

(6)

where the symbol superscript \( s \) represents the spoofing signal, and the symbol superscript \( a \) represents the authentic signal. \( P(n) \) and \( Q_p(n) \) respectively represent the output of the L branch and Q branch of the P channel. \( P \) represents the received signal power, \( D(n) \) represents the message bit level with value of \( \pm 1 \), \( \tau_p \) represents the phase difference between copied C/A code and received C/A code of the P channel, \( d \) represents the distance between two adjacent correlators, and \( R(\cdot) \) represents the code autocorrelation function. \( f_{\text{rep}} \) represents the frequency difference between local replica carrier and received signal carrier, \( T_{\text{coh}} \) represents the coherent integration time, and \( \phi_{\text{rep}} \) represents the phase difference between local replica carrier and received signal carrier. \( P(n) \) represents the C/A code autocorrelation amplitude of the P branch \([21]\). The asynchronous traction spoofing process is further described in detail below.
The asynchronous traction spoofing process is shown in Figure 2. From left to right, there are four stages sorted by time. In the first stage, the receiver tracks the green authentic signal. The yellow dot, the black dot, and the blue dot represent the early, prompt, and late correlation points of the loop, respectively. The red spoofing signal has a certain power advantage over the authentic signal and lags behind the authentic signal by a certain time delay but is not far away. In the second stage, the spoofing signal gradually approaches the authentic signal, and the correlation peaks of the two signals overlap. In the third stage, the correlation peaks of the spoofing signal and authentic signal are basically aligned, and the spoofing signal has a power advantage over the authentic signal, thereby taking over the loop. In the fourth stage, the spoofing signal continues to move and manipulates the receiver to change the positioning result. In Figure 2, we have highlighted the third stage, which is the key step to realize spoofing by forwarding signals.

![Figure 2. Asynchronous traction spoofing process.](image)

Another, perhaps more general, scenario is discussed below. That is, the retransmitted signal lags behind the authentic signal by a large time delay, and the correlation peaks of two signals basically do not overlap. At this time, the retransmitted signal will cause the tracking loop of the victim receiver to enter the state of losing lock and recapture through the high power. This is because the high-power retransmitted signal will bring stronger correlation noise, and the authentic signal will be submerged under the noise, so that the receiver will lose lock. Then the loop will capture and track the retransmitted signal with a large probability, thus realizing spoofing.

3. Evaluation of Scope of Action of Forwarding Spoofing

For a single forwarding spooper that uses an omnidirectional antenna to broadcast spoofing signals, it is necessary to evaluate the spoofing effect of the area covered by its spoofing signals, which is the premise of designing a spoofing area deployment algorithm in the next section.

First, the situation in Section 2.1 is still used. The purpose of the spooper is to spoof the positioning result of a victim receiver whose real physical location is \( P_{1r} \) to \( P_f \). In general, at this time, for a victim receiver at \( P_{1r} \) point, the spooper can adjust the broadcast power of the spoofing signal by observing the position of the victim receiver, so that the power advantage \( \eta \) of the spoofing signal relative to the authentic signal is 30 dB. It should be noted that many research results show that when the power gain of a forwarding spoofing signal at the antenna of a victim receiver is more than 30 dB relative to an authentic signal, the receiver tracking loop will lose lock, and the recapture will capture and track the forwarding spoofing signal with a high probability [11,22]. Therefore, here, the spooper uses a power gain of 30 dB as the minimum power gain value required to achieve spoofing. It should be noted that although the minimum power gain required by a spoofing signal to achieve spoofing will be different for different receivers with different configurations, the
spoofing signal adopts a 30 dB power gain here for the convenience of analysis, which does not affect the final analysis result.

For a victim receiver at any point other than \(P_1\), take victim receiver at point \(P_2\) in the case of Section 2.1 as an example. According to Equation (5), at this time, compared with the case of a spoofing victim receiver at point \(P_1\), for victim receiver at point \(P_2\), the common increment \(|P_T - P_2| - |P_T - P_1|\) of each pseudorange measurement of the spoofing signal is equivalent to the increased distance difference between the propagation delay of the spoofing signal and authentic signal. On the other hand, this will also cause free space propagation loss of GNSS signal power gain. Therefore, the influence of the code phase difference \(\tau\) between the spoofing signal and authentic signal and the power gain of the spoofing signal on the spoofing effect will be analyzed below.

Taking the typical commercial receiver loop configuration as an example, the distance between two adjacent correlators of the loop is \(d\), where the common value is 0.5 chips. The loop adopts the incoherent lead-minus-lag power method, and the calculation equation of the unitary phase detection result \(\delta_{cp}\) is Equation (7), where \(E\) and \(L\) represent the C/A code autocorrelation amplitudes of branch \(E\) and branch \(L\), respectively. The pull in range of the loop is \(|-d, +d|\), i.e., \(2d\). When the code phase difference between received signal and the local signal exceeds \(\pm d\), the loop will lose lock.

\[
\delta_{cp} = \frac{E^2 - L^2}{2(E^2 + L^2)}
\]  

(7)

On the other hand, according to the free space propagation loss equation of GNSS signal, if the propagation distance is \(L\) and the signal wavelength is \(\lambda\), the corresponding propagation loss is [20]:

\[
P_s = 20\log\left(\frac{\lambda}{4\pi L}\right)
\]  

(8)

When the forwarding spoofing signal reaches the receiver loop, when code phase difference between it and authentic signal is \(\Delta\tau = D\), \(D\) represents a negative value. The spoofing signal power gain is 30 dB. According to Equation (8), the relationship curve of spoofing signal power gain \(\eta\) with the code phase difference \(\Delta\tau\) is shown in Figure 3.

![Figure 3. Power gain versus code phase difference.](image)

It should be noted that, for the convenience of representation, the abscissa in Figure 3 has normalized the code phase difference; that is, when the power gain of the spoofing signal is 30 dB, the code phase difference \(\Delta\tau = D\) is represented by 0. According to Figure 3, when \(\Delta\tau < D\), the power gain \(\eta\) of the spoofing signal is much higher than 30 dB, while
\[ \Delta \tau > D, \text{ the power gain } \eta \text{ of the spoofing signal is much lower than 30} \text{ dB. To more vividly express the change of the correlation peak of the spoofing signal and authentic signal with the code phase difference, the schematic diagram of the correlation peak of the two signals is drawn as shown in Figure 4.} \]

\[ \frac{20 \log 4}{s P L} = \pi \]

\[ \text{Figure 4. Schematic diagram of correlation peak between spoofing signal and authentic signal.} \]

According to the above analysis, the following conclusions can be obtained:

\[ \begin{align*}
\Delta \tau &= D, \ \eta = 30, \text{ Successful spoofing} \\
\text{if } (D < -4d), \ &D < \Delta \tau < -4d, \ \eta \gg 30, \text{ Successful spoofing} \\
\text{if } (D < -4d), \ &-4d \leq \Delta \tau < 0, \ \eta \gg 30, \text{ Successful spoofing} \\
\text{if } (D > -4d), \ &-4d \leq \Delta \tau < D, \ \eta \ll 30, \text{ Spoofing failed} \\
\text{if } (D > -4d), \ &\Delta \tau < -4d, \ \eta \ll 30, \text{ Spoofing failed}
\end{align*} \]

Equation (9) will be described below. When the retransmitted spoofing signal reaches a receiver loop, when the code phase difference between it and the authentic signal is \( \Delta \tau = D \), the power gain of the spoofing signal is 30 dB. At this time, forwarding spoofing can be realized. Since the receiver is in the critical state of losing lock, it can also be called critical spoofing; this is also critical power forwarding spoofing. However, there are two cases in which the spoofing signal lags behind the authentic signal delay; that is, the correlation peaks of the two still overlap and do not overlap, as shown in Figure 4a,b.

The phase difference between the forwarding spoofing signal and authentic signal is usually less than 0, and when the phase difference is greater than \(-4d\), the correlation peaks of the two will overlap. Therefore, if \( D < -4d \), when code phase difference \( \Delta \tau \) is between \( D \) and \(-4d\), there is no overlap between the correlation peak of the spoofing signal and the correlation peak of the authentic signal; that is, the spoofing signal does not generate correlation interference with the authentic signal, but because the power gain \( \eta \) of the spoofing signal is much higher than 30 dB, the loop can be unlocked and the spoofing signal can be recaptured, and the spoofing is successful, that is, the situation in Figure 4b.

If \( D < -4d \), when code phase difference \( \Delta \tau \) is between \(-4d \) and 0, the correlation peak of spoofing signal and correlation peak of authentic signal still overlap; that is, the spoofing signal can generate correlation interference to the authentic signal, and the power gain \( \eta \) of the spoofing signal is much higher than 30 dB, and then the loop can be unlocked and spoofing signal can be recaptured, and spoofing is successful, that is, the situation in Figure 4a.

If \( D > -4d \), when code phase difference \( \Delta \tau \) is between \(-4d \) and \( D \), the correlation peak of spoofing signal and correlation peak of authentic signal still overlap; that is, the spoofing signal can generate correlation interference to the authentic signal, but the power
gain $\eta$ of spoofing signal is much lower than 30 dB, and then spoofing fails, that is, the situation in Figure 4c.

If $D > -4d$, when code phase difference $\Delta \tau$ is less than $-4d$, there is no overlap between the correlation peak of the spoofing signal and correlation peak of the authentic signal; that is, the spoofing signal does not generate correlation interference with the authentic signal, and the power gain $\eta$ of the spoofing signal is much lower than 30 dB, and then spoofing fails, that is, the situation in Figure 4c.

According to the above analysis, it is possible to obtain the schematic diagram of the action range of different spoofing effects of a forwarding spoofing device that uses an omnidirectional antenna to broadcast spoofing signals. The three-dimensional and two-dimensional plane schematic diagrams are shown in Figure 5(top), (bottom), respectively.

![Three-dimensional schematic diagram](image1)

![Two-dimensional schematic diagram](image2)

**Figure 5.** Three-dimensional schematic diagram (top) and two-dimensional schematic diagram (bottom) of action scope of different spoofing effects.

As shown in Figure 5(top), when a victim receiver is located on the red surface, the spoofer can realize successful critical spoofing on it and define the red surface position as a critical spoofing area. When a victim receiver is located in the green area, the spoofer can
successfully cheat it. When a victim receiver is located in the blue area, the spoofer cannot realize any kind of spoofing.

As shown in Figure 5(bottom), when a victim receiver is located on the red line, the spoofer can realize successful critical spoofing on it and define the red line position as a critical spoofing area. When a victim receiver is located in the green area, the spoofer can successfully cheat it. When a victim receiver is located in the blue area, the spoofer cannot cheat it.

4. Forwarding Spoofer Area Deployment Algorithm for MSMT

According to the spoofing purpose of a spoofer to the group of multiple receivers, we propose two forwarding spoofer area deployment algorithms for MSMT scenarios. The first is the multi-target same-point spoofing algorithm (MSPSA), and the second is the multi-target different-point spoofing algorithm (MDPSA). The scenarios are all conducted in a two-dimensional plane. In actual spoofing, it is impossible for the spoofer to be infinitely far away from receivers. It is assumed that the possible deployment location of a spoofer is also limited; that is, we demarcate all spoofers and receivers within a given geometric area \( RE \), which is also a given area of the spoofing scene. At this time, the deployment location of a spoofer can only be selected within a given area.

4.1. MSPSA for Group Multiple Receivers

In this scenario, a spoofer expects to spoof the positioning results of six receivers located at different positions in the group to the same spoofing point \( P_f \). We define this situation as “same-point spoofing”. To achieve the purpose of spoofing, according to Section 2.1, at this time, a spoofer can cheat multiple receivers at the same time through a forwarding spoofer. The MSPSA applicable to this scenario will be described in detail below.

Step 1: it is assumed that a spoofer obtains the positions of the six victim receivers in the group by radar observation, which are expressed as \( P_r_1, P_r_2, \cdots, P_r_6 \).

Step 2: a unique circle can be determined according to the three noncollinear points on the plane. Among the six victim receivers, any three receivers located in noncollinear positions \( P_r_1, P_r_2, \) and \( P_r_3 \) can be selected. Taking these three receivers as points on the circle, a unique circle can be formed. According to the principle of permutation and combination, if any three receivers in the group are not collinear, there will be \( W = \binom{6}{3} = \frac{6!}{3!(6-3)!} = 20 \) combinations.

Take one of the combinations, \( i \), as an example. It is assumed that in combination \( i \), three receivers \( P_r_1, P_r_2, \) and \( P_r_3 \) form a circle, which is defined as the forwarding spoofing circle \( C_1 \). In fact, this is a forwarding spoofing circle formed by a single GNSS forwarding spoofing device deployed in \( P_f \), as shown in Figure 5(bottom). \( P_f \) is also the center position of the forwarding spoofing circle \( C_1 \). The victim receivers located on the circle will be subjected to critical spoofing, while receivers located inside the circle will be subjected to higher-power forwarding spoofing. To improve the concealment of spoofing, the spoofer obviously prefers that victim receivers are all located at the critical spoofing position because this requires the minimum power to realize forwarding spoofing; it is considered here that forwarding signals will hardly affect the receiver located outside the circle.

Step 3: calculate the positional relationship between the remaining three receivers located at \( P_r_4, P_r_5, \) and \( P_r_6 \) and the spoofing circle \( C_1 \). If one of the remaining three receivers is located on the spoofing circle \( C_1 \), it will be subjected to critical spoofing by the spoofing device located at \( P_f \). If there is one located within spoofing circle \( C_1 \), it will be spoofed by higher-power forwarding spoofing by a spoofer located at \( P_f \). If there is one outside spoofing circle \( C_1 \), it will not be affected by the spoofer at \( P_f \).

Step 4: according to the judgment in step 3, there will be the following four situations.

(1) Case 1: among the remaining three receivers, three are outside spoofing circle \( C_1 \). The unique spoofing circle \( C_2 \) is formed by three noncollinear receivers, \( P_r_4, P_r_5, \) and
other than spoofing circle \( C_1 \), which is formed by a single GNSS forwarding spoofing device deployed in \( P_{72} \), as shown in Figure 6.

![Figure 6. Schematic diagram of forwarding spoofer deployment in MSPSA.](image)

Subsequently, it is determined that the three receivers located at \( P_{11}, P_{22}, \) and \( P_{33}, \) other than the receivers located at \( P_{44}, P_{55}, \) and \( P_{66}, \) intersect with spoofing circle \( C_1 \) and spoofing circle \( C_2 \). The equation is expressed as (10); \( d_{2i} \) and \( d_{1i} \), respectively, represent the distances from the center \( (x_2, y_2) \), \( (x_1, y_1) \) of the corresponding spoofing circle to the \( i \)th receiver. When the receiver is located on spoofing circle \( C_2 \), the spoofing fails because of signal crosstalk with spoofing circle \( C_1 \). When the receiver is located inside spoofing circle \( C_2 \), spoofing fails in the same way. When the receiver is outside spoofing circle \( C_2 \) and on spoofing circle \( C_1 \), the receiver is critically spoofed. When the receiver is outside spoofing circle \( C_2 \) and within spoofing circle \( C_1 \), the receiver is spoofed by higher-power forwarding spoofing.

\[
\begin{cases}
    d_{2i} = R_2, & \text{Spoofing failed} \\
    d_{2i} < R_2, & \text{Spoofing failed} \\
    (d_{2i} > R_2) \& \& (d_{1i} = R_1), & \text{Critical spoofing} \\
    (d_{2i} > R_2) \& \& (d_{1i} < R_1), & \text{Higher power forwarding spoofing}
\end{cases}
\] (10)

Thus, the deployment positions of the two spoofers are determined, and the spoofing situations of the receivers are obtained.

(2) Case 2: two of the remaining three receivers are outside spoofing circle \( C_1 \). ① When the two receivers \( P_{45} \) and \( P_{66} \) form a spoofing circle, spoofing circles \( C_2 \) and \( C_3 \) pass through the two receivers respectively.

Spoofing circle \( C_2 \) is determined by the optimal programming algorithm. First, the center \( (x_2, y_2) \) of spoofing circle \( C_2 \) is on the perpendicular line of line segment \( P_{45}P_{66} \). Furthermore, to pursue the concealment of a spoofer in the geographical position, the shortest sum of the distances between the center \( (x_2, y_2) \) of spoofing circle \( C_2 \) and all six receivers is taken as the objective function. At the same time, there are two constraints: the first is that the other six receivers cannot intersect with spoofing circle \( C_2 \), and the second is that spoofing circles \( C_2 \) and \( C_1 \) cannot intersect, as shown in Equation (11).

\[
\begin{cases}
    \min f(x_2, y_2) = d_{21} + d_{22} + d_{23} + d_{24} + d_{25} + d_{26} \\
    \text{s.t.} \begin{cases}
    R_2 < d_{31}, R_2 < d_{32}, R_2 < d_{33}, R_2 < d_{34} \\
    R_1 + R_2 < D_{12}
    \end{cases}
\end{cases}
\] (11)

According to Equation (11), the spoofing circle \( C_2 \) can be determined by the optimization programming algorithm.
(3) Case 3: among the remaining three receivers, one receiver located at \( P_{r6} \) is outside spoofing circle \( C_1 \). Spoofing circle \( C_2 \) is determined by the optimal programming algorithm. To pursue the concealment of spoofing in the geographical position, the shortest sum of the distances between the center \((x_2, y_2)\) of spoofing circle \( C_2 \) and all six receivers is taken as the objective function; At the same time, there are two constraints: the first is that the other five receivers cannot intersect with spoofing circle \( C_2 \), and the second is that spoofing circles \( C_2 \) and \( C_1 \) cannot intersect, as shown in Equation (12).

\[
\begin{align*}
\min f(x_2, y_2) &= d_{21} + d_{22} + d_{23} + d_{24} + d_{25} + d_{26} \\
\text{s.t.} \quad &R_2 < d_{31}, R_2 < d_{32}, R_2 < d_{33}, R_2 < d_{34}, R_2 < d_{35} \\
& R_1 + R_2 < D_{12}
\end{align*}
\]

According to Equation (12), spoofing circle \( C_2 \) can be determined by the optimization programming algorithm.

(4) Case 4: among the remaining three receivers, 0 is outside spoofing circle \( C_1 \). In this case, there is only one spoofer, and the relationship between the six victim receivers and spoofing circle \( C_1 \) is clear.

Step 5: steps 2–4 are all about combination \( i \). At this time, all combinations are traversed. After all the above combinations are processed, the following four indexes, SN, \( \sum d_{nm}^{Tr} \), CSR, and SSR, are proposed as the performance criteria for judging a spoofer deployment scheme:

1. SN: number of GNSS forwarding spoofers used;
2. \( \sum d_{nm}^{Tr} \): the sum of the distances from each spoofer to each victim receiver;
3. CSR: critical spoofing rate (CSR), the proportion of critical spoofed receiver to the number of all spoofed receivers;
4. SSR: spoofing success rate (SSR), the proportion of spoofed receivers in the total number of receivers.

In MSPSA, the above four indexes will be calculated.

It is easy to understand that from the perspective of the equipment costs of a spoofer, it is expected that the less the index 1, the better. From the concealment of spoofing in geographical space, index 2 is the sum of all elements of \( D_{Tr} \) in (13), where \( d_{nm}^{Tr} \) represents the straight-line distance from the \( n \)th spoofing device to the \( m \)th victim receiver, and the larger the better. Index 3 is used to evaluate the concealment degree of spoofing performed by spoofer. The higher the CSR is, the more the spoofed receivers are subjected to critical spoofing. Index 4 is used to evaluate the success rate of spoofing task completed by spoofing device. The higher the SSR, the more receivers are successfully spoofed.

\[
D_{Tr} = \begin{bmatrix}
d_{11}^{Tr} & \cdots & d_{1m}^{Tr} & \cdots & d_{1n}^{Tr} \\
\vdots & \ddots & \vdots & \ddots & \vdots \\
d_{m1}^{Tr} & \cdots & d_{nm}^{Tr} & \cdots & d_{mn}^{Tr} \\
\vdots & \ddots & \vdots & \ddots & \vdots \\
d_{n1}^{Tr} & \cdots & d_{nm}^{Tr} & \cdots & d_{nn}^{Tr}
\end{bmatrix}
\]

However, the importance of the four indexes will not be ranked here, which will be determined by the intention of spoofer. This means that spoofers will decide which deployment scheme to choose according to their specific actual needs, and MSPSA will provide all possible deployment schemes and corresponding indexes for a spoofer to choose.

According to the above detailed description of the algorithm steps, the key flow of MSPSA is given, as shown in Figure 7.
However, the importance of the four indexes will not be ranked here, which will be determined by the intention of spoofer. This means that spoofer will decide which deployment scheme to choose according to their specific actual needs, and MSPSA will provide all possible deployment schemes and corresponding indexes for a spoofer to choose.

According to the above detailed description of the algorithm steps, the key flow of MSPSA is given, as shown in Figure 7.

**Figure 7.** MSPSA execution flow chart.

### 4.2. MDPSA for Group Multiple Receivers

In this scenario, a spoofer expects to spoof the positioning results of six victim receivers located at different positions $P_{r1}, P_{r2}, \ldots, P_{r6}$ in the group to different spoofing points $P_{f1}, P_{f2}, \ldots, P_{f6}$, while maintaining the relative positional relationship between the real positions of the receivers among these spoofing points. This situation is defined as “different-point spoofing”. To achieve the purpose of spoofing, according to Section 2.1, at this time, a spoofer needs to deploy six GNSS forwarding spoofing devices to spoof multiple receivers at the same time; that is, a single spoofing device only completes the spoofing of one receiver because this is “different-point spoofing”. The regional deployment algorithm applicable to this scenario will be described in detail below.

Step 1: it is assumed that a spoofer obtains the positions of the six victim receivers in the group by radar observation, which are expressed as $P_{r1}, P_{r2}, \ldots, P_{r6}$.
Step 2: each spoofer spoofs one receiver, corresponding to the receiver located at \( P_1 \). A single GNSS forwarding spoofer deployed at \( P_1 \) forms forwarding spoofing circle \( C_1 \), as shown in Figure 5 (bottom). \( P_1 \) is the center position of forwarding spoofing circle \( C_1 \). The receiver located at \( P_1 \) will be subjected to critical spoofing. Similarly, the receiver located inside the circle will be subjected to higher-power forwarding spoofing. The receiver outside circle will not be affected by a signal broadcast by a spoofer. Therefore, corresponding to the six victim receivers, the six spoofers will form six forwarding spoofing circles, \( C_1, C_2, \cdots, C_6 \), as shown in Figure 8.

\[
\begin{align*}
\text{Schematic diagram of forwarding spoofer deployment in MDPSA.} \\
\text{Step 3: the restriction conditions of six forwarding spoofing circles need to be considered. On the one hand, for any one of the forwarding spoofing circles } C_m, \\
\text{except for the receiver located in } P_{1m} \text{ that it is responsible for spoofing, no victim receiver in other areas can intersect with forwarding spoofing circle } C_m; \\
\text{otherwise, it will obviously cause unnecessary signal collision to the spoofing of other receivers and lead to possible spoofing failure. On the other hand, all spoofers are deployed in a given area } RE, \text{ as shown in Equation (14).} \\

\begin{align*}
P_{11} & \in C_1, P_{12}, P_{13}, \cdots, P_{16} \not\subset C_1 \\
P_{12} & \in C_2, P_{11}, P_{13}, P_{14}, \cdots, P_{16} \not\subset C_2 \\
& \cdots \\
P_{16} & \in C_5, P_{11}, P_{12}, \cdots, P_{15} \not\subset C_6 \\
P_{11}, P_{12}, \cdots, P_{16} & \subseteq RE \tag{14}
\end{align*}
\]

Step 4: after the above restrictions are given, we still take the SN, \( \sum d_{nm}^T \), CSR, and SSR proposed in MSPSA as the performance criteria for evaluating the spoofing deployment scheme. However, it should be noted that SN = 6, CSR = 100%, and SSR = 100% are easy to achieve in different-point spoofing. Therefore, we take index \( \sum d_{nm}^T \) as the objective function and take \( x \) as the constraint condition to optimize the solution.

According to the above detailed description of the algorithm steps, we give the key processes of MDPSA, as shown in Table 1.
Table 1. Process of MDPSA.

| MDPSA Different-Point Spoofing Algorithm for Group of Multiple Receivers |
|---------------------------------------------------------------|
| **Input positions of 6 victim receivers:** P_r1, P_r2, ⋅⋅⋅, P_r6 |
| Form 6 forwarding spoofing circles: C_1, C_2, ⋅⋅⋅, C_6: (x - x_{P^r_i})^2 + (y - y_{P^r_i})^2 = |P^r_i - P^r_i|^2 |
| Satisfy the constraints: |
| \[ P^r_1 \subseteq C_1, P^r_2, P^r_3, \ldots, P^r_6 \notin C_1 \] |
| \[ P^r_2 \subseteq C_2, P^r_1, P^r_3, P^r_4, \ldots, P^r_6 \notin C_2 \] |
| \[ \ldots \] |
| \[ P^r_6 \subseteq C_6, P^r_1, P^r_2, \ldots, P^r_5 \notin C_6 \] |
| \[ P^r_1, P^r_2, \ldots, P^r_6 \subseteq RE \] |
| Objective \( \max(\sum_{i=1}^{6} d_{Tr_{nm}}^i) \), execute optimal algorithm |
| Calculate 4 indexes SN, \( \sum_{i=1}^{6} d_{Tr_{nm}}^i \), CSR, SSR |
| Get the best deployment scheme of spoofing |

5. Experimental Analysis of Different MSMT Spoofing Scenarios

To fully verify and evaluate the performance of forwarding spoofer area deployment algorithms MSPSA and MDPSA for MSMT, the same-point spoofing experiment and different-point spoofing experiment on multiple receivers in the group are carried out in Sections 5.1 and 5.2, respectively. The experiment is carried out on a self-developed spoofing software platform based on MATLAB. In the software platform, if the same-point spoofing or different-point spoofing is selected according to the two-dimensional coordinates of the victim receiver input, the MSPSA algorithm and the MDPSA algorithm are executed respectively. All mathematical models of these two algorithms are introduced in detail in Sections 4.1 and 4.2 for repeatable research. After the implementation of the algorithm, the software finally gives the best deployment scheme of the spoofer according to the spoofer’s spoofing purpose and each scheme’s indexes.

5.1. Same Point Spoofing Experiments on Multiple Receivers in Group

In the experimental scenario, the spoofer intends to spoof all six receivers to the same spoofing point \( P^f_1 \), and the plane coordinates of \( P^f_1 \) are (1018, 1015). The spoofer obtains the positions of six victim receivers in the group \( P^r_1, P^r_2, \ldots, P^r_6 \), and the corresponding plane coordinates are shown in Table 2.

Table 2. Two-dimensional coordinates of victim receivers in MSPSA.

| Victim Receiver | X (m) | Y (m) |
|-----------------|-------|-------|
| \( P^r_1 \)     | 812   | 376   |
| \( P^r_2 \)     | 512   | 735   |
| \( P^r_3 \)     | 312   | 838   |
| \( P^r_4 \)     | 512   | 212   |
| \( P^r_5 \)     | 1012  | 370   |
| \( P^r_6 \)     | 812   | 648   |

After implementing the MSPSA algorithm proposed in Section 4.1, 25 deployment schemes will be given. Next, according to the different needs of the spoofer, the most suitable deployment scheme of the spoofer is obtained through analysis and comparison.

(1) When the spoofer expects to use the least number of spoofing devices to complete spoofing, there will be the following two schemes. The specific schemes and their performance indexes are shown in Table 3.

Table 3. Deployment scheme and various performance indexes when expect least spoofing devices.

| Scheme Number | SR | Number of Critical Spoofed Receivers | Number of Higher Power Forwarding Spoofed Receivers | \( \sum_{i=1}^{6} d_{Tr_{nm}}^i \) (m) | CSR | SSR |
|---------------|----|-------------------------------------|----------------------------------------------------|-------------------------------------|-----|-----|
| 1             | 1  | 3                                   | 3                                                  | 1890.8                              | 50% | 100%|
| 2             | 1  | 3                                   | 3                                                  | 3815.6                              | 50% | 100%|
According to Table 3, when the number of spoofers is one, compared with the above two schemes, the total distance $\sum d_{\text{in}}^{\text{TR}}$ between the spoofer and each receiver in scheme 2 is larger, $\sum d_{\text{in}}^{\text{TR}} = 3815.6$ m, and the deployment diagram of scheme 2 is shown in Figure 9.

![Figure 9. Deployment diagram of spoofers with the least-spoofing device.](image)

$RE$ refers to the allowable deployment range of the spoofer mentioned at the beginning of Section 4. Therefore, when a spoofer expects to use the least number of spoofing devices to complete spoofing, we think it is best to choose scheme 2 in Table 3.

(2) When a spoofer expects the total distance $\sum d_{\text{in}}^{\text{TR}}$ between each spoofer and each receiver to be the largest, we list all schemes with $\sum d_{\text{in}}^{\text{TR}} > 21$ km and their performance indexes in Table 4.

| Scheme Number | SR | Number of Critical Spoofed Receivers | Number of Higher Power Forwarding Spoofed Receivers | $\sum d_{\text{in}}^{\text{TR}}$ (m) | CSR | SSR |
|---------------|----|-------------------------------------|---------------------------------------------------|---------------------------------|-----|-----|
| 1             | 3  | 5                                   | 1                                                 | 40,345.1                        | 83.3% | 100% |
| 2             | 3  | 5                                   | 1                                                 | 40,276.4                        | 83.3% | 100% |
| 3             | 3  | 5                                   | 1                                                 | 35,800.2                        | 83.3% | 100% |
| 4             | 3  | 5                                   | 1                                                 | 25,147.7                        | 83.3% | 100% |
| 5             | 3  | 5                                   | 1                                                 | 24,342.8                        | 83.3% | 100% |
| 6             | 3  | 5                                   | 1                                                 | 22,991.1                        | 83.3% | 100% |
| 7             | 2  | 4                                   | 2                                                 | 22,212.4                        | 66.7% | 100% |
| 8             | 2  | 5                                   | 1                                                 | 21,928.1                        | 83.3% | 100% |

The eight schemes in Table 4 have the largest $\sum d_{\text{in}}^{\text{TR}}$ among all 25 schemes. Although a spoofer mainly pursues $\sum d_{\text{in}}^{\text{max}}$ at this time, it should be noted that the number of spoofing devices used in schemes 7 and 8 in Table 4 is 2, and the cost of the spoofing devices is lower than that of schemes 1 to 6. However, at the same time, the CSR of scheme 7 is reduced to 66.7%, that is, concealment of spoofing becomes worse. Although the CSR of scheme 8 is still 83.3%, but $\sum d_{\text{in}}^{\text{TR}} = 21,928.1$ m, compared with schemes 1 and 2, the $\sum d_{\text{in}}^{\text{TR}}$ of scheme 8 is significantly reduced, which makes it difficult to meet the requirements of the spoofer. The deployment diagrams of schemes 1 and 2 are shown in Figure 10,a,b.
Figure 10. Deployment diagram of spoofers with the largest distance sum.

Figure 10a,b show that three spoofers spoofed six receivers, five of which suffered critical spoofing and one of which suffered higher power forwarding spoofing.

Therefore, when a spoofer expects the sum $\sum d_{nm}$ of the distances between each spoofer and each receiver to be the largest, we think that it is best to select schemes 1 and 2 in Table 4.
(3) When a spoofer pursues the max of CSR and SSR at the same time, the number of spoofing devices are kept at two through statistics. Therefore, we list the deployment scheme and its performance indexes that satisfy CSR = 100% and SSR = 100% in Table 5.

Table 5. Deployment scheme and various performance indexes when expect max of CSR and SSR.

| Scheme Number | SR | Number of Critical Spoofed Receivers | Number of Higher Power Forwarding Spoofed Receivers | $\sum d_{nm}^{Tr} (m)$ | CSR  | SSR  |
|---------------|----|-------------------------------------|--------------------------------------------------|------------------------|------|------|
| 1             | 2  | 6                                   | 0                                                | 13,803.5               | 100% | 100% |
| 2             | 2  | 6                                   | 0                                                | 5199.7                 | 100% | 100% |

The two schemes in Table 5 ensure that the CSR and SSR are 100% in all 25 schemes (in this case, the number of spoofers must be two). On the basis of meeting the needs of a spoofer, we consider ensuring that $\sum d_{nm}^{Tr}$ reaches the maximum. Obviously, scheme 1 and scheme 2 in Table 5 reach the max $\sum d_{nm}^{Tr} = 13,803.5$ m and the sub max $\sum d_{nm}^{Tr} = 5199.7$ m of $\sum d_{nm}^{Tr}$, respectively. The deployment of scheme 1 and scheme 2 are shown in Figure 11a,b.

Therefore, when a spoofer pursues the max CSR and SSR at the same time, we think it is very appropriate to choose scheme 1 and scheme 2 in Table 5.

Figure 11. Cont.
5.2. Different-Point Spoofing Experiments on Multiple Receivers in Group

In the experimental scenario, the spoofer intends to spoof six receivers to different spoofing points \( P_{f1}, P_{f2}, \ldots, P_{f5} \). The spoofer obtains the positions of the six victim receivers in the group, \( P_{r1}, P_{r2}, \ldots, P_{r5} \), and the corresponding plane coordinates are shown in Table 6.

| Victim Receiver | X (m)  | Y (m)  |
|-----------------|-------|-------|
| \( P_{r1} \)    | 11    | 11    |
| \( P_{r2} \)    | 511   | −639  |
| \( P_{r3} \)    | 911   | 11    |
| \( P_{r4} \)    | 511   | 711   |
| \( P_{r5} \)    | −239  | 811   |
| \( P_{r6} \)    | −229  | 1011  |

After executing the MDPSA algorithm proposed in Section 4.2, the following deployment scheme is given. The plane coordinates and action radius of each spoofer are shown in Table 7.

| Victim Receiver | X (m)  | Y (m)  | Action Radius |
|-----------------|-------|-------|---------------|
| \( P_{T1} \)    | −1106.3 | −626.5 | 1286.3        |
| \( P_{T2} \)    | 993.7  | −1500 | 987.1         |
| \( P_{T3} \)    | 3000   | 1293.5 | 2451.3       |
| \( P_{T4} \)    | 225.7  | 910.8 | 348.3         |
| \( P_{T5} \)    | −397.8 | 684.6 | 202.9         |
| \( P_{T6} \)    | −1500  | 3000  | 2360.4        |

The performance indexes of the deployment scheme are shown in Table 8.
Table 8. Deployment scheme and various performance indexes in MDPSA.

| Scheme Number | SR | Number of Critical Spoofed Receivers | Number of Higher Power Forwarding Spoofed Receivers | $\sum d_{\text{max}}^T$ (m) | CSR | SSR |
|---------------|----|-------------------------------------|----------------------------------------------------|-----------------------------|-----|-----|
| 1             | 6  | 6                                   | 0                                                  | 70,106.4                    | 100%| 100%|

The deployment diagram of scheme 1 is shown in Figure 12.

Figure 12. Schematic diagram of spoofing device deployment for different spoofings.

According to the scheme in Table 7, six spoofing devices will be deployed at this time, all six receivers will be subjected to critical spoofing, and the CSR and SSR will reach 100%. At this time, $\sum d_{\text{max}}^T$ will reach the max of 70,106.4 m, so this will be the best spoofing deployment scheme given.

In our MSPSA and MDPSA algorithms, for the same-point spoofing, when the spoofer expects to use the least spoofer to complete spoofing, one spoofer can complete spoofing, and the total distance between the spoofer and the receiver is 3815.6 m, and CSR and SSR are 50% and 100%, respectively. When a spoofer expects the maximum total distance between the spoofer and the receiver, five spoofers can be used to complete spoofing, and the total distance between the spoofer and the receiver is 40,345.1 m, and CSR and SSR are 83.3% and 100%, respectively. When the spoofer expects the CSR and SSR to be the maximum together, six spoofers can be used to complete spoofing. The total distance between the spoofer and the receiver is 13,803.5 m, and the CSR and SSR are 100% and 100%, respectively.

For the different-point spoofing, the deceiver uses six cheaters to complete the deception, and the total distance between the cheater and the receiver will reach the maximum of 70,106.4 m, with CSR and SSR of 100% and 100%, respectively.

The algorithm we proposed is based on the scope of the forwarding spoofing and realizes same-point spoofing and different-point spoofing. According to the different purposes of the spoofer, such as the minimum number of spoofers, the maximum distance between the spoofer and the receiver, and the maximum CSR and SSR together, the optimal spoofer deployment scheme is given.
6. Conclusions and Future Work

To realize effective distributed forwarding spoofing for multiple receiver sensors in the area, we have done some useful research work. (1) The research status and key problems of distributed GNSS forwarding spoofing are summarized; (2) the forwarding spoofing model of GNSS is established, including a forwarding spoofing mathematical model and asynchronous traction spoofing method; (3) the scope of action of forwarding spoofing is evaluated in detail, and the schematic diagram of the scope of action of different spoofing effects is given; (4) two forwarding spoofer area deployment algorithms for MSMT are proposed—MSPSA is suitable for the same-point spoofing of multiple receiver sensors, and MDPSA is suitable for the different-point spoofing of multiple receiver sensors; and (5) the experimental tests of MSPSA and MDPSA for MSMT are carried out. The experimental results show that MSPSA and MDPSA can give the most appropriate deployment scheme of spoofing according to the different spoofing needs of spoofers, and the performance of the deployment scheme can meet the needs of spoofers.

Future work will be carried out from the following three aspects: (1) when the number of receivers in the area is larger and the types are different, it is necessary to explore more effective distributed spoofer deployment algorithms; (2) the area where the receiver is deployed may be at low altitude, which will bring many challenges to the deployment of spoofers—it is necessary to research the distributed spoofer deployment algorithm under low altitude conditions; and (3) when multiple receiver sensors in the area have certain anti-spoofing techniques, the spoofing strategy of a spoofing device needs to be adjusted flexibly, and the distributed spoofing device deployment algorithm for multiple anti-spoofing receivers needs to be explored.

Author Contributions: Methodology, Y.G.; writing—original draft preparation, Y.G.; writing—review and editing, Y.G. and G.L. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the State Key Laboratory of Geo-Information Engineering, grant number SKLGIE2020-Z-2-1.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data used in this research are not publicly available.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Zhou, M.; Li, H.; Wang, C.; Ma, T.; Lu, M. Induced spoofing detection of global navigation satellite system. *J. Natl. Univ. Def. Technol.* **2019**, *41*, 7.
2. Guo, Y.; Wu, M.; Tang, K.; Tie, J.; Li, X. Covert Spoofing Algorithm of UAV based on GPS/INS Integrated Navigation. *IEEE Trans. Veh. Technol.* **2019**, *68*, 6557–6564. [CrossRef]
3. Huang, K.; Wang, H. Combating the Control Signal Spoofing Attack in UAV Systems. *IEEE Trans. Veh. Technol.* **2018**, *67*, 7769–7773. [CrossRef]
4. Xinran, Z.H.; Hong, L.I.; Chun, Y.A.; Mingquan, L.U. Influence of spoofing interference on GNSS vector tracking loop. *J. Tsinghua Univ. (Sci. Technol.)* **2021**, *62*, 163–171.
5. Zhou, M.; Li, H.; Lu, M. Calculation of the lower limit of the spoofing-signal ratio for a GNSS receiver-spoofer. *EURASIP J. Wirel. Commun. Netw.* **2018**, *2018*, 44. [CrossRef]
6. Humphreys, T.E.; Ledvina, B.M.; Psiaki, M.L.; O’Hanlon, B.W.; Kintner, P.M. Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofor. In Proceedings of the 21st International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS 2008), Savannah Convention Center Savannah, Savannah, GA, USA, 16–19 September 2008; pp. 1169–1180.
7. Zhang, H.S.; Gao, G.G.; Kou, L. Deception jamming technology of GPS based on the track induction method. *J. Proj. Rocket. Missiles Guid.* **2013**, *33*, 149–152.
8. Wang, S.; Gao, J.; Wang, Y.; Liu, J.; Li, H. GPS repeater deception jamming technology based on delay control. *Missiles Space Veh.* **2017**, *2*, 4.
9. Huang, L.; Lu, Z.; Ren, C.; Liu, Z.; Xiao, Z.; Song, J.; Li, B. Research and Simulation of Intelligent Repeater Deception Jamming Technology Based on Low Earth Orbit Satellite Platform. In Proceedings of the 9th China Satellite Navigation Conference, Beijing, China, 9 July 2018; pp. 39–43.
10. Liu, Y.; Su, W.; Yan, S. Efficiency analysis of repeater deception jamming GPS repeater. *J. Air Force Radar Acad.* 2004, 18, 4–6.
11. Shi, P.; Wang, X.; Xue, R. Research on power control strategy of GNSS repeater deception jamming. *Mod. Navig.* 2021, 12, 11.
12. Bitner, T.; Preston, S.; Bevly, D. Multipath and Spoofing Detection Using Angle of Arrival in a Multi-Antenna System. *Proc. Int. Tech. Meet. Inst. Navig.* 2015, 822–832.
13. Zhang, X.; Pang, J.; Su, Y.; Ou, G. Spoofing detection technique on antenna array carrier phase double difference. *J. Natl. Univ. Def. Technol.* 2014, 36, 6.
14. Fan, G.G.; Huang, Y.B.; Wu, W.; Zhu, X.W.; Sun, G.F. Detection of spoofing threats by inertial assisted three elements antenna. *J. Natl. Univ. Def. Technol.* 2017, 39, 5.
15. Wang, Z.; Li, H.; Zhou, Z.; Lu, M. A direction finding method of the GNSS spoofer for commercial receivers. *SCIENTIA SINICA Inf.* 2022, 52, 17.
16. Yang, J.S.; Zeng, F.L.; Sheng, H.; Zhu, L.X. A Jamming System Through Section Mapping for GPS Navigation. *Acta Electron. Sin.* 2005, 6, 1036–1038.
17. Tippenhauer, N.O.; Pöpper, C.; Rasmussen, K.B.; Capkun, S. On the requirements for successful GPS spoofing attacks. *Comput. Commun. Secur.* 2011, 75–86. [CrossRef]
18. He, T. Improvement of the method of GNSS retransmission deception interference model. *Bull. Surv. Mapp.* 2019, 4, 71.
19. Zhang, S.; Yang, J.; Pan, G.; Dong, T. Station embattling optimization and moving model of the GPS area-mapping deceiving units battlefield navigation integrative system. *J. Univ. Sci. Technol. China* 2011, 41, 746–752.
20. Xie, G. Principles of GPS and Receiver Design. *Publ. House Electron. Ind.* 2009, 7, 61–63.
21. Gao, Y.; Lv, Z.; Zhang, L. Asynchronous Lift-Off Spoofing on Satellite Navigation Receivers in the Signal Tracking Stage. *IEEE Sens. J.* 2020, 20, 8604–8613. [CrossRef]
22. Yan, Z.; Wang, X. Effecting of Spoofing Signal on Carrier Loop of GNSS Receiver. *Mod. Navig.* 2017, 6, 25–30.